Copyright
© 2007 Secure Computing Corporation. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of Secure Computing Corporation.

Trademarks

Software License Agreement
The following is a copy of the Software License Agreement as shown in the software:

CAREFULLY READ THE FOLLOWING TERMS AND CONDITIONS BEFORE LOADING THE SOFTWARE. THIS AGREEMENT GOVERNS THE USE OF THE SOFTWARE (AS DEFINED BELOW). BY CLICKING “I ACCEPT” BELOW, OR BY INSTALLING, COPYING, OR OTHERWISE USING THE SOFTWARE, YOU ARE SIGNING THIS AGREEMENT, THEREBY BECOMING BOUND BY ITS TERMS. BY INDICATING YOUR AGREEMENT, YOU ALSO REPRESENT AND WARRANT THAT YOU ARE A DULY AUTHORIZED REPRESENTATIVE OF THE ENTITY THAT HAS PURCHASED THE SOFTWARE AND THAT YOU HAVE THE RIGHT AND AUTHORITY TO ENTER INTO THIS AGREEMENT ON THE ENTITY’S BEHALF. IF YOU DO NOT AGREE WITH THIS AGREEMENT, THEN CLICK “I DO NOT ACCEPT” BELOW OR DO NOT USE THE SOFTWARE AND RETURN ALL COPIES OF THE SOFTWARE AND DOCUMENTATION TO SECURE COMPUTING CORPORATION (“SECURE COMPUTING”) OR THE RESELLER FROM WHOM YOU OBTAINED THE SOFTWARE.

1. DEFINITIONS.
1.1 “Documentation” means the published user manuals and documentation that are made available for the Software.
1.2 “Sidewinder Software” means the machine-readable object-code version of Secure Computing's Sidewinder software as indicated on your invoice and any updates or revisions of the Sidewinder Software that you may receive.
1.3 “Software Module” shall mean software applications that Secure Computing licenses to its customers in addition to the Sidewinder Software (for example, without limitation, anti-virus software, anti-spam software and web filtering software) as indicated on your invoice and any updates or revisions of the Software Module that you may receive.
1.4 “Software” shall mean, collectively the Sidewinder Software and, if purchased by you, the Software Module(s).

2. GRANT OF LICENSE. Secure Computing grants to you, and you accept, (a) a non-exclusive, and non-transferable license to use the Sidewinder Software solely on and in conjunction with the Secure Computing appliance on which the Sidewinder Software is installed, and, if purchased by you, (b) a non-exclusive, non-transferable license to use the Software Module(s) for a specific period of time and for the specific number of licensed users as each is indicated on your invoice solely on and in conjunction with the Secure Computing appliance on which the Software Module is installed. Under no circumstances will you receive any source code of the Software. Secure Computing also grants to you, and you accept, a non-exclusive, and non-transferable license to use the Documentation solely in conjunction with the Software.

3. LIMITATION OF USE. You may not: 1) copy, except to make one copy of the Software solely for back-up or archival purposes; 2) transfer, distribute, rent, lease or sublicense all or any portion of the Software or Documentation to any third party; 3) translate, modify, adapt, decompile, disassemble, or reverse engineer any Software in whole or in part; 4) modify or prepare derivative works of the Software or the Documentation; or 5) use the Software to process the data of a third party. You agree to keep confidential and use your best efforts to prevent and protect the contents of the Software and Documentation from unauthorized disclosure or use. Secure Computing reserves all rights that are not expressly granted to you.

4. DISCLAIMER OF WARRANTIES. Secure Computing does not warrant that the functions contained in the Software will meet your requirements or that operation of the program will be uninterrupted or error-free. The entire risk as to the results and performance of the Software is assumed by you. THE SOFTWARE IS FURNISHED, “AS IS” WITHOUT ANY WARRANTY OF ANY KIND, AND SECURE COMPUTING AND ITS LICENSORS HEREBY DISCLAIM ALL WARRANTIES, EXPRESS, IMPLIED OR STATUTORY IN RESPECT OF THE SOFTWARE INCLUDING, WITHOUT LIMITATION, ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND ANY WARRANTIES AS TO NON-INFRINGEMENT. SOME STATES AND COUNTRIES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO THE ABOVE EXCLUSION MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS WHICH VARY BY STATE OR COUNTRY.
5. LIMITATION OF REMEDIES. SECURE COMPUTING'S AND ITS LICENSORS ENTIRE LIABILITY UNDER, FOR
BREACH OF, OR ARISING OUT OF THIS AGREEMENT, IS LIMITED TO A REFUND OF THE PURCHASE PRICE OF THE
PRODUCT OR SERVICE THAT GAVE RISE TO THE CLAIM. IN NO EVENT SHALL SECURE COMPUTING OR ITS
LICENSORS BE LIABLE FOR YOUR COST OF PROCURING SUBSTITUTE GOODS. IN NO EVENT WILL SECURE
COMPUTING OR ITS LICENSORS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, INCIDENTAL,
EXEMPLARY, OR OTHER DAMAGES WHETHER OR NOT SECURE COMPUTING HAS BEEN ADVISED OF THE
POSSIBILITY OF SUCH LOSS OR DAMAGE.

6. TERM AND TERMINATION. This license is effective until terminated. You may terminate it at any time by destroying the
Software, including all computer programs and Documentation, and erasing any copies residing on computer equipment.
This Agreement also will automatically terminate if you do not comply with any terms or conditions of this Agreement. Upon
such termination you agree to destroy the Software and Documentation and erase all copies of the Software residing on
computer equipment. Notwithstanding the foregoing, each license to use a Software Module will automatically terminate on
expiration of its applicable term (as set forth on your invoice) unless it is renewed prior to such termination.

7. PROTECTION OF CONFIDENTIAL INFORMATION. The Software and Documentation are delivered to you on a
confidential basis and you are responsible for employing reasonable measures to prevent the unauthorized disclosure or use
thereof, which measures shall not be less than those measures employed by you in protecting your own proprietary
information. You may disclose the Software or Documentation to your employees as necessary for the use permitted under
this Agreement. You shall not remove any trademark, trade name, copyright notice or other proprietary notice from the
Software or Documentation.

8. OWNERSHIP. The Software and Documentation are licensed (not sold) to you. All intellectual property rights including
trademarks, service marks, patents, copyrights, trade secrets, and other proprietary rights in or related to the Software and
Documentation are and will remain the property of Secure Computing or its licensors, whether or not specifically recognized
or protected under local law. You will not remove any product identification, copyright notices, or other legends set forth on
the Software or Documentation.

9. EXPORT RESTRICTIONS. You agree to comply with all applicable United States export control laws, and regulations,
as from time to time amended, including without limitation, the laws and regulations administered by the United States
Department of Commerce and the United States Department of State. You have been advised that the Software is subject to
the U.S. Export Administration Regulations. You shall not export, import or transfer Software contrary to U.S. or other
applicable laws, whether directly or indirectly, and will not cause, approve or otherwise facilitate others such as agents or any
third parties in doing so. You represent and agree that neither the United States Department of Commerce nor any other
federal agency has suspended, revoked or denied your export privileges. You agree not to use or transfer the Software for
end use relating to any nuclear, chemical or biological weapons, or missile technology unless authorized by the U.S.
Government by regulation or specific license.

10. U.S. GOVERNMENT RIGHTS. Any Software or Documentation acquired by or on behalf of a unit or agency of the United
States Government is “commercial computer software” or “commercial computer software documentation” and, absent a
written agreement to the contrary, the Government's rights with respect to such Software or Documentation are limited by the
terms of this Agreement, pursuant to FAR § 12.212(a) and its successor regulations and/or DFARS § 227.7202-1(a) and its
successor regulations, as applicable.

11. ENTIRE AGREEMENT. This Agreement is our offer to license the Software and Documentation to you exclusively on the
terms set forth in this Agreement, and is subject to the condition that you accept these terms in their entirety. If you have
submitted (or hereafter submit) different, additional, or other alternative terms to Secure Computing or any reseller or
authorized dealer, whether through a purchase order or otherwise, we object to and reject those terms. Without limiting the
generality of the foregoing, to the extent that you have submitted a purchase order for the Software, any shipment to you of
the Software is not an acceptance of your purchase order, but rather is a counteroffer subject to your acceptance of this
Agreement without any objections or modifications by you. To the extent that we are deemed to have formed a contract with
you related to the Software prior to your acceptance of this Agreement, this Agreement shall govern and shall be deemed to
be a modification of any prior terms in their entirety.

12. GENERAL. Any waiver of or modification to the terms of this Agreement will not be effective unless executed in writing
and signed by Secure Computing. If any provision of this Agreement is held to be unenforceable, in whole or in part, such
holding shall not affect the validity of the other provisions of this Agreement. You may not assign this License Agreement or
any associated transactions without the written consent of Secure Computing. This License Agreement shall be governed by
and construed in accordance with the laws of California, without regard to its conflicts of laws provisions.
Other Terms and Conditions

This product includes software developed by Cavium Networks. Copyright © 2003-2005 Cavium Networks (support@cavium.com). All rights reserved.

This product includes software developed by Tarari, Inc. Copyright © 2003-2007 Tarari, Inc. All rights reserved.

This product includes software and algorithms developed by RSA Data Security Inc., including the RSA Data Security, Inc. MDS Message Digest Algorithm.


This product contains software developed by the Net-SNMP project. Copyright © 1989, 1991, 1992 by Carnegie Mellon University. Copyright © 2001-2003, Networks Associates Technology, Inc. All rights reserved. Portions of this code are copyright © 2001-2003, Cambridge Broadband Ltd. All rights reserved. Portions Copyright © Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, USA, All rights reserved. Portions Copyright © 2003-2006 Sparta, Inc. All rights reserved. Portions Copyright © 2004 Cisco, Inc and Information Network Center of Beijing University of Posts and Telecommunications, All rights reserved. Portions Code are copyright © 2003 Fabaosof R&D Software GmbH & Co KG.


This product contains software developed by Sendmail, Inc. Copyright © 1998-2006 Sendmail, Inc. All rights reserved.

This product includes software developed by the Python Software Foundation. All rights reserved.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org) Copyright © 1998-2005 The OpenSSL Project. All rights reserved.

This product utilizes MySQL (http://www.mysql.com). Copyright © 1995, 1996, 2000 Tcx AB & Monty Program KB & Detron Stockholm SWEDEN, Helsingfors FINLAND and Uppsala SWEDEN. All rights reserved.

This product incorporates compression code from the Info-ZIP group. There are no extra charges or costs due to the use of this code, and the original compression sources are freely available from http://www.info-zip.org or ftp://ftp.info-zip.org on the Internet.

This product includes software developed at the Information Technology Division, US Naval Research Laboratory. Copyright © 1995 US Naval Research Laboratory (NRL). All Rights Reserved.

This product includes software developed by Computing Services at Carnegie Mellon University (http://www.cmu.edu/computing/). Copyright © 1998-2003 Carnegie Mellon University. All rights reserved.

This product incorporates the Mailshell Anti-Spam SDK, which is Copyright © 1999-2007 Mailshell.

This product incorporates the PCRE library package, which is open source software, written by Philip Hazel, and copyrighted by the University of Cambridge, England.

This product also uses libspf, an implementation of the Sender Policy Framework, which is Copyright © 2004 James Couzens & Sean Comeau All rights reserved.


Redistribution and use in source and binary forms of the above listed software, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.
THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT
LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE
DISCLAIMED. IN NO EVENT SHALL LICENSORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE
GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND
ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR
OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY
OF SUCH DAMAGE.

This product uses unmodified GNU software. GNU source code is available on request by contacting Secure Computing.

Technical Support information
Secure Computing works closely with our reseller partners to offer the best worldwide Technical Support services. Your
Secure Computing reseller is the first line of support when you have questions about our products and services; however, if
you require additional assistance, contact us directly.
• To contact Secure Computing Technical Support directly, telephone +1.800.700.8328 or +1.651.628.1500. If you prefer,
visit http://support.securecomputing.com and file a help ticket.
• To inquire about obtaining a support contract, refer to our "Contact Secure" Web page for the latest information at
• To use the Secure Knowledge Base, go to www.securecomputing.com/supportkb.cfm. Enter your company ID.

Customer Advocate information
To suggest enhancements in a product or service, or to request assistance in resolving a problem, please contact a Customer
Advocate at +1.877.851.9080. If you prefer, send an e-mail to customer_advocate@securecomputing.com.

If you have comments or suggestions you would like to make regarding this document or any other Secure Computing
document, please send an e-mail to techpubs@securecomputing.com.

Printing history

<table>
<thead>
<tr>
<th>Date</th>
<th>Part number</th>
<th>Software release</th>
</tr>
</thead>
<tbody>
<tr>
<td>March 2007</td>
<td>SWOP-MN-ADMN70-A</td>
<td>Sidewinder 7.0.0.00</td>
</tr>
<tr>
<td>July 2007</td>
<td>SWOP-MN-ADMN70-B</td>
<td>Sidewinder 7.0.0.03</td>
</tr>
<tr>
<td>December 2007</td>
<td>SWOP-MN-ADMN70-C</td>
<td>Sidewinder 7.0.0.05</td>
</tr>
</tbody>
</table>
INTRODUCTION

CHAPTER 1

Introduction ................................................. 1
What is the Sidewinder network gateway? ...................... 2
The Type Enforcement environment .......................... 4
   How Type Enforcement works .............................. 4
   Type Enforcement’s effects .............................. 6
Sidewinder operating characteristics ........................ 7
   Burbs and network stack separation .................... 7
   Access control ........................................ 8
   Attack protection ....................................... 10
Sidewinder management options ............................. 11

CHAPTER 2

Quick Deployment ............................................ 13
Eleven steps to a deployed Sidewinder appliance .......... 14
Configuring a VPN ........................................ 16
Configuring HA or OTM ................................... 16
Configuring SmartFilter on Sidewinder .................... 17
Configuring TrustedSource ................................ 18
Configuring the anti-virus add-on module .................. 19
Configuring the anti-spam add-on module .................. 20
Configuring signature-based IPS .......................... 20
Configuring the SSL add-on module ....................... 21

CHAPTER 3

Administrator Basics ........................................ 23
Managing your appliance ................................... 24
   Understanding Sidewinder appliance management .... 24
# Table of Contents

Admin Console basics ................................................. 26  
Using the Admin Console ........................................... 30  
Logging directly into the appliance ............................... 34  
Configuring Admin Console access ............................... 35  
  Modifying the Admin Console rule .............................. 36  
  Configuring the Admin Console server ......................... 37  
Restarting or shutting down the system ......................... 39  
  Rebooting or shutting down using the Admin Console ........ 40  
  Rebooting or shutting down using a command line interface ... 42  
Managing administrator accounts ................................ 44  
Changing administrator passwords ............................... 48  
Using the Admin Console File Editor ......................... 48  
  Opening and saving files in the File Editor .................. 49  
  Creating a backup file in the File Editor ...................... 50  
  Restoring a file .................................................. 51  
Using the Find/Replace option ..................................... 52  
Administering the Sidewinder appliance using Secure Shell .... 54  
  Configuring the Sidewinder appliance as an SSH server ...... 55  
  Configuring and using the Sidewinder appliance as an SSH client 59  
  Tips on using SSH with the Sidewinder appliance ............... 61  
Administering the Sidewinder appliance using Telnet .......... 62  
  Setting up an internal (trusted) Telnet server ................. 62  
  Setting up an external Telnet server ............................ 62  
  Connecting to the Sidewinder appliance using Telnet .......... 63  
Configuring the Sidewinder appliance to use a UPS ............. 64

## POLICY

### CHAPTER 4 General Policy Configuration ........................................ 69  
Understanding traffic basics ........................................ 70  
A brief guide to planning your policy .............................. 71  
Using groups to simplify policy management ..................... 72  
Ordering rules within your policy ................................. 75  
Example of a simple rule ............................................ 77

### CHAPTER 5 Rules ...................................................... 81  
Understanding rules .................................................. 82  
  Condition rule elements ........................................... 82  
  Action rule elements ............................................... 84  
Using NAT and redirection in rules ............................... 85  
  Understanding and configuring NAT ............................. 85  
  Understanding and configuring redirection ..................... 86  
Viewing and ordering rules and rule groups ................. 87  
Organizing your security policy .................................. 87  
About the default Sidewinder policy ............................. 88
<table>
<thead>
<tr>
<th>Table of Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating an alternate policy</td>
</tr>
<tr>
<td>Using the main Rules window</td>
</tr>
<tr>
<td>Customizing the main Rules window view</td>
</tr>
<tr>
<td>Viewing and exporting your active policy</td>
</tr>
<tr>
<td>Creating, modifying, and duplicating rules</td>
</tr>
<tr>
<td>Creating and modifying rule groups</td>
</tr>
<tr>
<td>Viewing and modifying rule elements</td>
</tr>
<tr>
<td>Services</td>
</tr>
<tr>
<td>Time periods</td>
</tr>
<tr>
<td>Source burbs, endpoints, and NAT</td>
</tr>
<tr>
<td>Destination burbs, endpoints, and redirection</td>
</tr>
<tr>
<td>Application Defenses</td>
</tr>
<tr>
<td>IPS response mapping and signature groups</td>
</tr>
<tr>
<td>Authentication</td>
</tr>
<tr>
<td>Chapter 6 Services</td>
</tr>
<tr>
<td>Understanding services</td>
</tr>
<tr>
<td>Understanding proxy agents and services</td>
</tr>
<tr>
<td>Expected connections for proxy agents</td>
</tr>
<tr>
<td>Passing traffic transparently and non-transparently</td>
</tr>
<tr>
<td>When to disable Fast Path Sessions</td>
</tr>
<tr>
<td>Selecting the appropriate proxy service</td>
</tr>
<tr>
<td>Available proxy services</td>
</tr>
<tr>
<td>T.120 and H.323 proxy considerations</td>
</tr>
<tr>
<td>Understanding the Session Initiation Protocol (SIP)</td>
</tr>
<tr>
<td>Changing the FTP server response configuration</td>
</tr>
<tr>
<td>Understanding filter agents and services</td>
</tr>
<tr>
<td>How traffic is filtered if stateful packet inspection is enabled</td>
</tr>
<tr>
<td>How traffic is filtered if stateful packet inspection is disabled</td>
</tr>
<tr>
<td>Using NAT and redirection for filter rules</td>
</tr>
<tr>
<td>Stateful session failover in an HA cluster</td>
</tr>
<tr>
<td>Understanding server agents and services</td>
</tr>
<tr>
<td>Using the main Services window</td>
</tr>
<tr>
<td>Creating and modifying services</td>
</tr>
<tr>
<td>Configuring service-specific properties</td>
</tr>
<tr>
<td>Configuring an agent’s global properties</td>
</tr>
<tr>
<td>Configuring servers</td>
</tr>
<tr>
<td>Creating and modifying service groups</td>
</tr>
<tr>
<td>Chapter 7 Application Defenses</td>
</tr>
<tr>
<td>Understanding Application Defenses</td>
</tr>
<tr>
<td>Creating HTTP or HTTPS Application Defenses</td>
</tr>
<tr>
<td>Configuring the HTTP/HTTPS: Enforcements tab</td>
</tr>
<tr>
<td>Configuring the HTTP/HTTPS: HTTP URL Control tab</td>
</tr>
<tr>
<td>Configuring the HTTP/HTTPS: FTP URL Control tab</td>
</tr>
<tr>
<td>Configuring the HTTP/HTTPS: HTTP Request tab</td>
</tr>
<tr>
<td>Configuring the HTTP/HTTPS: HTTP Reply tab</td>
</tr>
</tbody>
</table>
Configuring the HTTP/HTTPS: MIME/Virus/Spyware tab . . . . . . . 175
Configuring the HTTP/HTTPS: Content Control tab . . . . . . . . . . 180
Configuring the HTTP/HTTPS: SmartFilter tab . . . . . . . . . . . . . . 181
Configuring the HTTP/HTTPS: Connection tab . . . . . . . . . . . . . . 182
Creating Mail (Sendmail) Application Defenses . . . . . . . . . . . . . . 184
Configuring the Mail (Sendmail): Control tab . . . . . . . . . . . . . . 184
Configuring the Mail (Sendmail): Size tab . . . . . . . . . . . . . . . . . 186
Configuring the Mail (Sendmail): Keyword Search tab . . . . . . . . 187
Configuring the Mail (Sendmail): MIME/Virus/Spyware tab . . . . . 191
Creating Mail (SMTP proxy) Defenses . . . . . . . . . . . . . . . . . . . . . . . 196
Configuring the Mail (SMTP proxy): Enforcements tab . . . . . . . . 196
Configuring the Mail (SMTP proxy): Commands tab . . . . . . . . . . 197
Configuring the Mail (SMTP proxy): Destination Address tab . . . . 198
Creating Citrix Application Defenses . . . . . . . . . . . . . . . . . . . . . . . . 200
Configuring the Citrix: Enforcements tab . . . . . . . . . . . . . . . . . 200
Configuring the Citrix: Filters tab . . . . . . . . . . . . . . . . . . . . . . . . . 201
Creating FTP Application Defenses . . . . . . . . . . . . . . . . . . . . . . . . . 202
Configuring the FTP: Enforcements tab . . . . . . . . . . . . . . . . . . . . 202
Configuring the FTP: Command Filter tab . . . . . . . . . . . . . . . . . . 203
Configuring the FTP: Virus/Spyware tab . . . . . . . . . . . . . . . . . . . 204
Creating IIOP Application Defenses . . . . . . . . . . . . . . . . . . . . . . . . . 209
Configuring the IIOP: Filter tab . . . . . . . . . . . . . . . . . . . . . . . . . . . 209
Creating T.120 Application Defenses . . . . . . . . . . . . . . . . . . . . . . . . 210
Configuring the T.120: General tab . . . . . . . . . . . . . . . . . . . . . . . . . 210
Configuring the T.120: Filter tab . . . . . . . . . . . . . . . . . . . . . . . . . . . 211
Creating H.323 Application Defenses . . . . . . . . . . . . . . . . . . . . . . . . . 212
Configuring the H.323: General tab . . . . . . . . . . . . . . . . . . . . . . . . . 212
Configuring the H.323: Filter tab . . . . . . . . . . . . . . . . . . . . . . . . . . . 213
Creating Oracle Application Defenses . . . . . . . . . . . . . . . . . . . . . . . . 215
Configuring the Oracle: Enforcements tab . . . . . . . . . . . . . . . . . . . 215
Configuring the Oracle: Service Name (SID) tab . . . . . . . . . . . . . 216
Creating MS SQL Application Defenses . . . . . . . . . . . . . . . . . . . . . . . 216
Creating SOCKS Application Defenses . . . . . . . . . . . . . . . . . . . . . . . 217
Configuring the SOCKS: SOCKS 5 Filter tab . . . . . . . . . . . . . . . . . . 217
Configuring the SOCKS: Connection tab . . . . . . . . . . . . . . . . . . . . 218
Creating SNMP Application Defenses . . . . . . . . . . . . . . . . . . . . . . . . 219
Configuring the SNMP: Filter tab . . . . . . . . . . . . . . . . . . . . . . . . . . 219
Configuring the SNMP: v1 tab . . . . . . . . . . . . . . . . . . . . . . . . . . . . 220
Creating SIP Application Defenses . . . . . . . . . . . . . . . . . . . . . . . . . 223
Configuring the SIP: General tab . . . . . . . . . . . . . . . . . . . . . . . . . . 223
Configuring the SIP: Media Filters tab . . . . . . . . . . . . . . . . . . . . . . . 224
Creating Packet Filter Application Defenses . . . . . . . . . . . . . . . . . . 225
Configuring the Packet Filter: General tab . . . . . . . . . . . . . . . . . . . 226
Configuring the Packet Filter: Advanced tab . . . . . . . . . . . . . . . . . . 227
Configuring Application Defense groups . . . . . . . . . . . . . . . . . . . . . . 228
Configuring the Application Defense Groups window . . . . . . . . 229
**CHAPTER 8**

**Content Inspection** .................................................. 233  
Configuring IPS inspection ............................................ 234  
Understanding signature-based IPS .................................. 235  
Adding IPS inspection to rules ....................................... 237  
About signature file updates ......................................... 239  
Using IPS with other Sidewinder attack protection tools ...... 240  
Configuring a response mapping ..................................... 241  
Configuring a signature group ....................................... 245  
Configuring IPS signature file updates ............................ 249  
Configuring virus scanning services ............................... 251  
Configuring virus scanning signature updates .................. 252  
Configuring the advanced virus scanning features .......... 255  
Configuring TrustedSource for Sidewinder ..................... 257  
Understanding TrustedSource ....................................... 257  
Enabling TrustedSource ............................................... 259  
Configuring spam filtering services .............................. 261  
Configuring the Whitelist ............................................. 262  
Configuring the spamcatcher.conf file ......................... 265  
Configuring SmartFilter for Sidewinder ......................... 267  
Obtaining the SmartFilter Control List ......................... 268  
Setting up SmartFilter for Sidewinder ............................ 269

**CHAPTER 9**

**Network Objects and Time Periods** ............................. 271  
Creating network objects ............................................ 272  
About the Network Object: Domain window ..................... 275  
About the Network Object: Host window .......................... 276  
About the Network Object: IP Address window ................. 278  
About the Network Object: IP Range window .................... 279  
About the Network Object: Netmap window ...................... 280  
About the Network Object: Subnet window ....................... 282  
About the Network Object: Netgroup window .................... 283  
Creating time periods ................................................. 288

**CHAPTER 10**

**Authentication** .......................................................... 291  
Understanding authentication ...................................... 292  
Who gets authenticated ............................................... 292  
Weak and strong authentication .................................... 293  
Types of authentication methods ................................... 295  
Alternate authentication methods .................................. 299  
Authentication scenario ............................................... 299  
Configuring an authenticator ....................................... 301  
Setting up Passport authentication ............................... 304  
Setting up standard password authentication .................. 309  
Setting up LDAP authentication ..................................... 311  
Setting up Windows domain authentication ..................... 317  
Setting up RADIUS authentication ................................ 320
Table of Contents

Setting up SafeWord authentication ................................................. 322
Telnet and FTP considerations ...................................................... 324
Setting up users to change their own passwords ............................... 325
Authenticating groups from an external group source ......................... 327
Authenticating groups from an internal group source ......................... 329
  About the Create New User/Group window .................................... 332
  About the Group Objects: Group Information tab .............................. 334
  About the Group Objects: User Group Membership tab ....................... 335
  About the User Objects: User Information tab ................................ 336
  About the User Objects: User Password tab .................................. 337

CHAPTER 11 Network Defenses ......................................................... 341
  Viewing Network Defense information ........................................... 342
  Configuring the TCP Network Defense .......................................... 345
  Configuring the IP Network Defense ............................................. 347
  Configuring the UDP Network Defense .......................................... 349
  Configuring the ICMP Network Defense ....................................... 351
  Configuring the ARP Network Defense ........................................ 353
  Configuring the IPsec Network Defense tab ................................... 355

MONITORING

CHAPTER 12 Auditing ................................................................. 359
  Understanding the Sidewinder audit process ................................... 360
    Audit components ......................................................................... 361
    Audit file names ........................................................................ 363
    Tools for viewing and customizing audit events ............................... 364
  Viewing audit information using the Admin Console ......................... 365
    Selecting an audit range to view ................................................... 365
  Exporting audit data ..................................................................... 370
  Filtering audit data ..................................................................... 371
  Creating custom audit filters ......................................................... 378
    Learning filter syntax ................................................................. 378
    Filter examples ......................................................................... 380
  Managing audit information using the Admin Console ....................... 382
  Understanding audit messages ....................................................... 388
  Configuring syslog for off-box reporting tools .................................. 389
    Understanding syslog on the Sidewinder appliance ......................... 389
    Redirecting audit output to a syslog server .................................... 390
    Viewing syslog messages ............................................................. 391
  Generating reports using SecurityReporter ...................................... 392
  Formatting and exporting audit data for use with external tools ............ 393
    Overview of supported log file formats ......................................... 393
    Using Sidewinder formatting and exporting tools ............................ 395
CHAPTER 13 IPS Attack and System Event Responses ................. 399
Understanding attack and system event responses .......... 400
Creating IPS attack responses .................................. 401
  Modifying an IPS attack response ............................. 403
  Configuring the e-mail response settings ....................... 409
Creating system responses ........................................ 411
  Modifying a system response ................................... 412
  Configuring the e-mail settings ................................ 416
Ignoring network probe attempts ................................ 417
Sidewinder SNMP traps .............................................. 418

CHAPTER 14 Service Status ........................................... 421
Understanding processes that control server status .......... 422
daemond .............................................................. 422
  Network Services Sentry (NSS) ................................. 425
Viewing service status .............................................. 426
Viewing a service’s process information ......................... 429

CHAPTER 15 The Dashboard ............................................ 431
Monitoring Sidewinder status using the dashboard .......... 432
Viewing device information ........................................ 434
Viewing network traffic information ............................. 438
Viewing IPS attack and system event summaries ............. 443
  Understanding audit event severities ............................ 443
  Viewing the summary statistics ................................ 445

NETWORKING

CHAPTER 16 Burbs and Interfaces .................................... 451
Configuring burbs .................................................... 452
Configuring interfaces ............................................. 456
  About the Interfaces: Interfaces tab ......................... 457
  About the Interfaces: Aliases tab ............................. 461
Configuring Quality of Service .................................. 462
  Example QoS scenarios ........................................... 469

CHAPTER 17 E-mail ..................................................... 471
Overview of mail on Sidewinder ................................ 472
  About transparent mail (SMTP proxy) ......................... 472
  About Sidewinder-hosted mail (sendmail) ..................... 473
Setting up and reconfiguring mail ............................... 474
Understanding sendmail on Sidewinder ......................... 476
Using sendmail on Sidewinder ................................... 476
Mail filtering services on Sidewinder ......................... 478
Editing sendmail files on Sidewinder ......................... 480
Configuring advanced sendmail features ........................................ 484
  Configuring sendmail to strip message headers ....................... 484
  Configuring sendmail to use the RealTime Blackhole list .......... 486
  Allowing or denying mail on a user basis ............................... 487
  Configuring sendmail to hide internal e-mail addresses .......... 488
  Enabling Sendmail TLS ................................................... 489
Managing mail queues .......................................................... 490
  Viewing the mail queue .................................................... 490
  Changing how long a message waits between delivery attempts . 491
  Manually attempting to deliver queued messages ................... 492
  Changing how long a message waits before it is returned to its sender 493
Receiving mail sent by Sidewinder ............................................ 494
  Setting up e-mail aliases for administrator accounts ............... 494
  Viewing administrator mail messages on Sidewinder ................. 495

CHAPTER 18

DNS (Domain Name System) ...................................................... 497
  What is DNS? ............................................................... 498
  About transparent DNS .................................................... 499
  About Sidewinder-hosted DNS ............................................. 500
  Designating an authoritative server .................................... 501
  Using master and slave servers in your network ..................... 501
  Configuring clients and hosts to use Sidewinder-hosted DNS ...... 502
  Enabling and disabling hosted DNS servers ........................... 503
  Using hosted sendmail with Sidewinder-hosted DNS .................. 504
  More points about Sidewinder-hosted DNS ............................. 505
Configuring transparent DNS .................................................. 506
  Configuring Sidewinder-hosted DNS servers .......................... 507
  Configuring the Server Configuration tab ............................ 509
  Configuring the Zones tab ............................................... 513
  Configuring the Master Zone Attributes tab ......................... 518
  Configuring the Master Zone Contents tab ............................ 523
Reconfiguring DNS ............................................................... 528
  Reconfiguring transparent DNS ......................................... 528
  Reconfiguring single server hosted DNS ............................... 530
  Reconfiguring split server hosted DNS ................................. 531
Manually editing DNS configuration files .................................. 533
  DNS message logging ...................................................... 534

CHAPTER 19

Virtual Private Networks ....................................................... 535
  Understanding VPN on Sidewinder appliance .......................... 536
  An introduction to IPsec technology .................................... 537
  VPN configuration options ................................................. 538
  Configuring a VPN client ................................................. 541
  Extended Authentication for VPN ......................................... 542
  What type of VPN authentication should I use? ....................... 543
# Table of Contents

Using rules to direct VPN traffic .................................................. 545
Creating VPN definitions ............................................................ 555
Managing VPN definitions ......................................................... 556
About the VPN Properties: General tab ........................................... 560
About the VPN Properties: Remote Authentication tab ....................... 564
Configuring the ISAKMP service .................................................. 574
Configuring the ISAKMP server .................................................... 574
Allowing access to the ISAKMP server .......................................... 576
Configuring Certificate Management ............................................. 577
Configuring the Certificate server ................................................ 577
Understanding Distinguished Name syntax .................................... 580
Selecting a trusted source .......................................................... 583
Configuring and displaying CA root certificates .............................. 584
Configuring and displaying Remote Identities ............................... 587
Configuring and displaying firewall certificates ............................ 589
Configuring and displaying remote certificates ............................. 592
Assigning new certificates for Admin Console services ................... 595
Importing and exporting certificates ............................................. 596
Creating and using a virtual burb with a VPN ................................. 602
Configuring client address pools .................................................. 603
Configuring a client address pool ................................................ 604
Configuring the Subnets tab ....................................................... 605
Configuring the DNS and/or WINS servers ................................... 607
Configuring the fixed IP map ...................................................... 609
Example VPN Scenarios .............................................................. 611
Scenario 1: Sidewinder-to-Sidewinder VPN via shared password . 611
Scenario 2: Simple deployment of remote users ............................... 613
Scenario 3: Large scale deployment of clients ................................. 617

## Chapter 20

Routing ................................................................. 623
An overview of routing on Sidewinder ........................................ 624
Modifying static routes ............................................................ 625
RIP on Sidewinder ..................................................................... 627
  A general overview of RIP processing ..................................... 628
Configuring RIP (ripd) ............................................................... 629
  About basic ripd configuration .............................................. 630
  RIP processing options ....................................................... 632
  Enabling ripd on a single Sidewinder burb ............................... 635
  Enabling RIP processing on multiple Sidewinder burbs ............... 636
Viewing and comparing ripd configurations .................................. 638
OSPF on Sidewinder ................................................................. 640
Configuring OSPF (ospfd) .......................................................... 643
  About basic ospfd configuration .......................................... 643
  OSPF processing options ................................................... 645
Viewing and comparing OSPF configurations .............................. 647
BGP on Sidewinder ................................................................. 648
Table of Contents

Configuring BGP (bgpd) ............................................ 649
  About basic bgpd configuration .................................. 649
  BGP processing options ......................................... 651
Viewing and comparing BGP configurations .................... 652
PIM-SM on Sidewinder ........................................... 654
Configuring
  PIM-SM (pimd) .................................................. 655
  Create policy rules ............................................ 655
  Configure the pimd (XORP server) service ....................... 658
  Configure IGMP .................................................. 660
  Configure PIM-SM ................................................. 661
  Restart the pimd (XORP server) service ......................... 664
  Exceptions to making PIM-SM changes .......................... 664
Viewing PIM-SM configurations ................................ 666
Troubleshooting dynamic routing issues ........................ 667

CHAPTER 21

The SNMP Agent .................................................. 669
Understanding SNMP options ..................................... 670
Overview of Sidewinder as a managed node ....................... 671
  Communicating with an SNMP management station ............... 671
  About Sidewinder SNMP traps .................................. 673
  About Sidewinder SNMP MIBs .................................. 673
  About the management station ................................ 675
Setting up the SNMP agent on Sidewinder ....................... 676
  Configuring the SNMP agent .................................. 677
  Creating a rule to allow access to the SNMP agent ............ 679
Sending SNMP traffic through Sidewinder ....................... 680

MAINTENANCE

CHAPTER 22

General Maintenance Tasks ....................................... 683
Setting the system date and time ................................ 684
  Setting the date and time ..................................... 684
  Understanding Network Time Protocol .......................... 686
References .......................................................... 690
Configuration file backup and restore ......................... 691
  About the Configuration Backup: Configuration Backup tab .... 692
  About the Configuration Backup: Configuration Restore tab .... 698
  About the Configuration Backup: Schedule tab ................. 703
Activating the Sidewinder license ............................. 705
  Licensing from an appliance connected to the internet ........ 706
  Licensing from an appliance on an isolated network .......... 707
  Configuring the Firewall License tabs ......................... 708
Protected host licensing and the Host Enrollment List ......... 713
Software management ............................................. 716
### Table of Contents

- DNS ................................................................. 811
- About automatic (cron) jobs ................................. 812
- Default cron jobs .............................................. 812
- The roll audit cron job ........................................ 813
- Working with files on the appliance ....................... 814
- About editing Sidewinder files ................................ 814
- Checking file and directory permissions (ls command) ...... 815
- Changing a file’s type (chtype command) .................. 815
- Creating your own scripts ..................................... 816

### APPENDIX B

#### Basic Troubleshooting ........................................ 817

- Troubleshooting rules ....................................... 818
- Failed connection requests ................................... 818
- Monitoring allow and deny rule audit events ............... 820
- Active rules and DNS .......................................... 822
- Troubleshooting logging in ................................... 823
- Restoring access to the appliance ............................ 823
- Changing a forgotten password ................................ 824
- Manually clearing an authentication failure lockout ........ 824
- Changing authentication requirements for emergency maintenance mode ........................................ 824
- Re-install and recovery options .............................. 825

- Overview of recovery options ............................... 825
- Re-installing your appliance from the virtual CD ........ 830
- Re-installing your appliance from a CD-ROM ............. 832
- About the disaster recovery option via USB flash drive .. 834
- Re-installing without a CD-ROM drive ...................... 838
- How CD-less re-installing works ............................ 838
- System requirements .......................................... 839
- Re-installing the Sidewinder ................................ 840
- Updating the image on the Sidewinder 7 PXE Imaging Server ........ 847

#### Troubleshooting licensing problems ..................... 850

#### Troubleshooting High Availability ....................... 851

- Viewing configuration-specific information ................ 851
- Viewing status information ................................... 853
- Identifying load-sharing addresses in netstat and ifconfig ..................................................................... 856
- Interface configuration issues with HA ..................... 856
- Troubleshooting remote interface test failover for peer-to-peer HA ..................................................... 856

#### Troubleshooting NTP ........................................... 857

#### Troubleshooting VPNs ......................................... 860

### Glossary .......................................................... 861

### Index .............................................................. 875
Who should read this guide

This guide is intended for a Sidewinder Network Gateway appliance administrator. You should read this guide if you are responsible for configuring and managing a Sidewinder appliance.

This guide assumes you have:

- A working knowledge of UNIX and Windows operating systems.
- A basic understanding of system administration.
- A working knowledge of the Internet and its associated terms and applications.
- An understanding of networks and network terminology, including TCP/IP protocols.

Where to find additional information

The Management Tools CD includes the Sidewinder documentation in .pdf format. When you install the Management Tools on a Windows-based system, the documents are automatically loaded onto your hard drive. When you install a patch, the related Release Notes will be added to this directory. You can view them by selecting Start > Programs > Secure Computing > Sidewinder Admin Console 7 > Documentation.

Note: To view Sidewinder documents prior to installing the Windows-based tools, browse to the \Manuals directory on the Management Tools CD.
Table 1: Summary of Sidewinder documentation

<table>
<thead>
<tr>
<th>Document</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Startup Guide</strong></td>
<td>Steps you through setting up your initial Sidewinder appliance configuration.</td>
</tr>
<tr>
<td><strong>Administration Guide</strong></td>
<td>This is the guide you are currently reading. It provides complete administration information on all Sidewinder functions and features. You should read this guide if you are responsible for configuring and managing a Sidewinder appliance.</td>
</tr>
<tr>
<td><strong>Online help</strong></td>
<td>Online help is built into the Sidewinder software. The Quick Start Wizard provides help for each configuration window. The Admin Console program provides detailed context-sensitive online help.</td>
</tr>
<tr>
<td><strong>Application notes</strong></td>
<td>Provides detailed instructions for setting up specific configurations, such as setting up the Sidewinder appliance to work with another vendor’s product or environment. Application notes are located at: <a href="http://www.securecomputing.com/goto/appnotes">www.securecomputing.com/goto/appnotes</a></td>
</tr>
<tr>
<td><strong>Knowledge Base</strong></td>
<td>Supplemental information for all other Sidewinder documentation. Articles include helpful troubleshooting tips and commands. All manuals and application notes are also posted here. The Knowledge Base is located at: <a href="http://www.securecomputing.com/goto/kb">www.securecomputing.com/goto/kb</a></td>
</tr>
</tbody>
</table>

For the latest information regarding Sidewinder and other Secure Computing products, refer to our Web site at: www.securecomputing.com.
Online help

The Sidewinder graphical user interface (known as the Admin Console) provides comprehensive online help. To access online help, click the help icon in the toolbar.

Man (or “manual”) pages provide additional help on Sidewinder-specific commands, file formats, and system routines. To view the available information for a specific topic, enter one of the following commands:

```
man -k topic
```

or

```
apropos topic
```

where `topic` is the subject that you want to look up.

Reference materials

If you are new to system administration, you may find the following resources useful:

- *Managing Internet Information Services* by Liu, et al. (O'Reilly and Associates, Inc.)
- A standard reference on computer security is *Firewalls and Internet Security* by Cheswick and Bellovin (Addison-Wesley).
- For network management information, see *TCP/IP Network Administration* by Craig Hunt (O'Reilly & Associates, Inc.).
- For information on handling mail on UNIX networks, see *Sendmail* by Bryan Costales, with Eric Allman and Neil Rickert (O'Reilly & Associates, Inc.).
- For Domain Name System information, see *DNS and Bind* by Cricket Liu and Paul Albitz (O'Reilly & Associates, Inc.).
- For information about Internet Review for Comment (RFC) documents, refer to one of the following Web sites:
  
  * [http://www.cse.ohio-state.edu/cs/Services/rfc/index.html](http://www.cse.ohio-state.edu/cs/Services/rfc/index.html)
  * [http://www.ietf.org/rfc.html](http://www.ietf.org/rfc.html)

*Note:* Some of these resources are referenced throughout this guide.
This guide uses the following typographic conventions:

**Table 2: Conventions used in this guide**

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>boldface courier</strong></td>
<td>Commands and keywords you type at a system prompt are in boldface.</td>
</tr>
<tr>
<td>\ (backslash character in a command string)</td>
<td>When a command does not fit on the same line in this document, the backslash () character is used to indicate continuation. Enter the command as shown, ignoring the backslash.</td>
</tr>
<tr>
<td><strong>courier italic</strong></td>
<td>Place holders for text you type. Words that appear in square angle brackets &lt;xxx&gt; are placeholders for optional text.</td>
</tr>
<tr>
<td><strong>courier plain</strong></td>
<td>Text displayed by this product on a computer screen.</td>
</tr>
<tr>
<td><strong>plain text italics</strong></td>
<td>Names of files and directories.</td>
</tr>
<tr>
<td><strong>Body Text Highlight</strong></td>
<td>Buttons, field names, and tabs in procedures that require user interaction.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>Means reader take note. Notes contain helpful suggestions or references to material not covered elsewhere in the manual.</td>
</tr>
<tr>
<td><strong>Tip:</strong></td>
<td>Means the following information will describe a time-saving action or help you solve a problem.</td>
</tr>
<tr>
<td><strong>Important:</strong></td>
<td>Means the following text will provide information essential to the successful completion of a task or procedure.</td>
</tr>
<tr>
<td><strong>Caution:</strong></td>
<td>Means reader be careful. In this situation, you might do something that could result in loss of data or an unpredictable outcome.</td>
</tr>
<tr>
<td><strong>Security Alert:</strong></td>
<td>Emphasizes information that is critical to maintaining product integrity or security.</td>
</tr>
<tr>
<td>127.10.3.4</td>
<td>IP addresses, screen captures, and graphics within this document are intended as examples. They do not necessarily represent a proper or complete configuration or the configuration that is appropriate to your needs. Often features are enabled so they are clear in the screen capture. Not all features are appropriate or desirable for your Sidewinder setup.</td>
</tr>
</tbody>
</table>
CHAPTER 1

Introduction

In this chapter...

What is the Sidewinder network gateway? ........................................... 2
The Type Enforcement environment .................................................... 4
Sidewinder operating characteristics ................................................. 7
Sidewinder management options ....................................................... 11
What is the Sidewinder network gateway?

The Sidewinder network gateway security appliance allows you to connect your organization to the Internet while protecting your network from unauthorized users and attackers, while also protecting internal users as they access the Internet. It combines an application-layer firewall, IPsec VPN capabilities, Web filtering (SmartFilter), global-reputation-based filtering (TrustedSource), anti-spam/anti-fraud and anti-virus/anti-spyware filtering engines, and SSL decryption into one Unified Threat Management (UTM) security appliance, designed to offer centralized perimeter security.

The Sidewinder appliance provides a high level of security by using SecureOS®, an enhanced UNIX operating system that employs Secure Computing’s patented Type Enforcement® security technology. SecureOS removes the inherent security risks often found in a network application running on non-security focused commercial operating systems, resulting in superior network security and no emergency security patches to apply.

Tip: For more information regarding the Sidewinder appliance and its benefits, refer to our Web page at www.securecomputing.com/hardware. Information about the hardware warranty is available at www.securecomputing.com/goto/warranty.

The appliance prevents host identification masquerading (IP spoofing), making it very difficult for attackers to infiltrate your protected networks. It also offers advanced authentication and encryption software. Encryption allows authorized users on the Internet access to your protected network without fear of attackers eavesdropping (IP sniffing) or stealing access credentials and other valuable information.

The Sidewinder appliance allows public services such as e-mail, a public file archive (FTP), and Web (HTTP/HTTPS) access while protecting the other computers on your protected networks. It also provides powerful configuration options that allow you to control access by your employees to almost any publicly available service on the Internet.

The default Sidewinder configuration supports two network interfaces. However, you can add additional physical and virtual network interfaces for a total of up to 63 network connections. The appliance can be used as a gateway between your internal network and the Internet, or between any networks with different security needs. Figure 1 shows the appliance protecting a company’s internal network.
Chapter 1: Introduction
What is the Sidewinder network gateway?

Figure 1: Protecting your organization's network with Sidewinder

The configuration shown in the following figure is useful in providing protection for two otherwise separate networks within your organization, or between your organization and a strategic business partner. This configuration uses three network interfaces.

Figure 2: Protecting multiple networks with Sidewinder
As mentioned earlier, the Sidewinder appliance runs on SecureOS, a version of BSD that Secure Computing has enhanced with a patented security technology called Type Enforcement. Type Enforcement was originally developed by Secure Computing Corporation for the Secure Network Server, a product that meets strict U.S. government standards for computer security.

For the most part, Type Enforcement does not require any extra effort on your part. The following subsections describe areas that affect how you use the system and access files that you should be aware of.

### How Type Enforcement works

UNIX is not known to be a particularly secure operating system. Logging in as super-user (root) gives you access to all system files; an intruder who knows how to acquire root privileges can access any files or applications on a system. In addition, UNIX does not have tight control over how data files are shared among the processes running on a system. This means that an intruder who managed to break into one area of a system, such as e-mail, may be able to easily gain access to other files on the system.

The Sidewinder Type Enforcement software is designed to plug these security holes. This is done by using the following mechanisms (each of the mechanisms is described below):

- Provides maximum network protection
- Provides Type Enforced domain processes
- Controls Type Enforced attributes applied to files and sockets
- Controls inter-domain operations, such as signals
- Controls access to system calls
- Controls the files a process can access

### Maximum network protection

Secure Computing's patented Type Enforcement technology provides network security protection that is unique to the industry. By using Type Enforcement within the operating system, the Sidewinder appliance provides the highest level of security.

Type Enforcement is based on the security principle of least privilege: any program executing on the system is given only the resources and privileges it needs to accomplish its tasks. On the Sidewinder appliance, there is no concept of a root super-user. Type Enforcement controls all interactions between domains and file types. Domains must have explicit permission to access specific file types, communicate with other domains, or access system functions. Any attempts to the contrary fail as though the files do not exist.
**Type Enforcement domain processes**

A standard UNIX system separates processes with user and group identities. Therefore, UNIX identities can be completely subverted by users who obtain root privileges. The Sidewinder appliance prevents this by providing separate, Type-Enforced domains for each process running on the system. Type-enforced domains provide more intricate control over what each process is allowed to do, as shown here in Figure 3.

![Figure 3: Example of the Sidewinder domain separation structure](image)

**Type Enforced attributes**

When an administrator initially logs into the Sidewinder appliance at a command line prompt, they are automatically placed in the *User* domain, which allows no access to sensitive files. An administrator may then switch to their defined administrative role’s domain using the `srole` command (for Admn) or `srole adminro` (for AdRO). The Admn domain allows an administrator to access to all administrative functions. The AdRO domain allows read-only access to the system configuration areas, as well as the ability to generate reports. An administrator with read-only access cannot make system modifications.

This guide assumes that most commands will be issued by administrators with read/write access, and therefore only includes the `srole` command. If you are a read-only administrator and have reason to access the command line, always use `srole adminro` instead of `srole` alone.

For information on assigning administrator roles, see “Managing administrator accounts” on page 44.

**Inter-domain operations**

Interactions between domains, such as signalling, are also controlled by Type Enforcement. For example, a process running in the SMTP domain cannot send a signal to the Telnet server running in the Telnet domain.
Access to system calls

A typical UNIX system has many privileged system calls that could enable malicious users to access the kernel directly and compromise the system. The appliance solves this problem with a set of flags for each domain that indicate which system calls can be made from that domain.

Files available to a process

Process-to-file access is controlled by a Domain Definition Table that maps out the various classes of data files and processes that may be running on the appliance. The table specifies which process domains can access different types of files and what type of access is allowed (such as read/write/execute). This table cannot be circumvented.

Your system is pre-configured so that domains have access only to the files they need. The Domain Definition Table cannot be changed while the Operational kernel is running. This prevents intruders from tricking the kernel into modifying the table. Also, Type Enforcement prevents intruders from installing software that may be used to circumvent Sidewinder security mechanisms.

The backup and restore functions on your system have been modified to be aware of Type Enforcement. When you restore files, they are automatically restored with the correct Type Enforcement properties.

Type Enforcement’s effects

The previous section outlined how Type Enforcement works. Listed below are the major ways in which Type Enforcement affects you and other users:

• Non-administrative users will not be aware of Type Enforcement unless they try to perform unauthorized activities.

• The concept of a super-user who can have complete system control does not exist. The “root” account has no special privileges. The Admin role operating in the Admn domain has access to most system files, but is still not as powerful as root on a standard UNIX system.

• Domains make it difficult for an intruder to do damage. Breaking into the domain in which an application is executing does not provide access to the files required for administering that application.
Sidewinder operating characteristics

This section lists additional significant differences between the Sidewinder appliance and a standard UNIX system.

**Burbs and network stack separation**

While installing or managing the Sidewinder appliance, you will notice the use of the term *burb*. *Burb* is a term that refers to an interface and all the systems it connects. Each burb must have a unique name. The two default burbs are named *internal* and *external*.

As an example of how burbs are used, suppose your organization has two internal (protected) networks that need to be connected to the external network (Internet), but the corporate security policy requires that there be limited or no information flow between the two internal networks. In this scenario, you would configure three burbs for your Sidewinder appliance, as shown in Figure 4. The security policy must be defined to enforce the required control over information flow between the two internal security burbs and between the external burb and the individual internal burbs, while also protecting the internal burbs from unauthorized access from the Internet.

![Figure 4: Multiple Type Enforced areas (burbs)](image)

One of the unique aspects of the SecureOS is the use of multiple logical network stacks to strengthen the enforcement of the inter-burb aspects of the system security policy. A network stack consists of different layers of software responsible for different aspects of the communications. For example, one layer checks a message’s routing information to ensure that it is transmitted to the correct network. Normal computing systems, and firewalls that operate on an unsecured OS, have only one network stack.
The SecureOS includes modifications that provide stronger separation of communication between different burbs. There are checks at all layers of the software to ensure that the network stack data from one burb is not mixed with, or impacted by, data associated with another burb. This logical separation of the network stacks by the security burb is augmented by the Type Enforcement security policy, which is integral to SecureOS. It controls all operational aspects of the system, including enforcement of the separation data processing by the security burb. This ensures that information passes from one burb to another only if the network security policy says the specific information flow is allowed.

Figure 5 shows this logical network separation involved in the transfer of data between the network stacks associated with each burb. Before a process can interact with a network stack, the Type Enforcement security policy must indicate that the process is allowed to interact with that burb’s network stack. The degree to which the appliance inspects a packet is determined by the agent processing the packet.

**Figure 5:** Logical network protocol stacks provide network separation

---

**Access control**

In the Sidewinder appliance, the rule set determines what traffic is permitted into and through the appliance, and what is denied. Each rule requires a service. A service associates a traffic’s transport layer with a specific agent that is responsible for managing the service’s traffic. The transport layer information includes elements such as the protocol, the ports, and the connection or session timeouts. There are three types of agents: proxy, packet filter, and server.

**Note:** See the Policy section for details information on policy configuration, rules, and services.
Proxy agents and services

The Sidewinder appliance uses special programs called proxy agents to forward application data between two burbs, such as your internal network and the Internet. Proxy agents essentially provide a go-between that can communicate with the burbs on the appliance. For example, when a user on an internal burb tries to establish an Internet connection, the appliance intercepts the connection attempt and opens the connection on the user’s behalf. All Internet connections are made by the appliance so that the internal network never communicates directly with the Internet burb. For some proxy agents, you can configure transparency on a per-service basis. For transparent connections, the client is unaware of the appliance. The appliance is implicitly included in the path based on routing. For non-transparent, the client is aware of the appliance and explicitly connects to the appliance.

The Sidewinder appliance supports HTTP, Telnet, and many other TCP-based proxies. The appliance also supports proxies for routing SNMP, NTP, DNS, and other types of services that require UDP transmissions. You can also create your own special proxies for other services. In addition, the appliance provides proxies that use multiple TCP and/or UDP sessions such as FTP, RealMedia, and Oracle SQLNet.

Most proxy agents are disabled by default. When you use a proxy service in a rule, the appliance automatically enables that service’s agent in the rule’s source burb. That allows traffic to flow from the source to its destination. For example, you can configure rules that allow all internal users to access all Internet Web sites, or you can prohibit users from accessing the Web from specific internal systems or from accessing specific Web sites.

Filter agents and services

You can configure the appliance to securely forward IP packets between networks using filter services in rules. Unlike proxy agents, which operate at the application layer and in most cases on TCP or UDP traffic, filters operate directly on IP packets allowing non-TCP/UDP (as well as TCP/UDP) traffic to pass between the networks. For example, with a filter service you can pass encrypted VPN sessions through the appliance.

Filtering services work by inspecting many of the fields within a packet, including the source and destination IP address, port, and protocol. Each packet that arrives at the appliance will be inspected and compared to an enabled filter rule that you have configured. Packets that match an allow rule will then be forwarded to the destination network.

You can configure filtering services to inspect TCP, UDP, and many other protocols. With TCP, UDP, and ICMP, the appliance can actively track individual sessions by performing stateful inspection. This ensures that only packets valid for a new session or a portion of an existing session are sent on to the final destination. In addition, the Sidewinder supports the ability to perform Network Address Translation (NAT) and redirection when using filters.
Server agents and services

Sidewinder servers provide a variety of system functions, but generally do not pass traffic between burbs. Rules that allow access to a Sidewinder server typically have the same source and destination burbs. Therefore, proxy agents are not used to control an external (Internet) user’s access to the external side of the Sidewinder appliance. For example, when an external user accesses an SSH server that you have made publicly available on the external side of the appliance, there will be no proxy agent to intervene. For users on the Internet, proxy agents are only used when they cross burb boundaries to access systems in the an internal burb.

Attack protection

The first step in protecting your network is creating a rule set based on a least-permissions philosophy and using the application-aware proxy agents to pass traffic. The next step is to use Sidewinder attack protection to defend against attacks in both allowed and denied traffic. The appliance has multiple layers that work together to protect against known and unknown attacks. Some of these defenses occur automatically, and some of them must be configured. The following sections explain the different options.

Network Defenses

The Sidewinder appliance is pre-configured to block an extensive list of suspicious traffic at the data link, network, and transport layers. Packets that do not adhere to their protocol standards are always dropped, as are packets that match known attack configurations.

Application Defenses

Application Defenses offer customizable protection at the application layer. The defenses can be used to enforce RFC (Request for Comments) standards and allowed parameters. Configurable parameters include headers, commands, versions, and file sizes. You can use these controls to deny any parameters that are not essential to your business needs and to minimize your network’s attack surface; the fewer the number of parameters allowed into your network, the fewer parameters an attacker can use to attack. The controls can also provide the following key inspection services:

- Anti-virus filtering
- Anti-spam
- Reputation-based filtering
- URL-based Web filtering

Note: The listed services are premium features.
Signature-based Intrusion Prevention Services

The Sidewinder Intrusion Prevention Service uses signature-based files to detect and prevent known network-based intrusion attacks, such as hacker-generated exploits and protocol anomalies. IPS can be added to rules to inspect allowed, incoming traffic for these attacks as the traffic enters the appliance. If an attack is detected, the rule handles the attack according to the configured response. Response options range from completely ignoring the traffic to blackholing all traffic sent from the originating host. This attack protection is particularly valuable when you cannot minimize your attack surface because your organization requires services with known vulnerabilities.

Note: This is a premium feature.

IPS Attack Responses

Even attacks that are not allowed through the appliance can cause problems if allowed to continue. For this reason, the Sidewinder appliance has IPS Attack Responses, which can be configured to notify administrators when audit events are generated by suspicious traffic. If a specified attack audit occurs a certain number of times in a given time period, the appliance can alert an administrator, blackhole all traffic from the IP address originating the attack, or both. Being aware of attempted attacks is an important part of maintaining your network's security.

Use these tools to configure and manage your Sidewinder appliance:

- **Sidewinder Admin Console** — The primary management tool. It is a proprietary graphical user interface program that you install on a Windows® operating system. All Admin Console sessions are encrypted.

- **Command-line clients** — Used for troubleshooting. Sessions can be initiated from a Windows, UNIX, or other workstation with an installed SSH client or command-line access.
  - SSH
  - Telnet

Caution: Since command-line clients are a secondary management tool, changes made during command line sessions may be overwritten by the Admin Console.

CHAPTER 2

Quick Deployment

In this chapter...

Eleven steps to a deployed Sidewinder appliance .........................14
Configuring a VPN..........................................................................16
Configuring HA or OTM..................................................................16
Configuring SmartFilter on Sidewinder...........................................17
Configuring TrustedSource ............................................................18
Configuring the anti-virus add-on module .................................19
Configuring the anti-spam add-on module ................................20
Configuring signature-based IPS ................................................20
Configuring the SSL add-on module ...........................................21
Eleven steps to a deployed Sidewinder appliance

This section is a high-level process overview of the basics needed to deploy your Sidewinder Network Gateway appliance according to your organization’s security policy. This list assumes that you have already completed the Sidewinder appliance’s initial configuration. It covers the key services needed by most organizations, as well as best practices for setting up your new appliance. To make things easy to find, we’ve included the path to each window you will configure.

When you finish this list, your appliance will be passing the traffic you need. It will also be using the latest software version, have troubleshooting tools, and have a configuration backup available.

Tip: A good way to become familiar with Sidewinder administration is to take on the free web-based training course located here: http://www.securecomputing.com/WBT/syllabus-sw70.cfm

1 Write down your security policy. This includes:
   • What network areas, if any, need to be separated from other network areas. These are your burbs.
     For example, if you need to allow inbound access to a web server, it’s best to put that web server in a DMZ burb to keep it separate from your other internal systems.
   • What you will allow in and out of your protected network. Write down what protocols you need (HTTP, HTTPS, FTP, etc.) and any restrictions for those protocols’ traffic, such as who can use them, when they can be used, etc. These parameters will become your rules.
     Read Chapter 4, “General Policy Configuration,” on page 69 for help planning your rules.
   • How mail will get in and out of your protected network. You will either use Sidewinder’s hosted sendmail server or a third-party mail server, such as Microsoft Exchange.
   • Add-on modules, if any. Options are anti-virus, anti-spam, web filtering, Intrusion Prevent Services (IPS), and SSL decryption.
   • A One-to-Many or High Availability configuration, if any.
   • Virtual private networks (VPNs), if any.

2 Set up the Admin Console and log in.

3 Verify your license is activated: Select Maintenance > License.
   If the Activation Key field is empty, you may have network connectivity problems. Check that your appliance is cabled correctly. (Refer to the Port Identification Guide, found in the Sidewinder documentation packet). Continue to test connectivity from one system to another until you can successfully reach the Internet and re-submit your license.

4 Update your appliance to the most recent available patch level: Select Maintenance > Software Management.
Chapter 2: Quick Deployment

Eleven steps to a deployed Sidewinder appliance

5 Add burbs and burb groups needed in your security policy: Select **Network > Burb Configuration**.

6 Configure the necessary network interfaces: Select **Network > Interfaces**.

7 Create your security policy’s rules: Select **Policy > Rules**.
   You can create most of your rule elements (services, network objects, time periods, authenticators, etc.) from the New Rule window.
   However, for best results, create your rule elements before creating your rules. If you plan to use any of the add-on modules, see:
   - “Configuring SmartFilter on Sidewinder” on page 17
   - “Configuring TrustedSource” on page 18
   - “Configuring the anti-virus add-on module” on page 19
   - “Configuring the anti-spam add-on module” on page 20
   - “Configuring signature-based IPS” on page 20
   - “Configuring the SSL add-on module” on page 21
   Confirm that the required traffic is passing from several internal stations to the Internet using the appliance’s real-time audit: Select **Monitor > Audit**.

8 Set up command-line access for troubleshooting purposes: Select **Policy > Rules**. In the Administration rule group, enable the default SSH rule.
   Change the endpoints and authentication as needed.
   Open an SSH client and confirm you can connect to your appliance.

9 Set up DNS:
   a If you are using transparent DNS, make sure the off-box name servers are properly configured to work with the Sidewinder appliance. Consult the name servers’ documentation for help.
   b Select **Maintenance > Reconfigure DNS** and configure your DNS mode.
   c Select **Policy > Rules** and create the rules necessary to pass your DNS.
   Verify that you can send and receive DNS queries.

10 Set up mail:
   a If you are using transparent mail, make sure the off-box mail servers are properly configured to work with the Sidewinder appliance. Consult the mail servers’ documentation for help.
   b Select **Maintenance > Reconfigure Mail** and configure your mail mode.
   c Select **Policy > Rules** and create the rules necessary to pass your mail.
   Verify that you can send and receive mail from an internal mail account to an external mail account.

11 Create a configuration backup so you can easily recover in the event of a failure or an undesirable configuration change: Select **Maintenance > Configuration Backup**.
Configuring a VPN

VPNs extend the boundaries of you internal network by encrypting and authenticating data. Perform the following high level tasks to set up a VPN:

1. Plan the VPN implementation from end to end.
2. Create the necessary burbs: Select Network > Burb Configuration.
3. Configure the ISAKMP server: Select Policy > Rule Elements > Services and double-click isakmp. Click Properties, then configure the server options and the XAUTH method.
4. Define the VPN: Select VPN Configuration > VPN Definitions.
   You can create certificates and remote identities from this area. However, if you will be using several certificates, it is easier to create them at Maintenance > Certificate Management.
5. Create rules to pass the VPN’s traffic: Select Policy > Rules.
6. Once your VPNs are complete, create a configuration backup: Select Maintenance > Configuration Backup.

For more information on VPNs, see Chapter 19, “Virtual Private Networks,” on page 535: (www.securecomputing.com/goto/manuals).

Configuring HA or OTM

The High Availability (HA) configuration is two appliances that are set up to fail over for each other and therefore reduce network downtime in the event of a system failure. The One-to-Many (OTM) configuration is two or more appliances located in the same network, usually behind load balancers, that automatically synchronize their Sidewinder policies. Perform the following high level tasks to set up an HA or OTM configuration:

1. Make sure both Sidewinder appliance’s are configured identically, particularly the version, the number and names of burbs, and the number and types of interfaces.
2. Configure a dedicated heartbeat burb and interface on each appliance: Select Network > Burb Configuration and Network > Interfaces.
3. Run the State Change Wizard: Select the dashboard and then, in the Device Information area, click the State Change link.
4. Once your new configuration is complete, create another configuration backup: Select Maintenance > Configuration Backup.

For more information on OTM and HA, see Chapter 23, “One-to-Many Clusters,” on page 733 and Chapter 24, “High Availability,” on page 747.
Configuring SmartFilter on Sidewinder

SmartFilter is a web filtering application that helps protect organizations from the risks associated with employee Internet use by filtering out spyware and phishing scams and enforcing an Internet-use policy. Perform these tasks to begin using SmartFilter services through Sidewinder appliance.

- The SmartFilter plugin software is pre-installed on the Sidewinder appliance.
- Make sure you have a SmartFilter serial number.
- Make sure you have purchased a SmartFilter subscription. You do not need to update your Sidewinder license.
- Make sure you have installed the SmartFilter Administration Console and SmartFilter Administration Server software. Use the most recent version available.

In the Sidewinder Admin Console:

1. Set the SmartFilter Server password: Select Policy > Rule Elements > Services, and double-click the sfadmin server service. Click Properties and set the password.
2. Enable Web filtering for the desired HTTP/HTTPS traffic by enabling SmartFilter on the appropriate HTTP and/or HTTPS Application Defenses: Select Policy > Application Defenses > Defenses > HTTP and/or HTTPS. Configure according to your site’s policies.
   - Enable the default SmartFilter rule group.
   - Create a rule for HTTP or HTTPS traffic that you want SmartFilter to monitor and select the application defense you modified in step 2.

In the SmartFilter Administration Console:

1. Add the Sidewinder appliance as a plugin: Select Enterprise Settings > Plugins.
   - Type — Select Sidewinder.
   - Address — Enter the IP address of the burb that has network connectivity from the Sidewinder appliance to the SmartFilter admin server.
   - Password — Enter the password you previously set in the Sidewinder Admin Console (see step 1 in the previous section).

   **Note:** Do not create any groups until you have deployed this information to the SmartFilter plugin.

2. Deploy the plugin.

The appliance is now using SmartFilter to monitor your users’ Web traffic.

For more information, see “Configuring SmartFilter for Sidewinder” on page 267.
Configuring TrustedSource

TrustedSource is a reputation service that filters incoming mail connections and then provides precise information about an e-mail sender's reputation based on its IP address. The TrustedSource reputation service is a tool for reducing the amount of spam that reaches your organization's inboxes. However, unlike spam filters which evaluate message content, TrustedSource focuses on a sender's reputation score. A reputation score is similar to a credit score in that it indicates a sender's trustworthiness. With TrustedSource, the lower the score, the more you can trust the sender.

Perform these tasks to begin using TrustedSource to reject mail from untrustworthy sources.

1 Ensure that your appliance meets these criteria:
   • Is using hosted sendmail
   • Has DNS set up with access to the Internet
   • Is on your network's perimeter
   • Is licensed for TrustedSource — Using TrustedSource on the Sidewinder appliance requires a TrustedSource subscription. The activation is handled by the TrustedSource infrastructure. You do not need to have the Sidewinder Anti-Spam feature licensed to use TrustedSource on Sidewinder.

2 Configure TrustedSource: Select Policy > Application Defenses > Trusted Source. Select the Perform TrustedSource filtering on inbound mail check box. In the Reputation threshold field, set the threshold to a value from 0 to 120. Messages from senders with reputation scores above that value are rejected. The default threshold is 80.

TrustedSource is now checking the reputation of all IP addresses sending mail to the appliance and reject mail from senders with reputation scores above the configured threshold.

For more information, see “Configuring TrustedSource for Sidewinder” on page 257.
Chapter 2: Quick Deployment

Configuring the anti-virus add-on module

The Sidewinder anti-virus add-on module can scan HTTP traffic, FTP traffic, and mail messages for viruses, spyware, and prohibited MIME extensions. Perform these tasks to configure anti-virus & anti-spyware properties.

**Note:** You must be running hosted sendmail servers (Secure Split SMTP servers).

1. If you have purchased your anti-virus add-on module but not yet licensed it, update your license: Select **Maintenance > License**.

   **Note:** If you have not yet purchased this add-on module and would like to use its services, contact your sales representative.

2. Download and install the anti-virus signatures and configure the scanner: Select **Policy > Application Defenses > Virus Scanning**.
   - Advanced tab — Configure settings according to your site’s policies.
   - Signatures tab — Enable automated signature and engine updates.

3. Configure mail anti-virus filtering: Select **Policy > Application Defenses > Defenses > Mail (Sendmail)**.
   - Control tab — Enable MIME/Virus/Spyware.
   - MIME/Virus/Spyware tab — Configure settings according to your site’s policies.

   - Enforcements tab — Enable MIME/Virus/Spyware.
   - MIME/Virus/Spyware tab — Configure settings according to your site’s policies.

   **Note:** For HTTPS anti-virus filtering, see “Configuring the SSL add-on module” on page 21.

   - Enforcements tab — Enable Enforce Virus/Spyware Scanning.
   - Virus/Spyware tab — Configure settings according to your site’s policies.

6. Create rules for the appropriate traffic using application defenses you used in the previous steps: Select **Policy > Rules**.

The appliance is now scanning the designated traffic for viruses, spyware, and disallowed MIME types.

For more information, see “Configuring virus scanning services” on page 251 or the online help.
Configuring the anti-spam add-on module

The Sidewinder anti-spam add-on module can filter your mail for spam and identity-theft related content. Perform these tasks to configure the anti-spam and anti-fraud properties.

**Note:** You must be running hosted sendmail servers (Secure Split SMTP servers).

1. If you have purchased your anti-spam add-on module but not yet licensed it, update your license: Select **Maintenance > License**.

   **Note:** If you have not yet purchased this add-on module and would like to use its services, contact your sales representative.

2. Configure the spam filter server: Select **Policy > Application Defenses > Spam Filter**.
   - **Whitelist Configuration area** — Specify hosts, headers, and regular expressions that, per your site’s policies, the spam filter should ignore.
   - **spamcatcher.conf** — Configure spam thresholds and other parameters to customize how the spamfilter reacts when it encounters spam.

3. Enable the anti-spam filter for mail: Select **Policy > Application Defenses > Defenses > Mail (Sendmail)**, and select the appropriate Application Defense. In the Control tab, enable the Spam/Fraud mail filter option.

4. Create rules for the appropriate mail traffic using the Mail (Sendmail) Application Defense from step 3: Select **Policy > Rules**.

The appliance is now filtering spam out of your mail traffic.

For more information, see “Configuring spam filtering services” on page 261.

Configuring signature-based IPS

The Sidewinder signature-based Intrusion Prevent Services (IPS) prevent network-level attacks from entering your protected network. Perform these tasks to configure content inspection using signature-based IPS.

1. If you have purchased your IPS add-on module but not yet licensed it, update your license: Select **Maintenance > License**.

   **Note:** If you have not yet purchased this add-on module and would like to use its services, contact your sales representative.

2. Download and install the IPS signatures: Select **Policy > IPS**, and click the **Signature Updates** tab.

3. Configure IPS: Select **Policy > IPS**.
   - Configure the Response Mappings.
   - Configure the Signature Groups.

4. Create rules for the appropriate traffic using those response mappings and signature groups: Select **Policy > Rules**.

The appliance is now inspecting the designated traffic for the suspected attacks indicated in the signature categories and responding to it as directed in the response mappings.

For more information, see "Configuring IPS inspection" on page 234.
Perform these tasks to configure SSL decryption. For more details, see the Sidewinder online help.

You may use a supported hardware accelerator board in your Sidewinder appliance to off-load decryption, increasing system performance. If you do not currently have a supported hardware accelerator board installed on your appliance and would like to use one, contact your sales representative for assistance.

1 If you have purchased your SSL decryption add-on module but not yet licensed it, update your license: Select **Maintenance > License**.

   **Note:** If you have not yet purchased this add-on module and would like to use its services, contact your sales representative.

2 [Optional] If using a hardware accelerator, enable the hardware accelerator: Select **Network > Interfaces**, and click the **Hardware Acceleration** tab.

3 [If you have the anti-virus & anti-spyware add-on module] Enable and configure the scanner: Select **Policy > Application Defenses > Virus Scanning**.
   - Advanced tab — Configure settings according to your site’s policies.
   - Signatures tab — Enable automated signature and engine updates.


   **Note:** Be sure to set Type to Server.

   - Enforcements tab — Select Decrypt Web Traffic and configure settings according to your site’s policies.
   - [If you have the anti-virus & anti-spyware add-on module] MIME/Virus tab — Configure settings according to your site’s policies.

5 Create rules for the appropriate traffic using HTTPS Application Defenses: Select **Policy > Rules**.

The appliance is now decrypting SSL traffic.
Chapter 2: Quick Deployment

Configuring the SSL add-on module
CHAPTER 3

Administrator Basics

In this chapter...

Managing your appliance ...............................................................24
Configuring Admin Console access ...............................................35
Restarting or shutting down the system .........................................39
Managing administrator accounts ..................................................44
Changing administrator passwords ................................................48
Using the Admin Console File Editor..............................................48
Administering the Sidewinder appliance using Secure Shell ..........54
Administering the Sidewinder appliance using Telnet .................62
Configuring the Sidewinder appliance to use a UPS .................64
Managing your appliance

This section explains basic Sidewinder appliance management.

- “Understanding Sidewinder appliance management” on page 24
- “Admin Console basics” on page 26
- “Using the Admin Console” on page 30
- “Logging directly into the appliance” on page 34

Understanding Sidewinder appliance management

You can manage the Sidewinder appliance in one of two ways:

- **Admin Console** — The Administration Console (or Admin Console) is the graphical software that runs on a Windows computer within your network.
  - The Admin Console is installed using the “Management Tools” CD.
  - This CD also installs the Quick Start Wizard, which is used to initially configure your Sidewinder appliance.

  See the *Sidewinder Startup Guide* for information on installing the Admin Console software and running the Quick Start Wizard.

  **Note:** The Admin Console is occasionally referred to as “cobra” in some command line tools.

- **command line interface (CLI)** — If you are experienced with UNIX, you can also use the command line interface to configure and manage the appliance. Command line interface refers to any UNIX prompt. The command line interface supports many Sidewinder-specific commands as well as standard UNIX commands you can enter at a UNIX prompt. For example, the `cf` command can perform a wide range of configuration tasks.

  For help using the command line interface, refer to the following:
  - Appendix A, Command Line Reference
  - Manual (man) pages included on the appliance: log into the appliance at a command prompt, type `man` followed by the name of a command, and then press **Enter**
Whether you use the Admin Console or the command line interface, you can manage the appliance from a number of locations. Figure 6 highlights the administration interface options available to you.

**Note:** Normal administration is possible only when the Operational kernel is booted. The appliance in emergency maintenance mode is offline and does not pass traffic.

- The appliance must allow secure sessions for the burb in which the Admin Console workstation resides.
- By default, access is enabled on the appliance’s internal burb. For information on changing Admin Console access on an active Sidewinder appliance, see “Configuring Admin Console access” on page 35.
Admin Console basics

To start the Admin Console on a Windows workstation, do one of the following:

- Select Start > Programs > Secure Computing > Sidewinder 7 Admin Console > Sidewinder Admin Console.
- Double-click the Sidewinder 7 Admin Console icon located on the desktop.

The following window appears:

![Main Admin Console menu](image)

Use this window to connect to and manage one or more appliances.

The main Admin Console window is divided into three areas: the toolbar, the left pane, and the right pane.
About the toolbar

The toolbar at the top of the Admin Console window contains five icons for various shortcut actions:

![Admin Console toolbar](Image)

Table 1: Admin Console toolbar

<table>
<thead>
<tr>
<th>Icon</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Firewall</td>
<td>Click this icon to add an appliance. For more information on adding a new appliance, see “Adding an appliance to the Admin Console” on page 31.</td>
</tr>
<tr>
<td>Save</td>
<td>Save changes to the appliance that you make in the Admin Console by clicking <strong>Save</strong>.</td>
</tr>
<tr>
<td>Rollback</td>
<td>Cancel (or rollback) any unsaved changes in the Admin Console by clicking <strong>Rollback</strong>.</td>
</tr>
<tr>
<td>Refresh</td>
<td>Refresh or update the screen by clicking <strong>Refresh</strong>.</td>
</tr>
<tr>
<td>Help</td>
<td>Access context-sensitive online help for the current Admin Console window that is displayed by clicking <strong>Help</strong>.</td>
</tr>
</tbody>
</table>

The top portion of the window also contains the following menu options:

- **File** — The following options and their respective shortcut keys are available under this menu:
  - **New Firewall (Ctrl+N)**: Add an appliance that can be managed using the Admin Console.
  - **Save (Ctrl+S)**: Save changes.
  - **Cancel (Ctrl+E)**: Cancel changes.
  - **Exit (Alt+X)**: Exit the Admin Console.

- **Help** — The following options are available under this menu:
  - **Window Help**: Display information for the Admin Console window that is selected in the tree. The title for this menu option correlates to the window selected.

  _Note: If you use a browser with a pop-up blocker turned on, you must allow blocked content to view the Sidewinder help._

  - **About (Ctrl+H)**: Display information about the current version of the Admin Console software.
**About the left pane of the Admin Console window**

The left pane of the window contains the Admin Console tree. You can add or delete an appliance from the tree without being connected. Once you are connected to a specific appliance, you can click any of the items in the Admin Console tree to manage that area of your appliance.

You can also right-click an appliance in the Admin Console tree to perform the following actions:

- Delete an appliance from the Admin Console.
- Connect or disconnect an appliance from the Admin Console.
- Expand or collapse all or sections of the branch items beneath an appliance icon.

**About the right pane of the Admin Console window**

The right pane of the Admin Console window displays configuration information for the appliance that is currently selected in the tree:

- **Name** — The name of the appliance.
- **IP Address** — The IP address of the appliance.
- **Port** — The port number used to connect to the appliance.
- **Version** — This is a read-only field that displays the current version of the appliance.
- **Sidewinder State** — This is a read-only field that displays the current appliance state (standalone or part of an HA or One-To-Many cluster).
- **Connect** — Click this to connect to the selected appliance.
Chapter 3: Administrator Basics
Managing your appliance

Admin Console conventions
When using the Admin Console, the following conventions and tips will help you avoid common mistakes:

• To sort or filter a table based on the contents of a single column, right-click a column heading and select the filter criteria for which you want to filter. To customize a filter, select the (Custom) option. To view all items in a table, select the (No Filter) option.

You can also reverse the order of the table within a column by clicking the appropriate column heading. To return the table to its original order, click the column heading a second time.

Note: To filter rules, you must open the Active Rules window.

• You can select an item to modify from a list by double-clicking it, selecting it and then clicking Modify, or right-clicking it and selecting Modify. (Read-only administrators can click View to view an item.)

• When a box preceding an option is filled in or contains a check mark, it is enabled or selected. When the box is empty (a check mark does not appear), the option is disabled.

• On some windows, you need to use the scroll bar to view all of the information or options.

• To delete an item from a list or table in an Admin Console window, click the item to select it, and then click Delete.

• When you leave a window that you have modified, you will automatically be prompted to save your changes before you exit the window. You can also save your modifications at any time by clicking the Save icon in the toolbar (or an OK button for some pop-up windows).

• When you exit a window and do not want to save your changes, click No when prompted to save your changes. You can also cancel your changes at any time by clicking the Rollback icon (or the Cancel button in some windows) to restore the current window’s settings to the last saved version.

• For assistance on any of the Admin Console windows, click the Help icon located in the top portion of the window. The online help provides information about each of the Admin Console windows. To view the entire list of available help topics, click the TOC tab from within the help system.

Note: If you use a browser with a pop-up blocker turned on, you must allow blocked content to view the Sidewinder help.

• To exit the Admin Console, do one of the following:
  – From the File menu, select Exit.
  – Click the X icon in the upper right corner of the Admin Console window.
  – Press Alt+X.

Important: If you have any active connections when you exit the Admin Console, those connections, as well as any unsaved changes, will be lost. You will not be prompted to save before exiting.
Using the Admin Console

Be aware of these conditions when using the Admin Console to manage an appliance:

• This version of the Admin Console is not compatible with 6.x versions of the Admin Console or the Sidewinder appliance.

• The Sidewinder appliance must allow secure sessions for the burb in which the Admin Console workstation resides. By default, access is enabled on the Sidewinder appliance’s internal burb. For information on changing Admin Console access on an active appliance, see “Configuring Admin Console access” on page 35.

Use these procedures to add appliances to the Admin Console tree and to connect and disconnect from an appliance:

• “Adding an appliance to the Admin Console” on page 31
• “Connecting to an appliance” on page 32
• “Disconnecting from an appliance” on page 34
Adding an appliance to the Admin Console

Before you can manage an appliance using the Admin Console, you must first add it to the Admin Console tree.

To add an appliance to the tree, use one of these methods to open the Add Firewall window:

- From the File menu, select New Firewall.
- In the Admin Console toolbar, click the New Firewall icon.
- In the Admin Console left pane, right-click the Firewalls icon and select New from the pop-up menu.

The following window appears:

![Add Firewall window](image)

1 In the Firewall Name field, type a descriptive name for the appliance you are adding. For example, you might specify the host name you used during the installation process. Only alphanumeric characters, dashes (-), and underscores (_) can be used; spaces are not allowed.

2 In the Firewall IP Address field, type the IP address you want to use to access the appliance. The address must be a valid IP address for an interface on the appliance. Also, the interface must be contained within a burb selected for Admin Console access.

3 Click Add to save the information and exit this window. The appliance is displayed in the Admin Console tree in the left pane.
Connecting to an appliance

**Note:** You cannot connect to a 6.x version of the Sidewinder appliance using a 7.x version of the Admin Console.

To connect to a specific appliance, select the appropriate icon from the Admin Console tree and then click **Connect**. The Login window appears.

![Admin Console Login window](image)

The first time you attempt to connect to an appliance using the Admin Console, a pop-up window appears presenting you with the firewall certificate that will be used for all subsequent administrative connections. To accept the certificate, click **Yes**.

If you want to verify the certificate before accepting it, you must obtain the certificate fingerprint before you log into the Admin Console. To obtain the certificate fingerprint, log into the appliance via command line and enter the `srole` command to change to the Admin domain. (If you have not configured remote access, you will need to attach a monitor and keyboard directly to your appliance.) Enter the following command:

```
cf cert view fw name=cert_name
```

The contents of the certificate are displayed. The certificate fingerprint is located at the bottom of the certificate directly beneath the END CERTIFICATE identifier. This fingerprint can be used to verify the fingerprint that is displayed when you initially connect to the appliance via the Admin Console.
To log into an appliance:

1. In the **Username** field, enter your user name.
2. In the **Authenticator** drop-down list, select the appropriate authentication method for the appliance to which you are connecting.
   - **Password** is the default authentication method. Other authentication methods must be configured on the appliance before they are available in this drop-down list.
   - If you want to have a backup authentication method, duplicate the Admin Console rule and select a different authenticator.
   - All methods other than the password method require access to a separate authentication server.
3. Click **OK**. The Password Authentication window appears.
4. Enter your password, and then click **OK**.

When you connect for the first time, the Feature Notification window displays the status of each licensed feature.

**Tip:** If you do not want this window to appear each time you connect, select the **Don't show this again** check box.

5. When you are finished viewing the window, click **Close**.

The main Admin Console window appears.
**Disconnecting from an appliance**

To end an Admin Console session for an appliance:

- In the left tree, select the appliance icon, and click **Disconnect** in the main Admin Console window.
- In the left tree, right-click the appliance icon and select **Disconnect** from the pop-up menu.

This disconnects the Admin Console from the appliance. It does not shut down the appliance.

**Logging directly into the appliance**

You can manage the appliance by command line interface by logging directly into the appliance.

To log directly into the appliance:

1. At the login prompt, type your user name and press **Enter**. The Password prompt appears.
2. Type your password and press **Enter**. The User domain prompt appears:
   
   `appliance_name:User {1} %`

   When you initially log into the appliance using a command prompt, you are logged into the User domain by default. The User domain allows very little access, including no access to sensitive files.
3. To change to the Admin domain, which allows access to all appliance domains (based on your administrative role), enter the following command:
   
   `srole`

4. To return to the previous domain role and shell, enter the following command:
   
   `exit`

   You are returned to the User domain.

*Note: If you have read-only privileges, type srole adminro*
Configuring Admin Console access

The Sidewinder appliance is managed from a Windows workstation installed with the Sidewinder Admin Console. The Admin Console is the graphical user interface used to manage your appliance.

- The Quick Start Wizard enables access on the internal burb. If you want to establish an Admin Console connection to a different burb, modify the Admin Console rule. See “Modifying the Admin Console rule” on page 36 for details.

- When the Admin Console connects to a Sidewinder appliance for the first time, you are prompted to accept a certificate before the connection will continue. A default SSL certificate is initially assigned to the Admin Console.

  Secure Computing recommends assigning a new certificate to the Admin Console before using the appliance in an operational environment. See “Configuring the Admin Console server” on page 37 for details.

- You can configure a banner message that appears when the Admin Console connects to the appliance. This message is generally to alert users that they are accessing proprietary information. The banner window has an Accept button that must be clicked to proceed.

  See “Configuring the Admin Console server” on page 37 for details.

- The default port for the Admin Console is 9003.
  - See Table 32 on page 425 for details on selecting valid ports.
  - To change the port or timeout properties for the Admin Console, see “Configuring the Admin Console server” on page 37.
Modifying the Admin Console rule

Perform this procedure to enable Admin Console access to different burbs.

To modify the Admin Console rule:

2. In the Rules list, expand the Administration rule group, select Admin Console, and click Modify. The Modify Server Rule window appears.
3. From the Source and Destination Burb drop-down lists, select the appropriate burb for your Admin Console connection.
4. Save your changes.
Configuring the Admin Console server

The Admin Console is the graphical user interface used to manage your Sidewinder appliance. The Admin Console connects to the appliance using an SSL connection to a dedicated port (port 9003). When the Admin Console connects to an appliance for the first time, you are prompted to accept a certificate before the connection will continue. The Admin Console service also enforces the TCP idle timeout.

To configure these properties, select **Policy > Rule Elements > Services** and double-click the Admin Console service. The following window appears.

![Figure 13: The Admin Console service window](image)

You can perform the following actions:

- Change the Admin Console’s port and idle timeout values. Defaults are:
  - TCP port: 9003 (See Table 32 on page 425 for details on selecting valid ports.)
  - TCP idle timeout: 0 seconds (This means that there are no timeouts.)
    
    You can click **Restore Defaults** at any time to restore the timeout value.

- Click **Properties** to change the SSL certificate and create an optional logon greeting.

Once the properties match your site’s security policy, click **OK** to return to the main Services window and then save your changes.
About the Admin Console Properties window

Use this window to select the certificate that the Admin Console uses when connecting to the Sidewinder appliance. You can also create a login banner message.

1 In the **SSL Certificate** drop-down list, select a certificate. The certificate will be one of the following:
   - The default certificate
   - A self-signed, RSA/DSA certificate that is defined on the Firewall Certificates tab of the Certificate Management window

2 To use a certificate that is not in the list or to view an existing certificate’s properties, click **Certificates**. The Firewall Certificates window appears. For detailed information on certificates, refer to “Configuring and displaying firewall certificates” on page 589.

3 [Optional] In the Message field, type the text you want to appear when a user connects to the appliance with the Admin Console. This message is generally to alert users that they are accessing proprietary information. The banner window has an **Accept** button that must be clicked to proceed.
   - If you select **Required**, the banner message appears each login attempt.
   - If **Required** is cleared, a **Don’t show this again** option appears on the banner window.
   - Click **Preview** to see a preview of the banner message.

4 Click **OK** to return to the Admin Console service window.

Be sure to save your changes once you return to the main Services window.
You have four shutdown options on the Sidewinder appliance:

- **Reboot to Operational Kernel**
  - The appliance boots to the Operational kernel by default. You can boot to the Operational kernel through the Admin Console or by pressing the power button.
  - You can log into the appliance via the Admin Console and perform administrative tasks.

- **Shutdown to Emergency Maintenance Mode**
  - Emergency Maintenance Mode (EMM) allows you to do repair work with other services turned off. You should use EMM only if directed by Secure Computing Technical Support.
  - The # prompt appears on the appliance, indicating that you are in a login shell and can start issuing Sidewinder or UNIX commands.
  - The appliance in EMM is offline and does not pass traffic.
  - You must connect a console to the appliance in order to work with it. You cannot access the appliance via the Admin Console, SSH, or telnet in emergency maintenance mode.

- **Halt System**
  - The operating system shuts down, but the system remains powered on.
  - Halt System is useful if you need to connect directly to the appliance to access the BIOS.

- **Power Down System**
  - You completely shut down the appliance without restarting.
  - Power down the system before you move your appliance to a new location or make hardware changes.

You can reboot or shut down a Sidewinder appliance from the Admin Console or the command line.

- When the appliance is rebooted or shutdown, a record of who issued the action is logged in the `/var/log/messages` file. This applies to a reboot or shutdown issued from the Admin Console or using the `shutdown` command.

- If the boot process fails, contact Secure Computing Technical Support.
Chapter 3: Administrator Basics

Restarting or shutting down the system

Rebooting or shutting down using the Admin Console

To reboot the Sidewinder appliance or to shut down the appliance completely, select **Maintenance > System Shutdown**. The following window appears:

**Figure 15: System Shutdown window**

To reboot or shut down the appliance:

1. In the **Shutdown Options** area, select the action you want to perform:
   - **Reboot to Operational Kernel** — Restarts the system in the Operational kernel.
   - **Shutdown to Emergency Maintenance Mode** — Restarts the system in emergency maintenance mode and displays the `#` prompt, indicating that you are in a login shell and can start issuing Sidewinder appliance or UNIX commands.
     - While the appliance is in emergency maintenance mode, it is offline and does not pass traffic.
     - You must connect a console to the appliance before you can administer the system in emergency maintenance mode.
   - **Halt System** — Shuts down the operating system, but the system remains powered on. Run this command if you need to connect directly to the appliance to access the BIOS.
   - **Power Down System** — Completely shuts down the appliance software without restarting. Run this command before you move your appliance to a new location or make hardware changes.
2 [Optional] If you want a shutdown message to appear informing users of a pending shutdown, type the message text in the **Shutdown Message** field.

3 In the **Shutdown Time** field, select the shutdown time from the following options.
   - **Shutdown Immediately** — The system will shutdown immediately when you click **Perform Shutdown**.
   - **Delay Shutdown for** — The shutdown will be delayed for the amount of time specified in the **Hours** and **Minutes** fields. You can enter values in these fields that will delay the shutdown for up to 24 hours and 59 minutes.

4 Click **Perform Shutdown** to implement the shutdown.
   Any connections to the Admin Console will be lost when the appliance shuts down. New connections to the appliance will not be allowed once the shutdown process has been executed.
Chapter 3: Administrator Basics

Restarting or shutting down the system

Rebooting or shutting down using a command line interface

The `shutdown` command reboots or shuts down the system from a command line interface. Use this command to indicate how and when you want the appliance to shut down.

The table below shows some common shutdown commands from the command line.

- More information about shutdown options is available on the `shutdown` man page.
- For information on shutting down a Sidewinder appliance that belongs to an HA cluster, see “Scheduling a soft shutdown for a load-sharing HA cluster Sidewinder appliance” on page 775.

**Table 2:** Shutdown commands on the command line

<table>
<thead>
<tr>
<th>Command</th>
<th>Type of shutdown</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>shutdown -r [time]</code></td>
<td>Restarts the system in the Operational kernel.</td>
</tr>
<tr>
<td></td>
<td>For example, <code>shutdown -r +120</code> would reboot the appliance into its Operational kernel in two hours (120 minutes).</td>
</tr>
<tr>
<td><code>shutdown [time]</code></td>
<td>Restarts the system to emergency maintenance mode.</td>
</tr>
<tr>
<td></td>
<td>For example, <code>shutdown now</code> would immediately reboot the appliance into emergency maintenance mode.</td>
</tr>
<tr>
<td><code>shutdown -h [time]</code></td>
<td>Shuts down the appliance without restarting.</td>
</tr>
<tr>
<td></td>
<td>For example, <code>shutdown -h 0601312359</code> would halt the appliance at one minute to midnight on January 31, 2006.</td>
</tr>
<tr>
<td><code>shutdown -p [time]</code></td>
<td>Completely shuts down the system without restarting.</td>
</tr>
<tr>
<td></td>
<td>For example, <code>shutdown -p now</code> would immediately shut down the appliance.</td>
</tr>
</tbody>
</table>

More...
Chapter 3: Administrator Basics

Restarting or shutting down the system

A load-sharing HA cluster always performs a soft shutdown. A soft shutdown provides a buffer period before the actual shutdown occurs.

By default, the soft shutdown process will begin 30 minutes before a scheduled shutdown. If the shutdown is scheduled to occur in less than 30 minutes, the soft shutdown process will begin immediately and will remain in effect until the actual shutdown time occurs.

You can schedule a specific shutdown time for a cluster, or a number of minutes until the shutdown, by using -s. For example:

```
shutdown -r -s +45 +60
```

(reboot in one hour, with soft shutdown in 15 minutes)

```
shutdown -r -s 1500 1800
```

(reboot at 6:00, starting soft shutdown at 3:00)

*Note:* You must include a soft shutdown time if you use the -s command.

<table>
<thead>
<tr>
<th>Command</th>
<th>Type of shutdown</th>
</tr>
</thead>
<tbody>
<tr>
<td>shutdown [-rh] -s soft_time time</td>
<td>A load-sharing HA cluster always performs a soft shutdown. A soft shutdown provides a buffer period before the actual shutdown occurs. By default, the soft shutdown process will begin 30 minutes before a scheduled shutdown. If the shutdown is scheduled to occur in less than 30 minutes, the soft shutdown process will begin immediately and will remain in effect until the actual shutdown time occurs. You can schedule a specific shutdown time for a cluster, or a number of minutes until the shutdown, by using -s. For example: shutdown -r -s +45 +60 (reboot in one hour, with soft shutdown in 15 minutes) shutdown -r -s 1500 1800 (reboot at 6:00, starting soft shutdown at 3:00) <em>Note:</em> You must include a soft shutdown time if you use the -s command.</td>
</tr>
</tbody>
</table>
Managing administrator accounts

Each Sidewinder administrator must have an account created on the system. The initial administrator account, including user name and password for login authentication to the Sidewinder appliance, is created during startup configuration using the Quick Start Wizard. This section describes how to set up and maintain Sidewinder accounts for other administrators.

**Note:** Only administrators have accounts directly on the appliance. People who use Sidewinder networking services have “user” (or network login) accounts, not Sidewinder administrator accounts. See “Authenticating groups from an internal group source” on page 329 for information on creating non-administrative user accounts.

When you add an administrator account, you also assign the new administrator a role. The following table describes the available administrator roles. The following processes explain how to view, add, edit, or delete administrator account information or change role assignments.

**Table 3: Administrator roles**

<table>
<thead>
<tr>
<th>Role</th>
<th>Authorized to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>• Access all windows, menus, and commands within the Admin Console.</td>
</tr>
<tr>
<td></td>
<td>• Add and remove users and assign roles.</td>
</tr>
<tr>
<td></td>
<td>• Do incremental back-ups and restore the system.</td>
</tr>
<tr>
<td></td>
<td>• Use all other system functions and commands.</td>
</tr>
<tr>
<td>adminro</td>
<td>Read access to all windows, menus, and commands within the Admin Console (including monitoring, reporting,</td>
</tr>
<tr>
<td></td>
<td>and auditing). Accessible buttons and windows are labeled View for read-only administrators.</td>
</tr>
<tr>
<td></td>
<td>This role is generally used as an auditor role.</td>
</tr>
<tr>
<td>no admin privileges</td>
<td>Maintains an existing or new administrator account with limited access to the User domain. This role is</td>
</tr>
<tr>
<td></td>
<td>generally used to temporarily disable an administrator account.</td>
</tr>
</tbody>
</table>
To view and manage administrator accounts, select **Maintenance > Administrator Accounts**. The Administrator Accounts window appears.

![Figure 16: Administrator Accounts window](image)

This window displays the administrator accounts currently established on the Sidewinder appliance.

The table identifies the administrator user name, full name, role, and home directory path for each administrator.

You can perform the following actions:

- **Create a new administrator account** — Click **New** and enter the account information in the New Administrator window.

- **Modify an existing administrator account** — Select an administrator in the table and click **Modify**, then make the desired changes in the Modify Administrator window.

- **Delete an existing administrator account** — Select an administrator in the table and click **Delete**.
  - When you delete an administrator account, the user database entry for that administrator is also removed.
  - To automatically delete an account’s home directory when the account is deleted, select **Delete Home Directory Upon Deletion Of User**.
About the New/Modify Administrator window

Use this window to create or modify a Sidewinder administrator account.

**Figure 17:** Administrator Information tab

1. In the **Username** field, type the user name for the administrator. The name can be up to 16 alpha-numeric characters.
   
   If you are modifying an existing account, you cannot change the user name.

   **Important:** **Do not** use uppercase characters in the **username** field, because sendmail will automatically convert the user name to lowercase before mail is delivered. Therefore, any mail addressed to a user name that contains uppercase characters will not be forwarded.

2. In the **Password** field, type a password for this administrator. This is the password the administrator uses when logging into the appliance. Use the following guidelines to create a more effective password:
   
   - Use passwords that are at least 7 or 8 characters in length.
   - Use a mix of upper- and lowercase letters, and non-alphabetic characters such as symbols and numbers.
   - Do not use any easily guessed words or words found in a dictionary, including foreign languages.

   **Note:** If you are modifying the account, dots are displayed in this field.

3. In the **Confirm Password** field, retype the password.

4. [Optional] In the **Full Name** field, type the full name of the administrator.

5. [Optional] In the **Office** field, type the office address of the administrator.
6 [Optional] In the **Office Phone** field, type the office phone number of the administrator.

7 [Optional] In the **Home Phone** field, type the home phone number of the administrator.

8 In the **Directory** field, specify the home directory for this administrator. The default value for this field is /home/username. This field can be modified only if you are creating a new administrator account.

9 In the **Login Shell** drop-down list, specify the UNIX shell that will be used when this administrator logs in.

10 In the **Roles** drop-down list, select the authorized role for this administrator:
   - **admin** — Select this option if you want the user to have administrator privileges for all areas on the appliance.
   - **adminro** — Select this option to allow read privileges only. This role will allow an administrator to view all system information, as well as create and run audit reports. An administrator with read-only privileges cannot commit changes to any area of the appliance.
   - **no admin privileges** — Select this option to limit an administrator’s access to the appliance. An administrator with no admin privileges cannot log into the appliance.

11 Click **Add** or **OK** and save your changes.

You are done creating or modifying this administrator account.
Changing administrator passwords

To change an administrator account password (also known as a UNIX account password), do the following:

**Note:** If you forget your password, you can use the emergency maintenance mode to change your password. See “Changing a forgotten password” on page 824.

1. Select **Maintenance > Administrator Accounts**. The Administrator Accounts window appears.
2. Select the administrator account whose password you want to change, then click **Modify**. The Firewall Accounts: Modify Administrator window appears.
3. In the **Password** field, enter the new administrator account password, then confirm the new password.
4. Click **OK**.

Using the Admin Console File Editor

While administering the Sidewinder appliance, you may find it necessary to modify a text file or a configuration file. Although the typical UNIX editors are available for you to use (vi and emacs), you may find it easier to use the **File Editor** provided with the Admin Console. The File Editor is an easy-to-use editor that is available directly from the Admin Console. The File Editor simplifies the editing process, enabling you to perform virtually every necessary editing task from the Admin Console instead of using a command line.

The File Editor also provides some additional conveniences such as unique file backup and restore features. (UNIX aficionados are still welcome to use the editor of their choice if they prefer.) In addition, using the File Editor through the Admin Console provides a secure connection.

To access the File Editor, select **Maintenance > File Editor**, and then click **Start File Editor**. The following window appears:
Chapter 3: Administrator Basics

Using the Admin Console File Editor

The File Editor window contains three different menu options:

• **File** — This menu contains the basic action options. Use it to open new or existing files, and to save files. The File menu also provides two unique capabilities: it enables you to create a backup copy of a file, and it enables you to restore a file from a previously saved backup copy.

  See “Creating a backup file in the File Editor” on page 50 and “Restoring a file” on page 51 for details.

• **Edit** — Use the functions in this menu to cut, copy, paste, and find/replace text.

  See “Using the Find/Replace option” on page 52 for information on finding and replacing text.

• **Help** — The following options are available under this menu:
  – **File Editor Help** — Displays specific information for the File Editor window.
  – **About Help** — Displays information about the current version of the Admin Console software.

### Opening and saving files in the File Editor

To open a file or save a file with a different name or location: from the File menu, select **Open** or **Save As**. The Open File or Save As window appears.

![Figure 19: Open File window](image)

Follow the steps below.

1. In the **Source** field, select where the source is located:
   - **Local File** — Indicates the file is located on the local Windows workstation or on a network connected to the workstation.
   - **Firewall File** — Indicates the file is located on the appliance.

2. In the **File** field, type the full path name of the file.

   If you do not know the full path name, click **Browse...** to browse the available directories. When you locate the file, click **OK**. The file name appears in the **File** field.

3. Click **OK** to open or save the file, or click **Cancel** to cancel the request.
Creating a backup file in the File Editor

When modifying the Sidewinder configuration files, it is normally a good practice to create a backup copy of the file before you begin editing the file. That way, if you make a mistake while editing the file you can revert to the original file.

The File Editor provides an easy method for creating a backup copy of a file. You can even make a backup after you begin modifying a file. The key is to create the backup before you save your changes. Once you save your changes you will not be able to create a backup file that mirrors the original file.

To make a backup copy of a file, open the file. From the File menu, select Backup. The following window appears:

1. In the Name of Backup File field, specify a name for the backup file. By default, the file is given the same name as the original file but with a .bak extension.
   The backup file will be created in the directory listed in the Current Directory field. This is the directory in which the original file currently resides, and cannot be modified.

2. Click OK to save the information and exit the window, or click Cancel to exit the window without saving the backup file.
Restoring a file

Use the Restore function to restore a file to its original contents.

- The file must be open within the File Editor.
- You must have previously created a backup copy of the file.

From the File menu, select Restore. The following window appears.

![Figure 21: Restore window](image)

1 In the Restore From File field, specify the name of the backup file to use when restoring the file to its original condition. If you do not know the name of the backup file, click Select... to browse the available files. When you locate the file, click Open. The file name appears in the Restore From File field.

   *Note: If a backup file exists, it will appear in the same directory as the current file, because you are only allowed to create a backup in the same directory. The Current Directory field displays the name of that directory and cannot be modified.*

2 Click OK to save the information and exit the window, or click Cancel to exit the window without restoring from the backup file.
Using the Find/Replace option

Use the Find/Replace function to locate character strings, and to replace them with different character strings.

From the Edit menu, select Find/Replace.... The following window appears:

Figure 22: Find/Replace window

1. In the Find what field, specify the character string you want to search for within the file.

2. [Optional] If you want to replace the character string specified in the Find what field with a different character string, type the new string in the Replace with field.

3. In the Search field, specify which direction in the file the search should be performed:
   - **Down** — From your current position within the file, the File Editor will search down (forward) in the file for the specified character string.
   - **Up** — From your current position within the file, the File Editor will search up (backward) in the file for the specified character string.

4. In the Case field, specify whether the File Editor should find any matching character string, or if it should consider upper and lower case when performing the search:
   - **Match** — Find only those character strings that exactly match the case as specified in the Find what field.
   - **Ignore** — Find all matching character strings regardless of upper and lower case.

5. Click Find Next to start the character search and to locate the next occurrence within the file.

   [Optional] If the character search locates a match, you can click Replace to replace the found character string with the character string specified in the Replace with field. To replace all occurrences of the character string, click Replace All. An Info window will appear indicating how many times the character string was replaced. Click OK to close the Info window.
6 To find additional occurrences of the character string, continue to click **Find Next** for each occurrence. When there are no additional occurrences, a message will appear telling you that the search is complete.

7 When you are finished searching, click **Close** to exit this window.
Administering the Sidewinder appliance using Secure Shell

Secure Shell (SSH) provides secure encrypted communication between two hosts over an insecure network, allowing you to securely manage your appliance from a remote location. This section describes how to configure and use the appliance as an SSH server and/or an SSH client.

- The procedures covered in the following sections are based on the use of OpenSSH version, which provides support for SSH version 1.5 and 2.0 sessions.
- sftp and sftp-server are included in OpenSSH and installed on the appliance.

Configuring the SSH server

Your appliance can act as an SSH server, an SSH client, or both.

- If it will act as a server, use the sshd service window to generate a host key.
- If it will act as an SSH client that connects to other Sidewinder appliances, use the sshd service window to generate a client key. See “Configuring and using the Sidewinder appliance as an SSH client” on page 59 for details.

To configure the SSH server:

2. In the list of services, select sshd, and then click Modify.
3. If necessary, change port and timeout settings.
4. Click Properties. The following window appears:

![SSH Server Configuration window](image-url)
Use this window to generate host and client keys, and to specify whether RSA/DSA authentication is allowed. Follow the steps below.

**Tip:** If you plan to export client keys to other appliances, use the Admin Console to connect to the other appliances before starting this procedure.

1. If you want to allow SSH connections to be authenticated using RSA/DSA authentication, select the **Allow RSA Authentication** check box.

   RSA/DSA authentication is a common encryption and authentication system that uses an exchange of public and private keys between the server and the client. It is based on the RSA/DSA algorithm. If this check box is not enabled, all SSH connections must be authenticated using the authentication method selected in the SSH rule.

2. To generate an SSH host authentication key that will be used when the appliance is acting as the server in an SSH connection, click **Generate New Host Key**. The appliance automatically generates the following three authentication keys: RSA1, RSA, and DSA.

3. To generate the SSH version 1.5 client authentication key that will be used when the appliance is acting as a client in an SSH connection, click **Generate New Client Key**.

4. [Conditional] To export the client key to another Sidewinder appliance, click **Export Client Key**.

   A new window appears, listing all Sidewinder appliances with which your Admin Console has an active session. Select which appliances will receive the key and click **OK**.

   You can only export the client key if:

   • you generated a client key as described in step 3, and
   • you currently have an active Admin Console connection with one or more additional Sidewinder appliances (the appliance[s] that will act as the SSH server).

5. Click **OK** to return to the SSH service window.

Be sure to save your changes once you return to the main Services window.

**Configuring the Sidewinder appliance as an SSH server**

On the appliance, SSH is typically used by administrators to log into the appliance securely from a remote machine. In this case the appliance acts as the SSH server.

When configuring the SSH server you have the option to use RSA/DSA authentication. If you use RSA/DSA authentication, the authentication is accomplished via an exchange of public and private keys between the server and the client. The downside of RSA/DSA authentication is that it requires a bit more of an administrative effort. If you elect NOT to use RSA/DSA authentication, the SSH clients must enter their Sidewinder user name and authentication information when initiating the SSH connection.
The following sub-sections provide specific information on configuring the appliance as an SSH server using RSA or DSA authentication, as well as general information on configuring the SSH server.

**Configuring SSH when not using RSA/DSA authentication**

If you are *not* using RSA/DSA authentication, follow the steps below to configure SSH.

1. Disable RSA authentication:
   a. Select **Policy > Rule Elements > Services**.
   b. In the list of services, select **sshd**, and then click **Modify**.
   c. Click **Properties**. The SSH Server Configuration window appears.
   d. Ensure that **Allow RSA Authentication** is disabled.
   e. Click **OK**.
   f. Click **OK** and save your changes.

2. Enable and modify the Secure Shell Server rule:
   a. Select **Policy > Rules**.
   b. In the Rules list, expand **Administration Server**, select **Secure Shell Server**, and then click **Modify**. The Modify Server Rule window appears.
   c. Select **Enable**.
   d. Select the desired source and destination burbs.
   e. Select an authentication method.
   f. Click **OK** and save your changes.

3. [Conditional] If a Host Key Pair does not exist, you will be prompted to confirm that the Admin Console will create an SSH host key. Click **Yes**.

**Note:** *If the client has previously established an SSH connection to the appliance, the information associated with the previous connection must be deleted from the client.*

The appliance is now ready to accept SSH connection requests. Remember that a client must have an administrator account on the appliance in order to log in.
Configuring SSH when using RSA/DXA authentication

If you are using RSA/DXA authentication to authenticate SSH, follow the steps below.

1. Configure the SSH server:
   b. In the list of services, select sshd, and then click Modify.
   c. Click Properties. The SSH Server Configuration window appears.
   d. Verify or select Allow RSA Authentication.
   e. If you do not currently have an SSH host key pair, click Generate New Host Key. Click OK to acknowledge that the new key pair has been created.

You must have at least one SSH host key pair for the SSH server to operate. If you have an existing key pair, you do not need to create a new one. The host key pairs are stored in the /etc/ssh directory and have the following file names:

- `ssh_host_key`            SSH version 1.5 rsa private key
- `ssh_host_key.pub`        SSH version 1.5 rsa public key
- `ssh_host_rsa_key`        SSH version 2.0 rsa private key
- `ssh_host_rsa_key.pub`    SSH version 2.0 rsa public key
- `ssh_host_dsa_key`        SSH version 2.0 dsa private key
- `ssh_host_dsa_key.pub`    SSH version 2.0 dsa public key

f. Click OK.

g. Click OK and save your changes.
2 Create public key directories for each user:
   a From a command line prompt, create a subdirectory named 
      ./ssh in each administrator’s home directory.

   Example: If an administrator named lloyd has a home directory named
   /home/lloyd, create the ./ssh subdirectory by typing the following com-
   mands:

   ```bash
   srole
cd /home/lloyd
mkdir .ssh
   ```

   b Use a text editor to create a file named authorized_keys in each
   administrator’s ./ssh directory.

   Do this using the File Editor provided in the Admin Console, or your
   favorite UNIX editor.

   c Paste each user’s public key into the respective authorized_keys file.

   The method you use to get the public keys onto the Sidewinder appli-
   ance is up to you. You might use FTP, or you might copy/paste from one
   window to another.

3 Enable and modify the Secure Shell Server rule:
   a Select Policy > Rules.

   b In the Rules list, expand Administration Server, select Secure Shell
   Server, and then click Modify. The Modify Server Rule window appears.

   c Select Enable.

   d Select the desired source and destination burbs.

   e Select an authentication method.

   f Click OK and save your changes.

The appliance is now ready to accept connections from SSH clients.
Remember that an administrator must have an account on the appliance in
order to log in.
Configuring and using the Sidewinder appliance as an SSH client

It is also possible for the appliance to act as an SSH client. For example, you might want to establish an SSH connection between two appliances. In this case one appliance operates as the server (via the SSH server), and the other operates as an SSH client. You have the option to use RSA/DSA authentication with the SSH client.

Note: On non-Sidewinder systems, an SSH client that is run from root will bind to a reserved port. As a security feature, the appliance SSH client is not allowed to bind to a reserved port. This is prevented by Type Enforcement.

If not using RSA/DSA authentication

There is nothing to configure on the appliance if you are not using RSA/DSA authentication. To use the appliance as an SSH client, follow the steps below:

1. From a console attached to the appliance, log in and enter srole to switch to the Admn domain.

2. Establish the connection with the SSH server by typing one of the following commands:
   
   ```
   ssh -l login_name address
   
   or
   
   ssh login_name@address
   ```
   
   where:
   
   ```
   login_name = the name used when logging onto the SSH server.
   
   address = the name or address of the host with which you are establishing an SSH connection.
   ```
   
   You have the option to use an authentication method other than the default method when connecting to another Sidewinder appliance. Type a colon and the name of the authentication method after the `login_name` field. For example, to use SafeWord you would type:

   ```
   ssh -l login_name:safeword address
   ```
If using RSA/DSA authentication

To use the Sidewinder appliance as an SSH client while using RSA/DSA authentication, you must perform several configuration steps before initiating the SSH connection.

Configuring the Sidewinder appliance as an SSH client

2. In the list of services, select sshd, and then click Modify.
3. Click Properties. The SSH Server Configuration window appears.
4. Click Generate New Client Key to generate a public and private key pair that the appliance can use when acting as an SSH client. The client public and private keys are created in the /home/username/.ssh directory, where username is the user name you used when connecting to the Admin Console. The file names vary, depending on the SSH version:
   - SSH version 1.5 — The client public key file name is identity.pub and the private key file name is identity.
   - SSH version 2.0 — The client public key file names are id_rsa.pub and id_dsa.pub. The corresponding private key file names are id_rsa and id_dsa.
5. [Conditional] If the SSH server that you will be connecting to is another Sidewinder appliance, connect to that appliance using the Admin Console at this time.
   If needed, click the New Firewall button in the top portion of the Admin Console and add the other appliance(s) to the list of appliances you can administer.
6. If the SSH server that you will be connecting to is another Sidewinder appliance, click Export Client Key to export the public client key to the other Sidewinder appliances. Otherwise, use the best available method (FTP, cut and paste, etc.) to export the public client key to the SSH server.
7. Select the appliance to export to, and click OK.
Using the Sidewinder appliance as an SSH client

1. At a Sidewinder command prompt, enter the following command to switch to the Admn role:
   
   \texttt{srole}

2. Establish the connection with the SSH server by typing the following command:
   
   \texttt{ssh -l login\_name hostname}

   where:

   \texttt{login\_name} = the user name used when logging onto the SSH server

   \texttt{hostname} = the host name or address of the host with which you are establishing an SSH connection

   See the \texttt{ssh} man page for more details.

On the appliance, the SSH client must be run from the Admn domain. Many SSH servers, however, do not allow root users to connect to the SSH server. To get around this, be sure to use the \texttt{-l} option when logging in. This allows you to login as a different user.

---

Tips on using SSH with the Sidewinder appliance

Please note the following information about SSH on the appliance.

- There are two configuration files associated with SSH:
  - For the SSH server: \texttt{/etc/ssh/sshd\_config}
  - For the SSH client: \texttt{/etc/ssh/ssh\_config}

- See the \texttt{ssh}, \texttt{sshd}, \texttt{ssh\_config}, \texttt{sshd\_config}, and \texttt{ssh\_keygen} man pages for additional details.

- The appliance’s SSH server and client are based on the \textit{OpenSSH} implementation. See \url{http://www.openssh.com} for more information.
To troubleshoot Sidewinder appliance problems using a command line interface rather than the Admin Console, you can configure Telnet services that allow you to connect from a system within your network. You can also allow trusted users to use a Telnet client to log into Internet systems remotely.

Setting up an internal (trusted) Telnet server

Telnet provides a way to log into a system in your network from another system. All you need to know is the name of the system in which you want to log in. Once you have established a connection, you are logged in just as you would be if you were physically located at that system.

A Telnet server is defined for each burb on your appliance: one for the external (Internet) burb and one for each of the internal (or trusted) burbs. This gives you the capability to Telnet to the appliance from any system on an internal burb so you can perform administrative tasks remotely.

**Note:** For security reasons, the Telnet servers are not initially enabled.

Create a rule to access the trusted Telnet server. Include these selections:

- Select **telnetd (Telnet Server)** as the service.
- Select the source and destination burbs you want the Telnet server to access.
- Select an authentication method. All users accessing a Telnet server must be authenticated.

To perform Sidewinder administration tasks, you must have an account on the appliance as described on “Managing administrator accounts” on page 44. Aside from your account and authentication information, all you need to log into the appliance is the name or address. To log into the appliance using Telnet, see “Connecting to the Sidewinder appliance using Telnet” on page 63.

Setting up an external Telnet server

The Sidewinder appliance allows you to enable an external Telnet server. An external server resides on the external network side of the appliance, and is available to Internet users once you set up the appropriate “allow” rules. (The other Telnet servers reside on the internal side of the appliance and are available only to trusted users.)

**Security Alert:** Setting up a Telnet server on the external side of your appliance can raise security issues. Contact Secure Computing Technical Support before attempting this.
Connecting to the Sidewinder appliance using Telnet

**Note:** You must enable the Telnet server in the appropriate burb(s) before you will be allowed to Telnet. See “Setting up an internal (trusted) Telnet server” on page 62.

1. Telnet to the appliance and log in by typing the following command, using your Sidewinder host name.

   ```bash
   telnet hostname
   ```

   When prompted, enter your Sidewinder authentication information. Depending on the authentication method configured for you on the appliance, you must provide a valid password or a special passcode or personal identification number (PIN) before you are logged on to the appliance.

2. Enter the following command:

   ```bash
   srole
   ```

   Enter commands from the UNIX prompt as required. Refer to Appendix A or the `man` pages for information on using individual commands.
Many organizations connect the Sidewinder appliance to an Uninterruptible Power Supply (UPS). This allows the Sidewinder appliance to continue to be operational if a power outage occurs. If the power outage is long enough, however, the battery in the UPS will begin to fail. To avoid an uncontrolled shutdown, you can configure the appliance to initiate an orderly shutdown before the UPS fails. The appliance is much more likely to restart in a good condition following an orderly shutdown than from an uncontrolled shutdown.

[Conditional] If you connect your UPS device to the Sidewinder appliance’s COM1 port, you must perform this procedure before configuring UPS:

1. From a console attached to the appliance, log in and enter `srole` to switch to the Admn domain.
2. At the Admn prompt, type the following command:
   
   ```
   setconsole video
   ```
3. Reboot the Sidewinder appliance.

To configure the appliance to use a UPS:

1. Connect the UPS’s serial cable to the appliance’s COM1 or COM2 port. (Use a simple signaling cable.)

   **Important:** You must connect the UPS to the appliance before enabling UPS in the Admin Console. If you enable UPS without an attached UPS, the system shuts down immediately.

2. Select Maintenance > UPS. The UPS window appears.

![Figure 24: UPS window]
3 Select **Enable Uninterruptible Power Supply (UPS)**.
   • If a UPS is enabled and a power outage occurs, the appliance will monitor the UPS and will perform an orderly shutdown when the UPS battery begins to run low.
   • If a UPS is not enabled, and a power outage occurs, and the appliance *is* connected to a UPS, the appliance will not monitor the UPS and will not perform an orderly shutdown when the UPS battery begins to run low.

4 From the **UPS Serial Port** drop-down list, select the port the UPS is connected to.

5 In the **Battery Time** field, specify the estimated amount of time (in seconds) that the UPS battery will last before running low. The appliance will initiate an orderly shutdown when this timer expires, regardless of the amount of battery power remaining in the UPS.

6 Save your changes.
Configuring the Sidewinder appliance to use a UPS
In this chapter...

Understanding traffic basics ...........................................................70
A brief guide to planning your policy ..............................................71
Using groups to simplify policy management .................................72
Ordering rules within your policy ....................................................75
Example of a simple rule ................................................................77
Understanding traffic basics

Your site’s security policy is implemented and enforced by applying rules to all traffic that passes through the Sidewinder appliance. Each rule is basically a mini policy that contains criteria which are used to inspect incoming or outgoing traffic. Rules determine whether that traffic will be allowed to continue to its destination. This section introduces the different ways traffic can be directed through or into the appliance.

Your security policy needs to cover what your organization wants to allow out of its perimeter (outbound traffic), what it wants to allow through its perimeter (inbound traffic), and what is allowed into the Sidewinder appliance (management traffic, such as SSH). When planning your security policy, consider your organization’s traffic requirements and how they fit into these categories. If your site has more than two burbs, you may need to create rules that start in one burb and end in another without heading out to the Internet.

The source endpoint specifies where a connection is allowed to initiate. The destination endpoint controls where a connection is allowed to go. When the appliance allows a system to initiate a connection, it automatically allows the response to that session, without needing a separate rule. For example, if you allow outbound HTTP requests, you do not need a separate rule to allow the replies to those requests; the appliance handles this for you.

**Figure 25:** Types of rules you can use in your security policy

![Diagram of different types of rules](image)

**Inbound policy**

Inbound rules govern traffic that initiates in an untrusted network area. By default, the appliance does not allow any inbound traffic. Inbound rules represent a prominent threat to your network’s security, and therefore should be controlled with authentication or directed to a sacrificial burb that only contains publicly-accessible servers that can recover quickly from attacks and do not contain confidential information. You can also increase your network’s security by creating an inbound policy that is as specific as possible. The source should be the smallest possible unit, such as an IP address, or a narrow subnet or IP address range if it cannot be that precise. Other available protections include using authentication and directing traffic into a burb that does not have access to systems with confidential or business-critical information. Your inbound security policy should address any filtering, scanning, or inspection services you want the appliance to provide.
**Outbound policy**

Outbound rules govern traffic that is allowed to initiate on a protected, trusted burb and then heads for an external destination. Your outbound policy should focus on providing your internal employees and systems access to the resources needed for them to do their jobs. Smaller organizations can probably use the default policy, which includes commonly used services such as HTTP, HTTPS, and RealMedia™. Larger organizations probably need access to more services than those in the default policy and will need to create customized rules. Since the initiators of outbound rules are generally trusted, these rules are less likely to be candidates for filtering services, but there are exceptions. For example, filtering your internal users' web requests using SmartFilter can reduce bandwidth consumption. Also, if an attack or virus does manage to get into your network, inspecting outgoing traffic for malicious content can help contain damage to others.

**Management policy**

A small but important part of your policy will cover traffic that talks directly to a server on the appliance as opposed to passing traffic through it. Sidewinder servers provide the following: management and administration services, routing services, VPN services, communication with external clients, and inter-appliance communication in clustered and enterprise-distributed Sidewinder appliances. Examine the default server rules and determine if your organization will need to enable any of the existing rules or create additional server rules. When creating these rules, make the endpoint as specific as possible to increase security.

Creating an effective security policy requires careful planning and implementation. The following steps are guidelines to creating the policy that is right for your organization:

1. Determine your site’s overall security policy. This involves writing down detailed instructions about what can and cannot pass through your network perimeter. In most organizations, it is important to get the policy approved by one or more levels of management.

2. Once the policy is documented and approved, determine what rules are needed to put the approved policy into place.

3. Search your policy for patterns, such as rules that allow access to the same sources and destinations but use different services. These similarities are opportunities to create groups within your policy that will simplify the long-term task of managing your security policy.

4. Once all needed rules are identified, order your rule set. Put frequently-used rules at the top and infrequently-used rules at the bottom, as this optimizes processing. Also be sure to put more restrictive rules before less-restrictive rules.

Adequate preparation greatly improves the quality of your security policy and reduces future management overhead.
Using groups to simplify policy management

Using groups can be an efficient way to reduce the footprint of your security policy. A group is a way to set up a one-to-many relationship for elements that have similar security requirements. While a typical rule regulates access for a single element, a single rule that is implemented using groups can regulate access for multiple elements. Once the rules are created, the rules themselves can also be grouped to reduce management overhead. Grouping enables you to reduce the overall number of rules you define, which in turn reduces the complexity of your rule database. A less complex rule database means there is less chance of introducing errors that may affect the integrity of your security policy.

Several rule elements can be grouped to reduce the number of rules in your policy. Once you know what rules you need to implement your security policy, search for patterns of rules having similar requirements, such as traffic from different internal burbs using similar services to reach the Internet. Read the following sections to learn more about grouping different Sidewinder elements.

**Service groups**

A service group is a group of services of the same type; it cannot contain a mix of proxies, filters, and servers.

A rule will always apply the same properties to all services in a service group. The services in a service group can be either all allowed or all denied. It is not possible to use the same rule to allow access to a subset of services in a service group while at the same time deny access to a different subset of services. Service groups are extremely effective when implemented in a rule that regulates access for a user group or netgroup. Keep in mind, however, that all members in the user group or netgroup must conform to the same security policy (that is they will all be allowed or denied access to the same collection of services).

You can only use both service groups and authentication in a rule if all the services in the group support authentication.

**Burb groups**

Burb groups are a way to categorize multiple burbs that require a similar security policy. When you select a burb group as an endpoint in a rule, that rule will apply to each burb in the burb group. A source burb or a destination burb cannot contain both a burb group and an individual burb, but can contain multiple burb groups or multiple individual burbs. However, the source and destination can be different. For example, the source could contain one or more individual burbs and the destination could contain one or more burb groups.
Netgroups

Netgroups are a way to use multiple network objects in a single rule. The netgroup can be made up of any combination of available network objects: host, domain, IP address, IP range, netmap, and subnet. You may find it more convenient to create all of your network objects before defining your netgroup objects. That way, as you set up your netgroup objects, you will be able to immediately assign the desired network objects to the group.

Application Defense groups

Application Defenses can be grouped to be used in rules that use service groups. When you create an Application Defense group, you select a single Application Defense from each category (for example, HTTP, HTTPS, FTP, etc.) to populate that Application Defense group, although only the Application Defenses that apply to that rule’s services will be implemented in the rule.

You can also set an Application Defense group as the default group. The purpose of this group is to be a container for each application’s default settings. For example, you would make sure that the each Application Defense in group (HTTP, HTTPS, FTP, etc.) was configured using your site’s most common settings for that application. The default Application Defense group is used in all new rules using an Application Defense.

Rule groups

After you plan and create all of the rules you need to enforce your security policy, you can organize them into sets, called rule groups. A rule group can consist of both rules and nested rule groups. A nested rule group is a rule group that you place within another rule group. You can nest multiple rule groups within a rule group.

Figure 26 demonstrates the basic structure of a rule group that uses nested rules.

Use rule groups to keep rules with similar functions together. This simplifies management overhead for when you need to enable or disable all rules for this function or change their placement in your policy.
**Example of using groups in a rule**

Here’s an example that illustrates the power of using groups. Not all types of groups are used in the example, but the management properties are similar for those groups not included.

Assume you have a netgroup named eng_netgroup that consists of all subnets assigned to engineers in your organization. If you want to grant HTTP, FTP, and MS SQL access to this group, you might do so by defining three separate rules. Table 4 illustrates how these three rules might look in the rule database.

Important: In general, user groups can be used in an allow rule only if the specified service supports authentication (login, Telnet, FTP, HTTP, or secure shell [SSH]). If you want to authenticate other protocols based on user groups, use the Passport authenticator to provide single sign-on access.

**Table 4: Typical rules not using groups**

<table>
<thead>
<tr>
<th>Name</th>
<th>Service</th>
<th>Source</th>
<th>Source endpoint</th>
<th>Destination</th>
<th>Destination endpoint</th>
<th>Application Defense</th>
</tr>
</thead>
<tbody>
<tr>
<td>http_out</td>
<td>HTTP</td>
<td>internal</td>
<td>eng_netgroup</td>
<td>Lab</td>
<td>&lt;any&gt;</td>
<td>HTTP_default</td>
</tr>
<tr>
<td>ftp_out</td>
<td>FTP</td>
<td>internal</td>
<td>eng_netgroup</td>
<td>Lab</td>
<td>&lt;any&gt;</td>
<td>FTP_default</td>
</tr>
<tr>
<td>mssql_out</td>
<td>MS SQL</td>
<td>internal</td>
<td>eng_netgroup</td>
<td>Lab</td>
<td>&lt;any&gt;</td>
<td>MSSQL_default</td>
</tr>
</tbody>
</table>

A better option, however, is to use a service group. This enables you to accomplish the same thing with one rule. Create a service group that contains the HTTP, FTP, and MS SQL proxies, then use this service group when defining the rule. You can also make sure that your default Application Defense group has the proper HTTP, FTP, and MS SQL settings. Table 5 illustrates the resulting rule using the service group and the default Application Defense group.

**Table 5: Sample rule using groups**

<table>
<thead>
<tr>
<th>Name</th>
<th>Service</th>
<th>Source</th>
<th>Source endpoint</th>
<th>Destination</th>
<th>Destination endpoint</th>
<th>Application Defense</th>
</tr>
</thead>
<tbody>
<tr>
<td>eng_to_lab</td>
<td>EngServGrp (HTTP, FTP, MS SQL)</td>
<td>internal</td>
<td>eng_netgroup</td>
<td>Lab</td>
<td>&lt;any&gt;</td>
<td>default_group</td>
</tr>
</tbody>
</table>
Ordering rules within your policy

The order in which rules and nested groups appear in your security policy is significant. When the appliance is looking for a rule match, it searches the enabled rules in sequential order (beginning with the first rule or nested group within the group, then the second, and so on). If the traffic does not match the first rule, it is forwarded on to the next rule. The first rule that matches all the characteristics of the connection request (service, source, destination, and so on) manages the connection. Once a rule match is found, the traffic is processed according to that rule and the search stops. You should always place rules that allow or deny the most frequent traffic near the top of your security policy to reduce processing time.

The default policy contains a Deny All rule at the end of the policy. This rule denies any traffic that reaches it. The rule itself is a reminder that any traffic that does not match a rule is automatically denied; even if the rule is deleted, the appliance denies any traffic that does not find an exact match in your security policy.

The following figure depicts first-match processing.

Figure 27: How traffic finds its matching rule

Note: In general, proxy and filter rules can be listed in any order and will be processed sequentially. However, for proxy rules where the source or destination endpoint includes a domain object to be processed correctly, those rules must be placed after the last filter rule.
For example, suppose you want to allow access to FTP services on the Internet for all systems except those included in a netgroup called *interns*. The scenarios below illustrate both the incorrect and correct rule placement.

**Incorrect placement of rules**

The following shows a rule group order that is *incorrect* for this scenario.

| Rule 1: | Allow FTP service for all internal systems to all external systems. |
| Rule 2: | Deny FTP service for the netgroup *interns* to all external systems. |

The first rule in the rule group allows all systems (via a wildcard) to use FTP and the second rule denies one particular netgroup.

**Problem:** When a system specified in the “*interns*” netgroup requests an FTP connection to somewhere in the Internet, the appliance will check rule 1. Because that rule allows all systems FTP service to the Internet, the appliance detects a match, stops searching the rule group, and grants the connection.

**Correct placement of rules**

To deny a particular netgroup, the deny rule should be placed *before* the allow rule. The correct way to order the rules in this rule group is as follows.

| Rule 1: | Deny FTP service for the netgroup *interns* to all external systems. |
| Rule 2: | Allow FTP service for all internal systems to all external systems. |

**Important:** As a basic guideline when configuring a rule group, place specific rules *before* any general (wildcard) rules.

The following scenario walks you through the basic process used by the appliance to process an outbound H.323 proxy connection request. This scenario assumes that the active rules consist of the following items:

- An enabled rule named **Internet Services**, which includes a service group that allows access to the most commonly used Internet services.
- An enabled rule group named **Administration**, which allows Sidewinder administrators to access the appliance.
- A disabled rule named **VoIP H.323** that allows voice over IP access via the H.323 proxy service.
- An enabled rule named **NetMeeting** that allows users to use audio and video conferencing components for NetMeeting®. This rule includes a service group that allows access to the H.323 and the T.120 proxy services.
- An enabled **Deny All** rule that will deny any requests that did not match any other rules.
The following steps outline the basic processing that takes place when an outbound H.323 connection request arrives at an appliance with the above rules in place:

1. An outbound H.323 request arrives at the appliance.
2. The request is processed by the first rule, which is the Internet Services rule. The request does not match the rule criteria.
3. The request is forwarded to the next rule, a rule group called Administration, and is inspected in sequential order by each rule contained within that group. No match is found in this rule group.
4. The request bypasses the VoIP H.323 rule because the rule is disabled.
5. The request is forwarded to the next rule, the NetMeeting rule. A match is found (because the H.323 proxy service is included in the service group used in this rule).
6. The request is processed according to the specifications in the NetMeeting rule. The request bypasses all other rules and groups contained in the active rules, and the request is granted.

Example of a simple rule

This section provides an example of a simple rule to help you better understand how the appliance uses a rule to determine whether to allow or deny a connection request, and how to handle allowed connections. For a detailed explanation of rules elements and their function in a rule, see “Understanding rules” on page 82.

The following table lists the condition elements for a rule that permits any client in an internal burb to connect to any Web server located in the external burb. Conditional elements are the elements that a rule examines to see if a packet matches that rule. Figure 28 on page 79 shows where these settings are in the Rule window. The fields corresponding to the criteria described in the table are indicated in the figure.

There are also a number of action elements you can configure for each rule. After a rule determines that a packet matches its condition elements, the rule handles the packet according to the action elements’ values. The action elements are whether or not to allow the connection or session, what amount of audit data to generate, if the address should be translated, what Application Defense settings to enforce, and if the traffic will be compared to a set of IPS signatures.
### Table 6: Rule elements that determine if a packet will match a rule

<table>
<thead>
<tr>
<th>Condition rule elements</th>
<th>Setting</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>Checked</td>
<td>Disabled rules do not process traffic.</td>
</tr>
<tr>
<td>Service</td>
<td>HTTP (HTTP Proxy)</td>
<td>This rule uses the default HTTP proxy service, which is for TCP traffic on port 80 with default timeout and expected connection values, and passes traffic transparently (browsers do not need to point to the Sidewinder appliance).</td>
</tr>
<tr>
<td>Source Burb</td>
<td>internal</td>
<td>Traffic will originate in the internal burb.</td>
</tr>
<tr>
<td>Source Endpoint</td>
<td>&lt;Any&gt;</td>
<td>Traffic can originate from any IP address in the internal burb.</td>
</tr>
<tr>
<td>Destination Burb</td>
<td>external</td>
<td>Traffic will be delivered to the external burb.</td>
</tr>
<tr>
<td>Destination Endpoint</td>
<td>&lt;Any&gt;</td>
<td>Traffic can be delivered to any IP address reachable via the external burb.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Passport</td>
<td>Users must authenticate the first time they use this rule to connect to an external Web server. Subsequent connection will be authenticated from a cache.</td>
</tr>
</tbody>
</table>
Figure 28: Screen shot of a basic rule with condition elements identified
Chapter 4: General Policy Configuration

Example of a simple rule
In this chapter...

Understanding rules ................................................................. 82
Using NAT and redirection in rules ........................................ 85
Viewing and ordering rules and rule groups ....................... 87
Creating, modifying, and duplicating rules ....................... 95
Creating and modifying rule groups .................................. 102
Viewing and modifying rule elements ............................... 103
Understanding rules

A rule is made up of many elements. The basics include the service (which provides the protocol and port requirements), the source and destination, a time period, and authentication requirements; these are known as condition elements. If a packet matches all these parameters exactly, the appliance then refers to the rule’s action elements for instructions on how to handle the packet. Action elements include the allow/deny/drop action, the audit level, the application defense settings, and the intrusion protection parameters.

The following sections describe the different rule elements and how to use them in a rule.

Condition rule elements

This section describes the elements that a rule examines to see if a packet matches that rule. If the packet does not match all of these elements’ values, the packet passes to the next rule. If the packet does match all of these elements’ values, the rule handles the packet according to the action elements’ values.

Services

Services determine a rule’s protocol, port, and timeout values. There are three distinct service types:

- **Proxies** — Proxy services inspect traffic at the application layer. Proxy rules determine whether traffic will be allowed or denied using basic criteria such as protocol, port, source and destination address, but can also inspect the traffic to make sure it complies to its protocol’s standards. Many proxy services also allow for advanced filtering and scanning services.

  For more information, see “Understanding proxy agents and services” on page 116.

- **Filters** — Filter services inspect traffic at the network and transport layers. Filters operate directly on the IP packets, allowing the appliance to securely forward IP packets between networks. Filter rules determine whether traffic will be allowed or denied using basic criteria such as protocol, port, source and destination address. Very little protocol and content inspection is available when using filter services. Because filters are inherently less secure than proxies, filter services should be used only when necessary.

  For more information, see “Understanding filter agents and services” on page 134.

- **Servers** — Server services allow you to control access to Sidewinder-hosted servers. Servers are typically used in management traffic rules where an administrator or another system needs to communicate directly with the appliance. Many of the server rules are created and enabled automatically. A few servers, such as the Sendmail® server, allow for extensive configuration of its server properties, but most servers do not require changes to their default settings.
Sources and destinations

A rule’s source and destination determine what can initiate traffic and what can respond to traffic that passes through, or into, the appliance. The source and destination consist of these properties:

- **Burb** — The area of the network containing the endpoint. This value can be a single burb, multiple burbs, a burb group, or multiple burb groups.

- **Endpoint** — The network object that can initiate or respond to connections or sessions. Network objects can be a host, a domain, an IP address, a range of IP addresses, a subnet, a netmap (a way to map multiple IP addresses and subnets to alternate addresses without creating numerous rules), or a group that contains any combinations of those objects.

- **Network address translation (source)** — The address that replaces the original source address.
  
  See “Using NAT and redirection in rules” on page 85 for more information.

- **Address redirection (destination)** — The address that replaces the original destination address. Redirection can also change the original destination port to a different port.
  
  See “Using NAT and redirection in rules” on page 85 for more information.

Time periods

Time period rule elements determine the segment of time a rule is in effect. Time periods can be recurring, meaning the rule is active for the same time on the same day every week, or continuous, which means the rule is only active for a single period of time.

When creating a rule, you also have the option to set start and end times for rules. Delayed start times and scheduled end times are useful for making policy changes with minimal disruption to your production network.

Authentication

Authentication validates a user’s identity before he or she is allowed to access a network service or server. Authentication works together with user groups to control who can access what services. Authentication can be used on rules controlling access to the appliance and through the appliance. Available authentication methods are: Password, Passport (single sign on), SafeWord®, Radius, iPlanet, Active Directory, OpenLDAP, Custom LDAP, and Windows Domain.
Action rule elements

After a rule determines that a packet matches its condition elements, the rule handles the packet according to the action elements’ values.

Action

A rule’s action determines what the appliance will do once it matches traffic to that rule. Options are:

- **Allow** — Permits the traffic to continue to its destination.
- **Deny** — Prevents the traffic from going through the appliance and sends the source a message that its request was rejected.
- **Drop** — Prevents the traffic from going through the appliance but does not send a RST response to the originating host. This option is used to save processing cycles or to mask that the appliance is listening on a given port.

Audit

Audit levels determine how much audit data a rule will generate on a per-rule basis. By default, all rules generate connection data that includes the packet’s source, destination, and service. The amount of audit data generated can be increased to aid in troubleshooting or decreased to view errors only.

Application Defenses

Application Defenses determine advanced application-specific properties. They can be used with packet filter services, most proxy services, and the sendmail server service.

- Application Defenses for proxy services can be used to enforce RFC (Request for Comments) standards and allowed parameters. Configurable parameters include headers, commands, versions, and file sizes. Key inspection services, such as anti-virus/anti-spyware, anti-spam/anti-fraud, SSL decryption, and Web services management, are enabled in their respective proxy’s Application Defense.

- Application Defenses for filter services can be used to control request and response rates, error and control messages, and the audit rate for denied filter rules.

Intrusion Prevention Systems (IPS)

The IPS area consists of both a signature group and a response mapping. The signature group identifies which signatures of known network-based intrusion attacks to compare to the packet. The response mappings indicate what to do if an attack payload in the packet matches an attack signature. Available options are to allow, deny, drop, or blackhole the offending packet.
Using NAT and redirection in rules

You can configure rules to perform NAT (network address translation) or redirection. NAT and redirection are essentially the same thing: replacing an original address with another specified address. NAT indicates that the appliance will rewrite the source address. Redirect indicates that the appliance will rewrite the destination address. The following sections give examples of when to use address translation and how to configure NAT and redirection in rules.

Understanding and configuring NAT

NAT refers to rewriting a packet’s source address. When the appliance receives the packet, it removes the original source address and replaces it with the address or host name specified in the matching rule. The destination host is only aware of the translated address.

A common reason to use NAT is that your internal network uses private addressing that needs to be replaced by a publicly routable address. By default, all outbound rules are translated to use localhost. Localhost is a network object that automatically maps to the IP address of the specified burb, which is often the destination burb.Aliases are also frequently used in NAT.

In the example shown in Figure 29, a host on internal network 172.17.0.0 requires Telnet access to the external network 192.101.0.0. The IP address of a host on the privately addressed internal network should not be passed through the appliance; traffic sent from the internal network to the external network should appear as if it originated at the appliance’s publicly routable IP address.

![Figure 29: Example of network address translation](image)

The associated outbound rule must translate the internal host address to the appliance’s external address. Configure the rule’s NAT information as follows:

<table>
<thead>
<tr>
<th>Source burb: internal</th>
<th>Destination burb: external</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source endpoint: 172.17.0.0 (internal subnet)</td>
<td>Destination endpoint: 192.101.0.2 (destination address)</td>
</tr>
<tr>
<td>NAT address: localhost</td>
<td>Redirect: None</td>
</tr>
</tbody>
</table>

Note: In an audit entry for a rule using NAT, the source IP will be the original source IP. The NAT address will not appear in the audit.
Understanding and configuring redirection

Redirection refers to rewriting the destination address of the packet. The originating host sends the packet to one address, and then the appliance sends the packet to the specified redirection address. The original destination address is often the IP address of appliance’s external burb or an alias assigned to that burb.

A common reason to direct traffic to one address and then redirect it to another address is when the internal object has a non-Internet routable address. Other uses include redirecting several different aliases to the same backend server for the purpose of data collection, and allowing authenticated users access to a protected server while redirecting all other uses to another server.

In the example shown in Figure 30, an external network at 192.101.0.0 requires Telnet access to the internal host at 172.17.120.123. However, 192.101.0.0 is not allowed to directly route to the internal host. External hosts must initiate a Telnet connection to the appliance’s external side.

**Figure 30:** Example of redirection

The associated inbound rule must rewrite the destination address to that of the internal host and forward the traffic onward. Configure the rule’s redirection information as follows:

<table>
<thead>
<tr>
<th>Source burb: external</th>
<th>Destination burb: internal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source endpoint: 192.101.0.0 (source subnet)</td>
<td>Destination endpoint: localhost</td>
</tr>
<tr>
<td>NAT address: &lt;None&gt;</td>
<td>Redirect: 172.17.120.123 (internal host)</td>
</tr>
</tbody>
</table>

*Note:* In an audit entry for a rule using redirection, the destination IP will be the final destination IP. The original destination address will not appear in the audit.
Rules are the basis of your security policy. They determine what traffic will be allowed to pass through your Sidewinder appliance and what will be denied. To view or manage your rules, select **Policy > Rules**. The main Rules window appears.

This window provides an overview of your security policy. It is where you view rules, adjust rule order, and enable or disable rules. It is also the starting point for creating and modifying rules and rule groups.

### Organizing your security policy

The order of your rules determines the order in which traffic is processed. When the appliance receives a packet, it starts with the first rule in its access control list (list of rules) and continues until it finds an exact match.

The following are guidelines for organizing and maintaining your security policy:

- Organize rules based on how frequently they are used. If you expect a rule to be widely used, such as a rule granting company-wide outbound HTTP access, put that rule near the beginning of your policy.
- Place specific rules before general rules. If you want to deny access to one group, such as contractors, while still allowing access for employees, put the rule denying contractors’ access before the rule allowing employees’ access.
- Audit your rules periodically. Look for rules that are no longer in use and rules that can be combined by using groups, such as service groups, netgroups, or application defense groups.

**Important:** Do not disable or delete the login rules located in the Administration rule group, or place them below the Deny All rule. If these rules have been modified and you can no longer log in, see “Troubleshooting logging in” on page 823 for assistance.
About the default Sidewinder policy

The Sidewinder appliance’s default configuration creates a few commonly used rules for you. This policy includes outbound rules and management rules, but no inbound rules. The default rules that are deemed essential for basic management or standard functionality are enabled. During the Quick Start Wizard, you can choose to also enable a rule that allows access to a pre-configured group of commonly used Internet services. The other default rules are rules that you are likely to use at some point, but do not need to enable until required by your site’s policy.

The initial enabled rules are listed in the following table:

Table 7: Initial active policy

<table>
<thead>
<tr>
<th>Proxy rule name</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>dnsp (names vary)</td>
<td>Allow DNS traffic to proxy between indicated burbs. Which rules are created depends on the location of the DNS resolver IP addresses (internal burb, external burb, or assumed to be reachable by the default route) provided in the Network Information window.</td>
</tr>
<tr>
<td>Admin Console</td>
<td>Allows administrators on the internal burb to connect to the appliance’s internal interface using the Admin Console.</td>
</tr>
<tr>
<td>Login Console</td>
<td>Allows administrators to log in directly at the appliance using an attached keyboard and monitor.</td>
</tr>
</tbody>
</table>
| Internet Services | Allows users access to a pre-configured group of commonly used Internet services.  

*Note: This rule is only enabled if you select Allow administrative and basic outbound Internet services during the Quick Start Wizard.*

The Internet Services rule regulates access to these proxies:

- FTP
- HTTP
- HTTPS
- Ping
- RealMedia
- RTSP
- Telnet

| Passport | Allows authentication to the Passport server and facilitates the use of single sign-on authentication. |
| Deny All | Denies all connections from any source burb to any destination burb. |
Creating an alternate policy

Many organizations need an alternate policy that is usually not in use but can be implemented quickly, such as a policy that limits inbound access if an attack is discovered. A good way to implement an alternative policy is:

1. Create a rule group for the alternate policy.
2. In that group, place all the rules needed to implement that policy. Groups can nest within groups. Be sure to create a Deny All rule as the bottom-most rule of the alternate policy.
3. Once the policy is finished, disable the policy by selecting the main rule group and clicking Disable.
4. When you need to use the policy, move the group to the top of the rule tree and enable it. The appliance begins enforcing your alternate policy.

Preparing policies for different disaster recovery scenarios can save valuable time in a crisis.

Using the main Rules window

This section provides information on using the main Rules window. You can perform several tasks from here, such as repositioning rules and rule groups, deleting rules and rule groups, and creating or editing rules. You can also rearrange the columns layout, view a flat, non-nested list of all enabled rules and export that list, and use the Find feature to help you locate rules quickly.

Use the toolbar or right-click the menu to perform the tasks in Table 8.
Chapter 5: Rules
Viewing and ordering rules and rule groups

Figure 32: Tasks available in the Rules window

<table>
<thead>
<tr>
<th>Icon/Menu item</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Rule</td>
<td>Create a new rule by clicking <strong>New Rule</strong>. The New Rule window appears. See “Creating, modifying, and duplicating rules” on page 95 for more information.</td>
</tr>
</tbody>
</table>
| New Rule Group | Create a new rule group by clicking **New Group**. A window appears asking for a name and description for this group. You can add rules to a group two ways:  
  * Select the rules to group together and then create a new group.  
  * Create a new group and then move rules into it. |
| Modify         | Modify a rule or rule group by double-clicking it or by selecting the rule and then clicking **Modify**. (Read-only administrators can click **View** to view a rule.)  
  * For rules, this opens the Modify Rule window. See “Creating, modifying, and duplicating rules” on page 95 for more information.  
  * For rule groups, this opens the Modify Group popup, where you modify the group’s description. |

Table 8: Rules window tasks
<table>
<thead>
<tr>
<th>Icon/Menu item</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete</td>
<td>Delete a rule or rule group by selecting the item(s) to delete and clicking <strong>Delete</strong>. Deleting a rule group also deletes the rules in the group. If you do not want to delete a rule group member, move the rule out of the group before clicking <strong>Delete</strong>.</td>
</tr>
<tr>
<td>Cut/Paste</td>
<td>Cut and paste rules and groups to move items from one area of the rule tree to another. You can also move items by dragging and dropping them.</td>
</tr>
<tr>
<td>Duplicate</td>
<td>Duplicate a rule by selecting a rule and clicking <strong>Duplicate</strong>. The Duplicate Rule window appears, with “Copy of rule name” in the Name field. See “Creating, modifying, and duplicating rules” on page 95 for more information. This task is useful for creating a rule that shares many properties with another rule. For example, you may need one FTP rule allowing access to one user group and one denying access to a different user group. Duplicating the first rule, then changing the action and user group, would be a quick way to accomplish this task.</td>
</tr>
<tr>
<td>Rename</td>
<td>Rename a rule or group by clicking <strong>Rename</strong>.</td>
</tr>
<tr>
<td>View Audit</td>
<td>View all available audit data for a rule. You can also view audit data by right-clicking a rule and selecting the time frame: real time, last minute, last 15 minutes, last hour, or all available.</td>
</tr>
<tr>
<td>Enable/Disable</td>
<td>Enable or disable rules and rule groups by selecting one or more items and then clicking the appropriate icon.</td>
</tr>
<tr>
<td>Move Up/Move Down</td>
<td>Move rules and groups up or down one position by selecting the item and then clicking the appropriate arrow. To move a rule into a group, expand the group and then move the rule to the appropriate position. You can also move items by dragging and dropping them.</td>
</tr>
<tr>
<td>Find/Clear</td>
<td>Find items by entering a search term in the <strong>Find</strong> field and then clicking the magnifying glass 🕵️. The search is not case sensitive. Click the magnifying glass again to select the next instance of the search term. All columns are included in the search. Return to the full rule list by clicking <strong>Clear</strong>.</td>
</tr>
</tbody>
</table>

*More...*
When you add a new rule or rule group, the placement is determined by the part of the rule tree that is selected when you click **New**. Possibilities are:

- If you select the policy node or do not have any items selected, the new rule or rule group is added to the bottom of the tree.
- If you select a group, the new rule or rule group is added to the bottom of that group.
- If you select a rule, the new rule or rule group is added directly below that rule.
- If you select multiple items, the position of the new rule or rule group depends on the last item selected.

<table>
<thead>
<tr>
<th>Icon/Menu item</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expand All/Collapse</td>
<td>Expand all rule groups so that all rules are visible or collapse the rules so that only the policy node is visible.</td>
</tr>
<tr>
<td>Active Rules</td>
<td>View all enabled rules in a flat list format. Use this window to sort and filter rules. See “Viewing and exporting your active policy” on page 94 for more information.</td>
</tr>
<tr>
<td>Columns</td>
<td>Change the column view by clicking <strong>Columns</strong>. A window appears that allows you to choose which columns to display and in what order to display them. The Name column cannot be hidden or moved.</td>
</tr>
</tbody>
</table>
Customizing the main Rules window view

The Column Selection window allows you to change what columns are displayed and in what order they appear. To access this window, select Policy > Rules, and then click Columns. The following window appears:

Use this window to change how columns are arranged and which columns are displayed. The Name column will always be first, on the far left.

- **Hide a column** — Select one or more columns in the Show these column in this order list and then use the arrow to move your selections to the Available Columns list. To move multiple consecutive entries, press the Shift key as you select the entries. To move multiple non-consecutive entries, press the Ctrl key as you select the entries.

- **Display a column** — To display a hidden column, select one or more columns in the Available Columns list and then use the arrow to move your selections to the Show these columns in this order list. To move multiple consecutive entries, press the Shift key as you select the entries. To move multiple non-consecutive entries, press the Ctrl key as you select the entries.

- **Re-order the columns** — Select a single column and then use the Up and Down buttons to move it to a new location. You cannot move more than one column at a time.

- **Return to the default view** — Click Default to automatically display all columns in their original order.

When you finish changing the column view, click OK to return to the main Rules window.
**Viewing and exporting your active policy**

The Active Rules window lists your policy’s enabled rules. This list can be exported in a comma separated value (CSV) format. To access this window, select **Policy > Rules** and click **Active Rules**. The following window appears:

![Active Rules Window](image.png)

Use the Active Rules window to view only the enabled rules. Position inconsistencies (for example, listing position 4 and then position 6) represent disabled rules, or enabled rules in a disabled group.

- **Sort the rules** — Click that column’s header to sort the active rules based on the contents of a single column.
- **Filter** — Right-click a column’s header to filter the active rules based on the contents of a single column.
- **Refresh** — Click the **Refresh** button in the upper-right corner to refresh the view to include rules created since this window opened.
- **View a rule in a full-window display** — Select a rule and click **View**.
- **Export the list** — Click **Export (csv)** to save this list as a .csv file. To change which columns are displayed in this file, adjust the displayed columns on the main Rules window.

When you have finished viewing the active rules, click **Close** to return to the main Rules window.
Creating, modifying, and duplicating rules

This section provides information on creating, modifying, and duplicating rules. It describes how to fill out this window, how fields can interact with each other, and valid values for fields.

To begin working with rules, select **Policy > Rules**. Several different actions provide access to a rule’s parameters:

- Click **New** to start a new rule.
- Double-click a rule, or select it and then click **Modify**, to change an existing rule. (Read-only administrators can click **View** to view a rule.)
- Click **Duplicate** to create a duplicate of an existing rule. This is useful for creating a rule that shares many properties with another rule.

The following window appears:

![Figure 35: The new/modify/duplicate rule window](image)

Use this window to enter all the information the appliance uses to identify and manage traffic. Each field’s drop-down list contains all existing options for that field. If you know which options you want to use, type the appropriate entry or select it from the drop-down list. Burbs, burb groups, and authentication user groups support selecting multiple options. If you want to view or search all available options or create a new entry, click .

When updates are made to a rule, the window displays the user who last modified the rule along with the date and time (bottom left corner).
Fill in, modify, or view the following:

1 In the **Name** field, enter a name that helps identify the purpose of this rule. For example, the pre-configured rule that allows typical Internet services is called “Internet Services.”

   Valid values include alphanumeric characters, periods (.), dashes (-), underscores (_), and spaces ( ). However, the first and last character of the name must be alphanumeric. The name cannot exceed 256 characters. You can rename the rule later.

2 [Optional] In the **Description** field, enter any useful information for this rule (for example, a description of what makes this rule different from a similar rule).

3 Check the **Enable** option to enable this rule. All new rules are enabled by default. You can also change this setting on the main Rules window.

4 In the **Action** field, select what will happen to traffic when it matches this rule:
   - **Allow** — (Default) Permits the traffic to pass. Since all traffic is denied by default, most rules you create will be allow rules.
   - **Deny** — Denies the traffic and generates an audit message. It also notifies the initiator that the traffic was denied.
   - **Drop** — Denies the traffic, but does not send a response to the initiator.

   **Important:** Do not use a rule where the action is **Drop** and the service, source, and destination are set to *<Any>*. Such a rule would block traffic for servers on the Sidewinder appliance (such as DNS, NTP, or Admin Console).

   *If you use Drop with a qualifier of *<Any>* for service, source, or destination, then be specific (do not use *<Any>*) for at least one of the remaining service, source, or destination fields.*

5 In the **Service** field, select the service or service group this rule will allow or deny.

   What you select here determines what values are considered valid for the rest of this window. For example, if you select a service that can use application defenses, the Application Defense field is populated with that service’s application defense options.

   **Note:** If you change your service selection, check your other selections as well, as the new service may use different options.
Chapter 5: Rules

Creating, modifying, and duplicating rules

6 In the **Audit** field, set the audit level. Options are:
   - **Standard (Recommended)** — (Default) This is the most common setting. It outputs major errors and informational messages.
   - **Verbose (Most)** — Use this level when troubleshooting. This audit output is useful for detecting configuration issues.
   - **Errors (Least)** — Use this level only if an issue with your system requires you to increase performance and reduce the size of your audit logs. Only errors are audited at this level.

   See Chapter 12, "Auditing" on page 359 for more information on audit.

7 In the **Effective Times** area, specify when this rule will be enforced by doing the following:
   a. Select the time period during which this rule will be active. By default, all rules are always active.
   b. If you want to start enforcing this rule at a specific date and time, select **Start on** and then set the date and time.
   c. If you want to stop enforcing this rule at a specific date and time, select **Expire on** and then set the date and time.

8 In the **Source** area, specify where this rule’s traffic can initiate:
   - **Burb** — Select the burb or burbs where the source endpoint is located. You can select one or more burbs, or one or more burb groups. You can select multiple burbs and/or burb groups by typing the names in a comma-separated list (for example, “internal, DMZ”) or by clicking and selecting multiple options.
   - **Endpoint** — Select the network object (for example, IP address, domain, netmap, etc.) that is allowed to initiate traffic.
   - **NAT** — Select the network object that will replace the original source address as the traffic leaves the appliance. By default, NAT is on and uses the IP address of Sidewinder’s interface that matches the destination burb (**localhost**). If using NAT, note the following:
     - If this rule’s Destination **Burb** field includes a virtual burb, do not set this field to **localhost**.
     - If you selected a netmap in the Source **Endpoint** field, the appropriate NAT properties are automatically supplied based on the mapping configured for each IP address or subnet in that netmap. For more information on netmaps, see “About the Network Object: Netmap window” on page 280.
     - If the service uses:
       - a TCP/UDP packet filter service with stateful inspection enabled, and
       - the allowed source ports include port 1024 and above, and
       - you need to preserve the source port,
you must specify an alias IP address or a subnet that contains at least one alias IP address.

View the service's **Service Properties** area to verify the service's source ports.

- **[Conditional] Preserve source port** — Check this field to translate the rule as follows: the source address is translated to the associated NAT address, but the source port will not be translated.

When using this option, the translated address is obtained one of two ways:

- If the port range included ports above 1023, this address must be an alias; it cannot be a native IP address. If the port range is below 1024, the address can be a native or *localhost*.
- From a pool of IP addresses. This requires that there be one or more alias addresses defined for the destination burb’s interface and that the NAT field be set to include those addresses. The NAT field can be set to a single IP address or a subnet that includes the alias addresses. The total number of connections is therefore dependent on the number of alias addresses defined for that interface.

**Caution:** To use this feature with ports above 1023, you must have at least one alias configured for the destination burb’s interface or traffic will not pass.

This field appears only when the selected service’s agent is a filter and is most commonly used in rules handling IKE traffic when the related Security Association does not use NAT-T.
9 In the Destination area, select where this rule’s traffic can go by configuring the following:

*Note: When using redirection, match the destination burb to the destination endpoint, even if the redirect endpoint is in another burb.*

- **Burb** — Select the burb or burbs where the destination endpoint is located. You can select a single burb, multiple burbs, a burb group, or multiple burb groups.

  You can select multiple burbs and/or burb groups by typing the names in a comma-separated list (for example, “internal, DMZ”) or by clicking *...* and selecting multiple options.

- **Endpoint** — Select the network object (for example, IP address, subnet, netmap, etc.) to which this traffic is sent.

- **Redirect** — If the traffic needs be redirected to a different endpoint, the original destination redirects to the network object you select here.

  If you selected a netmap in the Destination **Endpoint** field, the appropriate redirection properties are automatically supplied based on the mapping configured for each IP address or subnet in that netmap. For more information on netmaps, see “About the Network Object: Netmap window” on page 280.

- **[Conditional] Redirect Port** — This is the port to which the connection redirects. Note the following:
  - The default is blank. This means the port remain unchanged. Entering a 0 in this field also leaves the port unchanged.
  - Valid values are 1 – 65535 (inclusive).
  - This field is not available for all services.
10 In the Inspection area’s **Application Defense** field, do the following:

**a** Select the application defense or group this rule will use to inspect this rule’s advanced application-level content. The default is the Application Defense group currently set to the default.

Advanced content includes headers, commands, and filters. This is also where premium features, such as virus scanning, spam filtering, and web filtering, are added to rules.

Some proxy services and some servers do not have configurable application defenses; this field will be grayed out when those services are selected. All filter services require the use of an application defense.

**Note:** Rules that use HTTPS Application Defenses with the **Decrypt Web Traffic** option enabled must have redirection configured.

**b** Move the slider to change the degree to which traffic is inspected:

- **Full** — (Default) All configured application defense settings are enforced.
- **Partial** — This prevents filtering and scanning, such as header filtering and virus scanning. Some protocol inspection is used as necessary to allow traffic to pass.
- **None** — This essentially disables defense inspection and greatly limits how deeply the traffic is inspected. Only disable defense inspection for troubleshooting purposes, or in very detailed rules created to allow non-standards compliant traffic into your site.

**Note:** If the slider associated with the rule’s Application Defense is set to None, services will act like a packet filter and some services may stop passing traffic typical of their protocol.

- Non-transparent functionality will be lost, which affects HTTP, FTP, and Telnet proxies.
- In-band data inspection to authorize secondary connections will be lost, which affects FTP, T.120, H.323, NetMeeting, and SOCKS proxies.
- The SIP proxy authorizes SIP calls, not point-to-point transport layer sessions, so the SIP proxy will drop all traffic when its inspection level is set to None.
- FTP traffic will be allowed when the HTTP Application Defense is set to None, even if the GET and PUT options are deselected in the FTP URL control tab of the HTTP Application Defense.

**c** In the **IPS Signature Group** field, select the IPS signature group to search when inspecting this rule’s traffic.

**d** In the **IPS Response Mapping** field, select the response mapping this rule will use when it finds a suspected IPS attack.
11 [Optional] In the Authentication area, select the authenticator that will be used to authenticate this rule. Also determine how this rule will handle users who authenticate successfully:

- (Default) **Allow all successfully authenticated users** — Select this option if you want to allow all users who successfully authenticate.
- **Allow only users in these groups** — Select this option if you want to require users who belong to a particular group to be allowed to authenticate. You can select multiple user groups by typing the names in a comma-separated list (for example, “sales, engineering, contractors”) or by clicking ... and selecting multiple options.

If the rule is an *allow* rule, those users will be allowed to use the service.

If the rule is a *deny* or *drop* rule, the users will authenticate and then be denied access to the service. You can use authentication in a deny rule to deny a service to one group while allowing others access. For example, you can use a deny rule to deny corporate insiders access to stock trading web sites during blackout windows to prove due diligence.

You can select multiple user groups by typing the user group names in a comma-separated list (for example, “contractors, interns”) or by clicking ... and selecting multiple options.

Almost all proxies can be authenticated using the Passport authenticator.

Services that support authentication even if not using Passport include:

- Proxies: FTP, HTTP, HTTPS, SOCKS, and Telnet
- Servers: login, Admin Console, Telnetd, sshd, and ssod

You are not allowed to create a rule using a service group if one of the services does not support that authenticator.

Not all filter services and related service groups support authentication.

12 Click **OK**.

13 Save your changes.

This rule is now a part of your security policy. For additional information on how to configure each option, see “Viewing and modifying rule elements” on page 103.
Creating and modifying rule groups

This section provides information on creating and modifying rules groups. You can create an empty rule group, or you can select existing rules and add them directly to a new group. You can also nest groups within another group. To begin working with rule groups, select Policy > Rules.

To create an empty rule group

1. Determine where in the rule list your new rule group will go and then select the rule or rule group that will be directly above it. If nothing is selected, the rule group will be added to the bottom of the list.

2. Click New Group.

3. Enter a name and a description for the new group.

4. Click OK.

You can now add rules and other rule groups to this new rule group. Be sure to save your changes.

To place existing rules into a new rule group

1. Select the rules and rule groups to add to the new group.

2. Click New Group.

3. Enter a name and a description for the new group.

4. Check Move selected items into new group.

5. Click OK.

6. Verify that the rules are in the desired order.

You can now add rules and other rule groups to this new rule group. Be sure to save your changes.

To modify an existing rule group

1. Expand the rule group.

2. Select the rules to move into or out of the group. Hold down the Shift key to select multiple adjacent rules or the Ctrl key to select multiple non-adjacent rules.

3. Move the rules using any of these methods: dragging and dropping the rules, using cut and paste, or using the Up and Down arrows.

4. Verify that the rules are in the desired order.

5. If needed, modify the description.

You can now add rules and other rule groups to this new rule group. Be sure to save your changes.
Viewing and modifying rule elements

This section provides additional information on each part of a rule. It also describes the windows that appear when you click next to a field.

- “Services” on page 103
- “Time periods” on page 104
- “Source burbs, endpoints, and NAT” on page 105
- “Destination burbs, endpoints, and redirection” on page 107
- “Application Defenses” on page 109
- “IPS response mapping and signature groups” on page 110
- “Authentication” on page 111

Services

Clicking next to the Service field brings you to the Rule: Service window, where you can view the full list of existing services and service groups. You can also create new services and service groups or view a service’s properties while using this window. Services are methods for getting traffic through the appliance (proxies and filters) or into the appliance (servers).

![Figure 36: The Rules: Service window](image)

This window displays a list of all configured services. They are grouped by service (proxies, filters, servers) and then alphabetized.
Use this window to do the following:

- Find a service or service group by entering a character string related to the object you are searching for in the **Find** field. The search function searches all columns, and filters as you type. The search is not case sensitive. For example, if you are searching a service based on the HTTP proxy, typing “http” reduces the list to only the services containing that character string. Clear the **Find** field to show all options again.

- Add another service or service group by clicking **New** in the appropriate area. Once the new item is created, it is added to the list and can be used in this rule.

- View more information about a service by clicking **View**. Displayed information includes:
  - Name and description
  - Agent
  - Global properties (click **Properties**)
  - Service properties

After you have determined which service or service group to use in this rule, select that item and then click **OK**. This service appears on the dependent rule, and the application defense options change accordingly.

To learn more about services and how to modify them, see Chapter 6, "Services" on page 113.

### Time periods

Clicking **** next to the Time Period field brings you to the Time Periods window, where you can view the full list of existing time periods. You can also create new time periods or view a time period’s properties while using this window. Time periods determine the specific times when a rule will be active.

![Figure 37: The Rules: Time Period window](image)

On a new rule, this window defaults to *always active*. 
Use this window to do the following:

- Add another time period by clicking **New**. Once the new time period is created, it is added to the list and can be used in this rule.
- View a time period’s setting by clicking **View**. Displayed information includes:
  - Name and description
  - Days and times, if any

After you have determined which time period to use in this rule, select **Active during scheduled period**. Then select the time period to use and click **OK**.

To learn more about time periods and how to modify them, see “Creating time periods” on page 288.

### Source burbs, endpoints, and NAT

Clicking ![ ] in the Source area brings you to the Source Options window, where you can view the full list of existing burbs and burb groups, as well as network objects that can be used as endpoints and NAT values. You can also create new burbs, burb groups, and network objects, or view an item’s properties, while using this window. A rule’s source is what can initiate a connection through, or into, the appliance.
On a new rule, the Source area defaults are an endpoint of <Any>, the NAT address of localhost (Host), and Preserve source port disabled.

Use the Source Options window to select the values for this rule's source. You can perform the following tasks:

- Add another burb, burb group, or rule element by clicking New in the appropriate area. Once the new item is created, it is added to the list and can be used in this rule.

- Find a network object by entering a character string related to the object you are searching for in the Find field. The search function searches both the name and properties, and filters as you type. The search is not case sensitive. For example, if you are searching a network object in the 192.168 subnet, typing "192.168" reduces the list to only network objects containing that character string.

Clear the Find field to show all options again.

- View more information about an item by clicking View. Displayed information includes:
  - A burb's name, description, ID, group membership, and connection options
  - A burb group's members
  - A network object's full description

- Select the item or items to use in this rule. Use Select all/Deselect all to select or clear the check boxes next to all options above the button.

- [Conditional] Set Preserve source port. Check this field to translate the rule as follows: the source address is translated to the associated NAT address, but the source port will not be translated.

When using this option, the translated address is obtained one of two ways:

- From the address in the NAT field. This address must be an alias; it cannot be a native IP address.
- From a pool of IP addresses. This requires that there be one or more alias addresses defined for the destination burb's interface and that the NAT field be set to localhost. The total number of connections is therefore dependent on the number of alias addresses defined for that interface.

**Caution:** To use this feature, you must have at least one alias configured for the destination burb's interface or traffic will not pass.

This field appears only when the selected service's agent is a filter. The field is most commonly used in rules handling IKE traffic when the related VPN Definition does not use NAT-T.
After you have determined which the values to use for this rule’s source, indicate that you are going to make a customized selection by selecting **Selected Burbs**, **Selected Burb Groups**, or **Selected Endpoint**. Then select the appropriate item or items and click **OK**. These values will appear on the dependent rule.

To learn more about the elements that make up a source and how to modify them, see the following sections:

- “Creating network objects” on page 272
- “Configuring burbs” on page 452

**Destination burbs, endpoints, and redirection**

Clicking the destination area brings you to the Destination Options window, where you can view the full list of existing burbs and burb groups, as well as network objects that can be used as endpoints and redirect values. You can also create new burbs, burb groups, and network objects, or view an item’s properties, while using this window. A rule’s destination is what can receive or respond to traffic initiated by the rule’s source.

*Figure 39: The Rules: Destinations Options window*
On a new rule, the Destination area defaults are an endpoint of <Any>, a Redirect address of <None>, and Redirect port set to blank or 0 (do not translate).

Use the Destination Options window to select the values for this rule’s destination. You can perform the following tasks:

- Add another burb, burb group, or rule element by clicking New in the appropriate area. Once the new item is created, it is added to the list and can be used in this rule.

- Find a network object by entering a character string related to the object you are searching for in the Find field. The search function searches both the name and properties, and filters as you type. The search is not case sensitive. For example, if you are searching a network object in the 192.168 subnet, typing “192.168” reduces the list to only network objects containing that character string.

  Clear the Find field to show all options again.

- View more information about an item by clicking View. Displayed information includes:
  - A burb’s name, description, ID, group membership, and connection options
  - A burb group’s members
  - A network object’s full description

- Select the item or items to use in this rule. Use Select all/Deselect all to select or clear the check boxes next to all options in the list above the button.

- [Conditional] Set the Redirect Port. This is the port to which the connection redirects. Note the following:
  - The default is blank. This means the port remains unchanged. Entering a 0 in this field also leaves the port unchanged.
  - Valid values are 1 – 65535 (inclusive).
  - This field is not available for all services.

After you have determined which values to use for this rule’s destination, indicate that you are going to make a customized selection by selecting Selected Burbs, Selected Burb Groups, or Selected Endpoint. Then select the appropriate item or items and click OK. These values will appear on the dependent rule.

To learn more about the elements that make up a destination and how to modify them, see the following sections:

- “Creating network objects” on page 272
- “Configuring burbs” on page 452
Application Defenses

Clicking next to the Application Defense field brings you to the Rule: Application Defense window, where you can view the full list of application defenses and application defense groups that are appropriate for the selected service. You can also create new application defenses, or view an application defense’s properties, while using this window. Application defenses contain the settings for inspecting advanced application-level content, such as headers, commands, and filters. They also enable additional features such as virus scanning, spam filtering, and Web filtering.

On a new rule, this window defaults to the default group associated with the selected service or service group. None of the servers use configurable application defenses, except sendmail and some of the proxies.

Use this window to do the following:

• Add another application defense by clicking New. Once the new application defense is created, it is added to the list and can be used in this rule.

• View an application defense’s settings by clicking View.

To select a different application defense or application defense group to use in this rule, first select Custom Application Defense. Then select the application defense or group and click OK. This item appears on the dependent rule.

To learn more about application defenses and how to modify them, see Chapter 7, "Application Defenses" on page 159.
IPS response mapping and signature groups

IPS inspection consists of two rule elements: Signature Groups and Response Mappings. Clicking next to the Response Mapping field brings you to the Rule: IPS Options window, where you can view the full list of signature groups and response mappings. You can also create new groups and mappings, or view the contents of a signature group or mapping, while using this window. Signature groups each contain one or more signature categories, which identify the type of intrusion this rule is searching for. IPS mappings contain the settings for how the appliance responds when it identifies a known network-based attack.

The following window appears:

![Figure 41: The Rules: IPS Options window](image)

On a new rule, this window defaults to No Inspection. Not all services support the use of IPS inspection.

Use this window to do the following:

- Add another signature group or response mapping by clicking New. The new mapping is then added to the list and can be used in this rule.
- View an item’s settings by selecting that item and clicking View.

After you have determined which signature group and response mapping to use in this rule, select the items and click OK. These items appear on the window.

To learn more about intrusion protection services, see Chapter 8, "Content Inspection" on page 233.
Authentication

Clicking [ ] in the Authentication area brings you to the Authentication window, where you can view the list of possible authenticators for the selected service, as well as corresponding authorization properties. You can also create new authenticators or view an authenticator’s properties. Authenticators are applications that validate a person’s identity before he or she is allowed to log into a network service. Authorization determines which users will use that authentication method.

Figure 42: The Rules: Authentication window

On a new rule, this window defaults to no authentication (None).
Use this window to do the following:

- Find a user group by entering a character string related to the group you are searching for in the **Find** field. The search is not case sensitive. For example, if you are searching for an Engineering department user group, typing “Eng” reduces the list to only network objects containing that character string.

  Clear the Find field to show all options again.

- Add another authenticator by clicking **New** in the appropriate area. Once the new item is created, it is added to the list and can be used in this rule.

- View more information about an authenticator by clicking **View**. Displayed information includes:
  
  – Name, type, and description
  – Login settings
  – Password requirements
  – Affiliated users and user groups and their properties, or external groups

- Check the item or items to use in this rule. Use **Select all/Deselect all** to select or clear the check boxes next to all the user groups.

After deciding which authenticator to use in this rule, do the following:

1. Select **Selected authenticator**.

2. Select an authenticator.

3. [Conditional] If authentication will be limited based on user group or external group, select **Allow only users in the select groups** and then select one or more groups.

4. Click **OK**.

To learn more about authentication and authorization, see Chapter 10, "Authentication" on page 291.
CHAPTER 6  Services

In this chapter...

Understanding services ................................................................. 114
Understanding proxy agents and services .................................... 116
Selecting the appropriate proxy service ..................................... 120
Understanding filter agents and services .................................... 134
Understanding server agents and services ................................ 142
Using the main Services window .................................................. 145
Creating and modifying services .................................................. 147
Configuring servers ..................................................................... 154
Creating and modifying service groups ....................................... 156
Understanding services

In the Sidewinder appliance, a service associates a traffic’s transport layer with a specific agent that is responsible for managing the service’s traffic. The transport layer information includes elements such as the protocol, the ports, and the idle timeout. Rules use services, along with source and destination information, to determine what traffic that rule will allow or deny. You create a service by selecting an agent, assigning it specific transport-layer properties, and then giving it a name and saving it.

An agent is responsible for handling traffic and can be one of these types:

- Proxy (see “Understanding proxy agents and services” on page 116)
- Filter (see “Understanding filter agents and services” on page 134)
- Server (see “Understanding server agents and services” on page 142)

The proxy and filter agents can be used to create new services. Their configurable service properties vary widely. An agent’s properties can be very basic, such as the Ping Proxy agent, which only allows configuration of response timeout and fast path information. Other agents have more options, such as the Telnet Proxy agent, which includes ports, timeouts, fast path information, and connection transparency (transparent, non-transparent, or both).

The server agents (also called daemons) cannot be used to create new services. All server services are created during the initial configuration and cannot be deleted. You can modify the server services’ basic properties, such as port and timeout values. Some servers also have advanced properties that may need to be configured, such as the sendmail server’s configuration files.

Some of the agents have global properties, meaning the values apply to every service using that agent. When this value involves a connection, the connection total is a sum off all connections using that agent, even if they are distributed through multiple services and rules. Proxy agents’ global property setting controls the number of proxy instances running based on the expected connection volume. Filter agents’ global property settings controls the maximum number of TCP sessions, UDP sessions, and the port range reserved for filter sessions.

All services are disabled until they are used in an enabled rule. The first time a server, filter, or proxy service is used in an enabled rule, the service is enabled (posts a listen) in the source burb or burbs. When all rules using a given service are disabled or deleted, the service is automatically disabled.

**Note:** To view which services are currently running and if they’re running as expected, go to Monitor > Service Status. This window displays which services are enabled and where they are being used (which rules, ports, etc.). It also gives you the ability to stop or restart a service, if necessary. See Chapter 14, “Service Status,” on page 421 for more information on monitoring service status.
When planning your security policy, study the agents and the default services to determine which ones you will need and what values to assign them. Consider the following:

- Decide what type of inspection is needed for each allowed service. Proxy agents inspect traffic at the application layer. Filter agents tend to inspect traffic at the transport layer.

- When possible, use an application-aware or protocol-aware proxy agent instead of a generic proxy agent. When choosing between the Generic Proxy and the TCP/UDP Packet Filter agent, always try to use the proxy agent because it does not allow the client to connect directly to the server. Instead, the appliance maintains a separate connection to server on the client’s behalf, thereby providing more security. See “Understanding proxy agents and services” on page 116 for more information.

- Consider how traffic will get from one burb to another. Ensure the appropriate routing is in place and that you know what connection types are needed (transparent, non-transparent, or both).

- Review the server services to see which ones your policy requires, and which of those servers need modification. Some servers have advanced properties, such as the ability to add extended authentication to the ISAKMP server or to modify the single sign-on (SSO) server’s banners.

Security Alert: There is a security risk involved with using non-application aware services. The appliance has greater control over traffic managed by proxies because it can manipulate independent proxy connections on each side of the appliance.
Understanding proxy agents and services

A proxy agent is a program that controls communication between clients on one side of a Sidewinder appliance and servers on the other side. The client and server do not communicate directly. Instead, the client and server both “talk” to the proxy agent running on the appliance, which forwards the data back and forth.

The appliance increases a proxy connection’s security by receiving each packet, rebuilding it, and then sending it on its way. The traffic’s source, or initiator, sends out a request that is routed through the appliance. It inspects the packet, making sure the security policy allows the request. Next the appliance checks if any advanced checks, such as IPS or application defense inspection, are required. Once the appliance is finished handling the request, it rebuilds the packet and sends it to its destination. The appliance also keeps track of what requests were allowed and permits the appropriate responses.

The proxy agents are used to create proxy services. By default, proxy services are disabled. When you use a proxy service in an enabled rule, the appliance automatically enables that service in the corresponding source burb or burbs.

Network applications are typically accessed using one of two lower-level communication protocols: TCP or UDP. TCP is a connection-based protocol that guarantees data is delivered in the same order as sent and ensures address and data integrity. UDP is a connectionless service that delivers data with minimum overhead.

The appliance provides predefined TCP-based proxy services for a variety of Internet services including HTTP, Telnet, FTP, and many others. The appliance also supports proxy services for routing UDP transmissions for applications based on protocols such as SNMP and NTP. Many of these predefined services are based on application-aware proxy agents that can reject packets that do not comply with the protocol’s standards. This greatly increases the security and integrity of traffic passed by these proxies. When possible, use the application-aware proxy agents to pass traffic.
The following proxy agents are application-aware: DNS, FTP, H323, HTTP, HTTPS, IIOP, MS-SQL, Oracle, Ping, RealMedia, RSH, SMTP, SIP, SNMP, SOCKS, SUN RPC, T120, and Telnet.

Any proxy services that use the Generic Proxy agent are not application-aware. If you must use a service based on the Generic Proxy, increase security for these protocols by restricting the allowed ports and limiting timeout values.

See Table 9 on page 121 for a complete list of proxy services and their descriptions.

### Expected connections for proxy agents

Certain proxy agents can be configured to enable multiple instances of the same agent in order to load the traffic across the multiple instances. They are the Citrix Proxy agent, the FTP Proxy agent, the Generic Proxy agent, the HTTP Proxy agent, the HTTPS Proxy agent, the MS-SQL Proxy agent, the Oracle Proxy agent, the SMTP (Mail) Proxy agent, and the SOCKS Proxy agent.

Multiple instantiation of proxy agents is useful for hardware configurations with multiple CPUs or sites that have experienced problems due to an exceedingly large amount of concurrent connections through one of those proxies. A single proxy instance for any of these agents can generally handle up to 2000 sessions (a session consists of two connections for most protocols). By default, most proxy agents are configured for 4 proxy instances, or about 8000 sessions. This quantity is more than adequate for most sites. However, if your site is consistently recording concurrent sessions that hover around the 8000 range (or if you have experienced problems because the number of connection attempts is significantly higher) for any of these proxies, you may need to increase an agent’s number of expected connections in order to enable additional instances for that proxy agent.

To monitor the number of concurrent connections for any of the proxy agents listed above, select the Admin Console’s dashboard. The upper-right portion of the dashboard contains a link titled **Proxy Connections**. Click that link to see a list of all proxy and server services that are currently running and the current number of connections that exist for each.

To increase a proxy agent’s number of expected connections, see “Setting expected connections limits” on page 152.
Passing traffic transparently and non-transparently

The Sidewinder FTP, HTTP, HTTPS, Oracle, and Telnet proxy agents can be configured to be transparent or non-transparent. For transparent connections, the client is unaware of the appliance. The appliance is implicitly included in the path based on routing. For non-transparent, the client is aware of the appliance and explicitly connects to the appliance. The connection type is determined on the client’s side (browser settings or user inputting the appliance’s IP address). Proxy services can be configured to allow only transparent connections, only non-transparent connections, or both, depending on which option is indicated in the service’s Service Property area.

When using transparent settings, the user appears to connect directly to the desired network’s server without connecting to the appliance first. For example, to initiate an outbound Telnet session using a transparent Telnet proxy service, a user would issue the following command from his or her workstation and then connect directly to the external Telnet server:

```
telnet destination
```

With a non-transparent Telnet proxy service, a user must first Telnet to the Sidewinder appliance and specify a destination for the Telnet session. For example, the following shows how an internal user would initiate a Telnet session to a server in an external network using a non-transparent proxy that requires standard password authentication.

```
>telnet source (connection message from the Sidewinder appliance appears...)
>Enter destination: destination
>Username: username
>Password: password

(connection message from the destination Telnet server appears...)
>login: username
>Password: password
```

Non-transparent proxy configurations are typically used in networks that use NAT. For example, you would use a non-transparent service if your end users need to access a non-standard port or if there is no direct route between the client and the intended server.

**Note:** Certain transparent and non-transparent proxy configurations can require users to authenticate before they are allowed to connect. See Chapter 10, “Authentication,” on page 291 for more information.
Allowing non-transparent traffic requires configuring end-users’ browsers to point to the Sidewinder appliance. To set up browsers to work with the non-transparent proxy option, there are two basic steps:

- Specify the Sidewinder appliance’s fully-qualified host name or IP address in the browser’s proxy line.
- Specify the port number configured in the proxy service’s Properties area.

Consult your browser’s documentation for defining an HTTP proxy server.

**When to disable Fast Path Sessions**

By default, the appliance enables a Fast Path Sessions option that improves system performance by lessening the load placed on the system kernel when passing proxy data through the appliance. These sessions involve allowing the kernel to do a raw data transfer instead of copying the data from the kernel to the proxy agent and back. Performance is improved when the Fast Path Sessions option is enabled for protocols that use many small packets, such as Telnet, and for sessions where the proxy can determine that there is no longer any need for data stream inspection (the data channel of an FTP session, the encrypted data from an SSL session, or most data transferred in generic proxies).

In most cases, the Fast Path Sessions option enhances system performance, and in many of these cases the improvement is significant. For this reason, this option rarely needs to be disabled. However, there are a few rare cases where the Fast Path Sessions option may negatively affect performance. Large data transfers on heavily loaded systems, primarily FTP or HTTP traffic, can overload a system. The appliance will also throttle these connections under very heavy load conditions to prevent them from adversely affecting system performance, such as when LAN speeds on both sides of a connection are extremely fast.

The Fast Path Session option is a service property and is configurable on a service-by-service basis. For information on configuring Fast Path Session options, see “Creating and modifying services” on page 147.
Selecting the appropriate proxy service

The appliance provides a variety of pre-defined proxy services to control connections to popular Internet services using the standard port numbers (see /etc/services or www.iana.org/assignment/port-numbers for a list of commonly recognized protocols). These services can be used to quickly set up typical rules. Table 9 shows an alphabetical listing of the proxy services. Determine if these services are appropriate for your site’s security policy.

If you determine that your security policy requires proxy services with other properties, the appliance gives you the flexibility to create new services. Each service can be customized and saved under an easily recognizable name. For example, if you want contractors to have shorter timeouts for their FTP sessions than your regular employees, create two services: FTP contractors and FTP standard. To create additional proxy services, refer to “Creating and modifying services” on page 147.

See the following sections for additional notes on certain services:

- The proxy services that work together to provide VoIP services such as Microsoft’s NetMeeting application require more advanced configuration to interact correctly with the Sidewinder appliance. See “T.120 and H.323 proxy considerations” on page 125 for instructions.
- If you need information on configuring the Session Initiation Protocol service, see “Understanding the Session Initiation Protocol (SIP)” on page 132.
- If you need to change how the appliance handles FTP server responses, see “Changing the FTP server response configuration” on page 133.

Available proxy services

The following table lists the default proxy services. Note the following:

- If you selected Standard Internet services during the initial installation, the proxies listed in **bold** are automatically used in the default rule set. This means they are used in enabled rules.
- Agents for the other proxy services will not listen for or manage traffic until they are used in enabled rules.
- Rows containing application-aware proxy agents are shaded.
**Table 9: Pre-defined proxy services**

<table>
<thead>
<tr>
<th>Service name</th>
<th>Agent</th>
<th>Type and port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aol</td>
<td>Generic Proxy</td>
<td>TCP 5190</td>
<td>Allows America Online (AOL) members to run their AOL client software and connect directly to America Online.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Note:</strong> AOL’s instant messenger client (AIM) does not limit itself to this port. You cannot grant nor deny AIM access by using this service in a rule.</td>
</tr>
<tr>
<td>dns</td>
<td>DNS Proxy</td>
<td>TCP/UDP 53</td>
<td>Allows DNS query traffic and DNS zone file transfers.</td>
</tr>
<tr>
<td>finger</td>
<td>Generic Proxy</td>
<td>TCP 79</td>
<td>Allows the UNIX finger command.</td>
</tr>
<tr>
<td>ftp</td>
<td>FTP Proxy</td>
<td>TCP 21</td>
<td>Allows transparent or non-transparent access to FTP (File Transfer Protocol) servers.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>If you require FTP services over HTTP, configure that using an HTTP proxy service and application defense. The HTTP service must be configured as <strong>Non-Transparent or Both</strong>.</td>
</tr>
<tr>
<td>fwregisterp</td>
<td>Cluster Registration Client</td>
<td>TCP 9010</td>
<td>Allows your appliance to join a High Availability (HA) cluster.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Important:</strong> This proxy is required for internal communication. Do not modify any of its properties unless instructed to do so by Secure Computing Technical Support.</td>
</tr>
<tr>
<td>gopher</td>
<td>Generic Proxy</td>
<td>TCP 70</td>
<td>Allows communication between Gopher clients and servers.</td>
</tr>
<tr>
<td>h323</td>
<td>H323 Proxy</td>
<td>TCP/UDP 1720</td>
<td>Allows audio and video features for H.323 applications, such as Microsoft’s NetMeeting application and Cisco® Call Manager. This protocol is commonly used by VoIP-applications.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>See “T.120 and H.323 proxy considerations” on page 125 for more information.</td>
</tr>
<tr>
<td>http</td>
<td>HTTP Proxy</td>
<td>TCP 80</td>
<td>Allows transparent and non-transparent connections to Web servers via HTTP.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>To allow FTP over HTTP, the HTTP service must be configured as <strong>Non-Transparent or Both</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>To deny FTP over HTTP when the service is non-transparent, clear the <strong>GET</strong> and <strong>PUT</strong> checkboxes on the FTP URL Control tab of the HTTP application defense.</td>
</tr>
</tbody>
</table>
## Chapter 6: Services

### Selecting the appropriate proxy service

<table>
<thead>
<tr>
<th>Service name</th>
<th>Agent</th>
<th>Type and port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>https</td>
<td>HTTPS Proxy</td>
<td>TCP 443</td>
<td>Allows transparent and non-transparent connections to Web servers via SSL-encrypted HTTP. This proxy can be configured to handle decryption.</td>
</tr>
</tbody>
</table>
| ica           | Citrix Proxy| TCP 1494, UDP 1604 | Allows remote clients to access applications within a Citrix server farm using the Citrix ICA (Independent Computing Architecture) protocol. Locate these Citrix applications either by configuring the client directly, or by pointing them to a master browser. A master browser is a Citrix server that is configured to be responsible for tracking the ICA functions that are available for clients to access, such as applications or other Citrix servers (known as member browsers).  
  - If you are using Citrix XML Service, to locate the master browser you will need to configure the port that the Citrix server is configured to use in the HTTP proxy service.  
  - For the Citrix Proxy agent, the UDP ports are a global property. Therefore, if you change the UDP port on one service, all services using the Citrix Proxy agent will be updated with that value.  
  - For information on using the altaddr feature on your Citrix server farm, refer to your Citrix documentation. |
| ident         | Generic Proxy| TCP 113      | Allows the UNIX ident command.                                                                                                               |
| iiop          | IIOP Proxy  | TCP 683       | Allows the Internet Inter-ORB Protocol (IIOP), the wire protocol used by CORBA (Common Object Request Broker Architecture) applications to interoperate in a heterogeneous network environment. The IIOP proxy allows the Sidewinder administrator to exercise control over the dialogue between the CORBA applications.  
  **Note:** For more information on CORBA, refer to [www.omg.org](http://www.omg.org). |
| imap          | Generic Proxy| TCP 143      | Allows the Internet Message Access Protocol, which is used to access e-mail, commonly from a local server.                                   |
| irc           | Generic Proxy| TCP 6667     | Allows chat via the Internet Relay Chat (IRC) protocol.                                                                                     |
| ironmail-admin | HTTPS Proxy| TCP 10443     | Allows traffic between an Ironmail® appliance and its management client.                                                                     |
| ironmail-support | Generic Proxy| TCP 20022 | Allows traffic between Ironmail software and anti-virus updates.                                                                          |

*More...*
### Chapter 6: Services

#### Selecting the appropriate proxy service

<table>
<thead>
<tr>
<th>Service name</th>
<th>Agent</th>
<th>Type and port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lotus</td>
<td>Generic Proxy</td>
<td>TCP 1352</td>
<td>Allows the Lotus Notes applications.</td>
</tr>
<tr>
<td>msn</td>
<td>Generic Proxy</td>
<td>TCP 569</td>
<td>Allows Microsoft network members to run their MSN client software and connect directly to MSN through the appliance.</td>
</tr>
<tr>
<td>mssql</td>
<td>MS-SQL Proxy</td>
<td>TCP 1433</td>
<td>Allows Microsoft servers and clients to pass SQL traffic.</td>
</tr>
<tr>
<td>netbios-tcp</td>
<td>Generic Proxy</td>
<td>TCP 139</td>
<td>Allows the generic NetBIOS TCP proxy, which is also known as the NetBIOS Session Service (NBSS). This proxy generally provides access to files and printers. Commonly used with the netbios-udp service.</td>
</tr>
<tr>
<td>netbios-udp</td>
<td>Generic Proxy</td>
<td>UDP 137, 138</td>
<td>Allows the generic NetBIOS UDP proxy, which is also known as the NetBIOS Name Service (NBNS). The proxy generally is used for name service resolution in conjunction with the NetBIOS Session Service. Commonly used with the netbios-tcp service.</td>
</tr>
<tr>
<td>news</td>
<td>Generic Proxy</td>
<td>TCP 119</td>
<td>Allows access to Usenet News.</td>
</tr>
<tr>
<td>ntp</td>
<td>Generic Proxy</td>
<td>UDP 123</td>
<td>Allows clock synchronization via Network Time Protocol (NTP).</td>
</tr>
<tr>
<td>oracle</td>
<td>Oracle Proxy</td>
<td>TCP 1521</td>
<td>Allows SQL traffic between Oracle servers and clients.</td>
</tr>
<tr>
<td>ping</td>
<td>Ping Proxy</td>
<td>ICMP (na)</td>
<td>Relays ICMP ECHO (ping) requests and ICMP Echo-REPLY messages through the appliance.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Note:</strong> Enabling the ping proxy does not allow traceroute through the appliance. In addition to security risks, NAT prevents most sites from getting a return from the external network (Internet) because of non-routable addresses. To run traceroute, follow it to the appliance and then initiate a second traceroute from the appliance itself.</td>
</tr>
<tr>
<td>pop</td>
<td>Generic Proxy</td>
<td>TCP 110</td>
<td>Allows Post Office Protocol (POP) connections.</td>
</tr>
<tr>
<td>printer</td>
<td>Generic Proxy</td>
<td>TCP 515</td>
<td>Allows the UNIX lpr command.</td>
</tr>
</tbody>
</table>

*More...*
### Chapter 6: Services

#### Selecting the appropriate proxy service

<table>
<thead>
<tr>
<th>Service name</th>
<th>Agent</th>
<th>Type and port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>realmedia</td>
<td>RealMedia Proxy</td>
<td>TCP/UDP 7070</td>
<td>Allows RealMedia audio and video data packet connections.</td>
</tr>
<tr>
<td>rlogin</td>
<td>RSH Proxy</td>
<td>TCP 513</td>
<td>Allows connections to rlogin servers.</td>
</tr>
<tr>
<td>rsh</td>
<td>RSH Proxy</td>
<td>TCP 514</td>
<td>Allows RCP (a remote file copy protocol) and RSH (remote shell login).</td>
</tr>
<tr>
<td>rtsp</td>
<td>RTSP Proxy</td>
<td>TCP/UDP 554</td>
<td>Allows the RealMedia Player and QuickTime Multimedia Player protocols.</td>
</tr>
<tr>
<td>sip</td>
<td>SIP Proxy</td>
<td>UDP 5060</td>
<td>Allows the Session Initiation Protocol (SIP). This protocol is commonly used by VoIP-applications. See “Understanding the Session Initiation Protocol (SIP)” on page 132.</td>
</tr>
<tr>
<td>smtp</td>
<td>Mail Proxy</td>
<td>TCP 25</td>
<td>Allows Simple Mail Transfer Protocol messages through the appliance.</td>
</tr>
<tr>
<td>snmp</td>
<td>SNMP Proxy</td>
<td>UDP 161-162</td>
<td>Supports remote management using the SNMP protocol.</td>
</tr>
<tr>
<td>socks</td>
<td>SOCKS Proxy</td>
<td>TCP 1080</td>
<td>Allows the SOCKS5 protocol. The only available connection type is non-transparent. When using a SOCKS service in a rule, make sure the associated application defense’s Connection tab specifies which destination ports are allowed.</td>
</tr>
<tr>
<td>ssh</td>
<td>Generic Proxy</td>
<td>TCP 22</td>
<td>Allows the UNIX Secure Shell command, which provides secure shell access through the appliance to remote systems.</td>
</tr>
<tr>
<td>streamworks</td>
<td>Generic Proxy</td>
<td>TCP 1558</td>
<td>Allows Streamworks streaming audio and video.</td>
</tr>
<tr>
<td>sunrpc</td>
<td>SunRPC Proxy</td>
<td>TCP/UDP 111</td>
<td>Relays requests between RPC clients and remote servers.</td>
</tr>
<tr>
<td>sybase</td>
<td>Generic Proxy</td>
<td>TCP 4000</td>
<td>Allows the Sybase SQL proxy.</td>
</tr>
</tbody>
</table>
## T.120 and H.323 proxy considerations

The T.120 and H.323 proxy agents can be configured to work together, allowing you to make use of both the data-sharing and audio/video features of data conferencing products, such as Microsoft NetMeeting, in a single conference. This section provides an overview of each agent and its role in data conferencing. It also provides information on configuring the two agents to work together to enable the complete realm of NetMeeting features.

<table>
<thead>
<tr>
<th>Service name</th>
<th>Agent</th>
<th>Type and port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>syslog</td>
<td>Generic Proxy</td>
<td>UDP 514</td>
<td>Allows the UNIX syslog protocol.</td>
</tr>
<tr>
<td>t120</td>
<td>T120 Proxy</td>
<td>TCP 1503</td>
<td>Allows T.120 applications, such as Microsoft’s NetMeeting application. This protocol is commonly used by VoIP-applications. See “T.120 and H.323 proxy considerations” on page 125 for more information.</td>
</tr>
<tr>
<td>telnet</td>
<td>Telnet Proxy</td>
<td>TCP 23</td>
<td>Allows transparent or non-transparent access to Telnet servers.</td>
</tr>
<tr>
<td>wais</td>
<td>Generic Proxy</td>
<td>TCP 210</td>
<td>Allows connections between WAIS client software and a database service called WAIS.</td>
</tr>
<tr>
<td>whois</td>
<td>Generic Proxy</td>
<td>TCP 43</td>
<td>Allows the UNIX <code>whois</code> command. <code>whois</code> looks up records in the Network Information Center.</td>
</tr>
<tr>
<td>wins</td>
<td>Generic Proxy</td>
<td>UDP 42</td>
<td>Allows Microsoft Windows Network Services.</td>
</tr>
<tr>
<td>Xwindows</td>
<td></td>
<td>TCP 6000</td>
<td>Allows UNIX-based X Windows sessions to pass through the appliance. For instance, an X Windows process running on one terminal could send screen output through the appliance to another window at a different terminal. While redirecting X Windows is a common practice at larger UNIX sites with X Windows environments, X Windows is not a secure application. Using this proxy strictly for sending X Windows traffic through the appliance is not recommended for most sites. However, if the appliance has been placed between two networks, both of which are within your organization (sometimes called “inter-walling”), the Xscreen0 proxy might not pose serious security hazards. This depends on the nature of the site’s two networks.</td>
</tr>
<tr>
<td>X500</td>
<td>Generic Proxy</td>
<td>TCP 103</td>
<td>Supports the X500 directory server.</td>
</tr>
</tbody>
</table>
About the T.120 proxy agent

The T.120 proxy agent provides support for applications built using the International Telecommunication Union (ITU) T.120 recommendations. The T.120 recommendations are most prevalent in data conferencing applications. T.120 defines several standardized data conferencing services including application sharing, text chat, shared whiteboard, and multipoint file transfer.

Microsoft's NetMeeting is a popular example of a T.120 enabled application. The T.120 proxy agent enables you to use all of the standard T.120 data conferencing services, and provides you with a means to control which services are accessible. The T.120 proxy agent also provides support for the Microsoft NetMeeting chat and application sharing, which are non-standard T.120 application services.

Note: The audio, video, ILS, and ULS features of NetMeeting are not supported by the T.120 agent. These features are supported in the H.323 agent. To use this functionality, enable the default NetMeeting rule. This will ensure that services using both agents remain synchronized with one another. See “Synchronizing T.120 and H.323 for use with NetMeeting” on page 131 for more information.

When configured, the T.120 proxy agent is transparent to the participants of the data conference. The T.120 proxy agent comes into play when a conference participant attempts to join an existing conference or attempts to invite another participant that resides in a different burb. The T.120 proxy agent intercepts and mediates the session between the pair of conference host machines. These host machines are referred to as nodes in T.120 parlance.

T.120 conferences are arranged into a hierarchy of nodes. The placement of the Sidewinder appliance with respect to the nodes in the conference affects how many sessions are created through the proxy agent and the communication path of the conference data. When a first conference participant joins a conference in a different burb, a T.120 session is created between the participant’s node and the contacted node. If a second conference participant attempts to contact the new conference node, a separate session is created.

The preconfigured NetMeeting rule, when enabled, will apply to each participant’s respective node IP address. If the second participant contacts the first participant and asks to join the conference, the same proxy session will be used. The NetMeeting rule that applies to the first participant’s node will also apply to this session.

The T.120 proxy is configured to use port 1503 by default. This can be changed as described in “Creating and modifying services” on page 147.
About the H.323 proxy agent

H.323 is an International Telecommunications Union (ITU) standard that provides support for audio and video conferencing across a shared medium such as the Internet. The H.323 proxy agent provides standard functions such as filtering on source and destination hosts and burbs, and NAT and redirection. The H.323 proxy agent is a protocol-aware, application layer agent that examines H.323 packets for correctness and adherence to site security policy. In addition to the standard filtering mentioned above, the H.323 agent provides a mechanism for allowing or disallowing certain codecs (audio or video encoding schemes) within the H.323 protocol.

Microsoft NetMeeting is a popular implementation of the H.323 protocol. The H.323 proxy agent enables you to use the audio and video features of data conferencing products like NetMeeting.

Note: The standard data conferencing features, as well as the chat and application sharing features of NetMeeting, are not supported by the H.323 agent. These features are supported in the T.120 agent. To use this functionality, enable the default NetMeeting rule. This will ensure that services using both agents remain synchronized with one another. See “Synchronizing T.120 and H.323 for use with NetMeeting” on page 131 for more information.

The H.323 proxy agent can function between two endpoints (a single client implementation such as NetMeeting), or between one or more endpoints and a Multi-point Control Unit (MCU). The MCU enables two or more endpoints to simultaneously participate in a call. Each endpoint sends its audio and video signals through the Sidewinder appliance to the MCU. The MCU then combines the audio signals and selects one or more video signals to return to each endpoint.

Note: The H.323 agent does not recognize any configuration difference between an endpoint and an MCU.

The H.323 proxy agent must examine the contents of the protocol packets for encoded addresses and port numbers. Therefore, any sort of encryption of H.323 sessions is not possible in conjunction with the H.323 proxy agent. When implementing the H.323 protocol, you must disable NetMeeting’s security features, or the security features of any other endpoint or MCU you may be using. Additionally, you must not route H.323 traffic through a VPN.

Also, any calls originating from the outside network and destined for a host on the internal network may be configured to use the netmaps feature. (For information on using netmaps, see “About the Network Object: Netmap window” on page 280.) This provides a form of redirection that allows you to hide a group of addresses behind the Sidewinder appliance while still allowing the inbound caller to reach the proper destination machine.
About using a gatekeeper with the H.323 proxy

The H.323 proxy agent can also function between endpoints and a gatekeeper. A gatekeeper sits between source and destination endpoints and typically provides services such as authentication, authorization, alias resolution, billing and call routing. The RAS (Registration, Admission, and Status) protocol is used between the endpoints and the gatekeeper. RAS uses UDP port 1719.

If endpoints are configured to make use of the services of a gatekeeper, the appliance must be configured to properly handle this traffic. The preconfigured VoIP H.323 rule allows both conferencing services and RAS services to be provided by an H.323 proxy service. The conferencing services include audio/video and data, as in the NetMeeting rule previously discussed. When the endpoints are configured to use a gatekeeper, use an H.323 rule rather than the default NetMeeting rule.

A gatekeeper can operate in one of two modes: direct and routed. The gatekeeper’s mode is important when configuring the VoIP H.323 rule on the appliance. In direct mode, the gatekeeper grants permission for the call, but the call setup and call data are passed directly from endpoint to endpoint. In routed mode, the gatekeeper grants permission for the call and handles the call setup. Call data is then passed directly from endpoint to endpoint. The Sidewinder policy must allow for the proper communication paths.

To appropriately restrict access for the H.323 proxy rule, configure networks objects that describe the hosts receiving calls and sending calls. Also configure a network object for the gatekeeper. The source and destination of the H.323 rule should contain the endpoints and the gatekeeper as appropriate for the mode of operation configured on the gatekeeper. This may include adding netmaps to add all call endpoints and the gatekeeper to a single rule, and making changes to the H.323 configuration file to support your gatekeeper environment.
If the gatekeeper is on the internal network, configure a netmap to allow hosts on the outside network to communicate with the gatekeeper as well as with endpoints on the internal network. The netmap needs to include the gatekeeper, the hosts allowed to initiate calls, and the hosts allowed to receive calls. The internal gatekeeper and internal hosts permitted to send and receive calls must be mapped to external address. If the internal hosts are exchanging calls with terminals on the Internet, then the mapped addresses must be publicly routable.

If the gatekeeper is not on the same subnet as the hosts permitted to receive incoming calls, then the netmap must include a mapping of the gatekeeper to itself so the gatekeeper is a recognized destination.

**Figure 44:** Rule source and destination netmaps when gatekeeper is internal

<table>
<thead>
<tr>
<th>Original</th>
<th>Mapped</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.131.0.0/24</td>
<td>111.131.0.0/24</td>
</tr>
<tr>
<td>10.111.1.5</td>
<td>111.131.10.65</td>
</tr>
<tr>
<td>111.153.0.0/24</td>
<td>111.153.0.0/24</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Original</th>
<th>Mapped</th>
</tr>
</thead>
<tbody>
<tr>
<td>111.131.0.0/24</td>
<td>10.131.0.0/24</td>
</tr>
<tr>
<td>111.131.10.65</td>
<td>10.111.1.5</td>
</tr>
<tr>
<td>111.153.0.0/24</td>
<td>111.153.0.0/24</td>
</tr>
</tbody>
</table>
If the gatekeeper is on the external network, then a connection may be made from the gatekeeper to any internal host permitted to receive calls. Configure a netmap that includes the internal terminals and a mapping of the gatekeeper to itself, so that the gatekeeper is a recognized destination. If external terminals will be allowed to initiate or receive calls, they should also be added to the netmap.

**Figure 45:** Rule source and destination netmaps when gatekeeper is external

<table>
<thead>
<tr>
<th>Internal subnet 10.131.x.x</th>
<th>External subnet 111.131.0.0/24 interface 111.131.10.65</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Gatekeeper</strong> 111.111.1.5</td>
<td><strong>Sidewinder</strong> 111.111.1.5</td>
</tr>
</tbody>
</table>

If the gatekeeper is in a burb completely separate from the call endpoints, you need to adjust the H.323 configuration file. To edit the file so the appliance recognizes that the gatekeeper is in a burb separate from the call endpoints, do the following:

1. Using a file editor, open `/secureos/etc/proxy/h323p.conf`.
2. Locate the following lines:
   ```
   gatekeeper_alone [NO]
   ```
4. Save your changes and exit the file.
5. Restart the H.323 Proxy agent:
   a. Select Monitor > Service Status.
   b. Select h323.
   c. Click Restart.

The Sidewinder appliance adjusts its routing accordingly.
In general, gatekeepers pass the IP address of the call-initiator endpoint to the call-receiver endpoint. This allows the systems to verify both ends of the connection. However, some gatekeepers pass their own IP address instead of the call initiator’s address. When the Sidewinder appliance cannot verify the other endpoint, it ignores the connection and generates the following audit message:

```
H.245 connect received from unknown_ip_addr while expecting one from known_ip_addr. Unexpected connect ignored.
```

If your gatekeeper does not pass the call initiator’s IP address, you need to adjust the H.323 configuration file. To edit the file so the appliance allows connections where the initiating IP address cannot be verified, do the following:

Caution: Making this change decreases security. Do not edit this value unless it is required for your gatekeeper configuration.

1. Using a file editor, open `/secureos/etc/proxy/h323p.conf`.
2. Locate the following line:
   ```
   accept_anonymous_endpoint [NO]
   ```
4. Save your changes and exit the file.
5. Restart the H.323 Proxy agent:
   a. Select **Monitor > Service Status**.
   b. Select **h323**.
   c. Click **Restart**.

The Sidewinder appliance now accepts H.245 connections from unknown IP addresses.

**Synchronizing T.120 and H.323 for use with NetMeeting**

The T.120 and H.323 proxy agents can work together, allowing you to make use of both the data-sharing and audio/video features of NetMeeting in a single conference as follows:

- The T.120 proxy agent enables you to use all of the standard T.120 data conferencing services and provides you with a means to control which services are accessible. The T.120 proxy agent also provides support for the Microsoft NetMeeting chat and application sharing, which are non-standard T.120 application services.
- The H.323 proxy agent provides support for the audio and video features of NetMeeting.
To make use of both the data-sharing and audio/video features of NetMeeting in a single conference, you must ensure that both the T.120 and H.323 proxy services are enabled in the same burbs. This is necessary because for a single NetMeeting session, part of the traffic (the H.323 portion) is routed through the H.323 proxy, and part of the traffic (the T.120 portion) is routed through the T.120 proxy. If the H.323 and T.120 proxy configurations are out of synchronization, it is likely that NetMeeting conferences will not function correctly or completely (for example, audio and video work, but data-sharing does not work).

To prevent the two services from becoming out of synchronization, enable the preconfigured NetMeeting rule. The NetMeeting rule allows access to both the T.120 and H.323 proxy services (using the preconfigured NetMeeting Service Group), and allows access to all available NetMeeting features.

You can modify the default NetMeeting rule or create your own rules to allow only a portion of NetMeeting’s features, such as the chat and whiteboard features. These properties are configured via the Multimedia Application Defense. For information on configuring Application Defenses for H.323/T.120, see “Creating T.120 Application Defenses” on page 210.

To appropriately restrict access for the NetMeeting proxy rule, configure network objects or other rule elements. For example, if you want to allow only administrators access to all NetMeeting features, create and specify a network object within a rule that contains the IP addresses for all of your administrators.

**Understanding the Session Initiation Protocol (SIP)**

The Session Initiation Protocol (SIP) is defined by Internet Engineering Task Force (IETF) RFC 3261. SIP is an application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants. These sessions include Internet telephone calls, multimedia distribution, and multimedia conferences. The SIP proxy agent provides standard functions such as filtering on source and destination hosts and burbs, and NAT and redirection. The SIP proxy is a protocol-aware, application-layer agent that examines SIP packets for correctness and adherence to site security policy. The SIP agent may be configured to prevent audio and/or video connections from being established via SIP.

SIP is used to locate a user agent and negotiate a multimedia session between user agents. Once a session is negotiated, RTP is used to exchange the multimedia information between the user agents. The SIP proxy agent only examines the SIP traffic that negotiates the multimedia session. The RTP traffic itself is passed unexamined through the proxy. This traffic will make use of the Fast Path Sessions capability if the option is enabled for this service.
Changing the FTP server response configuration

By default, the appliance restricts which FTP servers responses it will accept. Accepted FTP server response codes range from 100 to 599. To alter which codes are accepted or to turn off server response checking, do the following:

**Note:** Only experienced administrators should edit configuration files.

1. From a console attached to the appliance, log in and enter `srole` to switch to the Admin domain.
2. Using a file editor, open `/secureos/etc/proxy/pftp.conf`.
3. If you want to turn off server response checking, find the following line:
   
   ```
   validate_server_response[yes]
   ```
   
   and change `[yes]` to `[no]`.
4. If you want to limit which FTP server responses the appliance accepts, edit the values in the following lines:
   
   ```
   min_server_response_code[100]
   max_server_response_code[599]
   ```
   
   Valid values are between 000 and 999.
5. Save your changes.
6. Restart the FTP agent to apply the changes by doing the following:
   
   ```
   cf daemond restart agent=ftp
   ```

The FTP proxy has now been restarted and is using the updated configuration file.
Filter agents are another method for client and servers in different burbs to communicate. They pass traffic at the network layer or the transport layer of the network stack. Filter rules filter incoming packets based on source IP address, destination IP address, and ports. Like proxy rules, filter rules have the option of using network address translation or redirection. Unlike proxy agents, filter agents are not application aware and cannot enforce traffic based on the application protocol. As shown in the following figure, filters inspect traffic at the transport (TCP/UDP) and network (IP) layers. Available agents are the TCP/UDP Packet Filter agent, the ICMP Packet Filter agent, and the Other Protocol Packet Filter agent.

TCP, UDP, and ICMP filters can actively track individual filter sessions using stateful inspection. This ensures that only packets valid for a new session or a portion of an existing session are sent on to the final destination.

Filter services are useful in the following situations:

- Traffic that is a protocol other than TCP or UDP, such as AH, ESP, and GRE.
- TCP/UDP protocols where you need a wide port range or maximum performance with minimal security.
- Proprietary traffic that has invalid TCP/UDP headers.

Filter processing can be configured to reject the following source address packets:

- Packets with broadcast source addresses.
- Packets with source addresses on a loopback network that were received on a non-loopback device.

**Note:** Packets that are rejected for source route information generate a netprobe audit event.
The following sections summarize how filtering works when stateful packet inspection (also known as session tracking) is enabled and when it is not enabled. The sections also provide information on what criteria are used to determine rule matches and what happens after the appliance checks the packet against the enabled filter rules.

### How traffic is filtered if stateful packet inspection is enabled

When the appliance receives TCP, UDP, and ICMP traffic, it starts by checking a filter session record database to determine if an active session record exists for this traffic. A session record indicates that this traffic is in response to a previous successful match to an allow rule. Session records only exist if the matching rule had stateful packet inspection enabled. Stateful packet inspection is only an option for TCP, UDP, and ICMP filter rules.

**If an active session record exists, the following occurs:**

- a Perform address and port rewriting, if required
- b Perform session processing
- c Forward packet directly to the correct destination interface without any additional processing

**If no active session record exists, the following occurs:**

The appliance uses the criteria in Table 10 to check the active filter rules and find a match. The description for how the packet proceeds through the appliance comes after the table. The flowchart in Figure 47 illustrates the complete process.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Criteria</th>
</tr>
</thead>
</table>
| TCP/UDP  | - source IP address  
           | - destination IP address  
           | - ports |
| ICMP     | - packet type (echo, message, timestamp)  
           | - source IP address  
           | - destination IP address |
• If a matching allow rule does exist, the following occurs:
  a  Add a session record to the session record database.
  b  Perform Network Address Translation (NAT) if required.
  c  Session processing occurs.
  d  Forward packet directly to the correct destination interface without any additional processing by the appliance.
• If a matching deny rule exists, an RST packet is sent to close the connection. If a drop rule exists, the packet is discarded without further processing.
• If a matching absorb proxy or server rule exists, the packet is sent directly to application-layer processing.

  **Note:** Absorb rules are counterparts to proxy and server rules that are used to expedite processing by sending the appropriate packet directly to application-level processing instead of checking it against all filters rules.

• If no matching filter rule exists, the packet is generally denied. Exceptions:
  – If the packet arrived on a burb that is configured to hide port unreacheables, the packet is dropped instead of denied.
  – If a proxy is listening on the packet’s port, the proxy handles the packet according to its protocol standards.
Figure 47: Filtering on packets with rules that have stateful packet inspection enabled

TCP/UDP/ICMP packet

Sidewinder

- in
- does a session exist?
  - yes: translate as required
  - no: match proxy or server rule?
    - yes: match allow rule?
      - yes: discard packet
      - no: add a session
    - no: match deny or drop rule?
      - yes: perform application-layer processing
      - no: forward message w/o further processing

- out

forward message w/o further processing
How traffic is filtered if stateful packet inspection is disabled

When the appliance receives traffic, it checks the active filter rules for a matching rule. If a rule does not have stateful packet inspection enabled, the appliance checks the criteria in Table 11 to find a match.

Table 11: Rule matching criteria without stateful packet inspection enabled

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP/UDP</td>
<td>• source IP address</td>
</tr>
<tr>
<td></td>
<td>• destination IP address</td>
</tr>
<tr>
<td></td>
<td>• ports</td>
</tr>
<tr>
<td>ICMP</td>
<td>• source IP address</td>
</tr>
<tr>
<td></td>
<td>• destination IP address</td>
</tr>
<tr>
<td>Other</td>
<td>• source IP address</td>
</tr>
<tr>
<td></td>
<td>• destination IP address</td>
</tr>
</tbody>
</table>

Using these criteria, the appliance determines if the packet matches any of the active allow, absorb, or deny/drop rules. The appliance then does one of the following:

- If a rule match is found, the packet source or destination address are translated according to the translation information that is configured for that rule. The packet is then forwarded on for any further Sidewinder processing. The flowchart in Figure 48 illustrates this process.
- If there are no matching rules in the filter database, the appliance sends the packet onto application-layer processing.

Figure 48: Filtering packets when stateful inspection is disabled
Using NAT and redirection for filter rules

In general, NAT and redirection are configured the same in filter rules as they are in proxy rules. However, there are some exceptions, particularly in how ports are handled. See the following sections for details.

Limitations of NAT and redirection for filter services

Note the following limitations when setting up rules involving address rewriting for TCP/UDP/ICMP protocols.

- NAT and redirection are not allowed for bi-directional filter rules with stateful packet inspection enabled.
- If stateful inspection is disabled and you want to rewrite an address, the rewritten address must have significant bits value of 32. For example, on an inbound rule the redirect address must be an IP address or hostname network object.

Reserving the port range to use when rewriting source ports

When an outbound packet reaches the appliance and matches a filter rule with NAT configured, the source port and source address will be rewritten and the packet will then be forwarded to its destination.

To facilitate this process, the appliance reserves a range of ports that are to be used exclusively for rewriting source ports. The OS does not allow any processes to bind to a port in this range; configuring proxy services to use ports in this port range will not work.

The default range is set to 9120–9995. If you need to use a port in this range for a different purpose, such as for a new Generic Proxy service, you can adjust the range by doing the following:

1. From a command line, run `netstat -an` to view the current port usage. Verify that none of the ports in your selected range are in use.
2. Adjust the reserved port range accordingly by editing the Reserved port range field in the Global Properties for TCP/UDP Packet Filters window. See “Setting session maximums, port ranges, and intra-burb forwarding for the TCP/UDP Packet Filter agent” on page 153.

Note: In general, this default range should be sufficient unless you need numerous connections to the same destination and port.
Rewriting the address but reserving a packet’s specified source port

The appliance enables you to rewrite the source address but maintain the packet’s source port. This capability is typically only used when connecting to an application that requires the source port to be a specific value. In some cases, the application requires the source port to be the same value as the port on which the application is listening. This capability is implemented by configuring NAT with Preserve source port selected.

The following bullets explain the difference between translating and preserving the source port:

- **Source port is translated** — Each connection uses the same IP address but gets its source port from the reserved port range. The total number of connections can be limited by the number of ports reserved in the Global Properties for TCP/UDP Packet Filters window.

- **Source port is preserved** — Each connection uses the original client source port, but gets its translated IP address one of two ways:
  - If the port range included ports above 1023, this address must be an alias; it cannot be a native IP address. If the port range is below 1024, the address can be a native or localhost.
  - From a pool of IP addresses. This requires that there be one or more alias addresses defined for the destination burb’s interface and that the NAT field be set to include those addresses. The NAT field can be set to a single IP address or a subnet that includes the alias addresses. The total number of connections is therefore dependent on the number of alias addresses defined for that interface.

  **Caution:** To use this feature with ports above 1023, you must have at least one alias configured for the destination burb’s interface or traffic will not pass.

This configuration only applies to uni-directional (source > destination) filter rules with stateful inspection enabled.

By specifying one or more IP aliases, you can have multiple connections because each connection uses the same port number but a different IP address. Figure 49 and Figure 50 illustrate the differences in the two implementations.
**Figure 49:** NAT with a translated source port

Possible connections from workstation A to application B when translating the source port

<table>
<thead>
<tr>
<th>Internal IP</th>
<th>Source IP</th>
<th>Source Port</th>
<th>Dest IP</th>
<th>Dest Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.27.18.9</td>
<td>11.80.1.1</td>
<td>9142</td>
<td>192.1.1.1</td>
<td>50</td>
</tr>
<tr>
<td>172.27.18.9</td>
<td>11.80.1.1</td>
<td>9877</td>
<td>192.1.1.1</td>
<td>50</td>
</tr>
<tr>
<td>172.27.18.9</td>
<td>11.80.1.1</td>
<td>9812</td>
<td>192.1.1.1</td>
<td>50</td>
</tr>
<tr>
<td>172.27.18.9</td>
<td>11.80.1.1</td>
<td>9884</td>
<td>192.1.1.1</td>
<td>50</td>
</tr>
</tbody>
</table>

**Figure 50:** NAT with a preserved source port

Possible connections from workstation A to application B when preserving the source port

<table>
<thead>
<tr>
<th>Internal IP</th>
<th>Source IP</th>
<th>Source Port</th>
<th>Dest IP</th>
<th>Dest Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.27.18.9:50</td>
<td>11.80.1.4</td>
<td>50</td>
<td>192.1.1.1</td>
<td>50</td>
</tr>
<tr>
<td>172.27.18.9:50</td>
<td>11.80.1.5</td>
<td>50</td>
<td>192.1.1.1</td>
<td>50</td>
</tr>
<tr>
<td>172.27.18.9:50</td>
<td>11.80.1.6</td>
<td>50</td>
<td>192.1.1.1</td>
<td>50</td>
</tr>
<tr>
<td>172.27.18.9:50</td>
<td>11.80.1.7</td>
<td>50</td>
<td>192.1.1.1</td>
<td>50</td>
</tr>
</tbody>
</table>
Stateful session failover in an HA cluster

When filter session sharing is configured for an HA cluster, the processing appliance sends out multicast messages over the heartbeat interface to notify the other nodes (such as the secondary or standby) of packet filter session activity (such as a new session, closed session, or change in session state). Each time a node receives a message, it updates its local session table accordingly. All sessions received from the primary will have a status of shared on the secondary/standby.

When HA causes a secondary/standby to take over as the acting primary, the shared sessions on the acting primary become available. When a packet is received for a session, it will be validated against the rules of the processing node. The processing node will then begin sending multicast state-change messages.

Understanding server agents and services

Sidewinder servers provide a variety of system functions, but generally do not pass traffic between burbs. Rules that allow access to a Sidewinder server typically have the same source and destination burbs, as shown in the following figure.

Common services include the Admin Console server (used for GUI management), the SSH server (used for command line management), and sendmail. Unlike proxies and filters, you cannot create new server services.

*Note:* By default, server services are disabled. When you use a server service in an enabled rule, the appliance automatically enables that service in the corresponding source burb or burbs.
Servers can be classified as belonging to one of the following categories:

- **Management** — Used for management and administration of the Sidewinder appliance.
- **Service** — Provides access to a networked service.
- **Routing** — Provides routing services on the appliance.
- **VPN** — Used in VPN connections.
- **Sidewinder-specific** — An inter- or intra-appliance server used in Sidewinder clustering or centralized management.

See the following table for a list of the functions provided by each server.

**Table 12: Available servers**

<table>
<thead>
<tr>
<th>Service</th>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin Console (Admin Console)</td>
<td>Management</td>
<td>Used when administrators log into the appliance using the Sidewinder Admin Console.</td>
</tr>
<tr>
<td>bgpd (BGP Server)</td>
<td>Routing</td>
<td>Used in routing with the Border Gateway Protocol (BGP). See “BGP on Sidewinder” on page 648.</td>
</tr>
</tbody>
</table>
| ccmd ccms (CommandCenter Management Server) | Sidewinder-specific | Used in registration and communication among the CommandCenter and managed Sidewinder appliances.  
- ccmd is used to send data from the CommandCenter appliance to the Sidewinder appliance.  
- ccms is used to send data from the Sidewinder appliance to the CommandCenter appliance. |
| changepw (Change Password Server) | Service    | Allows external users to use a browser to change their Sidewinder, SafeWord PremierAccess, or LDAP login password. See “Setting up users to change their own passwords” on page 325. |
| entrelayd (Enterprise Relay Server) | Sidewinder-specific | Used for services that need to communicate with each other in Sidewinder multi-appliance configurations.                                                                                              |
| fwregisterd (Cluster Registration Server) | Sidewinder-specific | Used for registration and communication among Sidewinder appliances in High Availability (HA) pairs and in One-to-Many (OTM) clusters.                                                                |
| gated (Gateway Routing Server) | Routing    | This server has been deprecated. Secure Computing recommends using the ospfd server instead. See “Configuring OSPF (ospfd)” on page 643.                                                                |
| isakmp (ISAKMP Server)        | VPN        | Used to generate and exchange keys for VPN sessions. See “Configuring the ISAKMP service” on page 574.                                                                                                   |
| login (Login Console)         | Management | Used when administrators log in at a console attached to the Sidewinder appliance.                                                                                                                           |
### Chapter 6: Services

#### Understanding server agents and services

<table>
<thead>
<tr>
<th>Service</th>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ospfd (OSPFD Server)</td>
<td>Routing</td>
<td>Used in routing with the Open Shortest Path First (OSPF) protocol. See “OSPF on Sidewinder” on page 640.</td>
</tr>
<tr>
<td>routed (Network Routing Server)</td>
<td>Routing</td>
<td>This server has been deprecated. Secure Computing recommends using the ripd server instead. See “Configuring RIP (ripd)” on page 629.</td>
</tr>
<tr>
<td>sendmail (Sendmail Server)</td>
<td>Service</td>
<td>Used when running hosted sendmail on a Sidewinder appliances. See “Editing sendmail files on Sidewinder” on page 480.</td>
</tr>
<tr>
<td>sfadmin (SmartFilter Admin Console)</td>
<td>Service</td>
<td>Used when communicating with the SmartFilter Administration Console. See “Setting up SmartFilter for Sidewinder” on page 269.</td>
</tr>
<tr>
<td>sfredirect (SmartFilter Redirect Server)</td>
<td>Service</td>
<td>Used when responding to denied or coached web requests. See “Configuring SmartFilter for Sidewinder” on page 267.</td>
</tr>
<tr>
<td>snmpd (SNMP Agent)</td>
<td>Service</td>
<td>Used in communication with SNMP management stations.</td>
</tr>
<tr>
<td>sshd (SSH Server)</td>
<td>Management</td>
<td>Used when administrators log into the appliance using an SSH client. Often used in troubleshooting and when editing files. See “Administering the Sidewinder appliance using Secure Shell” on page 54. The default policy contains a disabled rule allowing internal access to this SSH server. To enable this rule, select Policy &gt; Rules, expand the Administration rule group, and then enable the Secure Shell Server rule. For added security, modify the rule to make it more restrictive.</td>
</tr>
<tr>
<td>ssod (Passport Authenticator)</td>
<td>Service</td>
<td>Used in single sign-on, or out-of-band, authentication and is the basis for the Passport authenticator. See “Setting up Passport authentication” on page 304.</td>
</tr>
<tr>
<td>telnetd (Telnet Server)</td>
<td>Management</td>
<td>Used when administrators log into the appliance using a Telnet client. <strong>Caution:</strong> Telnet sessions are passed in the clear and should only be used within a protected network. For security reasons, always try to use the SSH server for command line sessions.</td>
</tr>
</tbody>
</table>
To view the available services, select **Policy > Rule Elements > Services**. The main Services window appears.

**Figure 52:** The main Services window

This window is the main window for viewing and creating services. You can perform several tasks directly from this window. Use the toolbar or the right-click menu, shown here, to perform the tasks listed in Table 13.

**Figure 53:** Tasks available in the Services window
Table 13: Tasks that can be performed from the main Services window

<table>
<thead>
<tr>
<th>Icon/Menu item</th>
<th>Task</th>
</tr>
</thead>
</table>
| New Service    | Create a new service by clicking **New Service**. The New Service window appears.  
See “Creating and modifying services” on page 147 and “Configuring servers” on page 154 for more information. |
| New Service Group | Create a new service group by clicking **New Group**. The New Group window appears.  
See “Creating and modifying service groups” on page 156 for more information. |
| Modify         | Modify a service or service group by double-clicking it, or selecting the item and then clicking **Modify**. (Read-only administrators can click **View** to view a service or service group.)  
• For services, this opens the Modify Service window. See “Creating and modifying services” on page 147 and “Configuring servers” on page 154 for more information.  
• For service groups, this opens the Modify Service Group popup, where you modify the group’s description and selected services. |
| Delete         | Delete a service or service group by selecting the item(s) to delete and clicking **Delete**. |
| Rename         | Rename a service or group by clicking **Rename**. |
| Usage          | View what rules and rule groups use a service or service group by selecting an item and then clicking **Usage**. |
| Find           | Find a service or service group by entering a character string related to the item you are searching for in the **Find** field. The search function searches all columns, and filters as you type.  
For example, if you are searching a service based on the HTTP proxy, typing “http” reduces the list to only the services containing that character string.  
Clear the Find field to show all options again. |
Creating and modifying services

This section provides information on creating and modifying services.

Several different actions provide access to a service:

- Select **Policy > Rule Elements > Services**, then click **New** to create a new proxy or filter service.
- Select **Policy > Rule Elements > Services**, then double-click a service (or select it and then click **Modify**) to change an existing service. You can change the service’s description, its service properties, or its global agent properties.
  - Use **Rename** to change a service’s name.
  - Read-only administrators can click **View** to view a service.
- Select **Policy > Rules**, open a rule and, next to the Service field, click ![icon]. On the Services popup, click **New > Service**.

**Note:** You cannot create new servers, or rename or delete existing servers.

The New/Modify Service window appears. See the following sections for information on configuring each property.

![Figure 54: The new/modify service window]
Chapter 6: Services

Creating and modifying services

Configuring service-specific properties

Use the New/Modify Service window to create or modify services. Once a service is saved, it is available for use in rules. When you create a rule that uses a new service and that rule is enabled, the appliance automatically enables the service’s agent in the rule’s source burbs which begins managing traffic using this agent. The appliance disables an agent when all rules using that agent are deleted or disabled.

**Note:** Once a service has been saved, you cannot modify its agent.

1. In the **Name** field, type a descriptive name that quickly identifies this service.
   - Valid values include alphanumeric characters, periods (.), dashes (-), underscores (_), and spaces ( ).
   - The name cannot exceed 256 characters.

2. [Optional] In the **Description** field, add any useful information about this service.

3. In the **Agent** field, select the agent to use in this service.
   
   **Note:** This window’s fields and property options change based on the agent. Once an agent is selected, only the appropriate fields display.

4. Adjust the default service properties as needed.
   
   The sections following this procedure describe the general properties that are available for each service.

5. Click **Add** or **OK** to return to the main Services window.

6. Save your changes.

This service is now available for use in a rule.
General proxy properties

The proxy service properties are:

• **TCP/UDP ports** — Select the port or ports on which this service will accept traffic:
  – Enter the port or port range directly, or click ![ ] to display a list of protocols and their default ports.
  – Do not specify a port number or range that is currently being used by another proxy agent or server agent running on the appliance in the same burb. Use the Monitor > Service Status window to see if a different service is already listening on a given port. See Chapter 14, “Service Status,” on page 421 for more information.

  **Important:** If you set up your own proxies or reconfigure established proxies, **do not use ports 9000–9010. These ports are reserved by the appliance for administration purposes.**

• **Timeouts** — Set the length of time, in seconds, that the appliance will wait before closing a connection. Return to an agent’s default timeout values at any time by clicking **Restore Defaults**.

  In most cases, the defaults should be appropriate.
  – TCP idle timeout — Set the length of time, in seconds, that the TCP connection can remain idle before it is closed.
  – UDP idle timeout — Set the length of time, in seconds, that the UDP “session” can remain idle before it is closed.

• **Connection type (transparent, non-transparent, or both)** — Select the transparency this service will allow:
  – Select **Transparent** to allow only transparent connections.
  – Select **Non-Transparent** to allow only non-transparent connections.
  – Select **Both** to allow either connection type.

  For the SOCKS, FTP, HTTP, and HTTPS proxy services, if you select **Non-Transparent** or **Both**, make sure the application defense used in a rule with this service specifies which destination ports are allowed. This setting is located on the application defense’s Connection tab. See Chapter 7, “Application Defenses,” on page 159 for more information.

  See “Passing traffic transparently and non-transparently” on page 118 for more information.

• **Enable fast path sessions** — Leave this option checked unless you are experiencing performance problems.

  See “When to disable Fast Path Sessions” on page 119 for more information.
General filter properties

The filter service properties are:

- **TCP/UDP ports** — Select the port or port ranges on which this service will accept traffic. Click ... to view or search a port list. If you know which port you want to use, enter that port number directly in the field.

  **Note:** Do not use ports 9000–9010. These ports are reserved by the appliance for administration purposes.

- **Stateful packet inspection** — Select the Enable stateful packet inspection check box. This option must be selected in order to configure the other fields in this area. This option is enabled by default.

  To disable stateful packet inspection, clear the Enable stateful packet inspection check box.

  When enabled, the configurable fields are:

  - **Enable stateful session failover:** Select this option to have existing filter sessions transferred to an HA cluster’s secondary node during a failover event. This option is enabled by default.

    **Tip:** You may want to disable this option for short-lived connections.

    For more information on stateful session sharing, see “Stateful session failover in an HA cluster” on page 142.

  - **Reset TCP connections after connection timeout** — When the connection times out, a TCP Reset packet is sent to the client and server.

  - **Timeouts** — Set the length of time, in seconds, that the appliance will wait before closing a connection.

    - **TCP connection timeout** — Set the length of time, in seconds, that is allowed for the TCP connection to establish. Valid values are 1–65535.

    - **TCP idle timeout** — Set the length of time, in seconds, that the TCP connection can remain idle before it is closed. Valid values are 1–65535.

    - **UDP idle timeout** — Set the length of time, in seconds, that the UDP session can remain idle before it is closed. Valid values are 1–65535.

    - **(ICMP Packet Filter only) Response timeout** — Set the length of time, in seconds, that a session will await responses after the final request. Valid values are 1–100000.

    - **Require UDP checksum** — Requires the UDP packet to contain a checksum. If this option is enabled and a packet does not contain a UDP checksum, the packet is dropped.
• **Restrict source port** — Specify the port or range of ports (inclusive) from which connections are allowed to be initiated. Note the following:
  – Valid values are 1–65535.
  – To specify “any port,” leave the field blank.

• **Bi-directional** — Allows traffic or session to be initiated from either source or destination addresses. Use this only if your source port and destination port are the same.

  *Note:* NAT and redirection are not allowed for bi-directional rules with stateful packet inspection enabled.

• **(ICMP Packet Filter only) Message type** — Select the ICMP message types that you want to this service to filter by checking the check box next to each desired message type. Available options are:
  – **echo** — Selecting this matches echo requests and responses used by ping.
  – **info** — Selecting this matches ICMP information requests and responses.
  – **timestamp** — Selecting this matches timestamp requests and responses.

  *Note:* ICMP control and error messages generated by TCP/UDP traffic are managed using TCP/UDP rules, as opposed to ICMP rules. For example, if you want to pass “host unreachable” error messages for a specific rule’s undelivered TCP packets through the appliance, you would configure this option on the Packet Filter application defenses instead of using the ICMP service.

• **(Other Protocol Packet Filter only) Protocol** — Expand the drop-down list and select the protocol to use for this service.

**General server properties**

Server properties vary greatly from one server to the next. See “Configuring servers” on page 154 for detailed information on each server.

**Configuring an agent’s global properties**

Some proxy and filter agents have properties that are global, meaning the values are shared among all services using that agent. Proxy agents have the expected connection setting, which determines the number of agents that are started to handle the expected traffic volume. Filter agents have settings for the maximum numbers of TCP sessions, UDP sessions, and the reserved port range. Global properties are related to the agent and not the service. This means that if you have five services using the same agent, such as the TCP/UDP Packet Filter agent, those five services must all share the same reserved port range. If you change a global property value while editing a service, all services using that agent are updated to use the new value.
If an agent has one or more configurable global properties, a Properties button appears next to the Agent field. The following sections explain which agents have global properties and how the values affect that agent’s behavior.

**Note:** For the Citrix Proxy agent, the UDP ports are a global property. Therefore, if you change the UDP port on one service, all services using the Citrix Proxy agent will be updated with that value.

### Setting expected connections limits

Certain proxy agents have the ability to start additional instances to improve performance when experiencing heavy traffic volumes. Agents that have this ability are: the Citrix Proxy agent, the FTP Proxy agent, the Generic Proxy agent, the HTTP Proxy agent, the HTTPS Proxy agent, the MS-SQL Proxy agent, the Oracle Proxy agent, the SMTP (Mail) Proxy agent, and the SOCKS Proxy agent.

When you click the Properties tab next to any of those agents, the following window appears:

![Figure 55: Service properties: Expected Connections](image)

Use this window to specify the total number of connections expected for this agent.

For example, if you change this value while creating a new service based on the FTP Proxy agent, then the value changes for all services based on the FTP Proxy agent. If you have two rules using two FTP-based services and the expected connection total is 8000, those rules are expected to support a combined total of 8000 connections.

The default value for all agents is 8000 connections. Other possible values are:

- **1000** — Select this value to open a single instance of a proxy agent.
- **2000** — Select this value to open a single instance of a proxy agent.
- **4000** — Select this value to open two instances of a proxy agent.
- **8000** — Select this value to open four instances of a proxy agent.
- **16000** — Select this value to open eight instances of a proxy agent.
- **32000** — Select this value to open sixteen instances of a proxy agent.

For specific information on when to enable multiple proxy instances, see “Expected connections for proxy agents” on page 117.
Creating and modifying services

Chapter 6: Services

Setting session maximums, port ranges, and intra-burb forwarding for the TCP/UDP Packet Filter agent

When you click the Properties tab next to the TCP/UDP Packet Filter agent, the following window appears:

![Figure 56: Service properties](image)

Use this window to set the global properties for the TCP-UDP Packet Filter agent.

1. In the **Maximum TCP Sessions** field, specify the maximum number of TCP sessions allowed to use the TCP/UDP Packet Filter agent at one time. Valid values are 0–1000000.

2. In the **Maximum UDP Sessions** field, specify the maximum number of UDP sessions allowed to use the TCP/UDP Packet Filter agent at one time. Valid values are 0–1000000.

3. In the **Reserved port range** field, specify the port range that the TCP/UDP Packet Filter agent will reserve for its own use. Valid values are 1024–65533. The default is 9120-9995.

4. [Optional] If you want to forward traffic between network interfaces located within the same burb, select **Allow intra-burb forwarding**.

To enforce intra-burb forwarding, create a rule that:

- has the same source and destination burb.
- uses the TCP/UDP Packet Filter agent as its service.

These values are now set for all services using the TCP/UDP Packet Filter agent.
To begin working with server services, select **Policy > Rule Elements > Services**. To access a server service, double-click it, or select it and then click **Modify**. You can change the service’s description, its service properties, or its global agent properties.

Unlike proxy and filter services, the appliance has a pre-defined list of services that cannot be deleted or added to. You can modify some of these servers’ properties. For a list of all servers, see Table 12 on page 143.

The Login Console server has no configurable properties.

The following servers use the basic service properties that can be adjusted to suit your policy: changepw, entrelayd, fwregisted, and telnetd. They do not have any other configurable properties.

The servers listed in the following table have important configurable properties. The right-hand column gives an overview of what properties are configurable and lists what section to see for detailed configuration information:

**Table 14: Servers with advanced configuration properties**

<table>
<thead>
<tr>
<th>Server</th>
<th>Configurable properties</th>
</tr>
</thead>
</table>
| Admin Console| Change the SSL certificate used by the Admin Console client to authenticate to the Admin Console server and the login banner that greets Sidewinder administrators after they log in.  
See “Configuring the Admin Console server” on page 37. |
| gated        | Edit and validate *gated.conf* at **Network > Routing > Dynamic Routing**, and then click the **Advanced** tab. Only experienced administrators should edit configuration files.  
See cxref. |
| ISAKMP       | Configure the audit level for this server’s traffic, negotiation properties, and extended authentication parameters.  
See “Configuring the ISAKMP server” on page 574. |
| routed       | Configure routed properties at **Network > Routing > Dynamic Routing**.  
See “Configuring RIP (ripd)” on page 629. |
| sendmail     | Edit the sendmail configuration files. You can also run the Reconfigure Mail tool from this service’s Property window.  
See “Setting up and reconfiguring mail” on page 474. |
<table>
<thead>
<tr>
<th>Server</th>
<th>Configurable properties</th>
</tr>
</thead>
</table>
| sfadmin | Change the password that is sent by the Sidewinder appliance to the SmartFilter server. You must make the same change to the SmartFilter Admin Console’s Plugin Definition Admin Password.  
See “Configuring SmartFilter for Sidewinder” on page 267. |
| snmpd | Configure communities, trap destinations, and whether or not to send the authentication failure trap.  
See “Setting up the SNMP agent on Sidewinder” on page 676. |
| sshd | Generate new host keys, and generate and export new client keys.  
See “Administering the Sidewinder appliance using Secure Shell” on page 54. |
| ssod | Configure the login and logout page banners displayed to users when they use the Web login page to start or end a single sign-on session.  
See “Setting up Passport authentication” on page 304. |
Creating and modifying service groups

A service group is a collection of services that have similar security requirements. When your policy requires several services to have identical rules, grouping these services simplifies your policy by reducing the total number of rules. Also, it allows you to change the rule once and update how your organization uses several services, instead of changing each rule individually. The group can contain proxy services, or packet filter services, or servers, but a group cannot contain a mixture of service types.

Use the Service Group window to create new service groups or modify existing service groups.


2. Do either of the following:
   • To create a new service group, click New Service Group.
   • To modify a service group, select a service group from the list and click Modify. (Read-only administrators can click View to view a service group.)

Service groups have a folder icon, and are listed as groups in the Agent column.

The following window appears:

![New/Modify Service Group window](image-url)
3 If creating a new service group, enter a name for the service group in the **Name** field.

**Note:** To rename an existing service group, use Rename on the main Services window.

4 [Optional] In the Description field, enter any information about the service group that may be helpful.

5 At Group Type, select the type of service to appear in the Available services list: **Proxy**, **Packet Filter**, or **Server**.
   - To add a new service to the Available services list, click **New** and enter properties in the New Service window.
   - To see the properties of an existing service, select a service from the Available services list and click **View**.

6 Add or remove services from the service group:
   - To add a service to the service group, select a service in the Available services list, and then click the arrow button.
     Select multiple consecutive entries by pressing the Shift key as you select the entries. To select multiple non-consecutive entries, press the Ctrl key as you select the desired entries.
   - To remove a service from the service group, select the service in the Selected services list, and then click the arrow button.

7 When you are done creating or modifying the service group, click **OK**.

8 Save your changes.

The service group is now available for use in a rule.
Chapter 6: Services

Creating and modifying service groups
CHAPTER 7

Application Defenses

In this chapter...

Understanding Application Defenses ...........................................160
Creating HTTP or HTTPS Application Defenses..........................163
Creating Mail (Sendmail) Application Defenses .........................184
Creating Mail (SMTP proxy) Defenses.........................................196
Creating Citrix Application Defenses............................................200
Creating FTP Application Defenses .............................................202
Creating IIOP Application Defenses.............................................209
Creating T.120 Application Defenses ...........................................210
Creating H.323 Application Defenses ..........................................212
Creating Oracle Application Defenses .........................................215
Creating MS SQL Application Defenses ......................................216
Creating SOCKS Application Defenses ........................................217
Creating SNMP Application Defenses.........................................219
Creating SIP Application Defenses .............................................223
Creating Packet Filter Application Defenses...............................225
Configuring Application Defense groups ....................................228
Use Application Defenses to configure advanced properties for rules. You can refine rules for specific applications that use proxies and filter agents. You can also configure key services such as anti-virus/anti-spyware, anti-spam/anti-fraud, SSL decryption, and web services management.

- You configure Application Defenses in the appropriate Application Defense window.
- An Application Defense is selected in the Rules window. Certain services have related Application Defenses that you can apply to the rule you are creating.

To view the Application Defenses windows, select **Policy > Application Defenses > Defenses**, and then select the type of Application Defense you want to view from the tree. A window similar to the following appears:

![Figure 58: Application Defenses window (HTTP)](image-url)
The top pane of each Application Defense window consists of a table that lists all of the Application Defenses (by row) that are currently configured for the category selected in the tree.

- The Application Defenses that are displayed in the table will vary depending on the defense category you select from the tree.
- The table columns display the attributes for the selected defense. The columns will vary by application defense.
- Basic default defenses (such as default) are pre-configured for each category of Application Defense.

You can perform the following actions in any of the Application Defense windows:

- **Create a new Application Defense** — To create a new Application Defense:
  a. Select the appropriate type of defense in the tree, then click **New**. The New Application Defense window appears.
  b. Type a name for your application defense. If you are creating an HTTP or HTTPS Application Defense, select a type.
  c. Click **OK** and modify the properties in the lower portion of the window.

- **Duplicate an existing Application Defense** — To duplicate an existing Application Defense:
  a. Select the appropriate defense from the table, then click **Duplicate**. The New/Duplicate Application Defense window appears.
  b. Type a name for your application defense. (If you are duplicating an HTTP or HTTPS Application Defense, you cannot select a type.)
  c. Click **OK** and modify the properties in the lower portion of the window.

- **Modify an existing Application Defense** — Select the defense that you want to modify from the table. The configuration information is displayed in the bottom portion of the window.

  To modify the Application Defense in a pop-up window format, click **Modify**. (Read-only administrators can click **View** to view an Application Defense in a pop-up window.)

- **Rename an existing Application Defense** — Select the appropriate Application Defense from the table and click **Rename**, then type a new name in the Rename window.

- **Delete an existing Application Defense** — Select the appropriate Application Defense from the table and click **Delete**.

**Note:** You cannot delete an Application Defense if it is being used in a rule. If the Application Defense is used in a rule, a pop-up window will appear informing you which rules are currently using this defense. Before you can delete the defense, you will need to modify each of the rules to remove the specified defense from those rules.
• View the rules in which an Application Defense/Group is currently used — 
   Select the appropriate defense (or group) and click **Usage**. A pop-up 
   window appears listing the rule names that are currently using the specified 
   defense. Click **Close** when you are finished viewing the rule list.

The bottom portion of each window (or pop-up, if you clicked **Modify**) displays 
the actual configuration information for the selected Application Defense. The 
information will vary depending on the Application Defense category you 
select. The following fields remain constant among all Application Defense 
windows:

• **Name** — This field contains the name of the Application Defense that you 
  are viewing. If you need to rename an Application Defense, click **Rename** 
  and type a new name.

• **[HTTP/HTTPS only] Type** — Use this field to specify whether a defense will 
  be used to protect a server, client, or both. For more information about the 
  Type field, see “Creating HTTP or HTTPS Application Defenses” on page 
  163.

• **Description** — Use this field to provide information about the Application 
  Defense to help you more easily identify it.

For information on configuring a specific Application Defense, see the 
following:

– HTTP/HTTPS (page 163)
– Mail (Sendmail) (page 184)
– Mail (SMTP proxy) (page 196)
– Citrix (page 200)
– FTP (page 202)
– IIOP (page 209)
– T.120 (page 210)
– Multimedia (page 210)
– H.323 (page 212)
– Oracle (page 215)
– MS SQL (page 216)
– SOCKS (page 217)
– SNMP (page 219)
– SIP (page 223)
– Packet Filter (page 225)

**Note:** For information on configuring Application Defense groups, see 
“Configuring Application Defense groups” on page 228.
Creating HTTP or HTTPS Application Defenses

The HTTP/HTTPS Application Defenses allow you to configure advanced parameters for HTTP or HTTPS and SSO proxy rules. To create HTTP or HTTP Application Defenses, select Policy > Application Defenses > Defenses and then select HTTP or HTTPS. One of the following windows appears.

Figure 59: Application Defense (default): HTTP and HTTPS
Chapter 7: Application Defenses
Creating HTTP or HTTPS Application Defenses

Configuring the HTTP/HTTPS: Enforcements tab

Use the Enforcements tab to select the feature enforcement tabs that you want to make available for configuration, as well as relax enforcement of HTTP proxy standards. If you are configuring an HTTPS Application Defense, you can also configure SSL decryption properties in the Enforcements tab.

In the Type drop-down list, you can specify whether this defense will be used to protect a server, client, or both:

• **Combined** — [HTTP only] This option allows you to create an Application Defense that can protect both an HTTP client (outbound) and an HTTP server (inbound) behind the Sidewinder appliance. When you select this option, all of the configuration options for this defense will appear. However, some of the options that you configure will only apply to the client or server. (For example, HTTP Request properties do not apply to the client. Therefore, if you select Combined, HTTP Request properties that you configure will only apply to the server.)

• **Client** — This option allows you to create an Application Defense that protects a client behind the Sidewinder appliance. Options that do not apply for client protection (such as HTTP Requests) will not be available for configuration.

• **Server** — This option allows you to create an Application Defense that protects a server behind the Sidewinder appliance. Options that do not apply for server protection (such as Content Control options other than SOAP) will not be available for configuration.

To enable enforcement of HTTP proxy standards in a manner that allows traffic from systems that do not adhere to strict RFC standards for the HTTP proxy, select the Relax Protocol Enforcements option. Enabling relaxed mode allows the following RFC infractions:

• Media types in Content-Type: headers in a relaxed form, where the subtype is not required
• Empty headers
• Duplicated responses from the server where the response is the same but the version is different
• Query strings containing arbitrary data

**Caution:** Each listed infraction introduces an element of risk into your security policy, particularly if enabled on server-side rules. Use this mode only when necessary, and implement on a rule-by-rule basis.
Select the **Relax Protocol Enforcements** option if the above infractions are acceptable or required in your network. When you enable this option, you will also need to specify whether the protocol enforcements will be relaxed when receiving HTTP traffic from clients, servers, or both by selecting one of the following options from the drop-down list:

- **Client** — Select this option to relax protocol enforcements only when receiving HTTP traffic from clients.
- **Server** — Select this option to relax protocol enforcements only when receiving HTTP traffic from servers.
- **Client and Server** — Select this option to relax protocol enforcements when receiving HTTP traffic from both clients and servers.

**Enabling HTTP/HTTPS configuration tabs**

To configure an HTTP or HTTPS tab, enable the service on the Enforcements tab. You cannot configure a tab unless it is enabled.

- The Connection tab for HTTP and HTTPS does not need to be enabled before you can configure it.
- If you are configuring an **HTTPS** defense and you select the **Decrypt HTTP Traffic** check box, you can enable any of the tabs below. If you select the **Do Not Decrypt HTTP Traffic** check box, you can enable only the SmartFilter tab.

The following tabs can be enabled:

- **HTTP URL Control** — Use the HTTP URL Control tab to configure filtering on the URL contained in the HTTP request. To enable URL filtering, select this check box. To configure HTTP URL filtering properties, select the HTTP URL Control tab and see “Configuring the HTTP/HTTPS: HTTP URL Control tab” on page 168.
- **FTP URL Control** — Use the FTP URL Control tab to configure filtering on the URL contained in an HTTP request for FTP traffic. To enable FTP URL filtering, select this check box. To configure FTP URL filtering properties, select the FTP URL Control tab and see “Configuring the HTTP: FTP URL Control tab” on page 170.
- **HTTP Request** — Use the HTTP Request tab to configure header filtering on HTTP requests. To enable HTTP header filtering for HTTP requests, select this check box. To configure HTTP header request properties, select the HTTP Request tab and see “Configuring the HTTP/HTTPS: HTTP Request tab” on page 171.
- **HTTP Reply** — Use the HTTP Reply tab to configure header filtering on HTTP replies. To enable HTTP header filtering for HTTP replies, select this check box. To configure HTTP header reply properties, select the HTTP Reply tab and see “Configuring the HTTP/HTTPS: HTTP Reply tab” on page 173.
• **MIME/Virus/Spyware** — Use the MIME/Virus/Spyware tab to configure MIME (Multi-Purpose Internet Mail Extensions) and anti-virus/spyware filtering, and infected file handling. To enable filtering for MIME/virus/spyware, select this check box. To configure MIME/virus/spyware properties, select the MIME/Virus/Spyware tab and see “Configuring the HTTP/HTTPS: MIME/Virus/Spyware tab” on page 175.

• **Content Control** — Use the Content Control tab to configure filtering for Web content types including ActiveX, Java, scripting languages, and SOAP. (For HTTPS, you can only configure SOAP filtering.) To enable content filtering, select this check box. To configure content control properties, select the Content Control tab and see “Configuring the HTTP/HTTPS: Content Control tab” on page 180.

• **SmartFilter** — Use the SmartFilter tab to enable filtering of Web traffic using SmartFilter.

⚠️ **Important:** Do not alter the default SmartFilter settings. They enable communication with the SmartFilter server. They do not filter traffic.

For information on configuring the SmartFilter tab, see “Configuring the HTTP/HTTPS: SmartFilter tab” on page 181.
Configuring SSL decryption properties [HTTPS server only]

The Sidewinder appliance can perform SSL decryption services at the firewall level on a per-rule basis, increasing the security of your data transactions.

To use SSL decryption services on the Sidewinder appliance, you must have the following features licensed:

- **Strong Cryptography** — This feature is included with the basic Sidewinder appliance license.
- **SSL Decryption** — This feature is an add-on module. If it is purchased after the Sidewinder appliance’s initial activation, you will need to relicense your appliance to activate this feature. For licensing information, see “Activating the Sidewinder license” on page 705.

To configure decryption properties for an HTTPS Application Defense, follow the steps below.

**Important:** Proxy rules that use HTTPS Application Defenses with the Decrypt HTTP Traffic option enabled must have redirection configured.

1 Select from the following:
   - To enable SSL decryption for an Application Defense, select Decrypt HTTP Traffic. Remember to verify that the SSL Decryption and Strong Cryptography features are licensed.
   - To allow HTTP traffic to pass through without being decrypted, select Do Not Decrypt HTTP Traffic. SSL connections will be validated when this option is selected. If you select this option, you can select the SmartFilter check box to enable Web filtering and enable the SmartFilter tab for configuration.

2 [Conditional] If you are configuring an HTTPS defense to allow clientless VPN sessions to access a Microsoft Exchange® Server, select the Rewrite Microsoft OWA HTTP check box.

3 Select the appropriate firewall certificate from the Firewall Certificate drop-down list. This is the certificate that is used to authenticate the Sidewinder appliance to the remote HTTPS/SSL client. For information on configuring firewall certificates, see “Configuring Certificate Management” on page 577.

4 Click SSL Settings to configure SSL properties. Configurable properties include specifying the accepted SSL/TLS versions and the minimum cryptography strength.

5 Save your changes.
Creating HTTP or HTTPS Application Defenses

Chapter 7: Application Defenses

Configuring the HTTP/HTTPS: HTTP URL Control tab

Use the HTTP URL Control tab to configure URL control properties, such as which HTTP operations will be allowed and which URLs will be explicitly denied.

Figure 60: HTTP/HTTPS: HTTP URL Control tab

To configure the HTTP URL Control tab:

1. In the Allow Selected HTTP Commands area, select the commands (operations) that you want to allow users to issue by clicking in the corresponding check box(es).

   To select all of the commands, click Select All. To clear all of the commands, click Deselect All. A description of each command is provided within the window.

2. To disallow special characters in a query, select the Enforce Strict URLs check box. If you select this option, URLs with certain special characters will be disallowed under certain circumstances (such as RFC violation). For example: quote ("), back quote (‘), brackets ([], {}, < >), pipe (|), back slash (\), and caret (^).

3. To allow international multi-byte characters in a query, select the Allow Unicode check box.

4. [Server or Combined only] In the Maximum URL Length field, specify the maximum length allowed for a URL. The default value is 1024 characters. Valid values are 1–10000.

5. To require that the HTTP version be included in all requests, select the Require HTTP Version in Request check box.
6  [Conditional] If you selected **Require HTTP Version in Request** in the previous step, specify the HTTP versions that you want to allow in the **Allow Selected HTTP Versions** area: version 1.0 and 1.1 are available.

7  In the **Deny Specified URL Matches** table, you can specify strings that can be matched to parts of the URL. If the string is found in a particular URL, the request is explicitly denied. The table lists any match strings that are currently denied.

   To add a match string to the list, click **New**. To modify a match string in the list, select the URL and click **Modify**.
Configuring the HTTP: FTP URL Control tab

Use this tab to control access to FTP servers through HTTP proxies. Access to FTP servers is allowed by default.

You can perform the following actions:

• **Select the type of commands you will allow** — You can allow FTP traffic to upload and/or download files and directories from an FTP server.
  - Select **GET** to allow files to be downloaded. Clear this option to deny downloaded files.
  - Select **PUT** to allow files to be uploaded. Clear this option to deny uploaded files.
  - Use the **Select All** and **Deselect All** buttons to select or clear both options at once.

• **Select the data connection type** — Select which commands the appliance sends to the FTP server to initiate the data exchange:
  - **Active** — Select this option to tell the FTP server which port to send data to.
  - **Passive** — Select this option to allow the FTP server to specify which port to send data to.
  - **Both** — Select this to make both options available. The passive option is tried first. This is the default selection.
Configuring the HTTP/HTTPS: HTTP Request tab

Use the HTTP Request tab to configure header filtering for HTTP requests. This tab is only available if you selected Server or Combined in the Type field.

![Figure 62: HTTP/HTTPS: HTTP Request tab](image)

**Note:** The fields in this tab will be disabled unless you select the HTTP Request check box on the Enforcements tab.

To configure the HTTP Request tab:

1. Select the type of HTTP header filtering you want to allow or deny in the Selected HTTP Request Header Filter Types area:

   **Note:** The X-* filter type is a wildcard filter that will allow or deny all X-xxx request headers (commonly found in user-defined headers). If you create an Allow list and do not include the X-* filter type, most HTTP traffic will be denied.

   - **None** — Select this option if you want to clear all HTTP request header filter types in the list. (You can also clear all of the types by clicking Deselect All.)
   - **Standard** — Select this option if you want to automatically select all of the header types contained in the list. (You can also select all header types by clicking Select All.)
   - **Paranoid** — Select this option if you want to exclude all options not defined in the RFC.
   - **Custom** — Select this option if you want to manually select which HTTP header types you will allow or deny.

   **Note:** Header types that are not in the list are handled the same as unselected header types.
2 In the **Filter Option** field, determine whether you want to allow or deny the header types you select, as follows:

- **Allow** — Select this option to *allow* all header types that are selected in the HTTP Request Header Filter Types window. All other types will be denied.
- **Deny** — Select this option to *deny* all header types that are selected in the HTTP Request Header Filter Types window. All other types will be allowed.

3 In the **Denied Header Action** area, select one of the following options:

- **Block Entire Page** — Select this option to block the entire page when an HTTP header is denied.
- **Allow Page Through Without Denied Headers** — Select this option to mask the denied HTTP header, but still allow the page to be viewed. (A denied HTTP header will be overwritten with Xs.)

4 In the **Denied header values** area, you can create a list of headers and matching values that you want blocked. If a specified header appears in a request or response, and it contains the specified value, it is dropped from the message.

- Full header names must be used.
- Regular expressions are not supported.
- Values are matched in a case-insensitive manner, and are used exactly as specified.

Click **New** to create a new header and value. Click **Modify** to change an existing header.

5 To block headers that contain binary data, select **Deny binary data**.

Every header is scanned to detect binary data. This prevents attacks that put binary data in requests.

- Binary data means ASCII codes 0x00 to 0x1f and 0x7f hexadecimal.
- This does not affect escaped characters that convert to legal ASCII characters. For example, `%41` in a header would convert to the letter *A* in ASCII.

*Note:* This feature reduces your appliance’s performance.
Chapter 7: Application Defenses

Creating HTTP or HTTPS Application Defenses

Configuring the HTTP/HTTPS: HTTP Reply tab

Use the HTTP Reply tab to configure header filtering for HTTP replies. Follow the steps below.

Figure 63: HTTP/HTTPS: HTTP Reply tab

Note: The fields in this tab will be disabled unless you select the HTTP Reply check box on the Enforcements tab. Also, this tab is not available for HTTPS if you select Client in the Type field.

To configure the HTTP Reply tab:

1. Select the type of HTTP header filtering you want to allow or deny in the Selected HTTP Reply Header Filter Types area. The following options are available:

   Note: The X-* filter type is a wildcard filter that will allow or deny all X-xxx reply headers (commonly found in user-defined headers). If you create an Allow list and do not include the X-* filter type, most HTTP traffic will be denied.

   - **None** — Select this option if you want to clear all HTTP reply header filter types in the list. (You can also clear all of the types by clicking Deselect All.)
   - **Standard** — Select this option if you want to automatically select all of the header types contained in the list. (You can also select all header types by clicking Select All.)
   - **Paranoid** — Select this option if you want to exclude all options not defined in the RFC.
   - **Custom** — Select this option if you want to manually configure which HTTP reply header types you will allow or deny.

   Note: Header types that are not in the list are handled the same as unselected header types.
2 In the Filter Option field, determine whether you want to allow or deny the header types you select, as follows:
   • Allow — Select this option to allow all header types that are selected in the HTTP Reply Header Filter Types window. All other types will be denied.
   • Deny — Select this option to deny all header types that are selected in the HTTP Reply Header Filter Types window. All other types will be allowed.

3 In the Denied Header Action area, select one of the following options:
   • Block Entire Page — Select this option to block the entire page when an HTTP reply header is denied.
   • Allow Page Through Without Denied Headers — Select this option to mask the denied HTTP reply header, but still allow the page to be viewed. (A denied HTTP reply header will be scrubbed.)

4 In the Denied header values area, you can create a list of headers and matching values that you want blocked. If a specified header appears in a request or response, and it contains the specified value, it is dropped from the message.
   • Full header names must be used.
   • Regular expressions are not supported.
   • Values are matched in a case-insensitive manner, and are used exactly as specified.

Click New to create a new header and value. Click Modify to change an existing header.

5 To block headers that contain binary data, select Deny binary data.

Every header is scanned to detect binary data. This prevents attacks that put binary data in requests.
   • Binary data means ASCII codes 0x00 to 0x1f and 0x7f hexadecimal.
   • This does not affect escaped characters that convert to legal ASCII characters. For example, %41 in a header would convert to the letter A in ASCII.

Note: This feature reduces your appliance’s performance.
Configuring the HTTP/HTTPS: MIME/Virus/Spyware tab

Use the MIME/Virus/Spyware tab to configure filtering for MIME, virus, and spyware scanning services. The tab contains a rule table that displays any MIME/Virus/Spyware filtering rules that have been created. The tab also contains various virus scanning and handling configuration options.

![Figure 64: HTTP/HTTPS: MIME/Virus/Spyware tab](image)

**Security Alert:** If you want to perform virus and spyware scanning, you must create the appropriate MIME rules with Virus/Spyware Scan selected in the Action field. Rules that are configured only to allow or deny traffic based on rule criteria will not perform virus and spyware scanning. (See step 1 for information on configuring MIME/Virus/Spyware filter rules.)

- The fields in the MIME/Virus/Spyware tab will be disabled unless you select the MIME/Virus/Spyware check box on the Enforcements tab.
- For HTTP defenses, MIME/Virus/Spyware scanning services are not available if you select Server in the Type field.
- For HTTPS defenses, MIME/Virus/Spyware scanning services are not available if you select Client in the Type field.
- The MIME type tells the browser or server what type of information it is receiving.
- Virus and spyware scanning is performed on data sent from the client if the request method is either PUT or POST, and the appropriate file type is specified for scanning in the MIME/Virus/Spyware filtering rules table.

**Important:** You must license scanning services before the MIME/Virus/Spyware filter rules you create will scan HTTP/HTTPS traffic. See “Configuring virus scanning services” on page 251.
To configure the MIME/Virus/Spyware tab:

1. Configure the appropriate MIME/Virus/Spyware filter rules in the **MIME/Virus/Spyware Filter Rules** table:
   - **Create a new filter rule** — To create a new filter rule, click **New**. See “About the MIME Rule Edit window” on page 177.
   - **Modify an existing filter rule** — To modify an existing filter rule, select the rule you want to modify, and click **Modify**. See “About the MIME Rule Edit window” on page 177. (If you are modifying the default MIME filtering rule, see “Configuring the Default filtering rule action” on page 179.)
   - **Delete a filter rule** — To delete an existing filter rule, select the rule you want to delete and click **Delete**.

2. Determine how infected files will be handled in the **Infected File Handling** area as follows:
   - To discard infected files, select **Discard Infected Files**.
   - To remove the virus from the file and then continue processing the file, select **Repair Infected Files**.

3. To reject all files in the event that scanning is not available, select the **Reject All Files If Scanning Is Unavailable** check box. If you select this option, the connection will be dropped if scanning is unavailable (for example, due to out-of-date virus data, an expired license, or a configuration error).

4. In the **Scan File Size Limit (KB)** field, specify the maximum file size that will be allowed in KB. If a file exceeds the size specified in this field, filtering will not take place and the file will be denied.

   **Note:** To allow files over the size limit without scanning, clear the **Reject All Files If Scanning Is Unavailable** option.
About the MIME Rule Edit window

Use this window to add or modify MIME/Virus/Spyware filtering rules.

- Rules that are configured with an allow or deny action will allow or deny traffic based on the rule criteria that is defined for those rules. Allow and deny rules do not perform virus scanning. To perform virus scanning for traffic that matches a rule before it is allowed, you must specify Virus/Spyware Scan in the rule’s Action field.

- Rules that specify both a MIME type/subtype and file extensions will allow or deny any traffic that matches either the MIME Type or a File Extension type. That is, the traffic does not need to match both criteria to match the rule.

To add or modify MIME/Virus/Spyware filtering rules:

1. In the MIME Type drop-down list, select the MIME type for which you want to filter. If you select the asterisk (*) option, the filter rule will ignore this field when determining a match.

2. In the MIME Subtype drop-down list, select a subtype for the MIME type that you selected in the previous step (the available options will vary depending on the MIME type you selected). If you select the asterisk (*) option, the filter rule will ignore this field when determining a match.
3 In the **File Extensions** area, specify the type of file extensions that you want to filter:

- **Ignore Extensions (•)** — Select this option to ignore extensions when determining a match.
- **Archive Extensions** — Select this option to specify basic archive extensions (such as .tar, .zip, etc.) for the specified MIME types/sub-type.
- **Standard Extensions** — Select this option to specify the standard file extensions associated with the selected MIME type/subtype. For example, if you select text in the **MIME Type** field, and HTML in the **MIME Subtype** field, the .htm and .html file extensions will appear in the standard list.
- **Custom** — Select this option to create a custom list of file extensions for the selected MIME type/subtype.
  - To add a file extension to the list, click **New** and type the extension *(without the leading period)* that you want to add.
  - To delete a file extension, select the extension you want to delete and click **Delete**.
  - You can use the **Reset** button to clear all extensions from the list, or to select a different file extension list (Archive or Standard).

4 In the **Action** area, select one of the following options:

- **Allow** — Select this option if you want to explicitly allow the file extensions that you specified in this window. (Virus scanning will not be performed.)
- **Deny** — Select this option if you want to explicitly deny the file extensions that you specified in this window. (Virus scanning will not be performed.)
- **Virus/Spyware Scan** — Select this option if you want to perform virus scanning on the file extensions that you specified in this window. If no viruses are detected, the file will be allowed through the system.
Configuring the Default filtering rule action

The Default filter rule is a catch-all rule designed to occupy the last position in your rule table.

To modify the default action for the default MIME filtering rule:

1 Select the default rule in the table and click Modify. The MIME Default Action window appears.

2 Select the appropriate action for this rule and then click OK.
   • Allow — The default rule is initially configured to allow all data that does not match other filter rules. If you leave the default rule as an allow rule, you must create filter rules that require virus scanning or explicitly deny any MIME types that you do not want to allow, and place them in front of the default allow rule.
   • Deny — If you prefer the default rule to deny all data that did not match a filter rule, you must create the appropriate virus scan and allow rules and place them in front of the default deny rule.
   • Virus/Spyware Scan — If you want to perform virus and spyware scanning for traffic that does not match any allow or deny filter rules you create, select this option. You will then need to create the appropriate allow and deny rules that will not require scanning.

3 Save your changes.
Configuring the HTTP/HTTPS: Content Control tab

Use the Content Control tab to configure filtering to deny certain types of embedded objects. Follow the steps below.

![HTTP/HTTPS: Content Control tab](image)

**Note:** If you are configuring an HTTP or HTTPS defense for type Server, you will only be allowed to select the Deny SOAP option. If you are configuring an HTTP defense for type Client, the Deny SOAP option is not available.

To configure the Content Control tab:

1. Select the **Deny ActiveX Controls** check box to scrub the ActiveX embedded objects from the Web content.
2. Select the **Deny Java Applets** check box to scrub the Java Applet objects from the Web content.
3. Select the **Deny Scripting Languages** check box to scrub scripting languages from the Web content.
4. Select the **Deny SOAP** check box to scrub SOAP embedded objects from the Web content. In some cases, selecting this option can cause the entire page to be denied if it contains SOAP embedded objects.
Configuring the HTTP/HTTPS: SmartFilter tab

When SmartFilter is configured, use this window to determine whether requests will be rejected if the SmartFilter server is unavailable.

Select the **Reject all requests if SmartFilter is unavailable** check box to reject any requests that occur when the SmartFilter server on the appliance is unavailable.

For more information about configuring SmartFilter, see “Configuring SmartFilter for Sidewinder” on page 267.
Configuring the HTTP/HTTPS: Connection tab

Use the HTTP/HTTPS Connection tab to configure whether to send traffic to an upstream proxy, and to define ports that non-transparent proxies can send traffic to.

To configure the Connection tab:

1. To forward requests to upstream proxies:
   a. In the Upstream proxies area, click **New** and define the upstream proxy:
      - **Scheme** — Enter the scheme of the requests to be forwarded. A scheme is the protocol identifier in the URI naming structure, for example, `gopher`.
      - **IP address** — Enter the IP address of the upstream proxy where the request is being sent.
      - **Port** — Specify the port of the upstream proxy where the request is being sent.
      - **Enabled** — Select this check box to allow the defined scheme to be forwarded.
   b. Click **OK** and save your changes.
• HTTP and FTP traffic by default is handled locally by the Sidewinder appliance. To forward HTTP or FTP requests to an upstream proxy, select the scheme and click **Modify**, then define the upstream proxy.

• HTTP requests can be transparent or non-transparent. If you allow transparent HTTP connections when using this option, the URL will be rewritten to contain an IP address rather than a hostname. If you allow transparent connections, you must first ensure that the upstream proxy server will accept an IP address.

• The HTTP scheme handles both HTTP and HTTPS, if non-transparent HTTPS is allowed through the proxy.

• Non-HTTP requests must be non-transparent so that the protocol can be identified. The HTTP service must be set to allow Non-Transparent or Both connection types.

• The connection request must match existing HTTP rules.

• An upstream proxy must be available.

2 To define allowable destination ports for non-transparent proxies: In the **Destination ports allowed through non-transparent HTTP proxy** area, click **New**. Specify a port, a port range, or select from pre-defined ports on the **Edit a Port** window.

   • Pre-defined ports are 80, 443, 1024–65535.

   • To modify an existing port entry, select the entry and click **Modify**.

   • To delete an existing port entry, select the entry and click **Delete**.

   **Note:** This table identifies the destinations the non-transparent proxy is allowed to send traffic to. If no destinations are identified, proxy connection will be denied. (HTTP and FTP connections will still be processed.)

3 [HTTP only] To allow non-transparent HTTPS traffic through the HTTP proxy, select the **Allow non-transparent HTTPS traffic through the HTTP proxy** check box. (The service must allow non-transparent connections.)

4 [HTTP only] To define allowable destination ports for FTP traffic through non-transparent proxies: In the **Destination ports allowed through non-transparent HTTP proxy using FTP** area, click **New**. Specify a port, a port range, or select from pre-defined ports on the **Edit a Port** window.

   • The pre-defined port is 21.

   • To modify an existing port entry, select the entry and click **Modify**.

   • To delete an existing port entry, select the entry and click **Delete**.
Creating Mail (Sendmail) Application Defenses

Mail (Sendmail) Application Defenses are used in SMTP proxy rules. To configure Mail (Sendmail) Application Defenses, select Policy > Application Defenses > Defenses > Mail (Sendmail).

**Note:** You must have Secure Split SMTP mail servers configured to use mail filtering.

### Configuring the Mail (Sendmail): Control tab

Use this tab to configure filtering for sendmail services.

**Figure 69: Mail (Sendmail): Control tab**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Default mail application defense.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Enable Mail Services:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anti-Relay</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Enable Mail Filters:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size</td>
</tr>
<tr>
<td>Keyword Search</td>
</tr>
<tr>
<td>MIME/Viru/Spyware</td>
</tr>
<tr>
<td>Spam/Fraud</td>
</tr>
</tbody>
</table>

**Note:** The Anti-Relay feature prevents your mailhost from being used by a hacker as a relay point for spam to other sites. This option is automatically enabled for all mail defenses and cannot be disabled.
To configure a Mail (Sendmail) Application Defense:

1. To enable (or disable) a particular type of filtering, you must select the appropriate check box in the **Enable Mail Filters** area. Once you enable a mail filter, you can configure it by selecting the appropriate tab. You cannot configure a mail filter unless you have selected it in this tab. The following filters can be enabled:
   - **Size** — The Size filter allows you to specify the maximum size for mail messages. To configure the Size filter once it has been enabled, select the Size Filter tab. See “Configuring the Mail (Sendmail): Size tab” on page 186.
   - **Keyword Search** — The Keyword Search filter allows you to filter mail messages based on the presence of defined key words (character strings). To configure the Keyword Search filter once it has been enabled, select the Keyword Search tab. See “Configuring the Mail (Sendmail): Keyword Search tab” on page 187.
   - **MIME/Virus/Spyware** — The MIME/Virus/Spyware filter allows you to configure MIME, virus, and spyware filtering for e-mail messages. To configure the filter once it has been enabled, select the MIME/Virus/Spyware tab. See “Configuring the Mail (Sendmail): MIME/Virus/Spyware tab” on page 191.
   - **Spam/Fraud** — The Spam/Fraud filter allows you to filter out mail messages that fall under the “spam” and “fraud” profile. The Spam/Fraud filter can only be enabled or disabled in this window.
     - To enable spam and fraud filtering, select this check box. To disable spam and fraud filtering, clear the check box.
     - To receive automatic updates for the spamfilter server, enable the spamfilter cron job. See “Default cron jobs” on page 812 for more information.
     - If desired, you can modify the default actions for the Spam/Fraud filter in the appropriate configuration file(s) using the Admin Console File Editor. See “Configuring spam filtering services” on page 261 for details.

   **Note:** Before using anti-spam service, the Anti-Spam add-on module must be licensed.

2. To specify how mail messages that are rejected should be handled, select one of the following options in the **Rejected Mail Handling** field:
   - **Discard** — Select this option if you want to discard rejected mail messages without notifying the sender.
   - **Return To Sender** — Select this option if you want to send a rejection notice to the sender.

   **Note:** If a message is denied by the MIME/Virus/Spyware filter rules (configured in the MIME/Virus/Spyware tab), that message will be discarded without sending a rejection notice regardless of which option you select here.
Configuring the Mail (Sendmail): Size tab

Use this tab to configure size restrictions for a Mail (Sendmail) defense.

The Size filter checks e-mail messages for the number of bytes the message contains, including the message header. A message is rejected if it is greater than or equal to the threshold size you specify when you configure a filter.

To configure the Size filter, in the **Maximum Message Size** field specify the maximum message size (in KB) that will be allowed to pass through the appliance. The default is 1024KB. Valid values are 1–2147483647 KB.
Configuring the Mail (Sendmail): Keyword Search tab

Use this tab to configure the Sidewinder appliance to perform a search for specified character set(s), or key words, within an e-mail message. The search scans the message's header and body sections.

- If the mail body contains MIME encoded attachments, the encoded attachments are scanned.
- If the filter finds a specific number of key word matches, the message is rejected.
- If the filter does not match a specific number of key words, it passes the message onto the next filter or to the intended recipient.

Select your key words carefully. For best results:

- Use spaces before and after each defined phrase.
- Create a comprehensive list of phrases instead of relying on wildcard-like searching.
- Note that key word searching is most reliable on MIME attachments with ASCII content-types. If dealing with non-ASCII types of attachments, false positives are likely if the length of the key words are short and the attachments are large.

Following these guidelines can decrease the chance of mistakenly rejecting a legitimate message.
To configure character sets to search for:

1 In the **Minimum Number of Phrase Matches Required for Rejection of Message** field, specify the number of key word matches that must be found in a message before it is rejected.

2 In the **Total Number of Phrase Matches to Verify Before Rejection** field, specify whether the filter will search the entire message for key words, or whether it will stop searching for key words if the minimum number of matches is met:
   - **Minimum** — Select this option if you want the filter to stop searching and fail the message if the minimum number of key word matches is met. This is based on the number that you enter in the previous step. The filter will reject a mail message once the minimum number of key words are matched.
   - **All** — Select this option if you want the filter to continue searching the message for key words after the minimum number of key word matches is met, for auditing purposes. After searching the entire message for key word matches, the message is rejected.

3 The Phrase List table provides the list of phrases that will be filtered for this Application Defense. The table contains three columns:
   - **Before** — This column indicates whether a space is required immediately before the specified phrase to match the filter. An asterisk (*) indicates that the phrase will not match unless there is a space immediately in front of the phrase.
   - **Phrase Text** — This column lists each phrase for which the filter will search.
   - **After** — This column indicates whether a space is required immediately after the specified phrase to match the filter. An asterisk (*) indicates that the phrase will not match unless there is a space immediately following the phrase.

To add a phrase, click **New**. To modify a phrase, highlight the appropriate row and click **Modify**. The Keyword Search: Phrase Edit window appears.
Chapter 7: Application Defenses

Creating Mail (Sendmail) Application Defenses

Configuring the Keyword Search: Phrase Edit window

Use this window to add or modify character strings (known as “key words”).

Figure 72: Keyword Search: Phrase Edit window

To configure a keyword search:

1. In the **Text** field, type the text you want to filter. The keyword search is not case sensitive. The character string must consist of at least two characters. You can include any printable character, as well as spaces.

   **Note:** Some special characters, such as a space, will be displayed in the Key Word list using their hexadecimal equivalents.

   You can also define a key word entry that consists partly or entirely of binary characters. The binary characters you want to search for are entered into the Key Word list using their hexadecimal equivalents. Each character must be preceded with a back slash (\). This distinguishes the character from a regular character. You can specify several characters in a row, but each character must be preceded by a back slash. You can also intermingle the binary characters with regular characters. For example, the following are valid entries in the Key Word list:

   - `\ac\80\fe`
   - `\ff\00\fb\40secrets`
   - `password\df\01\04`

   Valid hexadecimal characters are allowed immediately following a back slash. To use the back slash character as part of a key word entry, you must type a double back-slash (\\).

   **Note:** The exception is `\0a` (the new line character). The filter will not detect a key word that contains this character unless it is the first character in the key word entry or unless the character is preceded by `\0d` (the line feed) character (e.g., `\0d\0a`).
2 If you want to require that there be white space directly in front of and/or after a key word, select the **Require whitespace immediately before phrase** and/or **Require whitespace immediately after phrase** check boxes. This prevents the filter from misidentifying character strings that innocently appear as part of another word.

For example, if you require whitespace before and after the key word “for,” words like “forest,” “formula,” “information,” and “uniform” will be allowed to pass through the filter, while the word “for” would not. If you do not require whitespace before and after the key word “for,” the “for” string within the word would match the filter and cause the message to be rejected (if the specified number of matches are found).

3 To add the new or modified key word, click **OK**.
Configuring the Mail (Sendmail): MIME/Virus/Spyware tab

Use the MIME/Virus/Spyware tab to configure MIME, virus, and spyware filtering services. The tab contains a rule table that displays any MIME/Virus/Spyware filtering rules that have been created. It also contains various virus/spyware scanning and handling configuration options.

**Important:** You must license and configure additional services before the MIME/Virus/Spyware filter rules you create will scan mail messages. See “Configuring virus scanning services” on page 251.

To configure MIME/Virus/Spyware properties for an Application Defense, verify that the Control tab’s **MIME/Virus/Spyware** check box is selected and then follow the steps below.

**Security Alert:** If you want to perform virus and spyware scanning, you must create the appropriate MIME rules with **Virus/Spyware Scan** selected in the **Action** field. Rules that are configured only to allow or deny traffic based on rule criteria will not perform virus and spyware scanning. (See step 1 for information on configuring MIME/Virus/Spyware filter rules.)
1 Configure the appropriate MIME/Virus/Spyware filter rules in the **MIME/Virus/Spyware Filter Rules** table, as follows:

- **Create a new filter rule** — To create a new filter rule, click **New** and see “About the MIME Rule Edit window” on page 177.
- **Modify an existing filter rule** — To modify an existing filter rule, select the rule you want to modify, and click **Modify**. See “About the MIME Rule Edit window” on page 177. (If you are modifying the default MIME filtering rule, see “Configuring the Default filtering rule action” on page 179.)
- **Delete a filter rule** — To delete an existing filter rule, select the rule you want to delete and click **Delete**. You will be prompted to confirm your decision.

2 Determine how infected files will be handled by selecting one of the following options:

- **Discard Infected Files** — Select this option to discard infected files.
- **Repair Infected Files** — Select this option to remove the virus from the file and then continue processing the file.

3 To reject all files in the event that scanning is not available, select the **Reject All Files If Scanning Is Unavailable** check box. If you select this option, files will either be discarded or returned to sender as specified by the **Rejected Mail Handling** option selected on the Mail (Sendmail) Control tab. (Scanning might be unavailable due to out-of-date virus data, an expired license, or a configuration error.)

4 In the **Scan File Size Limit (KB)**, specify the maximum file size that will be allowed (in KB). If a file exceeds the size specified in this field, scanning will not take place and the file will be denied.

5 Establish how denied attachments are handled:

- **Select Full Scan of Entire Mail Message** if you want to perform scanning on the entire mail message (that is, the message with all of its MIME types is scanned as a single entity). A mail message is scanned only if one or more of its extensions match the MIME type/subtype settings on a filter rule with Virus/Spyware Scan selected.
- **Select Discard mail with denied attachments** if you want to discard mail once a MIME/Virus/Spyware filter rule denies its attachment(s). If you select this option, files will either be discarded silently (sender is not notified) or returned to sender, as specified by the **Rejected Mail Handling** option selected on the Mail (Sendmail) Control tab.
  - If **Discard mail with denied attachments** is selected, the entire message is discarded if it contains a denied attachment.
  - If **Discard mail with denied attachments** is not selected, the message is sent on without the denied attachment.
About the MIME Rule Edit window

Use this window to add or modify MIME/Virus/Spyware filtering rules.

• Rules that are configured with an allow or deny action will allow or deny traffic based on the rule criteria that is defined for those rules. Allow and deny rules do not perform virus scanning. To perform virus scanning for traffic that matches a rule before it is allowed, you must specify Virus/Spyware Scan in the rule’s Action field.

• Rules that specify both a MIME type/subtype and file extensions will allow or deny any traffic that matches either the MIME Type or a File Extension type. That is, the traffic does not need to match both criteria to match the rule.

Figure 74: Mime Rule Edit window
To add or modify MIME/Virus/Spyware filtering rules:

1. In the **MIME Type** drop-down list, select the MIME type for which you want to filter. If you select the asterisk (*) option, the filter rule will ignore this field when determining a match.

2. In the **MIME Subtype** drop-down list, select a subtype for the MIME type that you selected in the previous step (the available options will vary depending on the MIME type you selected). If you select the asterisk (*) option, the filter rule will ignore this field when determining a match.

3. In the **File Extensions** area, specify the type of file extensions that you want to filter:
   - **Ignore Extensions (*)** — Select this option to ignore extensions when determining a match.
   - **Archive Extensions** — Select this option to specify basic archive extensions (such as .tar, .zip, etc.) for the specified MIME types/subtype.
   - **Standard Extensions** — Select this option to specify the standard file extensions associated with the selected MIME type/subtype. For example, if you select text in the **MIME Type** field, and HTML in the **MIME Subtype** field, the .htm and .html file extensions will appear in the standard list.
   - **Custom** — Select this option to create a custom list of file extensions for the selected MIME type/subtype.
     - To add a file extension to the list, click **New** and type the extension (without the leading period) that you want to add.
     - To delete a file extension, select the extension you want to delete and click **Delete**.
     - You can use the **Reset** button to clear all extensions from the list, or to select a different file extension list (Archive or Standard).

4. In the **Action** area, select one of the following options:
   - **Allow** — Select this option if you want to explicitly allow the file extensions that you specified in the previous steps. (Virus scanning will not be performed.)
   - **Deny** — Select this option if you want to explicitly deny the file extensions that you specified in the previous steps. (Virus scanning will not be performed.)
   - **Virus/Spyware Scan** — Select this option if you want to perform virus scanning on the file extensions that you specified in the previous steps. If no viruses are detected, the file will be allowed through the system.
Configuring the Default filtering rule action

The Default filter rule is a catch-all rule designed to occupy the last position in your rule table.

To modify the default action for the default MIME filtering rule:

1. Select the default rule in the table and click **Modify**. The MIME Default Action window appears.

2. Select the appropriate action for this rule and then click **OK**.
   - **Allow** — The default rule is initially configured to *allow* all data that does not match other filter rules. If you leave the default rule as an allow rule, you must create filter rules that require virus scanning or explicitly deny any MIME types that you do not want to allow, and place them in front of the default allow rule.
   - **Deny** — If you prefer the default rule to *deny* all data that did not match a filter rule, you must create the appropriate virus scan and allow rules and place them in front of the default deny rule.
   - **Virus/Spyware Scan** — If you want to perform virus and spyware scanning for traffic that does not match any allow or deny filter rules you create, select this option. You will then need to create the appropriate allow and deny rules that will not require scanning.
Creating Mail (SMTP proxy) Defenses

The Mail (SMTP proxy) Application Defense allows you to filter mail using the SMTP proxy based on destination address and determine if source routing is supported. It also allows you to limit the length of replies received from mail servers.

To configure Mail (SMTP proxy) Application Defenses, select **Policy > Application Defenses > Defenses > Mail (SMTP proxy).**

**Configuring the Mail (SMTP proxy): Enforcements tab**

Use the Mail (SMTP proxy) Enforcements tab to enable destination-based mail filtering and to limit the length of replies received from mail servers.

To configure the Enforcements tab:

1. Select **Enforce SMTP Command Filtering** to configure the Command tab, which sets the list of the allowed mail commands.

2. If you enabled SMTP command filtering, select **Enforce Destination Address Filtering** to configure the Destination Address tab, which sets the filtering parameters.

3. To filter replies from mail servers, select one of these two options:
   - **Allow any size of server replies** — Select this option if you do not want a limit enforced.
   - **Enforce limit on server reply length** — Select this option to put a limit on the length of messages received from mail servers. A message is rejected if it is greater than the specified character limit. The default is 256 characters. Valid values are 3–1024.
Configuring the Mail (SMTP proxy): Commands tab

Use the Commands tab to specify which set of commands are allowed with a mail message.

Select from the following options:

**Note:** If you allow starttls, xexch50, xexps, or xlink2state and a session includes one of those commands, the Sidewinder appliance will disallow any further SMTP command filtering for the rest of that session.

- **Basic** — Select this option to allow the commands typically expected when sending mail to a generic mail server.
- **Exchange** — Select this option to allow the commands typically expected when sending mail to a Microsoft Exchange Server.
- **Sendmail** — Select this option to allow the commands typically expected when sending mail to a sendmail server.
- **Custom** — Select this option to create a customized set of allowed commands. If you selected Basic, Exchange, or Sendmail and alter the commands set, the Admin Console will automatically change your selection to Custom.
Configuring the Mail (SMTP proxy): Destination Address tab

Use the Destination Address tab to filter mail based on destination address and allow or deny source routing.

You can configure the following options:

- **Allow Source Routing** — Select this option to forward mail that includes source routing information in the \texttt{RCPT TO} command.

  \textit{Note: Most mail does not contain source routing information.}

- **Allow mail to any destination** — Select this option to allow mail to any destination.

  However, if Allow Source Routing is \textit{not enabled}, any \texttt{RCPT TO} command that contains source routing will be rejected. \texttt{RCPT TO} commands without source routing will be forwarded.

- **Only allow mail to defined destinations** — Select this option to specify the domains, IP address, and IP ranges to which the appliance will forward mail. The Sidewinder appliance allows mail based on the contents of its \texttt{RCPT TO} field; if the domain name portion of the \texttt{rcpt to} field matches a character string in the domain address list, the mail is allowed to pass.

  To create or change a definition, click \textbf{New} or \textbf{Modify}. To delete a definition, select the definition and click \textbf{Delete}. 

Figure 77: Mail (SMTP proxy): Destination Address tab
About the Allowed SMTP Destination window

Use this window to allow a new mail destination or modify an existing mail destination.

Figure 78: Destination Address: Allowed SMTP Destination window

Match the entry to the destination’s expected format in the `rcpt to:` field. Identify an allowed SMTP destination by doing one of the following:

- **Specify a Fully Qualified Domain Name** — Select this option to specify a fully qualified domain name (FQDN). In the Domain field, enter a FQDN, such as `example.com`. Check **Include Subdomains** to include the specified FQDN’s subdomains.

  **Tip:** This is the most reliable option, as most destinations in the RCPT TO: field are formatted as the domain name.

- **Specify an IP Address** — Select this option to specify a single IP address. In the **IP Address** field, enter the destination as a valid IP address.

- **Specify an IP Range** — Select this option to specify an address range. In the **Beginning of IP Address Range** and **End of IP Address Range** fields, specify the range of addresses that are allowed.
Creating Citrix Application Defenses

Use a Citrix Application Defense to configure advanced ICA proxy parameters.

To configure Citrix Application Defenses, select Policy > Application Defenses > Defenses > Citrix.

Configuring the Citrix: Enforcements tab

Use the Enforcements tab to enable or disable Citrix filtering. The Citrix Filters check box must be selected in order to select and enforce values in the Citrix Filters tab.

To disable Citrix filtering, clear the Citrix Filters check box.

Figure 79: Citrix: Enforcements tab
Configuring the Citrix: Filters tab

Use the Citrix Filters tab to configure filtering properties for Citrix.

To configure filters in Citrix, select the items that you want to deny. Each entry in the list represents a type of application or communication channel supported by Citrix. A check box will appear in front of types that will be denied. Clear the check boxes for the items you want to allow in Citrix.

To deny all of the types listed, click Select All. To allow everything (no filter restrictions), click Deselect All.
Creating FTP Application Defenses

Use an FTP Application Defense to configure FTP permissions and the scanning of FTP files.

To configure FTP Application Defenses, select **Policy > Application Defenses > Defenses > FTP.**

**Configuring the FTP: Enforcements tab**

To enable or disable FTP feature enforcement tabs, you must first select the appropriate check box in the Enforcements tab. When you select the check box for a feature, that tab becomes enabled.

![Figure 81: FTP: Enforcements tab](image)

The following tabs can be enabled:

- **Enforce Command Filtering** — Use the FTP Command Filter tab to specify the categories of FTP commands that you want to allow your users to issue.

- **Enforce Virus/Spyware Scanning** — Use the Virus/Spyware tab to set the filtering parameters, such as infected file handling, which commands to scan, and which extensions to allow or deny.
Configuring the FTP: Command Filter tab

Use this tab to specify the categories of FTP commands that you want to allow your users to issue. The available FTP commands, as well as a description of each, are included in the **Allowed FTP Command Categories** area. For example, selecting *GET* allows the FTP commands necessary to download files from a server.

**Figure 82: FTP: Command Filter**

Select one of the following options:

- **None** — Select this option if you do not want to allow any FTP commands. (None of the check boxes will be selected.)
- **All** — Select this option if you want to allow all of the categories of FTP commands that are displayed. (All of the check boxes will be selected.)
- **Custom** — Select this option if you want to allow only certain FTP commands. To select the categories of FTP commands that will be allowed, click the appropriate check box. A check mark appears in front of commands that are allowed.

*Note:* If you select *None* or *All* and then make modifications to the commands, the **Custom** option will automatically become selected.
Configuring the FTP: Virus/Spyware tab

Use this tab to configure virus and spyware scanning services. The tab contains a rule table that displays any virus and spyware filtering rules that have been created. The tab also contains various virus and spyware scanning and handling configuration options.

![Figure 83: FTP: Virus/Spyware tab](image)

**Important:** You must license and configure scanning services before the Virus/Spyware filter rules you create will scan FTP traffic. See “Configuring virus scanning services” on page 251.

To configure the Virus/Spyware tab:

1. Configure the appropriate virus and spyware filter rules in the **Virus/Spyware Filter Rules** table, as follows:
   - **Create a new filter rule** — To create a new filter rule, click **New**. See “Configuring Virus/Spyware filtering rules” on page 206.
   - **Modify an existing filter rule** — To modify an existing filter rule, select the rule you want to modify, and click **Modify**. See “Configuring Virus/Spyware filtering rules” on page 206. (If you are modifying the default filtering rule, see “Configuring the Default filtering rule action” on page 208.)
   - **Delete a filter rule** — To delete an existing filter rule, select the rule you want to delete and click **Delete**.
2 Determine how infected files will be handled in the **Infected File Handling** area as follows:
   - To discard infected files, select **Discard Infected Files**.
   - To remove the virus or spyware from the file and then continue processing the file, select **Repair Infected Files**. If the virus or spyware cannot be removed, the file will be discarded.

3 To reject all files in the event that scanning is not available, select the **Reject All Files If Scanning Is Unavailable** check box. If you select this option, the FTP proxy will not pass any files through the appliance until scanning is available again. (Scanning might be unavailable due to out-of-date virus data, an expired license, or a configuration error.)

4 Determine which commands to scan by selecting one of the following options:
   - **Uploads (PUT)** — Scan all files going to the FTP server.
   - **Downloads (GET)** — Scan all files coming from the FTP server.
   - **Uploads and Downloads (PUT, GET)** — Scan all files going to (put) and coming from (get) the FTP server.
Configuring Virus/Spyware filtering rules

Use this window to add or modify virus/spyware filtering rules.

**Important:** Rules that are configured with an allow or deny action will allow or deny traffic based on the rule criteria that is defined for those rules. Allow and deny rules do not perform virus and spyware scanning. To perform virus and spyware scanning for traffic that matches a rule before it is allowed, you must specify **Virus/Spyware Scan** in the rule’s **Action field**.

By default, a single *allow* rule is contained in the filter rule table. If you choose to leave the default allow rule as the last rule in your table (that is, all traffic that isn’t explicitly denied will be allowed), you will need to configure the appropriate virus/spyware scan and/or *deny* rules and place them in front of the default allow rule. If you configure the default rule action to deny (that is, all traffic that is not explicitly allowed will be denied) you will need to configure the appropriate virus/spyware scan and/or allow rules and place them in front of the default deny rule.
To create Virus/Spyware filter rules:

1. In the **Action** area, select one of the following options:
   - **Allow** — Select this option if you want to explicitly allow the file extensions that you will specify in the next step. (Virus and spyware scanning will not be performed.)
   - **Deny** — Select this option if you want to explicitly deny the file extensions that you will specify in the next step. (Virus and spyware scanning will not be performed.)
   - **Virus/Spyware Scan** — Select this option if you want to perform virus and spyware scanning on the file extensions that you will specify in the next step. If no viruses or spyware are detected, the file will be allowed through the system.

2. In the **File Extensions** area, specify the type of file extensions that you want to filter:
   - **Perform action on all file extensions** — Select this option to perform the action specified in step 1 on all file extensions.
   - **Choose from predefined categories** — Select this option to perform the action specified in step 1 on file extensions associated with a particular category, such as image, audio, video, etc.
     To choose the file extension, select the appropriate category from the Category drop-down list. Check the desired extensions.
   - **Custom List** — Select this option to create a custom list of file extensions.
     - To add a file extension to the list, click **New** and type the extension (*without* the leading period) that you want to add. The file extension is added to the **Custom** file extension list.
     - To delete a file extension, select the extension you want to delete and click **Delete**.
     - You can use the **Clear** button to clear all extensions from the list.

3. Click **OK** to save the rule.
Chapter 7: Application Defenses
Creating FTP Application Defenses

Configuring the Default filtering rule action

Use this window to modify the default action for the default virus/spyware filtering rule. The default filter rule is a catch-all rule designed to occupy the last position in your rule table.

Figure 85: FTP: MIME
Default Action window

To configure the MIME default action:

1 Select the default rule in the table and click Modify. The Default Action window appears.
2 Select the appropriate action for this rule and then click OK.
   • Allow — The default rule is initially configured to allow all data that does not match other filter rules. If you leave the default rule as an allow rule, you must create filter rules that require virus scanning or explicitly deny any extensions that you do not want to allow, and place them in front of the default allow rule.
   • Deny — If you prefer the default rule to deny all data that did not match a filter rule, you must create the appropriate virus scan and allow rules and place them in front of the default deny rule.
   • Virus/Spyware Scan — If you want to perform virus and spyware scanning for traffic that does not match any allow or deny filter rules you create, select this option. You will then need to create the appropriate allow and deny rules that will not require scanning.
IIOP (Internet Inter-ORB Protocol) is a protocol that makes it possible for distributed programs written in different programming languages to communicate over the Internet.

To configure IIOP Application Defenses, select Policy Configuration > Application Defenses > Defenses > IIOP.

### Configuring the IIOP: Filter tab

Use this tab to configure filtering properties for the Internet Inter-ORB Protocol (IIOP) proxy.

![IIOP Filter tab](Image)

To configure the Filter tab:

- **Allow Bi-directional GIOP** — Select this option to enable support for bi-directional 1.2 GIOP (General Inter-ORB Protocol).

- **Validate Content Format** — Select this option to filter the message encapsulated in the GIOP PDU (protocol data unit), and verify that the header content, message direction, and message length are valid for the GIOP message type identified in the GIOP header.

  **Note:** The data in the GIOP header portion of the PDU is always validated.

- **Maximum message size (PDU)** — Enter the largest message allowed through the proxy. The default is 72000.
Creating T.120 Application Defenses

T.120 is a standard for realtime data conferencing. The T.120 Application Defense allows you to use T.120 applications such as Microsoft’s NetMeeting application.

To configure T120 Application Defenses, select Policy > Application Defenses > Defenses > T120.

Configuring the T.120: General tab

Use this tab to enable the T.120 filter, which is commonly used to allow Microsoft’s NetMeeting. You cannot configure the T.120 properties unless you have selected the check box.
Configuring the T.120: Filter tab

Use this tab to specify which T.120 services you will allow your users to access. One of the more common T.120 applications is Microsoft’s Netmeeting.

You can select from the following options:

- Whiteboard (T.126)
- File Transfer (T.127)
- Base Application Sharing (T.128)
- Legacy Application Sharing (T.128)
- Chat (Microsoft specific)
Creating H.323 Application Defenses

H.323 is a standard that provides support for audio and video conferencing across a shared medium such as the Internet.

To configure H.323 Application Defenses, select Policy > Application Defenses > Defenses > H.323.

Configuring the H.323: General tab

Use this tab to enable the H.323 Filter.

1. To enable H.323 configuration, select the Enforce Permission Checking for H.323 check box. You cannot configure the H.323 properties unless you have selected the check box.

2. Enter a maximum call duration in seconds. The default is 86400 seconds.
Configuring the H.323: Filter tab

Use this tab to select H.323 codecs you will allow your users to access.

You can select from the following options:

- **Required** — Select this option to allow only the codecs required by H.323 for compliance.
- **Required + Low Bandwidth Audio** — Select this option to allow the required H.323 codecs as well as low bandwidth options.
- **Required + All Audio** — Select this option to allow all H.323 codecs except the codecs that allow video.
- **Required + All Audio + Video** — Select this option to allow all available H.323 codecs.
- **Custom** — Select this option to specify which codecs you want to allow. To allow a codec, select the appropriate check box. A check mark appears in the corresponding check box when a codec is allowed.
- **Select All** — Click this button to select all of the H.323 codecs (all codecs will be selected).
- **Deselect All** — Click this button to clear all of the H.323 codecs.

*Note:* If you select an option other than **Custom** and then make modifications to the selected codecs, the **Custom** option will automatically become selected.
The following list provide an example of codecs commonly used by Microsoft’s NetMeeting:

- **G.711** — The G.711 codec options can transmit audio at 48, 56, and 64 kB per second (kBps). Select this codec for audio that is being passed using high speed connections.

- **G.723** — The G.723 codec options determine which format and algorithm will be used for sending and receiving voice communications over a network. This codec transmits audio at 5.3 and 6.3 kBps, which will reduce bandwidth usage.

- **H.261** — The H.261 codec will transmit video images at 64 kBps (VHS quality). Select this codec for video that is being passed using high speed connections.

- **H.263** — The H.263 codec determines which format and algorithm will be used to send and receive video images over a network. This codec supports common interchange format (CIF), quarter common interchange format (QCIF), and sub-quarter common interchange format (SQCIF) picture formats. It is also a good match for Internet transmission over low-bit-rate connections (for example, a 28.8 kBps modem).
Creating Oracle Application Defenses

Use an Oracle Application Defense to configure continuous session monitoring to prevent spoofing and tunneling attacks while sessions are in progress for the SQL proxy.

To configure Oracle Application Defenses, select **Policy > Application Defenses > Defenses > Oracle.**

### Configuring the Oracle: Enforcements tab

Use this tab to enable or disable Oracle service name checking. Service name checking allows you to restrict access to the SQL server by specifying which service names will be explicitly allowed. If service name checking is enabled, only sessions that match a service name specified in the Service Name (SID) tab will be allowed.

You cannot configure service name checking on the Service Name (SID) tab unless the **Enforce Service Name Checking** check box is selected. When this check box is selected, the values you configure in the Service Name (SID) tab will be enforced.

To disable service name checking, clear the **Enforce Service Name Checking** check box.
## Configuring the Oracle: Service Name (SID) tab

Use this tab to configure which service names will be allowed access to the SQL server. If you do not specify any service names, service names will not be used in determining whether a session is allowed or denied.

### You can perform the following actions:

- To configure a service name, click **New**. In the **Service Name (SID)** field, type the service name you want to add. The service name you enter must be an exact match (including capitalization) of the full service name that is in the Oracle tnsnames.ora file.

- To modify a service name, select the service name you want to modify, and click **Modify**. In the **Service Name (SID)** field, modify the service name.

- To delete a service name, select the appropriate service name and click **Delete**.

## Creating MS SQL Application Defenses

The MS SQL Application Defense is not currently available. It is reserved for future features.
Creating SOCKS Application Defenses

Use the SOCKS Application Defense to configure advanced properties for the SOCKS proxy.

To configure SOCKS Application Defenses, select Policy > Application Defenses > Defenses > SOCKS.

Configuring the SOCKS: SOCKS 5 Filter tab

Use this tab to configure the type of SOCKS traffic that will be allowed when using the SOCKS5 proxy.

The following options are available:

- **Allow TCP SOCKS traffic** — Select this option to allow TCP traffic.
- **Allow UDP SOCKS traffic** — Select this option to allow UDP traffic.
- **Allow Both** — Select this option to allow both TCP and UDP traffic.
- **Enforce SOCKS 4 Filtering** — Select this option if you want to support SOCKS at version 4. (If this check box is not selected, you will not be able to pass traffic using SOCKS 4.)
Configuring the SOCKS: Connection tab

Use this tab to configure which ports will be open for the SOCKS proxy.

To define allowable destination ports for non-transparent proxies, click **New**, then specify a port, a port range, or select from pre-defined ports on the Edit a Port window.

To modify a destination port, select it in the list and click **Modify** and make your changes in the pop-up window.

To delete a destination port, select it in the list and click **Delete**.

*Note:* This table identifies which ports the SOCKS proxy is allowed to send traffic to. If no ports are identified, the proxy connection will be denied.
Creating SNMP Application Defenses

Use the SNMP Application Defense to configure advanced properties for the SNMP proxy.

To configure SNMP Application Defenses, select Policy > Application Defenses > Defenses > SNMP.

Configuring the SNMP: Filter tab

Use this tab to specify the SNMP version you want to configure.

The options that you can configure within the subsequent SNMP tabs will vary depending on which option you select. The following options are available:

- **Allow SNMP v1 filtering** — Select this option to allow SNMP v1 traffic and configure object ID (OID) filtering. For information on configuring OID filtering for SNMP v1 traffic, see “Configuring the SNMP: v1 tab” on page 220.

- **Allow SNMP v2c traffic** — Select this option to allow SNMP v2c traffic. OID filtering is not available for SNMP v2c traffic.

- **Allow SNMP v1 and v2c traffic** — Select this option to allow SNMP v1 and v2c traffic. OID filtering is not available when both SNMP v1 and v2c are allowed.

To set a maximum message size, type the maximum protocol data unit (PDU) allowed for a message in the **Maximum message size (PDU)** field. The default is 535.
Configuring the SNMP: v1 tab

Use this tab to configure Object ID (OID) filtering for SNMP v1 traffic.

![SNMP: SNMP v1 tab](image)

**Figure 96: SNMP: SNMP v1 tab**

**Note:** Filtering is not available for SNMP v2c. If you selected **Allow SNMP v2c Traffic** or **Allow SNMP v1 and v2c Traffic** on the SNMP Filter tab, you cannot configure any options on this tab.

To configure the SNMP v1 tab:

1. In the **Options** area, determine the types of requests and events that the SNMP proxy will filter:
   - **Allow Read Requests** — Select this option to allow the **Get** and **Get Next** requests. (If you select SNMP v2c, this is automatically allowed.)
   - **Allow Write Requests** — Select this option to allow the **Set** request. (If you select SNMP v2c, this is automatically allowed.)
   - **Allow Notify Events** — Select this option to allow v1 traps. (If you select SNMP v2c, this is automatically allowed.)

   **Note:** Additional SNMP requests are not supported in SNMP v1.

2. Select the **Enable OIDs Filtering** check box to configure object IDs (OIDs) for the SNMP proxy. OIDs are a unique, numeric representation of a device within the SNMP network.
3 In the Actions field, determine whether the list of OIDs that you define will be allowed or denied:
   - Allow — Select this option to allow only the OIDs that you specify in the table. All other OIDs will be denied.
   - Deny — Select this option to deny only the OIDs that you specify in the table. All other OIDs will be allowed.

4 To manage OIDs:
   - To add an OID to the table, click New. See “Configuring the SNMP v1: OID Editing window” on page 221.
   - To modify an existing OID, select that ID and click Modify. See “Configuring the SNMP v1: OID Editing window” on page 221.
   - To delete an existing OID, select that ID and click Delete.

**Configuring the SNMP v1: OID Editing window**

Use this window to add a new object ID (OID). You can select from the list of standard OIDs, or you can create your own OID using the custom option.

![SNMP v1: OID Editing window](image)
To add a new object ID:

1. In the **OID Options** area, select whether the OID will be **Standard** (pre-defined) or **Custom** (you determine and enter the OID manually).
   - If you select **Standard**, select the appropriate OID from the **Standard OIDs** drop-down list.
   - If you select **Custom**, type the OID number in the **Customized OID** field using the standard OID structure. The numbering scheme for each object is determined by the object’s management information base (MIB) location, as shown in the figure below.

For example, the object ID for the SCC node in the private enterprise portion of the network would be `.1.3.6.1.4.1.1573`.

**Note:** The object ID will always begin with the pattern `.1.3.6.1`. For assistance on obtaining object IDs, visit the Internet assigned numbers authority web site at [www.iana.org/assignments/enterprise-numbers](http://www.iana.org/assignments/enterprise-numbers) or contact the appropriate vendor.

**Figure 98:** Example of OID numbering scheme

2. Click **Add** to add the OID to the table. Repeat these steps for each OID you want to add or modify.

3. Click **Close** to return to the SNMP v1 tab.
Creating SIP Application Defenses

Use the SIP Application Defense to configure media filtering, call duration, and peer types for the Session Initiation Protocol (SIP) proxy.

SIP is used to locate a user agent and negotiate a multimedia session between user agents. A user agent is a device that terminates one side of a call (for example, the calling or answering phone).

To configure SIP Application Defenses, select Policy > Application Defenses > Defenses > SIP.

Configuring the SIP: General tab

Use this tab to enable media filtering, to set the call duration, and to configure the types of peers that may participate in a SIP call.

![SIP: General tab](image)
You can perform the following actions:

- **Enable media filtering** — Select Enforce Media Filtering to enable SIP filtering. Use the Media Filters tab to select the desired filters.
- **Set the duration of calls** — Use the Maximum Call Duration field to enter the maximum number of seconds a call can last.
- **Configure peer types** — Select whether SIP calls may be negotiated by intermediaries.
  - Select **The SIP peers must be user agents** to require that all calls be negotiated by the SIP user agents of a call. The source and destination of each SIP message must be the SIP user agents (for example, SIP phones). Some SIP routers and gateways can masquerade as SIP user agents.
  - Select **The SIP peers can be routers** to allow SIP devices to negotiate calls on behalf of other SIP user agents. In this case, the source and destination of SIP messages processed by the proxy may differ from the SIP user agents that are participating in the call.

**Configuring the SIP: Media Filters tab**

Use this tab to configure media filters for an SIP session.

- Select **Audio** to allow audio streams via SIP.
- Select **Video** to allow video streams via SIP.

Use the **Select All** and **Deselect All** buttons to select or clear both options at once.
Creating Packet Filter Application Defenses

Use the Packet Filter Application Defense to configure advanced properties for rules that use filter agents.

To use a Packet Filter Application Defense, you need to create a service that uses a filter agent, which is then applied to a rule. Services can be created using the following filter agents:

- **Generic Filter** — Used for creating services for the TCP and UDP protocols.
- **ICMP Filter** — Used for creating services for the ICMP protocol.
- **Other Protocol Filter** — Used for creating services for a number of protocols, such as GRE and AH.

**Security Alert:** Secure Computing strongly recommends that you use a filter agent only for non-TCP/UDP protocols, such as PUP, GRE, AH, etc. Using a filter agent for a TCP/UDP protocol will, in most cases, severely degrade the effectiveness of the Sidewinder appliance and will expose your network to security hazards.

For more information about creating services with filter agents, see “Creating and modifying services” on page 147.

To configure Packet Filter Application Defenses, select **Policy > Application Defenses > Defenses > Packet Filter**.
Configuring the Packet Filter: General tab

Use this tab to specify the request rate and the audit parameters.

You can perform the following actions:

- **Limit the number of requests that will be allowed per second in either direction** — Select **Limit request rate to** and enter the number of packets that you want allowed per second.

- **Specify how frequently the Sidewinder appliance will generate audit records for deny rules** — Enter the number of denied requests and the time frame in the appropriate fields of the **Audit the first x denied requests every y seconds** area. Audit will be created for the first x occurrences in every y seconds. An additional audit event will be generated to record how many other audit events were suppressed.

  For example, the audit is limited to generating an audit event for the first 1 occurrences for every 1 seconds. If the appliance stopped 100 netprobes in 1 second, one record would be generated for the first denial, and then another audit record would be generated stating that 99 occurrences were suppressed.

- **Specify the number of packets allowed by a rule before an informational audit is generated** — Select **Provide informational audits every [ ] requests**, and enter an appropriate number of requests. To limit auditing for this Packet Filter rule to only connection or session information, set the value to zero (0).
Configuring the Packet Filter: Advanced tab

Use this tab to select the response types you want to allow for a rule.

In the **Allowed control and error responses** area, select the response types that you want to allow for a rule. These selections control the ICMP messages generated by the rule’s TCP/UDP traffic.
Application Defense groups are used in rules to specify advanced properties for service groups.

- When you create an Application Defense group, you select a single Application Defense from each category (for example, HTTP, HTTPS, FTP, etc.) to populate that Application Defense group.

- You set one Application Defense group as the default. The default group is used in all new rules using an Application Defense, unless you select a different Application Defense group in the Rules window.

- Only the Application Defenses that apply to that rule’s services will be implemented in the rule.

*Note:* For more information on how Application Defense groups are used in a rule, see Chapter 5, “Rules,” on page 81.

Configuring the Application Defense Groups window

Use the Application Defense Groups window to create and manage Application Defense groups.

**Figure 103: Application Defense Groups window**

- The upper pane lists all of the Application Defense groups that are currently configured. Each column shows which Application Defense is selected for the group.
- The lower pane lists each Application Defense category in the left table. When you select a category in the table, the available Application Defenses appear in the list on the right.
You can perform the following actions:

**To create a new Application Defense group:**

1. In the upper pane, click **New**. The New Groups Application Defense window appears.
2. Type a name for the group, then click **OK**. The group appears in the list in the upper pane.
3. In the lower pane, select an Application Defense for each category:
   a. In the left pane, select the appropriate Application Defense category. A list of available Application Defenses for that category appears in the right pane.
   b. In the right pane, select the Application Defense you want to associate with the selected category. The selected Application Defense appears in the Name column of the selected category.
   
   Perform this for each Application Defense category.
4. Save your changes. The selections in the Name column appear in the corresponding columns in the upper pane.

**To modify an Application Defense group:**

In the upper pane, select the appropriate Application Defense group. In the lower pane, make the desired changes for the Application Defense categories. (To make your changes in a pop-up window, select the Application Defense group and then click **Modify**.)

**To rename an Application Defense group:**

In the upper pane, select the appropriate Application Defense group. Click **Rename** and type a new name in the pop-up window.

**To delete an Application Defense group:**

In the upper pane, select the appropriate Application Defense group, then click **Delete**.

**To make a group the default Application Defense group:**

In the upper pane, select the appropriate Application Defense group, then click **Set Default**.

The default group is used in any rule using an Application Defense, unless you select a different Application Defense group in the Rules window.
To see which areas are using an Application Defense group:

In the upper pane, select the appropriate Application Defense group, then click *Usage*. A pop-up window appears listing the rule names that are currently using the selected group.

To duplicate an Application Defense group:

In the upper pane, select the appropriate Application Defense group, then click *Duplicate*. Type a name for the duplicated group in the pop-up window, then make the appropriate modifications to the duplicated Application Defense group.

To create or modify an Application Defense:

In the lower pane, select the appropriate Application Defense category. In the lower pane, click New or Modify and configure the Application Defense in the pop-up window.
Chapter 7: Application Defenses

Configuring Application Defense groups
CHAPTER 8

Content Inspection

In this chapter...

Configuring IPS inspection ........................................................... 234
Configuring virus scanning services ............................................. 251
Configuring TrustedSource for Sidewinder ................................. 257
Configuring spam filtering services ............................................. 261
Configuring SmartFilter for Sidewinder ..................................... 267
Configuring IPS inspection

The Sidewinder appliance’s Intrusion Prevention System (IPS) feature is a signature-based inspection tool that identifies attacks before they pass through the appliance. IPS plays an important role in protecting hosts and services that have known vulnerabilities and exploits, yet are required components of your organization.

Before the appliance will compare traffic to its IPS signatures, you must ensure the following conditions have been met:

- The IPS and IPS Signature features must be licensed. To verify that these features are licensed, select Maintenance > License, and click the Firewall tab. If you are not licensed for IPS and IPS Signature, contact your sales representative.
- The signature files are current. Select Policy > IPS and then click the Signature Updates tab. Secure Computing strongly recommends that you enable automated signature download and install.
- You must create the appropriate signature groups and response mappings. Select Policy > IPS and click the Signature Groups and Response Mapping tabs.
- The rules governing the traffic you want inspected must have the appropriate signature categories and response mappings selected.

The following sections explain how Sidewinder IPS inspection is designed, how it interacts with other Sidewinder attack protection tools, how it is used in rules, and how to configure its basic components and signature file download schedule.

- “Understanding signature-based IPS” on page 235
- “Adding IPS inspection to rules” on page 237
- “About signature file updates” on page 239
- “Using IPS with other Sidewinder attack protection tools” on page 240
- “Configuring a response mapping” on page 241
- “Configuring a signature group” on page 245
- “Configuring IPS signature file updates” on page 249
Understanding signature-based IPS

The Sidewinder appliance IPS inspection uses signatures to detect and prevent known network-based intrusion attacks, such as hacker-generated exploits. How the appliance responds to an attack is configurable; options range from allowing but auditing the attack to blackholing all traffic coming from the attacker.

IPS inspection is controlled on a per-rule basis. Each proxy, filter, or server rule that uses IPS inspection is assigned a signature group and a response mapping. The signature group is used to limit scanning to relevant signatures. The response mapping specifies the action to take when a packet or session is identified as an attack.

The foundation of IPS inspection is its signatures. The signatures are the data for recognizing attacks. Each signature has a category attribute, a threat level attribute, and a class type attribute.

The signature category is classified by the network service targeted for attack, and consists of a main category and a subcategory. One or more categories can be added to a signature group. For example, to create a signature group to add to an inbound rule for an Oracle server, create a group named Oracle that includes the categories DB:Oracle, Component:Encoder, and Component:Shellcode. The appliance also provides default signature groups based on common attack targets, such as the Database Servers group and the Internal Desktops group.

Within each category and response mapping, the signatures have a threat level attribute: IPS or IDS. This threat level indicates a relationship between confidence level and severity. Signatures classified as IPS are confirmed attacks that are also considered dangerous. Signatures classified as IDS either identify attacks that are considered minor, such as probe or discovery activity, or they are suspected attacks, meaning the signature may be likely to incorrectly identify legitimate traffic as an attack. The default signature groups and response mappings include both the IPS and IDS threat levels.

The class type identifies the attack’s intended purpose, such as Root Level Exploit or Discovery. Based on class type and threat level, you configure the response the appliance will take when an attack matches a signature. Options are to allow the packet or session, deny it, drop it, or blackhole it. These options generally include an IPS audit that records the action. In general, the response should correspond to the severity of the attack. Categories labeled IDS may generate some false positives or may be probing or discovery attacks. Therefore, attacks of this threat level should generally never be blackholed.
For example, to create a response mapping that protects against root level exploits against an Oracle server, create a mapping named Oracle and set Root Level Exploit type IDS to Allow and Root Level Exploit type IPS to Blackhole for 10,000 seconds. The process, illustrated in Figure 104, is as follows: An Oracle attack matches an Oracle proxy rule. That rule is configured for signature-based IPS inspection. The packet is compared to the signatures in the signature group and a match is found. The appliance then checks the rule’s response mapping for instructions on responding to the attack. If the identified attack matches a signature with a threat level of IDS, the connection is allowed through but generates an IPS audit event. If the identified attack matches a signature with a threat level of IPS, the connection is blackholed for 10,000 seconds, so all traffic from the source’s IP address is blackholed for that length of time.

**Figure 104:** IPS process flow

- Oracle attack
- Matches Oracle rule
  - Rule has IPS configured? yes → Checks response mapping
    - Allow no audit
      - Pass traffic
      - No IPS audit
    - Allow (IDS)
      - Pass traffic
      - Generate IPS audit
    - Deny
      - Deny traffic
      - Generate IPS audit
    - Drop
      - Drop traffic
      - Generate IPS audit
    - Drop no audit
      - Drop traffic
      - No IPS audit
    - Blackhole (IPS)
      - Drop all traffic from host IP address
      - Generate IPS audit
  - Rule has IPS configured? no → Process without further IPS inspection
  - Matches a signature in the signature group? yes → Check response mapping
    - No yes → Process without further IPS inspection
    - No no → Process without further IPS inspection

236
Adding IPS inspection to rules

As explained in the previous section, IPS inspection is controlled on a per-rule basis. Inspecting all traffic using IPS signatures can greatly reduce your appliance’s performance. Enabling IPS inspection only when needed allows you to focus your appliance’s resources on traffic that is most likely to contain attacks, such as HTTP traffic. Use signature groups, which limit scanning to relevant areas of the signature file database, to improve inspection efficiency.

**Note:** If your policy does call for extensive IPS inspection, you may be able to install a hardware accelerator to improve performance. This option is not available on low-end models. Contact your sales representative for more information.

When planning your security policy, determine what traffic and systems are likely to be targets for network-based attacks. IPS is most commonly used to inspect inbound connections, since attacks typically come from external, untrusted sources. If an internal server, such as a Web server on your DMZ, were to be compromised, scanning its outbound connections is useful for containing damage and preventing attacks from spreading to other systems. Enable IPS on the rules governing likely targets. Traffic that does not have IPS inspection enabled will not be inspected for network-based attacks.

**Tip:** If you want to blackhole an attack that is identified by the signature-based IPS when it first occurs, set that action in the response mapping. If you want to blackhole an attack only if it occurs multiple times, set that action in the IPS Attack Responses (Monitor > IPS Attack Responses).

The following figure is an example of a rule with IPS inspection enabled. When HTTP traffic destined for the vulnerable_web_server reaches the appliance, the appliance checks that traffic against signatures in the “Web Server Attacks” signature group. When the traffic’s pattern matches an attack, the appliance checks the “Exploit Protection” response mapping to see how it should respond to that attack’s associated class type.
For more information on enabling IPS inspection in rules, see Chapter 5, "Rules" on page 81.

**Figure 105:** A rule with IPS enabled

<table>
<thead>
<tr>
<th>General</th>
<th>Effective Times</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action: Allow ☑</td>
<td>□ Deny ☐  □ Drop ☐</td>
</tr>
<tr>
<td>Service: http (HTTP Proxy)</td>
<td>□ &lt;Any&gt; ☐</td>
</tr>
<tr>
<td>Audit: Standard (recommended)</td>
<td>□ &lt;Any&gt; ☐</td>
</tr>
<tr>
<td>Time period: &lt;Any&gt;</td>
<td>□ Start on: 10/29/2007 12:00 AM</td>
</tr>
<tr>
<td>□ Expire on: 10/29/2007 12:00 AM</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>Burb: external</td>
<td>Burb: internal</td>
</tr>
<tr>
<td>Endpoint: &lt;Any&gt;</td>
<td>Endpoint: Vulnerable web server (Host)</td>
</tr>
<tr>
<td>NAT: localhost (Host)</td>
<td>Redirect: &lt;None&gt;</td>
</tr>
<tr>
<td>□ Preserve source port</td>
<td>Redirect port:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Inspection</th>
<th>Response mapping: Exploit Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Defense: default (http)</td>
<td>□ Full ☐ None</td>
</tr>
<tr>
<td></td>
<td>All configured settings of the application defense are enforced.</td>
</tr>
<tr>
<td>IPS Signature group: Web Server Attacks</td>
<td>□ Full ☐ None</td>
</tr>
</tbody>
</table>

Searches signatures related to web server attacks. Checks this response mapping to see what it should do with the connection.
About signature file updates

Since new attacks are being identified all the time, it is important to update the signatures frequently. When new signatures are added to the appliance, they will go into effect based on how the existing signatures categories and response mappings are configured. Therefore, if a new signature comes in and, based on its category and class type, is associated with a signature group that is assigned to a rule, that signature will go into effect immediately. Any attack matching that signature will be handled based on the response mapping for the signature’s class type.

**Note:** Signatures with any risk of false positive are always given a threat level of IDS. Therefore, do not deny, drop, or blackhole traffic for class types with a threat level of IDS.
Using IPS with other Sidewinder attack protection tools

There are several different approaches to protecting your internal network. One approach is to prohibit any traffic from entering your network. While this solution is secure, it is also impractical. Another approach is to attempt to scan all incoming traffic for known attacks, viruses, etc., but this can slow down the appliance, and therefore your network connectivity.

The best solution is first use tools to minimize your network’s attack surface, and then use scanning to protect services that must be allowed. You can reduce your network’s attack surface by creating the minimum number of rules necessary to allow essential inbound traffic and limiting the source and destination endpoints to hosts or address ranges. In addition, Application Defenses can be used to further refine what traffic is allowed into your network by prohibiting unnecessary commands, header, protocol versions, and other parameters. Once your policy is sufficiently restrictive, use IPS and other signature-based services such as anti-virus and anti-spam to inspect traffic destined for vulnerable yet essential services.

For example, an administrator is running a web server that requires allowing inbound HTTP traffic. The administrator knows that the Content Length header and the Content Location header are often used in attacks. The Content Location header is not required by the web server, and therefore does not need to be allowed into the network. The administrator uses the HTTP Application Defense to deny that header. The Content Length header is required, so the administrator allows it but adds IPS inspection to the rule allowing that traffic to make sure known attacks using that header are blocked.

While a small attack surface and inspection tools are a strong defense, you should still use IPS Attack Responses to monitor attack activity. Even attacks that are not allowed through the appliance are noteworthy as they may be an attempt from a hacker who will later try a more sophisticated attack. IPS Attack Responses can send out alerts when your network is under attack. These alerts will notify you of situations that may require a configuration change to increase the security of your network or investigation into the reason for the attack. For information on monitoring attack audits, see Chapter 13, "IPS Attack and System Event Responses" on page 399.
Configuring a response mapping

A response mapping contains a list of class types, their threat level, and their response settings. Each class type refers to a set of known network-based attacks. Class types classified as IPS are confirmed attacks that are also considered dangerous. Class types classified as IDS are either suspected attacks or are considered less dangerous, such as probe or discovery activity. Once a response mapping is configured, it can then be selected on the Rules window to indicate how the appliance will respond when a related attack is detected.

Response mappings are configured on the Response Mapping tab. They can then be selected on the Rules window to indicate how the appliance will respond when an attack is detected.

To configure a response mapping, select Policy > IPS. The Response Mapping window appears.

Figure 106: The IPS Response Mapping tab

The upper pane contains the toolbar and the existing response mappings. When you select a mapping, its properties appear in the lower pane.
Figure 107: Response Mappings toolbar

Use the toolbar and table in the upper pane to perform the actions listed here:

Table 15: The Response Mappings toolbar

<table>
<thead>
<tr>
<th>Icon/Menu item</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td>Create a new response mapping by clicking <strong>New</strong>. The New Response Mapping window appears.</td>
</tr>
</tbody>
</table>
| Modify | Modify a response mapping:  
  • Select it and modify its properties in the lower pane.  
  • Double-click it and modify it in the new window.  
  • Select it, click **Modify**, and edit it in the new window.  
  *Note:* Read-only administrators can view a response mapping. |
| Delete | Delete a response mapping by selecting it and clicking **Delete**. |
| Duplicate | Create a copy of an existing response mapping by selecting the mapping, clicking **Duplicate**, and customizing the copy as needed. |
| Rename | Rename a response mapping by selecting it and clicking **Rename**. |
| Usage | View what rules currently use a response mapping by selecting a mapping and clicking **Usage**. |
| Find | Search for a specific element(s) in the list using the **Find** field. Type your search criteria, and signature groups with matching elements will appear in the list. Clear this field to see the full list again. |
When you click New, Modify, or Duplicate, the New/Modify Response Mapping window appears:

To configure a response mapping:

1. In the **Name** field, enter a name that identifies the purpose of the response mapping. For example, if you create two mappings to address different threat levels to your web servers, you would name one “web server high” and “web server low.”

   Valid values include alphanumeric characters, dashes (-), underscores (_), and spaces ( ). However, the first and last character of the name must be alphanumeric. The name cannot exceed 256 characters. You can rename the mapping later.

2. [Optional] In the **Description** field, enter any useful information about this mapping. For example, a mapping that allows but audits probe and discovery attacks would be named “Probe-Discovery audit only.”

3. In the **Class Types** area, identify the class types to which you want the appliance to respond by setting the responses to one of the following:
   - **Allow no audit** — Allows the traffic to pass and does not generate an IPS audit event. This is the default for all class types when creating a new response mapping.
   - **Allow** — Allows the traffic to pass and generates an IPS audit event. Use this setting for traffic that is an anomaly and appears suspicious but is not an identifiable attack.
   - **Drop** — Denies only those packets that are suspect while allowing trusted packets. The appliance will not alert the attacker that the connection was closed. This generates an IPS audit event.
• **Deny** — Similar to Drop except that this response sends a TCP reset informing the originating host the connection was deliberately closed. This generates an IPS audit event.

  **Caution:** Use this setting only when troubleshooting or when instructed by Technical Support. Sending a TCP reset or other connection-denied response could notify the attacker that the appliance has recognized the attack, prompting the attacker to switch to a new attack.

• **Deny no audit** — Similar to Deny except that this response does not generate an IPS audit event.

• **Blackhole** — Denies all traffic from the host originating the hostile traffic for a set period of time. This generates an IPS audit event. The appliance will not alert the attacker that the connection was closed. Use this setting when you are sure all traffic coming from an address is malicious.

  In the **Duration** field, enter the time in seconds that the traffic will be denied. Valid values are 1–100000 seconds.

  **Tip:** See the Dashboard for a current list of blackholed IP addresses.

4 Click **Add**.

5 Save your changes.

This response mapping is available for use in a rule.
Configuring a signature group

A signature group can contain one or more signature categories. A signature category is a category of signatures that all involve the same type of attack. The IPS engine provides the categories and may update them occasionally.

Signature categories are configured on the Signature Categories tab. They can then be selected on the Rules window to focus IPS inspection on relevant attacks.

To configure a signature group, select **Policy > IPS** and click **Signature Groups**. The Signature Groups window appears.

The upper pane contains the toolbar and the existing signature groups. When you select a signature group in the list, the properties of that group appear in the lower pane.
Use the toolbar and table in the upper pane to perform the actions listed here:

**Table 16:** The Signature Groups toolbar

<table>
<thead>
<tr>
<th>Icon/Menu item</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>New</strong></td>
<td>Create a new signature group by clicking <strong>New</strong>. The New Signature Group window appears.</td>
</tr>
<tr>
<td><strong>Modify</strong></td>
<td>Modify a signature group:</td>
</tr>
<tr>
<td></td>
<td>• Select it and modify its properties in the lower pane.</td>
</tr>
<tr>
<td></td>
<td>• Double-click it and modify it in the pop-up window.</td>
</tr>
<tr>
<td></td>
<td>• Select it, click <strong>Modify</strong>, and edit it in the new window. (Read-only administrators can click <strong>View</strong> to view a signature group.)</td>
</tr>
<tr>
<td><strong>Delete</strong></td>
<td>Delete a signature group by selecting it and clicking <strong>Delete</strong>.</td>
</tr>
<tr>
<td><strong>Duplicate</strong></td>
<td>Create a copy of an existing signature group by selecting the group, clicking <strong>Duplicate</strong>, and customizing the copy as needed.</td>
</tr>
<tr>
<td><strong>Rename</strong></td>
<td>Rename a signature group by selecting it and clicking <strong>Rename</strong>.</td>
</tr>
<tr>
<td><strong>Usage</strong></td>
<td>View what rules use a given signature group by selecting a group and clicking <strong>Usage</strong>.</td>
</tr>
<tr>
<td><strong>Find</strong></td>
<td>Search for a specific element(s) in the list using the <strong>Find</strong> field. Type your search criteria, and response mappings with matching elements will appear in the list. Clear this field to see the full list again.</td>
</tr>
</tbody>
</table>
When you click **New**, **Modify**, or **Duplicate**, the New/Modify Signature Group window appears:

![Signature Groups New/Modify window](image)

Use this window to create, modify, or duplicate a signature group.

To configure a signature group:

1. **In the Name field**, enter a name that describes the purpose of the signature group. For example, if you wanted a signature category that searches both HTTP and FTP attack signature files, you would name it `HTTP_FTP`.

   Valid values include alphanumeric characters, dashes (-), underscores (_), and spaces ( ). However, the first and last character of the name must be alphanumeric. The name cannot exceed 256 characters. You can rename the mapping later.

2. **[Optional] In the Description field**, enter any useful information about this group. For example, a signature category designed to inspect Oracle-related connections would be named `Oracle` and include the categories `DB:Oracle`, `Component:Encoder`, and `Component:Shellcode`
3 Configure the **Signatures** area:

   a In the **Use** column, select each category to include in signature group.

   b For each selected category, select IPS, IDS, or both:

      • Select **IPS** to identify attacks that are an exact match to a signature file.
      
      • Select **IDS** to identify attacks that are considered minor, such as probe or discovery activity, or suspected attacks, meaning the signature may have incorrectly identified legitimate traffic as an attack.

      Both options are selected by default.

4 Click **Add**.

5 Save your changes.

This signature group is now available for use in a rule.
Configuring IPS signature file updates

Use this tab to configure the IPS signature file update properties. The appliance can automatically download and install updates at intervals that you determine. You can also manually download and install updated signature files at any time.

**Important:** Secure Computing recommends downloading the latest signature files prior to enabling IPS inspection on any active rules.

![Figure 112: The IPS Signature Updates tab]

Use this window to configure the IPS signature file update properties.

**Note:** While most sites will use Secure Computing-provided IPS signature files, the appliance also supports using user-defined files. User-defined IPS signature files can only be created or updated using the command line interface. See Knowledge Base article #6600 at [www.securecomputing.com/supportkb.cfm](http://www.securecomputing.com/supportkb.cfm) for details.
To configure updates:

1. In the Source area, verify/modify the following fields:

   - **Download Site** — This is the site from which the package will be downloaded. The default site is `downloads.securecomputing.com`.

     *Caution:* Changing these defaults may prevent the appliance from obtaining updated signatures file, resulting in inadequate IPS protection.

     *Note:* If the download fails, troubleshoot the problem by verifying that the site name resolves to an IP address and is reachable from the Sidewinder appliance.

   - **Directory** — The path name on the download site that contains the update. The default directory is: `cgi-bin/sigupdate.py`

2. [Conditional] To configure automatic signature file updates, follow the sub-steps below. To manually download and install the signature files, skip to step 3.

   a. Select Enable Automated Signature Download and Install.

   b. In the **Frequency** field, specify how frequently you want to download and install updated signature files:

      - (Recommended) To download and install every hour, select **Hourly**.
      - To download and install every day, select **Daily**.
      - To download and install once a week, select **Weekly**. Also specify the day of the week on which you want downloads to occur.

   c. For all frequency options, in the **Time** field, specify the time of day you want the appliance to download and install the updates.

     *Note:* Downloading and installing updates has a minimal impact on your system. Traffic that is received while the download and installation are in process will be inspected using the current version. Once installation is complete, all traffic will be scanned using the updated information.

   d. If you want to receive e-mail notification when the updates are downloaded and installed, select the **Enable Email Notification** check box. If you select this option, you will also need to specify an e-mail address in the **Recipient** field.

3. [Conditional] To update the signature files manually, click **Download and Install Signatures Now**. A progress bar appears while the files are downloaded, then a message appears stating that the update is complete.

4. To view the current version of the signature file you are using, click **Show Installed Signatures File Version Number Now**. An Info window appears displaying the current installed version. When you are finished viewing the version, click **OK**.

5. Save your changes.

The IPS engine is now using the current signature files.
Configuring virus scanning services

The anti-virus service is a licensed add-on module that uses a Sidewinder-hosted virus scanner that allows you to configure rule-based MIME, virus, and spyware scanning. Use scanning services on HTTP and HTTPS traffic, FTP files, and mail messages. When using scanning services, you can specify the number of server processes to be dedicated to various data sizes, allowing the appliance to process data more efficiently. You can also configure how often to update the signature files.

Before the appliance will scan traffic for viruses, you must ensure the following conditions have been met:

• The Anti-Virus feature must be licensed. To verify that the feature has been licensed, select Maintenance > License, and click the Firewall tab. If you are not licensed for Anti-Virus, contact your sales representative.

• The rules governing the traffic you want filtered must have the appropriate Application Defenses options selected:
  – To scan web traffic, create rules using an HTTP or HTTPS application defense with the MIME/Virus/Spyware option configured. See “Creating HTTP or HTTPS Application Defenses” on page 163 for more information.
  – To scan mail messages, create rules using the sendmail server and a Mail (Sendmail) application defense with the MIME/Virus/Spyware option configured. See “Creating Mail (Sendmail) Application Defenses” on page 184 for more information.

To configure scanning services, select Policy > Application Defenses > Virus Scanning. The Virus Scanning window appears with the Signature tab displayed.
Configuring virus scanning signature updates

Use this tab to configure the anti-virus update properties. The appliance can automatically download and install updates at intervals that you determine. (This window mainly deals with updating signature files, but has an option to make sure the virus engine is also up-to-date.) You can also manually download and install updated signature files at any time.

**Important:** Secure Computing recommends downloading the most recent engine patch (for example, 700SOV16) and the latest signature files prior to enabling anti-virus services.

![Virus Scanning: Signature tab](image)
To configure the anti-virus update properties:

1  In the **Source** area, verify/modify the following fields:

   **Caution:** Changing these defaults may prevent the appliance from obtaining updated signatures file, resulting in inadequate virus and spyware protection.

   • **Download Site** — This is the name of the site from which the package will be downloaded. The default site is downloads.securecomputing.com.
     
     If the download fails, troubleshoot the problem by verifying that the site name resolves to an IP address and is reachable from the Sidewinder appliance.
   
   • **Directory** — The path name on the download site that contains the update. The default directory is cgi-bin/avupdate.

2  [Conditional] To configure automatic virus updates, follow the sub-steps below. To manually download and install the signature files, skip to step 3.

   Automatically updating both the scanner engine and the signature files is strongly recommended. If your engine is out-of-date, the appliance will not install the most recent files.

   **Important:** Failure to regularly update your anti-virus engine and signature files will result in inadequate virus and spyware protection. For best results, also select **Automatically check for and load packages** (Maintenance > Software Management > Load Packages tab).

   a  Select **Enable Automated Signature Download and Install**.

   b  In the **Frequency** field, specify how frequently you want to download and install updated signature files:

     • (Recommended) To download and install every hour, select **Hourly**.
     • To download and install every day, select **Daily**.
     • To download and install once a week, select **Weekly**. Also specify the day of the week on which you want downloads to occur.

   c  For all frequency options, in the **Time** field, specify the time of day you want to download and install the updates.

     **Note:** Downloading and installing updates has a minimal impact on your system. Traffic that is received while the download and installation are in process will be scanned using the current version. Once installation is complete, all traffic will be scanned using the updated scanner information.

   d  Select **Enable Automated Scanner Engine Updates** to automatically check for new loaded (but not installed) anti-virus engine updates (for example, patch 700SOV14) when installing new virus signature files. If an uninstalled engine update exists, the appliance will install it the next time it installs the new signature files. This installation does not interrupt system processes.
e  If you want to receive e-mail notification when the updates are downloaded and installed, select the **Enable Email Notification** check box. If you select this option, you will also need to specify an e-mail address in the **Recipient** field.

f  Proceed to step 5.

3  [Conditional] To update the virus definition manually, do the following:

a  Click **Download and Install Signatures Now**. A pop-up window appears.

b  Click **Background** to perform the update in the background, or click **Wait** to receive a notification and status pop-up when the update is complete. Proceed to step 5.

4  To view the current version of the signature file you are using, click **Show Installed Signatures File Version Number Now**. An Info window appears displaying the current installed version. When you are finished viewing the version, click **OK**.

5  Save your changes.

The virus scanner is now using a supported engine and the current signature files.
Configuring the advanced virus scanning features

Use this tab to configure how your appliance distributes scanner processes for incoming and outgoing traffic. This is done by configuring the number of scanners to be run to service each of the defined file size ranges.

Figure 114: Virus Scanning: Advanced tab

- The **File Size Range** column displays the size limits for each range. Ranges are **Up to 40K**, **Up to 100K**, **Up to 1MB**, and **Unlimited**.

- The **Scanners** column displays the number of scanner processes dedicated to each range.

You cannot modify the existing size ranges or add new size ranges in the Admin Console.

Files are handled by the first file size range that is greater than the file’s size. For example, a 39K file will be processed by a scanner process assigned to the **Up to 40K** file size range, but a 40K file will be processed by a scanner process assigned to the **Up to 100K** file size range.

**Tip:** While using additional scanners may speed up virus scanning, it can slow down your appliance’s overall performance. Try using more restrictive MIME/Virus/Spyware rules, configured on the Application Defenses, to make virus scanning more efficient.

This tab also allows you to view the current virus scanner engine version.
To configure virus scanning’s advanced properties:

1. To configure the number of scanner processes for a particular size range, select the file size range in the table and click **Modify**. The Edit Scanners window appears.

   In that window’s **Scanners** field, specify the number of scanner processes you want to dedicate for the selected group. Valid values are between 1 and 10, and the total number of scanner processes should not exceed a combined total of 20 processes. (Configuring more than 20 total processes may have a negative impact on performance, particularly on smaller appliances.) Click **OK** to return to the Advanced tab.

   **Note:** *If you decrease the number of scanners, you must restart the virus scanner on the Monitor > Service Status window.*

2. In the **Scan Buffer Size** field, specify the size of information (in KB) that can be held in the memory buffer before a backup file is created to temporarily hold the traffic for processing. This value must be between 8KB and 64KB. The default value is 50KB.

3. In the **Archive Scan Buffer Size** field, specify the amount of memory to be used to contain the contents of archive files before the anti-virus engine temporarily writes the contents to disk to perform the virus scan. The default is 128 MB.

4. In the **Maximum Number of Files to Scan in an Archive** field, specify the maximum number of files to be scanned within an archive (such as a .zip file, etc.). If the number of files in an archive exceeds the number specified in this field, scanning does not take place.

5. [Optional] The **Scan Encrypted Files** option controls how the Virus Scanner behaves when it scans password-protected files (primarily .xls and .zip files), which the scanner classifies as encrypted. This is relevant for mail attachments, HTTP traffic, and FTP transmissions. Determine how the scanner will handle encrypted files by doing one of the following:
   - If you leave this option clear, the scanner generates an error and rejects the password-protected files.
   - If you select this option, the scanner ignores those errors and scans any unencrypted parts of the file. If no virus is found, the file is allowed.

6. To view the virus scanner engine version number that is currently installed, click **Show Installed Engine Version Number Now**. A pop-up window appears displaying the current version. To close the pop-up window, click **OK**.

7. Save your changes.

The changes to virus scanning’s advanced properties are now applied.
TrustedSource is a reputation service that filters incoming mail connections and then provides precise information about an e-mail sender's reputation based on its originating IP address. The TrustedSource reputation service is a tool for reducing the amount of spam that reaches your organization's inboxes. However, unlike spam filters which evaluate message content, TrustedSource focuses on a sender's reputation score. A reputation score is similar to a credit score in that it indicates a sender's trustworthiness. With TrustedSource, the lower the score, the more you can trust the sender.

**Note:** To use TrustedSource, you need to purchase or evaluate a TrustedSource subscription. The activation is handled by the TrustedSource infrastructure. Contact your Secure Computing channel partner or sales representative for information on evaluating or purchasing TrustedSource. You do not need to have the Sidewinder Anti-Spam feature licensed or enable the anti-spam server to use TrustedSource on Sidewinder.

**Understanding TrustedSource**

To determine reputation scores, TrustedSource uses servers around the world to gather and analyze billions of messages dynamically. TrustedSource assigns a score between 0 and 120 to an IP address based on the type of mail, legitimate and spam, this particular host generates. The Sidewinder administrator can configure what score is a tolerable threshold for your network. If a sender's score is higher than your threshold, messages from that sender are rejected by the Sidewinder appliance. The TrustedSource servers are constantly communicating so as one server identifies a spam flood in progress, it can alert all TrustedSource servers moments after the attack starts and update that sender's reputation score.

The process works like a real-time blackhole list. A sending server contacts a Sidewinder appliance running hosted sendmail. The appliance then sends a modified DNS query using the server's IP address to a TrustedSource server to get its reputation score. The appliance then compares the score to the threshold value. If the score is lower than that threshold, e-mail messages from the server are accepted. If the score is higher than the threshold, the appliance rejects the message, audits the violation, and closes the connection. This process is illustrated in the following figure:
Figure 115: Example of a Trusted Source query

To filter mail using TrustedSource, the appliance must be located on your network’s perimeter, be configured for hosted sendmail, and have functioning DNS with access to the Internet. Licensing is handled by the TrustedSource server as opposed to the Sidewinder license. Once enabled, TrustedSource automatically starts filtering all inbound mail; you do not need to alter the existing mail rules or create new rules.

With spammers, rejecting one mail message and closing the connection is rarely enough to protect your network from them. Even though the malicious content is prevented from entering your network, the server typically attempts to resend its message. The processing effort and bandwidth to continuously query TrustedSource and reject each message can constitute a Denial of Service attack.

Secure Computing recommends that in addition to enabling TrustedSource filtering, you configure an IPS attack response that is triggered by the audit violation and that blackholes all traffic coming from the untrusted server. In addition to silently dropping that host's incoming connections, blackholing immediately closes all existing connections with that host. This is particularly useful if the sender's reputation score was updated after the spam flood began.
Enabling TrustedSource

The following procedures explain how to enable TrustedSource and how to blackhole senders that are considered untrustworthy.

To enable TrustedSource filtering

1. Ensure that your appliance meets these criteria:
   - Is using hosted sendmail
   - Has DNS set up with access to the Internet
   - Is on your network's perimeter

   Also ensure that you have obtained a TrustedSource subscription. If you do not have a TrustedSource subscription, contact your Secure Computing channel partner or sales representative.

2. Select Policy > Application Defenses > TrustedSource. The following window appears:

   **Figure 116: The TrustedSource window**

<table>
<thead>
<tr>
<th>TrustedSource Filtering</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perform TrustedSource filtering on inbound mail</td>
</tr>
<tr>
<td>Reputation threshold: 80</td>
</tr>
</tbody>
</table>

3. Select Perform TrustedSource filtering on inbound mail.

4. In the Reputation threshold field, set the threshold to a value from 0 to 120. Messages from senders with reputation scores above that value are rejected. The default threshold is 80.

   Trustworthy senders receive low scores and untrustworthy senders receive high scores. The values map to five reputation classes:
Table 17: TrustedSource reputation classes

<table>
<thead>
<tr>
<th>Value</th>
<th>Class</th>
<th>Class description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Inoffensive</td>
<td>The IP address is a legitimate sender or a source of substantial amounts of legitimate e-mail.</td>
</tr>
<tr>
<td>1–25</td>
<td>Neutral</td>
<td>The IP address is likely a legitimate sender but may send small amounts of e-mail requiring further inspection.</td>
</tr>
<tr>
<td>26–50</td>
<td>Unverified</td>
<td>The IP address may be a legitimate sender but displays a few properties suggesting further content inspection of e-mails received from that address.</td>
</tr>
<tr>
<td>51–80</td>
<td>Suspicious</td>
<td>The IP address shows many spam sender characteristics, and e-mail received from this address may be subject to higher scrutiny.</td>
</tr>
<tr>
<td>80+</td>
<td>Spam</td>
<td>The IP address has either been used to send spam or should not send any e-mail messages in general.</td>
</tr>
</tbody>
</table>

5 Click Save.

The appliance now uses the TrustedSource reputation service to filter inbound e-mail.

**To blackhole senders with ratings above the set threshold**

1 Select Monitor > IPS Attack Responses.

2 Select the TrustedSource attack response.

   Its preconfigured settings are:
   - Attack Frequency — Always Respond
   - Alerts — Send e-mail, and wait 120 seconds between alerts
   - Strikeback — Blackhole each host responsible for 100% of the attacks for 21600 seconds (6 hours)

3 Right-click the TrustedSource attack response and select Enable.

4 Save your changes.

The Sidewinder appliance now blackholes hosts that have TrustedSource scores that do not meet the set threshold and are trying to send mail to your network. Use the Blackholed IPs feature on the Dashboard to manage blackholed IP addresses.

For more information on TrustedSource, visit [www.trustedsource.org](http://www.trustedsource.org).
Configuring spam filtering services

The anti-spam service is a licensed add-on module that uses a spam filter on the Sidewinder appliance that allows you to filter out spam, fraud, and identity theft mail messages. When using spam filter services, you can specify hosts, headers, and regular expressions that will always be allowed (known as whitelisting those items). You can also determine what actions the spam filter will take when it encounters messages that are suspected to be spam or fraud by editing the `spamcatcher.conf` file.

Before the appliance will filter out spam, you must ensure the following conditions have been met:

- The Anti-Spam feature must be licensed. To verify that the feature has been licensed, select **Maintenance > License**, and then click the **Firewall** tab. If you are not licensed for anti-spam, contact your sales representative.
- The Sidewinder appliance must be configured for hosted sendmail.
- The rules governing the traffic you want filtered must use the following:
  - The sendmail server
  - A Mail (Sendmail) application defense with the Spam/Fraud option configured

See “Creating, modifying, and duplicating rules” on page 95 and “Creating Mail (Sendmail) Application Defenses” on page 184 for more information.

To configure spam filter services, select **Policy > Application Defenses > Spam Filter**. The Whitelist Configuration area appears.
Configuring the Whitelist

Use the Whitelist Configuration window to specify domains, IP addresses, and headers that will be allowed to pass through the appliance unmodified, regardless of any rules that have been created.

To configure a whitelist for the internal or external (Internet) burb, select Policy > Application Defenses > Spam Filter. The following window appears:

Figure 117: The Spam Filter window

The Allowed Host Entries tab contains a table listing all hosts that are currently allowed. The table displays the host name, the burbs for which this host is allowed, the host IP address, and a description of the host.

- To add a new host, click New.
- To modify an existing host, select the host you want to modify and click Modify. (Read-only administrators can click View to view an existing host.)
- To delete a host, select the host you want to delete and click Delete.

For more information on creating and modifying host entries, see “About the New/Modify Host Whitelist Entry window” on page 263.
The **Allowed Header and Regular Expression Entries** tab contains a table that lists the substrings or regular expressions in a header that are currently allowed. The table displays the entry name, the burbs for which the entry is allowed, the header type (standard or custom), and a description of the entry.

- To add a new entry, click **New**
- To modify an existing entry, select the entry you want to modify and click **Modify**.
- To delete a entry, select the entry you want to delete and click **Delete**.

For more information on creating and modifying host entries, see “About the New/Modify Header Whitelist Entry window” on page 264.

**About the New/Modify Host Whitelist Entry window**

To configure a new host or modify an existing host for the whitelist, follow the steps below.

1. In the **Entry Name** field, type a descriptive name for the host.
2. In the **Host** field, select one of the following:
   - **IP Address** — To specify the host IP address, select this option and type the IP address in the corresponding text box. Enter the full address; subnets are not supported.
   - **Host Address** — To specify the host address, select this option and type the host address in the corresponding text box.
3. In the **Burb Restriction** field, specify the burbs for which this host will be allowed:
   - **Apply rule to all burbs** — Select this option to allow this host for all burbs.
   - **Apply rule to Internet burb** — Select this option to allow this host only for the Internet burb.
   - **Apply rule to non-internet burbs** — Select this option to allow this host only for non-internet burbs.
4. [Optional] In the **Description** field, enter any useful information about this host entry (for example, a brief description of the host).
5. Click **OK** to save the changes and return to the Whitelist Configuration tab.

Mail from this host will not be considered spam and will be passed along according to the specified restrictions.
About the New/Modify Header Whitelist Entry window

To configure a new header or modify an existing header, follow the steps below.

1. In the **Entry Name** field, type a descriptive name for this header.
2. In the **Header** field, select one of the following:
   - **Standard** — Select this option to specify a standard header (for example: to, from, cc, etc.). Select the header from the drop-down list.
   - **Custom** — Select this option to specify a custom header. Enter the custom header in the corresponding text field.
3. In the **Burb Restriction** field, specify the burbs for which this host will be allowed:
   - **Apply rule to all burbs** — Select this option to allow this host for all burbs.
   - **Apply rule to Internet burb** — Select this option to allow this host only for the Internet burb.
   - **Apply rule to non-internet burbs** — Select this option to allow this host only for non-internet burbs.
4. In the **Regular Expression** field, enter the desired expression to match in the header (for example, @.*gov, @example.com)

   **Note:** Do not configure this field until you are familiar with regular expressions.

5. [Optional] In the **Description** field, enter any useful information about this entry (for example, a brief description of the header or regular expression).
6. Click **OK** to save your changes.

The specified headers and regular expressions will be passed along according to the specified restrictions.
Configuring the `spamcatcher.conf` file

The `spamcatcher.conf` file allows you to determine the actions that will be taken by the spam filter on a per-user basis when it encounters messages that are suspected to be spam or fraud, including identity theft and phishing messages. These configuration options are stored in `/secureos/etc/mailshell.SMFn/spamcatcher.conf`. The `spamcatcher.conf` file contains a list of the actions that will be taken based on the disposition of an e-mail message (that is, the likelihood of the message being spam).

**About the spamcatcher.conf thresholds and features**

Following are the settings in `spamcatcher.conf`. Use a file editor to change the settings.

---

**Important:** After making changes to `spamcatcher.conf`, you must rebuild the file, using `cf daemond restart agent=spamfilter` or the restart the spamfilter server on the Monitor > Service Status window, for the changes to take effect.

---

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
| SpamThreshold         | This option indicates the spam score above which a message will be identified as spam.  
• A high spam score indicates that a message is likely to be spam.  
• A low spam score indicates that a message is unlikely to be spam.  
• Threshold values can be any integer from 0–100.  
For example, if the spam threshold is 90 and a message’s spam score is 91, the mail will be identified as spam. |
| RejectionThreshold    | This option indicates the threshold above which mail will be rejected.  
• Mail messages that have spam scores equal to or above this value will be rejected.  
• If you do not specify a value, all spam messages will be delivered.  
For example, if the rejection threshold is 97, and a message’s spam score is 98, the mail will not be delivered. |
| DeletionThreshold     | Indicates the spam threshold which forces the mail to be discarded. Mail messages that have spam probabilities equal to or above this value will be discarded. If no value is specified by the user, spam messages will be delivered.                                                                                     |
| TagMessageIfSpam      | Indicates whether or not to add or change headers and change the subject line if a message is spam.                                                                                                                                                                                 |
| SubjectChange         | Indicates whether or not to change the subject line if a message is spam.                                                                                                                                                                                                       |
About editing the spamcatcher.conf file

To edit the spamcatcher.conf file, do the following:

1. Select Maintenance > File Editor. The File Editor window appears.
2. Click Start File Editor and select File > Open. The Open File window appears.
3. Select the Firewall File radio button. The Open File window appears.
   The spamcatcher.conf file is located in the /secureos/etc/mailshell.SMF\n   directory, where \( n \) is the burb index for the corresponding spam filter. For example, /secureos/etc/mailshell.SMF1/spamcatcher.conf is the configuration file for burb index 1.
4. Type the following path in the File field:
   /secureos/etc/mailshell.SMF\n   where \( n \) is the corresponding burb index for the burb you want to configure.
5. Click OK to open the file. The spamcatcher.conf file for the burb you selected is displayed.
6. Change the thresholds and features according to your site’s spamfilter policy. See the previous section or the spamfilter man page for more information on each feature.
7. Save and then close the file.

The spam filter begins processing the changes.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verbose_Header</td>
<td>Allows you to add headers to the message.</td>
</tr>
<tr>
<td>enable_spf</td>
<td>Controls whether or not to do Sender Policy Framework (SPF) database checks.</td>
</tr>
</tbody>
</table>
Configuring SmartFilter for Sidewinder

SmartFilter is a content management solution that controls your company’s users’ access to the Internet. SmartFilter relies on a database of millions of URLs that have been categorized based on their content. Category examples include gambling, general news, and shopping/merchandising. SmartFilter manages Web access at several levels, ranging from simple access restrictions for specific sites to thorough blocking of all web sites categorized as unproductive or non-business related.

SmartFilter and the Sidewinder appliance work together to enforce your web filtering policy. The policy is configured on SmartFilter, using the Control List’s categories. SmartFilter sends that policy to the Sidewinder sfadmin server. The Sidewinder appliance checks users’ web requests and allows or denies the requests based on that policy. If a connection is not allowed, the sfredirect server sends a message to the user making the request. See Figure 118 for an example of this process.

**Note:** Downloading the SmartFilter administration software is free. You can then choose to evaluate the Control List (database of categorized web sites that is updated frequently) for 30 days, or a purchase a subscription. SmartFilter is licensed through SmartFilter and is not a Sidewinder license feature.

Figure 118: Example of Sidewinder and SmartFilter denying a user’s HTTP request

Here is an overview of how to get SmartFilter to filter Sidewinder web traffic:

1. Obtain a SmartFilter serial number. You can either evaluate SmartFilter and its Control List for 30 days or purchase a Control List subscription.
2. Download and install the SmartFilter administration software. (This software is to be installed on a platform other than your Sidewinder appliance.)
3. Using the Sidewinder Admin Console, set up the SmartFilter services and then configure the rules that will govern the web traffic you intend to filter.
4. Using the SmartFilter Admin Console, configure your SmartFilter policy and push it to the Sidewinder appliance. Consult the SmartFilter documentation before configuring.

Complete these tasks to begin using SmartFilter services through the Sidewinder appliance. For more details, see the following sections.
Obtaining the SmartFilter Control List

SmartFilter uses a Control List that contains millions of URLs. These URLs are categorized into pre-defined categories. Your SmartFilter policy contains which categories are allowed, blocked, warned, delayed, or monitored. You must have either a temporary or permanent serial number to install SmartFilter and download its Control List.

- Downloading and management of the Control List is managed via the SmartFilter Admin Console. Refer to the SmartFilter Installation Guide and the SmartFilter Primer for more information, available at www.securecomputing.com/goto/sf/downloads.
- For a list of the categories and a description of each category, go to www.securecomputing.com/goto/controllist.

Evaluating the SmartFilter Control List

If you are not a current SmartFilter user, you can evaluate the full Control List by following the steps contained in the sections that follow.

You can retrieve a 30-day evaluation copy of the full Control List by performing the following steps:

2. Select Sidewinder 7.0.0.00 or later.
3. Click Evaluate this version.
4. Complete and submit the registration form.

Within one business day after you complete and submit the registration form, you will receive an e-mail that includes an evaluation serial number. Enter this serial number into the SmartFilter Administration Console during or after installation to obtain the Control List.

**Note:** If the evaluation expires before you purchase a subscription, the Sidewinder appliance will either block or allow all sites, according to a selection made during installation. To change this behavior, renew your subscription or stop using SmartFilter on the Sidewinder appliance.

Subscribing to the SmartFilter Control List

1. Order the SmartFilter service option through Secure Computing or your reseller.
   
   After you submit your order, you will be e-mailed an activation certificate with a serial number.

2. Enter this serial number into the SmartFilter Administration Console’s Enterprise > License window to download the Control List.

Once you have a SmartFilter serial number, you can download, install, and configure SmartFilter for Sidewinder.
Setting up SmartFilter for Sidewinder

Complete these tasks to begin using SmartFilter to monitor your end users’ web access.

From the SmartFilter download center:

Go to http://www.securecomputing.com/goto/sf/downloads to download and install the platform-appropriate Administration Software. (Supported platforms are Linux, Solaris, and Windows.) This installs the SmartFilter Administration Console.

In the Sidewinder Admin Console:

Before you begin, note the following:

- When configuring the sfadmin service, you need to update the sfadmin password. You should not need to change the other service properties on the two SmartFilter services (sfadmin and sfredirect).
- Do not make any changes to the SmartFilter Redirect or the SmartFilter Admin application defenses or rules.
- To use SmartFilter to filter HTTPS traffic, set the service’s Allowed Connection Types setting to Non-Transparent.
- In the SmartFilter Admin Console, do not create any groups until you have deployed the Sidewinder IP address and password to the SmartFilter plugin on the Sidewinder appliance.

1. Configure the SmartFilter server password:
   a. Select Policy > Rule Elements > Services, and then double-click sfadmin.
   b. Click Properties. The SmartFilter Admin Console Agent Properties window appears.
   c. Enter, and confirm, a password to be used when authenticating the SmartFilter Server Plugin requests. This password must match the password entered in when configuring the Sidewinder Plugin on SmartFilter. If you are changing the password, changes must be made in both applications.

   Password changes are effective immediately.

2. Enable web filtering by selecting the SmartFilter option on the appropriate HTTP and/or HTTPS Application Defenses:
   a. Select Policy > Application Defenses > Defenses > HTTP and/or HTTPS.
   b. For each application defense that will be used in a rule governing traffic to be inspected by SmartFilter, check the SmartFilter option. Configure the rest of the application defense according to your site’s policies.
3 Manage SmartFilter rules: Select **Policy > Rules**.
   - Enable the default SmartFilter rule group. This group contains the rules governing communication with the SmartFilter Admin Console.
   - Create rules for HTTP and/or HTTPS traffic that you want SmartFilter to monitor. Use the application defense you configured in step 2 in those rules.

**In the SmartFilter Administration Console:**

1 Add Sidewinder as a plugin: Select **Enterprise Settings > Plugins**.
   - **Type** — Select **Sidewinder**.
   - **Address** — Enter the IP address of Sidewinder interface that connects to your SmartFilter Administration Console. (For example, if the system where you installed SmartFilter is in the internal burb, put the internal burb’s IP address here.)
   - **Password** — Enter the password you previously set for the sfamin server (see step 1 above).

2 If you do not intend to use the default SmartFilter policy, configure a SmartFilter policy to use with the Sidewinder appliance.

3 Deploy the plugin. This also pushes the SmartFilter policy.

4 Download the SmartFilter control list by clicking **Download Control List** in the toolbar.

   For additional configuration information, see the *SmartFilter Installation Guide*. One-to-Many and High Availability clusters, in particular, require procedures found in that guide.

The Sidewinder appliance is now filtering traffic according to your SmartFilter policy.
CHAPTER 9

Network Objects and Time Periods

In this chapter...

Creating network objects ..............................................................272
Creating time periods .................................................................288
Creating network objects

A network object is the source or destination of a connection to or through the Sidewinder appliance. A network object can be any of the following:

- Domain
- Host
- IP address
- IP range
- Netmap
- Subnet
- Netgroup

Each network object that you create is available for selection from the source and destination Endpoint drop-down lists on the Rules window.

To view, create, and maintain network objects, select **Policy > Rule Elements > Network Objects**. The Network Objects window appears.

![Network Objects window](image1)

This window lists the network objects currently configured on the Sidewinder appliance. Use the toolbar to perform the tasks listed in Table 19.

![Network Objects toolbar](image2)

New Group

Duplicate

Search

Manage netgroup membership

New network object options
Table 19: Network Objects toolbar tasks

<table>
<thead>
<tr>
<th>Icon</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td>Create a network object by clicking <strong>New</strong> and selecting an object from the drop-down menu. Configure the selected Network Objects window that appears:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Domain</strong> — For information on creating a domain object, see “About the Network Object: Domain window” on page 275.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Host</strong> — For information on creating a host object, see “About the Network Object: Host window” on page 276.</td>
</tr>
<tr>
<td></td>
<td>• <strong>IP Address</strong> — For information on creating an IP address object, see “About the Network Object: IP Address window” on page 278.</td>
</tr>
<tr>
<td></td>
<td>• <strong>IP Range</strong> — For information on creating an IP range object, see “About the Network Object: IP Range window” on page 279.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Netmap</strong> — For information on creating a netmap object, see “About the Network Object: Netmap window” on page 280.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Subnet</strong> — For information on creating a subnet object, see “About the Network Object: Subnet window” on page 282.</td>
</tr>
<tr>
<td>New Group</td>
<td>Create a netgroup by clicking <strong>New Group</strong>. The Netgroup window appears.</td>
</tr>
<tr>
<td></td>
<td>See “About the Network Object: Netgroup window” on page 283 for more information.</td>
</tr>
<tr>
<td>Modify</td>
<td>Modify an existing network object or netgroup by selecting it from the list and clicking <strong>Modify</strong>. Make your changes in the pop-up window.</td>
</tr>
<tr>
<td></td>
<td>(Read-only administrators can click <strong>View</strong> to view a network object or netgroup.)</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete an existing network object or netgroup by selecting it in the list and clicking <strong>Delete</strong>.</td>
</tr>
<tr>
<td>Duplicate</td>
<td>Create a duplicate of an existing network object or netgroup by selecting it in the list and clicking <strong>Duplicate</strong>. Change the name and make any desired changes, then click <strong>Add</strong>.</td>
</tr>
<tr>
<td>Rename</td>
<td>Rename a network object or netgroup by selecting it in the list and clicking <strong>Rename</strong>. Type the new name in the pop-up window and click <strong>OK</strong>.</td>
</tr>
</tbody>
</table>

*More...*
### Creating network objects

<table>
<thead>
<tr>
<th>Icon</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Usage</td>
<td>View the areas (netgroup, netmap, proxy rule) that are currently using a particular network object or netgroup by selecting it in the list and clicking <strong>Usage</strong>.</td>
</tr>
<tr>
<td>Find</td>
<td>Search for specific elements in the list by typing your search criteria in the <strong>Find</strong> field. Objects with matching elements appear in the list.</td>
</tr>
<tr>
<td>Group Objects In</td>
<td>Add or remove a network object from a netgroup by selecting the netgroup and clicking <strong>Groups Object In</strong>. See “Managing netgroup membership” on page 287 for more information.</td>
</tr>
</tbody>
</table>
About the Network Object: Domain window

Use this window to define information about a domain. Each domain you define becomes a network object that can be used in a rule.

Domain objects have features that set them apart from other network objects. Before using domain objects in rules, note the following:

• Since domains are dependent on DNS, which is out of your control, the use of domain network objects can be a security risk.
• Domain objects require a DNS lookup and therefore incur a DNS performance penalty each time they are used.
• For a proxy rule that includes a domain object to be processed correctly, that rule must be placed after the last filter rule.

**Figure 121: Network Object: Domain window**

- **Name** — Type a name for this domain object (for example, “example” for example.com).
  - Valid values include alphanumeric characters, periods (.), dashes (-), underscores (_), and spaces ( ).
  - The name cannot exceed 100 characters.

  _Note:_ The name you create here is what you will see in the Endpoint drop-down list when you create a rule. You will not see any of the object’s values, so make a descriptive name to ensure that you will recognize it in the Rules window.

  This field cannot be edited if you are modifying an existing domain.

- [Optional] **Description** — Enter any useful information for this domain object.

- **Domain** — Enter the domain to use for this object (for example, example.com).

Click **Add** to add the domain object, or **OK** if you modified an existing domain object.
About the Network Object: Host window

Use this window to define information about a host. Each host you define becomes a network object that can be used in a rule.

**Note:** In IP filter rules, the localhost network object is supported, but DNS-resolvable host names should be avoided. DNS-resolvable host names become inoperative during any periods when the appropriate DNS server is unavailable or unreachable.

- **Name** — Type a name for the host.
  - Valid values include alphanumeric characters, periods (.), dashes(-), underscores (_), and spaces ( ).
  - The name cannot exceed 100 characters.

**Note:** The name you create here is what you will see in the Endpoint drop-down list when you create a rule. You will not see any of the object’s values, so make a descriptive name to ensure that you will recognize it in the Rules window.

This field cannot be edited if you are modifying an existing host.

- [Optional] **Description** — Enter any useful information about this host.
- **Host** — Enter the hostname for this host object (for example, mail.example.com).
• **DNS** — Determine whether this host will use DNS:
  - **DNS** — Select this option to perform normal DNS look-ups.
  - **No DNS** — Select this option if you do not want to perform DNS lookups for this host.

  *Note:* The `dig` (Domain Information Groper) command gathers information from DNS based on an IP address, and obtains the corresponding host name. A `dig` is useful in determining if a host is resolvable before creating a network object.

  
  ```bash
  dig -x ipaddress any any
  ```

• [Conditional] **Override TTL** — If you selected DNS and you need to override the DNS time-to-live value, select this check box. Enter a time value and select a time increment for the new time-to-live value.

  *Note:* Overriding the default DNS time-to-live value is not recommended.

• **IP Addresses For The Host** — To create and maintain IP addresses for a host, you can do the following:
  - Click **New**, then type the IP address in the pop-up window.
  - Select an IP address, then click **Modify** and type a replacement IP address in the pop-up window.
  - Select an IP address, then click **Delete** to delete an IP address.

  Click **Add** to add the host object, or **OK** if you modified an existing host object.
Chapter 9: Network Objects and Time Periods

Creating network objects

About the Network Object: IP Address window

Use this window to define information about an IP address. Each IP address you define becomes a network object that can be used in a rule.

![Network Object: IP Address window](image)

- **Name** — Type a name for the IP address.
  - Valid values include alphanumeric characters, periods (.), dashes(-), underscores (_), and spaces ( ).
  - The name cannot exceed 100 characters.

  *Note: The name you create here is what you will see in the Endpoint drop-down list when you create a rule. You will not see any of the object’s values, so make a descriptive name to ensure that you will recognize it in the Rules window.*

  This field cannot be edited if you are modifying an existing IP address.

- **[Optional] Description** — Enter any useful information about this IP address object.

- **IP Address** — Type the value of the IP address.

Click **Add** to add the IP address object, or **OK** if you modified an existing IP address object.
About the Network Object: IP Range window

Use this window to define information about an IP range. The IP range you define becomes a network object that can be used in a rule.

**Figure 124: Network Object: IP Range window**

- **Name** — Type a name for the IP range.
  - Valid values include alphanumeric characters, periods (.), dashes (-), underscores (_), and spaces ( ).
  - The name cannot exceed 100 characters.

  *Note: The name you create here is what you will see in the Endpoint drop-down list when you create a rule. You will not see any of the object’s values, so make a descriptive name to ensure that you will recognize it in the Rules window.*

  This field cannot be edited if you are modifying an existing IP range.

- [Optional] **Description** — Enter any useful information about this IP range object.

- **Starting IP Address** — Type the value of the IP address at the beginning of the range.

- **Ending IP Address** — Type the value of the IP address at the end of the range.

Click **Add** to add the IP range object, or **OK** if you modified an existing IP range object.
Chapter 9: Network Objects and Time Periods

Creating network objects

About the Network Object: Netmap window

Use this window to define information about a netmap. Each netmap you define becomes a network object that can be used in a rule.

Netmap objects allow you to map multiple IP addresses and subnets to alternate addresses without creating numerous rules.

- A netmap consists of one or more netmap members.
- A netmap member is any IP address or subnet that you add to a netmap.
- Each member in the netmap is mapped to an alternate address or subnet that you specify.

![Network Object: Netmap window](image)

**Figure 125: Network Object: Netmap window**

- **Name** — Type a name for the netmap.
  - Valid values include alphanumeric characters, periods (.), dashes(-), underscores (_), and spaces ( )
  - The name cannot exceed 100 characters.

  *Note: The name you create here is what you will see in the Endpoint drop-down list when you create a rule. You will not see any of the object’s values, so make a descriptive name to ensure that you will recognize it in the Rules window.*

This field cannot be edited if you are modifying an existing netmap.

- **[Optional] Description** — Enter any useful information for this netmap.
• **Netmap members list** — This list displays existing netmap members. You can perform the following actions:
  - **Create a new netmap member** — Click **New** and make a selection in the pop-up menu to create a netmap member.
    * **IP Address** — Select this option if you want to map an IP address to a different IP address.
    * **Subnet** — Select this option if you want to map a subnet address to a different subnet address.
  - **Modify an existing netmap member** — Select a netmap member in the list and click **Modify**, then make the desired selections in the pop-up window.
  - **Delete an existing netmap member** — Select a netmap member in the list and click **Delete**.
  - **Sort** — Click a column heading to sort the list by that column’s content. Click again to reverse the sort order.

Click **Add** to add the netmap information, or **OK** if you modified an existing netmap.

**About the Netmap Members: IP Address/Subnet Netmap Selections window**

**Figure 126: Netmap Members window**

Use the IP Address Netmap/Subnet Selections window to map an IP address or a subnet to an alternate address within a netmap.

1. In the **Original** list, select the IP or subnet address that you want to map to a different address.

2. In the **Mapped** list, select the IP address that the original IP address will be mapped to, or select a subnet address of the same size that the original subnet address will be mapped to.

3. Click **Add**.
Chapter 9: Network Objects and Time Periods

Creating network objects

About the Network Object: Subnet window

Use this window to define information about a subnet. Each subnet you define becomes a network object that can be used in a rule.

![Network Object: Subnet window](image)

- **Name** — Type a name for the subnet.
  - Valid values include alphanumeric characters, periods (.), dashes (-), underscores (_), and spaces ( ).
  - The name cannot exceed 100 characters.

  *Note: The name you create here is what you will see in the Endpoint drop-down list when you create a rule. You will not see any of the object’s values, so make a descriptive name to ensure that you will recognize it in the Rules window.*

  This field cannot be edited if you are modifying an existing subnet.

- [Optional] **Description** — Type any useful information about the object.

- **Subnet** — Enter the following information:
  - In the text field, type the subnet address.
  - In the numeric text box, enter the number of significant bits for the subnet address. You must enter an integer value in the range 0–32. For example, if you enter 16, only the first 16 bits of the address are important.

  Click **Add** to add the subnet object, or **OK** if you modified an existing subnet object.
About the Network Object: Netgroup window

Use this window to define information about a netgroup. Each group you define becomes a network object that can be used in a rule.

**Tip:** You may find it more convenient to create all of your network objects before defining your netgroup objects. That way, as you set up your netgroup objects, you will be able to immediately assign the desired network objects to the group.

- **Name** — Type a name for the netgroup. The name will be used by rules to identify the netgroup when you set up Sidewinder connections.
  - Valid values include alphanumeric characters, periods (.), dashes(-), underscores (_), and spaces ( )
  - The name cannot exceed 100 characters.

**Note:** The name you create here is what you will see in the Endpoint drop-down list when you create a rule. You will not see any of the object’s values, so make a descriptive name to ensure that you will recognize it in the Rules window.

This field cannot be edited if you are modifying an existing group.

- **[Optional] Description** — Enter any useful information about this group.
• The Available Members list displays all of the network objects that you can add to this netgroup. The Chosen Members list displays the network objects that are currently members of this netgroup.
  – To add a member to this netgroup, select the desired member in the Available Members list, then click the > arrow button to move it to the Chosen Members list.
  – To remove a member from this netgroup, select the desired member in the Chosen Members list, then click the < arrow button.
  – To add or remove multiple consecutive members at one time, select the first member, then press the Shift key while selecting the last member. To add or remove multiple non-consecutive members at one time, press the Ctrl key while selecting each desired member.

Click Add to add the netgroup, or OK if you modified an existing netgroup.
Example of rules using netgroups

For the configuration shown in Figure 129, the Sidewinder administrator has grouped all internal systems into one of three netgroups: marketing (mkt_net_group), engineering (eng_net_group), and accounting (acct_net_group).

Suppose you want to allow all groups access to external FTP sites but only the engineering group access to FTP host 192.55.12.3. Table 20 shows the rules in the order that they should be added to the rule group. The following table shows the rules in the order that they should be added to the rule group.

Table 20: Rules for sample configuration shown in Figure 129

<table>
<thead>
<tr>
<th>Rule Criteria</th>
<th>Rule 1: allow_eng_ftp</th>
<th>Rule 2: deny_other_ftp</th>
<th>Rule 3: allow_oth_ftp</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service</td>
<td>FTP</td>
<td>FTP</td>
<td>FTP</td>
</tr>
<tr>
<td>Action</td>
<td>Allow</td>
<td>Deny</td>
<td>Allow</td>
</tr>
<tr>
<td>Source Burb</td>
<td>internal</td>
<td>internal</td>
<td>internal</td>
</tr>
<tr>
<td>Source Endpoint</td>
<td>eng_net_group</td>
<td>&lt;Any&gt;</td>
<td>&lt;Any&gt;</td>
</tr>
<tr>
<td>Destination Burb</td>
<td>external</td>
<td>external</td>
<td>external</td>
</tr>
<tr>
<td>Destination Endpoint</td>
<td>192.55.12.3</td>
<td>192.55.12.3</td>
<td>&lt;Any&gt;</td>
</tr>
<tr>
<td>Authenticator</td>
<td>SafeWord</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Group</td>
<td>any (leave blank)</td>
<td>any (leave blank)</td>
<td>any (leave blank)</td>
</tr>
<tr>
<td>Time Period</td>
<td>Fri 7am-7pm</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Defense (FTP)</td>
<td>Allow Put/Get</td>
<td>Deny All</td>
<td>Allow Put/Get</td>
</tr>
</tbody>
</table>
The following list summarizes key points to consider for the proxy rules listed in Table 20.

• Rule 1 allows all systems in the engineering group authenticated FTP access to IP address 192.55.12.3 on the Internet, but only on Friday between 7:00 a.m. and 7:00 p.m.

• This rule requires users to authenticate themselves via SafeWord before an FTP connection is allowed.

• Rule 2 denies all systems in the trusted burb named internal from FTP service to IP address 192.55.12.3 on the Internet.

• Rule 3 allows FTP service from all systems in the internal trusted burb to any external system in the Internet burb.
Managing netgroup membership

You can add or remove members in an existing group in two ways:

- In the Network Objects window, select the desired netgroup from the list and click **Modify**, then make the membership changes in the Netgroup window. See “About the Network Object: Netgroup window” on page 283.

- In the Network Objects window, select a network object from the list and click **Groups Object In**. The Group Membership window appears.

![Figure 130: Group Membership window](image)

Use the Group Membership window to see which groups the object belongs to and to add or remove the object from group membership.

The **Available** list displays all the available groups. The **Selected** list displays the groups to which the object currently belongs.

- To add this network object to another group, select the group in the **Available** list, then click the > arrow button to move it to the **Selected** list.

- To remove a network object from a group, select the group in the **Selected** list, then click the < arrow button to move the group to the **Available** list.

- To select multiple consecutive entries, press the **Shift** key while selecting the groups. To select multiple non-consecutive entries, press the **Ctrl** key while selecting the desired entries.

When you are finished, click **OK**.
Creating time periods

A time period is a rule element that can specify a segment of time a rule is in effect. The time periods you create here can be selected from the Time period drop-down list on the Rule window.

To create time periods for rules, select Policy > Rule Elements > Time Periods. The Time Periods window appears.

The upper pane lists the existing time periods. The lower pane shows the settings for the selected time period.
Use the toolbar to perform the actions listed in Figure 21.

Figure 132: Time Periods toolbar

![Time Periods toolbar]

Table 21: Time Periods toolbar tasks

<table>
<thead>
<tr>
<th>Icon</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td>Create a new time period by clicking <strong>New</strong>. A pop-up window appears where you set the appropriate properties. See “About the New/Modify Time Period: New Days and Times window” on page 290 for more information.</td>
</tr>
<tr>
<td>Modify</td>
<td>Modify an existing time period by selecting a time period from the list and modifying the settings in the lower pane. To modify the settings in a pop-up window, click <strong>Modify</strong>. (Read-only administrators can click <strong>View</strong> to view a time period.) See “About the New/Modify Time Period: New Days and Times window” on page 290 for more information.</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete an existing time period by selecting a time period from the list and clicking <strong>Delete</strong>.</td>
</tr>
<tr>
<td>Rename</td>
<td>Rename an existing time period by selecting a time period from the list and clicking <strong>Rename</strong>. Type a new name in the pop-up window.</td>
</tr>
<tr>
<td>Usage</td>
<td>View which rule is using an existing time period by selecting a time period from the list and clicking <strong>Usage</strong>. A pop-up window shows which rules use the selected time period.</td>
</tr>
<tr>
<td>Find</td>
<td>Search for specific elements in the list by typing your search criteria in the <strong>Find</strong> field. Time periods with matching elements appear in the list.</td>
</tr>
</tbody>
</table>

You can make the following modifications in the lower pane:

**Description** — Type a description of the time period to further identify it.

**Days and Times** — This list shows the parameters of the time period.

- **New** — Click this button to set day and time parameters for this time period.
- **Modify** — Click this button to modify the selected days and times.
- **Delete** — Click this button to delete the selected days and times.
About the New/Modify Time Period: New Days and Times window

Use this window to set the day and time parameters of a rule.

**Figure 133:** New/Modify Days and Times window

- **Continuous time period** — Select this option to make a rule active for one episode per week.
  - **Start** — Select the day and time that the rule will become active each week.
  - **End** — Select the day and time that the rule will become inactive until the following week.

- **Recurring time period** — Select this option to make a rule active on specified days and times every week.
  - **Days** — Select the days that this rule will be active each week.
  - **Start** — Set the time that this rule will become active each selected day.
  - **End** — Set the time that this rule will become inactive each selected day.
  - **All day** — Select this option to make the rule active 24 hours of each selected day.
CHAPTER 10 Authentication

In this chapter...

Understanding authentication...............................................................292
Configuring an authenticator .............................................................301
Telnet and FTP considerations.............................................................324
Setting up users to change their own passwords.................................325
Authenticating groups from an external group source.........................327
Authenticating groups from an internal group source...........................329
Understanding authentication

Authentication refers to a process that validates a person’s identity before he or she is allowed to pass traffic through the Sidewinder appliance.

Depending on the authentication method used, a person must provide a user name and valid password and/or a special passcode or personal identification number (PIN) before being logged into a server. If a user enters an invalid password, passcode, or PIN, then the policy will not pass network traffic.

Who gets authenticated

The Sidewinder appliance authenticates two types of users:

- Administrators connecting to the appliance
- Proxy users connecting through the appliance

Administrator authentication

This is for administrators who maintain or audit the Sidewinder appliance. Administrators log directly into the appliance.

- The initial administrator account, including user name and password for login authentication to the appliance, is created during startup configuration using the Quick Start Wizard.
- Additional administrator accounts can be created or modified on the Administrator Accounts window.
- Administrators can use SSH to access an appliance remotely via a command line interface.

Note: Secure Computing recommends using a strong authentication method for administrators logging in remotely.
Proxy authentication

This is for network users attempting to create a proxy connection from one side of the appliance to the other.

• You can authenticate internal-to-external, external-to-internal, and internal-to-internal connections.

• You can authenticate access for any service through the appliance.

• You can allow access to multiple services with a single successful authentication method by using Passport (also known as single sign-on).

• You can require authentication by selecting an authentication method on the Rules window when you create a rule.

• You can set up authentication on a user-by-user basis. Some authenticators allow you to create user groups to identify multiple users by a single name, or to add groups from an external authentication server. You can assign groups to use an authentication method for a rule in the Rules window.

See “Configuring an authenticator” on page 301.

Weak and strong authentication

An authentication method is weak or strong, depending on the level of security it provides.

Weak authentication

A weak authentication method merely requires a user to enter the same password each time he or she logs in.

For example, in the standard UNIX password authentication, the password you provide is maintained in the user database, and the Sidewinder appliance checks the database to validate your password.

This is considered to be a weak authentication method. If someone “sniffs” the password off the phone line or network as it is transmitted, they can conceivably use that password to break into the system.

Because your internal network is thought to be trusted, this type of authentication is generally used for authenticating internal-to-external proxy connections.
Strong authentication

Strong authentication uses multiple factors to positively identify who is accessing your networks and to keep passwords secure.

For all authentication methods (except standard password), an authenticator in the Sidewinder appliance communicates with an authentication server to validate users. An authenticator provides an interface between the proxy software and the various authentication services.

- An authentication server stores dynamic passwords (passcodes) or challenge/response information, as well as detailed information about user accounts and connection times. It typically resides on the internal network burb.
- The user has a hardware or software authenticator (token) that generates a unique passcode for each login attempt. Since each passcode is unique, they are immune to passcode sniffing or theft. Since the passcodes are generated by a cryptographic algorithm, they are essentially impossible to guess.
  - A hardware authenticator is a small, hand-held device that looks similar to an ordinary calculator. It displays the proper login response on a digital display.
  - A software authenticator is installed directly on the user’s computer. A valid PIN unlocks the software authenticator, which then calculates and returns the proper login response.

An extra layer of security is added in two-factor authentication, where a PIN allows access to the token, and the token generates the unique passwords.

- A Sidewinder appliance coordinates the passcode prompt-and-response process between the authentication server and the user.

Strong authentication is generally desired for external-to-internal proxy connections and for external administration access to the appliance.
Types of authentication methods

The Sidewinder appliance supports the following authentication methods:

**Passport**

**Security level:** Weak

Passport (also known as single sign-on) works in conjunction with a specified authentication method to allow access to multiple services with a single successful authentication to the appliance. Passport also allows authentication for encrypted services and services that do not handle authentication.

A successful Passport authentication caches the source IP address for a specified time. All further proxy connections that require Passport authentication will check that cache for a successfully authenticated user. If the source IP address exists in the cache, and Passport is the authentication method for the rule, the connection is allowed without being prompted for authentication.

You can configure the Sidewinder appliance to revoke the Passport after a specified time period has passed (for example, you may choose to require each user to re-authenticate every two hours). You can require a user to re-authenticate after a specified period of idle time (for example, a user must re-authenticate if the Passport has not been accessed for one hour or more). You can also manually revoke a Passport for a specific user or for all users at any time.

**Password**

**Security level:** Weak

Standard password authentication requires a user to enter the same password each time he or she logs in.

Standard password authentication is typically used for internal-to-external SOCKS5, Telnet, FTP, and HTTP connections, and for administrators logging into the appliance from the internal (trusted) network.

Since internal users are generally trusted, a weak authentication method may be all that is required. You may want to authenticate internal-to-external connections not so much for security reasons but to track usage of the system.

**iPlanet**

**Security level:** Weak

LDAP (Lightweight Directory Access Protocol) server owned by iPlanet, Inc.
Active Directory

Security level: Weak

LDAP (Lightweight Directory Access Protocol)/Active Directory is a protocol that you can use to provide fixed password authentication for SOCKS5, Telnet, FTP, and HTTP sessions through the Sidewinder appliance. It can also be used to authenticate logins and SSH logins to the appliance.

You can set up an LDAP directory server containing users and passwords. Use any valid combination of LDAP attributes and values as an optional filter string to distinguish authorized Sidewinder appliance users.

OpenLDAP

Security level: Weak

OpenLDAP Software is a free, open source implementation of LDAP developed by the OpenLDAP Project.

Custom LDAP

Security level: Weak

Use Custom LDAP to customize the directory user identifier and directory member identifier, the attributes used in the LDAP server searches.

Windows Domain

Security level: Weak

If your organization operates a Windows primary domain controller (PDC) or backup domain controller (BDC), you can use it to provide weak authentication for login, SOCKS5, Telnet, FTP, HTTP, and SSH sessions to the Sidewinder. The PDC or BDC can be used to provide password authentication. Be sure the domain controller does not allow blank or default logins that can be easily guessed by outsiders.

You can also use transparent browser authentication. For more information about configuring your organization’s PDC or BDC to use transparent browser authentication on the Sidewinder appliance, see the related application note located at www.securecomputing.com/goto/appnotes.

Note: Transparent browser authentication is also known as NTLM or integrated Windows authentication.
RADIUS

Security level: Varies with the authentication server or method

If your organization operates a RADIUS server, you can use it to provide strong authentication for SOCKS5, Telnet, FTP, and HTTP sessions through the Sidewinder appliance. It can also be used to authenticate logins and SSH logins to the appliance. SafeWord RemoteAccess and SafeWord PremierAccess are RADIUS servers that have been certified for full interoperability with the appliance.

SafeWord

Security level: Strong

The SafeWord family of authentication servers that interoperate with the Sidewinder appliance includes SafeWord RemoteAccess and SafeWord PremierAccess.

With SafeWord PremierAccess, you can use fixed passwords or passcode authentication for Telnet and FTP sessions through the appliance, and for administrator login attempts directly to the appliance or through an SSH session. You can authenticate HTTP sessions using either fixed passwords or passcodes without the challenge/response option (not all tokens support this option).
The following table provides a reference to better understand each server’s authentication capabilities when interoperating with Sidewinder appliance.

**Table 22:** Authentication capabilities of SafeWord servers

<table>
<thead>
<tr>
<th>Feature/Capability</th>
<th>SafeWord RemoteAccess</th>
<th>SafeWord PremierAccess</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sidewinder appliance authentication methods supported</td>
<td>RADIUS only</td>
<td>SafeWord &amp; RADIUS</td>
</tr>
<tr>
<td>Fixed passwords</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Dynamic passcodes w/o challenge</td>
<td>Hardware tokens only</td>
<td>Hardware and software tokens</td>
</tr>
<tr>
<td>Dynamic passcodes with challenge</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Location of user database</td>
<td>Active Directory</td>
<td>SafeWord</td>
</tr>
<tr>
<td>Connectivity w/ Sidewinder appliance</td>
<td>RADIUS ports only</td>
<td>RADIUS ports or port 5030 (default)</td>
</tr>
</tbody>
</table>

This method is available with both SafeWord RemoteAccess and SafeWord PremierAccess.

The biggest advantages of using a tightly coupled configuration such as SafeWord PremierAccess authentication are the following:

- An improvement in performance over RADIUS
- The ability for PremierAccess to forward role information for a user from the PremierAccess database to the Sidewinder appliance. (While SafeWord PremierAccess can be connected to the appliance via standard RADIUS ports, configuration changes to the user’s role cannot be made available to the appliance.)

**Note:** SafeWord RemoteAccess is always connected to the Sidewinder appliance via the standard RADIUS protocol and therefore cannot be assigned the SafeWord authentication method. Aside from the ability to return a user’s role, SafeWord RemoteAccess provides equally strong user authentication via the RADIUS interface.
Alternate authentication methods

You can select only one authenticator in a rule. If you want alternate authentication methods for a service — for example, to ensure that you can connect to the Admin Console if an authentication server is down — you can create more rules for that connection.

To use an alternate authentication method:

1. Duplicate the rule allowing that connection and select a different authenticator for the duplicated rule.

2. Specify the alternate authentication method when logging in:
   - If it is an Admin Console connection, select the alternate method from the Authenticator drop-down list on the Login window.
   - If it is another service, at the login prompt, enter your user name followed by a colon and the name of the alternate authenticator:

     ```
     login_name:authenticator
     ```

Authentication scenario

In the following scenario, the user is authenticated using SafeWord PremierAccess, which implements a strong challenge/response authentication process. See Figure 134 for an illustration. (Note that the process is different for other authentication methods.)

1. A user tries to make a network connection via Telnet or FTP.
2. The Sidewinder appliance checks the rules to determine whether the connection between the source and destination addresses is allowed and to determine which authenticator to use.
3. If the connection is allowed, the proxy contacts the appropriate authenticator in the appliance.
4. The authenticator passes the login request to the appropriate authentication server. The authentication server checks the database to verify the user’s login name is registered.
5. The login challenge is sent to the user. Using client software or a hardware authenticator (token), the user types in the proper response to the prompt.
6. The appliance sends the response to the authentication server. The authentication server checks the response and informs the appliance to either accept or reject the login request.
Chapter 10: Authentication

Understanding authentication

Figure 134:
Authentication servers supported by the Sidewinder appliance
Configuring an authenticator

Authenticators validate a person’s identity before he or she is allowed to pass traffic through the appliance. There may be multiple authenticators for each authentication method.

Authenticators are configured on the Authenticators window. They can then be selected on the Rules window to authenticate proxy connections.

To configure an authenticator, select Policy > Rule Elements > Authenticators. The Authenticators window appears.

![Authenticators window](Image)

Use this window to create, modify, and delete authenticators that validate login attempts by administrators and proxy users.

The upper pane lists the existing authenticators. When you select an authenticator in the list, the properties of that authenticator appear in the lower pane.

**Note:** Passport and Password are default authenticators and cannot be deleted. They can be sorted with the rest of the list.
Use the toolbar and table in the upper pane to perform the following actions:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td>Create a new authenticator by clicking <strong>New</strong> and selecting an authenticator from the drop-down menu. A pop-up window appears where you set the appropriate properties.</td>
</tr>
<tr>
<td>Modify</td>
<td>To modify an existing authenticator, select an authenticator from the list and change the settings in the lower pane. To modify the settings in a pop-up window, click <strong>Modify</strong>. (Read-only administrators can click <strong>View</strong> to view an authenticator.)</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete an existing authenticator by selecting it in the list and clicking <strong>Delete</strong>. You cannot delete an authenticator if it is referenced by a rule.</td>
</tr>
<tr>
<td>Rename</td>
<td>Rename an authenticator by selecting it in the list and clicking <strong>Rename</strong>. Type the new name in the pop-up window and click <strong>OK</strong>. You cannot rename an authenticator if it is referenced by a rule.</td>
</tr>
<tr>
<td>Usage</td>
<td>View the areas that are currently using a particular authenticator by selecting it in the list and clicking <strong>Usage</strong>.</td>
</tr>
<tr>
<td>Find</td>
<td>Search for specific elements in the list by typing your search criteria in the <strong>Find</strong> field. Objects with matching elements appear in the list.</td>
</tr>
<tr>
<td>Manage Authentication Failures</td>
<td>Configure the authentication failure lockout feature by clicking <strong>Manage Authentication Failures</strong>. This opens a window where you can configure the appliance to block access to a user if the number of consecutive failed authentication attempts reaches a configured number. This protects unauthorized users from multiple attempts at guessing a user’s password.</td>
</tr>
</tbody>
</table>
For setting up specific authenticators, see the following:

- “Setting up Passport authentication” on page 304
- “Setting up standard password authentication” on page 309
- “Setting up SafeWord authentication” on page 322
- “Setting up LDAP authentication” on page 311
- “Setting up Windows domain authentication” on page 317
- “Setting up RADIUS authentication” on page 320
Setting up Passport authentication

Passport (also known as single sign-on) works in conjunction with a specified authentication method to cache a user’s initial authentication, thereby allowing access to multiple services with a single successful authentication to the Sidewinder appliance. Passport also allows authentication for encrypted services and services that do not handle authentication.

- Passport is a default authenticator. It cannot be deleted.
- The Passport rule is part of the initial active policy of the Sidewinder appliance and is enabled by default. The rule allows authentication to the Passport server. Do not modify this rule.

To set up Passport authentication: In the list in the upper pane of the Authenticators window, select Passport.

The Passport: General tab appears in the lower pane.

Figure 137: Passport: General tab

To configure the Passport authenticator:

1. Enter identifying information:
   - **Name** — You cannot change the name of the Passport authenticator.
   - **Type** — This shows the type of authenticator. You cannot modify this field.
   - **Description** — If desired, you can modify the description to help you more easily identify this authenticator.
2 Select Passport authenticators:

a In the Authenticators to establish Passport credentials list, select the authenticators you want to be available to use as Passport authenticators.

Configured authenticators populate this list. Authenticators selected here populate the Default authenticator drop-down list.

b From the Default authenticator drop-down list, select the authenticator used for rules that have Passport as the Authenticator.

• The default authenticator should be the authenticator most commonly used by users.
• Rules that use an authenticator other than the Passport authenticator, even if it is the Passport default authenticator, will require authentication for each attempted connection.
• Other authenticators selected in the Authenticators to establish Passport credentials table can be used as alternate Passport authenticators. See “Using an alternate Passport authentication method” on page 308 for details.

3 [Optional] If you want to require users to log in through the Passport web login page, select Require Web login.

4 [Optional] Set the port and banner messages for users who log in through the web login page:

• Port — Type the port number that will be used to log into the web. The default port is 8111.
• Login page banner — Click Edit to write or modify the message displayed for successfully logging into Passport through the web login page. Click View to see the banner.
• Logout page banner — Click Edit to write or modify the message displayed for successfully logging out of Passport through the web login page. Click View to see the banner.

See “Accessing the web login and logout pages” on page 307 for more information.

5 Set the timeout parameters for Passport users:

• Authenticate inactive users every — Set how long a user can be inactive before he or she must log into Passport again.
• Force authentication every — Set the length of time between mandatory authentications. This setting applies even if a user is currently active.

6 [Optional] Click the Manage Passports button to view the current Passport-authenticated (cached) users, and to expire user Passport authentication for one or more users.
7  [Optional] To restrict proxy connections to a specific group of users that are created and managed on the Sidewinder appliance, click the **Users and User Groups** tab to create a user group.

See “Authenticating groups from an internal group source” on page 329 for detailed information on users and user groups.

8  Save your changes.

**Managing Passports**

Use this window to view the current Passport-authenticated (cached) users. In this window, you have the option to revoke user Passport authentication for one or more users.

![Figure 138: Manage Passports window](image)

The following fields are displayed in the table:

- **Name** — This column displays the name(s) of all users who currently have cached authentication.

- **External Group** — [Conditional] This column displays the external group to which a user belongs. This applies only when a user authenticates with an authentication method that supports external groups.

- **Authenticator** — This column displays the type of authentication used by a user.

- **IP Address** — This column displays the source IP Address from which the authentication originated.

- **Issued** — This column displays the time at which a user was initially authenticated and obtained a Passport.

- **Last Used** — This column displays the time at which a user last accessed a service that required authentication.
You can immediately revoke Passport authentication for selected users by doing the following:

- To revoke the Passport authentication cache for all users listed in the table, click **Revoke All Passports**.
- To revoke the Passport for a single user or group of users, select the users you want to revoke by clicking the appropriate table row(s).
- To revoke multiple users, press and hold the **Ctrl** key as you select users. Then click **Revoke Passport(s)** to expire the selected users from the Passport.

When you revoke the Passport for users, those users will be required to re-authenticate before they can again access any Passport-authenticated service.

**Note:** Subsequent authentication requests by an expired user will be cached when they re-authenticate, allowing them to again use Passport authentication.

### Accessing the web login and logout pages

When Web Login is configured for Passport, any time a user attempts to access the web, the login window appears prompting them to authenticate. A user can also access the authentication login page by directing their browser to:

```
https://appliance_address:8111/sidewinder/login.html
```

If a user wants to log out of the Passport cache manually (before their Passport authentication cache expires), they can point their browser to:

```
https://appliance_address:8111/sidewinder/logout.html
```

If a browser is configured for the proxy, you will need to configure that browser to NOT proxy requests going to the appliance on port 8111. The following steps provide an example of configuring an exception using Netscape.

1. Open Netscape and select **Edit > Preferences > Advanced > Proxies**.
2. Select **Manual Proxy Configuration**.
3. In the **No Proxy For** field, type the URL for the appliance (for example, *sidewindername.example.com*).
4. Click **OK** to save the information and exit.
Using an alternate Passport authentication method

If you need to use an authentication method other than the default for Passport authentication (for backup or test purposes, for example), you can enter a configured authenticator at the login prompt.

• The name of the authenticator can be abbreviated as long as it is unique. For example, `pass` is ambiguous because it matches `Password` and `Passport`, but `passw` would make it unique.

• The name of the authenticator is case-insensitive.

1 Configure the alternate authentication method in the Authenticators window.

2 On the Passport: General tab, select the alternate authentication method in the Authenticators to establish Passport credentials list.

3 When you attempt a connection and the login prompt appears, enter your user name followed by a colon and the name of the alternate authenticator:

   `login_name:authenticator`
Setting up standard password authentication

Standard password authentication requires a user to enter the same password each time he or she logs in. The password is maintained in the user database on the Sidewinder appliance.

To set up standard password authentication: In the list in the upper pane of the Authenticators window, select Password.

Note: Password is a default authenticator. It cannot be deleted.

The Password: General tab appears in the lower pane.

To configure the Password: General tab:

1. Enter identifying information:
   - **Name** — You cannot change the name of the Password authenticator.
   - **Type** — This shows the type of authenticator. You cannot modify this field.
   - **Description** — If desired, you can modify the description to help you more easily identify this authenticator.

2. Configure the login settings:
   - **Login prompt** — Enter the text to appear asking for user identification.
   - **Password prompt** — Enter the text to appear asking for a password.
   - **Expiration message** — Enter the text to appear when a password has expired.
   - **Password expiration** — Enter the number of days a password remains valid.
   - **Maximum retries** — Enter the maximum number of login attempts allowed before the connection is dropped.
3 Configure the password requirements:

- **Minimum password length** — Enter the minimum number of characters a password must contain.
- **Allow simple passwords** — Select this option if you do not want to specify any other password requirements.
- **Require complex passwords** — Select this option to configure and enforce complex password requirements.
  - **Require # of the four character groups in every password** — Specify the number of character groups required for passwords. The character groups are:
    - lowercase
    - uppercase
    - numbers
    - special characters (all printable characters that can be typed from the keyboard, such as ^ % $ @ !, etc.)

If you specify 2, passwords must use characters from any two of the four character groups.

- **Require at least # character(s) per required group in every password** — Specify the number of characters required from each character group.

If you specify 3 characters from each group, and two character groups are required, passwords must contain three characters from two different groups, such as a13c7b.

4 [Optional] To restrict proxy connections to a specific group of users that are created and managed on the Sidewinder appliance, click the **Users and User Groups** tab to create a user group.

See “Authenticating groups from an internal group source” on page 329 for detailed information on users and user groups.

5 Save your changes.
Setting up LDAP authentication

Use LDAP (Lightweight Directory Access Protocol) to provide fixed password authentication for SOCKS5, Telnet, FTP, and HTTP sessions through the Sidewinder appliance. It can also be used to authenticate logins and SSH logins to the appliance.

There are four LDAP types you can use:

- **iPlanet** — Select this option if using an iPlanet LDAP server.
- **Active Directory** — Select this option if using an Active Directory LDAP server.
- **Open LDAP** — Select this option if using an Open LDAP server.
- **Custom LDAP** — Select this option to customize the Directory User Identifier and Directory Member Identifier.

To set up LDAP authentication: In the upper pane of the Authenticators window, click **New** and select the appropriate LDAP type from the drop-down list.

The LDAP: General tab appears. For more information, see:

- “About the LDAP: General tab” on page 312
- “About the LDAP: Search tab” on page 315
About the LDAP: General tab

Use this tab to configure your Sidewinder appliance to work with an LDAP server.

The left pane displays a list of any current LDAP servers currently configured for the Sidewinder appliance, with the following columns:

- **Rank** — Which server the appliance will try first.
  - If the server returns any response, no further servers are queried.
  - If the server does not respond, the next server in the list is tried.
- **Host** — The host IP address for the LDAP server.
- **Port** — The port number the LDAP server should use. The default port is 389.

Click a column heading to sort the list by that column's content. Click again to reverse the sort order.
To configure the LDAP: General tab:

1 Enter identifying information:
   • **Name** — Type a name to identify this authenticator. If you are modifying this authenticator, you cannot change the name.
   • **Type** — This shows the type of authenticator. You cannot modify this field.
   • **Description** — Type a description to help you more easily identify this authenticator.

2 Define and rank the LDAP servers.

   *Note:* The maximum number of LDAP servers allowed at one time is four.

You can do the following:

   • **Create a new server** — Click New and enter the IP address and port of the new LDAP server in the pop-up window. The default port is 389.
   • **Modify an existing server** — Select the server and click Modify. Make the desired changes in the pop-up window.
   • **Delete an existing server** — Select the server and click Delete.
   • **Rank the servers** — Select a server and use the up and down arrows to change the rank.

3 Select how the appliance will connect to LDAP servers by selecting one of the following options:

   • **Connect to server(s) anonymously** — Select this option if the LDAP server allows the appliance to connect and search subcontainers without providing login information.
   • **Connect to server(s) with username/password** — Select this option if the LDAP server requires the Sidewinder appliance to submit the specified user name and password in order to connect and search subcontainers.
     • **Username** — Type the login name required by the LDAP server.
     • **Password** — Type a password required by the LDAP server.
     • **Confirm password** — Type the password again.
   • **Server Timeouts/Retries** — Click this to configure the login and retry limits. Enter the maximum number of retries and the login timeout in seconds.
   • **Console and Telnet LDAP Logins** — Click this to specify what you want to appear as prompts during the login process. The defaults are `Username:` and `Password:`.
4  [Optional] Select a group source.
   • To create internally managed groups that you can specifically allow in
     proxy connections, select internal, then click the Users and User
     Groups tab.
     See “Authenticating groups from an internal group source” on page 329
     for detailed information on users and user groups.
   • To add externally created groups that you can specifically allow in proxy
     connections, select external, then click the Groups tab.
     See “Authenticating groups from an external group source” on page 327
     for information on external authentication groups.

5  Click Add or OK and save your changes.
About the LDAP: Search tab

Use this tab to define the search parameters for LDAP authentication.

1 [Custom LDAP only] Enter the LDAP identifiers:
   - **Directory user identifier** — Enter the attribute used in the LDAP database for user names. The LDAP server searches for a match on the user name assigned to this attribute.
   - **Directory member identifier** — Enter the attribute used in the LDAP database for group names. The LDAP server searches for a match on the group name assigned to this attribute.

   **Note:** In iPlanet, Active Directory, and OpenLDAP, these are default attributes that cannot be modified.

2 Define the search filter option:
   - **Do not filter searches** — Select this option to disable filtering of the LDAP or Active Directory tree.
   - **Only allow users that match this filter** — Select this option to filter users based on the profile filter displayed here.

3 Select which containers will be searched:
   - **Search in all containers and sub-containers** — Select this option to search all listed containers and their subcontainers.
   - **Search in defined containers only** — Select this option to limit searches to containers listed here.
   - [Active Directory only] **Search in Active Directory domains** — Select this option to search only in Active Directory domains listed here. Each domain must be listed separately.
You can perform the following actions:

- **Create a new search container** — Click New and make entries in the pop-up window. Enter either a single container name or a concatenated container name.

  **Note:** The search string format depends on the type of server selected. Microsoft Active Directory searches use a format similar to sales.example.com. Standard LDAP searches use a format similar to dc=sales,dc=example,dc=com.

- **Modify an existing search container** — Select the search container and click Modify. Make the desired changes in the pop-up window.

- **Delete an existing search container** — Select the search container and click Delete.

- **Change the search container’s rank** — Select the search container and use the up and down arrows.
Setting up Windows domain authentication

Use a Windows primary domain controller (PDC) or backup domain controller (BDC) to provide password authentication for login, SOCKS5, Telnet, FTP, HTTP, and SSH sessions to the Sidewinder appliance. You can also configure transparent browser authentication (NTLM) for browsers that support it.

**Important:** Be sure the domain controller does not allow blank or default logins that can be easily guessed by outsiders.

To set up Windows authentication: In the upper pane of the Authenticators window, click New and select Windows from the drop-down list.

The Windows: General tab appears.

![Figure 142: Windows: General tab](image)

The Windows domain controllers table lists the Windows domain controllers currently configured for the Sidewinder appliance.

- **Rank** — Which Windows domain controllers the appliance will try first.
  - If the server returns any response, no further servers are queried.
  - If the server does not respond, the next server in the list is tried.
- **IP Address** — The Windows domain controller’s IP address.
- **Port** — The port used by the Windows domain controller. The default port is 139 and cannot be changed.
- **Name** — The name of the Windows domain controller.

Click a column heading to sort the list by that column’s content. Click again to reverse the sort order.
To configure the Windows: General tab:

1 Enter identifying information:
   • **Name** — Type a name to identify this authenticator. If you are modifying this authenticator, you cannot change the name.
   • **Type** — This shows the type of authenticator. You cannot modify this field.
   • **Description** — Type a description to help you more easily identify this authenticator.

2 Define and rank the Windows domain controllers.

   *Note: The maximum number of Windows domain controllers allowed at one time is four.*

   You can do the following:
   • **Create a new controller** — Click **New** and make entries in the pop-up window:
     • **IP address** — Type the IP address used by the Windows domain controller.
     • **Windows domain controller name** — Type the name of the Windows domain controller. Type only the host or computer name, not the fully qualified name. (You can determine the name by going into the Network window on the Windows controller.)
     • **Port** — The port cannot be changed.
   • **Modify an existing controller** — Select the controller and click **Modify**. Make the desired changes in the pop-up window.
   • **Delete an existing controller** — Select the controller and click **Delete**.
   • **Rank the controllers** — Select a Windows domain controller and use the up and down arrows to change the rank.

3 Modify the Login options:
   • **Login prompt** — This is the login prompt that displays to users.
   • **Password prompt** — This is the password prompt that displays to users.
   • **Failed authentication message** — This is the message that displays if a user’s authentication attempt fails.
4 Select prompted or transparent browser authentication:
   • **Domain (MSNT)** — Select this option to prompt users for a user name and password. This is typically used for older browsers that do not support transparent authentication.

   **Security Alert:** *The user password is not encrypted in this method.*

   • **Transparent (NTLM)** — Select this option if you want transparent browser authentication. If a user has already been authenticated by the Windows domain, they are not prompted for a user name and password when using a rule that requires this authenticator.

   If this option is selected and the user’s browser does not support transparent authentication, the authentication will fail. No further rule matching is attempted.

   • **Both** — Select this option to attempt both authentication methods. Transparent authentication is attempted first. If it is not supported, domain authentication is used.

5 [Optional] To restrict proxy connections to a specific group of users that are created and managed on the Sidewinder appliance, click the **Users and User Groups** tab to create a user group.

   See “Authenticating groups from an internal group source” on page 329 for detailed information on users and user groups.
Setting up RADIUS authentication

RADIUS is a standard protocol used to authenticate users before they are allowed access to your system.

To set up RADIUS authentication: In the upper pane of the Authenticators window, click New and select RADIUS from the drop-down list.

The RADIUS: General tab appears.

![Figure 143: RADIUS: General tab](image)

The Radius Servers table lists the RADIUS servers currently configured for the Sidewinder. The columns indicate the following:

- **Rank** — Which server the appliance will try first.
  - If the server returns any response, no further servers are queried.
  - If the server does not respond, the next server in the list is tried.
- **IP address** — The host IP address for each server entry.
- **Port Number** — The port number for each server entry. The default port is 1812.
- **Shared Secret** — The text string or phrase that matches the shared secret of the listed RADIUS server.

Click a column heading to sort the list by that column’s content. Click again to reverse the sort order.
To configure the RADIUS: General tab:

1 Enter identifying information:
   - **Name** — Type a name to identify this authenticator. If you are modifying this authenticator, you cannot change the name.
   - **Type** — This shows the type of authenticator. You cannot modify this field.
   - **Description** — Type a description to help you more easily identify this authenticator.

2 Define and rank the RADIUS servers.

   *Note: The maximum number of RADIUS servers allowed at one time is four.*

   You can do the following:
   - **Create a new server** — Click **New** and make entries in the pop-up window:
     - **IP address** — Type the host IP address for each server entry.
     - **Port Number** — Type the port number for each server entry. The default port is 1812.
     - **Shared Secret** — Type the text string or phrase that matches the shared secret of the listed RADIUS server.
   - **Modify an existing server** — Select the controller and click **Modify**. Make the desired changes in the pop-up window.
   - **Delete an existing server** — Select the controller and click **Delete**.
   - **Rank the servers** — Select a server and use the up and down arrows to change the rank.

3 Modify the Login options:
   - **Login prompt** — This is the login prompt that displays to users when they log in using RADIUS.
   - **Password prompt** — This is the password prompt that displays to users when they log in using RADIUS.
   - **Failed authentication message** — This is the message that displays if a user’s authentication attempt fails.

4 [Optional] Select a group source.
   - To create internally managed groups that you can specifically allow in proxy connections, select **internal**, then click the **Users and User Groups** tab.
     
     See “Authenticating groups from an internal group source” on page 329 for detailed information on users and user groups.

   - To add externally created groups that you can specifically allow in proxy connections, select **external**, then click the **Groups** tab.
     
     See “Authenticating groups from an external group source” on page 327 for information on external authentication groups.
Setting up SafeWord authentication


- To configure SafeWord PremierAccess authentication on the Sidewinder appliance, you must first install and configure the SafeWord PremierAccess Authentication Server. Refer to the appropriate product documentation.
- To configure SafeWord RemoteAccess authentication, use the RADIUS authenticator. See “Setting up RADIUS authentication” on page 320 for more information.

To set up SafeWord authentication: In the upper pane of the Authenticators window, click **New** and select **SafeWord** from the drop-down list.

The SafeWord: General tab appears.

![SafeWord: General tab](image)

The left pane displays a list of SafeWord servers currently configured for the Sidewinder, with the following columns:

- **Rank** — Which server the Sidewinder appliance will try first.
  - If the server returns any response, no further servers are queried.
  - If the server does not respond, the next server in the list is tried.
- **IP Address** — The host IP address for each server entry.
- **Port** — The port number for each server entry. The default port number for SafeWord PremierAccess is 5030.

Click a column heading to sort the list by that column’s content. Click again to reverse the sort order.
To configure the SafeWord: General tab:

1 Enter identifying information:
   • Name — Type a name to identify this authenticator. If you are modifying this authenticator, you cannot change the name.
   • Type — This shows the type of authenticator. You cannot modify this field.
   • Description — Type a description to help you more easily identify this authenticator.

2 Define and rank the SafeWord servers.

   Note: The maximum number of SafeWord servers allowed at one time is four.

   You can do the following:
   • Create a new SafeWord server entry — Click New and enter the IP address and port in the pop-up window. The default port number for SafeWord PremierAccess is 5030.
   • Modify an existing server entry — Select the server and click Modify. Make the desired changes, then click OK.
   • Delete an existing entry — Select the entry and click Delete.
   • Rank the servers — Select a server and use the up and down arrows to change the rank.

3 [Optional] Select a group source.
   • To create internally managed groups that you can specifically allow in proxy connections, select internal, then click the Users and User Groups tab.
     See “Authenticating groups from an internal group source” on page 329 for detailed information on users and user groups.
   • To add externally created groups that you can specifically allow in proxy connections, select external, then click the Groups tab.
     See “Authenticating groups from an external group source” on page 327 for information on external authentication groups.

4 Click Add or OK and save your changes.
Telnet and FTP considerations

There are some special considerations that users should be made aware of regarding Telnet and FTP authenticated connections through the Sidewinder appliance.

- **Changing user passwords and PINs for authentication methods**
  
  The Sidewinder appliance supports changing user passwords and PINs only under the Telnet proxy. For example, users can change their SafeWord PremierAccess PIN via the Telnet proxy. (Refer to the documentation for your authentication method for information on the commands used to change passwords and PINs.) Passwords and PINs cannot be changed using the FTP, HTTP, or SOCKS5 proxy. The user must either initiate a Telnet proxy session or they can contact their system administrator.

- **Switching authentication methods during a login session**
  
  The appliance allows you to use multiple authentication methods for a given service (for example, users might use SafeWord PremierAccess or Password for Telnet authentication). When logging in, if a user specifies the incorrect authentication method and authenticator, they can change to another authentication method by typing `:authenticator` after the user name.

- **Non-authenticated nontransparent FTP proxy prompts for authentication**
  
  Administrators should instruct end users that they will be prompted to supply a user name, authentication method, and destination, even if the associated allow rule does not require authentication. This is because the non-transparent FTP proxy needs the login and destination information in order to determine which rule will allow the connection.

  When end users attempt to connect to the FTP server, the appliance sends them the following prompt:

  220-Firewall ftp proxy. You must login to the proxy first.
  220 Use proxy-user:auth-method@destination.
  Name (si_ipaddr:proxy-user):

  Instruct users to respond to the `Name (si_ipaddr:username):` prompt by entering the @ sign followed by the FTP server’s IP address, as shown in this example:

  Name (si_ipaddr:proxy-user):@172.1.1.25

  Users who incorrectly put a user name before the prompt are still allowed access to the FTP server through the non-transparent FTP rule that does not require authentication. The appliance handles entries containing user names that do not match any existing FTP rule and entries without a user name in the same manner.
Setting up users to change their own passwords

The appliance changepw server allows users to use a web browser to change their Sidewinder appliance, SafeWord PremierAccess, or LDAP login password.

To allow this process, you must do the following:

• Create a change password rule that allows users to change their passwords.
• Inform users how they can change their own passwords using a web browser.

Create a change password rule

To create a change password rule: Select Policy > Rules and select the appropriate settings from the table below.

Table 24: Proxy rule settings to allow users to change their login passwords

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action:</td>
<td>Allow</td>
</tr>
<tr>
<td>Service:</td>
<td>changepw</td>
</tr>
<tr>
<td>Source Burb:</td>
<td>Desired curb (for example, internal)</td>
</tr>
<tr>
<td>Destination Burb:</td>
<td>Desired curb (for example, internal)</td>
</tr>
<tr>
<td>Source Endpoint:</td>
<td>Site dependent</td>
</tr>
<tr>
<td>Destination Endpoint:</td>
<td>localhost (a default host object)</td>
</tr>
<tr>
<td>Redirect:</td>
<td>Firewall (IP)</td>
</tr>
</tbody>
</table>
How users can change their own password

Using standard password authentication, you can authenticate trusted and Internet users who request SOCKS5, FTP, HTTP, and Telnet access via proxies. As an administrator, you should inform those users how they can change their own password from their terminal or workstation by using a web browser. However, there are some restrictions:

- Users can change their own password only if using standard password, SafeWord PremierAccess, or LDAP authentication.
- To allow users to change their login passwords, you must first create a rule for the appliance to allow this.

1 Start a web browser.

2 Configure your browser not to proxy requests going to the appliance on port 1999. For example, if you are using a Netscape browser do the following:
   a Open Netscape and select Edit > Preferences > Advanced > Proxies.
   b Select Manual Proxy Configuration.
   c In the No Proxy For field, type the URL for the appliance (for example, mysidewinder.example.com).
   d Click OK to save the information and exit.

3 Open an HTTP connection to the Sidewinder appliance. For example:
   http://mysidewinder.example.com:1999/
   A pre-defined HTML change password form appears.

4 Enter your user name.

5 Enter your current password. This is your current password for establishing network connections.

6 Enter your new password. This will be your new password for establishing network connections.

7 Re-enter the new password. This confirms the spelling of the new password.

8 Select one of the following password types:
   - If you are changing a Sidewinder appliance login password, select Password.
   - If you are changing a SafeWord PremierAccess login password, select SafeWord.
   - If you are changing an LDAP password, select LDAP.

9 Click Send Request.
   This sends the change password request to the appliance. You will be notified if the request failed or if it is accepted. If the request is accepted, the password database is updated and the new password must be used for all future connections.
Authenticating groups from an external group source

A group is a logical grouping of one or more users, identified by a single name. You can restrict proxy connections to specific groups created and managed on an external authentication server.

You can authenticate groups from external servers using LDAP, RADIUS, and Safeword authenticators:

- A group is created on an external authentication server. In the Admin Console, you add the matching group name on the Groups tab of an LDAP, RADIUS, or Safeword authenticator.
- When you select this authenticator in the Rules window, you can also select one or more groups that were added to the Groups tab. Proxy connections are restricted to users in the matching group(s) on the external authentication server.
- An external group added to an authenticator is not available globally. An external group is unique to the authenticator it is added to. If you want to use the same group for another authenticator, it must also be added to the Groups tab of that authenticator.

To add or modify external group names to an authenticator:

2. Open a new or existing LDAP, RADIUS, or Safeword authenticator window:
   - Click New and select the appropriate authenticator.
   - In the upper pane, select an existing authenticator.
3. On the General tab, select the external group source.
   
   **Note:** If the authenticator is being used in a rule, you cannot change the group source.

4. Click the Groups tab.

Figure 145: Authenticator: Groups tab
You can perform the following actions:

- **Add a new external group** — Click New, then type the name of a group that matches the group name residing on an external LDAP, RADIUS, or SafeWord authentication server. If you enter multiple groups, put each group on a separate line.

- **Modify an existing external group** — Select an external group name and click Modify, then make the appropriate changes in the Modify Group window.

- **Delete an existing external group** — Select an external group name and click Delete.

RADIUS group options [RADIUS authenticators only]:

Enter the attributes defined in the dictionary files on the RADIUS server. The Sidewinder appliance looks for these attributes in the RADIUS server's response.

- **Group type** — Enter an attribute type. The default is 26, which is a vendor-specific attribute.
  - **Vendor ID** — If the group type is 26, enter a vendor ID from the RADIUS server's dictionary files.
  - **Vendor type** — If the group type is 26, enter a vendor type from the RADIUS server's dictionary files.

- **Group delimiters** — If the RADIUS server sends attributes in a single string, enter the character(s) that separate the groups in the string. Multiple characters can be entered in this field consecutively, with no space or separators.

Save your changes.
A user is a person who uses the networking services provided by the Sidewinder appliance. A user group is a logical grouping of one or more users, identified by a single name. You can restrict proxy connections to specific groups created and managed on the Sidewinder appliance.

You can authenticate user groups using any Sidewinder authenticator.

- You create users and add them to user groups on the Authenticators windows.
- When you select an authenticator on the Rules window, you can also select one or more of these groups. Proxy connections are restricted to users in the selected group(s).
- Users and groups created on the Users and User Groups tab of an authenticator are available to all authenticators.

**Important:** When using an internal group source, users created and maintained on the Sidewinder appliance for LDAP, RADIUS, Windows, or Safeword authenticators must also be maintained on their external servers.

- You create administrators in the Administrator Accounts window. All administrator accounts that are created appear in the Users and User Groups tab.
  - On a newly installed appliance, the only user to appear in the Users and User Groups tab is the administrator created during installation.
  - If you delete an administrator in the Administrator Accounts window, that administrator is also deleted from the Users and User Groups tab.
  - If you delete an administrator in the Users and User Groups tab, that administrator is also deleted from the Administrator Accounts window.

To add or modify users and user groups:

1. Select **Policy > Rule Elements > Authenticators**.
2. Open a new or existing authenticator window:
   - Click **New** and select the appropriate authenticator.
   - In the upper pane, select an existing authenticator.
3. On the General tab, select the **internal** group source (not necessary for Passport, Password, and Windows authenticators).

**Note:** If the authenticator is being used in a rule, you cannot change the group source.
4 Click the Users and User Groups tab.

![Figure 146: Users and User Groups tab](image)

To manage the list of users and user groups:

- Display only users (Users), only groups (Groups) or both users and groups (All) by using the Show drop-down list.
- Filter the list by typing letters in the Find field. Only users or user groups that contain the corresponding string of letters appear in the list. For example, if you type br in the Find field, only users and groups whose name contains “br” will appear in the list. The Find field is case sensitive.
- To see which areas of the appliance are using a selected user or group, select the entry in the list and click Usage.

You can perform the following tasks in this window:

- “Create a new user” on page 330
- “Create a new group” on page 331
- “Modify an existing user or user group” on page 331
- “Block consecutive failed authentication attempts” on page 331
- “Delete an existing user or user group” on page 332

**Create a new user**

1 In the lower pane, click New. The Create New User/Group window appears.
2 Select New User.
3 Select a template: Select Use empty template or select a user from the list and select Copy from an existing user.
4 Click OK. The User Objects window appears.
5 Enter the appropriate information for the new user.
6 Click OK, then save your changes.
Create a new group

From the Users and User Groups tab:

1. In the lower pane, click New. The Create New User/Group window appears.
3. Click OK. The Group Objects window appears.
4. Enter the appropriate information for the new user group.
5. Click OK, then save your changes.

For more information, see:

- “About the Create New User/Group window” on page 332
- “About the Group Objects: Group Information tab” on page 334
- “About the User Objects: User Information tab” on page 336

Modify an existing user or user group

From the Users and User Groups tab:

1. In the lower pane, select a user or user group from the list. If necessary, use the Show drop-down list or the Find field to narrow the list choices.
2. Click Modify. The User Objects or Group Objects window appears.
3. Make the necessary changes.
4. Click OK, then save your changes.

For more information, see:

- “About the Group Objects: Group Information tab” on page 334
- “About the User Objects: User Information tab” on page 336

Block consecutive failed authentication attempts

From the Authenticators window:

1. From the toolbar, click Manage Authentication Failures. The Authentication Failure Lockout Properties window appears.
2. Select Enable to enable the lockout feature.
3. In the Lockout Threshold field, type the number of failed login attempts allowed for a single user before that user is locked out of the appliance.
4. [Conditional] To clear the lock for a user, select the user and click Clear. Click Clear All to clear all users in the list.

For more information, see “About the Authentication Failure Lockout Properties window” on page 338.
Delete an existing user or user group

From the Users and User Groups tab:

1. Select a user or user group from the list. If necessary, use the Show drop-down list or the Find field to narrow the list choices.
2. Click Delete. Save your changes.

*Note: If you select an administrator to delete, that administrator will also be deleted from the Administrator Accounts window.*

About the Create New User/Group window

Use this window to select whether you want to create a user or a user group. The selections you make in this window will open the appropriate window to enter information.

![Figure 147: Create New User/Group window](image-url)
1 Select one of the following options in the Create field:
   • New User — Select this option to create a new user.
   • New Group — Select this option to create a new user group.

2 [New User only] Select a source:
   • If you want to enter all new information, select Use empty template.
   • If you want to create a new user account using the information contained in an existing user account, select the Copy from existing user option and then select the user account that you want to copy.

   This option will copy the following information fields from the existing user’s account:
   • Organization
   • User Fields 1–4
   • Description
   • Employee ID
   • Group Membership

   You will still need to enter information for the Username and Password, as these fields contain information specific to each individual user.

3 Click OK.
   • If you are creating a new user group, the Group Objects window appears. See “About the Group Objects: Group Information tab” on page 334.
   • If you are creating a new user, the User Objects window appears. See “About the User Objects: User Information tab” on page 336.
Chapter 10: Authentication
Authenticating groups from an internal group source

About the Group Objects: Group Information tab

Use this tab to create or modify user groups.

Figure 148: Group Objects: Group Information tab

- **Group Name** — Type a name for this group.
  - Valid values include alphanumeric characters, periods (.), dashes(-), underscores (_), and spaces ( ).
  - The first and last character of the name must be alphanumeric.
  - The name cannot exceed 100 characters.

  **Note:** You cannot edit the name of an existing group from this window. To change a group name, delete the group and add it back using the new name. Be sure to add the group back to any rules that used the deleted group name.

- [Optional] **Comments** — Type additional information about the user group.

Use the User Group Membership tab to add or remove users or groups as members of this group.

When you are done creating or modifying this user group, click **OK** and save your changes.
About the Group Objects: User Group Membership tab

Use this tab to add or remove users or groups as members of this group. A group within a group is called a nested group.

To filter the list:

- Use the Show drop-down list to display only users (Users), only groups (Groups) or both users and groups (All).
- Filter the list by typing letters in the Find field. Only users or user groups that contain the corresponding string of letters appear in the list. For example, if you type br in the Find field, only users and groups whose name contains “br” will appear in the list. The Find field is case sensitive.

To add or remove members of the selected group:

- To add a user or group as a member of this group, select an entry in the Available Users and Groups list, and then click the > arrow button. Select multiple consecutive entries by pressing the Shift key as you select the entries. To select multiple non-consecutive entries, press the Ctrl key as you select the desired entries.
- To remove a user or group from this group, select the entry in the Current Group Members list, and then click the < arrow button.

Use the Group Information tab to enter information about the current group.

When you are done creating or modifying this user group, click OK and save your changes.
Chapter 10: Authentication

Authenticating groups from an internal group source

About the User Objects: User Information tab

Use this tab to enter descriptive information about a user.

![Figure 150: User Objects: User Information tab](image)

You can perform the following actions in this window:

- **Username** — Type the name the user will enter when he or she requests a connection that requires authentication. This entry can consist of up to 16 alphanumeric characters (upper or lower case). Apostrophes are not allowed (for example, *O'Hare*).

- [Optional] **Description** — Type any information about the user that may be helpful.

- [Optional] **Employee ID** — Type an employee ID number, if applicable.

- [Optional] **Organization** — Type the organization that the user is associated with, if applicable.

- [Optional] **User Field 1–4** — Enter any additional information that your organization requires. For example, if you will be generating chargeback reports for authenticated FTP, Telnet, or HTTP connections, you might enter account numbers in these fields.

  You cannot modify the field names.

Use the **User Password** tab to enter password information for a user.

When you are done creating or modifying this user, click **OK** and save your changes.
About the User Objects: User Password tab

Use this tab to enter password information for a user.

**Note:** This password is used only for the Password authenticator. For other authenticators, the password is determined on the external server.

---

**Figure 151:** User Objects: User Password tab

- **Password** — Create the user's password using one of these methods:
  - Manually create a password — If you want to manually create a password, type a password in the Password field, then retype the password in the Confirm Password field. The password must not exceed 64 characters.
  - Automatically generate a password — If you want the Sidewinder to automatically create a password, click Generate Password. Be sure to note the password that appears in the Generated Password window before clicking OK. Once you click OK, the password will no longer be visible, but can be changed at any time.

- **Expire Password** — Click this if you want the user's password to expire so they are required to change it. The Expire Password button changes to a Reinstate Password button.

- **Reinstate Password** — Click this if you need to re-instate a user's expired password. The Reinstate Password button changes to an Expire Password button.

- **Discard Password Info** — Click this to delete a user's password account from the database. For example, this can be used if you are changing a user's authentication method from password to SafeWord and need to remove the previous password information.
Use the **User Information** tab to enter descriptive information about a user.

When you are done creating or modifying this user, click **OK** and save your changes.

**About the Authentication Failure Lockout Properties window**

Use this window to configure the authentication failure lockout feature on your Sidewinder appliance. This feature allows you to configure the appliance to block access to a user if the number of consecutive failed authentication attempts reaches a configured number. This protects unauthorized users from multiple attempts at guessing a user’s password.

![Figure 152: Authentication Failure Lockout Properties window](image)

You can perform the following actions:

1. **Enable or disable the lockout feature** — To enable this feature, select the **Enable** radio button. To disable this feature, select the **Disable** radio button. When this feature is enabled, any time a user account reaches the specified authentication attempt threshold without a successful authentication, that user will be locked out until the lock is cleared by an administrator. The lock can also be cleared if the locked out administrator logs in at the appliance using the correct login information.

2. **View locked out users** — The **Locked Out Users** area lists any users who are currently locked out of the appliance due to exceeded authentication failures. It will also display the number of failed login attempts for each user.

---

**Important:** If all administrators become locked out of the appliance, see “Manually clearing an authentication failure lockout” on page 824.
• **Configure the lockout threshold** — Use the Lockout Threshold field to specify the number of failed login attempts that can occur for a single user account before that user is locked out of the appliance.

  *Note:* When a user is locked out, their authentication method will become invalid. They will **not** be notified that they are locked out.

• **Clear user locks** — To clear the lock for a user, select the user and click **Clear**. Click **Clear All** to clear all users in the list.

---

**Figure 153:** Locked-out user displayed in Authentication Failure Lockout Properties window
Chapter 10: Authentication

*Authenticating groups from an internal group source*
In this chapter...

Viewing Network Defense information .............................................342
Configuring the TCP Network Defense ..........................................345
Configuring the IP Network Defense ............................................347
Configuring the UDP Network Defense ........................................349
Configuring the ICMP Network Defense ......................................351
Configuring the ARP Network Defense .......................................353
Configuring the IPsec Network Defense tab .................................355
Network defenses allow you to control the audit output for suspicious traffic at the data link, network, and transport layers that is detected by the Sidewinder appliance when the appliance automatically prevents that traffic from entering the appliance. Some traffic is stopped because a packet, or sequence of packets, resembles a known attack. Other traffic is stopped because a packet does not comply with its protocol's standards. If network defenses are enabled, the audit reports provide detailed information on the denied traffic.

Figure 154: What happens when a network defense is enabled

When network defenses are enabled and the appliance recognizes an attack, it stops the attack and generates an IPS attack audit event.

If network defenses are not enabled, the appliance still stops suspicious traffic but does not generate audit.

Figure 155: What happens when a network defense is disabled

When network defenses are disabled, the appliance stops the attack but does not generate audit.

Once you decide that you want to view these denied packets' audit, you can configure the following options:

- Audit packets that the appliance determines to be part of an identifiable attack based on attack description (bad header length, bad redirect, etc.).
- Audit packets that are not specifically identified as a potential attack yet are not compliant with their protocol standards at the following levels:
  - All packets that do not comply with their protocol’s standards.
  - Packets that do not comply with their protocol’s standards and have been identified as a severe or moderate risk to your network.
  - Packets that do not comply with their protocol’s standards and have been identified as a severe risk to your network.
  - Do not generate audit when the appliance stops a packet because it does not comply to its protocol’s standard.
Network defenses represent one element of the appliance’s audit capabilities. Information about additional auditing tools can be found in the following chapters:

- Chapter 15, "The Dashboard" on page 431
- Chapter 12, "Auditing" on page 359
- Chapter 13, "IPS Attack and System Event Responses" on page 399

To view the Network Defenses, select Policy > Network Defenses. The Network Defenses window displays with the TCP tab displayed, as shown in Figure 156. All tabs are similar in appearance and function.

The Network Defenses tabs allows you to configure what audit the appliance generates for each of the specified protocols and how frequently to generate that audit.

For information on configuring a specific Network Defense, see the following:

- TCP (page 345)
- IP (page 347)
- UDP (page 349)
- ICMP (page 351)
- ARP (page 353)
- IPsec (page 355)
If you want to return the Network Defense settings to their defaults, click **Restore Defaults**. The following window appears:

![Network Defenses: Restore default values window](image)

This window allows you to restore the network defenses’ attack and protocol compliance issue settings to their system defaults. When the window appears, all network defenses are selected.

- If you want to restore the defaults for all network defenses, click **OK**.
- If you want to restore the defaults for selected network defenses, clear the check box next to the network defenses that need to keep their current settings. After clearing the appropriate check box(es), click **OK**.

The selected network defenses now display and enforce their default settings.
The TCP Network Defense allows you to customize audit output for TCP attacks and compliance issues stopped by the appliance. To configure the TCP Network Defense, select **Policy > Network Defenses > TCP**. The following window appears:

**Figure 158: Network Defenses: TCP tab**

### TCP Auditor

Use this tab to configure what audit to generate for TCP attack and compliance issues. The appliance automatically stops all listed attacks; selecting or clearing a check box only affects whether or not this behavior is audited.

1. In the **Audit the selected TCP attacks** section, select the attacks for which you want the appliance to generate audit.

2. In the **Audit the selected TCP compliance issues** area, select how you want the appliance to audit packets that are not known attacks, but are still not compliant with the TCP standards. Options are:
   - All TCP compliance issues
   - Severe and moderate TCP compliance issues
   - Severe TCP compliance issues
   - Do not audit any TCP compliance issues

Use this tab to configure what audit to generate for TCP attack and compliance issues. The appliance automatically stops all listed attacks; selecting or clearing a check box only affects whether or not this behavior is audited.
3 In the **TCP Audit Frequency** area, select how often to generate audit for TCP issues. Select one of the following:

- **Limit auditing (recommended)** — Generates an audit record for the first $x$ occurrences for every $y$ seconds. Other occurrences of the same audit event in that window will not be recorded. An additional audit event will be generated to record how many other audit events were suppressed.

For example, the audit is limited to generating an audit event for the first three (3) occurrences for every 60 seconds. If the appliance stopped 100 SYN-ACK probes in 60 seconds, then it generates three records for the first three denials, and then generates another audit record stating that 97 occurrences were suppressed in that 60 second window.

Limiting audit in this manner reduces system load.

- **Always audit** — Generates an audit record for every audit event.

**Caution:** Unlimited auditing runs the risk of overflowing the log partition and creating problems for the appliance.

Options for viewing the audit output generated by these selections include:

- The Admin Console **Dashboard**
- **Monitor > Audit**
- SecurityReporter
- Third-party reporting tools
The IP Network Defense allows you to customize audit output for IP attacks stopped by the appliance. To configure the IP Network Defense, select **Policy > Network Defenses > IP**. The following window appears:

![Network Defenses: IP tab](image)

Use this tab to configure what audit to generate for IP attack and compliance issues. The appliance automatically stops all listed attacks; selecting or clearing a check box only affects whether or not this behavior is audited.

1. In the **Audit the selected IP attacks** section, select the attacks for which you want the appliance to generate audit.

2. In the **Audit the selected IP compliance issues** area, select how you want to audit packets that are not known attacks, but are still not compliant with the IP standards. Options are:
   - All IP compliance issues
   - Severe and moderate IP compliance issues
   - Severe IP compliance issues
   - Do not audit any IP compliance issues
3 In the **IP Audit Frequency** area, select how often to generate audit for IP issues. Select one of the following:

- **Limit auditing (recommended)** — Generates an audit record for the first \( x \) occurrences for every \( y \) seconds. Other occurrences of the same audit event in that window will not be recorded. An additional audit event will be generated to record how many other audit events were suppressed.

For example, the audit is limited to generating an audit event for the first three (3) occurrences for every 60 seconds. If the appliance stopped 100 source routed packets in 60 seconds, then it generates three records for the first three denials, and then generates another audit record stating that 97 occurrences were suppressed in that 60 second window.

Limiting audit in this manner reduces system load.

- **Always audit** — Generates an audit record for every audit event.

| Caution: Unlimited auditing runs the risk of overflowing the log partition and creating problems for the appliance. |

Options for viewing the audit output generated by these selections include:

- The Admin Console **Dashboard**
- **Monitor > Audit**
- SecurityReporter
- Third-party reporting tools
Configuring the UDP Network Defense

The UDP Network Defense allows you to customize audit output for UDP attacks stopped by the appliance. To configure the UDP Network Defense, select Policy > Network Defenses > UDP. The following window appears:

Use this tab to configure what audit to generate for UDP attack and compliance issues. The appliance automatically stops all listed attacks; selecting or clearing a check box only affects whether or not this behavior is audited.

1. In the **Audit the selected UDP attacks** section, select the attacks for which you want the appliance to generate audit.

2. In the **Audit the selected UDP compliance issues** area, select how you want the appliance to audit packets that are not known attacks, but are still not compliant with the UDP standards. Options are:
   - All UDP compliance issues
   - Severe and moderate UDP compliance issues
   - Severe UDP compliance issues
   - Do not audit any UDP compliance issues
3 In the **UDP Audit Frequency** area, select how often to generate audit for UDP issues. Select one of the following:

- **Limit auditing (recommended)** — Generates an audit record for the first $x$ occurrences for every $y$ seconds. Other occurrences of the same audit event in that window will not be recorded. An additional audit event will be generated to record how many other audit events were suppressed.

  For example, the audit is limited to generating an audit event for the first three (3) occurrences for every 60 seconds. If the appliance stopped 100 zero source port UDP attacks in 60 seconds, then it generates three records for the first three denials, and then generates another audit record stating that 97 occurrences were suppressed in that 60 second window.

  Limiting audit in this manner reduces system load.

- **Always audit** — Generates an audit record for every audit event.

  **Caution:** Unlimited auditing runs the risk of overflowing the log partition and creating problems for the appliance.

Options for viewing the audit output generated by these selections include:

- The Admin Console **Dashboard**
- **Monitor > Audit**
- SecurityReporter
- Third-party reporting tools
Configuring the ICMP Network Defense

The ICMP Network Defense allows you to customize audit output for ICMP attacks stopped by the appliance. To configure the ICMP Network Defense, select Policy > Network Defenses > ICMP. The following window appears:

![Network Defenses: ICMP tab](image)

Use this tab to configure what audit to generate for ICMP attack and compliance issues. The appliance automatically stops all listed attacks; selecting or clearing a check box only affects whether or not this behavior is audited.

1. In the **Audit the selected ICMP attacks** section, select the attacks for which you want the appliance to generate audit.

2. In the **Audit the selected ICMP compliance issues** area, select how you want the appliance to audit packets that are not known attacks, but are still not compliant with the ICMP standards. Options are:
   - All ICMP compliance issues
   - Severe and moderate ICMP compliance issues
   - Severe ICMP compliance issues
   - Do not audit any ICMP compliance issues
3 In the ICMP Audit Frequency area, select how often to generate audit for ICMP issues. Select one of the following:

- **Limit auditing (recommended)** — Generates an audit record for the first \( x \) occurrences for every \( y \) seconds. Other occurrences of the same audit event in that window will not be recorded. An additional audit event will be generated to record how many other audit events were suppressed.

For example, the audit is limited to generating an audit event for the first three (3) occurrences for every 60 seconds. If the appliance stopped 100 invalid redirect ICMP attacks in 60 seconds, then it generates three records for the first three denials, and then generates another audit record stating that 97 occurrences were suppressed in that 60 second window.

Limiting audit in this manner reduces system load.

- **Always audit** — Generates an audit record for every audit event.

**Caution:** Unlimited auditing runs the risk of overflowing the log partition and creating problems for the appliance.

Options for viewing the audit output generated by these selections include:

- The Admin Console **Dashboard**
- **Monitor > Audit**
- SecurityReporter
- Third-party reporting tools
The ARP Network Defense allows you to customize audit output for ARP attacks stopped by the appliance. To configure the ARP Network Defense, select **Policy > Network Defenses > ARP**. The following window appears:

Use this tab to configure what audit to generate for ARP compliance issues. The appliance automatically stops all listed attacks; selecting or clearing a check box only affects whether or not this behavior is audited.

1. In the **Audit the selected ARP compliance issues** area, select how you want the appliance to audit packets that are not known attacks, but are still not compliant with the ARP standards. Options are:
   - All ARP compliance issues
   - Severe and moderate ARP compliance issues
   - Severe ARP compliance issues
   - Do not audit any ARP compliance issues
In the ARP **Audit Frequency** area, select how often to generate audit for ARP issues. Select one of the following:

- **Limit auditing (recommended)** — Generates an audit record for the first \(x\) occurrences for every \(y\) seconds. Other occurrences of the same audit event in that window will not be recorded. An additional audit event will be generated to record how many other audit events were suppressed.

  For example, the audit is limited to generating an audit event for the first three (3) occurrences for every 60 seconds. If the appliance stopped 100 ARP attacks in 60 seconds, then it generates three records for the first three denials, and then generates another audit record stating that 97 occurrences were suppressed in that 60 second window.

  Limiting audit in this manner reduces system load.

- **Always audit** — Generates an audit record for every audit event.

  **Caution:** Unlimited auditing runs the risk of overflowing the log partition and creating problems for the appliance.

Options for viewing the audit output generated by these selections include:

- The Admin Console **Dashboard**
- **Monitor > Audit**
- SecurityReporter
- Third-party reporting tools
The IPsec Network Defense allows you to customize audit output for IPsec attacks stopped by the appliance. Unlike the other network defenses, it also allows you to control non-malicious failure audits. To configure the IPsec Network Defense, select Policy > Network Defenses > IPsec. The following window appears:

Use this tab to configure what audit to generate for IPsec attacks, non-malicious failures, and compliance issues. The appliance automatically stops all listed attacks; selecting or clearing a check box only affects whether or not this behavior is audited.

Note: The IPsec Network Defense allows you to directly control audit output for some non-malicious failures because IPsec tends to have more of these types of failures than other protocols.

1. In the **Audit the selected IPsec attacks** section, select the attacks for which you want to generate audit.

2. In the **Audit the selected IPsec compliance issues** area, select how you want to audit packets that are not known attacks, but are still not compliant with the IPsec standards. Options are:
   - All IPsec compliance issues
   - Severe and moderate IPsec compliance issues
   - Severe IPsec compliance issues
   - Do not audit any IPsec compliance issues
3 In the **IP Audit Frequency** area, select how often to generate audit for IPsec issues. Select one of the following:

- **Limit auditing (recommended)** — Generates an audit record for the first \( x \) occurrences for every \( y \) seconds. Other occurrences of the same audit event in that window will not be recorded. An additional audit event will be generated to record how many other audit events were suppressed.

  For example, the audit is limited to generating an audit event for the first three (3) occurrences for every 60 seconds. If the appliance stopped 100 decryption failures in 60 seconds, then it generates three records for the first three denials, and then generates another audit record stating that 97 occurrences were suppressed in that 60 second window.

  Limiting audit in this manner reduces system load.

- **Always audit** — Generates an audit record for every audit event.

  **Caution:** Unlimited auditing runs the risk of overflowing the log partition and creating problems for the appliance.

Options for viewing the audit output generated by these selections include:

- The Admin Console **Dashboard**
- **Monitor > Audit**
- SecurityReporter
- Third-party reporting tools
In this chapter...

Understanding the Sidewinder audit process ........................................ 360
Viewing audit information using the Admin Console ......................... 365
Creating custom audit filters ............................................................. 378
Managing audit information using the Admin Console ..................... 382
Understanding audit messages .......................................................... 388
Configuring syslog for off-box reporting tools ................................. 389
Generating reports using SecurityReporter ....................................... 392
Formatting and exporting audit data for use with external tools ........ 393
Understanding the Sidewinder audit process

Monitoring, auditing, reporting, and attack and system event responses are closely related pieces of the audit process. They function together to provide information to you about the activity on your Sidewinder appliance. You can monitor the status of various processes in real time, view stored audit information, generate detailed reports, and have the appliance respond to audit events by alerting administrators and ignoring hosts sending malicious packets.

Auditing is one of the appliance’s most important features. It provides information on what is happening with your system and fulfills compliance regulations. The appliance generates audit information each time it or any of its services are stopped or started. It generates audit data for what configuration changes are made and who made them. Other relevant audit information includes:

- Identification and authentication attempts (successful and failed)
- Network communication (including the presumed addresses of the source and destination subject)
- Administrative connections (using srole)
- Modifications to your security policy or system configuration (including all administrator activity, such as changing the system time)

Because audit records are important, storing them is a high priority. The audit facilities monitor the state of log files to minimize the risk of lost data. Log files are compressed, labeled, and stored on a daily basis, and a new “current” log file is created. Using this mechanism, no audit data is lost during the storage transition.

The amount of available audit storage space is monitored very closely via the rollaudit and logcheck utilities. Those utilities monitor the log file size and rotate log files as needed.

Learn more about the Sidewinder audit process in the following sections:

- “Audit components” on page 361
- “Audit file names” on page 363
- “Tools for viewing and customizing audit events” on page 364

For information on using rollaudit, see “The roll audit cron job” on page 813. For information on using the logcheck utility, refer to the logcheck man page.
Audit components

There are three main components to the Sidewinder audit process:

• **auditd** — This is the audit logging daemon. This daemon listens to the Sidewinder audit device and writes the information to log files. The log files provide a complete record of audit events that can be viewed by an administrator. By default, auditd sends all audit data to a binary file called /var/log/audit.raw.

• **auditbotd** — This is the daemon that listens to the audit device and gathers the security-relevant information it finds. It tracks these events and uses its configuration to determine when the data might be indicating a problem and require a response, such as an attempted break-in. If it does detect an audit event that has a configured response, the appliance responds accordingly. For more information on configuring IPS attack and system event responses, refer to Chapter 13, "IPS Attack and System Event Responses," on page 399.

• **auditdbd** — This daemon maintains the audit database. auditdbd monitors the audit stream and sends reporting information to an audit database. The auditdbd server is disabled by default.

To use the on-box reporting service (**cf reports**), you must first enable the following components by entering the following commands:

```
cf daemond enable agent=auditsql
  cf daemond enable agent=auditdbd
```

**Important:** The auditsql agent must be enabled before the auditdbd agent.

If you are not using the Sidewinder on-box reporting tool, leave these agents disabled.

To view a list of audit databases, enter the following command:

```
cf audit listdb
```

A list of audit databases appears. The database named *auditdb_1* generally contains the previous day’s information. The database named *auditdb_2* is generally from two days ago, and so on.
The following diagram demonstrates how these pieces are related in the audit flow.

**Figure 164: Audit flow**

**Monitoring and alerts**
- **programs**
- **kernel**

**Auditing**
- audid reads `/dev/audit` and places the information into `audit.raw`.
- This is the recorded audit stream. This is now "history" and contains everything that might be worth viewing.

**Reporting**
- You can generate detailed, easy-to-read reports using SecurityReporter or a third-party reporting tool. You can generate very basic reports using `cf reports`.

**Live audit stream** aka `/dev/audit`.....

- auditbotd can trigger a response that alerts the administrator of suspicious activities.

You can monitor Sidewinder activity and status in real time using the Admin Console's Dashboard.

This is a database of information maintained by `auditdbd`. It contains the audit information relevant for the on-box command line reporting tool.
Audit file names

The audit information is saved in a binary format in the /var/log/audit.raw files. When the file is rolled, a timestamp is appended to the file name. The easiest method for viewing the contents of the audit.raw files is to use the Admin Console’s Audit Viewing window. Refer to “Viewing audit information using the Admin Console” on page 365.

Tip: If you prefer to view the file contents via command line, refer to the acat and showaudit man pages.

Audit log files use one of two file suffixes:

- *gz — This suffix is for files in compressed format. These files may be decompressed using acat or showaudit. The default file name format is audit.raw.YYYYMMDDhhmmsZZZ.YYYYMMDDhhmmsZZZ.gz, where the variables represent date and time (including time zone) of the beginning and end of that audit file’s contents. For example, 20051231020000CST.20060101020000CST.gz is a file that contains audit data from December 31, 2005 at 2:00 am to January 1, 2006 at 2:00 am.

- *.raw — This suffix is for files in raw audit format. These are binary formatted files that can be viewed in ASCII format using the Admin Console or command line.
Tools for viewing and customizing audit events

Many tools allow you to interact with the audit data. Use the following tools to generate, view, and respond to audit events:

- Audit output can be customized using Network Defenses (**Policy > Network Defenses**).
- Audit output can be viewed using these tools:
  - The Admin Console's dashboard
  - The Admin Console's audit viewing area (**Monitor > Audit Viewing**)
  - The off-box Secure Computing SecurityReporter
- Audit output can be viewed in these formats:
  - Sidewinder Export Format
  - WebTrends Log Format
  - HTTP
  - ASCII
  - Verbose ASCII
  - XML
- Audit output can be configured to trigger alerts using these tools:
  - IPS Attack Responses (**Monitor > IPS Attack Responses**)
  - System Event Responses (**Monitor > System Event Response**)
One tool for viewing audit output is the Admin Console’s Audit Viewing area. This area contains the View Mode and Filtering tabs, which allow you to focus audit output on the information you want to see. Once you customize the audit output, you can view it directly from this window or export it for use elsewhere.

The following sections describe how to use this Admin Console area:

- “Selecting an audit range to view” on page 365
- “Exporting audit data” on page 370
- “Filtering audit data” on page 371

## Selecting an audit range to view

Using the Admin Console, you can view the information contained in the audit log files. To view audit information, select **Monitor > Audit Viewing**.

The top portion of this window displays the **Audit Data Timespan**. This timespan shows the range of audit available, from the oldest event to the newest event.

The View Mode tab appears by default.

![Figure 165: View Mode tab](image-url)
Use this tab to configure the type of audit information you want to view. You can view the audit events via the Admin Console, or you can export the audit events to a text file for viewing or printing. Follow the steps below.

1. In the **Select a Viewing Mode** area, select one of the following:
   - **Real Time** — Select this option and go to step 3 if you want to view streaming audit in real time.
   - **Snapshot** — Select this option and continue to step 2 if you want to view audit messages within a specific time frame.

   **Important:** The **Audit Data Timespan** field (located in the top portion of the Audit Data window) displays the range of available audit data. If you select **Snapshot** mode, the audit time frame you select must fall within this range.

2. [Conditional] If you selected **Snapshot** mode, specify the start and end time for the period of audit data that you want to view, as follows:
   a. Select the start and end months in the corresponding month drop-down lists.
   b. Select the start and end years in the corresponding year lists, either by using the up and down arrows or clicking in the field and modifying it manually.
   c. Select the start and end days in the corresponding calendars by clicking the appropriate dates.
   d. Select the start and end time in the corresponding **Time** fields, either by using the up and down arrows or clicking in the field and modifying it manually.

   **Tip:** To set the start date to the earliest available date, click **Start of Data**. To set the end date to the current date and time, click **Now**. The date and time fields will automatically fill in the correct information.

3. In the **Lines Per Page** field, type the number of audit events that you want available within each page of audit. Valid values are 5–500. For example, if you select 50 audit events per page, you can scroll through 50 events at a time.

   Use the scroll bar to view all audit events within a page if needed.

4. [Conditional] If you want to set up filtering options for the audit data, select the Filtering tab and see “Filtering audit data” on page 371.

5. Once you have configured the time frame of audit events, do one of the following:
   - [Conditional] If you selected **Snapshot** in step 1, you can export the audit information to a text file that you can edit and print. Click **Export** and see “Exporting audit data” on page 370.
   - To view the results of your audit query, click **View**. The View Audit Data window appears as a separate pop-up window.
About the View Audit Data window

Use this window to view the audit events that you selected in the Audit Viewing window. Each audit event appears as a single row in the table. Use the scroll bars to view all of the information in the table.

**Note:** If you selected Real Time audit data, the table will be grayed out and will populate with audit events as they happen. You cannot modify the table or events while real time audit is running.

The number of audit events you can scroll through on each page is dependent on the **Lines Per Page** value you entered in the Audit Viewing window. For example, if you selected 50 audit events per page, you can scroll through 50 events at a time. To move to the next 50 events, click **Next Page** or **Previous Page**, accordingly.
The audit data is separated into the following columns:

- Time
- Type
- Service
- Source IP
- Source Burb
- Dest IP
- Dest Burb
- Info

When you select an audit event in the table, its information is displayed in the window’s bottom portion so that it is easy to read.

**Note:** Some audit types will not contain information for each table column. If a column is blank, that type of information does not apply to that particular audit event.

When viewing real-time audit results, if you would like to view individual audits or filter the columns, you must first click **Stop** to interrupt the real-time audit stream. This enables the table and allows you to use the window as you would if you were viewing a snapshot of audit events. It also gives you a chance to save the results. Click **Start** to view the real-time audit stream again. This clears the table’s existing audit records and displays new real-time audit events as they occur.

Click **Close** to close the window.

For descriptions of the audit fields, see “Understanding audit messages” on page 388.
Ordering the audit event table

Initially, the audit events are listed in chronological order. However, you can re-order any column alphabetically or numerically by clicking the heading. You can also right-click a heading to select a default filtering option or create a custom filter. For information on filtering tables, see “Admin Console conventions” on page 29.

![Figure 167: Accessing column-filtering options](image)

Saving audit events

When viewing a snapshot of audit results, or when you have stopped a real-time audit stream, you can save some or all audit events listed in the Audit Viewing window. Do one of the following:

- To save all of the audit events listed on this page, click **Save All**. The Export Audit Data window appears and allows you to save, or export, the data to a text file.

  Note: If you want to save multiple pages of audit data, use **Previous Page** or **Next Page** and repeat this procedure until all data is saved. If you frequently need to save multiple pages, increase the **Line Per Page** value on the **View Mode** tab.

- To save selected audit events, press and hold the **Ctrl** key while clicking in the row of each audit event you want to save. When you have selected all of the audit events on this page that you want to save, click **Save Selected**. The Export Audit Data window appears and allows you to save, or export, the data to a text file.

For more information on exporting data, see “Exporting audit data” on page 370.
Exporting audit data

To export audit data to a text file that can be viewed and printed:

1. From the View Mode tab, click Export. A Confirm Export message appears.
2. Click Yes to continue the export process. The Export Audit Data window appears.

3. In the Filename field, specify the file name and location for the audit data you are exporting. You can type the path and file name in the field, or you can click Browse and navigate to the desired location.

4. In the Export Format area, select one of the following:
   - ASCII Audit — Select this option to save the audit information in ASCII format. This allows you to open the file using any standard text editor, such as Notepad.
   - ASCII Sidewinder Export Format — Select this option if you want to save the data into ASCII text and export it in the Sidewinder Export Format (SEF). This format is used in the Secure Computing SecurityReporter and can also be used with third-party reporting tools.

   For information on interpreting SEF, see http://www.securecomputing.com/pdf/si_70_sef_an.pdf

5. Click one of the following options to save the file:
   - Save — Save the file to the specified location for later viewing.
   - Save and View — Save the file to the specified location and launch the file using a standard text editing program (such as Notepad).
   - Close — Exit the window without saving the file.

Once saved, the audit data is ready for viewing, either directly or by importing it into a reporting tool.
Filtering audit data

To filter the type of audit data you want to view, select the Filtering tab in the Audit Viewing window. The Audit Filtering tab appears.

Figure 169: Audit: Filtering tab

Use this tab to configure filters to display or exclude certain types of audit events. Using filters can greatly reduce your audit output and simplify troubleshooting.

In this tab, you can:

- View or export filter audit data. You can select from a list of available filters or create a new custom filter. See “Filtering audit data” on page 372.
- Save a new audit filter. See “Saving a custom audit filter” on page 373
- Delete existing audit filters. See “Deleting filters” on page 374.

Descriptions of default audit types are available in Table 25 on page 374.
Filtering audit data

1 In the Available filters area, select the audit filters that correspond to the audit output you want to view. For descriptions of these filters, see “Predefined audit filters” on page 374.
   • To see all available audit, select the all audit filter.
   • To clear all current selections, click Deselect All.

2 In the Advanced area, further refine the filter(s) you selected by specifying any of the following information:
   • Source Burb — To view audit events generated by the selected source burb, select this check box and specify a burb in the drop-down list.
   • Source IP Address — To view audit events generated by the specified source IP address, select this check box and enter an IP address. Also type the number of significant bits needed to create the subnet you want to filter.
   • Destination Burb — To view audit events generated by the selected destination burb, select this check box and specify a burb in the drop-down list.
   • Destination IP Address — To view audit events generated by the specified destination IP address, select this check box and enter an IP address. Also type the number of significant bits needed to create the subnet you want to filter.
   • Service — To view audit events generated by a service, select this check box and a service name. This list includes all configured services.

3 [Conditional] To customize the filter parameters, select the Custom check box. The Custom audit filter field is now editable.

   See “Creating custom audit filters” on page 378 for more information on audit syntax.

4 Click View or Export.

You can now analyze your audit output.
Saving a custom audit filter

1 Select available filters and advanced settings to use as building blocks in a custom filter. These selections populate the Custom audit filter field.

2 Click Save Filters. The Save Filter window appears.

3 Create a new filter:
   a Select whether the filter is for an Attack or System audit event.
   b Enter a name for the filter. Make the name as descriptive as possible.
   c Add a description of this filter’s function.
   d Edit the filter.
      By default, all filters in this window are created using the “and” and the “or” operators; you can edit the filter to include “not.” Use Boolean expressions.
   e In the SNMP trap number field, add an SNMP trap number that is to be associated with this filter. See “Sidewinder SNMP traps” on page 418 for a list of traps.
   f Click Add to save the filter. The new filter displays and is selected on the Available Filters list.

   For additional information on creating customized audit filters, see “Creating custom audit filters” on page 378.

4 Click View or Export.

You can now analyze your customized audit output.
Deleting filters

Audit filters are also used in IPS attack responses and system event responses. You cannot delete filters that are currently in use by a response.

Caution: All filters, including the default filters, can be deleted. There is no way to restore the defaults.

1. Click Delete Filter. The Delete Filter window displays all available filters.
2. Select the filters to delete. To select multiple adjacent filters, hold down Shift while clicking. To select multiple nonadjacent filters, hold down Ctrl while clicking.
3. Click Delete.

The filter is now deleted.

Predefined audit filters

The following list displays the default audit filters and describes the event types that each filter audits.

Table 25: Predefined audit filters

<table>
<thead>
<tr>
<th>Audit types</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL allow</td>
<td>Detects when a connection is allowed by a rule in the active policy.</td>
</tr>
<tr>
<td>ACL deny</td>
<td>Detects when a connection is denied by a rule in the active policy.</td>
</tr>
<tr>
<td>Access Control List</td>
<td>Detects all ACL audit events.</td>
</tr>
<tr>
<td>Application Defense violation all</td>
<td>Detects attacks of all severities that violate active policy defined by Application Defenses. This attack category includes mime and keyword filter failure attacks.</td>
</tr>
<tr>
<td>Application Defense violation severe</td>
<td>Detects when severe attacks violate active policy defined by Application Defenses, including mime and keyword filter reject audits. Severe attacks indicate something is occurring that an administrator should know.</td>
</tr>
<tr>
<td>DOS all</td>
<td>Detects Denial of Service attacks of all severities. This attack category also detects all severities of TCP SYN attacks and proxy flood attacks.</td>
</tr>
<tr>
<td>DOS severe</td>
<td>Detects severe Denial of Service attacks. This attack category also detects TCP SYN attacks and proxy flood attacks. Severe attacks indicate something is occurring that an administrator should know.</td>
</tr>
<tr>
<td>HA failover</td>
<td>Detects when a failover IP address changes because a High Availability cluster failed over to its secondary/standby.</td>
</tr>
<tr>
<td>IPFilter deny</td>
<td>Detects when a connection is denied by the active IP Filter policy.</td>
</tr>
<tr>
<td>IPsec error</td>
<td>Detects when traffic generates IPsec errors.</td>
</tr>
</tbody>
</table>

More...
<table>
<thead>
<tr>
<th>Audit types</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP SYN attack</td>
<td>Detects a possible attempt to overrun the appliance with connection attempts.</td>
</tr>
<tr>
<td>Type Enforcement</td>
<td>Detects when there is a TE violation due to an unauthorized user or process attempting to perform an illegal operation.</td>
</tr>
<tr>
<td>VPN</td>
<td>Detects VPN audit events.</td>
</tr>
<tr>
<td>all audit</td>
<td>Detects all attack and system events, regardless of type.</td>
</tr>
<tr>
<td>attack all</td>
<td>Detects attack events of all severities. This option also detects all severities of Application Defense violation attacks, buffer overflow attacks, DOS attacks, general attacks, policy violation attacks, protocol violation attacks, virus attacks, and spam attacks.</td>
</tr>
<tr>
<td>attack severe</td>
<td>Detects severe attacks. This option also detects Application Defense violation attacks, buffer overflow attacks, general attacks, DOS attacks, policy violation attacks, protocol violation attacks, virus attacks, and spam attacks. Severe attacks indicate something is occurring that an administrator should know.</td>
</tr>
<tr>
<td>buffer overflow attack</td>
<td>Detects attempted buffer overflow attacks targeted at systems protected by the Sidewinder appliance.</td>
</tr>
<tr>
<td>config change</td>
<td>Detects when the Sidewinder appliance’s configuration changes.</td>
</tr>
<tr>
<td>denied authentication</td>
<td>Detects when a user attempts to authenticate and enters invalid data. For example, if a user is required to enter a password and entered it incorrectly, the denied auth event would log the event.</td>
</tr>
<tr>
<td>error</td>
<td>Detects all system events identified as AUDIT_T_ERROR in the audit stream.</td>
</tr>
<tr>
<td>general attack all</td>
<td>Detects general attacks of all severities that do not fall into the predefined categories.</td>
</tr>
<tr>
<td>general attack severe</td>
<td>Detects severe general attacks that do not fall into the predefined categories. Severe attacks indicate something is occurring that an administrator should know.</td>
</tr>
<tr>
<td>hardware software failure</td>
<td>Detects some hardware failures, such as RAID, hard drive, and AMIR monitor failures.</td>
</tr>
<tr>
<td>host license exceeded</td>
<td>Detects when the number of hosts protected by the Sidewinder appliance exceeds the number of licensed hosts.</td>
</tr>
<tr>
<td>keyword filter failure</td>
<td>Detects when an SMTP mail message is rejected due to a configured keyword filter.</td>
</tr>
<tr>
<td>license expiration</td>
<td>Detects when a licensed feature is about to expire.</td>
</tr>
<tr>
<td>log overflow</td>
<td>Detects when the log partition is close to filling up.</td>
</tr>
<tr>
<td>Audit types</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| network probe            | Detects network probe attacks, which occur any time a user attempts to connect or send a message to a TCP or UDP port when the security policy does not include a service that is expecting to receive traffic on that port.  
  **Note:** The appliance does not blackhole netprobe attacks, as they are likely to be Denial of Service attacks from spoofed source addresses. |
| network traffic           | Detects all connections that successfully pass through the Sidewinder appliance.                                                                               |
| not config change        | Detects all attack and system events that are not configuration changes.                                                                                      |
| policy violation all      | Detects attacks of all severities that violate the active policy. This attack category also detects all severities of failed authentication attacks, ACL and IP Filter deny attacks, and Type Enforcement error attacks. |
| policy violation severe   | Detects severe attacks that violate the active policy. This attack category also detects failed authentication attacks, ACL and IP Filter deny attacks, and Type Enforcement error attacks. Severe attacks indicate something is occurring that an administrator should know. |
| power failure             | Detects when an Uninterruptible Power Supply (UPS) device detects a power failure and the appliance is running on UPS battery power. |
| protocol violation all    | Detects attacks of all severities that violate protocol compliance.                                                                                           |
| protocol violation severe | Detects severe attacks that violate proxy protocols (HTTP, Telnet, FTP, etc.). Severe attacks indicate something is occurring that an administrator should know. |
| proxy flood               | Detects potential connection attack attempts. A connection attack is defined as one or more addresses launching numerous proxy connection attempts to try and flood the system. When NSS receives more connection attempts than it can handle for a proxy, new connections to that proxy are briefly delayed (to allow the proxy to “catch up”), and the attack is audited. |
| signature IPS intrusion all | Detects all attacks identified by the signature-based IPS. This category detects attacks that were denied, dropped, or rejected, as well as suspected attacks that were allowed but were audited by IPS. |
| signature IPS intrusion blackholed | Detects attacks identified by the signature-based IPS where the attacker was blackholed.                                                                      |
| signature IPS intrusion deny | Detects attacks identified by the signature-based IPS where the offending network session was dropped or rejected, or the attacker was blackholed.                        |
| spam                     | Detects attacks of all severities that are spam.                                                                                                             |
| spam severe              | Detects severe attacks that are spam.                                                                                                                        |
| syslog                   | Detects all audit attacks and system events created via syslog.                                                                                             |
| system all               | Detects all system events of all severities, including power failures, hardware and software failures, failover events, license expiration, host license exceeded, log overflows, and IPsec errors. |
## Audit types and Description

<table>
<thead>
<tr>
<th>Audit types</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>system critical</td>
<td>Detects all critical system events, including power failures, hardware failures, critical software failures, and failover events. Critical system events indicate a component or subsystem stopped working, that the system is going down (expectedly or unexpectedly), or that the system is not expected to work again without intervention.</td>
</tr>
<tr>
<td>system critical and severe</td>
<td>Detects critical and severe system events including power failures, hardware failures, critical and severe software failures, failover events, license expiration, log overflows, and IPsec errors. Critical system events indicate a component or subsystem stopped working, that the system is going down (expectedly or unexpectedly), or that the system is not expected to work again without intervention. Severe attacks indicate something is occurring that an administrator should know.</td>
</tr>
<tr>
<td>TrustedSource</td>
<td>Detects attacks identified as spam by TrustedSource.</td>
</tr>
<tr>
<td>UPS system shutdown</td>
<td>Detects when a UPS is running out of battery power or has been on battery power for the estimated battery time.</td>
</tr>
<tr>
<td>virus</td>
<td>Detects attacks of all severities that are viruses.</td>
</tr>
<tr>
<td>virus severe</td>
<td>Detects severe attacks that are viruses.</td>
</tr>
</tbody>
</table>
Creating custom audit filters

The audit logs contain useful data for understanding what is happening at your network perimeter and within your appliance. However, the large volume of data can make it difficult to identify key information. By using customized filters, you can filter out less significant information and only see exactly what you want in the audit. The following sections explain the syntax for creating a filter and then provide filter examples.

- “Learning filter syntax” on page 378
- “Filter examples” on page 380

Learning filter syntax

You can create customized filters using the Admin Console or a command line interface. Once filters are saved, they are available to filter audit data before viewing or exporting it and when creating attack and system responses.

- To use the Admin Console, select Monitor > Audit Viewing. Click the Filtering tab and create a filter in the Custom audit filter field.
- To use the command line interface, enter a format similar to the following:
  ```
  acat -e 'sacap_filter(s)'/var/log/audit.raw'
  ```
  - To filter audit real-time, use `acat -ke`.
  - To filter existing audit, use `acat -e` (audit filters can be used with any raw audit file).

Use the following syntax when building expressions in either interface:

- Identify a filter using either single quotes (') or double quotes ("). All examples shown below use single quotes.
- Express “and” using either `and` or `&&`.
- Express “or” using either `or` or `||`.
- Express "not" using either `not` or `!`.
A filter should include:

- The type or facility you want to search for, using one of these formats:
  - The Name format (AUDIT_T_TYPE as in AUDIT_T_ATTACK, AUDIT_F_FACILITY as in AUDIT_F_LOGIN)
  - The Short Message format (attack, login)
  - The Short Message format prepended with classification indicator (t_attack, f_login)

  **Note:** This last format appears in audit records and is useful when copying or pasting directly from audit output.

- Additional fields to further specify the audit results. Fields can be separated by Boolean operators (and, or, not) and grouped by parentheses.

The following table provides a list of the available fields (for example, facility, type, service, user, etc.) that you can use to filter your audit search.

- The following table lists and describes the most commonly used fields for creating custom audit filters (sacap expressions). For a complete list of the codes that populate these fields, see `acat -c | more`.

### Table 26: Custom audit filter fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>facility</td>
<td>Specify an event facility code (such as f_login, f_proxy, etc.).</td>
</tr>
<tr>
<td>type</td>
<td>Specify an event type code (for example, type t_nettraffic).</td>
</tr>
<tr>
<td>category</td>
<td>Specify an event category code (for example, c_policy_violation).</td>
</tr>
<tr>
<td>event</td>
<td>Specify an event identifier code (for example, AUDIT_R_ACLDENY).</td>
</tr>
<tr>
<td>hostname</td>
<td>Specify a host name.</td>
</tr>
<tr>
<td>username</td>
<td>Specify a user name.</td>
</tr>
<tr>
<td>src_ip</td>
<td>Specify the source IP address. Separate optional mask bits with a slash (/).</td>
</tr>
<tr>
<td>dst_ip</td>
<td>Specify the destination IP address. Separate optional mask bits with a slash (/).</td>
</tr>
<tr>
<td>src_port</td>
<td>Specify the TCP or UDP source port.</td>
</tr>
<tr>
<td>dst_port</td>
<td>Specify the TCP or UDP destination port.</td>
</tr>
<tr>
<td>src_burb</td>
<td>Specify the source burb name or index number.</td>
</tr>
<tr>
<td>dst_burb</td>
<td>Specify the destination burb name or index number.</td>
</tr>
<tr>
<td>service</td>
<td>Specify the service name. (To filter on an agent, use the facility field.)</td>
</tr>
<tr>
<td>vpn_lgw</td>
<td>Specify a VPN local gateway using the standard dotted decimal IP version 4 notation with optional mask bits separated by a slash (/).</td>
</tr>
<tr>
<td>vpn_rgw</td>
<td>Specify a VPN remote gateway using the dotted decimal IP version 4 notation with optional mask bits separated by a slash (/).</td>
</tr>
</tbody>
</table>
Filter examples

The following examples demonstrate the basic structure used to create custom audit filters.

Tip: Knowledge base article 1260 at www.securecomputing.com/goto/kb contains additional examples. Also refer to man acat and acat -c | more.

Example 1: Filtering for login records

The following example shows the format used to display all system login records (successful and unsuccessful):

```
facility f_login
```

If you want to view login records for a specific user, include a user name as follows:

```
facility f_login and username Josephine
```

Example 2: Filtering for services and users

The following example shows the format used to display HTTP attack audit records for a user named Lloyd:

```
type t_attack and cmd httpp and username Lloyd
```

where:

- **type t_attack** — This field will filter audit records for all attack events.
- **cmd httpp** — This field will filter the attack audit events to include only HTTP service records.
- **username Lloyd** — This field will filter the HTTP attack events to include only events that are specific to actions performed by user name “Lloyd.”
Example 3: Filtering for specific ports and IP addresses

The following example shows the format used to display all network probe events on port 31337 and subnet 192.168.124.0/24 originating from burbs 3 or 4. Enter text on one line:

```
type t_netprobe and dst_port 31337 and dst_ip 192.168.124.0/24 and (src_burb 3 or src_burb 4)
```

where:

- **type t_netprobe** — This field will filter audit records for all network probe events.
- **dst_port 31337** — This field will filter the network probe events to include only records with a destination port of 37337.
- **dst_ip 192.168.124.0/24** — This field will filter the network probe events to include only records with a destination IP address of 192.168.124.0/24.
- **(src_burb 3 or src_burb 4)** — This information will filter the network probe events to include only records with a source burb of 3 or 4.

Example 4: Excluding information in a filter

You can explicitly exclude certain types of audit information by placing the word “not” in front of a field. For example, the custom filter shown below will display all audit records EXCEPT attack records originating for the source IP address 172.17.9.28:

```
not type t_attack and src_ip 172.17.9.28
```

where:

- **not type t_attack** — This field will exclude any attack-based audit events.
- **src_ip 172.17.9.28** — This field will filter the non-attack audit events for records with a source address of 172.17.9.28.
Managing audit information using the Admin Console

Use the Audit Management window to manage your audit log files, including:

- Exporting log files in a variety of formats to a specified host
- Scheduling exports
- Adding a signature to the log files
- Rolling the log files

Generally, you will set up this service during system startup, then test to make sure you are getting the results you intended. Once setup is complete, the log files transfer and roll automatically, giving you the audit data you need and keeping the Sidewinder appliance running freely.

Select **Monitor > Audit Management**. The Audit Management window appears, consisting of two panes:

- **Audit Options** (top of the window)
- **Logfile Options** (center of the window)

**Figure 171: Audit Management window**
Audit Options pane

The Audit Options pane contains the **Show system statistics in audit log** check box. Use this option to capture network and system utilization statistics, which appear in the dashboard.

**Note:** This option is enabled by default and should rarely, if ever, need to be disabled.

Logfile Options pane

From the Logfile Options pane, you can create export entries that allow the Sidewinder appliance to transfer its log files in a variety of formats to a specified host. From this pane, you can also schedule the exports, include a signature, and roll log files.

Use the toolbar to perform the actions described in Table 27.

**Figure 172:** Logfile Options toolbar

**Table 27:** Logfile Options toolbar tasks

<table>
<thead>
<tr>
<th>Button</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td>Click <strong>New</strong> to create an export entry. Complete the fields as described in “About the Export File window” on page 384. Click <strong>OK</strong>; the entry appears in the Logfile Options pane.</td>
</tr>
<tr>
<td>Modify</td>
<td>Double-click the entry you want to change (alternately, click once to highlight the entry, then click <strong>Modify</strong>). Make your changes, click <strong>OK</strong>, and save your changes.</td>
</tr>
<tr>
<td>Delete</td>
<td>Select the entry you want to delete, then click <strong>Delete</strong>. Click <strong>Yes</strong> to delete the entry or <strong>No</strong> to cancel the action.</td>
</tr>
<tr>
<td>Export selection now</td>
<td>Click <strong>Export selection now</strong> to immediately export a selected entry.</td>
</tr>
<tr>
<td>Search</td>
<td>To find an export entry, enter all or part of the name. When the system finds a match, it appears highlighted in the pane. If the system does not find a match, the pane appears blank. Use the <strong>Backspace</strong> key to find partial matches or delete the search term to return to the Logfile Options pane.</td>
</tr>
</tbody>
</table>
About the Export File window

When you click New or Modify on the toolbar, the Export File window displays.

![Figure 173: Export File window](image)

Complete the fields as described below.

- **Entry Name** — Enter a descriptive, single-word name.
- **Export Type** — Select the export type. For more information about supported log formats, refer to “Supported log formats and their uses” on page 393.

  __Note: If the export file will be used with SecurityReporter, select Sidewinder Export Format.____

- **Export with** — From the drop-down list, select FTP or SCP transfer protocol.
- **Host** — Enter the host name or IP address of the host that will receive the exported file.
- **Directory** — Enter the path name of the directory that will store the exported file.
- **Username** — Enter the username for the host you specified.
- **Password** — Enter the password for the host you specified.

Once you have created the export entries, test them to make sure the results are what you intended. See “Signing export files” on page 385 and “Exporting and rolling log files” on page 386.
Signing export files

Log files can be cryptographically signed to ensure data integrity. To add a signature:

1. In the Logfile Options pane, select the **Sign exported files** check box.
2. In the **Sign with** field, use the drop-down list to select the signature certification.
3. In the **Signature Options** area, select how you want to store the signature file:
   - **Append signature to file** — This option creates one .gz file that includes the signature at the end of the file.
   - **Put signature in separate file** — This option creates two files: a .gz file that contains the actual audit and a .gz.pem file that contains the signature.

For more information, see “Using Sidewinder formatting and exporting tools” on page 395.
Exporting and rolling log files

Once you configure and enable a schedule, the Sidewinder appliance will automatically check to see if it should export any log files and, if so, export those files. You can also export log files on request for a single export entry or all entries.

The appliance automatically rolls log files every morning at 2:00 a.m. You can change the schedule and export or roll log files on request. By default, the Sidewinder appliance maintains 20 rolled instances of the audit.raw file. This setting can be reconfigured in the /etc/sidewinder/rollaudit.conf file.

Configuring a schedule for exporting or rolling log files

Use the Crontab Editor to schedule an export program.

To configure a schedule for the Sidewinder appliance to export log files:

1. Click Change. The Crontab Editor window appears.

   ![Figure 174: Crontab Editor window](image)

2. Select the Enable check box to activate this schedule. If you leave the check box clear, the entry will be saved, but the Sidewinder appliance will not act on it.

3. [Conditional] To designate a standard frequency for exporting files (for example, every day at 2:00 a.m.):
   - **Frequency** — From the drop-down list, select the frequency for exporting the file (hourly, daily, or weekly).
   - If you selected Hourly, enter the number of minutes after the hour.
   - If you selected Daily, enter the time for export.
   - If you selected Weekly, enter the time and day. You can select multiple days.
   - **Description** — Enter a descriptive name for the task (such as Run export utility 35 minutes past every hour).
4  [Conditional] To define a custom frequency for exporting files:
   • **Custom** — Select this check box and complete the fields. Refer to
     `man 5 crontab` for options.

     **Note:** The Crontab Editor allows custom syntax. Make sure your syntax is
     correct, and verify your entry with `cf crontab query`.

   • **Description** — Enter a descriptive name for the task (such as Run
     export utility the 1st and 15th day of every month at 2:00 a.m.).

5  Click **OK** to accept the schedule.

**Exporting or rolling log files on request**

Click **Export All Now** to immediately export all log files.

Click **Roll Now** at the bottom of the Logfile Options pane to immediately roll all
log files. This option is generally used for testing and troubleshooting
purposes.
Understanding audit messages

When viewing audit messages in the Admin Console, the form may vary depending on the purpose and content of the message. The form of the first two lines is the same for all audit messages and provides general information about the process generating or causing the audit. The third line will vary but usually includes Type Enforcement information and possibly some additional information. The other lines of an audit message will vary depending on the type of audit message.

Important: To view audit message files, see “Viewing audit information using the Admin Console” on page 365.

The message below is an example of a Type Enforcement audit message (using the te_filter filter). The numbers have been added to link the example line with the bullets below.

(1) Nov 22 11:38:46 2006 EST  f_kernel a_tepm t_attack p_major
(2) pid: 11124 ruid: 100 euid: 100 pgid: 11124 logid: 100 cmd: 'cat'
(3) domain: User edomain: User hostname: python.a.net category: policy_violation
(4) event: ddt violation srcdmn: User filedom: Pass filetyp: file
(5) reason: OP: OP_FS_PERM_CHECK perm wanted: 0x1<read> perm granted: 0x0
(6) information: open /etc/spwd.db

• **Line 1** — This line lists the date and time, the facility that audited the message (such as the Kernel, FTP, or Telnet), the location (known as the area) in the facility that audited the message (such as general area or type enforcer), the type of audit message (such as attack, Type Enforcement violation, or access control list) and the priority of the message (such as major or minor).

• **Line 2** — This line lists the process ID, the real user ID, the effective user ID, the process group ID, the log ID, and the command associated with the process ID.

• **Line 3** — This line lists the real domain the process is running in and the effective domain (the domain of the process for which permission is given). It also lists the appliance’s host name and the audit event’s category.

• **Lines 4, 5, and 6** — The fourth line contains the integer representation of the permissions requested by the process and granted to the process, the domain of the requesting process, and the type of file that the process is requesting access to. The last two lines often contain the reason the audit event was generated and any additional information.
Configuring syslog for off-box reporting tools

The Sidewinder appliance uses the UNIX syslog facility to log messages sent by programs running on the system. These messages can be useful in tracking down unauthorized system users or in analyzing hardware or software problems. All syslog data is stored in the audit log files.

Understanding syslog on the Sidewinder appliance

Logging is set up to be handled automatically. However, if you want to send audit to an off-box reporting tool, you will need to change options, such as where log files are stored. Listed below are some basic points about syslog and how it works on the Sidewinder appliance.

Note: Secure Computing recommends that you edit these files only if you are an experienced UNIX administrator.

- syslog runs as a daemon process called syslogd.
- Each application determines whether it will use syslog and the types of messages that will be generated. Normally, applications generate messages of different severity levels, such as informational and critical.
- The syslog configuration file, /etc/syslog.conf, specifies what syslogd should do with messages that are sent to it. You can specify what should be done with each type of message. For example, you might choose to discard informational messages and store more important messages in a file. In addition, you can choose to send messages that may require immediate attention directly to a specific user’s screen or to send output to a different system on the network. You can edit the configuration file if you want to handle messages differently or send files to different locations. See the next section and the syslog.conf man page for details.
- Hackers will often try to edit syslog files to cover any evidence of their break-ins. The appliance uses Type Enforcement to protect the syslog files from being modified by unauthorized users.
- A copy of the syslog data is sent to the appliance’s audit log files.
- The log files generated by syslogd can get large and start using a lot of hard disk space. To solve this problem, the log files are periodically rotated. See “Monitoring Sidewinder status” on page 807 for more information on file rotation.
Redirecting audit output to a syslog server

If you would like other systems, such as the SecurityReporter, to generate and display reports based on the Sidewinder log files, you can configure the Sidewinder appliance to send audit output to a syslog server.

To redirect audit output to a syslog sever:

1. Using a file editor, open `/secureos/etc/auditd.conf`.
2. Specify what type of logging to send to the syslog server by adding the following line to the end of the file:
   \[
   \text{log}(\text{type dest filter format})
   \]
   where:
   - \text{type} = the kind of log rule this record is. Valid values are \text{file} and \text{syslog}.
   - \text{dest} = where to send the audit event:
     - If you selected \text{file} for the type, then enter a valid path name.
     - If you selected \text{syslog} for the type, enter a valid syslog facility (auth, daemon, kern, lpr, mail, news, syslog, user, uucp, or local0–local7).
   - \text{filter} = name of sacap filter to use in the output. Output all audit information by using \text{["NULL"]}.
   - \text{format} = output format (binary, ascii, vascii, sef, wt, xml, or http). If you are using SecurityReporter, enter \text{sef} as the format.

   For example, use \text{log(syslog local0 NULL sef)} to configure syslog to use the Sidewinder Export Format (SEF).

3. Save the changes and close the file.
4. Open `/etc/syslog.conf`.
5. Specify the IP address of the syslog server by adding the following line:
   \[
   \text{facility.* @x.x.x.x}
   \]
   where \text{facility} matches the facility in step 2 and \text{x.x.x.x} is the syslog server’s IP address.
6. Prevent redundant logging by changing this:
   \[
   \text{*.notice;auth,…uucp.none /var/logmessages}
   \]
   to
   \[
   \text{*.notice;auth,…uucp,\text{facility}.none /var/logmessages}
   \]
7. Save the changes and close the file.
8. Implement the changes by restarting the syslogd and audit processes, using the following commands:
   \[
   \text{cf daemond restart agent=syslog}
   \]
   \[
   \text{cf daemond restart agent=auditd}
   \]

The appliance begins sending audit data to the specified syslog server.
Viewing syslog messages

To view syslog messages, view the /var/log/messages file.

The following illustrates a sample network traffic audit Logfile Message in ASCII format:

```plaintext
```

The following illustrates a sample network traffic audit Logfile Message in SEF format:

```plaintext
auditd: date="Jan 4 21:55:11 2007 UTC",fac=f_ftp_proxy,area=a_libproxycommon,type=t_nettraffic,pri=p_major,pid=4999,ruid=0,euid=0,pgid=4999,logid=0,cmd=pftp,domain=PFTx,edomain=PFTx,hostname=donkey.int.g.test,event=proxy traffic end,service_name=ftp,netsessid=459d77bf00010de7,srcip=10.66.26.21,srcport=20,srcburb=external,protocol=6,dstip=10.66.24.2,dstport=51105,dstburb=internal,bytes_written_to_client=0,bytes_written_to_server=0,acl_id=ftp,cache_hit=1,remote_logname=test,request_command="PORT 10,66,24,2,199,162",request_status=0,start_time="Thu Jan 4 16:55:11 2007"
```
Generating reports using SecurityReporter

One method for generating and viewing reports of Sidewinder audit output is the SecurityReporter. SecurityReporter provides more advanced reporting capabilities than what is available directly on the Sidewinder appliance. Enhanced capabilities include:

- Generated reports for multiple Sidewinder appliances from a single user interface.
- Color-coded charts and graphs that are more user-friendly than text-only reports.
- Report availability in multiple languages.
- Report accessibility without logging into a Sidewinder appliance. This is particularly beneficial for companies that want to let auditors view reports without giving them Sidewinder administrator accounts.

To use SecurityReporter, the Sidewinder appliance must be configured to send its log files in the Sidewinder Export Format (SEF). You can then transfer the audit data to SecurityReporter via a syslog server or FTP. Refer to “Sending data via syslog server to SecurityReporter” on page 392.

- For information on sending log files to a syslog server, see “Redirecting audit output to a syslog server” on page 390.
- For information on using FTP to transfer data to the SecurityReporter, see “Formatting and exporting audit data for use with external tools” on page 393.

*The syslog server and the SecurityReporter may be installed on the same system.*

The appliance provides you with the option to convert audit data into various formats used by third-party reporting tools. To generate reports based on the log files, you must format the audit data and then export those files to the workstation or host that contains the software needed to generate log reports (for example, SecurityReporter). You can then generate the Sidewinder log reports on that machine.

### Overview of supported log file formats

Table 28 lists the log formats the appliance supports, as well as some uses for each format, commands for generating each format, and other important information.

<table>
<thead>
<tr>
<th>Format</th>
<th>Use</th>
<th>Commands</th>
<th>Comments</th>
</tr>
</thead>
</table>
| Sidewinder Export Format (SEF) | SecurityReporter, various third-party tools | `acat -X`  
`cf export add name=filename host=hostname user=name password=password format=sef`  
If using SmartFilter and SEF, set the audit level on the appropriate HTTP proxy rules to Verbose (Policy > Rules). |
| WebTrends Extended Logging Format (WELF) | WebTrends® reporting tools | `acat -W`  
`cf export add name=filename host=hostname user=name password=password format=wt`  
`targetdir=directory protocol=scp|ftp` |                                                                                                                                 |
| W3C Extend Log Format (HTTP)   | various third-party reporting tools      | `acat -H`  
`cf export add name=http_export host=hostname user=name password=password format=http`  
`targetdir=directory protocol=scp|ftp` | If using this format, set the audit level on the appropriate HTTP proxy rules to Verbose (Policy > Rules). |
| Extensible Markup Language (XML) | various third-party reporting tools      | `acat -m`  
`cf export add name=filename host=hostname user=name password=password format=xml`  
`targetdir=directory protocol=scp|ftp` |                                                                                                                                 |

More...
<table>
<thead>
<tr>
<th>Format</th>
<th>Use</th>
<th>Commands</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Binary or RAW (bin)</td>
<td>various third-party</td>
<td><code>acat -b</code>&lt;br&gt;`cf export add name=filename host=hostname user=name password=password format=bin targetdir=directory protocol=scp</td>
<td>ftp</td>
</tr>
<tr>
<td></td>
<td>reporting tools</td>
<td></td>
<td>Using the acat command is optional as this output is an exact copy of the audit raw file.</td>
</tr>
<tr>
<td>American Standard Code of</td>
<td>various third-party</td>
<td><code>acat</code>&lt;br&gt;`cf export add name=filename host=hostname user=name password=password format=ascii targetdir=directory protocol=scp</td>
<td>ftp</td>
</tr>
<tr>
<td>Information Interchange (ascii)</td>
<td>reporting tools</td>
<td></td>
<td>ASCII is the standard format and therefore does not require any arguments with acat.</td>
</tr>
<tr>
<td>Verbose American Standard Code</td>
<td>various third-party</td>
<td><code>acat -v</code>&lt;br&gt;`name=filename host=hostname user=name password=password format=vasci targetdir=directory protocol=scp</td>
<td>ftp</td>
</tr>
<tr>
<td>Information Interchange (vascii)</td>
<td>reporting tools</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Using Sidewinder formatting and exporting tools

You initiate the formatting and exporting process on the appliance using `acat` or the Sidewinder export utility (`cf export`). These tools allow you to format the collected raw audit data into SEF, WELF, XML, HTTP, BINARY, ASCII, and VASCII files.

**Using acat**

`acat` converts data, but does not export it. To format Sidewinder audit data using `acat`, follow the steps below.

1. Using a command line session, log into the appliance and type the following command to switch to the admn role:
   ```
srole
   ```
2. Change directories so that your present working directory (`pwd`) is where you want the converted files saved.
3. To convert your logs to an exportable format and save them to a file, enter the following command:
   ```
   acat -X /var/log/auditfile > filename.format
   ```
   where
   - `-X` indicates the new format. Use `-X` for SEF, `-W` for Webtrends, `-H` for W3C, `-v` for verbose ASCII, and `-m` for XML. Note that the first three arguments are capital letters.
   - `auditfile` is the log file to convert.
   - `filename.format` is the new file name and format, such as `audit012006.sef`.

   For example:
   ```
   acat -X /var/log/audit.raw.20067...CST.gz > audit.sef
   ```
   converts the existing audit file into the SEF format and saves it to a file named `audit.sef`.

   The specified file is now converted and ready to be manually exported via FTP or another method.
Using cf export

As an alternative to the Admin Console, the `cf export` utility both converts and exports the specified log files to a destination host you specify. This utility can also be used to create a cron job that initiates an export program on a regular basis. The export program uses SCP or FTP to transfer the export files from the Sidewinder appliance to the host you specify. The host can be on a trusted network protected by the appliance, or it can be a host that resides somewhere on the Internet. You can also choose to associate a certificate with the exported audit file, either by appending the certificate to the file or sending it separately.

**Note:** The Sidewinder export utility can only be used to export audit files. Exporting other file types using `cf export` is not supported.

To format and export Sidewinder audit data using `cf export`:

1. From a console attached to the appliance, log in and enter `srole` to switch to the Admn domain.

2. Configure the export utility by entering the following command on one line:
   ```
   cf export add name=filename host=hostname user=username password=password format=format targetdir=directory protocol=scp|ftp
   ```
   where:
   - `filename` = a name that describes the file to export
   - `hostname` = the host name or IP address to which you are exporting the files
   - `username` = the user name that will be used for SCP/FTP authentication
   - `password` = the password that will be used for SCP/FTP authentication
   - `format` = the desired file format (options listed in Table 28 on page 393)
   - `directory` = the directory in which you want the export files placed on the destination host
   - `protocol` = the protocol to use when exporting the file. Options are SCP and FTP. If no protocol is specified, `cf export` uses FTP.

3. Export all files that are currently configured and ready to be exported by entering the following command:
   ```
   cf export latest
   ```

4. [Optional] Enable a cron job that automatically determines which configured export files need to be exported, and that formats and exports those files, by entering the following command:
   ```
   cf export enable
   ```
   To disable the automatic cron job process, enter the following command:
   ```
   cf export disable
   ```

5. [Optional] Use `cf crontab` to modify the default 'audit export' cron job.
The file is now converted and exported to another system. The file name format is format_name.hostname.beginning_timestamp.ending_timestamp.gz

To export logs with a PKCS7 signature:

1. From a console attached to the appliance, log in and enter `srole` to switch to the Admn domain.

2. Display the list of available certificates by entering the following command:
   \[ cf cert query fw \]

3. Determine how the certificate will be associated with the formatted audit file:
   - To append the indicated certificate to the file, enter:
     \[ cf export set cert_name=cert attached_signature=yes \]
     where `cert` is a certificate name as listed in step 2.
   - To send the indicated certificate as a separate file, enter:
     \[ cf export set cert_name=cert attached_signature=no \]
     where `cert` is a certificate name as listed in step 2. The accompanying file name is `filename.pem`.

All exported audit files are now associated with a PKCS7 signature.
Chapter 12: Auditing

Formatting and exporting audit data for use with external tools
In this chapter...

- Understanding attack and system event responses .................. 400
- Creating IPS attack responses ........................................... 401
- Creating system responses ............................................... 411
- Ignoring network probe attempts ...................................... 417
- Sidewinder SNMP traps .................................................... 418
Sidewinder IPS attack responses and system event responses allow you to monitor your network for abnormal and potentially threatening activities ranging from an attempted attack to an audit overflow. Using the Admin Console, you can configure how many times a particular event must occur within a specified time frame before it triggers a response.

When the Sidewinder appliance encounters audit activity that matches the specified type and frequency criteria, the response you configured for that system event or attack type determines how the appliance will react. The appliance can be configured to respond by alerting an administrator of the event via e-mail and/or SNMP trap and by ignoring packets from particular hosts for a specified period of time (known as a Strikeback™).

Some default attack and system event responses are automatically created on the appliance during its initial configuration. The additional configuration options you select will depend mainly on your site’s security policy and, to some extent, on your own experiences using the features. You may want to start with the default options and make adjustments as necessary to meet your site’s needs.
IPS (Intrusion Prevention System) attack responses allow you to configure how the appliance responds when it detects audit events that indicate a possible attack, such as Type Enforcement violations and proxy floods. When you create a new response, the Add IPS Attack Response Wizard guides you through the options. You can modify these options at any time from the IPS Attack Responses main window.

To launch the wizard, view or configure attack responses, or change who should receive attack alerts, select **Monitor > IPS Attack Responses**. The following window appears:

![IPS Attack Responses main window](image)

**Figure 176:** IPS Attack Responses main window

<table>
<thead>
<tr>
<th>Name</th>
<th>Attack Type</th>
<th>Frequency</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL deny</td>
<td>ACL deny</td>
<td>Every 30 seconds</td>
<td>Email</td>
</tr>
<tr>
<td>Denied authentication</td>
<td>Denial authentication</td>
<td>20 in 60 seconds</td>
<td>Email</td>
</tr>
<tr>
<td>Pinned deny</td>
<td>Pinned deny</td>
<td>5 in 90 seconds</td>
<td>Email</td>
</tr>
<tr>
<td>IP</td>
<td>IP</td>
<td>Every time</td>
<td>Email</td>
</tr>
<tr>
<td>Keylog filter failure</td>
<td>Keylog filter failure</td>
<td>5 in 60 seconds</td>
<td>Email</td>
</tr>
<tr>
<td>Network probe</td>
<td>Network probe</td>
<td>50 in 30 seconds</td>
<td>Email</td>
</tr>
<tr>
<td>Proxy flood</td>
<td>Proxy flood</td>
<td>5 in 10 seconds</td>
<td>Email, Blockable</td>
</tr>
<tr>
<td>Signature IPS intrusion all</td>
<td>Signature IPS intrusion all</td>
<td>Every time</td>
<td>Email</td>
</tr>
<tr>
<td>Signature IPS intrusion blocked</td>
<td>Signature IPS intrusion blocked</td>
<td>Every time</td>
<td>Email, Blockable</td>
</tr>
<tr>
<td>Signature IPS intrusion delay</td>
<td>Signature IPS intrusion delay</td>
<td>Every time</td>
<td>Email</td>
</tr>
<tr>
<td>Span filter failure</td>
<td>Span severe</td>
<td>5 in 20 seconds</td>
<td>Email</td>
</tr>
<tr>
<td>TCP SYN attack</td>
<td>TCP SYN attack</td>
<td>Every time</td>
<td>Email</td>
</tr>
<tr>
<td>TrustboxSource</td>
<td>TrustboxSource</td>
<td>Every time</td>
<td>Email, Blockable</td>
</tr>
<tr>
<td>Type Enforcement</td>
<td>Type Enforcement</td>
<td>Every time</td>
<td>Email</td>
</tr>
<tr>
<td>Virus filter failure</td>
<td>Virus severe</td>
<td>5 in 20 seconds</td>
<td>Email</td>
</tr>
</tbody>
</table>
Use this window to perform the following tasks:

- **Configure a new IPS attack response** — To configure a new IPS attack response, click **New**. The Add Attack Response Wizard appears. Follow the on-screen instructions.

- **Modify an existing IPS attack response** — To modify an existing IPS attack response, select the appropriate item within the list and click **Modify**. (Read-only administrators can click **View** to view an IPS attack response.) See “Modifying an IPS attack response” on page 403 for more information.

- **Filter the list of IPS attack responses** — To modify the displayed list, right-click a column name and select from the current list of filters or create a custom filter. The list then displays only IPS attack responses of that type.

- **Delete an existing IPS attack response** — To delete an IPS attack response, select the list item you want to delete and then click **Delete**.

- **Disable/enable an IPS attack response** — The disable and enable options depend on an IPS attack response’s current status. If one or more responses with the same status are selected, their status can be changed to its opposite (for example, if all selected responses are enabled, you may disable all of them). When multiple responses with mixed statuses are selected, the only available action is enabling the responses.

- **Create the e-mail list to notify in the event of an attack** — To create or modify the list of e-mail addresses to notify if any IPS attack triggers an alert, click **Response Settings**. You can also blackhole a source IP address if the attack IP cannot be confirmed. See “Configuring the e-mail response settings” on page 409 for more information.
Modifying an IPS attack response

When you modify an IPS attack response, the following window appears:

Figure 177: IPS Attack Responses: Modify window

About the Modify Attack Responses: Attack tab

Use this tab to change this attack response’s attack filter. An attack is generally defined as suspect traffic at either the network or application level. Each attack filter identifies a different attack audit event.

1 Select the attack for which you want the appliance to send out a response. A complete list is provided in Table 29.
   To create additional attack filters, see “Saving a custom audit filter” on page 373.

2 Click OK or the next tab you want to modify.

Note: For descriptions of the audit severities, see “Understanding audit event severities” on page 443.
### Table 29: Descriptions of pre-defined attacks

<table>
<thead>
<tr>
<th>Attack</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL deny</td>
<td>Detects when a connection is denied by a rule in the active policy.</td>
</tr>
<tr>
<td>Application Defense violation all</td>
<td>Detects attacks of all severities that violate active policy defined by Application Defenses. This attack category includes mime and keyword filter failure attacks.</td>
</tr>
<tr>
<td>Application Defense violation severe</td>
<td>Detects when severe attacks violate active policy defined by Application Defenses, including mime and keyword filter reject audits.</td>
</tr>
<tr>
<td>attack all</td>
<td>Detects attack events of all severities. This option also detects all severities of Application Defense violation attacks, buffer overflow attacks, DOS attacks, general attacks, policy violation attacks, protocol violation attacks, virus attacks, and spam attacks.</td>
</tr>
<tr>
<td>attack severe</td>
<td>Detects severe attacks. This option also detects Application Defense violation attacks, buffer overflow attacks, general attacks, DOS attacks, policy violation attacks, protocol violation attacks, virus attacks, and spam attacks. Severe attacks indicate something is occurring that an administrator should know.</td>
</tr>
<tr>
<td>buffer overflow attack</td>
<td>Detects attempted buffer overflow attacks targeted at systems protected by the appliance.</td>
</tr>
<tr>
<td>denied authentication</td>
<td>Detects when a user attempts to authenticate and enters invalid data. For example, if a user is required to enter a password and entered it incorrectly, the denied auth event would log the event.</td>
</tr>
<tr>
<td>DOS all</td>
<td>Detects Denial of Service attacks of all severities. This attack category also detects all severities of TCP SYN attacks and proxy flood attacks.</td>
</tr>
<tr>
<td>DOS severe</td>
<td>Detects severe Denial of Service attacks. This attack category also detects TCP SYN attacks and proxy flood attacks. Severe attacks indicate something is occurring that an administrator should know.</td>
</tr>
<tr>
<td>general attack all</td>
<td>Detects general attacks of all severities that do not fall into the pre-defined categories.</td>
</tr>
<tr>
<td>general attack severe</td>
<td>Detects severe general attacks that do not fall into the pre-defined categories. Severe attacks indicate something is occurring that an administrator should know.</td>
</tr>
<tr>
<td>IPFilter deny</td>
<td>Detects when a connection is denied by the active filter policy.</td>
</tr>
<tr>
<td>Attack</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>keyword filter failure</td>
<td>Detects when an SMTP mail message is rejected due to a configured keyword filter.</td>
</tr>
<tr>
<td>network probe</td>
<td>Detects network probe attacks, which occur any time a user attempts to connect or send a message to a TCP or UDP port that is not configured. Note: If you select this attack, do not select Blackhole on the Attack Response tab. The appliance does not blackhole netprobe attacks, as they are likely to be denial of service attacks from spoofed source addresses.</td>
</tr>
<tr>
<td>policy violation all</td>
<td>Detects attacks of all severities that violate the active policy. This attack category also detects all severities of failed authentication attacks, network probe attacks, ACL and IP Filter deny attacks, and Type Enforcement error attacks.</td>
</tr>
<tr>
<td>policy violation severe</td>
<td>Detects severe attacks that violate the active policy. This attack category also detects failed authentication attacks, network probe attacks, ACL and IP Filter deny attacks, and Type Enforcement error attacks. Severe attacks indicate something is occurring that an administrator should know.</td>
</tr>
<tr>
<td>protocol violation all</td>
<td>Detects attacks of all severities that violate protocol compliance.</td>
</tr>
<tr>
<td>protocol violation severe</td>
<td>Detects severe attacks that violate proxy protocols (HTTP, Telnet, FTP, etc.). Severe attacks indicate something is occurring that an administrator should know.</td>
</tr>
<tr>
<td>proxy flood</td>
<td>Detects potential connection attack attempts. A connection attack is defined as one or more addresses launching numerous proxy connection attempts to try and flood the system. When NSS receives more connection attempts than it can handle for a proxy, new connections to that proxy are briefly delayed (to allow the proxy to “catch up”), and the attack is audited.</td>
</tr>
<tr>
<td>signature IPS intrusion all</td>
<td>Detects all attacks identified by the signature-based IPS. This category detects attacks that were denied, dropped, or rejected, as well as suspected attacks that were allowed but were audited by IPS.</td>
</tr>
<tr>
<td>signature IPS intrusion blackholed</td>
<td>Detects attacks identified by the signature-based IPS where the attacker was blackholed.</td>
</tr>
<tr>
<td>signature IPS intrusion deny</td>
<td>Detects attacks identified by the signature-based IPS where the offending network session was dropped, or rejected, or the attacker was blackholed.</td>
</tr>
</tbody>
</table>
Creating IPS attack responses

### About the Modify Attack Response: Attack Frequency tab

Use this tab to modify the parameters to be met before the appliance generates a response. The options are:

- **Always respond** — Select this option to have the appliance respond each time the attack specified on the Attack tab occurs.

- **Limit responses** — Select this option to respond only when the attack pattern matches the parameters set here:
  - **Respond if \( x \) attacks in \( y \) seconds** where:
    - Valid values for \( x \) are between 2 and 100000. The appliance responds when the \( x \) attack occurs.
    - Valid values for \( y \) are between 1 and 100000. This represents a buffer of \( y \) seconds, so the appliance checks the current time - \( y \).

    For example, if you have configured a response to filter for netprobe attempts, and you want to trigger an attack response if 5 or more probe attempts occur within a 30-second period, you would enter “Respond if 5 attacks in 30 seconds.”

    - **Reset attack count to zero after responding** — After \( x \) attacks, the appliance zeroes out its attack counter and waits until another \( x \) attacks occur in \( y \) seconds before sending out the next e-mail alert or SNMP trap.

    If this option is not selected, the same attacks may be used to generate additional alerts.

### Attack Description Table

<table>
<thead>
<tr>
<th>Attack</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>spam</td>
<td>Detects attacks of all severities that are spam.</td>
</tr>
<tr>
<td>spam severe</td>
<td>Detects severe attacks that are spam.</td>
</tr>
<tr>
<td>TCP SYN attack</td>
<td>Detects a possible attempt to overrun the appliance with connection attempts.</td>
</tr>
<tr>
<td>TrustedSource</td>
<td>Detects attacks identified as spam by TrustedSource.</td>
</tr>
<tr>
<td>Type Enforcement</td>
<td>Detects when there is a TE violation due to an unauthorized user or process attempting to perform an illegal operation.</td>
</tr>
<tr>
<td>virus</td>
<td>Detects attacks of all severities that are viruses.</td>
</tr>
<tr>
<td>virus severe</td>
<td>Detects severe attacks that are viruses.</td>
</tr>
</tbody>
</table>
About the Modify Attack Response: Attack Response tab

Use this tab to configure how the appliance should respond when the attack type’s pattern matches the criteria on the Attack Frequency tab. The options are:

- **Configure an alert** — The appliance can send an alert using an e-mail, an SNMP trap, or both.
  - **Send e-mail to:** Select this option and select a group from the drop-down list to send an e-mail to each address in the selected group.

  You can create different groups to receive e-mails for different types of attacks. Create groups of e-mail addresses from the main IPS Attack Response window. Additional information is available in “Configuring the e-mail response settings” on page 409.

  - **Send SNMP trap:** Select this option to send an SNMP trap to the location(s) configured for the snmpd server. (Configure the SNMP server at Policy > Services > snmpd. Additional information is available in “Sidewinder SNMP traps” on page 418.)

- [Conditional] If configuring an alert, specify how long the appliance should wait before sending the next e-mail or SNMP trap for the same attack type by using the **Wait x seconds between alerts** option.

  For example, suppose you configure an alert to trigger when 5 or more denied authentication attempts occur in a 30-second period, and you instruct the appliance to wait 300 seconds (five minutes) between alerts.

  In this configuration, if an intruder attempts to authenticate 5 times in a 30 second period, a response is triggered. However, if the intruder tries 5 more authentication attempts during the next 30 seconds, the appliance will not send another alert. Note that if the response calls for a Strikeback (see next section), traffic will continue to be blackholed.

  After five minutes, if the threshold is again reached, another alert will be triggered.

- **Configure Strikeback** — The appliance can **blackhole**, or ignore, traffic from a host that is sending suspect traffic.

  **Caution:** The appliance blackholes based on source address, as opposed to traffic type. If you choose to blackhole a host, all traffic from that host will be ignored.

  - **Blackhole:** Select this option to ignore all traffic from the suspect traffic’s source(s) for a set time period. The source of the attack is recorded in the audit event’s attack_ip field. The source of the suspect traffic may be the connection’s source IP address (a peer or a client) or destination IP address (if a server is attacking a client). If the appliance considers it likely that the source IP address could have been forged, it will leave the attack_ip field blank and not blackhole any IP address for this audit.
event. The apparent source and destination IP address is still recorded in the audit event.

If you select the Blackhole option, you must also specify for how long you want to blackhole traffic. Set a time limit in the **Blackhole packets for \(x\) seconds** field, where \(x\) is a value between 1 and 100000.

**Tip:** If you find you need to blackhole traffic for more than 100,000 seconds (a little over 24 hours), consider creating a TCP/UDP Packet Filter deny rule for that traffic.

- **All attacking hosts:** Select this option to blackhole all hosts involved in triggering the alert. For example, if you want an alert after 5 occurrences in 30 seconds and host A sent 4 occurrences and host B sent 1, all traffic from hosts A and B would be ignored for the set amount of time.

- **Each host responsible for \(y\)% of the attacks:** Select this option to limit blackholing on a percentage basis. For example, if you set the percentage at 50% and host A caused 4 out of 5 attacks and host B caused 1 out of 5 attacks, only traffic from host A would be ignored.

Use the Dashboard’s Blackholed IP window to view, delete, and manually add blackholed IP addresses.
Configuring the e-mail response settings

To view, add, modify, or delete the e-mail addresses that will receive alerts, click **Response Settings** in the IPS Attack Responses main window’s lower-right corner. The following window appears:

![Figure 178: Attack Responses: Settings window](image)

Use this window to configure groups of e-mail addresses that will receive alerts. The groups you create here can be selected in the Attack Response tab. For every triggered attack response that is set to send an e-mail alert, the selected group of e-mail addresses will receive an alert.
You can configure entries by using the buttons described here:

**Tip:** If you have not already done so, create an off-box alias for the root and administrators mail accounts. This ensures that system messages are sent to an account that is checked regularly. If mail is not forwarded or checked regularly, the local mailbox could fill up too much hard disk space and cause problems. See “Setting up e-mail aliases for administrator accounts” on page 494.

- **New** — Click this button to define a new group of e-mail addresses to receive attack alerts.
- **Modify** — Select an entry and click this button to modify an existing group of e-mail addresses.
- **Delete** — Select an entry and click this button to delete that group of e-mail addresses.
- **Blackhole source IP if attack IP cannot be confirmed [Attack Responses only]** — Select this check box to blackhole a source IP when the related audit message does not have an Attack IP field. No connections will be accepted from the IP address originating the attack.
  - This can be used to enforce thresholds on otherwise allowed behaviors (for example, limiting a connection rate for SSH traffic).
  - This feature can also be used to configure blackholing on netprobes, UDP attacks, and SYN attacks (all audit messages that do not contain an Attack IP field).

**Caution:** For netprobes, UDP attacks, and SYN attacks, it is possible for the attacker to forge the source IP address. A configuration which blackholes source addresses found in these audits may allow an attacker to trigger a blackhole for an unrelated third party, potentially interrupting desired traffic.
Creating system responses

System responses allow you to configure how the appliance responds when it detects audit events that indicate significant system events, such as license failures and log overflow issues.

To view or configure system responses, select Monitor > System Responses. The following window appears:

Use this window perform the following tasks:

- **Filter the list of system responses** — To modify the displayed list, right-click a column name and select from the current list of filters or create a custom filter. The list will then display only that system responses of that type.

- **Configure a new system event response** — To configure a new system response, click New. The Add System Response Wizard appears.

- **Modify an existing system response** — To modify an existing system response, select the appropriate item within the list and click Modify. (Read-only administrators can click View to view a system response.)

  For more information, see “Modifying a system response” on page 412.

- **Delete an existing system response** — To delete a system response, select the list item you want to delete and then click Delete.
Creating system responses

- **Disable/enable a system response** — The disable and enable options depend on a system response’s current status. If one or more responses with the same status are selected, their status can be changed to its opposite (for example, if all selected responses are enabled, you may disable all of them). When multiple responses with mixed statuses are selected, the only available action is enabling the responses.

- **Create the e-mail list to notify in the event of a system event** — To create or modify the list of e-mail addresses to notify if any system event triggers an alert, click **Response Settings**. See “Configuring the e-mail settings” on page 416 for more information.

### Modifying a system response

When you modify a system response, the following window appears:

![Figure 180: System Responses Modify window](image)

**About the Modify System Responses: Event tab**

Use this tab to change this system response’s event type. An event is generally defined as an important, generally unexpected, change in your system. Each event type identifies a different set of system changes.

1. Select the event for which you want the appliance to send out a response. A complete list is provided in the following table.

   To create additional system event types, see “Creating custom audit filters” on page 378.

2. Click **OK** or the next tab you want to modify.
**Note:** For descriptions of the audit severities, see “Understanding audit event severities” on page 443.

**Table 30: Description of pre-defined system events**

<table>
<thead>
<tr>
<th>Event</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control List</td>
<td>Detects all ACL audit events.</td>
</tr>
<tr>
<td>ACL allow</td>
<td>Detects when a connection is allowed by a rule in the active policy.</td>
</tr>
<tr>
<td>all audit</td>
<td>Detects all attack and system events, regardless of characteristics.</td>
</tr>
<tr>
<td>config change</td>
<td>Detects when the appliance’s configuration changes.</td>
</tr>
<tr>
<td>error</td>
<td>Detects all system events identified as AUDIT_T_ERROR in the audit stream.</td>
</tr>
<tr>
<td>HA failover</td>
<td>Detects when a failover IP address changes because a High Availability cluster failed over to its secondary/standby.</td>
</tr>
<tr>
<td>hardware software failure</td>
<td>Detects when a hardware or software component fails.</td>
</tr>
<tr>
<td>host license exceeded</td>
<td>Detects when the number of hosts protected by the appliance exceeds the number of licensed hosts.</td>
</tr>
<tr>
<td>IPSEC error</td>
<td>Detects when traffic generates IPSEC errors.</td>
</tr>
<tr>
<td>license expiration</td>
<td>Detects when a licensed feature is about to expire.</td>
</tr>
<tr>
<td>log overflow</td>
<td>Detects when the log partition is close to filling up.</td>
</tr>
<tr>
<td>network traffic</td>
<td>Detects all connections that successfully pass through the appliance.</td>
</tr>
<tr>
<td>not config change</td>
<td>Detects all attack and system events that are not configuration changes.</td>
</tr>
<tr>
<td>power failure</td>
<td>Detects when an Uninterruptible Power Supply (UPS) device detects a power failure and the appliance is running on UPS battery power.</td>
</tr>
<tr>
<td>syslog</td>
<td>Detects all audit attacks and system events created via syslog.</td>
</tr>
<tr>
<td>system all</td>
<td>Detects all system events of all severities, including power failures, hardware and software failures, failover events, license expiration, host license exceeded, log overflows, and IPSEC errors.</td>
</tr>
</tbody>
</table>
## About the Modify System Responses: Event Frequency tab

Use this tab to modify the parameters to be met before the appliance generates a response. The options are:

- **Always respond** — Select this option to have the appliance respond each time the event type specified on the Event tab occurs.

- **Limit responses** — Select this option to respond only when the event’s pattern matches the parameters set here:
  - **Respond if \( x \) events in \( y \) seconds** where:
    - valid values for \( x \) are between 2 and 100000. The appliance responds when the \( x \) event occurs.
    - valid values for \( y \) are between 1 and 100000. This represents the last \( y \) seconds, so the appliance checks the current time - \( y \).
  - **Reset event count to zero after responding** — After \( x \) events, the appliance zeroes out its event counter and waits until another \( x \) events occur in \( y \) seconds. If this option is not selected, each subsequent system event that occurs in \( y \) seconds will generate a response.

For example, if you want to respond to 5 events in 30 seconds, the appliance constantly checks the past 30 seconds. When the appliance receives 5 system events in that time frame, it responds according to the Event Response tab settings. If it zeroes out after responding, it waits until 5 more events occur in a 30 second time period before responding again.
About the Modify System Response: Event Response tab

Use this tab to configure how the appliance should respond when the event matches the parameters on the Event Frequency tab. The appliance can send an alert using an e-mail, an SNMP trap, or both. The options are:

- **Configure an alert.** The appliance can send an alert using an e-mail, an SNMP trap, or both.
  - **Send e-mail to:** Select this option and select a group from the drop-down list to send an e-mail to each address in the selected group.
    
    You can create different groups to receive e-mails for different types of events. Create groups of e-mail addresses from the main System Response window. Additional information is available in “Configuring the e-mail settings” on page 416.
  - **Send SNMP trap:** Select this option to send an SNMP trap to the location(s) configured for the snmpd server. (Configure the SNMP server at **Services Configuration > Servers > snmpd**. Additional information is available in “Sidewinder SNMP traps” on page 418)

- **[Conditional]** If configuring an alert, specify how long the appliance should wait before sending the next e-mail or SNMP trap for the same system event by using the **Wait x seconds between alerts** option. Valid values are between 0 and 65535.

For example, suppose you configure an alert to trigger when 10 or more IPsec errors occur in a 60 second period, and you instruct the appliance to wait 300 seconds (five minutes) between alerts.

In this configuration, if the appliance detects 10 errors in a 60 second period, a response is triggered. However, if it detects 5 more IPsec errors during the next 30 seconds, the appliance will not send another alert.

After five minutes, if the threshold is again reached, another alert will be triggered.
Configuring the e-mail settings

To view, add, modify, or delete the e-mail addresses that will receive alerts, click **Response Settings**, in the System Responses main window’s lower right corner. The following window appears:

![System Responses: Response Settings window](image)

Use this window to configure groups of e-mail addresses that will receive alerts. The groups you create here can be selected in the Event Response tab. For every triggered system event response that is set to send an e-mail alert, the selected group of e-mail addresses will receive an alert.

You can configure entries by using the buttons describe here:

- **New** — Click this button to define a new group of e-mail addresses to receive system event alerts.
- **Modify** — Select an entry and click this button to modify an existing group of e-mail addresses.
- **Delete** — Select a group and click this button to delete that group of e-mail addresses.
Ignoring network probe attempts

If a host on the network attempts to connect to the appliance for a service that is not running, an audit record is generated and may trigger an alarm. An ignore list can be set up to ignore unimportant network probe audit events, but save the audit to keep track of the probe attempts. However, if connection attempts are frequent and are coming from a trusted network, then it may be desirable to ignore them completely and not audit the connection attempt by configuring the appropriate filter rules.

To ignore network probes (commonly referred to as *netprobes*), you can create filter rules to deny connection requests for specific ports. For example, if you have problems with NetBios generating netprobes on the appliance, you can discard them and prevent audit events by creating a filter service and rule with the following key values:

- For the service, set the Agent field to **Generic Filter** and set the UDP ports field to **137**. See the following figure.

  ![Figure 182: Example of how to configure a service that can be used to deny NetBIOS netprobes](image)

  **Figure 182**: Example of how to configure a service that can be used to deny NetBIOS netprobes

- For the rule, set the Action to **Deny** or **Drop**, set Audit to **Errors only (least)**, set the source and destination burbs to **internal**, and the endpoints to **<Any>**. See the following figure.

  ![Figure 183: Example of how to configure a rule that can be used to deny NetBIOS netprobes](image)

  **Figure 183**: Example of how to configure a rule that can be used to deny NetBIOS netprobes
Sidewinder SNMP traps

An SNMP trap is an alert message (also known as an alarm message) that is sent as an unsolicited transmission of information from a managed node (router, Sidewinder appliance, etc.) to a management station. The appliance gives you the option of sending audit alert SNMP traps when an audit event, such as an IPS attack event or a system event, triggers a response. Pre-defined (default) alert events are shown in Table 31 on page 418. You also have the option to create custom traps; refer to Table 31.

- For instructions on creating a custom trap, see the `snmptrap` man page.
- To configure the appliance to send the following pre-defined traps, refer to “About the Modify Attack Response: Attack Response tab” on page 407 and “About the Modify System Response: Event Response tab” on page 415.

These traps can also be used in customized audit filters. See “Saving a custom audit filter” on page 373 and “Creating custom audit filters” on page 378 for more information.

Table 31: SNMP traps

<table>
<thead>
<tr>
<th>Number</th>
<th>Trap</th>
</tr>
</thead>
</table>
| 1      | NETWORK_TRAFFIC — This trap is sent when the number of traffic audit events written by the various proxies (WWW, Telnet, FTP, etc.) going through the appliance exceeds a specified number in a specified time period. This information can be useful for monitoring the use of the Sidewinder services by internal users.  
**Note:** Network traffic thresholds are reported as number of events per second, and not as number of bytes per second. |
| 2      | ATTACK_ATTEMPT — This trap is sent when an attack attempt (that is, any suspicious occurrence) is identified by one of the services on the appliance. For example, if the Network Services Sentry (NSS) detects a suspicious IP address on an incoming connection, it will issue an attack attempt trap. |
| 3      | TE_VIOLATION — This trap is sent when an unauthorized user or process attempts to perform an illegal operation on a file on the appliance. |
| 4      | ACCESS_CONTROL — This trap is sent when the number of denied access attempts to services exceeds a specified number. For example, you may set up your system so that internal users cannot FTP to a certain Internet address. If a user tried to connect to that address, the attempt would be logged as a denial. |
| 5      | BAD_PROXY_AUTH — This trap occurs when a user tries to get authenticated to the telnet or FTP proxy and enters invalid data. |
### Sidewinder SNMP traps

<table>
<thead>
<tr>
<th>Number</th>
<th>Trap</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>PROBE_ATTEMPT — This trap is</td>
<td>This trap is sent when network probe attempts are detected. A network probe is any time a user attempts to connect or send a message to a TCP or UDP port that either has no service associated with it or it is associated with an unsupported service. To ignore network probe attempts, create a filter deny rule to discard probes coming from recognized offenders. See “Ignoring network probe attempts” on page 417 for key values to configure.</td>
</tr>
<tr>
<td>7</td>
<td>FILTER_FAILURE — This trap</td>
<td>This trap occurs when the number of mail messages or HTTP messages that failed the keyword filter exceed a specified threshold in a specified time period.</td>
</tr>
<tr>
<td>8</td>
<td>IPSEC_FAILURE — The trap</td>
<td>The trap occurs when the IPSEC subsystem detects a failure in authentication or encryption of network traffic. This can be caused by a number of things ranging from key configuration errors, ISAKMP problems, interoperability issues, and network attacks.</td>
</tr>
<tr>
<td>9</td>
<td>FAILOVER_EVENT — This trap</td>
<td>This trap is sent any time a Sidewinder appliance changes its status in an HA cluster from secondary to primary, or from primary to secondary.</td>
</tr>
<tr>
<td>10</td>
<td>LOG_FILE_OVERFLOW — This trap</td>
<td>This trap is sent when the Sidewinder audit logs are close to filling the partition.</td>
</tr>
<tr>
<td>11</td>
<td>SYN_FLOOD_ATTACK — This trap</td>
<td>This trap is sent when the appliance encounters a SYN attack.</td>
</tr>
<tr>
<td>12</td>
<td>UPS_POWER_FAILURE — This trap</td>
<td>This trap is sent when a connected Uninterruptible Power Supply (UPS) has a power failure and the appliance is running on UPS battery power.</td>
</tr>
<tr>
<td>13</td>
<td>UPS_SYSTEM_SHUTDOWN — This</td>
<td>This trap is sent when the appliance has been running on UPS battery power for the estimated battery time. (See “Configuring the Sidewinder appliance to use a UPS” on page 64 for additional information on UPS.)</td>
</tr>
<tr>
<td>14</td>
<td>LICEXCEED_FILTER — This trap</td>
<td>This trap is sent when users are denied access through the appliance due to a user license cap violation.</td>
</tr>
<tr>
<td>26</td>
<td>CRIT_COMP_FAILURE — This trap</td>
<td>This trap is sent when the appliance detects that a critical component has failed. For example, this trap occurs when daemon detects a software module has failed.</td>
</tr>
<tr>
<td>27</td>
<td>VIRUSMIME — This trap</td>
<td>This trap occurs when the number of mail or HTTP messages that failed the MIME/Virus/Spyware filter exceeds a specified threshold in a specified time period.</td>
</tr>
<tr>
<td>Number</td>
<td>Trap</td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td>----------------------</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Custom traps</strong></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>USER_DEFINED_DEFAULT</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>USER_DEFINED_1</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>USER_DEFINED_2</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>USER_DEFINED_3</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>USER_DEFINED_4</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>USER_DEFINED_5</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>USER_DEFINED_6</td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>USER_DEFINED_7</td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>USER_DEFINED_8</td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>USER_DEFINED_9</td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>USER_DEFINED_10</td>
<td></td>
</tr>
</tbody>
</table>
In this chapter...

Understanding processes that control server status ....................422
Viewing service status ..................................................................426
Viewing a service’s process information ......................................429
Understanding processes that control server status

There are two significant processes involved in controlling and monitoring service status: daemond and NSS. daemond controls the starting, stopping, and restarting of services, and NSS handles port assignments.

Learn more about these processes in the following sections:

• “daemond” on page 422
• “Network Services Sentry (NSS)” on page 425

**daemond**

If you have administered a standard UNIX system, you are probably familiar with `init`, which manages process control initialization. On the Sidewinder appliance, `init` has been augmented with the **daemond** process. daemond is a powerful component that enhances overall security. It monitors and controls all of the major software components on the appliance.

The daemond process also detects and audits some classes of attacks against the appliance. For example, should someone try to attack a Sidewinder service (such as sendmail), causing the component to crash, the daemond process detects the failure, immediately restarts the failed component, and creates a critical event audit entry, which allows the administrator to be notified and respond to the attack.

daemond starts during the Sidewinder boot process. On start up, it reads the `/secureos/etc/daemond.conf` file to determine its configuration options. By default, daemond runs in its normal mode. This means that daemond attempts to start all enabled components in the `/etc/server.conf` and `/secureos/etc/nss.common.conf` files. daemond is capable of restarting and stopping processes both automatically and manually. A full description of daemond’s usage is available on the `cf_daemond` man page. If daemond detects certain failure events, it switches to failure mode. Failure mode is explained in “About failure mode” on page 424.
Chapter 14: Service Status

Understanding processes that control server status

Restarting processes

If a component dies unexpectedly, daemond restarts that component and audits the event in both the audit log and the daemond log. The message in /var/log/daemond.log is similar to this:

```
```

If a component quits within five seconds of starting three times in a row, daemond does not attempt to restart the component until the next time daemond gets a SIGHUP. This event will also be audited to both the audit log and the daemond log. The message in /var/log/daemond.log will look similar to this:

```
Jan 17 13:26:38 2007 EST: ftp (7061) died after restart; not restarting
```

You can manually restart an agent using the Service Status window or:
```
cf daemond restart agent=agentname.
```

**Note:** When you restart an agent, you restart all the processes related to that agent. If you have multiple services using the same agent, all those services are restarted.

Responsive service processes

daemond monitors some services for responsiveness. If a service does not respond to periodic messages within 15 seconds, daemond gathers diagnostic information, kills the process, and then restarts it.

These services are monitored:

- NSS
- HTTP proxy
- HTTPS proxy
- TCP proxy
- DNS proxy

The diagnostic information is gathered in a tar archive and stored in /var/diagnostics. If three tar archives are gathered for a service, daemond kills and restarts the process, but stops gathering diagnostics.

You can change the number of seconds that daemond waits for a response before starting the diagnostic program from the command line using:
```
cf daemond set ping_timeout=seconds
```

For more information, see the diagnostic man page.
**Stopping processes**

daemon is also responsible for *stopping* processes. If a Sidewinder administrator chooses to disable a process (using the Admin Console or cf commands), the configuration files are changed and a `SIGHUP` command is sent to daemon. The `SIGHUP` command signals daemon to reread the configuration files. If daemon finds an entry associated with a currently running process that is now marked as disabled, daemon will stop that process. The process will not be started again until it is re-enabled by an administrator. Re-enabling a process will cause another `SIGHUP` command to be sent to daemon, which will reread the configuration files and attempt to restart the process.

All component failure events are logged in the `/var/log/daemond.log` file and the audit log. If daemon fails during system startup, the daemon log file will record the reason for this failure. It will also record information each time daemon restarts a process that died unexpectedly. This is useful for tracking attacks on a particular component.

**About failure mode**

When a failure event occurs, daemon will start in failure mode. This mode is also called *safe mode*. This means that daemon only starts those components necessary to administer the system. Components that are not enabled for failure mode will not be started, which includes most proxy agents.

Failure mode is set under any of the following circumstances:

- a license check fails
- the audit partition overflows

Once the problem that sent the appliance into failure mode has been corrected, use `cf daemond set failure_mode=off` to resume normal operation.

**About High Availability and daemon**

If you configure a failover High Availability (HA) cluster, the standby Sidewinder appliance will run in standby mode with a limited set of services. If the primary becomes unavailable and the standby is required to take over as the primary, daemon will start all services for that appliance.

If the primary in an HA cluster goes into failure mode and the secondary/standby is not available, the primary will remain as the primary, but the priority value for that appliance will change to one, ensuring that if a secondary/standby becomes available, it can take over as the primary. For information on HA, see Chapter 24, "High Availability" on page 747.
Network Services Sentry (NSS)

If you have administered a standard UNIX system, you are probably familiar with **inetd**, which listens for connections and manages daemons for network services. Daemons are server processes that run continuously in the background and wait until they are needed. On the Sidewinder appliance, inetd has been replaced with the Network Services Sentry (NSS). There is an NSS configuration file for each burb defined on your appliance. NSS regulates the ability to change the default port. For example, the files are updated whenever you change a service’s ports.

You may use the Admin Console or the command line to edit a service’s default ports. The NSS configuration files are updated for you when you make these changes. For example, you might want to alter ports when the default conflicts with the port of another service, or when you want to create a portlist with non-continuous numbers.

When changing the port for a service, be sure to consider the criteria listed in Table 32 below.

**Table 32: Criteria for modifying a service port**

<table>
<thead>
<tr>
<th>Port type</th>
<th>Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>• Valid port values are between 1–65535.</td>
</tr>
<tr>
<td></td>
<td>• Must be unique within ports assigned to other enabled services of the same type</td>
</tr>
<tr>
<td>Port range</td>
<td>• Must be two valid ports separated by a single hyphen</td>
</tr>
<tr>
<td></td>
<td>• Must be listed in ascending order</td>
</tr>
<tr>
<td></td>
<td>• The range must have a maximum of 1995 ports. If a service requires more than 1995 ports, use a portlist.</td>
</tr>
<tr>
<td>Portlist</td>
<td>• May be non-continuous</td>
</tr>
<tr>
<td></td>
<td>• Valid ports and/or valid ranges separated by commas</td>
</tr>
</tbody>
</table>
Viewing service status

Knowing a service's status is an important part of monitoring your Sidewinder appliance. It can help you verify that a service is configured correctly, and it can help you determine if the service is running as expected. The Service Status window allows you to view configuration and status information on all services that are enabled on your appliance. It has shortcuts to audit and usage information so you can easily gather information about individual services. You can also restart a service from this window, which is sometimes required after certain configuration changes or as a troubleshooting step.

To view the services that are currently used in enabled rules, select Monitor > Service Status. The main Service Status window appears.

![Figure 184: The main Service Status window](image)

You can accomplish the tasks listed in the following table using the toolbar shown here.

### Figure 185: Tasks available in the Service Status window

<table>
<thead>
<tr>
<th>Process Information</th>
<th>Restart</th>
<th>Usage</th>
<th>Search</th>
<th>Refresh</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Audit Data</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Temporarily Disable</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Status</th>
<th>Service</th>
<th>Burbs</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>📈</td>
<td>Admin Console</td>
<td>external</td>
<td>9003/tcp</td>
</tr>
<tr>
<td>🗂️</td>
<td>dns</td>
<td>Firewall, external, internal</td>
<td>53/tcp, 53/udp</td>
</tr>
<tr>
<td>🗂️</td>
<td>ftp</td>
<td>internal</td>
<td>21/tcp</td>
</tr>
<tr>
<td>🗂️</td>
<td>http</td>
<td>internal</td>
<td>80/tcp</td>
</tr>
<tr>
<td>🗂️</td>
<td>https</td>
<td>internal</td>
<td>443/tcp</td>
</tr>
<tr>
<td>🗂️</td>
<td>ping</td>
<td>internal</td>
<td></td>
</tr>
<tr>
<td>🗂️</td>
<td>realmedia</td>
<td>internal</td>
<td>7070/tcp</td>
</tr>
</tbody>
</table>
### Table 33: Tasks that can be performed from the main Service Status window

<table>
<thead>
<tr>
<th>Icon/Menu item</th>
<th>Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process Information</td>
<td>View the service’s status (running as expected, running with errors, not running), its ports, burbs, and where it is listening by selecting a service and clicking <strong>Process Information</strong>. Opening this window is most useful for checking that a service is listening on the expected ports or for monitoring the status of a single service. For more information, see “Viewing a service’s process information” on page 429.</td>
</tr>
<tr>
<td>View Audit Data</td>
<td>View a service’s audit data by selecting a service and clicking <strong>View Audit Data</strong>. This displays the past 24 hours of data. Additional audit viewing is available at <strong>Monitor &gt; Audit</strong>.</td>
</tr>
<tr>
<td>Restart</td>
<td>Restart services by selecting one or more services and then clicking <strong>Restart</strong>. Clicking <strong>Restart</strong> also re-enables a disabled service. In this case, the Sidewinder appliance first checks the policy to verify that the service should be enabled. <strong>Caution:</strong> Before you restart a service, make sure you know which agent the service is using. A restart disables and enables the underlying agent, which means all connections using this agent will be dropped as opposed to just dropping the connections using this service.</td>
</tr>
<tr>
<td>Temporarily Disable</td>
<td>Temporarily disable services by selecting one or more services and then clicking <strong>Temporarily Disable</strong>. <strong>Tip:</strong> A quick way to safely re-enable all stopped agents is to change a rule or service’s description and save the changes.</td>
</tr>
<tr>
<td>Usage</td>
<td>View the rules that currently use a given service by selecting a service and then clicking <strong>Usage</strong>.</td>
</tr>
<tr>
<td>Find</td>
<td>Find a service by entering a character string related to the service you are searching for in the <strong>Find</strong> field. The search function searches all columns, and filters as you type. For example, if you are searching all services running in the DMZ burb, typing “DMZ” reduces the list to only the services containing that character string. Clear the Find field to show all options again.</td>
</tr>
<tr>
<td>Refresh</td>
<td>View current information for all services by clicking <strong>Refresh</strong>.</td>
</tr>
</tbody>
</table>
This window displays the following information about each service:

- **Status** Indicates if the service is running as expected
  - **Running** The service is processing traffic as expected.
  - **Running with errors** The service is processing traffic but it is generating errors and needs to be investigated, or is temporarily disabled.
  - **Not running** The service is not running, or no information is available about the service’s status. The service needs to be investigated.

- **Service** The service’s name
  - *Note:* *kvmfilter, spamfilter, and virus-scan appear when these options are selected on an enabled rule’s application defense. They are not associated with an agent. See the related service, such as *sendmail*, for complete burb and port information.*

- **Burbs** The burbs where a service is enabled
  When a service is used in a rule, the service is enabled in that rule’s source burb. All source burbs for rules that use this service are listed here. The icon indicates that the service is enabled in all burbs valid for that service.
  - *Note:* Certain services display the Firewall burb. This burb is used for Sidewinder internal processing and cannot be modified. Sendmail only runs in two burbs, even if the source burb is set to <Any>.

- **Ports** The ports configured for the service

- **Active Rules** The enabled rules that use this service
This section provides information on the Service Status Process Information window. You can access this window by selecting Monitor > Service Status and then double-clicking a service, or selecting a service and then clicking Process Information on the toolbar.

The Service Status Process Information window appears.

Use the Process Information window to view the burbs and ports on which the service should be listening, as well as the service's current status.

From this window, you can do the following:

- Refresh the data — Click Refresh to display current status information.
- Check a service's status — Status is displayed near the top of the window. Possible statuses are:
  - **Running** — The service is processing traffic as expected.
  - **Running with errors** — The service is processing traffic but it is generating errors and needs to be investigated, or is temporarily disabled.
  - **Not running** — The service is not running, or no information is available about the service’s status. The service needs to be investigated.
• View where the service is running and listening for connections —
  Configuration areas are:

  Configured Burb  When a service is used in a rule, the service is
  enabled in that rule's source burb. All source burbs
  for rules that use this service are listed here.

  Configured Port  All ports that are configured for this service are listed
  here.

  Listening  When a service is listening (accepting connections)
  on a port, a green check mark appears in this column.

  **Important:** If a port does not have a check mark next
to it, there is a problem with the service that needs to
be investigated. Contact Technical Support for
assistance.

  **Note:** The kvmfilter, spamfilter, and virus-scan services appear when these
options are selected on an enabled rule's application defense. They are not
associated with an agent. See the related service for complete burb and port
information.

• Restart or re-enable the service's agent — Click **Restart** to restart or re-
  enable the agent used by this service. Restarting a service disables and
  then immediately enables the service's agent. This action drops all current
  connections and resets any audit counts (for example, if an IPS attack
  response is checking the frequency of an attack before issuing an alert). Do
  not restart an agent unless it is part of a procedure, you have completed
  other troubleshooting measures, or have been instructed to by Secure
  Computing Technical Support.

  **Caution:** Restarting a service drops all current connections for that agent, not
  just the selected service.

• Temporarily disable the service's agent — Click **Temporarily Disable** to halt
  the agent used by this service. Temporarily disabling a service stops the
  service's agent. The agent is restarted as soon as any policy configuration
  changes are saved. Do not temporarily disable an agent unless it is part of
  a procedure, you have completed other troubleshooting measures, or have
  been instructed to by Secure Computing Technical Support.

  **Tip:** A quick way to safely re-enable all stopped agents is to change a rule or
  service's description and save the changes.

• View audit of errors — If a service is not running as configured, click
  **View Audit** to view audit output that is filtered to show this service's activity
  over the past 24 hours.

Click **Close** to return to the main Service Status window.
In this chapter...

Monitoring Sidewinder status using the dashboard..........................432
Viewing device information...........................................................434
Viewing network traffic information...........................................438
Viewing IPS attack and system event summaries.......................443
Chapter 15: The Dashboard

Monitoring Sidewinder status using the dashboard

The Admin Console allows you to monitor status information on your Sidewinder appliance using its dashboard. The `monitord` server records data about the system and traffic status. Auditbots detect packets and traffic patterns that may be of interest to administrators. The dashboard gathers this data from those and other Sidewinder components and provides a centralized view of important system and audit data. This window displays summary data and specific audit events.

The dashboard allows you to monitor the following Sidewinder areas:

- Device information (version, uptime, configuration state, etc.)
- Network traffic (active VPN and proxy sessions, interface status, etc.)
- Recently detected attack activity
- System events (hardware and software failures, log overflows, etc.)

You can set this information to refresh automatically or on demand.

While this window is a useful tool to observe your appliance, you may also want to take advantage of other audit and monitoring tools:

- For additional audit information, see Chapter 12, "Auditing," on page 359.
- For information on commands that monitor the appliance, see “Monitoring Sidewinder status” on page 807.

When you log into the Admin Console, the dashboard displays. To view the dashboard at any other time, click the top node of the tree labeled `appliance_name Dashboard`. A window similar to the following appears:

![The dashboard](image-url)
The dashboard allows you to monitor various Sidewinder areas. It displays statistics recorded since the last reboot. From the dashboard, you can:

- **Monitor the appliance’s status** — Monitor general system information, what traffic is passing through the appliance, and system and attack events. For more information on each area, see the following sections:
  - “Viewing device information” on page 434
  - “Viewing network traffic information” on page 438
  - “Viewing IPS attack and system event summaries” on page 443

- **View additional information** — Learn more about any given area by clicking the appropriate link or magnifying glass 🕵️.

- **Change the refresh rate** — Indicate how often the dashboard will refresh by using the Refresh Rate field. Valid values range from 30 seconds to 30 minutes. There is also a Manual Refresh option. The default is 5 minutes. When you modify the refresh rate, the change will not take effect until the next scheduled refresh time. To make the change take effect immediately, change the refresh value and click the Refresh icon.

- **Manage blackholed IP addresses** — View a list of the IP addresses the appliance is currently blackholing. You can also delete addresses that do not need to be blackholed and manually add new addresses to the list. To manage blackholed IP addresses, click Blackholed IPs.

- **Disconnect** — Disconnect the current Admin Console session by clicking the Disconnect button. If you hover the mouse pointer over the Disconnect button, a tool tip appears that includes the connected appliance’s IP address.
The dashboard’s Device Information area, shown in Figure 188, displays basic system information. The device information that this area monitors includes: the Sidewinder appliance host name, the amount of time since the last reboot, the date and time, the current version, the serial number, data about logged-in administrators, and basic system resource data for the whole system, with the option to view process-specific data as well.

The relevant information appears on separate tabs in the pop-up window.

In this area, you can do the following:

- View information about administrators who are logged into this appliance by clicking **Logged-In Administrators**.

- View process use and disk use information by clicking **System Resources**. The relevant information appears on separate tabs in the pop-up window.

- Receive feedback that a system resource may be experiencing trouble. If the value turns red, the memory or disk may be getting too full and requires attention. Click **System Resources** to view more information.
About the Logged-In Administrators window

Use this window to view information about administrators who are currently logged into this appliance.

![Figure 189: The Logged-In Administrator window](image)

The Logged-In Administrators window displays the following information:

- **Login Name** — Logged-in administrators’ user names
- **Access Type** — Management program/protocol (Admin Console, SSH, Telnet, System Console)
- **Remote Host** — If not using the Admin Console, the IP address or host name of the host that initiated the management session.
- **Login Time** — Time stamp of the most recent successful login
- **Idle Time** — Time since the administrator’s last action
- **Current Task** — What each administrator is doing when the window is refreshed (if known)

On this tab, you can do the following:

- Select one or more administrator’s rows and then click **Terminate Session(s)** to close an open session.
- Click **Refresh** to view current information. This window does not automatically refresh.
- Click **Close** to close this window and return to the dashboard.
About the Process Use tab

This tab displays the status of each process that is currently running on this Sidewinder appliance.

It provides the following details for each process:

- **Process** — This column displays the name of each running process.
- **CPU** — This column displays the percentage of CPU currently being used.
- **Process Size** — This column displays the amount of memory a process is using.
- **Resident Memory** — This column displays the amount of physical memory a process is using.

On this tab, you can do the following:

- Click **Refresh** to update this tab’s data.
- Click **Close** to close this window and return to the Dashboard.
About the Disk Use tab

This tab displays how much of the appliance’s hard disk space is currently being used.

**Note:** The /dev file system is a virtual file system and does not actually occupy space on your hard drive. The Percent Used column should display 100% used, and the Used value should be 1.00 KB.

![Figure 191: System information: Disk Use tab](image)

<table>
<thead>
<tr>
<th>Mounted On</th>
<th>Percent Used</th>
<th>Used</th>
<th>Available</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/dev</td>
<td>100%</td>
<td>1.00 KB</td>
<td>2.57 GB</td>
<td>Devices</td>
</tr>
<tr>
<td>/usr</td>
<td>21%</td>
<td>192.74 MB</td>
<td>717.35 MB</td>
<td>System tools and utilities such as man pages, Perl, and...</td>
</tr>
<tr>
<td>/</td>
<td>14%</td>
<td>20.88 MB</td>
<td>121.78 MB</td>
<td>Standard UNIX libraries and system configuration settings.</td>
</tr>
<tr>
<td>/home</td>
<td>6%</td>
<td>114.74 MB</td>
<td>1.67 GB</td>
<td>Home directories for administrator accounts</td>
</tr>
<tr>
<td>/proc</td>
<td>4%</td>
<td>101.15 MB</td>
<td>2.57 GB</td>
<td>Package data</td>
</tr>
<tr>
<td>/var</td>
<td>1%</td>
<td>33.66 MB</td>
<td>2.57 GB</td>
<td>Configuration backups, process run directories, package...</td>
</tr>
<tr>
<td>/root</td>
<td>1%</td>
<td>28.46 MB</td>
<td>2.57 GB</td>
<td>Configuration, policy, ARFF files</td>
</tr>
<tr>
<td>/swap</td>
<td>0%</td>
<td>0 KB</td>
<td>8.00 GB</td>
<td>Swap space</td>
</tr>
<tr>
<td>/var/spool</td>
<td>0%</td>
<td>292.00 KB</td>
<td>6.36 GB</td>
<td>Queued mail traffic, Admin Console package data</td>
</tr>
<tr>
<td>/var/log</td>
<td>0%</td>
<td>6.03 MB</td>
<td>8.23 GB</td>
<td>Auditing and logging information</td>
</tr>
<tr>
<td>/tmp</td>
<td>0%</td>
<td>12.00 KB</td>
<td>227.90 MB</td>
<td>Temporary files</td>
</tr>
</tbody>
</table>

It provides the following details for each disk partition:

- **Mounted On** — This column displays the name of each disk partition.
- **Percent Used** — The column displays the percent of that partition being used.
- **Used** — This column displays the amount of a given partition being used.
- **Available** — This column displays the amount of disk space available for use in the given partition.
- **Description** — This column displays a description of the disk partition.

On this tab, you can do the following:

- Click **Refresh** to update this tab’s data.
- Click **Close** to close this window.
Chapter 15: The Dashboard

Viewing network traffic information

The dashboard’s Network Traffic area, shown in Figure 192, displays information on network traffic passing through the appliance. View information such as number of interfaces up and receiving traffic, number of active filter rules, number of active VPN sessions, and number of active proxy and server service connections.

![Figure 192: Dashboard: Network Traffic area](image)

<table>
<thead>
<tr>
<th>Network Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Interface Status</strong></td>
</tr>
<tr>
<td>Up: 3 Down: 3</td>
</tr>
<tr>
<td><strong>Rate</strong></td>
</tr>
<tr>
<td>Inbound: 11 B/min Outbound: 9 B/min</td>
</tr>
</tbody>
</table>

- **Blackholed IPs**: 2

- **Packet Filter Sessions**: TCP: 0 UDP: 0
- **VPN Sessions**: Idle: 2 Active: 4
- **Proxy Connections**: TCP: 28 UDP: 11

Use this area of the dashboard to monitor the following:

- **Interface Status** — Displays the status of all physical and VLAN interfaces in the appliance. The displayed rate is data on the transfer speed in the last minute, reported in bytes per minute. The displayed total is the number of inbound/outbound bytes processed since the last reboot.
  
  Click **Interface Status** to view additional information about each interface. See "About the Interface Status window" on the following page for more information.

- **Blackholed IPs** — Click **Blackholed IPs** to view and manage the currently blackholed IP addresses. See “About the Blackholed IPs window” on page 440 for more information.

- **Packet Filter Sessions** — Displays the number of packet filter sessions that are currently open. A rule’s filter service must have Stateful Packet Inspection enabled to create a session.

- **VPN Sessions** — Click **VPN Sessions** to view additional information about configured VPNs. See “About the Active VPNs window” on page 441 for more information.

- **Proxy Connections** — Displays the current number of TCP and UDP sessions. Click **Proxy Connections** to view a list of each proxy and server service that is currently passing traffic and the number of instances each service. Click **TCP**: to display how many connections are in each state. See “About the Proxy Connections window” on page 441 and “About the TCP State Information window” on page 442 for more information.
About the Interface Status window

Use this window to view traffic information for each of the physical and VLAN network interfaces on this appliance.

The following information is provided:

- **Interface** — Displays the name of the interface
- **IP Address** — Displays the IP address assigned to that interface
- **Status** — Displays if the interface’s status is up (ready for an active network connection) or down (will not accept an active network connection)
- **Connected** — Displays the following statuses:
  - **Connected** if the appliance detects an active network connection
  - **Disconnected** if the interface is enabled but does not detect a carrier (active network connection)
  - **Unknown** if the interface is not enabled

You can also view this information at a command line interface by typing `ifconfig` or `netstat -i`.

On this window, you can do the following:

- Click **Refresh** to update this tab’s data.
- Click **Close** to close this window.
About the Blackholed IPs window

Use this window to view and manage the currently blackholed IP addresses.

Each entry in the table displays the IP address, burb, and the date and time at which the IP address will no longer be blackholed. You can perform the following actions in this window:

- **Add an IP address to blackhole** — To add an IP address to this list, click Add. In the Add Blackhole IP pop-up window, enter the IP address you want to blackhole and how long, in seconds, before the appliance will accept and respond to traffic from that IP address. This address is then automatically blackholed on all configured burbs.

- **Delete one or more entries** — To remove one or more entries from the list, select the row you want to delete and click Delete. To select multiple rows, press and hold the Ctrl key as you select the items.

- **Delete all IP entries** — To remove all of the entries that are listed in the table, click Delete All.

- **Update the window** — To retrieve an updated list of blackholed IP addresses, click the Refresh Now icon. The date and time when displayed data was captured is listed in the upper portion of the window.

Click Close to exit the window. Change are saved automatically.
About the Active VPNs window

Use this window to monitor the status of all configured VPNs.

The statuses include:

- **Idle** — No active session.
- **Active** — One or more VPNs have active sessions established for this VPN.

Click **Refresh** to update the information. Click **Close** to return to the main window.

About the Proxy Connections window

Use this window to monitor the type and number of active proxy sessions going through the appliance.
Chapter 15: The Dashboard

Viewing network traffic information

Information provided includes:

- **Name** — Name of the proxy passing traffic
- **Count** — Number of current instances

On this window, you can:

- Click **Refresh** to update the information.
- Click **Close** to return to the main window.

### About the TCP State Information window

Use this window to monitor the various states of the TCP proxy connections going through the appliance.

**Figure 197: Network Traffic: TCP State Information window**

<table>
<thead>
<tr>
<th>TCP State</th>
<th>Count</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Established</td>
<td>7</td>
<td>An open connection ready to transmit and receive data</td>
</tr>
<tr>
<td>Time Wait</td>
<td>61</td>
<td>A connection waiting to ensure the remote TCP session received the...</td>
</tr>
<tr>
<td>FIN Wait 1</td>
<td>0</td>
<td>A connection waiting for a termination request or an acknowledgement...</td>
</tr>
<tr>
<td>FIN Wait 2</td>
<td>0</td>
<td>A connection waiting for a termination request</td>
</tr>
<tr>
<td>Close Wait</td>
<td>0</td>
<td>Waiting for a termination request from the local user</td>
</tr>
</tbody>
</table>

Information provided includes:

- **TCP State** — Lists the different possible states of a TCP connection.
- **Count** — Number of TCP sessions in that state
- **Description** — Describes that row’s TCP state.

On this window, you can:

- Click **Refresh** to update the information.
- Click **Close** to return to the main window.
The statistics summary area of the dashboard displays a summary of the audit events the Sidewinder appliance detects. By default, the appliance audits packet and traffic patterns it assumes to be an attack. It also audits system events administrators tend to consider important. Each predefined audit event is related to a severity. The dashboard summarizes the audit events for a given time frame, providing administrators a quick overview of audit activity. View additional details by clicking the magnifying glasses, links, and audit rows.

### Understanding audit event severities

IPS attack audit events are based on anomaly detection. They are not necessarily detecting a specific attack attempt, but are detecting unexpected or suspicious deviations from allowed packets and patterns. The severities represent the assumed risk to the appliance and its protected systems if the attack had not been blocked. For example, an attack event generated by a commonly occurring packet that is used to gather information is considered a warning. An attack event made up of packets that appear to be crafted and, if not blocked, could crash a vulnerable system are considered severe or critical. Administrators should immediately investigate all critical attacks.

System audit events are generated by expected and unexpected system behavior. The severities are generally based on the type of action, if any, an administrator should take in response to the event. Whereas a critical event generally requires immediate investigation, a warning generally requires no action from the administrator.

Table 34 defines each severity in more detail.
### Table 34: Definitions of IPS attack and system event severities

<table>
<thead>
<tr>
<th>Severity</th>
<th>Definition</th>
</tr>
</thead>
</table>
| Critical | • Indicates activity that is definitely an attack and that could have significantly affected a protected system had it not been prevented.  
• Indicates that a system component or subsystem stopped working, that the system is going down (expectedly or unexpectedly), or that the system is not expected to work again without intervention.  
At the command line, these audit events are classified as emergency, alert, critical, and fatal priorities. |
| Severe   | • Indicates activity that represents a likely significant attack or policy violation.  
• Indicates something is occurring in the system that an administrator should know.  
At the command line, these audit events are classified as a major priority. |
| Warning  | • Indicates activity that may be an attack or information gathering, or that represents a minor attempted violation of the site security policy (for example, attempting to use a restricted FTP command).  
• Indicates something is occurring in the system that an administrator might want to know or might consider trivial.  
At the command line, these audit events are classified as minor or trivial priorities. |
Viewing the summary statistics

The summary statistics area is located in the lower portion of the dashboard, as shown in Figure 198.

**Figure 198: Summary statistics area**

In this area, you can:

- Change the displayed statistics based on a time period by selecting different options in the **Display summary statistics for** drop-down list. The range of options vary depending on the appliance’s uptime.
- Reset the displayed statistics to 0 by clicking **Reset Statistics**.
- View audit data for any system event or attack category by clicking the magnifying glass .
- View a snapshot of all attacks listed by service by clicking **Attacks by Service**. See “About the Attacks by Service window” on page 446 for more information.
- View and save attack audit data by clicking **Most Recent IPS Attacks**.
- View an individual audit record by double-clicking that audit event’s row. See “About the Audit Record window” on page 447 for more information.

Use this area of the dashboard to monitor the following:

- **System events by severity** — Lists system audit events according to severity.
- **Attacks by severity** — Lists audit attack events according to severity.
- **Attacks by service** — Lists audit attack events according to service.
- **Most recent IPS attacks** — Displays the audit events for recent attacks.
Chapter 15: The Dashboard
Viewing IPS attack and system event summaries

**Note:** Use the Admin Console’s IPS Attack Responses and System Event Responses to determine how the appliance reacts to different audit events. For more information, see the “IPS Attack and System Event Responses” chapter.

**About the Attacks by Service window**

Use this window to view audit of suspect traffic.

![Figure 199: Attacks by Service window](image)

Information provided includes:

- **Name** — Name of the service being attacked
- **Count** — Number of attack instances

On this window, you can:

- Click **Refresh** to update the information.
- Select a service and click **Show Audit** to see the audit output. You can also view the audit by clicking the magnifying glass on the main window.
- Click **Close** to return to the main window.
About the Audit Record window

When you double-click an audit event in the table, the detailed audit information for that attack appears in a pop-up window.

The displayed fields vary, depending on the audit type. In general, the data in an audit message is a tag name followed by a colon and the tag’s value. The following table provides examples and descriptions of fields that may appear in an audit record. Most administrators begin troubleshooting by noting the reason an event was audited and then examining the source and destination information.

More information on audit fields is available using `acat -c |more` at a command line interface and in the Sidewinder Export Format application note at [www.securecomputing.com/goto/appnotes](http://www.securecomputing.com/goto/appnotes).

**Table 35: Audit filter fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>facility</td>
<td>Specify an event facility code (such as f_login, f_proxy, etc.).</td>
</tr>
<tr>
<td>type</td>
<td>Specify an event type code (for example, type t_nettraffic).</td>
</tr>
<tr>
<td>category</td>
<td>Specify an event category code (for example, c_policy_violation).</td>
</tr>
<tr>
<td>eventid</td>
<td>Specify an event identifier code (for example, r_licexceeded).</td>
</tr>
<tr>
<td>hostname</td>
<td>Specify a host name.</td>
</tr>
<tr>
<td>username</td>
<td>Specify a user name.</td>
</tr>
<tr>
<td>src_ip</td>
<td>Specify the source IP address. Separate optional mask bits with a slash (/).</td>
</tr>
<tr>
<td>dst_ip</td>
<td>Specify the destination IP address. Separate optional mask bits with a slash (/).</td>
</tr>
</tbody>
</table>

More...
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>src_port</td>
<td>Specify the TCP or UDP source port.</td>
</tr>
<tr>
<td>dst_port</td>
<td>Specify the TCP or UDP destination port.</td>
</tr>
<tr>
<td>src_burb</td>
<td>Specify the source burb name or index number.</td>
</tr>
<tr>
<td>dst_burb</td>
<td>Specify the destination burb name or index number.</td>
</tr>
<tr>
<td>service</td>
<td>Specify the service name. (To filter on an agent, use the facility field.)</td>
</tr>
<tr>
<td>vpn_l_gw</td>
<td>Specify a VPN local gateway using the standard dotted decimal IP version 4 notation with optional mask bits separated by a slash (/).</td>
</tr>
<tr>
<td>vpn_r_gw</td>
<td>Specify a VPN remote gateway using the dotted decimal IP version 4 notation with optional mask bits separated by a slash (/).</td>
</tr>
</tbody>
</table>
In this chapter...

Configuring burbs ................................................................. 452
Configuring interfaces ......................................................... 456
Configuring Quality of Service ............................................. 462
A burb is a type enforced network area used to isolate network interfaces from each other.

- An internal burb and an external burb are defined in your Sidewinder appliance during the installation process.
- You create, modify, and delete burbs in the Burb Configuration window.
- You select these burbs as Source and Destination burbs when creating a rule in the Rules window.

To create, modify, and delete burbs, select **Network > Burb Configuration**. The following window appears:

![Burb Configuration window](image)

The upper pane lists the existing burbs and burb groups. When you select a burb or burb group in the table, the properties appear in the lower pane.

- You can configure a maximum of 63 burbs on a Sidewinder appliance.
- The **Internet** burb cannot be deleted. The Internet burb has pre-defined attributes, both configurable and non-configurable, to supply a secured connection to the internet.
- At least two burbs (in addition to the **Firewall** burb) must exist at all times.
- A virtual burb is a burb that does not contain a network interface card (NIC). Virtual burbs do not support ICMP.
Figure 202: Burb Configuration toolbar

Use the toolbar to perform these actions:

Table 36: Burb Configuration toolbar

<table>
<thead>
<tr>
<th>Icon</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Burb</td>
<td>Create a new Burb by clicking <strong>New Burb</strong> and entering Burb information in the pop-up window.</td>
</tr>
<tr>
<td></td>
<td>See “About the New/Modify Burb window” on page 454 for details.</td>
</tr>
<tr>
<td>New Burb Group</td>
<td>Create a new Burb group by clicking <strong>New Burb Group</strong> and entering information in the pop-up window. When configured, the group appears in the Groups list in the lower pane.</td>
</tr>
<tr>
<td></td>
<td>See “About the New/Modify Burb Group window” on page 455 for details.</td>
</tr>
<tr>
<td>Modify</td>
<td>Modify a Burb or Burb group by selecting it in the upper pane, and then clicking <strong>Modify</strong>. Modify the settings in the pop-up window. (Read-only administrators can click <strong>View</strong> to view a Burb or Burb group.)</td>
</tr>
<tr>
<td></td>
<td>You can also select a Burb or Burb group and modify the settings in the lower pane.</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete a Burb or Burb group by selecting the Burb in the upper pane and clicking <strong>Delete</strong>.</td>
</tr>
<tr>
<td></td>
<td>You cannot delete a Burb or Burb group that is currently referenced elsewhere on the system (for example, a rule or Interface configuration). To determine whether a Burb or Burb group is currently being referenced, select it and click <strong>Usage</strong>.</td>
</tr>
<tr>
<td>Usage</td>
<td>View all areas where a Burb or Burb group is currently being used by selecting the Burb in the upper pane and clicking <strong>Usage</strong>. The Burb Usage window appears listing every area in which the Burb is currently used.</td>
</tr>
<tr>
<td>Internet Burb</td>
<td>Designate the internet Burb by selecting the appropriate Burb from the <strong>Internet Burb</strong> drop-down list.</td>
</tr>
</tbody>
</table>
**About the New/Modify Burb window**

Use this window to create or modify a burb.

**Figure 203: New/Modify Burb window**

To create or modify a burb:

1. Type a name in the Burb name field. This is the name you will see in the Burb drop-down list in the Rules window.
   - Do not use “Firewall” or “firewall” as a burb name, as this name is already used elsewhere in the Sidewinder appliance.
   - Case matters in burb names. For example, if you create a burb named Joe and another burb named joe, they are separate burbs.
   - If you are modifying a burb, you cannot change the name.

2. [Optional] Type a more detailed description of the burb.

3. Select connection options for the burb:
   - **Honor ICMP redirect** — ICMP messages are used to optimize the routes for getting IP traffic to the proper destination. On a trusted network, honoring ICMP redirects can improve the throughput of the system. On an untrusted network, ICMP redirects can be used by hackers to examine, reroute, or steal network traffic. Enabling this parameter allows the appliance to honor ICMP redirects.
   - **Respond to ICMP echo and timestamp** — ICMP echo and timestamp messages (also known as ping messages) are used to test addresses on a network. The messages are a handy diagnostic tool, but can also be used by hackers to probe for weaknesses. Enabling this parameter allows the appliance to respond to these messages.
   - **Hide ICMPv6 parameter problems** — [Not currently available]
   - **Hide ICMPv6 policy unreachables** — [Not currently available]
• **Hide port unreachables** — If this parameter is enabled, the appliance will give no response if a node on the network attempts to connect to a port on which the appliance is not listening. This increases security by not divulging configuration information to potential hackers.

  **Note:** Do not select this option for a heartbeat burb in an HA cluster.

4  [Optional] In the Groups list, select a burb group or burb groups for this burb to belong to.

5  Click **OK** and save your changes.

**About the New/Modify Burb Group window**

Use this window to create or modify a burb group.

Burb groups are a way to apply a rule to multiple burbs. If you select a burb group in the Source and Destination areas in a rule, that rule will apply to each burb in the burb group.

**Figure 204:** New/Modify Burb Group window

To create or modify a burb group:

1  Type a name in the **Group name** field. This is the name you will see in the Burb drop-down list in the Rules window. (If you are modifying the burb group, you cannot change the name.)

2  [Optional] Type a more detailed description of the burb group.

3  In the Burbs list, select which burbs belong to this group.

4  Click **OK** and save your changes.
The internal and external network interfaces of the Sidewinder appliance are defined during the installation process. You can configure up to 63 interfaces, using a combination of physical and VLAN interfaces. You can configure the media type, the IP address, the subnet mask associated with an interface, and the burb assigned to an interface. You can also enable VLANs, DHCP, support for jumbo frames, and TCP checksum offloading.

To modify your interface configuration, select **Network > Interfaces**. The following window appears.

![Interfaces: Interfaces tab](image-url)
About the Interfaces: Interfaces tab

The Interfaces tab in the upper pane displays the configuration settings for each interface on the Sidewinder appliance in a table format. The Configuration tab in the lower pane displays the configuration information for the interface that is selected in the Interfaces table.

You can perform the following actions in the Interfaces tab:

- To see status information for each of the physical and VLAN network interfaces on this appliance, click **Interface Status**. You can also view this information at a command line interface by typing `netstat -in`.

  **Tip:** See the man pages for more netstat commands.

- To delete an interface, select the interface and click **Delete**. You can only delete interfaces that are disabled. Physical interfaces must have the NIC removed as well.

- To modify an interface, select that interface in the table. The configuration information appears in the lower pane.

To access the configuration information in a pop-up window, select the interface and click **Modify**. (Read-only administrators can click **View** to view an interface.)

- To switch the configuration settings between two interfaces, select the two interfaces whose properties you want to swap (press and hold the **Ctrl** key to select multiple interfaces), and then click **Swap Parameters**. A warning message will state that the system may not function properly until it is rebooted. To swap the parameters, click **Yes** and be sure to reboot your system. To cancel, click **No**.

  If you swap interfaces, the MTU settings will not be swapped. Therefore, if you swap an interface with modified MTU settings, you will need to reconfigure those settings after swapping the interfaces.

  **Caution:** Swapping interface parameters after you have initially configured your appliance could have unexpected results. This process should only be used immediately after installation, or when an interface has been added or replaced.
The Configuration tab in the lower pane displays the interface name and MAC address that you are modifying. The following interface settings can be modified:

- **Enable** — To enable an interface, select On. To disable an interface, select Off.

  **Note:** You must select a burb in the Burb drop-down list before you can enable an interface.

- **Interface Type** — Select one of the following options:
  - **Physical Interface** — Select this option to configure a standard physical interface.
  - **VLAN-Enabled Interface** — Select this option to configure VLANs (Virtual Local Area Network) for this interface. A VLAN is a virtual interface that allows administrators to segment a LAN into different broadcast domains regardless of the physical location.

  **Note:** VLANs are only supported on bce, bge, em, and fxp NICs.

When you select the **VLAN-Enabled Interface** option, the Configuration tab displays a table listing all of the VLANs that are currently configured for this interface. To configure VLANs for an interface, click **New** under the VLANs table.

  **Important:** You must use a network switch or router that can decipher VLAN traffic to use VLANs. Also, you cannot create VLANs on an interface that has DHCP enabled.

- **IP Address** — Select one of the following options:
  - **Obtain an IP address automatically** — This option allows you to use the Dynamic Host Configuration Protocol (DHCP) to centrally manage IP addresses within your network. When you select this option, the IP Address and Network Mask fields are filled in with a value of DHCP, indicating that DHCP will be used to manage IP addresses.

  **Important:** You cannot configure HA or One-To-Many on a Sidewinder appliance that has DHCP configured.

  - **Use the following IP address** — This option allows you to specify the IP address, network mask, and burb for a physical interface.
    - **IP Address** — Type the IP address of the physical interface.
    - **Network Mask** — To modify the Network Mask, enter the new network mask in this field. The value specified is used to identify the significant portion of the IP address.
    - **Burb** — To modify the burb, select the appropriate burb for this interface from the drop-down list.

- **Media Type** — To modify the media type, select the appropriate type from the drop-down list.
• **MTU** — Use this field to specify the size of the Maximum Transfer Unit (MTU) for outgoing packets. Select one of the following:
  – **Standard (1500)** — Select this option to use the standard MTU.
  – **Jumbo (9000)** — Select this option to allow jumbo frames. This option is only available on NICs that support jumbo frames.
  – **Custom (576–9216)** — Select this option if you need to specify a custom MTU. If the NIC does not support jumbo frames, the range for this option will be 576–1500.

  **Note:** The `receive_jumbo_frames` option (in the Hardware Capabilities area), allows the interface to receive larger MTUs. This option is automatically enabled when you specify a size that is larger than 1500 (standard). You must also ensure that the destination is able to receive the MTU size when using non-standard sizes.

  **Important:** If you swap interfaces, the MTU settings will not be swapped. Therefore, if you swap an interface with modified MTU settings, you will need to reconfigure those settings after swapping the interfaces.

• **Quality of Service Profile** — To enable Quality of Service (QoS), select a QoS profile from the drop-down list. See "Configuring Quality of Service" on page 462 for more information on QoS.

  **Note:** In High Availability clusters, Quality of Service must be configured only on the primary cluster member.

• **Hardware Capabilities** — This option appears only if the interface you are modifying has hardware capabilities that can be configured. The following options may be available for selection:
  – **rxcsum**: Enable hardware checksum verification for incoming IPv4 packets.
  – **txcsum**: Enable hardware checksum generation for outgoing IPv4 packets.
  – **receive_jumbo_frames**: This option is only available on NICs that support jumbo frames.

When you are finished modifying the interface, save your changes.
### Configuring VLANs

Use the VLAN-Enabled Interface Configuration: Modify Interface Configuration window to create and modify VLANs for an interface. You can assign up to 64 VLANs/NICs on the Sidewinder appliance. For example, if your appliance has three NICs, you could configure up to 61 VLANs. Other information about how VLANs function on the Sidewinder appliance include:

- VLANs are supported in a High Availability (HA) configuration. For best results, configure VLANs before configuring HA.
- You must use a network switch or router that can decipher VLAN traffic to use VLANs.
- You cannot create VLANs on an interface that has DHCP enabled.
- To filter traffic for a VLAN, use the following syntax:
  ```
  tcpdump -pn interface_name vlan vlanID
  ```

#### Figure 206: VLAN-Enabled Interface Configuration: Modify Interface Configuration window

To configure a VLAN:

1. In the **Enable** field, select one of the following options:
   - **On** — Select this option to enable this VLAN.
   - **Off** — Select this option to disable this VLAN.
2. In the **VLAN ID** field, specify a numeric ID for this VLAN. Valid values are 2–4094.
3. In the **IP Address** field, enter an IP address for the appliance on this VLAN.
4. In the **Network Mask** field, enter a network mask for the VLAN. The value specified is used to identify the significant portion of the IP address.
5. In the **Burb** drop-down list, select the burb for this VLAN.
6. Click **OK** to add the VLAN and return to the Interfaces: Interfaces tab.
7. Save your changes.
About the Interfaces: Aliases tab

The Interfaces: Aliases tab contains a table that displays any alias IP addresses defined for the selected network interface. Alias IP addresses are used in Multiple Address Translation (MAT).

Adding alias IP addresses to a network interface can be used for purposes such as:

- Specific logical networks connected to one interface can be consistently mapped to specific IP aliases on another interface when using address hiding.
- The NIC can accept connection requests for any defined alias.
- The NIC can communicate with more than one logical network without the need for a router.
- The NIC can have more than one address on the same network and have DNS resolve different domains to each host address.

You can perform the following actions:

- To delete an alias IP address, select the item and click **Delete**.
- To add an alias IP address, click **New** and enter a network address, alias address, and network mask in the pop-up window.
- To modify an alias IP address, select the item and click **Modify**, then make the appropriate changes.
Quality of Service (QoS) guarantees a certain level of performance for a data flow by using different priorities and queuing mechanisms to allocate available bandwidth. QoS is beneficial for networks with limited bandwidth that must pass latency-sensitive or bandwidth-intensive traffic.

From the Quality of Service window, you can create QoS profiles that can be applied to the network interfaces of the Sidewinder appliance. Each QoS profile contains one or more queues that allow you to prioritize network performance based on network traffic type. All queues are assigned a priority value, allocated a percentage of available bandwidth, and can be allowed to borrow bandwidth from other queues. When a queue is full, any additional packets matching that queue are dropped. Queues are applied to network traffic based on the services that are selected.

When QoS policy is applied to a network interface, only outgoing traffic on that interface is controlled by QoS — packets arriving on that interface are not affected. If you require traffic for a particular service to be controlled in both directions, that service must be present in the QoS policy of both interfaces where traffic for that service leaves the appliance. Consider the following QoS configurations and their effect on a connection between an internal client and external web server:

- The external interface’s QoS profile includes HTTP — Traffic sent from the internal client to the external web server is affected by QoS.
- The internal interface’s QoS profile includes HTTP — Traffic sent from the web server to the internal client is affected by QoS.
- Both internal and external interface QoS profiles include HTTP — All traffic between the client and web server is affected by QoS.

QoS is applied to network traffic at the IP and transport layers based on the service(s) selected in each queue. Protocols that use dynamic ports negotiated at the application layer like FTP or VoIP will not match QoS queues using those services, since QoS does not examine the application layer when processing packets.

Consider the case in which a QoS queue has been created with the FTP proxy service selected. QoS is applied to the control connection (tcp port 21) but not the data connection (high random tcp port or tcp port 20). Since the control connection is made on the port defined in the service, QoS policy is applied to it. However, QoS is not applied to the data connection because it is made on a port negotiated at the application layer between the client and server.

**Note:** To apply QoS to protocols that employ dynamic ports, create a service that includes the range of dynamic ports, and select this service on the QoS queue.
To apply QoS to a network interface:

1. Create a QoS profile.
2. Add QoS queues to the profile.
3. Apply the QoS profile to a network interface under **Network > Interfaces**.

**Note:** QoS cannot be configured on VLANs.

Select **Network > Quality of Service**.

The Quality of Service window consists of two panes:

- Profiles (upper pane) — Use this pane to configure QoS profiles.
- Queues (lower pane) — Use this pane to configure QoS queues for the profile selected in the Profiles pane.

Also see “Example QoS scenarios” on page 469.
Configuring QoS Profiles

QoS profiles contain QoS policy that can be assigned to a particular network interface. They behave as containers for QoS queues that make up the QoS policy.

Each profile contains a default queue that cannot be deleted or renamed. The default queue processes all packets that do not match any queues you have explicitly defined.

Use the toolbar to perform the actions described in this section.

**Figure 209:** Quality of Service profile toolbar

<table>
<thead>
<tr>
<th>Button</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td>Click <strong>New</strong> to create a new profile. The profile name must be seven characters or less.</td>
</tr>
<tr>
<td>Modify</td>
<td>To modify a profile, select it in the Profile pane and configure its attributes in the Queues pane (alternately, select the profile, then click <strong>Modify</strong>). See “Configuring QoS queues” below for more information.</td>
</tr>
<tr>
<td>Delete</td>
<td>Select the profile, then click <strong>Delete</strong>.</td>
</tr>
<tr>
<td>Duplicate</td>
<td>Click <strong>Duplicate</strong> to create a copy of an existing profile. Type a name and [Optional] description in the Modify Profile window that appears.</td>
</tr>
<tr>
<td>Rename</td>
<td>To change the name of an existing profile, click <strong>Rename</strong>. Enter the new name, then click <strong>OK</strong>.</td>
</tr>
<tr>
<td>Usage</td>
<td>To show which network interfaces are using a profile, click <strong>Usage</strong>.</td>
</tr>
<tr>
<td>Search</td>
<td>To find a profile, enter all or part of the name. When the system finds a match, it appears highlighted in the pane. If the system does not find a match, the pane appears blank. Use the <strong>Backspace</strong> key to find partial matches or delete the search term to return to the main window.</td>
</tr>
<tr>
<td>QoS Status</td>
<td>Click <strong>QoS Status</strong> to view QoS filter rules, and queue statistics. Statistics are reset when any QoS policy change is made. Queue names are presented in the format <code>queuename_profilename</code>.</td>
</tr>
</tbody>
</table>
Configuring QoS Queues

Use QoS queues to allocate available bandwidth based on traffic type. Queues make up the policy in QoS profiles — each queue in a profile is assigned a priority value and dedicated a percentage of available bandwidth.

![QoS Queues pane](image)

To create QoS policy, select the profile you want to modify in the profile pane, then use the Queue pane to make policy changes.

To prioritize bandwidth usage within a profile, configure the following attributes of each queue in the profile:

- **Priority** — A value between 0–7 (lowest–highest) that determines the order the queue is processed relative to the other queues in the profile. Higher priority queues are processed first, resulting in lower latency for them.

- **Allocated Bandwidth** — The percentage of available bandwidth to be dedicated to the queue. The available bandwidth for a QoS profile is determined by the link speed of the network interface it is associated with.

- **Services** — The types of traffic the queue applies to.

- **Can Borrow** — If enabled, allows the queue to borrow bandwidth from the other queues in the profile when it exhausts its allocated bandwidth.

Each profile contains a default queue that cannot be deleted or renamed. The default queue processes all packets that do not match any queues you have explicitly defined. Edit the **Priority**, **Bandwidth**, and **Can Borrow** attributes of the default queue to control how QoS allocates bandwidth for services that are not included in custom queues.
Figure 211: Quality of Service queue toolbar

New Delete Search

<table>
<thead>
<tr>
<th>Button</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td>Click New to create a new queue. See “About the New/Modify Queue window” on page 467.</td>
</tr>
<tr>
<td>Modify</td>
<td>Double-click the queue you want to change (alternately, select the queue, then click Modify). See “About the New/Modify Queue window” on page 467.</td>
</tr>
<tr>
<td>Delete</td>
<td>Select the queue, then click Delete.</td>
</tr>
<tr>
<td>Rename</td>
<td>To change the name of an existing queue, click Rename. Enter the new name, then click OK.</td>
</tr>
<tr>
<td>Find</td>
<td>To find a queue, enter all or part of the name. When the system finds a match, it appears highlighted in the pane. If the system does not find a match, the pane appears blank. Use the Backspace key to find partial matches or delete the search term to return to the main window.</td>
</tr>
</tbody>
</table>
About the New/Modify Queue window

Use this window to create new queues or modify existing queues.

Figure 212: New/Modify Queue window
To create or modify a QoS queue:

1. In the **Name** field, type a name for the new queue (Use **Rename** on the queue toolbar to rename an existing queue).

   **Note:** The queue name must be seven characters or less.

2. [Optional] In the **Description** field, type a more detailed description of the queue.

3. In the **Priority** field, type the priority value (0–7) for this queue.

4. In the **Bandwidth** field, type the percentage of bandwidth to be allocated for this queue. This value is limited to the amount of bandwidth not already allocated to other queues. Bandwidth cannot be set to 0.

5. To allow this queue to borrow bandwidth from the other queues, select the **Can borrow** box.

   **Note:** The **Can borrow** option is selected by default. Unless you want to allow this queue to appropriate bandwidth from queues with equal or lower priority, disable this option.

6. In the **Available Services** pane, select the service(s) that you want to associate with this queue. If you want to select a service that is not listed, you can create a new one by clicking **New**.

   **Note:** QoS queue policy is applied to packets that match the protocol and port of the selected service(s).

7. Click **OK** to finish configuring the queue.

Repeat this procedure for each additional queue you wish to add for this profile.
Example QoS scenarios

The interaction between multiple QoS queues with differing priorities, allocated bandwidth, and borrowing can be complex. Use the following example scenarios to familiarize yourself with QoS in practice.

In the examples below, two queues are configured — ssh and http. No other traffic is flowing, although other queues may be defined.

Case 1

SSH is allocated 10% of bandwidth at priority 7 with no borrowing allowed, and HTTP is allocated 10% of bandwidth at priority 7 with no borrowing allowed.

At congestion levels, exactly 10% of available bandwidth is allocated to each of the queues.

Case 2

SSH is allocated 10% of bandwidth at priority 0 with no borrowing allowed, and HTTP is allocated 10% of bandwidth at priority 7 with no borrowing allowed.

At congestion levels, exactly 10% of available bandwidth is allocated to each of the queues; however, HTTP traffic is processed before SSH traffic and hence experiences lower latency.

Case 3

SSH is allocated 30% of bandwidth at priority 7 with no borrowing allowed, and HTTP is allocated 10% of bandwidth at priority 7 with no borrowing allowed.

At congestion levels, exactly 30% of available bandwidth is allotted to the SSH queue with 10% going to the HTTP queue.

Case 4

SSH is allocated 30% of bandwidth at priority 7 with borrowing allowed, and HTTP is allocated 10% of bandwidth at priority 7 with borrowing allowed.

At congestion levels, a proportionally larger percentage of available bandwidth is allotted to the SSH queue, with the remaining traffic going to the HTTP queue. (Since SSH is allocated a larger portion of the bandwidth than HTTP, it gets more weight at the time of borrowing since they are of the same priority.)

Case 5

SSH is allocated 10% of bandwidth at priority 7 with borrowing allowed, and HTTP is allocated 10% of bandwidth at priority 7 with borrowing allowed.

At congestion levels, the two queues share the borrowed bandwidth equally (40% each).
Case 6

SSH is allocated 10% of bandwidth at priority 0 with borrowing allowed, and HTTP is allocated 10% of bandwidth at priority 7 with borrowing allowed.

At congestion levels, the HTTP queue commandeers all of the bandwidth since it is the highest priority queue and it is allowed to borrow.

Case 7

SSH is allocated 30% of bandwidth at priority 7 with no borrowing allowed, and HTTP is allocated 10% of bandwidth at priority 7 with borrowing allowed.

At congestion levels, the SSH queue uses 30% of available bandwidth and the HTTP queue commandeers all of the remaining bandwidth.

Summary

• If multiple queues have the same priority and borrowing is allowed, each queue borrows a percentage of available bandwidth. The amount of bandwidth each queue can borrow is determined by its allocated bandwidth in proportion to the allocated bandwidth of the other queues.

• If a queue with higher priority is allowed to borrow, it will starve lower priority queues, but not vice versa.

• If borrowing is not allowed, queues share available bandwidth per their allocated bandwidth value. Higher priority queues are serviced first, resulting in reduced latency for them at the expense of the lower priority queues.
CHAPTER 17  E-mail

In this chapter...

Overview of mail on Sidewinder ..............................................................472
Setting up and reconfiguring mail ............................................................474
Understanding sendmail on Sidewinder ..............................................476
Editing sendmail files on Sidewinder ......................................................480
Configuring advanced sendmail features .............................................484
Managing mail queues .........................................................................490
Receiving mail sent by Sidewinder .........................................................494
When you run mail on a network protected by the Sidewinder appliance, you have two options for getting messages through the appliance: use the SMTP proxy or use the Sendmail® server hosted on the appliance. If you use the Sidewinder-hosted Sendmail server, you can also use Sidewinder’s virus and spam filtering mail services.

The two mail configuration options are described in the following sections.

**Important**: A newly installed Sidewinder appliance is not configured to pass mail between burbs. If you want mail to pass through the appliance, you must run Maintenance > Reconfigure Mail and then create the appropriate rules. See “Setting up and reconfiguring mail” on page 474 for more information. Also make sure that DNS is correctly configured before setting up your mail services.

**About transparent mail (SMTP proxy)**

This configuration option allows you to use transparent SMTP services (without sendmail processes running directly on the appliance). Transparent SMTP service indicates that all inbound and outbound mail passes by proxy through the appliance, just as other proxy traffic does.

When using transparent mail services, mail filtering is limited to these features:

- Server reply length checks
- Mail command filtering
- Destination address filtering

The advantage of using Sidewinder’s transparent mail services is ease of use. It can be set up in a few steps and requires minimal maintenance directly on the appliance. However, this option is less secure than using hosted sendmail services and offers fewer Sidewinder-based filtering options.

Set up transparent mail by doing the following:

1. Make a configuration backup (Maintenance > Configuration Backup).
2. Select the transparent mail option. See “Setting up and reconfiguring mail” on page 474.
3. Create a rule using a mail proxy service and a Mail (SMTP Proxy) Application Defense.
   - To configure a rule, see “Creating, modifying, and duplicating rules” on page 95.
   - To configure a mail proxy service, see “Creating and modifying services” on page 147.
   - To configure a Mail (SMTP Proxy) application defense, see “Creating Mail (SMTP proxy) Defenses” on page 196.
About Sidewinder-hosted mail (sendmail)

This configuration option allows you to have two sendmail servers running directly on the Sidewinder appliance, each supported on its own burb: the external burb and one non-Internet burb that you choose. The Sidewinder sendmail servers will route mail through the appliance only for these two burbs.

This configuration protects your internal mailhost from malicious attacks, and offers a variety of additional mail-handling options. When using secure split mail services, the Sidewinder external sendmail server is the mail host to which all external SMTP hosts will connect. The Sidewinder internal sendmail server will connect with internal mail hosts in its same burb.

Your internal mail host must run mail software that can accept incoming messages from, and send outgoing messages to, the Sidewinder appliance. This system might be running sendmail or some other mail package such as Microsoft Exchange or cc:Mail with a Simple Mail Transport Protocol (SMTP) gateway.

When using hosted sendmail, you also have the option of purchasing anti-spam/anti-fraud and anti-virus/anti-spyware services that run directly on the Sidewinder appliance.

For instructions on setting up the hosted mail option, see “Setting up and reconfiguring mail” on page 474. From instructions on configuring anti-spam and anti-virus services, see Chapter 8, “Content Inspection”, on page 233. Using hosted sendmail services is a very secure option, but does require more mail administration on the Sidewinder appliance. Read the rest of this chapter for important management instructions.
Setting up and reconfiguring mail

The Reconfigure Mail window is used to configure both Sidewinder mail options. In the Admin Console, select Maintenance > Reconfigure Mail. (You can also access this window within the sendmail server’s Properties window.) The Reconfigure Mail window appears.

![Reconfigure Mail window](image)

Use this window to set your initial mail configuration or reconfigure your existing mail configuration. However, before you make any changes you should be aware of the following:

- If you manually edited any sendmail configuration files, changing your mail configuration in the Reconfigure Mail window will overwrite the changes you made.
- If you are using anti-spam services and you change to the transparent mail configuration, the anti-spam services will be disabled. Any mail-related anti-virus scanning will also be disabled.

To establish or change your mail configuration:

1. Verify that DNS is configured correctly.
2. Make a configuration backup before you change your mail configuration: Select Maintenance > Configuration Backup.
3. On the Reconfigure Mail window, expand the New SMTP Mode drop-down list and select the mail configuration mode you want to configure. The current mode is listed in the Current SMTP Mode field. The following options are available:
   - **Transparent** — Use this option when you want to pass mail by proxy through the Sidewinder appliance. If you select this option, only the files necessary to send administrative messages (including Sidewinder-generated alerts, messages, and logs) will be configured.
• **Secure Split SMTP Servers (Sidewinder-hosted)** — Use this option to use the Sidewinder-hosted sendmail server(s). This configuration allows you to take advantage of additional sendmail features, including header stripping, spam and fraud control, mail routing, aliases, and masquerading.

4 In the **Internal SMTP Burb** field, select the burb in which your site’s internal SMTP server resides.

5 In the **Internal SMTP Mail Server** field, type the fully qualified name of your site’s internal SMTP server. Do not use simple host names or IP addresses.

6 Click **Save** in the toolbar (or click **Apply** if you are accessing this window from the Services window) to reconfigure your mail mode. A confirmation window appears when the reconfiguration process is complete.

7 [Conditional] If you accessed Reconfigure Mail from the Services window, click **Close** to return to the sendmail server Properties window.

8 Select **Policy > Rules** and create or modify the necessary rules:
   • If you selected Transparent:
     • Create two rules: one for inbound mail and one for outbound mail.
     • Use the smtp (Mail Proxy) service.
     • Use two Mail (SMTP proxy) application defenses: one for inbound traffic and one for outbound traffic, each with direction-appropriate settings.
   • If you selected Secure Split SMTP Servers:
     • Create two rules: one for inbound mail and one for outbound mail.
     • Use the sendmail (Sendmail Server) service.
     • The rules’ destination burb must be `<Any>`. The endpoint must also be `<Any>`.
     • Use two Mail (Sendmail) application defenses: one for inbound traffic and one for outbound traffic, each with direction-appropriate settings.

See Chapter 5, “Rules”, on page 81, for more information on how to manage rules.

**Important:** If you are changing your mail configuration, you will need to update or replace your existing mail rules to reflect the new configuration.

9 Save your changes.

The Sidewinder appliance now has a new mail configuration.

• If you selected Transparent, mail management is primarily handled off-box and does not require changes to any Sidewinder mail files.

• If you selected Secure Split SMTP Servers and are an experienced mail administrator, you may want to edit the configuration files. See “Editing sendmail files on Sidewinder” on page 480 and “Configuring advanced sendmail features” on page 484 for more information.
Understanding sendmail on Sidewinder

Hosting sendmail on the Sidewinder appliance requires knowledge of both the sendmail application and how Sidewinder interacts with it. Read the following sections to learn about domain and file names, Interoperability considerations, and filtering services.

Using sendmail on Sidewinder

When you use the Reconfigure Mail window (Maintenance > Reconfigure Mail) to select secure split services, you specify a mail host on your internal network and the burb where that server is located. This is the internal mail host that will send mail to, and receive mail from, the Sidewinder-hosted mail server. The necessary configuration files and everything you need to run the Sidewinder-hosted mail server are automatically set up for you, such as:

- The three mail domains: \textit{mtac}, \textit{mtaX}, and \textit{mtaY} (where \(X\) = the number of the external burb, and \(Y\) = the number of an internal burb), are in place. Sendmail is already configured to route mail among the three sendmail servers.

- Mail addressed to users on your internal network will be forwarded to the mail host you specified in the Reconfigure Mail window.

- Messages that are sent to the person administering a mail system are generally addressed to “postmaster.” During the Quick Start Wizard (initial configuration), you set up an administrator’s account. Postmaster messages are automatically routed to that administrator’s Sidewinder-hosted mail account. (Secure Computing recommends that all administrators redirect their local mail to a non-Sidewinder-hosted e-mail account.)

\textbf{Note:} You will need to configure your internal mail server to forward non-local mail to the Sidewinder appliance. This procedure differs depending on the type of mail program your network runs. Refer to your mail software’s documentation for details.

When you configure secure split SMTP services, there are three separate sendmail servers that each have a different purpose:

- \textbf{Local}

  The local server handles mail that is sent directly from the Sidewinder appliance. For example, if an administrator sends a mail message from the appliance, it is sent through the local server. This sendmail process runs in the \textit{mtac} domain and forwards all mail to the Sidewinder’s internal network.
• **Internal**

  The internal server runs in the *mta#* domain, where # is the burb index of an internal burb that you specify when running Reconfigure Mail.

  This internal sendmail server *receives* mail from one of three sources:
  
  – a host on the internal network
  – a sendmail process transferring mail from the local sendmail server
  – a sendmail process transferring mail from the external sendmail server

  This internal sendmail server *delivers* mail to one of three places:
  
  – If the message is for a user local to the Sidewinder appliance, such as an administrator with a mailbox on the Sidewinder, it delivers the message to the user’s mailbox using the `mail.local` program.
  – If the message is for a user on the internal network, it connects to the mail host on the internal network and delivers the mail there.
  – If the message is not for either of the above, it assumes the message is for an external user and transfers the message to the external burb for that user.

• **external**

  The external server runs in the *mta#* domain, where # is the burb index of the Internet burb. This sendmail server *receives* mail from one of two sources:
  
  – a host on the external network
  – a sendmail process transferring mail from the internal sendmail server

  The external server *delivers* mail to one of two places:
  
  – If the message is for an external user, it connects to an external host and delivers the mail there.
  – If the message is for a user local to the Sidewinder (such as an administrator) or for a user on the internal network, it transfers the mail to the internal burb for delivery to that user.

When using Sidewinder-hosted SMTP services, all mail for a user local to the Sidewinder appliance goes to the internal *mta* domain for delivery. Local delivery does not take place in the external *mta* domain or the *mtac* domain. Running sendmail on the appliance works as it does in any other UNIX environment, with the following exceptions:

• The Sidewinder appliance runs three separate sendmail servers (as described in the previous section).

• Type Enforcement restricts sendmail so that its security flaws cannot be exploited. For example, Sidewinder administrators cannot execute shell scripts or other executables through sendmail, as they could do on a standard UNIX system.
• Aliases allow users to send their mail to another mailbox that may be at a different location. For example, Sidewinder administrators might choose to redirect their mail to a mailbox located on the internal network so they receive all of their mail in one place. Administrators can use the /etc/mail/aliases file, but this file cannot contain commands to run other programs, such as program mailers (for example, procmail). For more information on aliasing mail, see “Setting up e-mail aliases for administrator accounts” on page 494.

• If a server is too busy to send a message, or if the machine it is sending mail to is not responding, the messages are sent to a mail queue. The Sidewinder appliance has a separate queue for each sendmail server: /var/spool/mqueue.#, /var/spool/mqueue.#, and /var/spool/mqueue.c (# = the burb number).

**Important:** If mail cannot be delivered on the first attempt, it is placed in a queue. By default, the system checks the queues every 30 minutes and attempts redelivery.

You can check if there are messages in the mail queues by following the steps described in “Managing mail queues” on page 490.

Mail is an extremely complex subject and can require a great deal of effort to configure. If you want additional information on managing mail, the best resource is the book *sendmail* by Bryan Costales (O’Reilly & Associates, Inc.).

## Mail filtering services on Sidewinder

An advantage to using hosted sendmail is the ability to do on-box mail filtering. To filter messages, you must create rules using the sendmail server and a Mail Application Defense with the filter options configured. The following mail filtering services are available:

**Note:** You must have Secure Split SMTP mail servers configured to use the mail filtering listed here.

### MIME/Virus/Spyware filtering

The MIME/Virus/Spyware application defense options allow you to:

• Allow, deny, or scan specific types of MIME elements and specific file extensions

• Configure how to handle infected files

• Specify file attachment size restrictions (per message, not per attachment)

• Determine whether mail messages will be scanned as a whole (entire message is allowed or denied) or in segments (attachments may be dropped if they do not meet filtering criteria, but the acceptable portions of the mail message will still reach the recipient)

• Reject all mail if scanning services become unavailable
The virus scanner must be configured at **Policy > Application Defenses > Virus Scanning**. Virus scanning can then be applied per-rule using the rule's application defense. See “Configuring virus scanning services” on page 251 and “Configuring the Mail (Sendmail): MIME/Virus/Spyware tab” on page 191 for more information.

**Important:** You must purchase and activate the anti-virus add-on module before the MIME/Virus/Spyware filter rules you create will scan mail messages for viruses. MIME type filtering does not require the Anti-Virus license.

**Spam/fraud filtering**

Spam and fraud filtering is a licensed service. The appliance must be running Sidewinder-hosted mail (Sendmail). Spam filtering is applied on a per-rule basis using the Mail (Sendmail) application defense’s Spam/Fraud option. You can configure whitelist options at **Policy > Application Defenses > Spam Filter**. You can also adjust spam filter behavior by editing `spamfilter.cfg`.

See “Configuring spam filtering services” on page 261 and “Configuring the Mail (Sendmail): Control tab” on page 184.

**Important:** You must purchase and activate the anti-spam add-on module before the spam/fraud filter rules you create will scan mail messages.

**TrustedSource**

TrustedSource is a reputation service that filters incoming mail connections and then provides precise information about an e-mail sender's reputation based on its IP address. The TrustedSource reputation service is a tool for reducing the amount of spam that reaches your organization’s inboxes.

You can enable TrustedSource at **Policy > Application Defenses > TrustedSource**. Select **Perform TrustedSource filtering on inbound mail**, then set the threshold to a value from 0 to 120.

See “Configuring TrustedSource for Sidewinder” on page 257 for more information.

**Key word search filtering**

The Keyword Search filter allows you to filter mail messages based on the presence of defined key words (character strings).

See “Configuring the Mail (Sendmail): Keyword Search tab” on page 187.

**Configure size limitations for mail messages**

The size filter performs a check on e-mail messages for the number of bytes the message contains, including the message header. Messages that equal or exceed the specified size you specify will be rejected.

See “Configuring the Mail (Sendmail): Size tab” on page 186.
Anti-relay controls

Anti-relay control uses access control to prevent your mailhost from being used by a hacker as a relay point for spam to other sites. This option is automatically enabled for all Mail defenses and cannot be disabled.

See “Configuring the Mail (Sendmail): Control tab” on page 184.

Editing sendmail files on Sidewinder

If sendmail is hosted on your Sidewinder appliance, then the sendmail configuration information is stored in sendmail.cf files. These files contain information such as which delivery agents to use and how to format message headers. You should change your configuration options only if you are directed to do so by Secure Computing, or if you are an experienced sendmail user and want to customize the files for your site.

Sendmail allows you to create configuration files using macros written for the m4 preprocessor. Sections 19.5 and 19.6 in the UNIX System Administration Handbook describe these macros. You can also refer to the book sendmail by Bryan Costales (O’Reilly & Associates, Inc.).

The appliance sets up two mailertables for you: one internal and one external.

- The external mailertable, /etc/mail/mailertable.mta# (# = the number of the external burb), processes the mail and directs it to the internal mailertable.
- The internal mailertable, /etc/mail/mailertable.mta# (# = the number of an internal burb), sorts the mail by host name, and sends the mail to the correct internal mail host.

Figure 214 shows an example of the route along which incoming mail messages travel.

**Figure 214: Sidewinder mailertables**

<table>
<thead>
<tr>
<th>Incoming e-mail</th>
<th>Message destination</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:charlie@example.com">charlie@example.com</a></td>
<td>corphub <a href="mailto:linus@corp.example.com">linus@corp.example.com</a></td>
</tr>
<tr>
<td><a href="mailto:lucy@sales.example.com">lucy@sales.example.com</a></td>
<td>examplehub <a href="mailto:sally@ads.example.com">sally@ads.example.com</a></td>
</tr>
<tr>
<td><a href="mailto:linus@corp.example.com">linus@corp.example.com</a></td>
<td><a href="mailto:charlie@example.com">charlie@example.com</a></td>
</tr>
<tr>
<td><a href="mailto:sally@ads.example.com">sally@ads.example.com</a></td>
<td>saleshub <a href="mailto:lucy@sales.example.com">lucy@sales.example.com</a></td>
</tr>
</tbody>
</table>

Sidewinder external mailertable (/etc/mail/mailertable.mta#)

Example.com burbmailer-burb:localhost .example.com burbmailer-burb:localhost

Sidewinder internal mailertable (/etc/mail/mailertable.mta#)

Example.com smtp:examplehub .example.com smtp:examplehub corp.example.com smtp:corphub sales.example.com smtp:saleshub
The recommended method of editing the mail files is to change the sendmail server’s properties using the Admin Console. This opens a file editor that knows to automatically rebuild and restart the sendmail server when you save a file.

To edit the mail configuration files using this method:

**Caution:** Only experienced administrators should modify sendmail configuration files.

1. In the Admin Console, select **Policy > Rule Elements > Services** and then select **sendmail**.
2. Click **Properties**. The following window appears:

![Services: sendmail Properties window](image-url)
3 Select the configuration file you want to modify in the appropriate burb configuration file list. There are separate files for each sendmail server running on the appliance. You may edit the following files:

Tip: Before making any changes, select File > Backup and create a backup file. Also, for best results, do not edit these files with any other file editor, as those editors will not automatically rebuild and restart the sendmail server.

- **Access Table** — This file defines anti-relaying and anti-spamming policies for the SMTP server.
- **Aliases file** — (Available only in the internal burb.) This file defines the mail aliases that are used to redirect e-mail to another person or location.
- **Alternate Host Names file** — This file identifies alternate host names by which the appliance is known. E-mail addressed to any of the alternate names is treated as local mail by the appliance.
- **Domain Table** — This file provides a mapping from an old domain name to a new domain name. For example, you might modify this file if your organization’s external domain name changes.
- **M4 Config file** — This file defines the initial sendmail configuration. Modify this file as needed to account for your site-specific requirements.
- **Mailer Table** — This file maps a domain to a mail relay that is responsible for mail delivery in that domain.

Important: Only edit mail configuration files if it is necessary for your site’s e-mail functionality.

4 Save and then close the file.

5 Open the appropriate mailertable file and edit as necessary.

Important: Only edit mailertable files if it is necessary for your site’s e-mail functionality.

The mailertable files are named /etc/mail/mailertable.mta# (# = the appropriate burb number).
6 Enter the correct domain, mailer, and host in the following format:

```
domain <tab> mailer:host
```

On the internal side of the network, the mailertable appears as:

```
.example.net <tab> smtp:examplehub
example.net <tab> smtp:examplehub
corp.example.net <tab> smtp:examplehub
sales.example.net <tab> smtp:examplehub
```

On the external side of the network, the mailertable should appear as:

```
example.net <tab> burbmailer-burb:localhost
.example.net <tab> burbmailer-burb:localhost
```

where \texttt{burb} = the external burb number and \texttt{Y} = the internal (trusted) burb number.

The entries that begin with a dot (.) act as a wildcard, matching anything with that domain name. The entries that do not begin with a dot match the full domain name. See the \texttt{/usr/share/sendmail/README} file for more information on creating mailertables.

7 Save and then close the file.

8 Click Save to save the configuration changes and rebuild the configuration and database files. This will also automatically restart the sendmail servers.

\textit{Note: If at a command prompt, use cf sendmail rebuild and cf daemond restart agent=sendmail.}

The appliance has updated sendmail with your changes and is now ready to process mail.

This window also has a shortcut to the Reconfigure Mail area. See “Setting up and reconfiguring mail” on page 474 for details on changing your mail configuration.
Once you run Reconfigure Mail to set up hosted mail and create the appropriate rules, the basic mail services are enabled. However, sendmail provides several additional features that you may choose to configure. Of those listed here, mail routing, header stripping, and the RealTime Blackhole list are the most popular additional sendmail features. The details for implementing these features are described in the sections that follow.

- **Mail routing** — Enables you to reroute e-mail from one domain name to another domain name by editing the mailertable files.
  
  See “Editing sendmail files on Sidewinder” on page 480.

- **Header stripping** — Enables you to remove header information from an outbound message to conceal internal host information from the outside world.
  
  See “Configuring sendmail to strip message headers” on page 484.

- **Blackhole list** — Enables you to eliminate unwanted and unsolicited e-mail. The types of spam control you might implement include use of a Realtime Blackhole list, Promiscuous Relaying, and so on.
  
  See “Configuring sendmail to use the RealTime Blackhole list” on page 486.

- **Filter mail based on the user** — Enables you to allow or deny mail based on a specific user or users.
  
  See “Allowing or denying mail on a user basis” on page 487.

- **Masquerading** — Enables you to transform a local host address in the header of an e-mail message into the address of a different host.
  
  See “Configuring sendmail to hide internal e-mail addresses” on page 488.

**Tip:** You can also configure aliases for e-mail accounts. Creating aliases for the Sidewinder administrator accounts is particularly useful because system messages sent to these accounts can, if left unattended, fill up the Sidewinder hard drive.

### Configuring sendmail to strip message headers

During the normal operation of sendmail, the path a message traces is appended to the message by each host through which the mail passes. This enables internal host names and IP addresses to be allowed beyond the Sidewinder appliance.

**Note:** Header information can only be removed for outbound mail (that is, mail leaving the Sidewinder appliance). Therefore, you should only enable header stripping in the destination (or external) burb for a message. If you configure header stripping in the source burb of a message, header stripping will not happen for that message.
You can configure sendmail to strip (remove) or scrub (change to a different value) the following headers from messages leaving the appliance:

- Received (stripped)
- X400-received (stripped)
- Via (stripped)
- Mail-from (stripped)
- Return-path (stripped)
- Message-id (scrubbed)
- Resent-message-id (scrubbed)

**Note:** Stripping the headers will not alter the To and From hosts. The To and From hosts can be eliminated using rules in the **sendmail** configuration file. You can also modify the To and From hosts using masquerading or by editing the domain tables.

To configure sendmail to strip or scrub headers:

1. Select **Policy > Rules Elements > Services**.
2. Select **sendmail** and click **Modify**.
3. Click **Properties**. A list of mail files appears. Note that separate configuration files are maintained for each burb.
4. Select the **M4 Config File** in the external burb list and click **Edit File**.
   
   **Tip:** Before making any changes, select **File > Backup** and create a backup of this file.

5. Locate the **C{STRIP_DOMAINS}** line in the file and append the domain name on which to perform header stripping. For example:

   ```
   C{STRIP_DOMAINS} domainx
   ```

   where `domainx` = the domain name on which to perform header stripping.

   You can define multiple domains by entering multiple domain names on one line (for example, `C{STRIP_DOMAINS} abc.com xyz.com`).

   **Note:** STRIP_DOMAINS contains the list of domains that will trigger header stripping. Each message processed by **sendmail** in the external burb will be subjected to header stripping if it is received from a domain in this list.

6. Save and then close the file.
7. Click **OK** to return the main Services window.
8. Click **Save** to save the configuration changes and rebuild the configuration and database files. This will also automatically restart the sendmail servers.

   **Note:** If at a command prompt, use `cf sendmail rebuild` and `cf daemond restart agent=sendmail`. 
Configuring sendmail to use the RealTime Blackhole list

Sendmail is able to use the services of the RealTime Blackhole List (RBL). The Blackhole List, a list of known spam domain names, is maintained by an organization called MAPS (Mail Abuse Prevention System). The mail server checks each mail message against the Blackhole list. Any e-mail message originating from a domain in the list will be rejected.

**Note:** You must subscribe to the Trend Micro Blackhole List in order to use it. Go to [www.trendmicro.com/services/rbl](http://www.trendmicro.com/services/rbl) for details. Other blackhole lists may work with the Sidewinder appliance, but are not supported.

To configure the appliance to use a Realtime Blackhole List:

1. Select **Policy > Rules Elements > Services**.
2. Select **sendmail** and click **Modify**.
3. Click **Properties**. A list of mail files appears. Note that separate configuration files are maintained for each burb.
4. Select the **M4 Config File** in the external burb list and click **Edit File**.
   
   **Tip:** Before making any changes, select **File > Backup** and create a backup of this file.

5. Add the following line to the file.
   
   ```
   FEATURE('dnsbl', 'domain')
   ```
   
   The **domain** that you enter in the above line will depend on the type of service for which you have subscribed. If you subscribe to MAPS, they will provide you with the correct domain (for example, `blackholes.mail-abuse.org`) to use.

6. Save and then close the file.
7. Click **OK** to return the main Services window.
8. Click **Save** to save the configuration changes and rebuild the configuration and database files. This will also automatically restart the sendmail servers.

   **Note:** If at a command prompt, use `cf sendmail rebuild` and `cf daemond restart agent=sendmail`.

Now when the appliance receives mail, it will query the RBL to see if the sender’s domain is on the list. If the domain is a match, sendmail rejects the message.
Allowing or denying mail on a user basis

Sendmail will allow or deny mail on a domain basis. However, you can also instruct sendmail to allow or deny mail to/from specific users, IP addresses, and subnets within a domain. To do this, follow the steps below:

2. Select sendmail and click Modify.
3. Click Properties. A list of mail files appears. Note that separate configuration files are maintained for each burb.
4. Select the Access Table file for the appropriate burb and click Edit File.

**Tip:** Before making any changes, select File > Backup and create a backup of this file.

5. Add the specific allow (RELAY), deny and notify the sender (REJECT), and/or deny without notifying the sender (DISCARD) information to the access table.

For example, if you want to allow mail addressed to Lloyd and Sharon but deny mail addressed to everyone else, you would add the following lines:

```
# Allow mail addressed to these users
To:Lloyd@example.com RELAY
To:Sharon@example.com RELAY
# Deny mail for everyone else
To:example.com REJECT
```

**Note:** For additional information, see the README file in the /usr/share/sendmail directory on the appliance.

6. Save and then close the file.
7. Click OK to return the main Services window.
8. Click Save to save the configuration changes and rebuild the configuration and database files. This will also automatically restart the sendmail servers.

**Note:** If at a command prompt, use cf sendmail rebuild and cf daemond restart agent=sendmail.

Mail from those specified users, IP addresses, and subnets will now be handled as indicated in the file.
Configuring sendmail to hide internal e-mail addresses

Occasionally, you may use domain names on your internal network that you do not want the rest of the Internet to know about. You can sendmail instruct to change the header information so that it hides internal domains before relaying the mail on to the final destination. This is called masquerading. Masquerading also involves modifying the “From “ or “From:” field before the mail is relayed. To do this, follow the steps below:

**Tip:** Using masquerade_entire_domain field is effective, but it leaves open the possibility of showing internal addresses that are included on the message (such as the CC or To fields). Use masquerade_envelope field to masquerade all addresses in the envelope containing the domain using the specified domain.

2. Select sendmail and click Modify.
3. Click Properties. A list of mail files appears. Note that separate configuration files are maintained for each burb.
4. Select the M4 Config File for the Internet burb (generally the external burb).
   **Tip:** Before making any changes, select File > Backup and create a backup.
5. Identify the domains you want hidden:
   a. Locate the MASQUERADE_DOMAIN section. The default looks like this:
      ```
      dnl # MASQUERADE_DOMAIN('hide_me.acme.com hide_me_too.acme.com')
      ```
   b. Uncomment the line by deleting “dnl #”.
   c. Changed the listed domains to the domain or domains that you want to hide. For example, `hide_me.acme.com hide_me_too.acme.com` becomes `sales.example.net`.
6. Enter the domain you want to show:
   a. Locate the MASQUERADE_AS section. The default looks like this:
      ```
      dnl # MASQUERADE_AS('newdomain.com')
      dnl # FEATURE('masquerade_entire_domain')
      dnl # FEATURE('masquerade_envelope')
      ```
   b. Uncomment the section by deleting each “dnl #”.
   c. In the MASQUERADE_AS line, change the listed domain to the domain that should replace all internal domains. For example, `newdomain.com` becomes `example.net`.
7. Save and then close the file.
8. Click OK to return the main Services window.
9. Click Save to save the configuration changes and rebuild the configuration and database files. This will also automatically restart the sendmail servers.

**Note:** If at a command prompt, use `cf sendmail rebuild` and `cf daemond restart agent=sendmail`.
Enabling Sendmail TLS

The Sendmail implementation of RFC 2487, SMTP over TLS, is supported on the Sidewinder appliance.

Sendmail can act as either a client or server in a TLS session:

- When acting as the server, it advertises the STARTTLS feature in the response to the EHLO command, then responds positively to the subsequent STARTTLS command.
- When acting as the client, it issues the STARTTLS command if the remote server advertises STARTTLS on the EHLO response.

In both cases, after the STARTTLS command and positive response, the client and server negotiate a TLS session.

**Note:** As part of the implementation, Sendmail TLS also enforces FIPS mode.

For more information on enabling Sendmail TLS, see the Knowledge Base article 7093 at [www.securecomputing.com/goto/kb](http://www.securecomputing.com/goto/kb).
Managing mail queues

If a sendmail message cannot be delivered (for example, if the destination system is down), messages are temporarily placed in queues until they can be delivered. There are separate queues for each server: `/var/spool/mqueue.c` (local) and `/var/spool/mqueue.#` for the Internet and the trusted burbs. The following sections explain how to view mail, how to change some of the basic queue settings, and how to manually force sendmail to attempt to deliver queued mail.

Tip: You should check the queues periodically. If there are a lot of messages that are several days old, you may have a problem with your system or its configuration.

Viewing the mail queue

To view the mail queue output, type the following command:

```
mailq
```

The output of this command lists the messages currently in the queue you chose, along with information about each message. Each message is assigned a unique identification number, which is shown in the first column. In the following example, the external queue shows a message still in queue due to some temporary error. The internal queue shows a valid message ready to be delivered or possibly currently being delivered. The common_sendmail queue shows no mail queued up which should normally, but not always, be the case.

Listing the external Queue

```
/var/spool/mqueue.1 (1 request)
-----Q-ID----- --Size-- -----Q-Time----- ------------Sender/Recipient---------
KA6M17qb008045        4 Mon Nov  6 16:01 me@mydomain.com
    (Deferred: Connection refused by yourdomain.com.)
you@yourdomain.com
```

Total requests: 1

Listing the internal Queue

```
/var/spool/mqueue.2 (1 request)
-----Q-ID----- --Size-- -----Q-Time----- ------------Sender/Recipient---------
KA6M4gd8008045        4 Mon Nov  6 16:04 admin@fwdomain.com
    adminuser@internaldomain.com
```

Total requests: 1

Listing the common_sendmail Queue

```
/var/spool/mqueue.c is empty
```

Total requests: 0
Changing how long a message waits between delivery attempts

By default, undelivered e-mail messages remain in the mail queues 30 minutes before another delivery attempt is made. If you want to change the length of time e-mail messages remain in the mail queues before another delivery attempt is made, do the following:

2. Select sendmail and click Modify.
3. Click Properties. A list of mail files appears. Note that separate configuration files are maintained for each burb.
4. Select the M4 Config File for the burb that is running sendmail, and click Edit File.

   **Tip:** Before making any changes, select File > Backup and create a backup of this file.

5. Scroll to the Set the Queue Interval area and edit the following line:
   ```
   define(`confQUEUE_INTERVAL', `Xm')
   ```
   where:
   - $X$ is the amount of time that the message remains in the queue before an attempt is made to resend the message.
   - $m$ indicates that the time will be measured in minutes. You can also use other time measurements, such as seconds (s), hours (h), days (d), etc.

   **Note:** The default value is 30 minutes.

6. Save and then close the file.
7. Click OK to return the main Services window.
8. Click Save to save the configuration changes and rebuild the configuration and database files. This automatically restarts the sendmail servers.

The time a message waits before sendmail attempts to deliver it has now been changed.
Manually attempting to deliver queued messages

Occasionally, you may need to attempt to send all queued messages immediately instead of waiting for them to be pushed automatically. This process is called *flushing* the mail queue. If you want to force sendmail to attempt to deliver its queued messages, do the following:

1. At a Sidewinder command prompt, enter the following command to change to the Admn role:
   
   `srole`

2. Instruct sendmail to manually attempt to deliver mail in one or more mail queues:
   
   - `cf sendmail flush` — Flushes all three queues.
   - `cf sendmail flush queue=`burbname` — Flushes only the queue for that burb.
   - `cf sendmail flush queue=common` — Flushes the queue containing mail sent by the Sidewinder appliance, such as system updates and alerts.

The appliance immediately attempts to send all mail in the queue.
Changing how long a message waits before it is returned to its sender

By default, undelivered e-mail messages remain in the mail queues 5 days before they are returned to their senders as undeliverable and deleted from the queue. If you want to change the length of time e-mail messages remain in the mail queues before they are considered undeliverable, do the following:

2. Select sendmail and click Modify.
3. Click Properties. A list of mail files appears. Note that separate configuration files are maintained for each burb.
4. Select the M4 Config File for the burb that is running sendmail, and click Edit File.

Tip: Before making any changes, select File > Backup and create a backup of this file.

5. Locate the Set the Queue Interval area and edit the following line:

   ```
   define(`confTO_QUEUERETURN', `Xd')
   ```

   where:
   
   \( X \) is the amount of time that the message remains in the queue its sender is notified that it was undeliverable and the message is deleted.

   \( d \) indicates that the time will be measured in days. You can also use other time measurements, such as seconds (s), minutes (m), hours (h), etc.

   The default value is 5 days.

6. Save and then close the file.
7. Click OK to return the main Services window.
8. Click Save to save the configuration changes and rebuild the configuration and database files. This automatically restarts the sendmail servers.

The time an undelivered message waits before sendmail returns it to its sender has now been changed.
Receiving mail sent by Sidewinder

The Sidewinder appliance sends status updates and alerts to root and administrator accounts. By default, these accounts are hosted on the appliance and must be checked using a command line session. If you want to redirect mail from your administrators’ Sidewinder mailboxes to a different destination, you can edit the `/etc/mail/aliases` file. The following sections provide information on how to create e-mail aliases or access the mail messages directly on the appliance.

Setting up e-mail aliases for administrator accounts

On the Sidewinder appliance, messages and other files are often e-mailed to system users such as `root` and `postmaster`. To redirect these system messages to an external account, you can set up an alias.

*Tip:* Remember to update aliases when there are personnel changes.

Aliases are stored in the `/etc/mail` directory, which can be accessed through the sendmail service. Do the following to set up a mail alias for system users:

1. At a Sidewinder command prompt, enter the following command to change to the Admn role:
   
   `srole`

2. Using a file editor, open `/etc/mail/aliases`.

3. Locate the root line in the file. The default, root, is automatically aliased to the administrator account created during the Quick Start Wizard and looks like this:
   
   `#root: username`

4. Uncomment the line by deleting the #, and then replace the existing address with the off-box e-mail address of the person who will receive system messages. If you want to add multiple accounts, separate them with commas and do not included spaces.
   
   The line now looks like this:
   
   `root: username_a@example.com,username_b@example.com`

   By default, all other system roles are aliased to root, and mail sent to those accounts will also be sent to the e-mail address entered above. To redirect other system roles’ mail to other accounts, use the same format.

5. Save the changes and then close the file.

6. Enter the following commands:
   
   `cf sendmail rebuild`
   `cf daemond restart agent=sendmail`

   This rebuilds the configuration and database files, and restarts the sendmail servers.

System mail messages will now be sent to the aliased account instead of accumulating on the Sidewinder hard drive.
Viewing administrator mail messages on Sidewinder

By default, a root alias is created for the administrator you set up when you configured your system. This alias automatically redirects system messages addressed to root to that first administrator’s Sidewinder-hosted account. A mailbox will be created the first time an administrator sends or receives a mail message. Mailboxes for Sidewinder administrators are stored in the /var/mail directory.

**Important:** Do not ignore the e-mail that accumulates on the Sidewinder appliance as it contains important information about your network and the appliance, and also uses disk space. Routinely read and delete mail sent to the appliance, or have it redirected elsewhere. To redirect mail to another destination, see the previous section, “Setting up e-mail aliases for administrator accounts”.

To view system messages sent to Sidewinder-hosted accounts, follow the steps below.

1. At a Sidewinder command prompt, enter the following command to change to the Admn role:
   ```
   srole
   ```
2. View e-mail messages by entering one of the following:
   - `mail` — Displays your messages (messages for the logged-in administrator)
   - `mail -f root` — Displays messages addressed to root
   - `mail -f username` — Displays messages addressed to that administrator

   **Tip:** Refer to the `mail` man page for detailed information on using the `mail` command. If you prefer, you may use an alternate mail program.

Remember to check mail frequently, particularly if you have attack and system event responses sent to `root`.

**Note:** For more on responses, see Chapter 13, “IPS Attack and System Event Responses”, on page 399.
Chapter 17: E-mail

Receiving mail sent by Sidewinder
In this chapter...

What is DNS? ................................................................. 498
About transparent DNS ..................................................... 499
About Sidewinder-hosted DNS .......................................... 500
Configuring transparent DNS .......................................... 506
Configuring Sidewinder-hosted DNS servers ...................... 507
Reconfiguring DNS ......................................................... 528
Manually editing DNS configuration files ......................... 533
DNS message logging ...................................................... 534
What is DNS?

The domain name system (DNS) is a service that translates host names to IP addresses, and vice versa. DNS is necessary because while computers use a numeric addressing scheme to communicate with each other, most individuals prefer to address computers by name. DNS acts as the translator, matching computer names with their IP addresses.

Much of the traffic that flows into and out of your organization must at some point reference a DNS server. In many organizations this server resides on a separate, unsecured computer. The Sidewinder appliance provides the additional option to host the DNS server directly on the appliance, eliminating the need for an additional computer.

The Sidewinder appliance offers two main DNS configurations:

- **Transparent DNS** — Transparent DNS is designed for simple DNS configurations. The DNS server is on a separate computer, and DNS requests are proxied through the appliance. It is the default DNS configuration for a newly installed Sidewinder appliance. See “About transparent DNS” on page 499.

- **Sidewinder-hosted DNS** — Sidewinder-hosted DNS represents a more complex DNS configuration that uses the integrated Sidewinder DNS server. See “About Sidewinder-hosted DNS” on page 500.

Managing and changing your DNS configuration

Transparent DNS is the default configuration, created during initial configuration using the Quick Start Wizard. If you want to make changes to your existing DNS configuration, you can use one of two methods:

- **Admin Console** — Select Network > DNS to view and modify DNS settings. You can also click the Reconfigure DNS button to completely reconfigure your DNS settings. See the following for details:
  - “Configuring transparent DNS” on page 506
  - “Reconfiguring DNS” on page 528

  **Note:** Using the Admin Console to modify your DNS configuration will remove any comments you may have manually inserted into the DNS configuration files.

- **Manual** — You can manually edit the DNS configuration files. This should only be attempted by highly skilled DNS administrators. See “Manually editing DNS configuration files” on page 533 for details.

  **Note:** An excellent source of information on DNS is the Internet Software Consortium Web site at [www.isc.org](http://www.isc.org). The book DNS and BIND, by Albitz & Liu (O’Reilly & Associates, Inc.) is also a popular reference.
About transparent DNS

Transparent DNS represents a simplified DNS configuration. When transparent DNS is configured for the Sidewinder appliance, DNS traffic passes transparently through the appliance using a proxy. The appliance uses proxy rules that pass all DNS traffic by proxy to its appropriate burb. DNS requests are then handled by the remote name servers. Other machines do not “see” the Sidewinder appliance, which means there is minimal disruption to your current DNS configurations throughout your network.

Configuring transparent DNS requires specifying the IP address of one or more remote DNS servers. (Alternative server addresses may be used for redundancy.) If a customer is using NAT through the appliance, they should also have an additional DNS server on the outside of their network. The external DNS server handles the external zones of your network and its addresses. This configuration allows you to control which addresses are visible to the outside world.

There are two transparent DNS configuration options:

- **Single server** — The DNS traffic is proxied through the appliance. This configuration is generally used when you plan to use your existing DNS server. If you are using a single internal DNS server, external users have proxied access to your DNS server. External hosts are unaware that the appliance is “transparently” passing the DNS traffic.

- **Two servers** — The DNS traffic is proxied through the appliance, with a remote DNS server communicating with each interface. DNS queries are generally handled by both your internal DNS server and your external ISP. This configuration is more secure than using a single name server because your external server can limit access to your internal naming system. External hosts are unaware that the appliance is “transparently” passing the DNS traffic.

Transparent DNS is the default configuration on a newly installed Sidewinder appliance. One server or two server DNS depends on your entries in the Quick Start Wizard. If you want to change your DNS configuration, see “Reconfiguring DNS” on page 528.

**Note:** Transparent DNS is designed for simple DNS configurations. Complex DNS configurations may require DNS services to be hosted directly on the appliance.
About Sidewinder-hosted DNS

Sidewinder-hosted DNS represents a more complex DNS configuration that uses the integrated Sidewinder DNS server. When configured for hosted services, DNS servers run directly on the Sidewinder appliance. This places the DNS server(s) on a hardened operating system, preventing attacks against these servers from penetrating your network.

You can configure Sidewinder-hosted DNS to use a single server or split servers:

- **Hosted single server DNS** — In a Sidewinder-hosted single server configuration, one DNS server is hosted on the appliance. That server handles all DNS queries. The server is protected by the Sidewinder hardened OS, preventing attacks from penetrating your network. A single server configuration is generally used when you have no concerns for keeping your internal network architecture hidden, such as when your Sidewinder appliance is acting as an “intrawall” between two sets of private addresses. External hosts will need to be reconfigured to point to the Sidewinder server.

- **Hosted split server DNS** — In a Sidewinder-hosted split server configuration, two DNS servers are hosted on the appliance: one server (the external name server) is bound to the external burb and the other server (the “unbound” name server) is available for use by all internal burbs. Both servers are protected by the Sidewinder hardened OS, which is able to prevent attacks against them from penetrating your network.

Secure Computing recommends splitting the Sidewinder DNS servers when using hosted DNS. This configuration offers a good security benefit because the external burb of the appliance hides the DNS entries on the internal server from those who only have access to the external burb.

**Important:** You must use hosted split DNS if you want the appliance to hide your private IP addresses (via Network Address Translation).
Designating an authoritative server

If your site has multiple internal domains, and there are name servers for each of these domains, the Sidewinder appliance must be designated as an authoritative name server for all of the internal domains (the internal name servers also may be authoritative for one or more of the internal domains). This must occur regardless of whether the appliance is a master or a slave name server. The appliance must be an authoritative name server for all internal domains so that it can resolve queries for the internal domains. The appliance will otherwise automatically forward these internal name queries to the Internet, and the query will not be resolved.

In split DNS mode, if a DNS name occurs in the database of both servers, the name will resolve differently depending on the server that is queried. This occurs when the appliance is authoritative for the same domain both internally and externally. Because of this issue, if you try to access the Internet side of the appliance from an internal workstation you must use the appropriate machine name. For example, if the name of your appliance is *chloe*, then use the machine name *chloe-Internet*. This entry is automatically created during installation.

For more information on DNS, see *DNS and BIND* by Albitz & Liu, 3rd edition (O’Reilly).

Using master and slave servers in your network

In a hosted DNS configuration, the Sidewinder appliance requires information about your DNS authority. Generally, there should be only one master name server for any fully qualified domain (such as nyc.example.com), also called a zone. There may be many slave servers, for redundancy and better performance, but they derive their information from the one master for each domain.

Typically, a company will use two or more DNS servers to provide domain name service to their customers. This provides for load balancing and redundancy. When more than one DNS server is used, the local administrator designates one DNS server to host the master zone files. The other DNS servers are slave servers that merely retrieve copies of the zone files from the master server. To outside users there is no indication or need to know about which of the multiple servers is the master. They all provide equally authoritative answers to all queries. The designation of which DNS server will be the master is only significant to the DNS administrator, because changes are made only at the master DNS server and not at the individual slave servers.

*Important:* When DNS servers are in an HA cluster, Secure Computing recommends configuring the Sidewinder appliance name servers as DNS slaves for authoritative zones. This allows the Master DNS servers to update both appliances in the HA cluster. If you do not configure the Sidewinder name servers as DNS slaves for authoritative zones, DNS changes will be made to the secondary appliance with the next policy push.
If you use Sidewinder-hosted DNS, computers in your network must be configured to point to the appropriate DNS servers on the Sidewinder appliance.

- Internal computers going through a proxy transparently to access the Internet must be configured to direct DNS queries in either of these ways:
  - If you have internal name servers, the client computers must point to one or more of these name servers. The internal name servers should be authoritative for the internal domain, and should be configured to forward DNS queries to the Sidewinder appliance.
  - Reference the appliance on the client computers. For example:
    - In a UNIX system, enter the IP address of the Sidewinder’s DNS server in the /etc/resolv.conf file.
    - In a Windows system, enter the IP address of the Sidewinder’s DNS server in the TCP/IP Properties window.

- If you are using hosted split server DNS, external hosts must be configured to point to the external burb of the Sidewinder DNS servers.

- If you are hosting your own domain, your domain records can be configured to use the external Sidewinder DNS server as an authoritative name server for your domain. This is generally done with your domain registrar.
Enabling and disabling hosted DNS servers

When you configure Sidewinder-hosted DNS services, the Sidewinder appliance will use either one or two DNS servers. The DNS server(s) start automatically when you boot the appliance.

You can manually disable a DNS server on the Server Configuration tab of the DNS window by clearing the Enable [Unbound/Internet] Domain Name Server check box.

Keep the following points in mind, however, if you decide to disable a Sidewinder-hosted DNS server:

- **If you have one DNS server**
  In this situation, the server is known as an *unbound DNS server*. If you disable the DNS server, only connections that use IP addresses will still work; those that use host names will not.

- **If you have two DNS servers**
  This situation is also known as *split DNS mode*. Note the following:
  - If you disable the Unbound DNS server, connections that use IP addresses will still work; those that use host names will not.
  - If you disable the Internet server, external connections that require host names will not work unless the name is already cached (saved) in the unbound name server’s database. Connections that use IP addresses will work. E-mail will be placed in a queue since IP addresses cannot be resolved.
  - If you disable both name servers, connections will work only if they use IP addresses rather than host names. Also, mail will not work and other errors will happen as other parts of the system attempt to access the network by name.

In either case, once you disable a server, the server will remain disabled until you enable it again.
Using hosted sendmail with Sidewinder-hosted DNS

If you use hosted sendmail, you need to create mail exchanger (MX) records when you set up Sidewinder-hosted DNS services for your site. MX records advertise that you are accepting mail for a specific domain(s). If you do not create an MX record for your domain, name servers and users on the Internet will not know how to send e-mail to you. When an e-mail message is sent from a site on the Internet, a DNS query is made in order to find the correct mail exchange (MX) host for the destination domain. The sender’s mail process then sends the e-mail to the MX host. The appliance, through the use of mailertables, will forward the mail to the internal mail process, which in turn will forward it to the internal mail host. See “Editing sendmail files on Sidewinder” on page 480 for more information on mailertables.

Consider the example shown in the figure below. Someone in the Internet, Lloyd, wants to send one of your users, Sharon, an e-mail message, but all Lloyd knows is Sharon’s e-mail address: sharon@foo.com. The mailer at Lloyd’s site uses DNS to find the MX record of foo.com. Lloyd’s message for Sharon is then sent to the mailhost listed in the MX record for Sharon’s site.

**Figure 216:** Mail exchanger example

A master name server stores and controls your site's MX records. The master name server may be in the external burb of your appliance, or on a host outside of your network (for example, your Internet service provider). If your appliance controls the master name server, then you can make any necessary changes to your MX records; if another host controls your master name server, then changes have to be made on that host. For more information on MX records, see Chapter 5 of *DNS and Bind* by Albitz & Liu.

For information on creating MX records using the Admin Console, see “Configuring the Master Zone Attributes tab” on page 518.
More points about Sidewinder-hosted DNS

Listed below are some additional points about running DNS on your Sidewinder appliance:

• The Sidewinder appliance uses Berkeley Internet Name Domain (BIND 9).

• The configuration files for the unbound and the Internet name servers are `/etc/named.conf.u` and `/etc/named.conf.i`, respectively. The configuration files specify corresponding directories: `/etc/namedb.u` and `/etc/namedb.i`. When you boot your appliance, the name server daemon (`named`) is started. The `/etc/named.conf.u` and `/etc/named.conf.i` files specify whether the appliance is a master or a slave name server and list the names of the files that contain the DNS database records.

• If you choose to configure the appliance as a master name server on either the unbound (internal) or Internet (external) side, you can modify the `/etc/namedb.u/domain-name.db` and `/etc/namedb.i/domain-name.db` files (where `domain-name` = your site’s domain name). You can add the information that is being advertised for these zones.

• The appliance contains a non-blocking DNS resolver to support reverse IP address look-ups in the active proxy rule group, and name-to-address look-ups in the various proxies. The relevant resolver library calls are `gethostbyname()` and `gethostbyaddr()`. The non-blocking DNS resolver provides a small number of DNS resolver daemons (nbresd) that are handed queries to resolve on behalf of the client.
Configuring transparent DNS

If you have configured DNS to use transparent services, you can add, modify, or delete transparent name servers. Select **Network > DNS**. The following window appears:

**Note:** *If you want to completely reconfigure your existing DNS configuration (for example, change from transparent DNS to Sidewinder-hosted DNS or vice versa), you must use the Reconfigure DNS window. See “Reconfiguring DNS” on page 528 for details.*

Use this window to configure name servers for transparent DNS services. You can specify the Burb to which the name servers will be assigned from the *Burb* drop-down list. You can assign and order DNS servers for any configured Burb, plus the Firewall Burb.

The order in which the servers appear indicates the order in which the Sidewinder appliance queries them.

- To add a new name server to the list, click **New**. To modify a name server, select the name server and click **Modify**.
- To change the name servers’ order, select a name server and click the **Up** and **Down** buttons as appropriate.
- To delete a name server, select the name server and click **Delete**.
If you configure DNS to use Sidewinder-hosted services (single or split), you can define various name server information.

**Note:** If you want to completely reconfigure your existing DNS configuration (for example, change from transparent DNS to Sidewinder-hosted DNS or vice versa), you must use the Reconfigure DNS window. See “Reconfiguring DNS” on page 528 for details.

Select **Network > DNS**. The DNS window contains four tabs that allow you to define specific name server information.

- The **Server Configuration** tab is used to configure general information about a name server. See “Configuring the Server Configuration tab” on page 509 for details.

- The **Zones** tab defines each of the master and slave zones associated with the selected name server. See “Configuring the Zones tab” on page 513 for details.

- The **Master Zone Attributes** tab is used to configure attributes for each *master* zone defined on the **Zones** tab. See “Configuring the Master Zone Attributes tab” on page 518 for details.

- The **Master Zone Contents** tab defines the hosts associated with each *master* zone defined on the **Zones** tab. See “Configuring the Master Zone Contents tab” on page 523 for details.
Figure 219 below illustrates the different DNS objects you can configure, how they relate to each other, and which tab is used to configure each object.

**Figure 219:** DNS objects and the tab used to configure each object
Chapter 18: DNS (Domain Name System)  
Configuring Sidewinder-hosted DNS servers

Configuring the Server Configuration tab

The **Server Configuration** tab is used to define configuration settings for the selected name server.

![Server Configuration tab](image)

Use this tab to define alternate name servers that will be contacted if a query cannot be resolved by the selected name server. The alternate name servers are called *forwarders*. This window is also used to define advanced configuration settings for the name server. To modify the Server Configuration tab:

**Note:** To completely reconfigure your DNS settings (for example, change from Sidewinder-hosted single server to split server), click **Reconfigure DNS**. See “Reconfiguring DNS” on page 528 for details.

1. In the **Modify Server For** field, select the name server that you want to modify. (The Internet server is available only if you are using two servers.)
2. [Conditional] If you want to disable the selected name server, clear the **Enable Unbound/Internet Domain Name Server** check box. (The Internet Domain Name Server is available only if two servers are defined.)

See “Enabling and disabling hosted DNS servers” on page 503 for information about the effects of enabling or disabling the servers.

**Note:** The **File Directory** field displays the location of the files used to store information about the selected server. This field cannot be modified.
3 In the **Do Forwarding** field, specify whether the name server will forward queries it cannot answer to another name server. In a split DNS configuration, when modifying the unbound name server this field will default to Yes and will forward these unresolved queries to the Internet server (127.x.0.1, where x = the external [or Internet] burb number).

Forwarding occurs only on those queries for which the server is not authoritative and does not have the answer in its cache.

4 [Conditional] If you selected Yes in the previous step, configure the **Forward Only** field. Specify the following:

- If you select Yes, the name server will forward queries it cannot answer to the name servers listed in the Forward To list only. This is the default.
- If you select No, the name server forwards the query to the name servers listed in the Forward To list. If they cannot answer the query, the name server attempts to contact the root server.

5 In the **Forward To** field, specify the alternate name servers that will be used when attempting to resolve a query. This list is consulted only if Yes is selected in the **Do Forwarding** field. If multiple name servers are defined, the name servers are consulted in the order listed until the query is resolved. In a split DNS configuration, when modifying the unbound name server this list will by default contain four entries for the Internet name server (127.x.0.1, where x = the external [or Internet] burb number).

**Important:** If you are using a split DNS configuration, Secure Computing strongly recommends against defining additional alternate name servers for the unbound name server. The Internet (or external) name server should be the only alternate name server defined in this situation.

6 To add another entry to the list of authorized name servers, click **New** under the Forward To list, then type the IP address of the alternate name server. The alternate name servers are consulted if the primary name server cannot resolve a query.

7 To delete a name server from the Forward To list, highlight the name server you want to delete and click **Delete**.

8 [Conditional] To modify an advanced configuration setting for the name server, click **Advanced**. For more information on modifying the Advanced Server Options window, see “About the Advanced Server Options window” on page 511.

**Important:** Only experienced DNS administrators should modify an advanced configuration setting.

9 Save your changes. To configure additional name server information, see “Configuring the Zones tab” on page 513.
About the Advanced Server Options window

Use this window to define some of the more advanced DNS name server options.

- Do not change these options unless you are an experienced DNS system administrator.
- By default, the options on this window are disabled, meaning there are no restrictions. If your organization considers this to be a security risk, you should use these options to limit the amount of interaction this name server has with other devices. Use your organization’s security policy as a guide.

To modify advanced server options:

1. To enable the notify option, select the corresponding check box. Enabling this option allows you to specify whether the master server will notify all slave servers when a zone file changes. The notification indicates to the slaves that the contents of the master have changed and a zone transfer is necessary.

   If this field is not selected, the field defaults to Yes.
2 To enable the **allow-query** option, select the corresponding check box. Selecting this option affects who is able to query this name server. The options are the following:

- If not selected, all requesters are authorized to query the name server. This is the default.
- If selected and contains IP addresses, only the requesters defined in the allow-query list will be authorized to query this name server. Use the **New** and **Delete** buttons to modify this list.

*Note: If you select this option, be sure to include all IP addresses that might need to query the server, such as the heartbeat burbs’ IP addresses, loopback addresses, etc.*

3 To enable the **allow-transfer** option, select the corresponding check box. Selecting this option allows you to limit who is authorized to request zone transfers from this name server.

- If not selected, all requesters are authorized to transfer zones from the name server. This is the default.
- If selected and no IP addresses are added, no requesters will be authorized to transfer zones from this name server.
- If selected and contains IP addresses, only the requesters defined in the allow-transfer list will be authorized to transfer zones from this name server. Use the **New** and **Delete** buttons to modify this list.

4 Click **OK** to save your changes.
Configuring the Zones tab

A DNS server is responsible for serving one or more zones. A zone is a distinct portion of the domain name space. A zone consists of a domain or a subdomain (for example, securecomputing.com or sales.securecomputing.com). Each zone can be configured as either a master, slave or forward zone on this name server.

Figure 222: Sidewinder Hosted: Zones tab
Chapter 18: DNS (Domain Name System)

Configuring Sidewinder-hosted DNS servers

Use this tab to define zone information about the name server. Follow the steps below.

**Note:** To completely reconfigure your DNS settings (for example, change from Sidewinder-hosted single server to split server), click **Reconfigure DNS**. See “Reconfiguring DNS” on page 528 for details.

1. In the **Modify Server For** field, select the name server that you want to modify.

2. The **Zones** list defines the zones for which the name server is authoritative. This list initially contains a zone entry for each domain and each network interface defined to the appliance. You can add or delete zone entries as follows:
   - To add a new zone to the list, click **New** and type the name of the forward or reverse zone you want to add to the list.
   - To delete a zone, highlight a zone and click **Delete**.

Secure Computing strongly recommends against deleting or modifying the following entries:
   - Any 127 reverse zones (for example, `0.127.in-addr.arpa`). These zones represent local loopback addresses and are required.
   - The zone with `0.255.239.in-addr.arpa` in its name. This zone provides multicast support for the Sidewinder failover feature.

There can be two different types of entries in the **Zone** list:
   - **Reverse zones** (for example, `4.3.in-addr.arpa`): This format indicates the entry provides reverse lookup functions for this zone.
   - **Forward zones** (for example, `example.com`): This format indicates the entry provides forward lookup functions for this zone.

The **Related Zones** list displays the zones that are related to the selected zone. For example, if a forward zone is selected, the related reverse lookup zones are displayed. This list cannot be modified.
3 In the **Zone Type** field, specify whether the selected zone is a master zone, a slave zone, or a forward zone, as follows:

- **Master** — A master zone is a zone for which the name server is authoritative. Many organizations define a master zone for each sub-domain within the network. Administrators should only make changes to zones defined as a master.

---

**Important:** You should consider defining a matching reverse zone (an in-addr.arpa zone) for each master zone you configure.

---

- **Slave** — A slave zone is a zone for which the name server is authoritative. Unlike a master zone, however, the slave zone’s data is periodically transferred from another name server that is also authoritative for the zone (usually, the master). If you select **Slave**, the **Master Servers** field becomes active. Be sure to use the **Master Servers** field to define the name server(s) that will provide zone transfer information for this slave zone. Administrators should not make changes to zones defined as a slave.

---

**Caution:** When changing a zone from slave to master, the Admin Console changes the slave file into a master file and the file becomes the lookup manager for the zone. The DNS server will have no problems understanding and using the new master file. For large zones (class A or B), however, this file may become too complex to be managed properly using the Admin Console. Secure Computing recommends either leaving large zones as slaves on the appliance or manually modifying these files.

---

- **Forward** — A forward zone allows you to specify that queries for names in the zone are forwarded to another name server.

4 In the **Zone File Name** field, specify the name of the file that is used to store information about this zone. The file is located in the directory specified in the **File Directory** field on the Server Configuration tab. Secure Computing does not recommend changing this name.

5 [Conditional] When **Zone Type** is **Forward**, the **Forwarders** list defines one or more forwarders for a zone. You can add or delete forwarder entries as follows:

- To add a new forwarder to the list, click **New** and type the IP address.
- To delete a forwarder, select that item and click **Delete**.

6 [Conditional] When the **Zone Type** is **Slave**, the **Master Servers** list defines one or more master name servers that are authorized to transfer zone files to the slave zone. You can add or delete server entries as follows:

- To add a new master server to the list, click **New** and type the IP address.
- To delete a master server, highlight a server and click **Delete**.
7 [Conditional] To modify an advanced configuration setting for the selected zone, click Advanced. For more information on modifying the Advanced Server Options window, see “About the Advanced Zone Configuration window” on page 517.

⚠️ **Important:** Only experienced DNS administrators should modify an advanced configuration setting.

8 Save your changes.
About the Advanced Zone Configuration window

Use the Advanced Zone Configuration window to define some of the more advanced zone configuration options. This window allows you to configure certain options specifically for the selected zone, overriding similar options that may be configured for the global name server (the Unbound or the Internet name server). Follow the steps below.

**Important:** Only experienced DNS administrators should modify an advanced configuration setting.

1. To enable the **notify** option, select the corresponding check box. Enabling this option allows you to specify whether the master server will notify all slave servers when the zone changes. The notification indicates to the slaves that the contents of the master have changed and a zone transfer is necessary. The name servers that are notified are those defined in the **Zone NS Records** field on the **Master Zone Attributes** tab.

   If this field is not selected, the field defaults to **Yes**.

2. To enable the **allow-query** option, select the corresponding check box. Selecting this option affects who is able to query this zone. The options are the following:
   - If not selected, all requesters are authorized to query the zone. This is the default.
   - If selected and contains IP addresses, only the requesters defined in the allow-query list will be authorized to query this zone. Use the **New** and **Delete** buttons to modify this list.

   **Note:** If you select this option, be sure to include all IP addresses that might need to query the zone, such as the heartbeat burbs’ IP addresses, loopback addresses, etc.

3. To enable the **allow-update** option, select the corresponding check box. Selecting this option allows you to specify from whom the zone will accept dynamic DNS updates. If this option is selected, only the hosts in the allow-update list are authorized to update this zone. This option is only valid for master zones. Use the **New** and **Delete** buttons to modify this list.

   By default the **allow-update** option is not selected, meaning the server will deny updates from all hosts.

4. To enable the **allow-transfer** option, select the corresponding check box. Selecting this option allows you to limit who is authorized to request zone transfers from this zone.
   - If not selected, all requesters are authorized to transfer this zone from the name server. This is the default.
   - If selected and no IP addresses are added, no requesters will be authorized to transfer this zone from the name server.
   - If selected and contains IP addresses, only the requesters defined in the allow-transfer list will be authorized to transfer the zone from the name server. Use the **New** and **Delete** buttons to modify this list.
Configuring the Master Zone Attributes tab

Use the **Master Zone Attributes** tab to configure attributes for each master zone defined on the **Zones** tab. Slave zones are not included on this tab because you can only define attributes for those zones for which you are the master.

![Figure 223: Sidewinder Hosted: Master Zone Attributes tab](image)

Use this tab to define the attributes of each master zone defined for the selected name server. In particular, it defines the Name Server record(s) and the Start of Authority (SOA) record for each master zone. The window also enables you to define Mail Exchanger (MX) records for those entries that are forward lookup zones. Follow the steps below.

**Note:** To completely reconfigure your DNS settings (for example, change from Sidewinder-hosted single server to split server), click **Reconfigure DNS.** See “Reconfiguring DNS” on page 528 for details.

1. In the **Modify Server For** field, select the name server that you want to modify.

   The **Master Zones** list defines the zones for which the name server is master. A plus sign (+) will appear in front of any forward lookup zone that contains one or more sub-domains. Click the plus sign to view the sub-domains.

   To modify an entry in the list, click the entry name. A menu of options used to characterize the selected entry is presented on the right side of the window.

   **Note:** The **Forward Lookup Zone Name/Reverse Lookup Zone Name** field displays the full zone name associated with the entry selected in the **Master Zones** list.
2 To modify the **Zone SOA** tab, click the tab and follow the sub-steps below. The fields on the Zone SOA tab collectively define one Start Of Authority (SOA) record. An SOA record controls how master and slave zones interoperate.

![Figure 224: Master Zone Attributes: Zone SOA tab](image)

The **DNS Serial #** field displays the revision number of this SOA record. This field will increment by one each time you modify this zone. Slave zones use this field to determine if their zone files are out-of-date. You cannot modify this field. (See sub-step b for more details.)

- **a** In the **DNS Contact** field, specify the name of the technical contact that can answer questions about this zone. The name must be a fully-qualified name, with the @ character replaced by a period (for example, hostmaster@example.com becomes `hostmaster.example.com`).

- **b** In the **Refresh** field, specify in seconds how often a slave will check this zone for new zone files. The slave uses the **DNS Serial #** value to determine if its zone files need to be updated. For example, if the slave’s DNS serial number is 4 and the master zone’s DNS serial number is 5, the slave knows that its zone files are out-of-date and it will download the updated zone files. Values must be positive integers.

- **c** In the **Retry** field, specify in seconds how long a slave should wait to try another refresh following an unsuccessful refresh attempt. Values must be positive integers.

- **d** In the **Expiration** field, specify in seconds how long a slave can go without updating its data before expiring its data. For example, assume you set this value to 604800 (one week). If the slave is unable to contact this master zone for one week, the slave’s resource records will expire. After expiration, queries to that zone will fail. Values must be positive integers.
e In the TTL field, specify the time to live (TTL) value. This value defines how long a resource record from this zone can be cached by another name server before it expires the record. The value specified here is used as the default in records that do not specify a TTL value. Values must be positive integers.

f To add a sub-domain to the selected zone, click Add Sub.... This button is only available if a forward lookup zone is selected in the Zones list. For information on adding a sub-domain, see “Adding a forward lookup sub-domain” on page 522.

g To delete a sub-domain from the selected zone, click Delete Sub.... This button is only available if a forward lookup zone is selected in the Zones list.
To modify the **Zone Records** tab, click the tab. This tab contains NS (Name Server) and MX (Mail Exchange) records for forward zones. This tab contains only NS Records for reverse zones.

**Figure 225:** Master Zone Attributes: Zone Records tab

- **The Zone NS Records** table contains DNS NS records that indicate what machines will act as name servers for this zone. By default the table contains an entry for the machine you are currently using.
  - To add a Zone NS Records entry, click **New**. In the **NS Record** field, type the domain name associated with this NS record. The name must be a fully qualified name and must end with a period. The name you specify should be a pre-existing domain name that maps to a valid IP address.
  - To delete a Zone NS Records entry, select the entry and click **Delete**. If this zone is configured to notify all slave servers when a zone file changes, the notify commands are sent to all NS hosts specified here. (See “About the Advanced Zone Configuration window” on page 517 for a description of the **notify** field.)

- **The Zone MX Records** list is available only if the selected zone entry is a forward lookup entry. It is used to specify entries in the Mail Exchangers table for the selected zone. The Mail Exchangers table contains DNS MX records that indicate what machines will act as mail routers (mail exchangers) for the selected domain.
  - To add a Zone MX Records entry, click **New**. Type a fully qualified host name, and a priority level for this record. Valid values are 1–65535. The lower the value, the higher the priority.
  - To delete a Zone MX Records record entry, select the entry and click **Delete**.
• The **Zone A Record** field is available only if the selected zone entry is a forward lookup entry. It defines a DNS A record (an Address record) for the zone itself. A DNS A record is used to map host names to IP addresses. The address you specify must be entered using standard dotted quad notation (for example 172.14.207.27).

• The **TXT Record** field is available if the selected zone entry is a forward lookup entry. This optional field allows you to enter comments or additional information about this zone, such as sender id information.

4 Save your changes.

**Adding a forward lookup sub-domain**

Use this window to add a forward lookup sub-domain to the selected forward lookup zone. By adding a sub-domain you are delegating authority for a portion of the parent domain to the new sub-domain. Follow the steps below.

1 In the **Forward Sub-Domain Name** field, type the name of the sub-domain. Do not type a fully qualified name. For example, assume you have a domain named `example.com` that contains a sub-domain named `west`. You would type `west` in this field rather than `west.example.com`.

2 In the **Sub-Domain NS Records** field, specify entries in the Name Servers table for this sub-domain. The Name Servers table contains DNS NS records that indicate what machines will act as name servers for this sub-domain.
   • To add an NS Records entry, click **New**. In the **NS Record** field, type the domain name associated with this NS record. The name must be a fully qualified name and must end with a period. The name you specify should be a pre-existing domain name that maps to a valid IP address.
   • To delete an NS Records entry, select the entry and click **Delete**.

3 [Optional] In the **Sub-Domain MX Records** field, specify entries in the Mail Exchangers table for this sub-domain. The Mail Exchangers table contains DNS MX records that indicate what machines will act as mail routers (mail exchangers) for the sub-domain.
   • To add an MX Records entry, click **New**. Type a fully qualified host name, and a priority level for this record. Valid values are 1–65535. The lower the value, the higher the priority.
   • To delete an MX Records record entry, select the entry and click **Delete**.

4 Click **Add** to add the specified sub-domain. Click **Close** to exit the window.
Configuring the Master Zone Contents tab

The **Master Zone Contents** tab is used to define the hosts that are associated with each master zone.

When you select the **Master Zone Contents** tab, a window similar to the following appears.

**Note:** If you are adding a large number of hosts (hundreds or thousands) to a master zone, you may want to consider manually adding the required host information directly to the appropriate DNS files using one of the available editors on the appliance to save time. However, only experienced Sidewinder administrators should attempt this. (Using the manual method will still require you to manually define each host.)
For each host you define in a forward lookup zone you should also create a matching entry in the associated reverse lookup zone. Follow the steps below.

**Note:** To completely reconfigure your DNS settings (for example, change from Sidewinder-hosted single server to split server), click **Reconfigure DNS**. See “Reconfiguring DNS” on page 528 for details.

1. In the **Modify Server For** field, select the name server that you want to modify.

   The fields that are available on this tab will vary depending on whether a zone, a host in a forward lookup zone, or a host in a reverse lookup zone is selected.

2. [Conditional] If you are modifying a zone, do the following:
   
   a. In the Master Zones area, select the zone you want to modify.
   
   b. To add a host to the selected zone, click **Add Entry**.
      
      • If you are adding a host to a forward lookup zone, see “Adding a new forward lookup entry” on page 526 for details.
      
      • If you are adding a host to a reverse lookup zone, see “Adding a new reverse lookup entry” on page 527.
   
   c. To delete a host from the selected zone, click **Delete Entry**. The **Hosts in Zone** field lists all the hosts currently defined within the selected zone. Select the host you want to delete and click **Delete Host**. You can only delete one host at a time.

3. [Conditional] If you are modifying a host in a reverse lookup zone, the following two fields appear:
   
   • **Name (Host portion of IP)** — The field displays the host portion of either the IP address or of the fully-qualified domain name of this entry. You cannot modify this field. If you need to change the name, you must delete the entry from the list, then add the entry back using the new name.
   
   • **Fully-Qualified Domain Name** — This field displays the domain name of the host. You can modify this field by typing in a new value. Be sure to type the fully-qualified domain name of the host.

**Note:** The **Name** field and the **Fully-Qualified Domain Name Entry** field collectively define a PTR Record for the selected reverse lookup zone. The PTR record is used in a Reverse Addresses table and maps an IP address to a host name.
4 [Conditional] If a host in a forward lookup zone is selected, the following fields appear:
   • **Entry Name** — This field defines the host portion of the fully-qualified domain name of this entry.
   • **A Record IP** — This field defines a DNS A record (an Address record), which is used to map host names to IP addresses. In this case the field displays the IP address of the selected host. You can modify this field by typing in a new value. The address you specify must be entered using standard dotted quad notation (for example 172.14.207.27).
   • **CNAME Rec** — This field defines a DNS CNAME record, which is used to map an alias to its canonical name. The field, if populated, displays the name of the Canonical Record of the selected host. You can modify this field by typing in a new name. The name you specify must be entered using the fully qualified primary name of the domain.
   • **TXT Record** — This field allows you to enter comments or additional information about this zone, such as sender id information.
   • **Entry MX Records** — This field is used to specify entries in the Mail Exchangers table for the selected host. The Mail Exchangers table contains DNS MX records that indicate what machines will act as mail routers (mail exchangers) for the selected host.
     • To add an MX Records entry, click **New**. Type a fully qualified host name, and a priority level for this record. Valid values are 1–65535. The lower the value, the higher the priority.
     • To delete an MX Records entry, select the entry and click **Delete**.
   • **HINFO-Type** — This field provides information about a host’s hardware type.
   • **HINFO-OS** — This field provides information about a host’s operating system.

   **Important:** For security reasons, many organizations elect not to use the HINFO fields.

5 Save your changes.
Adding a new forward lookup entry

Use this window to define a new host for a forward lookup zone.

To add a forward lookup entry:

1. In the **Entry Name** field, specify the host portion of the fully-qualified domain name of this entry.
2. In the **A Record IP** field, specify a DNS A record (an Address record), which is used to map host names to IP addresses. The address you specify must be entered using standard dotted quad notation (for example 172.14.207.27). This field and the **CNAME Rec** field are mutually exclusive.
3. In the **CNAME Rec** field, specify a DNS CNAME record, which is used to map an alias to its canonical name. The name you specify must be entered using the fully-qualified primary name of the domain. This field and the **A Record IP** field are mutually exclusive.
4. [Optional] In the **TXT Record** field, enter comments or additional information about this zone, such as sender ID information.
5. [Optional] The **Entry MX Records** field lists entries in the Mail Exchangers table for this host. The Mail Exchangers table contains DNS MX records that indicate what machines will act as mail exchangers for the host.
   - To add an MX Records entry, click **New**. Type a fully qualified host name, and a priority level for this record. Valid values are 1–65535. The lower the value, the higher the priority.
   - To delete an MX Records record entry, select the entry and click **Delete**.
6. [Conditional] The **HINFO-Type** field provides information about a host’s hardware type.
7. [Conditional] The **HINFO-OS** field provides information about a host’s operating system.

**Important:** For security reasons, many organizations elect not to use the HINFO fields.

8. Click **Add** to save the new entry. Click **Close** to exit this window.
Adding a new reverse lookup entry

Use this window to define a new host for a reverse lookup zone. Follow the steps below.

1. In the **Entry Name** field, specify the host portion of the IP address of this entry.

2. In the **Fully-Qualified Name Entry** field, specify the domain name of the host. Be sure to type the fully-qualified domain name of the host.

   **Note:** The Entry Name field and the Fully-Qualified Name Entry field collectively define a PTR Record for the selected reverse lookup zone. The PTR record is used in a Reverse Addresses table and maps an IP address to a host name.

3. Click **Add** to save the new entry. Click **Close** to exit this window.
The Reconfigure DNS window allows you to completely reconfigure DNS on your Sidewinder appliance.

- Make sure you create a configuration backup before reconfiguring DNS.
- After using the DNS configuration utility, reboot the appliance.
- Any active DNS servers on the appliance will be disabled during the reconfiguration process.
- Any prior modifications you have made to your DNS configuration will be lost when you save your changes. You will need to re-apply the modifications.

Reconfiguring transparent DNS

To reconfigure DNS to use transparent services, select Maintenance > Reconfigure DNS. (You can also click the Reconfigure DNS... button on the DNS window.) The following window appears:
To reconfigure your DNS settings to use transparent DNS services:

1. In the **New DNS Configuration** drop-down list, select **Transparent**.

2. To configure the Sidewinder appliance to use the internal name servers:
   a. Select the **Internal Name Server** check box.
   b. In the corresponding **IP Address** field, type the IP address of the name server located in the internal burb.
   c. [Optional] In the **Alternate IP Address** field, type the IP address of an alternate name server.
   d. In the **Burb** drop-down list, select your internal burb.

3. To configure the Sidewinder appliance to use the external (Internet) name servers:
   a. Select the **Internet Name Server** check box.
   b. In the corresponding **IP Address** field, type the IP address of the name server located in the external (Internet) burb (that is, your ISP’s name server).
   c. [Optional] In the **Alternate IP Address** field, type the IP address of an alternate name server.
   d. Save your DNS settings. You will receive a pop-up message informing you whether the reconfiguration was successful.

⚠️ **Important:** The pop-up message that appears may contain additional information or warnings about your Sidewinder configuration. Please read this message carefully before you click **OK**.

4. Reboot the appliance: Select **Maintenance > System Shutdown**.
Reconfiguring single server hosted DNS

To reconfigure DNS to use single server hosted services, select **Maintenance > Reconfigure DNS**. (You can also click the **Reconfigure DNS...** button on the DNS window.) The following window appears:

![Reconfiguring Sidewinder Hosted (single server) DNS window](image)

To reconfigure your DNS settings to use hosted single server DNS services:

1. In the **New DNS Configuration** drop-down list, select **Sidewinder Hosted**.
2. Select the **1 Server** radio button.
3. In the **Domain** field, verify that the correct domain name appears.
4. In the **Authority** field, select one of the following options:
   - **Master** — Select this option if the server you are defining will be a master name server. A master name server contains name and address information for every computer within its zone.
   - **Slave** — Select this option if the server you are defining will be a slave name server. A slave name server is similar to a master name server, except that it does not maintain its own original data. Instead, it transfers data from another name server.
5. [Conditional] If you selected **Slave** in the previous step, type the IP address of the master authority server in the **Master IP** field.
6. Save your DNS settings. You will receive a pop-up message informing you whether the reconfiguration was successful.

**Important:** The pop-up message that appears may contain additional information or warnings about your Sidewinder configuration. Please read this message carefully before you click **OK**.

7. Reboot the appliance: Select **Maintenance > System Shutdown**.
Reconfiguring split server hosted DNS

To reconfigure DNS to use split server hosted services, select Maintenance > Reconfigure DNS. (You can also click the Reconfigure DNS... button on the DNS window.) The following window appears:

![Reconfiguring DNS: Sidewinder Hosted (split server) window]

To reconfigure your DNS settings to use hosted split server DNS services:

1. In the New DNS Configuration drop-down list, select Sidewinder Hosted.
2. Select the 2 Servers radio button.
3. To configure the Unbound server, do the following:
   a. In the Domain field, verify that the correct domain name appears.
   b. In the Authority field, select one of the following options:
      - Master — Select this option if the server you are defining will be a master name server. A master name server contains name and address information for every computer within its zone.
      - Slave — Select this option if the server you are defining will be a slave name server. A slave name server is similar to a master name server, except that it does not maintain its own original data. Instead, it transfers data from another name server.
   c. [Conditional] If you selected Slave in the previous step, type the IP address of the master authority server in the Master IP field.
4 To configure the Internet server, do the following:
   a In the Domain field, verify that the correct domain name appears.
   b In the Authority field, select one of the following options:
      • Master — Select this option if the server you are defining will be a master name server. A master name server contains name and address information for every computer within its zone.
      • Slave — Select this option if the server you are defining will be a slave name server. A slave name server is similar to a master name server, except that it does not maintain its own original data. Instead, it transfers data from another name server.
   c [Conditional] If you selected Slave in the previous step, type the IP address of the master authority server in the Master IP field.
5 Save your changes to reconfigure your DNS settings. You will receive a pop-up message informing you whether the reconfiguration was successful.

**Important:** The pop-up message that appears may contain additional information or warnings about your Sidewinder configuration. Please read this window carefully before you click OK.
If you prefer to edit the DNS configuration files manually, follow these steps.

**Note:** Files with a `u` extension are for the unbound nameserver, and files with an `i` extension are for the Internet nameserver.

**Important:** You should only edit zone files for a master name server. Never edit the slave name server files. The file names shown below are for a master name server.

1. From a console attached to the appliance, log in and enter `srole` to switch to the Admin domain.
   
   The following two steps assume you have zone files named `domain.db` and `reverse.db` in your system. Substitute your file names as required.

2. Open the `/etc/named.db/u/domain.db` and `/etc/named.db/i/domain.db` files in a UNIX text editor and make the necessary changes.

3. Open the `/etc/named.db/u/reverse.db` and `/etc/named.db/i/reverse.db` files in a UNIX text editor and make the necessary changes.

4. Open the `/etc/named.conf.u` and `/etc/named.conf.i` files in a UNIX text editor and make the necessary changes.

   **Note:** If you edit the `/etc/named.conf.*` files to change an existing master zone into a slave zone, you must also manually remove the old zone file in your `/etc/namedb.*` directories.

5. If you have added new files, you must change the files to the correct Type Enforcement types.

   To do this, type the following command and insert the names of the file(s) you edited in steps 2, 3 and 4:
   ```
   chtype DNSx:conf filename
   ```

   - For non-Internet (unbound) burbs, in place of `x` type the identifier `u`.
   - For the Internet burb, in place of `x` type the index number of the Internet burb. (Use the `region show` command to determine the index number.)

6. Increment the serial number after every change to the master files.

7. Enter the following command to restart DNS.
   ```
   cf daemond restart agent=named_unbound
   cf daemond restart agent=named_intenet
   ```

   **Note:** Any files created by named daemons, such as zone backup files or query log files, have types of DNSu:file or DNSx:file.

8. Check `/var/log/daemon.log` for any errors.
DNS message logging

DNS messages, Type Enforcement errors and process limit errors are logged in the following locations on the Sidewinder appliance.

- `/var/log/audit.raw`: Contains information in the Sidewinder audit format.
- `/var/log/daemon.log`: Contains traditional syslog format messages.

You can view the `audit.raw` file using the Audit windows in the Admin Console (See Chapter 12, "Auditing," on page 359 for more information). The `daemon.log` file can be viewed using any text editor. (See Appendix A for more information on using the different text editors.)
In this chapter...

Understanding VPN on Sidewinder appliance ........................................536
Creating VPN definitions ........................................................................555
Configuring the ISAKMP service ..........................................................574
Configuring Certificate Management ..................................................577
Configuring client address pools ..........................................................603
Example VPN Scenarios .......................................................................611
Understanding VPN on Sidewinder appliance

The Sidewinder VPN solution provides secure data transmission through an encryption and decryption process. The Sidewinder appliance uses the Internet Key Exchange (IKE) to support this process. The appliance also supports the use of manually configured encryption keys.

One of the most advanced features of the Sidewinder VPN solution is the fact that VPN has been embedded into the architecture, making it an operating characteristic of the OS. This integration not only lets you apply access rules to VPNs in exactly the same way you do for physically connected networks but also means that you use the Sidewinder VPN solution to coordinate corporate-wide network security policies.

As companies expand to new locations and employees spend more time working out of the office, VPN solutions are becoming more and more important to businesses. Consider the value of encrypting and authenticating data in these situations:

- passing traffic from appliance to appliance between offices located in different cities.
- passing traffic from employees working remotely to your network.
An introduction to IPsec technology

The Internet is a broadcast medium that is used to send information. While information is in transit, anyone can choose to monitor or intercept this information.

Sending information beyond your Sidewinder appliance via the Internet is like sending an unsealed envelope of important information via a courier service: you must trust that the courier will not read or steal the information.

Protecting your information

To address this danger, an organization known as IETF (Internet Engineering Task Force) developed a standard for protecting data on unprotected (or untrusted) networks such as the Internet. The standard has become known as IPsec, meaning Internet-Protocol Security. In brief, IPsec calls for encrypting the data before it leaves the local host, then decrypting it (removing its “cloak” of encryption) when it is received at the destination or remote host. Once it is decrypted, the data assumes its original form and can be read as intended. No matter how long or circuitous its route through the Internet, the data remains private by virtue of its encryption.

What are encryption and authentication?

The two main components of IPsec security are encryption and authentication.

- **Encryption** — Encryption is the means by which plain text is “cloaked.” It ensures that the transmitted data remains private and unreadable until properly decrypted. The Sidewinder appliance uses an encryption key to encipher and decipher each unit of data sent between your site and the “partner” or remote VPN site. (See “About IPsec keys” on page 538.)

- **Authentication** — VPN authentication prevents unauthorized individuals from tampering with the contents of the data being transmitted. It also prevents them from creating messages that claim to come from a particular place but are actually sent from somewhere else (such as the hacker’s home computer). Authentication is accomplished through two methods:
  - Data-integrity checking, which allows the receiver to verify whether the data was modified or corrupted during transmission.
  - Sender identification, which allows the receiver to verify whether the data transmission originated from the source that claims to have sent it.

When used together, encryption and authentication are very much like writing an encoded message, sealing it in an envelope, and then signing your name across the flap. The receiver can first verify that the signature is yours as a means of determining the origin of the message. Next, the receiver can determine if the contents have been viewed or altered by checking that the envelope seal has not been compromised. Once the receiver is assured of the authenticity of the message, they can decode the contents and “trust” that the contents are as intended.
VPN configuration options

VPN involves establishing an association (or a trust relationship) between your Sidewinder appliance and an IPsec-compliant remote appliance, host, or client. (These entities are referred to as “VPN peers.”) Once this trust relationship is defined, data sent between the two peers is encrypted and authenticated before it is transmitted. There are three important concepts that comprise the Sidewinder VPN:

- IPsec keys, which determine how the information is encrypted and decrypted, and may be manually or automatically exchanged.
- certificates, pre-shared passwords, and extended authentication, which authenticate the VPN peer.
- tunnel or transport encapsulation, two methods of how header information is passed.

Understanding the options associated with each concept will assist you greatly in creating your security association. Study the following information to help you determine which VPN configuration best suits your network environment.

About IPsec keys

A key is a number that is used to electronically sign, encrypt and authenticate data when you send it, and decrypt and authenticate your data when it is received. When a VPN is established between two sites, two keys are generated for each remote end: an encryption key and an authentication key.

To prevent these keys from being guessed or calculated by a third party, a key is a large number. Encryption and authentication (or session) keys are unique to each VPN security association you create.

Once generated, these keys are exchanged (either automatically or manually) between the sites, so that each end of the VPN knows the other end’s keys.

To generate key pairs, the appliance gives you two options:

- **Manual key generation** — If the remote site is not Internet Key Exchange (IKE)-compliant, you may want to choose the manual method of key generation. With this method, the appliance provides randomly-generated encryption and authentication keys (or you can create your own) which you must copy and pass to the remote end of the VPN via secure e-mail, diskette, or telephone. Repeat this process each time you generate keys. Manual keys are more labor intensive than automatic keys and rarely used.
• **Automatic key generation using IKE** — If the remote end of your VPN uses the IKE protocol, the appliance can manage the generation of session keys between sites automatically. This process also regularly changes the keys to avoid key-guessing attacks. Automatic keys are very common in today’s network environments.

IKEv1 and IKEv2 are both available options on the Sidewinder appliance. Some issues to note about the two versions:

– IKEv2 is simpler, more robust, and more reliable. However, not many products currently support the newer IKEv2. Check your product documentation.

– IKEv1 is not compatible with IKEv2. Both sides of a VPN connection must use the same version of IKE.

– When using IKEv2, each side of a VPN connection can use a different authentication method. With IKEv1, both sides must agree on an authentication method.

– In IKEv2, extended authentication (XAUTH) can be used as a standalone authentication method. In IKEv1, extended authentication must be used in conjunction with password/certificate authentication.
Authenticating IKE VPNs

If you are using manual key generation, each time you generate session keys you must communicate directly with the other end of the VPN via telephone, diskette, or e-mail. By contacting the remote end of the VPN each time you change session keys, you manually verify that the remote end is actually whom they claim to be.

With automatic key generation, once you gather the initial information for the remote end of the VPN, there is no further direct contact between you and the remote end of the VPN. Session keys are automatically and continually generated and updated based on this initial identifying information. As a result, the Sidewinder appliance requires a way to assure that the machine with which you are negotiating session keys is actually whom they claim to be — a way to authenticate the other end of the VPN. To allow automatic key generation, the appliance offers the following authentication techniques:

• **a pre-shared password** — When you must generate keys, the appliance and the remote end must both use the agreed upon password, defined during the initial configuration of the VPN, to authenticate each peer.

• **a single certificate** — Single certificate authentication requires that the appliance generate a certificate and private key to be kept on the appliance and a certificate and private key to be exported and installed on a client. Each certificate, once installed on its end of a VPN connection, acts as a trust point. A single certificate (also referred to as a “self-signed certificate”) differs from Certificate Authority (CA) based certificates in that no root certificate is necessary.

• **a Certificate Authority policy** — The appliance can be configured to trust certificates from a particular certificate authority (CA). Thus, it will trust any certificate that is signed by a particular CA and meets certain administrator-configured requirements on the identity contained within the certificate. Because of the nature of this type of policy, Secure Computing recommends that only locally administered Certificate Authorities be used in this type of policy. Certificate authorities are described further in “Configuring Certificate Management” on page 577.
Transport mode vs. tunnel mode

There are two methods for encapsulating packets in a VPN connection: transport mode and tunnel mode. The following paragraphs provide a description of each method.

• **Transport mode** — In transport mode, only the data portion of the packet gets encrypted. This means that if a packet is intercepted, a hacker will not be able to read your information, but will be able to determine where it is going and where it has originated. This mode existed before firewalls and was designed for host-to-host communications.

• **Tunnel mode** — In tunnel mode, both the header information and the data is encrypted and a new packet header is attached. The encryption and new packet header act as a secure cloak or “tunnel” for the data inside. If the packet is intercepted, a hacker will not be able to determine any information about the true origin, final destination or data contained within the packet. This mode is designed to address the needs of hosts that exist behind a Sidewinder appliance. Because the packet header is encrypted, private source or destination IP addresses can remain hidden.

Configuring a VPN client

To establish an encrypted session between a laptop or desktop computer with the Sidewinder appliance and gain access to a trusted network, the user needs to install a VPN client. For details on installing and configuring your VPN client, consult your product documentation.

In many cases the VPN client will be SoftRemote®. Secure Computing and SafeNet™ partner to make that VPN client available from Secure Computing. When you order your SoftRemote client software from Secure Computing, you receive a copy of the *VPN Administration Guide* available. This guide is also available at [www.securecomputing.com/goto/manuals](http://www.securecomputing.com/goto/manuals). It provides detailed instructions for implementing a VPN using a Sidewinder appliance and SoftRemote.
**Extended Authentication for VPN**

The Extended Authentication (XAUTH) option provides an additional level of security for remote access VPN clients. In addition to the normal authentication checks inherent during the negotiation process at the start of every VPN association, Extended Authentication goes one step further by requiring the person requesting the VPN connection to validate their identity. The Extended Authentication option is most useful if you have travelling employees that connect remotely to your network using laptop computers. If a laptop computer is stolen, without Extended Authentication it might be possible for an outsider to illegally access your network. This is because the information needed to establish the VPN connection (the self-signed certificate, etc.) is saved within the VPN client software. When Extended Authentication is used, however, a connection will not be established until the user enters an additional piece of authentication information that is not saved on the computer—either a one-time password, passcode, or PIN. This additional level of authentication renders the VPN capabilities of the laptop useless when in the hands of a thief.

Implementing Extended Authentication on the appliance is a simple two step process.

1. Specify the authentication method(s) that are available on your appliance. See “Types of authentication methods” on page 295 for information on supported methods.

   Do this by selecting Policy > Rule Elements > Services, then select isakmp from the list and click Modify. Click Properties and enable the desired methods in the Allowed XAUTH Methods field. See “Configuring the ISAKMP service” on page 574 for details.


**Note:** Extended Authentication must also be enabled on the remote client. See your client software documentation for information on configuring and enabling Extended Authentication.
What type of VPN authentication should I use?

The Sidewinder appliance supports four different VPN authentication methods. The characteristics of a remote VPN peer determine which type of authentication best fits your VPN configuration. Extended authentication may be added to any automated authentication method for increased security.

**Note:** Extended authentication not available for appliance-to-appliance configurations or any configuration that uses a manual key exchange.

### Table 39: VPN authentication options

<table>
<thead>
<tr>
<th>Authentication</th>
<th>Summary</th>
</tr>
</thead>
</table>
| Manual key VPN                     | • Suitable for gateways  
• Authenticates using a manual key exchanged over a telephone or other secure connection - keying information is cumbersome to enter and not changed often, which reduces security  
• Uncommon in today’s networks, but used for resolving interoperability problems with other vendors’ IPsec products  
• Cannot be used for dynamic IP-assigned clients or gateways  
• Each VPN peer requires its own Sidewinder VPN configuration |
| Automatic key shared password VPN  | • Suitable for gateways  
• Suited for clients when paired with a strong extended authentication, such as SafeWord PremierAccess  
• Primary authentication is password sharing with the VPN peer  
• May be used with dynamic IP-assigned clients, but the clients must be configured to use Aggressive Mode. |
| Automatic key single certificate VPN| • Suitable for gateways and clients  
• Authenticates using a self-signed public certificate - each VPN peer must first import the corresponding peer’s certificate  
• Ideally used for a small number of remote peers  
• Used with dynamic IP-assigned clients and gateways  
• Each peer certificate requires its own Sidewinder VPN definition |
| Automatic key certificate authority-based VPN | • Suitable for gateways and clients  
• Authenticates each VPN peer by using a certificate signed by a certificate authority trusted by the other peer  
• Ideally suited for roving client VPN peers (such as those using laptop computers)  
• Used with dynamic IP-assigned clients and gateways  
• Single Sidewinder VPN definition can be used to administer many VPN clients. |
Here are some general guidelines to follow when you are deciding which type of VPN to use:

- If the VPN peer is not a Secure Computing product, and all other types of VPN methods do not work, try the manual key VPN.
- For a small number of VPN peer clients with dynamically assigned IP addresses, the single certificate VPN is a cost-effective solution. A shared password VPN in conjunction with Extended Authentication is also an option.
- If the VPN peer has a static IP address, the pre-shared password VPN is the easiest to configure. Extended Authentication would not be used in a gateway to gateway configuration as there is no one to provide the challenge/response.
- If there is a large number of VPN peer clients with dynamically assigned-IP addresses (such as a traveling sales force), the CA-based VPN is often the easiest to configure and maintain. Another popular option is to use a pre-shared password VPN in conjunction with Extended Authentication.

<table>
<thead>
<tr>
<th>Authentication</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extended authentication (XAUTH)</td>
<td>• Suitable for clients</td>
</tr>
<tr>
<td></td>
<td>• If using IKEv1, both sides of a VPN connection must use the same version of IKE and the same authentication method.</td>
</tr>
<tr>
<td></td>
<td>• If using IKEv2, each side of a VPN connection can use a different authentication method.</td>
</tr>
<tr>
<td></td>
<td>• If using IKEv1, XAUTH can be used in conjunction with Password, Certificate and Certificate Authority, and Single Certificate.</td>
</tr>
<tr>
<td></td>
<td>• If using IKEv2, XAUTH can be used as the sole authentication method.</td>
</tr>
</tbody>
</table>

**General guidelines for selecting a VPN authentication type**

Extended authentication (XAUTH)

- Suitable for clients
- If using IKEv1, both sides of a VPN connection must use the same version of IKE and the same authentication method.
- If using IKEv2, each side of a VPN connection can use a different authentication method.
- If using IKEv1, XAUTH can be used in conjunction with Password, Certificate and Certificate Authority, and Single Certificate.
- If using IKEv2, XAUTH can be used as the sole authentication method.
Using rules to direct VPN traffic

You can use VPN definitions in conjunction with rules to gain more control over your network security policy.

There are several advantages to using rules to filter traffic bound for a VPN, including:

- Filtering of traffic based on protocol and port allows only selected services to be part of the VPN to the remote peer.
- Rule-level auditing of inbound/outbound connections. The VPN audit only indicates when the encrypted connection is established or torn down. The rules can include auditing for each separate connection between a VPN’s protected hosts.
- Applying application-level defenses and inspection of traffic for malicious content. All features of the Sidewinder rules can be used to protect internal resources and monitor what external resources are being used.
- Defining user-level controls, such as per-user authentication, using rules.

You can use virtual burbs and NAT/Redirection to further control VPN traffic.

Understanding virtual burbs

A termination burb is the burb in which VPN traffic transitions between plain-text and encrypted data. You can increase security and control of that transition by using a virtual burb as your termination burb.

A virtual burb is a burb that does not contain a network interface card (NIC). VPNs terminated in a virtual burb require policy rules to take traffic from the virtual burb to and from the internal burb. Using a virtual burb separates VPN traffic from non-VPN traffic, and it allows you to enforce a security policy that applies strictly to your VPN users.

Consider a VPN policy that is implemented without the use of a virtual burb. Not only will VPN traffic mix with non-VPN traffic, but there is no way to enforce a different set of rules for the VPN traffic. This is because proxies and rules are applied on a burb basis, not to specific traffic within a burb. By terminating the VPN in a virtual burb, you effectively isolate the VPN traffic from non-VPN traffic. Plus, you are able to configure a unique set of rules for the virtual burb that allow you to control precisely what your VPN users can or cannot do. Figure 231 illustrates this concept.
Understanding VPN on Sidewinder appliance

**Figure 231: Virtual burb vs. a non-virtual burb VPN implementation**

**VPN without a virtual burb**

- Traffic originating from the remote peer must now traverse a proxy from the virtual burb to the internal burb.
- A separate rule is used for traffic originating from the internal network destined for the remote peer.

Once the traffic is decrypted on the Sidewinder appliance, it must also traverse a proxy configured for traffic from the virtual burb to the internal burb. This allows administrators to have a finer grain of control of the services allowed inbound and outbound from their controlled networks.

You can define up to 63 physical and virtual burbs. For example, if you have two distinct types of VPN definitions and you want to apply a different set of rules to each type, create two virtual burbs, then configure the required proxies and rules for each virtual burb.

One question that might come to mind when using a virtual burb is: “How does VPN traffic get to the virtual burb if it doesn’t have a network card?” All VPN traffic originating from the Internet initially arrives via the network interface card in the Internet burb. A VPN connection, however, can internally route and logically terminate VPN traffic in any burb on the appliance. By defining a VPN connection to terminate the VPN in a virtual burb, the VPN traffic is automatically routed to that virtual burb within the appliance. Thus, the trusted network now recognizes the virtual burb as the source burb for your VPN traffic. From the virtual burb, a proxy and rule are needed to move the traffic to a trusted burb with network access.

See “Creating and using a virtual burb with a VPN” on page 602 for more information.
VPNs with rules using NAT and redirection

How does the Sidewinder appliance know that a packet between two networks is supposed to go from the internal burb to the VPN burb? Understanding how the Sidewinder appliance makes this determination leads to understanding how NAT and redirection can change how the Sidewinder appliance views a packet. When the Sidewinder appliance first receives a packet, it has three pieces of information:

- the source address/port of the packet
- the destination address/port of the packet
- the burb on which the packet was received.

Using this information, the appliance determines the burb to which the packet is destined. The destination burb, as well as the other pieces of packet information, are then used to make a determination on what policy rule applies to this packet.

The Sidewinder appliance determines the packet’s destination burb by consulting the IPsec security policy database (SPD). Each SPD entry contains a local or source network and remote or destination network along with the termination burb associated with that VPN. These parameters are configured in the Admin Console’s VPN Definitions area. The appliance compares the inbound packet’s source and destination against the networks in the SPD and, upon a successful match, returns the termination burb. This termination burb is used as the packet’s destination burb.

If a packet fails to match an SPD entry, the appliance consults the routing table to find a route associated with the destination address of the packet. The Sidewinder appliance then uses the burb associated with the matching route as the destination burb.
Figure 232 illustrates the information the packet provides the proxy. The Sidewinder appliance uses the IPsec policy engine, policy rules, and the existing packet information to route the packet to its intended destination.

**Figure 232:** Information initially provided by the packet

<table>
<thead>
<tr>
<th>source burb: internal to packet</th>
</tr>
</thead>
<tbody>
<tr>
<td>header</td>
</tr>
<tr>
<td>IP</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>TCP</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>additional packet information</td>
</tr>
</tbody>
</table>

As described above, the first action the Sidewinder appliance takes is to determine the intended destination burb for the packet. This is done by querying the IPsec policy table and routing table. For this example, a matching IPsec policy is found, as shown in Figure 233.

**Figure 233:** Matching packet information to determine the destination burb

Based on the local network and remote network, the packet’s destination burb is set to `vpn`.

![VPN Configuration Screenshot](image-url)
When the destination burb is determined, it is used with the source burb and the source and destination addresses to query the policy rules for a match. For this example, a matching Telnet rule is found (see Figure 234).

Source and destination burbs and source and destination addresses match the packet to this policy rule.
If the matching policy rule specifies that it must apply either NAT or redirection, further action is taken by the appliance prior to sending the packet to the intended destination.

First, we examine NAT. For example, suppose the rule has returned a NAT address of 192.168.200.1. The Sidewinder appliance rewrites the original packet so that it looks similar to Figure 235.

![Figure 235: Using NAT to change the source burb and address](image)

Notice the change in the source address and the source burb. The Sidewinder appliance rewrites the source address to match the NAT address returned by the rule query. The source burb has changed due to the appliance creating a new connection in the destination burb used in the original rule query. The result is that the appliance changed the source address and sent the packet into the vpn burb, which is a virtual burb. The kernel then examines the packet to determine which action to take next (for example, encrypt via VPN tunnel, route out via interface, send to proxies, etc.).

While the original packet may have matched the VPN policy in Figure 233, the transformed packet no longer does. Therefore, the packet will not be encrypted via the VPN definition. There is no interface associated with a virtual burb, so the packet cannot be sent directly. It must then be sent up the stack to any potential proxies, where it is likely either NSS will issue a netprobe (if no proxy is listening on the given port in the virtual burb) or a proxy will pick up the connection and go through the process of the policy evaluation, most likely ending up with a deny rule.

How can this situation be avoided for policies that require NAT to mask protected network addresses? The fundamental resolution is that the VPN policy must match the packet both before and after any address translation. This is done by either selecting a NAT address that falls within the range of one of the local networks of the VPN definition (for example, a NAT address of 192.168.100.254 would work in the above example) or by redefining the VPN policy to take into account any NAT translation. In our example, the VPN definition could be changed as shown in Figure 236.
Figure 236: Matching your security policy with your NAT policy

The Local Network includes the policy-specific NAT address.

The Local Network has been redefined to include both the protected subnet for which packets will be received and the specific NAT address associated with the rule.

Important: One of the common and useful features of rules that use NAT is to define a NAT address of localhost (Host) on the rule’s Source/Dest tab. Great care must be taken when using any rules with this NAT setting with VPNs using virtual burbs. The localhost (Host) setting cannot be used for connections where the destination burb is a virtual burb. The localhost (Host) setting is designed to use the interface address associated with the destination burb of a connection as the source address of that connection. In the case where the destination burb is a virtual burb, there can be no translation of localhost because no interface exists in a virtual burb! The result of attempting to apply this type of NAT substitution in a virtual burb will cause the connection to fail to establish. For best results, NAT to a specific IP address.
Next, consider how redirection interacts with proxy connections and VPN definitions. Again, consider the same original packet in Figure 237 and the original policy in Figure 238 (shown previously in Figure 232 and Figure 233).

Assume that the matching policy rule has NAT disabled, but specifies a redirection address of 172.16.222.1. To perform the redirection, the Sidewinder appliance needs to perform two tasks. First, the appliance rewrites the packet's destination address using the redirection address (172.16.222.1 in our example). The transformed packet now appears as shown in Figure 239.
Second, because we changed the destination address of the packet, the appliance needs to recompute the destination burb for the outbound connection. In this case, as with NAT, the packet will no longer match the intended VPN, so the destination burb will not be the virtual VPN burb. Failing to find a matching IPsec policy means that routing is then used to determine the destination burb, based on the destination address. Assuming that a matching route (or default route) exists, the destination burb will be the burb associated with that route. For our example, we assume that the new destination address falls through to the default route, and the default route is out the external burb. It is this burb that the Sidewinder appliance will use to create the outbound connection.

Once again, to remedy this situation and force the transformed packet to match the intended VPN, the VPN definitions and rule-defined address translation must be aligned so that the packet matches the intended VPN both before and after NAT and redirection have been applied. In our example, this means either choosing a redirection address within the existing VPN policy (for example, 172.17.1.1) or changing the VPN policy to include the new redirection address. As with NAT, the specific redirection address has been added to the policy definition in Figure 240 (this time to the remote or destination networks’ definition).

<table>
<thead>
<tr>
<th>source burb: internal to packet</th>
</tr>
</thead>
<tbody>
<tr>
<td>header</td>
</tr>
<tr>
<td>IP source IP: 192.168.100.1</td>
</tr>
<tr>
<td>dest IP: 172.17.222.1</td>
</tr>
<tr>
<td>TCP source port: 34567</td>
</tr>
<tr>
<td>dest port: 23</td>
</tr>
<tr>
<td>additional packet information</td>
</tr>
</tbody>
</table>
The Remote Network includes the policy-specific redirect address.

If a rule specified both NAT and redirection, the VPN policy would have to reflect changes to both local and remote network definitions.
A VPN definition contains all of the elements of a VPN connection. To configure definition settings to suit a specific VPN environment, you will make the following decisions:

- Is the VPN connecting to a single machine or a gateway that provides access for multiple machines?
- How will the Sidewinder appliance and the remote peer authenticate to each other?
- Is the IP address the VPN is connecting to always the same (static) or does it changes (dynamic)?
- Do you want to automatically manage the exchange and use of keys (using IKEv1 or IKEv2), or do you want to enter the session key manually at the remote end?
  - For automatic key exchange, you must decide on the type of authentication (either password or certificate) to be used between the appliance and the remote end.
  - For manual key exchange, you must decide on the type of authentication and encryption used between the appliance and the remote end and exchange these keys and Security Parameters Index (SPI) values with the remote end via a secure method (diskette, encrypted e-mail, or telephone). You are also required to provide the authentication and encryption keys provided by the remote end.

See “To create or modify VPN definitions:” on page 559 for instructions.

When creating a VPN, you might also need to configure other areas of the Sidewinder appliance:

- Configure the ISAKMP service to allow automatic key exchange. See “Configuring the ISAKMP service” on page 574 for details.
- Create an ISAKMP rule to allow traffic to the ISAKMP server. See “Allowing access to the ISAKMP server” on page 576 for details.
- Configure client address pools to simplify VPN client management. See “Configuring client address pools” on page 603 for details.
- Create virtual burbs to separate VPN traffic and enforce VPN-specific policy. See “Understanding virtual burbs” on page 545 for details.
Managing VPN definitions

Use the VPN Definitions window to manage, view, and order the current VPN definitions on the Sidewinder appliance. You can also check the status of VPNs, and create, modify, or delete VPN definitions.

The order of definitions in the VPN Definitions window affects how packets are matched to definitions. The first definition that matches a connection request is used to allow or deny that connection.

For example, the table below shows the first two positions in a list of VPN definitions. If a packet has a source IP address of 10.69.106.5 and a destination IP address of 10.69.104.20, it is matched to the first definition in the list. The search is stopped before the packet is compared to the more precise match in the second definition.

Table 40: VPN definition ordering

<table>
<thead>
<tr>
<th>Position</th>
<th>Local Network</th>
<th>Remote Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10.69.106.0/24</td>
<td>10.69.104.0/24</td>
</tr>
<tr>
<td>2</td>
<td>10.69.106.5/32</td>
<td>10.69.104.20/32</td>
</tr>
</tbody>
</table>

You can also select certain traffic to bypass IPsec policy evaluation and be sent outside the encrypted tunnel. Other security policy rules will apply to this traffic. You select this option on the VPN Definitions: General tab.

Example: Traffic between two networks at two different sites is encrypted, but you want traffic to and from the web server to be sent outside the encrypted tunnel. You would configure a Bypass definition and place it in front of a more general definition in the VPN Definitions list.

The table below shows a VPN Definitions list with a Bypass VPN definition in the first position.

Table 41: Bypass definition in the VPN Definitions list

<table>
<thead>
<tr>
<th>Position</th>
<th>Action</th>
<th>Local Network</th>
<th>Remote Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Bypass</td>
<td>10.69.106.0/24</td>
<td>10.69.104.20/32</td>
</tr>
<tr>
<td>2</td>
<td>IPsec</td>
<td>10.69.106.0/24</td>
<td>10.69.104.0/24</td>
</tr>
</tbody>
</table>

To view and order VPN definitions, select **Network > VPN Configuration > VPN Definitions**. The VPN Definitions window appears.
Use the toolbar to perform the following functions:

**Table 42: VPN toolbar**

<table>
<thead>
<tr>
<th>Icon</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td>Create a VPN definition by clicking <strong>New</strong>. The VPN Properties window appears. Enter distinct information about a VPN definition on the five tabs of the window. See “Creating VPN definitions” on page 555 for details.</td>
</tr>
</tbody>
</table>
| Modify         | Make changes to a VPN definition by selecting it and clicking **Modify**. The VPN Properties window appears. Make your changes in the VPN Properties window.  
**Note:** Read-only administrators can click **View** to view a VPN definition. |
| Delete         | Delete an existing VPN definition by selecting it and clicking **Delete**.                   |
| Duplicate      | Duplicate an existing VPN definition by selecting the original definition and clicking **Duplicate**. The default name of the new item is Copy_of_x, where x is the original definition’s name. |
| Rename         | Rename an existing VPN definition by selecting it and clicking **Rename**. Type the new name in the pop-up window and click **OK**. |
| Enable/Disable | Enable or disable a VPN definition by selecting it and clicking the appropriate icon. A disabled VPN definition is grayed out in the list.  
To select multiple consecutive definitions to enable or disable at one time, select the first definition, then press the **Shift** key while selecting the last definition. To select multiple non-consecutive definitions at one time, press the **Ctrl** key while selecting each desired definition. |

More...
<table>
<thead>
<tr>
<th>Icon</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Move Up/Move Down</td>
<td>Set the matching order of VPN definitions by selecting a definition in the list and clicking the <strong>Move Up</strong> and <strong>Move Down</strong> arrows to place it in the desired position for matching purposes. The first definition that matches a connection request is used to allow or deny that connection.</td>
</tr>
<tr>
<td>Find</td>
<td>Search for specific elements in the list by typing your search criteria in the <strong>Find</strong> field. Objects with matching elements appear in the list.</td>
</tr>
<tr>
<td>VPN Status</td>
<td>Click <strong>VPN Status</strong> to view the status of all configured VPNs in a pop-up window.</td>
</tr>
<tr>
<td></td>
<td>Click <strong>Refresh Now</strong> to update the information.</td>
</tr>
</tbody>
</table>
To create or modify VPN definitions:

Note: You cannot create more than 16,383 VPN definitions.

1. Select Network > VPN Configuration > VPN Definitions. The VPN Definitions window appears.
2. Click New or select an existing definition from the list and click Modify. The VPN Properties window appears.
   The VPN Properties window contains five tabs that are used to enter distinct information about a VPN definition.
3. Enter the necessary information to create a VPN definition.
4. When you are done entering information, save your changes.
5. Click Add to close the VPN Properties window and add the VPN definition to the VPN Definitions list.
6. Use the arrows to place the new definition in the desired position. See “Managing VPN definitions” on page 556 for more information.

The VPN Properties window contains the following tabs:

- **General** — Enter basic information about the VPN definition. See “About the VPN Properties: General tab” on page 560 for details.

- **Remote Authentication** — Define the authentication method that will be used by the remote peer in this VPN definition. You also define the characteristics of the selected authentication method.
  See “About the VPN Properties: Remote Authentication tab” on page 564 for details.

- **Local Authentication** — Define the authentication method that will be used by the appliance in this VPN definition. You also define the characteristics of the selected authentication method.
  See “About the Local Authentication: Password view” on page 567 for details.

- **Crypto** — Define the IPsec cryptographic properties according to the type of key exchange:
  - Automatic key exchange — Define the IPsec cryptographic and hashing algorithms used to in this VPN definition. See “About the VPN Properties: Crypto tab (Automatic key exchange)” on page 571 for details.

- **Advanced** — Define some of the more advanced points of a VPN definition on this tab, including NAT Traversal. Only administrators that are highly schooled in VPN should modify the information on this tab. This information is used only with automatic key exchange.
About the VPN Properties: General tab

Use the General tab to enter basic information about the VPN definition.

![Image: VPN Properties: General tab]

To configure the General tab, follow the steps below.

1. In the **Name** field, type the name of this VPN.
2. In the **Enabled** field, select **Yes** to enable this VPN definition, or select **No** to disable it.
3. From the **Mode** drop-down list, select how the remote end is operating:
   - **Fixed IP** — Select this option if the IP address of the remote end is always the same. You must also provide the IP address of the remote end in the **Remote IP** field.
   - **Dynamic IP Client** — Select this option if the remote end is a device whose IP address is not fixed. Example: A salesperson that gains Internet access from a laptop.
   - **Dynamic IP Restricted Client** — Select this option if the remote end is a device whose IP address is not fixed. The difference from the **Dynamic IP Client** option is that you restrict the range of IP addresses available to the remote end by using either the **Client Address Pool** field or the **Dynamic Virtual Address Range** field. An example is a salesperson that gains Internet access from a laptop.
   - You can use Dynamic IP Client or Dynamic IP Restricted Client only if automatic key management is used.
• **Manually keyed VPN** — Select this option if you want to exchange session keys manually (for example, over the phone). You configure specific properties of the manual key exchange on the Crypto tab. See “About the VPN Properties: Crypto tab (Manual key exchange)” on page 570 for detailed information.

• **Bypass** — Select this option if you want certain traffic to bypass IPsec policy evaluation and be sent outside the encrypted tunnel. Other security policy rules will apply to this traffic. See “Managing VPN definitions” on page 556 for more information.

4 [Conditional] If you want remote peers to make connections using only the IP addresses contained within one of the available client address pools, select a client address pool from the **Client Address Pool** drop-down list. The appliance then selects an IP address from the available pool and assigns it to the client.

• This field is available only if the Mode is **Fixed IP** or **Dynamic IP Restricted Client**.

• See “Configuring client address pools” on page 603 for information on creating a client address pool.

5 If you are using automatic key exchange, select which **IKE Version** to use.

– IKEv2 is simpler, more robust, and more reliable. However, not many products currently support the newer IKEv2. Check your product documentation.

– IKEv1 is not compatible with IKEv2. Both sides of a VPN connection must use the same version of IKE.

– When using IKEv2, each side of a VPN connection can use a different authentication method. With IKEv1, both sides must agree on an authentication method.

– In IKEv2, extended authentication (XAUTH) can be used as a standalone authentication method. In IKEv1, extended authentication must be used in conjunction with password/certificate authentication.

6 From the **Burb** drop-down list, select the burb you want to assign this VPN to. The appliance terminates each VPN in a burb so that access rules can be applied to the VPN.

See “Understanding virtual burbs” on page 545 for information about virtual burbs and VPNs.

7 In the **Encapsulation** field, select one of the following:

• **Tunnel** — The more common form of VPN encapsulation. Both the data and the source and destination IP addresses are encrypted within the encapsulated payload.

• **Transport** — Transport mode encrypts the data but the source and destination IP addresses are not concealed.

See “Transport mode vs. tunnel mode” on page 541 for a more detailed explanation of these terms.
8 In the **Local IP** field, indicate which IP address to use as the local gateway by selecting one of the following:

- **Use Localhost IP** — Select this option to have the appliance assign the IP address. The appliance uses its routing table to automatically determine which interface or alias address is associated with a route to reach the remote gateway.

- **Specify IP** — Select this option to configure a specific IP address. This IP address should be one of the appliance’s interface or alias addresses, and that interface must have a route to reach the remote gateway.

*Note: If configuring a VPN for an HA cluster, be sure to use the localhost option or specify an alias shared by the cluster.*

9 To add or modify a local network address to the **Local Network/IP** list, click **New** or select an address from the list and click **Modify**. The Local Network List window appears:

- a In the **IP Address** field, type the IP address used in this VPN definition.

- b In the **Number of bits in Netmask** field, use the up/down arrows to select the number of bits that are significant in the network mask. The value specified is used to identify the network portion of the IP address.

The **Local Network/IP** list shows the network names or IP addresses the appliance can use in a VPN definition. The addresses in this list and the addresses in the **Remote Network/IP** list together identify allowed and reachable addresses for this VPN tunnel.

10 [Conditional] In the **Remote IP** field, type the IP address of the remote peer. This field is available for **Fixed IP** and **Manually Keyed VPN** mode.

11 [Conditional] You can add or modify an entry in the **Remote Network/IP** list if the Mode is **Fixed IP**, **Manually Keyed VPN**, or **Bypass**: Click **New** or select an address in the list and click **Modify**. The Remote Network List window appears:

- a In the **IP Address** field, type the IP address used in this VPN definition.

- b In the **Number of bits in Netmask** field, use the up/down arrows to select the number of bits that are significant in the network mask. The value specified is used to identify the network portion of the IP address.

The networks configured here represent real networks located behind the remote VPN peer. The addresses in this list and the addresses in the **Local Network/IP** list together identify allowed and reachable addresses for this VPN tunnel.
12 [Conditional] If the Mode is **Dynamic IP Restricted Client**, you can add or modify an entry to the **Dynamic Virtual Address Range** list: click **New** or select an address range and click **Modify**. The Dynamic Virtual Address Range List window appears.

a In the **IP Address** field, type the IP address range a client can use when initiating a VPN connection.

b In the **Number of bits in Netmask** field, use the up/down arrows to select the number of bits that are significant in the network mask. The value specified is used to identify the network portion of the IP address.

- This list defines the range of addresses a client can use when initiating a VPN connection.
- These are the addresses of client machines on their remote networks. They can be internet-routable addresses or virtual addresses.
- With this option the client assigns their own IP address, although the address must be within the approved address range.

13 [Optional] In the **Comments** field, type a short description for this VPN definition.
About the VPN Properties: Remote Authentication tab

Use this tab to define the authentication method that the remote peer will use to authenticate to the Sidewinder appliance in this VPN definition. Authenticating the remote peer prevents access to the VPN from Internet hosts masquerading as the remote peer.

From the Remote Authentication Method drop-down list, select one of the following methods. The settings for the selected authentication method will populate the window.

- **Password** — Select this option if you and the remote end want to use a password to verify the key exchange. The same password must be used on both ends of this connection.
  
  See “About the Remote Authentication: Password view” on page 565 for detailed information.

- **Certificate + Certificate Authority** — Select this option if you want to use one or more trusted CAs and Remote Identities to validate the certificate of the remote end. This method is commonly used by organizations that have many remote users who must access resources behind the appliance.
  
  See “About the Remote Authentication: Certificate + Certificate Authority view” on page 566 for detailed information.

- **Single certificate** — Select this option if you want to validate the remote end using a self-signed certificate generated by the appliance, or using a certificate generated by a CA server. This method is commonly used by organizations that have a small number of people that travel but need secure access to your network.
  

- **[Conditional] XAUTH** — Select this option to verify the person rather than the machine. XAUTH uses the authentication methods configured to authenticate proxy users connecting through the appliance.
  
  Note: XAUTH must be enabled in the ISAKMP service Properties window.

The use of XAUTH is determined by the version of IKE you select:

- **XAUTH + Password/Certificate + Certificate Authority/Single Certificate** — With IKEv1, XAUTH is an added layer of security to be paired with one of the other remote authentication options. These are automatic key exchanges.

- **XAUTH** — With IKEv2, XAUTH is a separate remote authentication method available for selection.
About the Remote Authentication: Password view

Use this view to define the remote peer’s identity and the password that the remote peer uses in this VPN definition to authenticate to the appliance. The appliance must use the same password to authenticate to the remote peer.

**Note:** If you are using IKEv1, Password-based authentication should be used only with fixed IP-configured VPN or with extended authentication.

To define the remote peer’s identity and password:

1. In the Enter Remote Password field, type the password to be used each time automatic key exchange takes place.
2. In the Verify Remote Password field, confirm the password.
3. In the Remote Identity section, select an identity the remote peer will be required to use to authenticate to the Sidewinder appliance. The appliance uses this information to determine the password the remote peer should use.
   - Select Gateway IP Address (not specified) to require the remote peer to use its gateway address as its identity to authenticate to the Sidewinder appliance. This option is strongly recommended.
   - Select Remote One or More Remote IDs From List to require the remote peer to use the configured remote identity.

**Note:** The remote identity is optional for Fixed IP VPN definitions because the Sidewinder appliance can use the IP address to determine who the remote peer is and thus what password the remote peer should be using.

Chapter 19: Virtual Private Networks

Creating VPN definitions

About the Remote Authentication: Certificate + Certificate Authority view

Use this view to define the Certificate and Certificate Authority that the remote peer uses in this VPN definition to authenticate to the appliance.

1 In the Certificate Authorities section, select a Certificate Authority to use for this VPN definition. The remote VPN peer is required to use a certificate that was signed by one of the configured CAs for this VPN definition.

   To add Certificate Authorities to this list:
   a In the Certificate Authorities section, click the Certificate Authorities... button. The Certificate Authorities window appears.
   b Create the new Certificate Authority, then click Close to return to the Remote Authentication: Certificate + Certificate Authority view.

   See “Configuring and displaying CA root certificates” on page 584 for details. You can add several Certificate Authorities to this list.

2 In the Remote Identities section, select a remote identity to use for this VPN definition. This allows the system administrator to further restrict access.

   To create a new remote identity:
   a Click Remote Identities. The Remote Identities window appears.
   b Create the new identity, then click Close to return to the Remote Authentication: Certificate + Certificate Authority view.

   See “Configuring and displaying Remote Identities” on page 587 for details. You can add several remote identities to this list.

About the Remote Authentication: Single Certificate view

Use this view to define the single certificate that the remote peer uses in this VPN definition to authenticate to the appliance.

From the Remote Certificate drop-down list, select the certificate used on the remote end of the VPN. The remote VPN peer will be required to use this certificate to authenticate.

- The values used as the selected remote certificate appear in the field below the drop-down list. This value is filled in automatically using the information from the selected certificate. The field cannot be modified.

- To create or import a certificate for this definition:
  a Click Remote Certs.... The Remote Certificates window appears.
  b Create or import the new certificate, then click Close to return to the Remote Authentication: Single Certificate view.

   See “Configuring and displaying remote certificates” on page 592 and “Importing a remote certificate” on page 599 for details. You can add several remote identities to this list.
About the Remote Authentication: XAUTH view

[Applicable to IKEv2 only] Use this view to define extended authentication (XAUTH) that the remote peer uses in this VPN definition to authenticate to the appliance.

In the list of remote identities, select the identities who will use XAUTH to authenticate to the appliance. A check mark appears next to selected remote identities.

- XAUTH must be enabled in the ISAKMP server before it can be used in a VPN definition. See “Configuring the ISAKMP server” on page 574 for details.
- To create a new remote identity:
  a. Click Remote Identities. The Remote Identities window appears.
  b. Create the new identity, then click Close to return to the Remote Authentication: Certificate + Certificate Authority view.

See “Configuring and displaying Remote Identities” on page 587 for details. You can add several remote identities to this list.

About the Local Authentication: Password view

Use this view to define the password that the appliance uses in this VPN definition to authenticate to the remote peer.

The selections available on the Local Authentication tab are dependent on the version of IKE being used:

- **IKEv1** — The appliance must use the same authentication method as the remote peer. For example, if you select Password on the Remote Authentication tab, Password is automatically selected as the Local Authentication Method, and cannot be changed on the Local Authentication tab.
- **IKEv2** — The appliance can use a different authentication method than the remote peer. For example, if you select Password on the Remote Authentication tab, you can select Certificate on the Local Authentication tab.
To define a password:

1. [IKEv2 definition only] From the Local Authentication Method drop-down list, select **Password**.
   - If you are using IKEv1, this selection matches the remote method by default and cannot be changed in this view.
   - If you are using IKEv2 and you select **Certificate**, see “About the Local Authentication: Certificate view” on page 569 for details.

2. In the Enter Local Password and Verify Local Password fields, type and verify the password the appliance uses to authenticate to the remote peer. If Password is the remote authentication method, these fields are automatically populated with the remote password and cannot be modified here.

3. From the Local Identity Type drop-down list, select the type of identity to use when identifying the appliance to the remote peer:
   - E-Mail
   - Fully Qualified Domain Name
   - IP Address

   **Note:** E-mail addresses are not recommended, as they are rarely used in the context of a security gateway.

4. In the Value field, type the actual value used as the firewall identity. The value must be of the type selected as the Local Identity Type. For example, if you selected **IP Address** in the Local Identity Type drop-down list, you must type an IP address in the Value field.
About the Local Authentication: Certificate view

Use this view to define the certificate that the appliance uses in this VPN definition to authenticate to the remote peer.

The selections available on the Local Authentication tab are dependent on the version of IKE being used:

- **IKEv1** — The appliance must use the same authentication method as the remote peer. For example, if you select Certificate on the Remote Authentication tab, Certificate is automatically selected as the Local Authentication Method, and cannot be changed on the Local Authentication tab.

- **IKEv2** — The appliance can use a different authentication method than the remote peer. For example, if you select Password on the Remote Authentication tab, you can select Certificate on the Local Authentication tab.

To define a certificate:

1. **[IKEv2 definition only]** From the Local Authentication Method drop-down list, select **Certificate**.
   - If you are using IKEv1, this selection matches the remote method by default and cannot be changed in this view.
   - If you are using IKEv2 and you select **Password**, see “About the Local Authentication: Password view” on page 567 for details.

2. From the Local Certificate drop-down list, select the certificate used on the Sidewinder appliance end of the VPN. To create or import a certificate for this definition:
   
   a. Click **Local Certs...**. The Firewall Certificates window appears.
   
   b. Create or import the new certificate, then click **Close** to return to the Local Authentication: Certificate view.

   See “Configuring and displaying remote certificates” on page 592 and “Importing a remote certificate” on page 599 for details. You can add several remote identities to this list.

3. From the Local Identity Type drop-down list, select the type of identity to use when identifying the Sidewinder appliance to the remote peer. Only those identities defined within the selected certificate will be available in this field. Valid options are:
   - Distinguished Name
   - E-Mail
   - Fully Qualified Domain Name
   - IP Address

   The values used as the selected remote certificate appear in the **Value** field. This value is filled in automatically using the information from the selected certificate. The field cannot be modified.
About the VPN Properties: Crypto tab (Manual key exchange)

Use this tab to configure manual authentication for this VPN definition. The appliance generates key values that are shared with the remote peer. The appliance and remote peer must enter the key values exactly to authenticate to each other.

Follow the steps below.

1 In the IPSEC Transformations drop-down list, select the appropriate form of IPsec transformation. The valid options are:
   • Authentication Header (AH) — Provides authentication only.
   • Encapsulating Security Payload (ESP) — Provides encryption only.
   • Separate AH + ESP — Performs separate transformations for authentication and encryption.
   • Combined ESP + AH — Performs a single transformation that provides authentication and encryption.

2 In the Encryption drop-down list, select the type of encryption you and the remote peer have chosen to use. The choices are:

<table>
<thead>
<tr>
<th>Encryption type</th>
<th>Key length</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES256</td>
<td>256-bit</td>
</tr>
<tr>
<td>AES128</td>
<td>128-bit</td>
</tr>
<tr>
<td>CAST128</td>
<td>128-bit</td>
</tr>
<tr>
<td>3DES</td>
<td>168-bit</td>
</tr>
<tr>
<td>DES</td>
<td>56-bit</td>
</tr>
<tr>
<td>Null</td>
<td>0</td>
</tr>
</tbody>
</table>

3 In the Authentication Hash drop-down list, select the type of authentication you and the remote peer have chosen to use. The valid options are:
   • sha1
   • md5
4 Click **Generate Keys** to create keys and SPI index values. Randomly generated keys appear in the key and SPI fields.
   - The key and SPI fields available are dependent on the IPSEC Transformations selection.
   - You can type your own unique key and SPI index, but it is not recommended. Since manually generating random keys is difficult, the appliance provides randomly generated authentication and encryption keys and Security Parameters Index (SPI) value for you and the remote peer to use. It is highly recommended that you use the default keys provided.

**Important:** Once you have chosen the keys, they must be kept a secret. You should only exchange the keys by a secure method, such as diskette, encrypted e-mail (such as PGP), or via the telephone. If attackers learn the key, they can decrypt all of your VPN traffic.

5 Send the generated keys and SPI values to the remote peer via a secure method (diskette, encrypted e-mail, or telephone).

The remote peer must enter the inbound and outbound keys and SPIs in the opposite fields:

<table>
<thead>
<tr>
<th>If the key on the Sidewinder appliance is in this field:</th>
<th>that key is entered on the remote peer in this field:</th>
</tr>
</thead>
<tbody>
<tr>
<td>AH Inbound Key and SPI</td>
<td>AH Outbound Key and SPI</td>
</tr>
<tr>
<td>AH Outbound Key and SPI</td>
<td>AH Inbound Key and SPI</td>
</tr>
<tr>
<td>ESP Inbound Key and SPI</td>
<td>ESP Outbound Key and SPI</td>
</tr>
<tr>
<td>ESP Outbound Key and SPI</td>
<td>ESP Inbound Key and SPI</td>
</tr>
</tbody>
</table>

**About the VPN Properties: Crypto tab (Automatic key exchange)**

Use this tab to define the cryptographic and hashing algorithms that the appliance uses in this VPN definition to secure the traffic to and from the remote peer.

Follow the steps below.

1 In the **IPSEC Encryption Algorithms** pane, select an algorithm from the list of encryption algorithms. You can select multiple algorithms.
   - The Null option contains an encryption header but does not specify an encryption algorithm. It is generally only used during testing.
   - To authenticate only, without performing encryption, clear all encryption algorithms.

2 In the **IPSEC Authentication Algorithms** pane, select an algorithm from the list of authentication algorithms. You can select multiple algorithms.
About the VPN Properties: Advanced tab

The Advanced tab defines more advanced points of a VPN definition.

- As a general rule only administrators that are highly schooled in the nuts and bolts of VPN should modify the information on this tab.
- The information on this tab is used only with automatic key exchange.

The Advanced tab contains the following fields and buttons:

Internet Key Exchange (IKE) data fields

- **IKE V1 Exchange** — [If IKEv1 is the selected mode] Select which mode is used for key exchange:
  - **Main** — Has three exchanges between the initiator and the receiver; slower but secure. May not be used with dynamic IP clients with password authentication.
  - **Aggressive** — Has fewer exchanges between the initiator and the receiver; faster than Main mode, less secure.

- **Hard Limits** — Indicates how often the system must negotiate for new ISAKMP keys and how much ISAKMP traffic this phase can protect. The defaults are 3600 seconds (1 hour) and 0 (no limit to the amount of traffic).

- **Soft Percentage** — Indicates how far in advance of the hard limit to begin negotiating for new keys. This makes sure you have some new keys on hand by the time the hard limit expires.

- **Encryption Algorithms** — Specifies the encryption algorithm to use during Phase 1.

- **Hash Algorithms** — Specifies the hash algorithm to use during Phase 1.

- **PRF Algorithms** — Specifies the PRF algorithm to use during Phase 1 (IKEv2 only).

- **Key Exchange Group** — Indicates the Diffie-Hellman group to use for the derivation of ISAKMP keys.

- **Force XAuth on Rekey** — Select this option to force XAuth to be performed each time the phase 1 session is started or renegotiated.

- **Relax Strict Identity Matching** — Select this option to relax the identity matching restrictions. If you are experiencing issues associated with identity processing with the remote VPN peer, selecting this option can improve interoperability, but decreases security.

- **Enable NAT Traversal** — Allows multiple VPN users behind a NAT device to access a VPN tunnel. A UDP header is added to IPsec traffic and port 500 is changed to port 4500 to allow traffic across a NAT device.
  - Both sides of the VPN tunnel must have NAT Traversal capability.
  - Intended only for Dynamic IP policies.
  - This function works only in Tunnel mode.
• **Enable Initial Contact** — Enable this option to send and receive initial contact notify messages when first connecting with a VPN peer. This causes the peer to reload any previous state and is useful for resynching state after a device reboot.

• **Encrypt Final Aggressive Mode Packet** — For aggressive mode IKEv1 exchanges, this option will cause the appliance to encrypt the final aggressive mode packet in the exchange. You may need to enable this option if you are experiencing interoperability issues with your VPN peer using aggressive mode.

• **Enable Dead Peer Detection** — Enable this option to send and receive messages to a VPN peer at regular intervals to confirm that the peer is available. If a reply is not received for a period of time, the connection with the peer is ended and no traffic is sent to the peer. The VPN connection must be re-established to send traffic to the peer.

**Rekey data fields**

• **Hard Lifetimes** — Indicates how often the system must negotiate for new IPsec keys and how much traffic it can encrypt. The defaults are 700 seconds and 0 (meaning no traffic limit).

• **Soft Percentage** — Indicates how far in advance of the hard limit to begin negotiating for new keys. This makes sure you have some new keys on hand by the time the hard limit expires.

• **Forced Rekey** — Forces the connection to rekey when the limits are reached, even if no traffic has passed through the VPN since the last rekey.

---

**Important:** SCC strongly recommends enabling the **Forced Rekey** option if you are using SafeNet SoftRemote and have XAUTH configured.

---

**Caution:** Do not enable the **Forced Rekey** option if you have One-To-Many or HA/LS configured and are using static IP addresses for your VPNs. Doing so will cause all Sidewinder appliances in the cluster to attempt to instantiate the VPN at the same time, resulting in failure.

---

• **Enable Extended Sequence Numbers** — Selecting this option doubles the IPsec sequence number to a 64-bit number. This option is useful if you expect extremely heavy traffic, ensuring that you can pass traffic over a VPN without running out of sequence numbers.

• **PFS (Perfect Forward Secrecy)** — If this option is enabled, it ensures that the key material associated with each IPsec security association cannot be derived from the key material used to authenticate the remote peer during the ISAKMP negotiation.

• **Oakley Group** — Indicates the Diffie-Hellman group to use for the PFS derivation of IPsec keys. Available only if the PFS option is enabled.
Configuring the ISAKMP service

If you are using automatic key exchange, you will need to do the following before using any automatic key VPNs:

- Configure the ISAKMP (Internet Security Association and Key Management Protocol) server.
- Create a rule allowing access to and from the ISAKMP server.

Configuring the ISAKMP server

The ISAKMP (often pronounced “ice-a-camp”) server is used by the Sidewinder appliance to generate and exchange keys for VPN sessions. The ISAKMP server properties includes audit, negotiation and connection, and extended authentication parameters.

To configure the ISAKMP server:

1. Select **Policy > Rule Elements > Services**.
2. Select **isakmp** and click **Modify**.
3. Click **Properties**. The following window appears.

![Figure 243: The ISAKMP Properties window](image-url)
To configure the ISAKMP properties:

1. In the **Audit Level** field, select the type of audit output for the ISAKMP server.

   Use these levels in most situations:
   - **Error** — Logs only major errors.
   - **Normal** — (Default) This is the most common setting. It outputs major errors and informational messages.
   - **Verbose** — Use this level when initially troubleshooting VPN connectivity problems. This audit output is useful for detecting configuration issues.
   - **Debug** — Logs all errors and informational messages. Also logs debug information.

   **Note:** Only use **Debug** and **Error** if you are an experienced administrator or under guidance from Secure Computing Technical Support. In particular, debug can overflow your audit logs if left on for an extended period of time.

2. In the Advanced ISAKMP Server Options area, click **Properties**. The Advanced ISAKMP Options window appears with the following options:
   - Certificate negotiation — The default is to allow certificate negotiation. If you clear the **Allow certificate negotiation** check box, all certificates used to authenticate remote peers must either be in the local certificate database or be accessible via LDAP.
   - Negotiation properties — Set how long (in seconds) the ISAKMP server will wait for a response to its request to a remote peer before resending the packet, and how many times it will attempt to resend a packet if no response is received.
   - Control how many remote peers can establish a connection to the ISAKMP server at one time — The default is **unlimited**. However, if you have a large number of remote users whose sessions will immediately reconnect after reboot, you may experience connection establishment issues and should adjust this limit.

   Click **OK** to close the Advanced ISAKMP Options window.

3. In the XAUTH (Extended Authentication) Configuration area, configure how the ISAKMP server interacts with extended authentication:
   a. In the **Allowed XAUTH Methods** area, select the authentication method(s) you want to be made available for VPN definitions that use extended authentication. A check mark indicates an allowed authentication method.

   To add an authentication method to the list, click **New** and select a method from the pop-up menu. Configure the authenticator in the New Authenticator pop-up window.

   • See “Extended Authentication for VPN” on page 542 for a detailed description of Extended Authentication.
   • See “Configuring an authenticator” on page 301 for details about configuring an authenticator.
b If two or more authentication methods are selected, specify a default method from the Default XAUTH Method drop-down list. If you do not specify a default method, the first method selected in the list is used.

c Click Properties to open the Advanced XAUTH Options window and configure the following:

- Limit number of active VPNs per user — The default is one active VPN per authenticated user. This limit should work for most security policies. However, if your policy allows multiple users to use the same user name, generally from different VPN clients, you may need to remove this limit. (Secure Computing strongly advises against allowing more than one user per user name.)
- Negotiation properties — Set how long (in seconds) the ISAKMP server will wait for a response to its request to an authenticator before resending the packet, and how many times it will attempt to resend a packet if no response is received.

Click OK to close the Advanced XAUTH Options window.

4 Click OK to return to the main Services window.

5 Save your changes.

The ISAKMP service is now configured.

---

**Allowing access to the ISAKMP server**

A rule using the ISAKMP service is required in order to allow traffic to the ISAKMP server.

Select Policy > Rules, then click New to create a rule for the ISAKMP service. The ISAKMP rule must contain the following values:

- Service — isakmp (ISAKMP Server)
- Source Burb — The burb receiving traffic from the VPN peer(s)
- Source endpoint — <Any> (or addresses of remote VPN peer(s))
- Destination Burb — Match the source burb setting
If you are using automatic key generation and intend to use certificates for authentication, you should configure the certificate and/or Certificate Authority (CA) server information before you set up the VPN. This eliminates the need to configure certificates and CAs during the VPN process. To configure certificate or CA information, follow these general steps.

1. Review the section “Selecting a trusted source” on page 583 for details on certificates and CAs.

2. Decide if you will use a public CA server, your private CA server, or self-signed certificates generated by the appliance (which can be used between two appliances or between an appliance and a VPN client machine).

3. If you are using a public or private CA server, go to “Configuring and displaying CA root certificates” on page 584. You may also want to add remote identities to be used in conjunction with a Certificate Authority policy. See “Configuring and displaying Remote Identities” on page 587.

4. If you are using self-signed certificates, refer to the section titled “Configuring and displaying firewall certificates” on page 589.

5. If you are configuring a VPN between the appliance and a machine running the client version of the Sidewinder VPN solution, and if you are not using a CA, you must create a remote certificate, export it, then import the certificate into the VPN client. Refer to the section titled “Exporting remote or firewall certificates” on page 600.

### Configuring the Certificate server

The Certificate server performs a number of functions, including providing support for the certificate management daemon (CMD) and for an optional external LDAP server. If the LDAP function is configured, it can be used to automatically retrieve certificates and Certificate Revocation Lists (CRLs) from a Version 2 or Version 3 Lightweight Directory Access Protocol (LDAP) server. The appliance will attempt to retrieve any certificates and (optionally) any CRLs that it needs to validate certificates in a CA-based VPN. Note that the LDAP functionality is used only for non-Netscape Certificate Authorities (for example Entrust and etc.).

**Note:** In addition to configuring the Certificate server, a root certificate from the Certificate Authority must be imported into the Certificate Authorities tab for a certificate issued by the CA to validate.
To configure the Certificate server, select **Maintenance > Certificate Management**, then click the **Certificate Server** tab. The following window appears:

**Figure 244:** Certificate Management: Certificate Server tab

Use the Certificate Server tab to configure the Certificate Server.

To configure the Certificate Server tab:

1. To enable the LDAP feature, select the **Use LDAP to search for Certificates and CRLs** check box, and follow the sub-steps below. If enabled, the appliance will attempt to retrieve the certificates and CRLs it needs from an LDAP server.
   a. In the **LDAP Server Address** field, type the IP address of the LDAP server.
   b. In the **LDAP Server Port** field, type the port number on which the LDAP server listens. The port number is typically 389, but the server can be configured to listen on different ports.
   c. In the **LDAP Timeout** field, specify the maximum time (in seconds) that CMD will wait while performing an LDAP search. The valid range is between 0 and 3600 seconds. The recommend value is between 5 and 300 seconds.

2. In the **Maximum Validated Key Cache Size** field, specify the maximum number of validated keys that will be stored in cache memory. Caching validated keys can increase system performance. Valid ranges are 0–500. A value of 0 indicates that no keys will be cached. For most systems, a value of 100 is sufficient.

3. In the **Certificate Key Cache Lifetime** field, specify the maximum amount of time a certificate can remain in the validated key cache before it must be re-validated. The valid range is 0–168 hours (1 week). A value of 0 indicates that the certificate keys must be re-validated with each use.
4 Select the **Perform CRL Checking** check box to enable CRL checking. If this option is disabled, CRL lists will not be consulted when validating certificates.

5 In the **CRL Retrieval Interval for CA’s** drop-down list, specify how often a CA is queried in order to retrieve a new CRL.

6 In the **Audit Level** drop-down list, select the type of auditing that should be performed on this server. The options are:
   - **Error** — Logs only major errors.
   - **Normal** — (Default) This is the most common setting. It outputs major errors and informational messages.
   - **Verbose** — Use this level when initially troubleshooting VPN connectivity problems. This audit output is useful for detecting configuration issues.
   - **Debug** — Logs all errors and informational messages. Also logs debug information.

   **Note:** Only use **Debug** and **Error** if you are an experienced administrator or under guidance from Secure Computing Technical Support. In particular, debug can overflow your audit logs if left on for an extended period of time.

7 Save your changes.
Understanding Distinguished Name syntax

The Certificate Manager supports using distinguished names (DN) for a number of purposes, including identifying the subject of an X.509 certificate. DNs need to be entered using the proper syntax. As defined in the X.500 specifications, a DN is an Abstract Syntax Notation One (ASN.1) value. Within an X.509 certificate, a DN is represented as a binary value. When it is necessary to represent a DN in a human-readable format, as when entering information into the Certificate Manager, the appliance uses the string syntax defined by RFC 2253. This section summarizes the DN string syntax through a series of examples.


A distinguished name (DN) consists of a sequence of *identity components*, each composed of a type tag and a value. The components of a DN are sets of attribute type/value pairs. The *attribute type* indicates the type of the item, and the *attribute value* holds its contents. Each type/value pair consists of an X.500 attribute type and attribute value, separated by an equal sign (=). In the example `CN=Jane Smith`, “CN” is the attribute type and “Jane Smith” is the value.

The attribute type/value pairs are separated by commas (,). This example shows a DN made up of three components:

```
CN=Jane Smith,OU=Sales,O=Secure Computing
```

Plan out your organization’s certificate identification needs before creating any DNs. DNs have a hierarchical structure, reading from most specific to least specific. No preset hierarchy of attribute type exists, but the structure for a given organization needs to be consistent. In this example, the organization Secure Computing has organizational units, making the organizational unit attribute type more specific than the organization attribute type.

```
CN=Jane Smith,OU=Sales,O=Secure Computing
CN=Ira Stewart,OU=Engineering,O=Secure Computing
```

An attribute type is specified by a tag string associated with the X.500 attribute being represented. The Sidewinder appliance supports the attribute tag strings displayed in Table 43, which includes the most common ones recommended by RFC 2253. The tag strings are not case sensitive.
Table 43: Supported X.500 Attribute Type Tags

<table>
<thead>
<tr>
<th>Tag String</th>
<th>X.500 Attribute Name</th>
<th>Character String Type</th>
<th>Max. # of Characters</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>CountryName</td>
<td>PrintableString</td>
<td>2</td>
</tr>
<tr>
<td>CN</td>
<td>CommonName</td>
<td>DirectoryString</td>
<td>64</td>
</tr>
<tr>
<td>Email Address</td>
<td>EmailAddress</td>
<td>IA5String</td>
<td>128</td>
</tr>
<tr>
<td>L</td>
<td>LocalityName</td>
<td>DirectoryString</td>
<td>128</td>
</tr>
<tr>
<td>O</td>
<td>OrganizationName</td>
<td>DirectoryString</td>
<td>64</td>
</tr>
<tr>
<td>OU</td>
<td>OrganizationUnitName</td>
<td>DirectoryString</td>
<td>64</td>
</tr>
<tr>
<td>SN</td>
<td>Surname</td>
<td>DirectoryString</td>
<td>128</td>
</tr>
<tr>
<td>ST</td>
<td>StateName</td>
<td>DirectoryString</td>
<td>128</td>
</tr>
<tr>
<td>Street</td>
<td>StreetAddress</td>
<td>DirectoryString</td>
<td>128</td>
</tr>
<tr>
<td>UID</td>
<td>UserID</td>
<td>DirectoryString</td>
<td>128</td>
</tr>
</tbody>
</table>

The attribute value holds the actual content of the identity information, and is constrained by the associated attribute type. For the supported attribute types, Table 44 shows the corresponding string type (which limits the allowed set of characters) and its maximum length. For example, given “CN=Jane Smith” as a name component, the string “Jane Smith” is of type DirectoryString, and is constrained to a maximum of 64 characters. The maximum number of characters allowed in a DN (that is, the number of characters for all attribute values added together) is 1024.

Table 44 defines the allowed character set for each of the character string types used in Table 43.

Table 44: Character String Types

<table>
<thead>
<tr>
<th>Character String Type</th>
<th>Allowed Characters</th>
</tr>
</thead>
<tbody>
<tr>
<td>DirectoryString</td>
<td>All 8 bit characters without encoding. All non-8 bit characters with UTF-8 encoding.</td>
</tr>
<tr>
<td>PrintableString</td>
<td>A–Z, a–z, 0–9, ()+-/:=? , comma (‘,’), space (‘ ’), apostrophe (‘’).</td>
</tr>
<tr>
<td>IA5String</td>
<td>All 7 bit characters.</td>
</tr>
</tbody>
</table>
When representing attribute values, be careful when using special characters. The following characters have special meaning in the string syntax and must be preceded by a backslash character (\):

- comma (,)
- equal sign (=)
- plus sign (+)
- less than sign (<)
- greater than sign (>)
- pound sign (#)
- semicolon (;)
- backslash (\)
- quotation ("")

All other printable ASCII characters represent themselves. Non-printable ASCII must be have a backslash preceding the ordinal value of the character in two-digit hexadecimal (for example, the BEL character, which has an ordinal value of seven, would be represented by \07). Here are some examples of the escape conventions:

```
CN=Jane Smith\,DDS,OU=Sales,O=Secure Computing
CN=\4a\61\6e\65\20Smith,OU=Sales,O=Secure Computing
```

Attribute values may optionally be contained within double-quote characters, in which case only the backslash (\), double quote ("), and non-printable ASCII characters need to be preceded by a backslash. Here the double-quotes eliminate the need to escape the CN's comma:

```
CN="Jane Smith,DDS",OU=Sales,O=Secure Computing
```

**Note:** Entries containing backslashes or double-quotes will appear “normalized” (without extra characters or spaces) in the GUI once they are saved.

Use this supported syntax when entering information on the Admin Console’s Certificate Manager tabs.

**Note:** For additional information on DN syntax, see RFCs 2044, 2252, 2253, and 2256.
Selecting a trusted source

If you have decided to use certificate authentication, you must choose whether to use a single certificate or Certificate Authority root certificate. In both methods, when a key is generated, the trust point (the appliance or a trusted CA like Netscape, Entrust, etc.) places the key in an electronic envelope called an X.509 certificate. Every certificate contains a collection of information about the entity possessing the private key (the appliance or VPN client). This information may include an identity, a company name, and a residency.

Note: If you select Netscape as a CA server, note that only Netscape version 4.2 is supported at this time.

Single certificate versus Certificate Authority trusted sources

To validate this information, a certificate must be electronically verified and witnessed by a trusted source.

- A CA-based trusted source is best designed for larger deployments and allows for greater flexibility, as both the root (general authoritative certificate from the CA) and personal certificates may be retrieved online. However, a CA configuration does require managing the Certificate Authority server or paying someone else to manage it for you.

- A Sidewinder self-signed trust source is best for very small deployments, as a separate VPN definition must be created for each client. Certificates must be exported from the appliance and then installed on each client.

Public versus private Certificate Authorities

If you are planning to use a specific Certificate Authority to validate certificates created on the appliance, or as part of a group of trusted CAs from which the appliance can directly import certificates, you should set up these CAs before you begin configuring a VPN. You can use the following types of CA servers:

- **Private CA server** — You can purchase and install your own CA server and configure this server as the trusted authority for any VPNs you establish. This is an ideal solution for companies that prefer to allow only VPNs with certificates signed by a CA server on their own protected network.
  
  Note: Before you begin, you must install the CA server and make its URL accessible to the Sidewinder appliance. For details on installing and configuring a private CA server, review the manufacturer’s documentation.

- **Public CA server** — You can choose to accept certificates signed by trusted CAs administered elsewhere. This option allows remote machines to use one certificate for VPNs with more than one corporate partner.
Configuring and displaying CA root certificates

This section explains how to configure the Certificate Authorities tab and display the imported signed root certificate. CAs are used to validate (sign) certificates that are used in a VPN connection.

Select Maintenance > Certificate Management, then click the Certificate Authorities tab. The following window appears:

Use the Certificate Authorities tab to add certificate authorities (CAs) and to view the list of available CAs. CAs are used to validate (sign) certificates that are used in a VPN connection.

To display the properties of a specific certificate, select the certificate from within the Cert Authorities list. Its properties are displayed on the right portion of the window. For a description of these properties, see “About the New Certificate Authority window” on page 585.

From this tab, you can perform the following actions:

- **Add a new certificate to the list** — Click New and make entries in the New Certificate Authority window.
  
  See “About the New Certificate Authority window” on page 585 for details.

- **Delete a certificate from the list** — Select the certificate you want to delete and click Delete.

  *Note:* A Certificate Authority cannot be deleted if it is currently being used by one or more definitions (the Delete button is disabled).
• **Retrieve a certificate** — Click **Get CA Cert** to query the CA and import a certificate for the selected CA. The selected CA must be either Netscape 4.2 or an SCEP (Simple Certificate Enrollment Protocol) CA.

• **Export a certificate** — Click **Export** to export a CA certificate from the local cache to a file and/or a screen.

See “About the Export Certificate window” on page 586 for details.

• **Retrieve a CRL** — Click **Get CRL** to manually retrieve a new Certificate Revocation List (CRL) for this CA.
  - A CRL identifies certificates that have been revoked. CRLs expire on a regular basis, which is why you must periodically obtain a new CRL.
  - You generally only need to manually get a CRL for Netscape CAs when the CA is initially added. After that CRLs are automatically updated every 15 minutes or so for Netscape 4.2 CAs.

  **Note:** If you do not have access to a Netscape CA or if you do have access to an LDAP directory, you should disable the **Perform CRL Checking** button on the Certificate Server window.

---

**About the New Certificate Authority window**

Use the New Certificate Authority window to add a new Certificate Authority to the list of CAs used when authorizing certificates in a Sidewinder VPN connection.

To add a new Certificate Authority:

1. In the **CA Name** field, type a name for this certificate authority. Only alphanumeric characters are accepted in this field.

2. In the **Type** drop-down list, select the type of CA used by your location:
   - **Manual** — Indicates that the necessary files are obtained and loaded by an administrator rather than by a CA.
   - **Netscape 4.2** — Indicates that a Netscape version 4.2 CA is being defined.
   - **SCEP** (Simple Certificate Enrollment Protocol) — Indicates the CA being defined supports this widely used certificate enrollment protocol. The CA can be of any type (Netscape 4.2, Entrust, VeriSign, etc.) as long as it supports SCEP.

3. [Conditional] In the **File** field, type the name and location of the root certificate for the CA, or click **Browse** to browse your network directories for the location of the root certificate. The root certificate is used to verify certificates issued by this CA. (This field is available only if you select **Manual** in the **Type** field.)

  **Note:** Valid file formats are **X.509** and **ASN.1 (.pem or .der)**. For information on obtaining a root certificate, see the documentation that accompanied the CA.
4 [Conditional] In the URL field, type the URL address of the Netscape CA in the URL field. Certificates that need to be signed by the CA are sent to this address. (This field is available only if you select Netscape or SCEP in the Type field.)

5 [Optional] In the CA Id field, type the value used to identify this specific CA. Check with your CA administrator to determine the identifier to use. Many administrators use the fully qualified domain name of the CA as the identifier. (This field is available only if you select SCEP in the Type field.)

6 Click Add to add the CA to the Certificate Authority list.

7 Save your changes.

About the Export Certificate window

Use the Export Certificate window to export the selected certificate from the appliance to a separate file and/or to the screen.

- The certificate can be written to a file on the hard drive of a workstation, or it can be written to a transportable medium such as a diskette.

- You can export just the certificate, or you can export both the certificate and the private key. See your product documentation to determine which you should use.

To export the certificate:

1 Select the Export Certificate (Typical) radio button.

2 Select the export destination:
   • Export Certificate To File — Select this option to export the certificate to a file. Continue with step 3.
   • Export Certificate To Screen — Select this option to export the certificate to the screen.

3 [Conditional] If you are exporting the certificate to file, do the following:
   • In the File field, type the name and location of the file to which the client (or firewall) certificate will be written. If you want to overwrite an existing file, but you are not certain of the path name or the file name, click Browse.
   • In the Format field, select the appropriate format for the file.

4 Click OK to export the certificate to the desired location.

The certificate has now been exported.
Configuring and displaying Remote Identities

Remote Identities can be created for two purposes.

- If you choose to have a Certificate Authority policy defined for a VPN (whereby a group of trusted CAs is authorized to issue certificates for access to the VPN), you will also require a list of Remote Identities. Remote Identities are used as part of a VPN definition to determine which remote certificates from a CA may be used to authenticate to a VPN.

- You may also be required to configure a remote identity to be used in a VPN definition for a software client, such as the SafeNet SoftRemote client, using pre-shared passwords.

Select Maintenance > Certificate Management, then select the Remote Identities tab. The following window appears:

![Remote Identities tab](image)

Use this tab to view and modify the list of available remote identities. Remote identities are used to identify the authorized users who take part in a VPN definition and either have been issued a certificate from a particular CA or use a VPN client configured with a pre-shared password. For example, as part of a remote identity you might define a Distinguished Name that authorizes only people from the Sales department of Bizco corporation.
You can perform the following actions:

- To display the properties of a specific identity, select the identity from within the list. Its properties are displayed on the right portion of the window.
- To modify an identity, make the desired changes and click the **Save** icon. For specific information on modifying the properties that appear for a remote identity, see “About the Create New Remote Identity window” on page 588.
- To create a new remote identity, click **New**. The Create New Remote Identity window appears. See "About the Create New Remote Identity window" on page 588 for details.
- To delete an existing identity, highlight the identity you want to delete and click **Delete**.

### About the Create New Remote Identity window

The Create New Remote Identity window enables you to add a new remote identity. You can also modify an existing remote identity within the Remote Identities tab.

**Tip:** An asterisk can be used as a wildcard when defining the fields on this window. (Other special characters are not allowed.) For example; *, O=bizco, C=us represents all users at Bizco.

To add or modify a remote identity:

1. In the **Identity Name** field, type a name for this Remote Identity.
2. In the **Distinguished Name** field, create a distinguished name. See “Understanding Distinguished Name syntax” on page 580 for information on the format that should be used.
   
   **Note:** The order of the specified distinguished name fields must match the order listed in the certificate.

3. [Optional] In the **E-Mail Address** field, enter the e-mail address(es) to which you want to restrict access. Enter one e-mail address per identity or use a wildcard to indicate all e-mail addresses, such as *@example.com*.
4. [Optional] In the **Domain Name** field, type the specific domain name to which you want to restrict access. Enter one domain name per identity or use a wildcard to indicate all domain names, such as *.example.com*.
5. [Optional] In the **IP Address** field, type the unique IP address or group of IP addresses to which you want to restrict access. For example: 182.19.0.0/16 indicates that only users with IP addresses beginning with 182.19 (as contained in the certificate) will be authorized to use the VPN.
6. Click **Add** to add the identity to the Identities list.
7. Save your changes.
Configuring and displaying firewall certificates

A firewall certificate is used to identify the appliance to a potential peer in a VPN connection. When creating a certificate for the appliance, you have the option to submit the certificate to a CA for validation, or have the appliance generate a self-signed certificate. You should create these certificates before you begin configuring a VPN.

Select **Maintenance > Certificate Management**, then select the **Firewall Certificates** tab. The following window appears:

![Firewall Certificates tab](image)

Use the Firewall Certificates tab to view the list of available certificates. The appliance will use a firewall certificate to identify itself to a peer in a VPN connection. To display the properties of a specific certificate, select the certificate from the list and its properties are displayed on the right portion of the window. For a description of these properties, see “About the Firewall Certificates: Create New Certificate window” on page 590.

*Note:* You cannot modify the properties of a certificate from this window. To modify a certificate, you must delete it and then add it back using the new properties.

From this tab, you can perform the following actions:

- **Create a firewall certificate** — Click **New** to add a certificate to the Certificates list. See “About the Firewall Certificates: Create New Certificate window” on page 590 for details.

- **Delete a firewall certificate** — Select the certificate and click **Delete** to remove the selected certificate from the Certificate list.

*Note:* A certificate cannot be deleted if it is currently used by one or more areas (for example, VPN definitions, Application Defenses, etc.).
- **Import a firewall certificate** — Click Import to import an existing certificate and its related private key file. See “Importing a firewall certificate” on page 598 for more information.

- **Export a firewall certificate** — Click Export to export the selected certificate to a file. The export function is generally used when capturing the certificate information needed by a remote partner such as a VPN client. See “Exporting remote or firewall certificates” on page 600 for more details.

- **Retrieve a certificate** — If a certificate request has been submitted to be signed by a CA, click the Query button to query the CA to see if the certificate is approved. If yes, the Status field will change to SIGNED and the approved certificate will be retrieved.

  If the certificate request is Manual PKCS10, click the Load button to load the signed certificate from a file supplied by the CA.

  **Note:** By default, Netscape CAs and CAs that support the Simple Certificate Enrollment Protocol (SCEP) are checked every 15 minutes for any certificates waiting to be signed.

---

**About the Firewall Certificates: Create New Certificate window**

Use the Create New Firewall Certificate window to add a certificate to the Firewall Certificate list.

**Note:** The default certificate key size is 1024 bits. The default lifetime for self-signed certificates created on the Sidewinder appliance is five years.

---

To add a certificate:

1. In the **Certificate Name** field, type a name for this certificate.

2. In the **Distinguished Name** field, create a distinguished name. See “Understanding Distinguished Name syntax” on page 580 for information on the format that should be used. Note the following:
   - The order of the specified distinguished name fields must match the order listed in the certificate.
   - Some CAs will not support the optional identity types specified in step 3 through step 5.

3. [Optional] In the **E-Mail Address** field, type the email address associated with this firewall certificate.

4. [Optional] In the **Domain Name** field, type the domain name associated with this firewall certificate.

5. [Optional] In the **IP Address** field, type the IP address associated with this firewall certificate.
6 In the **Submit to CA** drop-down list, select the enrollment method to which the certificate will be submitted for signing. The valid options are:

- **Self Signed** — Indicates the new certificate will be signed by the firewall rather than by a CA.
- **Manual PKCS10** — Indicates the certificate enrollment request will be placed in a PKCS10 envelope and exported to the file designated in the **Generated PKCS10 File** field.
- The name of the CA to which the certificate is submitted for signing. The CA can be either private (one you own and manage) or it can be public (a trusted CA administered elsewhere).

7 In the **Signature Type** field, select the encryption format that will be used when signing the certificate. Select the format supported by the remote VPN peer. Valid options are **RSA** or **DSA**.

- RSA is faster at signature verification. It is the most commonly used encryption and authentication algorithm.
- DSA is faster at signature generation. DSA provides only digital signatures.

8 [Conditional] Depending on the method you select in the **Submit to CA** field, the **Other Parameters** area may contain additional fields, as described below:

- If you selected **Manual PKCS10** in the **Submit to CA** field, the **Generated PKCS10 File** field appears. Specify the name and location of the file that will contain the signed certificate, or click **Browse**... to browse the network directories for the location of the file you want to specify. This file contains a PKCS10 “envelope” that is used to send a certificate to a CA for signing.
- If you selected a method that uses SCEP, you will need to provide a password in the **SCEP Password** field that appears.

9 [Conditional] In the **Format** field, select the appropriate format for your PKCS10 certificate request.

10 Click **Add** to add the certificate to the Certificates list.

11 Save your changes.
Configuring and displaying remote certificates

A remote certificate identifies one or more peers that can be involved in a VPN connection with a Sidewinder appliance. The appliance can import existing certificates into its Remote Certificates database, or it can create new remote certificates. In either case, all certificates should be in place before you begin configuring a VPN.

Select **Maintenance > Certificate Management**, then select the **Remote Certificates** tab. The following window appears:

![Remote Certificates tab](image)

Use the Remote Certificates tab to view the list of available remote certificates. These certificates represent the potential peers with which appliance can establish a VPN connection. To display the properties of a specific certificate, select the certificate from within the list. Its properties are displayed on the right portion of the window. For a description of these properties, see “About the Firewall Certificates: Create New Certificate window” on page 590.

**Note:** You cannot modify the properties of a certificate from this window. To modify a certificate you must delete it and then add it back using the new properties.
From this window, you can perform the following actions:

- **Add a new certificate to the Certificate list**—Click **New** and see “About the Remote Certificates: Create New Certificate window” on page 593 for details.
- **Delete a certificate from the list**—Select the certificate you want to delete and click **Delete**.
- **Import certificates**—Click **Import** and see “Importing a remote certificate” on page 599.
- **Export certificates**—Click **Export** and see “Exporting remote or firewall certificates” on page 600.
- **Query the CA for Certificate status**—If a certificate request has been submitted to be signed by a CA, click the **Query** button to query the CA to see if the certificate is approved. If yes, the Status field will change to **SIGNED** and the approved certificate will be retrieved.

If the certificate request is Manual PKCS10, click the **Load** button to query and retrieve the signed certificate.

**Note:** By default, Netscape CAs and CAs that support the Simple Certificate Enrollment Protocol (SCEP) are checked every 15 minutes for any certificates waiting to be signed.

---

**About the Remote Certificates: Create New Certificate window**

The Create New Remote Certificate window enables you to add a certificate to the Remote Certificate list.

**Note:** The default certificate key size is 1024 bits. The default lifetime for self-signed certificates created on the Sidewinder appliance is five years.

To add a remote certificate:

1. In the **Certificate Name** field, type a name for this certificate.
2. In the **Distinguished Name** field, create a distinguished name. See “Understanding Distinguished Name syntax” on page 580 for information on the format that should be used. Note the following:
   - The order of the specified distinguished name fields must match the order listed in the certificate.
   - Some CAs will not support the optional identity types specified in step 3 through step 5.
3. [Optional] In the **E-Mail Address** field, type the email address associated with this remote certificate.
4. [Optional] In the **Domain Name** field, type the domain name associated with this remote certificate.
5  [Optional] In the **IP Address** field, type the IP address associated with this remote certificate.

6  In the **Submit to CA** drop-down list, select the enrollment method to which the certificate will be submitted for signing. The valid options are:

   - **Self Signed**: Indicates the new certificate will be signed by the appliance rather than by a CA.
   - **Manual PKCS10**: Indicates the certificate enrollment request will be placed in a PKCS10 envelope and exported to the file designated in the **Generated PKCS10 File** field.
   - The name of the CA to which the certificate is submitted for signing. The CA can be either private (one you own and manage) or it can be public (a trusted CA administered elsewhere).

   **Note**: The **CA option is only available if a CA is already configured on the Certificate Authorities tab.**

7  In the **Signature Type** box, select the encryption format that will be used when signing the certificate. Valid options are **RSA** or **DSA**.

8  [Conditional] In the **Generated PKCS10 File** field, specify the name and location of the file that will contain the signature request, or click **Browse** to browse the network directories for the file location.

   This file contains a PKCS10 “envelope” that is used to send a certificate to a CA for signing. This field is available only if **Manual PKCS10** is specified in the **Submit to CA** field.

   **Note**: To create a new file using the **Browse** button, enter the name and extension (allowed file formats are binary or .pem).

9  [Conditional] In the **Format** field, select the appropriate format for your PKCS10 certificate request.

10 [Conditional] In the **SCEP Password** field, type a password for this certificate. You will need this password if you ever need the CA to revoke this certificate. The password may not contain spaces or single quotes. This field is available only if the **Submit to CA** field displays a CA of type SCEP.

11 Click **Add** to add the certificate to the Certificates list.

12 Save your changes.
Assigning new certificates for Admin Console services

The default SSL certificates are unique to each Sidewinder appliance. However, if you would like to change your default certificate for any reason, follow the steps in this section.

**Note:** Keep in mind, it is the certificates on the Sidewinder appliance end that you are changing, not on the client end.

Before assigning a new certificate to these services you must first create the new certificates. You should create two new certificates, one for the Admin Console service and one for the synchronization server. You create the certificates from the **Firewall Certificates** tab. Each certificate must be:

- a firewall certificate
- a self-signed certificate
- of type RSA/DSA

See “Configuring and displaying firewall certificates” on page 589 for information on creating a firewall certificate.

To assign a new certificate for the Admin Console or the synchronization server, select **Maintenance > Certificate Management**, then select the **SSL Certificates** tab. The following window appears:

**Figure 249:** SSL Certificates tab

Use this tab to assign a new SSL certificate to the Admin Console service (cobra) and other firewall services.
The SSL Certificate tab allows you to view the proxies to which you can assign new certificates and identifies the name of the certificate currently assigned to each proxy. The certificate will either be 1) the default certificate or 2) a self-signed, RSA/DSA firewall certificate that is defined on the Firewall Certificates tab.

To assign a new certificate to a selected proxy, click **Modify** and select a new certificate to assign to this proxy.

**Note:** You will receive a warning message if you click **Modify** and there is not at least one self-signed RSA/DSA firewall certificate currently defined on the appliance. See “Configuring and displaying firewall certificates” on page 589 for information on defining this type of certificate.

---

**Importing and exporting certificates**

Once the certificates have been generated, they need to be exported and transferred to a VPN client such as SafeNet SoftRemote or to another Sidewinder appliance. Similarly, you may want to import certificates into the appliance originally created on another system. This section walks you through importing and exporting certificates on the appliance.

**Loading manual remote or firewall certificates**

If you chose to create a manual certificate, you must retrieve the certificate after it is signed by the CA; the appliance will not retrieve it automatically. For this process, the **Load** button appears when an unsigned requested certificate name is highlighted. Clicking this button will initiate the process to retrieve and import the certificate. The Load Certificates for PKCS 10 Request window appears. The following window appears:

*Figure 250: Load Certificate for PKCS 10 Request window*

Use the Load Certificate for PKCS 10 Request window to load signed certificates. It also functions to query an LDAP server for whether or not a requested certificate is signed.
To load a signed certificate:

1. In the **Certificate Source** field, select the source location of the certificate. The following options are available:
   - **File**: Indicates you will manually specify the location of the certificate.
   - **LDAP**: Indicates you will access the services of an LDAP (Lightweight Directory Access Protocol) directory to locate the certificate. The LDAP server can be version 2 or version 3.
   - **Pasted PEM Certificate**: Indicates you will paste or type in the certificate from another source, such as another open application window or personal communication.

2. [Conditional] In the **Certificate from File** field, if the certificate source is a file, type the location or **Browse** to the location.

3. [Conditional] In the **Manual (pasted) PEM Certificate** field, if the certificate source is a Pasted PEM Certificate, type or paste the certificate in this field.

4. Click **OK** to issue a query command for your requested certificate, or click **Cancel** to cancel the certificate request.
   - If you click **OK** and the certificate is available, it will automatically be imported and the status will change to SIGNED.

5. Save your changes.
Configuring Certificate Management

Chapter 19: Virtual Private Networks

Importing a firewall certificate

You can import a certificate to the list of firewall certificates defined on the appliance.

To import a firewall certificate, select Maintenance > Certificate Management, then select the Firewall Certificates tab and click Import. The following window appears:

*Note: The displayed fields will vary depending on which import source you select.*

![Firewall Certificate Import Window](image)

Figure 251: Import Firewall Certificate window

To import a certificate:

1. In the Import Source field, select either File or Encrypted File (PKCS12).
   
   *Note: The available fields will vary based on the import source you select.*

   - If you select File, you must identify the file on the Import Certificate From File field.
   - If you select Encrypted File (PKCS12), specify the certificate and key file.

2. In the Certificate Name field, type a local name for the certificate you are importing.

3. In the Import Certificate From File or the Import Certificate/Key field, type the name and location of the certificate file you will import. You may also click Browse to browse the network directories for the location of the file(s) you want to specify.

4. [Conditional] In the Private Key File field, type the name and location of the private key file associated with this certificate, or click Browse to browse the network directories for the location of the file(s) you want to specify. The file can be in either PK1 or PK8 format. (This field is only available if the Import Source field displays File.)

5. [Conditional] In the Password field, enter the password to decrypt the imported file. This password must match the password given when the file was encrypted. (This field is only available if the Import Source field displays Encrypted File(PKCS12).)
Importing a remote certificate

To import a certificate to the list of remote certificates defined on the appliance, select **Maintenance > Certificate Management**, then select the **Remote Certificates** tab and click **Import**. The following window appears:

![Figure 252: Import Remote Certificate window](image)

To import a remote certificate:

1. In the **Import source** field, select the source location of the certificate:
   - **File**: Indicates you will manually specify the location of the certificate file.
   - **Encrypted File**: Indicates you will manually specify the locations of the certificate and private key file.
   - **LDAP**: Indicates that you will access the services of an LDAP (Lightweight Directory Access Protocol) directory to locate the certificate. The LDAP server can be version 2 or version 3.
   - **Paste PEM Certificate**: Indicates you will import the certificate by performing a cut and paste. The Distinguished Name field will change to become the **Manual (pasted) PEM Certificate** field. Paste the certificate into this area.

2. In the **Certificate Name** field, type a local name for the certificate you are importing.

3. [Conditional] In the **Import Certificate From File** field, type the name and location of the certificate file you will import, or click **Browse** to browse the network directories for the location. (This field is available only if the **Import source** field displays **File**.)

4. [Conditional] In the **Password** field, enter the password to decrypt the imported file. This password must match the password given when the file was encrypted. (This field is only available if the **Import Source** field displays **Encrypted File**.)

5. Click **OK** to import the remote certificate.

6. Save your changes.
**Exporting remote or firewall certificates**

You can export certificates from either the Remote Certificates tab or the Firewall Certificates tab. The procedure you use is very simple and is the same from either tab. The reasons you export a certificate from one tab rather than the other, however, are quite different, as described below.

- **Exporting a Remote Certificate** — You are most likely to export a remote certificate if your users use a VPN client to establish a VPN connection between their computers and the appliance. The VPN client requires the use of a certificate to identify itself during the VPN connection negotiations. It is possible to use the appliance to create a self-signed certificate for the VPN client. Once it is created it may be converted to a new file format and then exported. From there it is imported to the VPN client program.

- **Exporting a Firewall Certificate** — This is used to export the firewall certificate to a remote peer. This allows the remote peer to recognize the appliance. On the remote peer the firewall certificate is imported as a remote certificate.

To export a certificate, select **Maintenance > Certificate Management**, then select either the **Remote Certificates** tab or the **Firewall Certificates** tab. Select the certificate you wish to export and click **Export**. The following window appears:

*Note:* The tab you select depends upon your reason for exporting the certificate. See the explanation in the previous paragraphs.

![Export Firewall Certificate window](image)

Use the Export Certificate window to export the selected certificate from the Sidewinder appliance to a separate file and/or to the screen. The certificate can be written to a file on the hard drive of a workstation, or it can be written to a transportable medium such as a diskette. You can export only the certificate, or both the certificate and the private key.
Exporting only the certificate

To export a certificate only:

1. Select the Export Certificate (Typical) radio button.
2. Select the export destination:
   - Export Certificate To File — To export the certificate to a file, select this option and proceed to step 3.
   - Export Certificate To Screen — Select this option to export the certificate to the screen.
3. [Conditional] If you are exporting the certificate to file, do the following:
   - In the File field, type the name and location of the file to which the client (or firewall) certificate will be written. If you want to overwrite an existing file, but you are not certain of the path name or the file name, click Browse.
   - In the Format field, select the appropriate format for the file.
4. Click OK to export the certificate to the desired location.

Exporting both the certificate and private key

To export both a certificate and private key:

1. Specify whether the certificate and private key will be exported as one file or two files by selecting one of the following options:
   - Export Certificate and Private Key as one file (PKCS12) — Select this option to export both the certificate and private key as a single file, and proceed to step 2. (This is the preferred method if you are using SoftRemote.)
   - Export Certificate and Private Key as two files (PKCS1, PKCS8, X.509) — Select this option to export the certificate and private key as two separate files. Proceed to step 3.
2. [Conditional] To export the certificate and private key as a single file, do the following:
   a. In the File field, type the name and location of the file to which the client (or firewall) certificate will be written. If you want to overwrite an existing file but you are not certain of the path name or the file name, click Browse. (The Format displays the file format.)
   b. In the Password field, enter the password that will be used to encrypt the certificate file.
   c. In the Confirm Password field, re-enter the password that you entered in the Password field.
   d. Click OK to export the certificate and private key as a single file.
3  [Conditional] To export the certificate and private key as two separate files, do the following:

a  In the **Certificate File** field, type the name and location of the file to which the client or firewall certificate will be written. If you want to overwrite an existing file but you are not certain of the path name or the file name, click **Browse**. In the **Format** field, select the appropriate format for the file.

b  In the **Private Key File** field, type the name and location of the file to which the key will be written. If you want to overwrite an existing file but you are not certain of the path name or the file name, click **Browse**. In the **Format** field, select the appropriate format for the file.

---

**Important:** If you use a transportable medium to store the private key file (for example .pk1, .pk8, or .pk12), the medium should be destroyed or reformatted after the private key information has been imported to the appropriate VPN client.

---

c  Click **OK** to export the certificate and private key as separate files.

---

### Creating and using a virtual burb with a VPN

This section explains how to create a virtual burb and how to use it in a VPN definition.

1  Create the virtual burb:

   a  Select **Network > Burb Configuration**.

   b  Click **New**.

      •  In the **Burb Name** field, type the name for your virtual burb.

      •  Select the appropriate connection options.

      •  Click **OK**.

2  Save your changes.

3  Configure the rules: Select **Policy > Rules** and define the rules that allow access to and from the virtual burb.

   The virtual burb should be specified as either the source or destination burb, depending on the type of rule being defined.

4  Terminate the desired VPN connection(s) in the virtual burb.

   See “Example VPN Scenarios” on page 611 for information on creating or modifying a VPN definition.
Client address pools are used to simplify the management of VPN clients. They do so by having the Sidewinder appliance manage certain configuration details on behalf of the client. All the client needs is:

- Client software that supports ISAKMP mode-config exchange
- Authorization information (a client certificate, a password, etc.)
- The address of the appliance

Here is how it works: you create a “pool” of IP addresses that will be used by remote peers when they attempt to make a VPN connection. When a client attempts a connection, the appliance assigns it one of the IP addresses available in the address pool. The appliance also negotiates with the client to determine other VPN requirements, such as which DNS and/or WINS servers will be made available to the client. If the negotiation is successful, the client is connected and the VPN connection is established.

Note: Not all VPN client software supports the negotiation of every client address pool parameter. Be sure to verify that your client(s) support the necessary features.

You define the number of IP addresses available in the client address pool. Even though the client may have a fixed IP address, the address used within the VPN definition is the address assigned to it from the address pool. The address pool works for both fixed and dynamic clients. See the following VPN scenarios where address pools could be used:

- “Scenario 2: Simple deployment of remote users” on page 613
- “Scenario 3: Large scale deployment of clients” on page 617

You can also create multiple client address pools. Grouping VPN clients into distinct pools allows you to limit the resources the clients in each group can access.

The following sections explain how to configure client address pools:

- “Configuring a client address pool” on page 604
- “Configuring the Subnets tab” on page 605
- “Configuring the DNS and/or WINS servers” on page 607
- “Configuring the fixed IP map” on page 609
**Configuring a client address pool**

To create or modify a Client Address Pool, select **Network > VPN Configuration > Client Address Pools**. The following window appears.

**Figure 254: Client Address Pools**

You can perform the following actions:

- **Create a new client address pool** — Click **New** in the **Pools** area and enter information in the New Pool window.
- **Delete a client address pool** — Select the pool in the Pools list and click **Delete**.
- **Configure a client address pool** — To configure the Client Address Pools tabs, see the following:
  - For information on configuring the Subnets tab, see “Configuring the Subnets tab” on page 605.
  - For information on configuring the Servers tab, see “Configuring the DNS and/or WINS servers” on page 607.
  - For information on configuring the Fixed IP Map tab, see “Configuring the fixed IP map” on page 609.
Configuring the Subnets tab

Use the Subnets tab to define the virtual address subnet for this address pool. You can also specify any local networks that you want to be accessible to remote clients using this pool.

To configure the virtual subnet address, select Network > VPN Configuration > Client Address Pools and select the client address pool that you want to configure from the Pools list in the left pane. The current configurations of the selected pool appears in the Subnets tab.

Figure 255: Client Address Pools: Subnets tab
To configure the Subnets tab:

1  Configure the **Virtual Subnet List**. This list defines the virtual subnets that define the IP address ranges that are available within this pool.

   **Important:** The virtual subnets should **not** match the internal network’s subnet, as this configuration could cause internal routing and connectivity issues. **Virtual addressing works only if the client address pool uses unassigned address space.**

You can perform the following actions:

- **Create a new virtual subnet** — Click **New** to define a new entry in the Virtual Subnet List.
  - Type the IP address that defines the network portion of the IP addresses used in the client address pool.
  - In the netmask field, specify the number of bits to use in the network mask. The network mask specifies the significant portion of the IP address.

   **Note:** The virtual subnet cannot already exist in the appliance’s routing table.

- **Modify a virtual subnet** — Select an existing subnet entry in the Virtual Subnet List and click **Modify**, then make your changes.

- **Delete a virtual subnet** — Select an existing entry from the Virtual Subnet List and click **Delete**.

2  Configure the **Local Subnet List**. This list defines the local networks available to remote peers that establish a VPN connection using an address from the client address pool. You can perform the following actions:

- **Create a new local subnet** — Click **New** to define a new entry in the Local Subnet List.
  - Type the IP address that defines the network portion of the local network available to remote peers establishing a VPN connection.
  - In the netmask field, specify the number of bits to use in the network mask. The network mask specifies the significant portion of the IP address.

- **Modify a local subnet** — Select an existing subnet entry in the Local Subnet List and click **Modify**, then make your changes.

- **Delete a local subnet** — Select an existing entry from the Local Subnet List and click **Delete**.
Configuring the DNS and/or WINS servers

Use the Servers tab to define the DNS server(s) and/or the WINS server(s) that will be made available to remote peers.

- These servers provide name and address resolution services for devices within the local network.
- The DNS servers you specify can reside on the appliance or be located on another machine in a local or remote network.
- WINS servers are never located on the appliance.

To configure the DNS and/or WINS servers, select Network > VPN Configuration > Client Address Pools and select the client address pool that you want to configure from the Pools list in the left pane. The current configurations of the selected pool appear in the Servers tab.

![Figure 256: Client Address Pools: Servers tab](image)
To configure the Servers tab:

1. The DNS Servers box lists the DNS servers that will be made available to VPN clients that establish a connection using an address from the client address pool. You can perform the following actions:
   - **Create a new DNS server** — Click **New** and type the IP address that specifies the location of the DNS server.
   - **Modify a DNS server** — Select an existing DNS server and click **Modify**, then make your changes.
   - **Delete a DNS server** — Select an existing DNS server and click **Delete**.

2. The NBNS/WINS Servers box lists the NBNS and WINS servers that will be made available to VPN clients that establish a connection using an address from the client address pool. You can perform the following actions:
   - **Create a new NBNS/WINS server** — Click **New** and type the IP address that specifies the location of the NBNS/WINS server.
   - **Modify an NBNS/WINS server** — Select an existing NBNS/WINS server and click **Modify**, then make your changes.
   - **Delete an NBNS/WINS server** — Select an existing NBNS/WINS server and click **Delete**.
Configuring the fixed IP map

Use the Fixed IP Map tab to define fixed addresses for selected clients.

- It enables each of the specified clients to connect to the appliance using its own unique IP address.
- It effectively reserves a specific IP address for a specified client.
- The fixed addresses you specify must be within the range of available IP address as defined by the client address pools.

**Caution:** Do not use network or broadcast addresses when mapping IP addresses to client IDs. These addresses are reserved and are not considered valid values for client address mappings. For example, if your address range is 192.168.105.0/24, then 192.168.105.0 (the network address) and 192.168.105.255 (the broadcast address) should not be used in a fixed IP client mapping. The network address is that address whose unmasked portion is all 0s, and the broadcast address is that address whose unmasked portion is all 1s.

One of the benefits of assigning fixed IP addresses to selected clients is that it allows you to govern what each client can do. For example, you might restrict access to certain clients, and you might grant additional privileges to other clients. You do this by creating a network object for a selected IP address and then using the network object within a rule.

The Fixed IP Map tab contains a **Fixed IP Client Address Mappings** box that lists the current IP address/client mappings. Each unique IP address can appear in the table only once. Multiple identities representing a single client, however, can be mapped to one IP address.

To configure the fixed IP map, select **Network > VPN Configuration > Client Address Pools** and select the client address pool that you want to configure from the Pools list in the left pane. The current configurations of the selected pool appears in the Fixed IP Map tab.
To define a new fixed IP client mapping address:

1. Click **New** to define an associate IP address and client identification strings.

2. In the **IP Address** field, enter the fixed IP address that will be associated with this mapping. The IP address must be within the virtual subnet for this pool.

3. Configure the client identification strings for this entry. All entries listed in the **Client Identification Strings** box will be mapped to the associated IP address. Because a client can use one of several different IDs (a distinguished name, an e-mail address, etc.) when negotiating a session, you can map multiple IDs to one IP address. However, you cannot map two separate clients to the same address.

   Defining all the possible IDs for a client means you will be ready regardless of which ID is presented during the negotiation. Note that if a user will be using extended authentication, their user name will override any other ID.

   Click **New** to add a client identification string. Select a string and click **Modify** to make changes. Select a string and click **Delete** to delete it.

   **Note:** Each client identification string must be entered separately.

4. When you have finished configuring the client identification strings, click **Add** to add the new pool entry to the list.
The following sections describe three typical VPN scenarios. Each scenario begins by describing a particular VPN requirement. It then explains how to implement the solution using the Admin Console. These scenarios assume that the proper rule(s) are defined to allow ISAKMP traffic on the proper burb(s). In the scenarios that follow it is assumed a rule has been defined that allows ISAKMP traffic on the Internet burb.

**Note:** The values used in the following scenarios are for demonstration purposes only.

---

**Scenario 1: Sidewinder-to-Sidewinder VPN via shared password**

The easiest type of VPN definition to configure is one that uses a shared password for authentication. A shared password is typically used to establish a VPN connection between two corporate offices that have static IP addresses. Such a situation occurs if you have a business partner that requires access to your network, or if you have one or more corporate divisions located in different cities.

The following figure provides the sample configuration information used in this scenario.

![Figure 258: VPN between two corporate offices](image)

**The requirements**

This VPN scenario requires the following:

- A VPN connection between two corporate offices
- Shared password authentication
- Static IP addresses for each peer in the VPN definition
How it is done

The following steps show the fields on the VPN menus that must be defined in order to create this VPN definition. The configuration steps are performed on the appliance named \texttt{fw.east.example.com}.

Select \textbf{Network > VPN Configuration > VPN Definitions}, and then click \textbf{New}.

1. On the \textbf{General} tab:
   - \texttt{Name = corporate\_west}
   - \texttt{Enabled = Yes}
   - \texttt{Mode = Fixed IP}
   - \texttt{Client Address Pool = <disabled>}
   - \texttt{IKE Version = V1}
   - \texttt{Burb = Trusted}
   - \texttt{Encapsulation = Tunnel}
   - \texttt{Local IP = localhost}
   - \texttt{Local Network / IP = 250.1.1.0/24}
   - \texttt{Remote IP = 100.1.1.1}
   - \texttt{Remote Network / IP = 50.1.0.0/16}

\texttt{Note: When configuring the appliance named fw.west.example.com, the Local Network/IP and the Remote Network/IP values are reversed and the Remote IP value is 200.1.1.1.}

2. On the \textbf{Remote Authentication} tab:
   - Remote Authentication Method = password
   - Enter Remote Password = \texttt{samplepassword}
   - Verify Remote Password = \texttt{samplepassword}
   - Remote Identity
   - Select gateway IP address

3. On the \textbf{Local Authentication} tab:
   - Local Authentication Method = password (not editable)
   - Enter Local Password = \texttt{samplepassword} (not editable)
   - Verify Local Password = \texttt{samplepassword} (not editable)
   - Local Identity Type = IP Address
   - Value = localhost

4. On the \textbf{Crypto} tab: Select the algorithms to match the other appliance.

5. On the \textbf{Advanced} tab: No changes needed.

6. Click \textbf{Add} to save the new VPN definition.

7. Save your changes.

Summary

The VPN can be used as soon as you configure the other appliance. Enter the same type of information, changing the IP addresses as appropriate.
Scenario 2: Simple deployment of remote users

A common reason for using a VPN is to allow your travelling employees to connect to your corporate network from a remote site. This connection is typically made between an employee’s laptop computer and your corporate Sidewinder appliance. In this type of VPN definition, single (also known as “self-signed”) certificates are generated by the appliance and distributed to each remote peer. This type of VPN can be used with dynamic IP-assigned clients and gateways. One definition must be created for each client, so this type of VPN is typically used only if you have a small number of remote peers.

The figure below provides the sample configuration information used in this scenario. Note that the remote end of this VPN connection (from the appliance point of view) is a laptop that will be using a dynamic IP address.

The assumptions

This VPN scenario assumes the following:
- A VPN connection between a remote computer and the appliance
- A self-signed firewall certificate that is generated by the appliance
- One or more remote certificates that is generated by the appliance and distributed to the remote peers
- One VPN definition per remote peer
- Each VPN definition is terminated in the Virtual burb
- VPN clients should have access to the 250.1.1.0 network but not the 192.168.182.0 network
- All clients make connections using a virtual IP address assigned from a client address pool
- All clients use VPN client software that supports mode-config

Important: When determining your deployment method, consider what steps you will take to ensure the protection of your private key material. Allowing unauthorized access to your private key material could compromise your entire network.
How it is done

The following steps show the fields on the VPN menus that must be defined in order to create this VPN definition. The basic idea is to:

- Create a firewall certificate that identifies the Sidewinder appliance. Export this public certificate to each client.
- Create a remote certificate that uniquely identifies each client. Export each certificate to the respective client.
- Create a client address pool.
- Create a VPN definition for each client.

1. In the Admin Console, select **Maintenance > Certificate Management**, and then enter the following information on each tab:

   a. On the **Firewall Certificates** tab, click **New** and create a firewall certificate by specifying the following:

      - Certificate Name = MyFirewall_cert
      - Distinguished Name: CN=MyFirewall,O=bizco,C=US
      - Submit to CA = Self Signed
      - Signature Type = RSA
      - Click **Add**.
      - Click the **Save** icon.

   b. [Optional] On the **Firewall Certificates** tab, click **Export** and export the firewall certificate by specifying the following:

      - Export Certificate
      - Export Firewall Certificate to File: Click **Browse** and specify where you want to save the firewall certificate. The firewall certificate is often saved to an accessible location (portable storage device or protected network) for distribution to the client.
      - Click **OK**.

   c. On the **Remote Certificates** tab click **New** and create a self-signed certificate for a client by specifying the following:

      - Certificate Name = Sales_A
      - Distinguished Name: CN=Sales_A,O=bizco,C=US
      - Submit to CA = Self Signed
      - Signature Type = RSA
      - Click **Add**.
      - Click the **Save** icon.

   d. Repeat step 1c for each remote peer.
e On the **Remote Certificates** tab, click **Export** and export the remote certificate by specifying the following:

- Select Export Certificate and Private Key.
- Select Export Certificate/Key As One File.
- Export Client Private Key to File: Click **Browse** and specify where you want to save the private key.

**Important:** If you are using SafeNet SoftRemote as your client software, you must export this file using the **PKS12** extension.

- Click **OK**.

f Repeat step 1e for each remote peer. When you are finished you should have the public firewall certificate as well as either the PKCS12-formatted object or the certificate/key file pair for that client saved to a location accessible by the remote peer (portable storage device or network).

2 In the Admin Console, select **Network > VPN Configuration > Client Address Pools**, and then click **New** to create a new client address pool.

Using a client address pool lets you define which local networks the clients can access. For this example, assume you want to permit access to the 250.1.1.0 network but not the 192.168.182 network.

**Note:** Your client software must support this capability. SafeNet SoftRemote currently does not support this capability—it must be manually configured with information about the locally protected subnet.

a **Enter New Pool Name** = SalesPool

b **Virtual Subnet** = 10.1.1.32/27

c Click **New**. In the **Local Subnet** field, enter 250.1.1.0/24 and then click **Add**.

d Click **Add** to add the new pool.

**Note:** The **Subnet and Number of Bits in Netmask** fields work in concert to determine the network portion of the addresses in the pool as well as the total number of addresses in the pool. The values shown here provide 30 possible addresses: 10.1.1.33 - 10.1.1.62. Modify these two values as appropriate for your situation. (For example, in this scenario you might alternatively specify **IP Address** = 10.1.1.16 and **Netmask** = 28, creating 14 possible addresses: 10.1.1.17 - 10.1.1.30.)

e On the **Servers** tab: If the client software you are using supports this mode-config capability, specify your internal DNS and WINS servers here.

f Click **Add**.
3 Select **Network > VPN Configuration > VPN Definitions**, and then click **New** to configure a new definition.

**a** On the **General** tab:
- Name = Sales_A
- Enabled = Yes
- Mode = Dynamic IP Restricted Client
- Client Address Pool = SalesPool
- Burb = Virtual
- Encapsulation = Tunnel
- Local IP = localhost

**b** On the **Remote Authentication** tab:
- Remote authentication method = Single Certificate
- Remote Certificate = Select the certificate you created in step 1C for this client

**c** On the **Local Authentication** tab:
- Local authentication method = Single Certificate (not editable)
- Firewall Certificate = Select the certificate you created in step 1A

**d** On the **Crypto** tab: No changes needed.

**e** On the **Advanced** tab: [Conditional] If the clients are expected to be behind a NAT device, select **Enable NAT Traversal**.

**f** Click **Add** to save the new VPN definition.

**g** Click the **Save** icon to save your changes.

4 Repeat step 3 for each client, changing the name in step 3A and the remote certificate in step 3b as appropriate.

**Summary**

Each individual VPN connection can be used as soon as the remote peers are configured. Each client will need the client-specific certificate and private key information you saved in steps 1B and 1C in order to configure their end of the VPN connection. If you saved this information to diskette you can either hand it to them in person, mail it to them, or perform the imports while the machine is within a trusted network. It is not safe to distribute certificate and private key information via e-mail.

**Note:** The configuration described above restricts VPN traffic by terminating it in a virtual burb. Proxies and rule entries must be configured to specify what access the VPN clients have to the trusted network.
Scenario 3: Large scale deployment of clients

This scenario is similar to Scenario 2 except that instead of a small number of remote peers it assumes you have hundreds or even thousands of remote peers. Because it is unreasonable to create a unique VPN definition for each client, a Certificate Authority (CA) will be used. The CA, in conjunction with the remote identities you define, allows you to create one VPN that is accessible by all of the clients.

The following figure provides the sample configuration information used in this scenario.

![Figure 260: One VPN definition for all clients](image)

**The assumptions**

This VPN scenario assumes the following:

- A VPN connection between a Sidewinder appliance and many clients
- A Certificate Authority-based VPN
- A single VPN definition for all clients with a like security policy rather than one definition per client
- The VPN connection is terminated in a virtual burb
- The clients can have dynamic or static IP addresses
- VPN clients should have access to the 250.1.1.0 network but not the 192.168.182.0 network
- All clients make connections using a virtual IP address assigned from a client address pool
- All clients are using VPN client software that supports mode-config

*Note: It is assumed in this scenario that the clients do not have access to the CA and must rely on the Sidewinder appliance to create and distribute the necessary certificates and private keys.*
How it is done

The following steps show the fields on the VPN menus that must be defined in order to create this VPN definition. The basic idea is to:

- Define the CA used with this VPN
- Create a firewall certificate that is signed by the CA
- Create one or more identities that define who is authorized to use this VPN
- Create a client address pool
- Create the VPN definition
- Create the client certificates for each client
- Provide certificate information and/or files to clients as necessary

**Tip:** Some VPN client software, such as SafeNet SoftRemote, allow users to self-enroll online to obtain their personal certificates, which can greatly reduce administrative effort. See the VPN Admin Guide for more details.

1. In the Admin Console, select **Maintenance > Certificate Management**, and then enter the following information on each tab.

   **a** On the **Certificate Authorities** tab, click **New** and create a CA by specifying the following:
   - CA Name = BizcoCA
   - Type = SCEP (or whatever value is appropriate)
   - URL = http://10.18.128.8
   - Click **Add**.
   - Click the **Save** icon to save your changes.
   - Click **Get CA Cert** (Retrieves the CA Cert from the URL address.)
   - Click **Get CRL** (Retrieves the Certificate Revocation List for this CA.)

   **b** On the **Firewall Certificates** tab, click **New** and create a firewall certificate by specifying the following:
   - Certificate Name = BizcoFW_by_CA
   - Distinguished Name: CN=BizcoFW_by_CA,O=Bizco,C=US
   - Submit to CA = BizcoCA
   - Signature Type = RSA
   - Click **Add**.
   - Click the **Save** icon to save your changes.

   At this point the Status field for this certificate will be **PENDING**. This is because the request has been sent to the CA but the certificate has yet to be created. The status will remain **PENDING** until the CA administrator approves your request.

   - Click **Query**. This queries the CA to see if the certificate is approved. If yes, the Status field will change to **SIGNED** and the certificate is imported.
Chapter 19: Virtual Private Networks

Example VPN Scenarios

Note: The Sidewinder appliance automatically queries the CA every 15 minutes to see if the request has been accepted. If the request has been accepted, the appliance will retrieve the resulting certificate.

c On the Remote Identities tab, click New and create one or more identities that define who is authorized to use this VPN.

• Identity Name = Sales_force
• Distinguished Name: CN=*,OU=sales,O=bizco,C=us
• Click Add.
• Click Close.
• Click the Save icon to save your changes.

2 In the Admin Console, select Network > VPN Configuration > Client Address Pools, and then click New to create a new client address pool.

Using a client address pool lets you define which local networks the clients can access. For this example, assume you want to permit access to the 250.1.1.0 network but not the 192.168.182 network.

Note: Your client software must support this capability. SafeNet SoftRemote currently does not support this capability—it must be manually configured with information about the locally protected subnet.

a Enter New Pool Name = SalesPool

b Virtual Subnet = 10.1.1.0/24

c Click New. In the Local Subnet field, enter 250.1.1.0/24 and then click Add.

d Click Add to add the new pool.

Note: The IP Address and Number of Bits in Netmask fields work in concert to determine the network portion of the addresses in the pool as well as the total number of addresses in the pool. The values shown here provide 254 possible addresses: 10.1.1.0–10.1.1.255. Modify these two values as appropriate for your situation.

If the client software you are using supports this mode-config capability, specify your internal DNS and WINS servers here:

e On the Servers tab:

f Click Add.

g Click the Save icon to save your changes.
3 Select **Network > VPN Configuration > VPN Definitions**, and then click **New** to configure a new definition.

a On the **General** tab:
   - Name = Large_scale_sales
   - Enabled = Yes
   - Mode = Dynamic IP Restricted Client
   - Client Address Pool = VPNPool
   - Burb = Virtual
   - Encapsulation = Tunnel
   - Local IP = localhost

b On the **Remote Authentication** tab:
   - Authentication method = Certificate + Certificate Authority
   - Certificate Authorities = BizcoCA (created in step 1A)
   - Remote Identities = Sales_force (created in step 1C)

c On the **Local Authentication** tab:
   - Authentication method = Certificate (not editable)
   - Firewall Certificate = BizcoFW_by_CA (created in step 1B)

d On the **Crypto** tab: Order the algorithms to match that of the client.

e On the **Advanced** tab: [Conditional] If the clients are expected to be behind a NAT device, select **Enable NAT Traversal**.

f Click **Add** to save the new VPN definition.

g Click the **Save** icon to save your changes.

4 In the Admin Console, **Maintenance > Certificate Management**. On the **Remote Certificates** tab click **New** and create a certificate for a client by specifying the following:

   **Note:** You can skip this step and step 5 for those clients that have online access to the CA. These clients can create and retrieve their own certificates.

   - Certificate Name = Sales_A
   - Distinguished Name: CN=Sales_A,OU=sales,O=bizco,C=US
   - Submit to CA = BizcoCA
   - Signature Type = RSA
   - Private Key: Click **Browse** and specify where you want to save the private key associated with this certificate. In this scenario it is common to save the certificate to the same location as the exported firewall certificate.
   - Certificate: Click **Browse** and specify where you want to save this certificate. In this scenario it is common to save the certificate to the same location as the private key and the exported firewall certificate.
   - Click **Add**.
   - Click the **Save** icon to save your changes.
5 In the Admin Console, **Maintenance > Certificate Management.** Export the CA certificate and the public firewall certificate to the same location used in step 4.

   a On the **Certificate Authorities** tab, select the CA certificate you created in step 1A, then click **Export** and export the certificate by specifying the following:
      • Destination = File
      • Generated CA Certificate File: Click **Browse** and specify where you want to save the CA certificate. Add the .pem extension to the file name.
      • Click **OK**.

   b [Optional] On the **Firewall Certificates** tab, select the firewall certificate you created in step 1B, then click **Export** and export the certificate by specifying the following:
      • Destination = File
      • Export Firewall Certificate to File: Click **Browse** and specify where you want to save the firewall certificate. Add the .pem extension to the file name.
      • Click **OK**.

6 Repeat steps 4 and 5 for each remote peer.

When you are finished your storage location should have four items for each remote peer: the CA certificate, the firewall certificate, the unique private key for the client, and the remote certificate public key for the client.

**Summary**

The Sidewinder appliance is ready to accept connections across this VPN as soon as the remote peers are configured. In order to configure their end of the VPN connection, each client will need the client-specific certificate and private key information you saved in step 4 as well as the firewall and CA certificates created in step 5. If you saved this information to diskette you can either distribute the information in person or mail it to them, or perform the imports while the machine is within a trusted network. It is not safe to distribute certificate and private key information via e-mail.

**Note:** The configuration described above restricts VPN traffic by terminating the VPN connection in a virtual burb. Proxies and rules must be configured to specify what access the VPN clients have to the trusted network.
Chapter 19: Virtual Private Networks

Example VPN Scenarios
In this chapter...

An overview of routing on Sidewinder .................................................................624
Modifying static routes .........................................................................................625
RIP on Sidewinder ..................................................................................................627
Configuring RIP (ripd) ..........................................................................................629
Viewing and comparing ripd configurations .......................................................638
OSPF on Sidewinder ..............................................................................................640
Configuring OSPF (ospfd) ....................................................................................643
Viewing and comparing OSPF configurations .....................................................647
BGP on Sidewinder ..................................................................................................648
Viewing and comparing BGP configurations .......................................................652
PIM-SM on Sidewinder ...........................................................................................654
Configuring PIM-SM (pimd) ..................................................................................655
Viewing PIM-SM configurations ..........................................................................666
Troubleshooting dynamic routing issues ..............................................................667
Traffic between machines on different networks or subnets requires routing. This routing information can be input manually using *static routes*, or learned automatically using *dynamic routing*. Each computer in your network also designates a specific route as its *default route*, to use when the computer cannot find an explicit route to the destination. This default gateway is generally a router which allows access to distant subnets.

The Sidewinder appliance can participate in routing using information from static routes or from dynamic routing, and can act as a default gateway for your network. The default route is set during the Quick Start Wizard. If you need to modify this IP address, you can edit it using the **Routing > Static Routing** area. You can also use the Routing area to manage other static routes for the appliance. See “Modifying static routes” on page 625 for details.

The appliance supports three dynamic routing protocols:

- Routing Information Protocol (RIP)
- the Open Shortest Path First (OSPF) protocol
- the Border Gateway Protocol (BGP)

This chapter provides a brief overview of how each protocol works, and guidelines and scenarios for configuring the dynamic routing protocols and servers on the Sidewinder appliance. The Sidewinder implementation of these protocols and their respective servers (ripd, ospfd, and bgpd) are based on the Quagga implementation. Any administrator planning on configuring RIP, OSPF, or BGP on a Sidewinder appliance is strongly encouraged to use the online help that is available when connected to a Sidewinder-hosted routing server using a command line interface, and the Quagga documentation available at [http://quagga.net/docs/quagga-0.98.pdf](http://quagga.net/docs/quagga-0.98.pdf).
Modifying static routes

However, if your network configuration should change, you may find it necessary to change this static route. To change a static route, select **Network > Routing > Static Routing**. The Static Routing window appears.

![Static Routing window](image)

Use the Static Routing window to view a static route definition table that lists all of the route definitions. To modify the currently defined static routes, follow the procedures below.

*Note:* *Interface routes cannot be modified or deleted.*
Modifying the default route

To change the IP address of the router that is used as your default route, type the new address in the Default Route field and save your changes.

**Note:** If your appliance is defined with two DNS servers, the IP address for the default route must be an address on the external burb.

Modifying other static routes

1. Determine if you want to create, modify, or delete a route:
   - To create a new static route, click New. The Static Route window appears.
   - To modify an existing static route, select the route you want to modify and click Modify. The Static Route window appears.
   - To delete an existing static route, select the route you want to delete, click Delete, and then save your changes. When you click this button, the system checks for any sessions that are currently using the address that you want to delete. If the address is in use, you will not be allowed to delete the entry.

2. In the Entry Type field, select the type of route: Net or Host.

3. [Conditional] If you selected Net, do the following:
   a. In the Net Address field, type the subnet address for this route.
   b. In the Gateway field, type the gateway address the route will use.
   c. In the Net Mask field, type the network mask that will be used for this route.

4. [Conditional] If you selected Host, do the following:
   a. In the Host Address field, type the subnet address for this route.
   b. In the Gateway field, type the gateway address the route will use.

5. Click Add to add the information you entered to the static route definition table.

6. Save your changes.

Saving your changes writes all non-interface routes to /etc/gateways and updates the system’s network routing table.
The Routing Information Protocol (RIP) passes dynamic routing information to be used by routers and servers performing routing functions. A router passing RIP traffic can be configured to receive routing information, install routes in its local routing table, and advertise routing information. A router uses this information to determine the shortest available path between networks. By default, routing information is exchanged every 30 seconds and when a router receives updates.

ripd operates by listening for UDP broadcasts on port 520. It sets a timer to send a RIP packet advertising its routing information every 30 seconds. When a RIP broadcast is received, the ripd server updates the local routing table with any new routes. When the 30 second timer expires, the ripd server reads and updates its local routing table, and then advertises its local routing information

Unlike other dynamic routing protocols on Sidewinder, which automatically broadcast routing information to all burbs, ripd is enabled on a burb-by-burb basis and can be enabled on multiple burbs. However, ripd support in clusters is limited to High Availability clusters in a primary/standby configuration.

The following sections contain scenarios that explain the general concept of RIP processing, some considerations when using RIP on a single burb, and some considerations when using RIP on multiple burbs.

For information on configuration RIP processing, see “Configuring RIP (ripd)” on page 629.

**Security Alert:** In general, dynamic routing is less secure than static routing. If your network requires dynamic routing using RIP, Secure Computing recommends using RIP v2, which is more secure than RIP v1 and also offers authentication. By default, Sidewinder ripd uses v2 without authentication. See the Quagga documentation for enabling authentication.
**A general overview of RIP processing**

This example describes how RIP processing aids in routing IP packets through a network that has a redundant routing architecture. Figure 262 illustrates this redundant architecture.

In this example, the Telnet server has a static route to router A, and the Telnet client has a static route to router B. The Telnet client has two different possible paths of reaching the server: (1) via B to A, and (2) via D to C to A. The routing table on router B has two possible routes to the Bizco network: one with a hop count equal to two (through router A), and the other with a hop count to three (through router D). All routers are using RIP to advertise, create, and receive routing information from the other routers.

Typically, when the Telnet client needs to connect to the Telnet server, it sends a connection request to router B (the client’s default route). B then forwards the request to router A, because that is the shortest route (two hops verses three hops). Router A then forwards the request to the Telnet server in the Bizco network, which uses the same route to respond to the request.

The dynamic routing capability of RIP can be seen when the link between router A and router B is lost. As soon as B notices that it is no longer receiving RIP updates from A, it updates its local routing table hop count for that route to 16 (route unreachable) and broadcasts this to others on its local network (this is to notify router D).

Next, the Telnet client sends another packet to the server via router A, unaware that the route between A and B has been lost. Router B looks at its local routing table and discovers there are two routes: one is unreachable and the other goes through router D. Because D is on the same network as the client, router B sends an ICMP Redirect back at the client stating that it can reach the Telnet server network through router D. The client updates its local routing table to point that host at router D. The client then re-sends its last packet to router D. Router D receives the packet and forwards it on to router C, which forwards it on to router A, etc. The session continues on through router D without interruption. When the link between A and B is re-established, the Telnet client will receive an ICMP Redirect from router D pointing it back at router A. The session will again continue without interruption.
Configuring RIP (ripd)

RIP processing is done via a Sidewinder server process called **ripd**. To implement RIP processing, a ripd server process must be configured and there must be an active rule that allows RIP broadcasts; ripd is then enabled in that rule’s source burb. RIP packets are UDP datagrams with destination port 520. For RIP version 1, the destination address is a limited broadcast address: 255.255.255.255. For RIP version 2, all the routers multicast the address 224.0.0.2. Each burb will have no more than a single ripd instance to handle the network traffic for all interfaces assigned to the burb.

These are the high level steps to set up RIP on the Sidewinder appliance.

1. Sketch a diagram showing your planned Sidewinder configuration (similar to the diagrams in “RIP on Sidewinder” on page 627). Include the following items on your diagram:
   - configuration of the routers to which the appliance connects
   - RIP areas in the network(s)
   - the Sidewinder interfaces (burbs)

2. Define one or more netgroups for the routers to which the appliance connects. See “Creating network objects” on page 272.

3. Configure one or more rules for the RIP traffic. See “Creating a rule for ripd” on page 630.

4. Configure the appropriate RIP parameters. See “RIP processing options” on page 632.

See the following sections for details on these high level steps.
About basic ripd configuration

Using RIP in your network is a two-step process: First you must create a rule that allows ripd to pass traffic. Then you must configure ripd with the appropriate network information and processing options.

Creating a rule for ripd

To pass RIP traffic, the appliance needs a rule with the Service field set to ripd. The source and destination burbs must be the same, and should be set to the burb on which you intend to receive RIP packets. The source endpoint represents who you want to accept RIP traffic from, such as a single router or a netgroup of routers and/or hosts. The destination endpoint will usually be set to Any, since the destination is the broadcast address that corresponds to the source and destination burb.

Using ripd in an enabled rule automatically enables the ripd server in the rule’s source burb. (You cannot access the ripd configuration files using the CLI until this rule is created and enabled.) You can disable the server by disabling or deleting all rules that use ripd as a service, and by disabling the ripd server in its configuration file.

To create a ripd rule:

1 Select Policy > Rules.
2 Click New Rule.
3 Enter a name and description that quickly identified this as the rule that provides access to the ripd server.
4 In the Service field, select ripd.
5 Set the Source Burb and the Destination Burb fields to the same burb. This enables ripd in that burb.

Note: You can enable ripd in multiple burbs. There is one configuration file per burb, and each file must be edited separately.

6 Configure the other Source and Destination fields as necessary to enforce your RIP security policy.
7 Save your changes.

For the appliance to pass RIP traffic, you now need to configure the ripd configuration file with the settings appropriate for your security policy. See the following section for the preferred method for enabling and disabling the ripd server.
Configuring basic ripd processing

There are several ways to configure ripd on the Sidewinder appliance. They are:

- Using Telnet to connect to the ripd server on the appliance.
- Using the Admin Console File Editor to edit the ripd configuration file.
- Using a different file editor, such as vi, to edit the ripd configuration file.

Because the CLI method provides ripd help and validates commands as they are entered, the following sections focus on this method. The same commands and functionality described here are valid when using the other methods, but require different formatting. Be sure that you are familiar with ripd formatting conventions before using those methods.

For additional documentation on RIP processing, see the official Quagga web site at www.quagga.net.

To enable basic ripd processing using a CLI:

1. Using a command line session, log into the appliance and switch to the Admn domain by entering:
   
   srole

2. Telnet into the Sidewinder ripd server on localhost by entering:

   telnet localhost_ n ripd

   where \( n \) = the burb index of the burb used as the source burb in the enabled ripd rule.

   **Tip:** Use cf burb query to look up a burb’s index. It is also listed on the Network > Burb Configuration window as the ID.

   A password prompt appears.

3. Enter zebra.
   
   A ripd> prompt appears.

4. Enable the full command set by entering:

   ripd>en

   The prompt changes to ripd# to indicate that the full command set is enabled.

5. Enable configuration mode by entering:

   (config)#conf t

   The prompt changes to ripd(conf)# to indicate that configuration mode is enabled.
6 Enable ripd and configure it to advertise routes, receive updates, and install routes in the local routing table by entering the following commands:

```
(config)#router rip
(config-router)#network X.X.X.X/mask
```

where X.X.X.X/mask is the subnet and network mask of the interface on which you are enabling RIP. You can enter multiple network statements.

7 [Optional] To make changes persistent across reboots, write the changes to the configuration file by entering:

```
(config)#write
```

Ripd is now enabled and is sending, receiving, and creating routing information. See the following section for information on other configuration options.

To disable ripd, follow step 1 through step 5 in the previous procedure, and then enter:

```
(config)#no router rip
```

Ripd is now disabled and will not participating in routing.

---

**RIP processing options**

The following is a list of common RIP configurations and the commands to implement these configurations. Only administrators who are experienced with routing in general, and RIP dynamic routing in particular, should configure ripd.

These commands are presented as they are entered at a command line interface. They also assume that you have entered the appropriate network statements when you first accessed the ripd server. Another option is to configure these options by using the Admin Console File Editor or other file editor to edit the configuration file directly. If you chose to modify the file directly, pay close attention to formatting. See the Quagga documentation at www.quagga.net for formatting assistance.

**Important:** Use the ripd online help, available when using the CLI, for details on modifying the commands given here as well as other supported configurations. To access the ripd online help, enter a mode (such as `router rip` or `route-map`) and then enter `?` or `list`. You must be currently running a mode to see its documentation.
• **Receive and create routes, but do not advertise routes**

This configuration enables RIP on all interfaces that are on the specified subnet. In this option, ripd receives updates and creates routes in the local routing table, but does not advertise routes.

Use these commands to configure this option:

```
(config)#router rip
(config-router)#passive-interface if_name
```

where `if_name` is the interface name of the burb that is to learn routes, but does not advertise routes. Use `default` instead of an interface name to set this configuration on all interfaces.

• **Advertise routing information, but do not receive or create routes**

This configuration enables ripd to send RIP updates that advertise local routing information available within the current burb. RIP ignores received updates and does not create routes in the local routing table.

Use these command to configure this option:

```
(config)#ip prefix-list name seq n deny x.x.x.x/mask
(config)#router rip
(config-router)#distribute-list prefix name in|out
```

where:

- `name` is the name of the prefix-list
- `n` indicates the order of the prefix-list. Sequences numbers are generally multiples of 5.
- `x.x.x.x/mask` is the IP address and netmask that identified the route. To include all routes, use `any`.
- use `in` to filter routes received by this burb and `out` to filter routes sent by this burb.

For example, you would create an `ip prefix-list` named `none` with a `seq 5` that denies all routes. The second command uses `distribute-list` to filter out all received (inbound) updates.

• **Advertise as the default route**

This configuration enables ripd to advertise the default route prefix.

Use this command to configure this option:

```
(config)#router rip
(config-router)#default-information originate
```
• **Advertise routes from other burbs**
  This option is used when ripd is enabled in multiple burbs. It specifies which additional burbs are to have their routing information included in RIP updates sent by the current burb. The additional burbs are identified by their interface names. ripd uses route information statements to learn RIP routes between burbs. The route-maps match only the interfaces within the burb that created the routes. Additional filtering by ip-address or nexthop is also possible.

  Uses these commands to configure this option:

  (config)#route-map name permit|deny n
  (config-route-map)#match interface if_name
  (config-route-map)#exit
  (config)#router rip
  (config-router)#redistribute rip route-map name

  where
  – name is the name of the route-map
  – use permit to allow this route-map and deny to deny it
  – n indicates the order of the route-map. Sequence numbers are generally multiples of 5.
  – if_name is the interface name for the burb that is receiving the routing information.

  For example, you would edit the internal burb configuration file to take routes that are learned in the external burb and advertise them out the internal burb by configuring the ripd internal configuration route-map to specify the external burb interface. This assures that only RIP routes from the external burb interface are redistributed.

• **Filter specific routes from other burbs**
  This option is used when ripd is enabled in multiple burbs. Instead of allowing all routing information to pass from one burb to another, it creates a filter that only allows routing information for one subnet in a burb, which automatically denies the other subnet(s) in that burb.

  Uses these commands to configure this option:

  (config)#access-list name permit|deny x.x.x.x/netmask
  (config)#router rip
  (config-router)#distribute-list name in/out

  where:
  – name is the name of the access-list
  – use permit to allow this access-list and deny to deny it
  – x.x.x.x/netmask is the IP address and netmask that identified the route.
    To include all routes, use any. To filter routes received by this burb, use in. To filter routes sent by this burb, use out.

  This example is represented in “Enabling RIP processing on multiple Sidewinder burbs” on page 636.
Enabling ripd on a single Sidewinder burb

A simple implementation of RIP on the Sidewinder appliance is to enable ripd in a single burb. This configuration is useful when the appliance has a burb that is connected to a network with a redundant routing topology and the appliance needs to participate in that routing infrastructure, but does not need to share that information with other burbs.

In this scenario, the company security policy calls for ripd to participate in dynamic routing internally without sharing routing information with any other burbs. To achieve this goal, an administrator enables ripd on the internal burb. If any of the internal routers (B, C, or D) becomes unreachable, ripd receives this information, updates its routing table accordingly, and then advertises the change. For example, if the Telnet client was using router B and it goes down, the client's host machine gets an update for the Sidewinder ripd and reroutes its request through router C and D. When router B is available, the client's host machine receives that update and begins using router B again. On the external burb, the appliance maintains a static route with router A.

To implement this policy, the administrator configures the following ripd options on the internal burb:

- Advertise routing information to the internal burb
- Distribute a default route
- Receive routing information from other routers on the internal burb
- Does not send or receive information from any other burbs

The configuration file for this policy would be similar to the following:

```
!ripd.conf.internal for internal burb
router rip
    network 10.10.2.0/24
    default-information originate
```
Enabling RIP processing on multiple Sidewinder burbs

**Important:** Because of Type Enforcement, no ripd server is allowed to update the local route table in a different burb.

Using ripd in multiple Sidewinder burbs involves more options than using it in a single burb. You can make decisions about what information to share and what information to filter out.

In this scenario, the company security policy calls for using RIP to pass limited routing information between the internal burb and the DMZ. The administrator must configure the ripd servers to pass routing information between the DMZ and the subnet containing the company’s SQL servers, but filter out the routing information for the subnet hosting the employees’ workstations.

To implement this policy, the administrator configures the DMZ burb to receive all information from the internal burb, but only advertise the SQL subnet information.

The configuration file for the DMZ burb would be similar to the following:

```plaintext
!ripd.conf.dmz for DMZ burb
router rip
    network 196.168.25.0/24
    redistribute rip route-map internal
    distribute-list prefix sql out

! ip prefix-list sql seq 5 permit 176.16.25.0/24
! route-map internal permit 10
    match interface em1
```
The administrator then configures these options on the *internal* burb:

- Advertise routing information to the internal burb
- Distribute a default route to the internal burb
- Receive routing information from other routers on the internal burb
- Only advertises routing information for the 172.16 subnet to the DMZ burb

The configuration file for this policy would be similar to the following:

```
!ripd.conf.internal for internal burb
router rip
    network 10.10.2.0/24
    redistribute rip route-map dmz
    default-information originate
    route-map dmz permit 5
        match interface em2
```
The Admin Console provides tools to help you manage your RIP configuration. You can use these tools to quickly view the entire configuration file, compare different states of the configuration file, or list items such as the RIP neighbors and routes. You can also use the RIP area to edit the configuration file using the File Editor and to manually overwrite the configuration to be used the next time the ripd restarts.

To use these tools, select **Network > Routing > Dynamic Routing > RIP** or **Policy > Rule Elements > Services > ripd**. The following window appears:

![Image of the RIP configuration comparison window](image)

Use this window to view and compare versions of the configuration file. The different versions are:

- **Starting configuration** — This is the version that is used when ripd server restarts. The following events update this version:
  - An administrator makes changes using the CLI and saves the changes using the `write` command.
  - An administrator uses the Admin Console File Editor to save the configuration file or uses the **Overwrite** button.
  - An administrator saves changes using a file editor, such as vi, and then restarts ospfd.

- **Running configuration** — This is the version currently being used by the appliance. This may differ from the configuration file and the starting configuration if an administrator logs into the server using the CLI and makes changes, but does not issue the `write` command.
• **Configuration file** — This is the most recent saved configuration. If an administrator makes changes using a non-Admin Console file editor but does not restart ripd, this version will be different from starting configuration file.

On this window, you can do the following:

• **Determine which configuration file to view and edit.** Each burb has a separate configuration file. Select a burb from the Burb drop-down list to determine which configuration file to manage.

  *Note:* In addition to editing a burb’s ripd configuration file, you must use the burb as a source burb in a ripd rule before it will pass RIP traffic. See “Creating a rule for ripd” on page 630.

• **Edit a configuration file.** Click Edit to open the selected burb’s configuration file using the Admin Console File Editor. Edit the file as needed and then save your changes. The appliance automatically restarts the ripd server. See “Configuring RIP (ripd)” on page 629 for more information.

• **View and compare files.** Select an option from the list and then click Retrieve. A pop-up window appears displaying the requested information. Close this pop-up to return to the main RIP window.

• **Save the running configuration to the configuration file.** Click Overwrite to save the running configuration. The running configuration and the starting configuration are now the same.
The Open Shortest Path First (OSPF) protocol passes link-state information about the internal routers in a given network. All routers communicating using OSPF use an algorithm to calculate the shortest path among the routers. On the Sidewinder appliance, OSPF processing is done via a Sidewinder server process called `ospfd`. To implement OSPF processing, an `ospfd` server process must be configured and there must be an active rule that allows OSPF broadcasts. Unlike ripd which is burb-specific, ospfd automatically advertises its routing information to all burbs on the appliance. OSPF runs as its own protocol (protocol 89) at the IP layer. OSPF uses 224.0.0.5 and 224.0.0.6 as broadcast addresses.

OSPF multicasts information frequently. When a host detects a change to a routing table or a change in the network topology, it immediately multicasts the information to all other hosts in the network. Unlike the RIP in which the entire routing table is sent, the host using OSPF sends only the part that has changed. With RIP, the routing table is sent to neighboring hosts every 30 seconds. OSPF multicasts updated information only when a change occurs.

Rather than counting the number of hops, OSPF bases its path descriptions on link states that factor in additional network information. Also, OSPF lets you assign cost metrics to a given host router so that some paths are given preference.

There are three phases to the OSPF protocol:

1. Routers discover neighboring OSPF routers by exchanging Hello messages. The Hello messages also determine which routers are to act as the Designated Router (DR) and Backup Designated Router (BDR). These messages are exchanged periodically to ensure connectivity between neighbors still exists.

2. Routers exchange their link state databases. Link state means the information about a system's interfaces, such as its IP address, network mask, the cost for using that interface, and whether it is up or down.

3. The routers exchange additional information via a number of different type of Link State Advertisements (LSAs). These supply the information needed to calculate routes. Some reasons for generating LSAs are interfaces going up or down, distant routes changing, static routes being added or deleted, etc.
At this point, all routers should have a full database. Each database contains consistent (not identical) information about the network. Based upon this information, routes are calculated via the “Dijkstra” algorithm. This algorithm generates the set of shortest routes needed to traverse the network. These routes are then enabled for use by IP.

All OSPF routers on a network do not exchange OSPF data — this limits network overhead. Instead, they communicate with the DR (and BDR), which are then responsible for updating all other routers on the network. Election of the DR is based upon the priority of that router. OSPF multicasts using the AllSPFRouters (224.0.0.5) and AllDRouters (224.0.0.6) addresses. The DR and the BDR receive packets on the second address.

**Important:** Since the Sidewinder appliance performs many other functions, Secure Computing recommends that customers should not configure the Sidewinder appliance to become DR (or BDR) unless forced to by network topology.

OSPF is considered an Interior Gateway Protocol (IGP). An IGP limits the exchange of routes to a domain of control, known as an Autonomous System (AS). An AS is a large network created under a central authority running a consistent routing policy that includes different routing protocols, such as the networks commonly run by ISPs. RIP V1 and V2 are also IGPs.

Routers on the edge of the AS generate special LSAs (AS-External-LSAs) for the rest of the AS. There is also an address-forwarding mechanism that allows an OSPF router to obtain a route from a specified location. This feature allows a customer to introduce static routes for their network from a central router.

Autonomous Systems can be large. It is not necessary for the whole AS to know everything about all routes. Each AS may be broken down into areas. All routing information must be identical within an area. Routing between areas goes through a backbone. All routers on a backbone have to be able to communicate with each other. Since they belong to the same area (area 0 of a particular AS), they also all have to agree. Area Border Routers (ABRs) have one interface defined to run in the backbone area. Other interfaces can then be defined to run in a different area.
The following figure is a sample configuration of OSPF areas. Figure 267 shows a large internal network and backbone terminating at a router.

Figure 267: OSPF areas

For additional documentation on OSPF processing, see the official Quagga web site at www.quagga.net.

**Tip:** You should use OSPF only if you have identified that your routing topology is too complicated to use only static routing or the Routing Information Protocol (RIP). OSPF is a complex IP routing protocol and deploying OSPF should involve discussions between routing subject matter experts and security subject matter experts.

To implement OSPF processing on the Sidewinder appliance, you must create an enabled rule with ospfd selected in the Service field and the Source and Destination Burbs set to Any. You can control which routers ospfd can communicate with by managing the source and destination endpoints in the ospfd rule. Each burb will have no more than a single ospfd instance to handle the network traffic for all interfaces assigned to the burb.

The Sidewinder appliance currently runs version 0.98.6 of ospfd. This is the most stable version of ospfd available from Quagga. The OSPF implementation on the Sidewinder appliance supports all of the standards specified in RFC 2328.
Configuring OSPF (ospfd)

See the following section for information on configuring OSPF processing.

These are the high level steps to set up OSPF on the Sidewinder appliance.

1 Sketch a diagram showing your planned Sidewinder configuration (similar to the diagrams in “RIP on Sidewinder” on page 627). Include the following items on your diagram:
   • configuration of the routers to which the appliance connects
   • OSPF areas in the network(s)
   • the Sidewinder interfaces (burbs)

2 Define one or more netgroups for the routers to which the appliance connects. See “Creating network objects” on page 272.

3 Configure one or more rules for the OSPF traffic. See “Creating a rule for ospfd” on page 643.

4 Configure the appropriate OSPF parameters. See “OSPF processing options” on page 645.

About basic ospfd configuration

Using OSPF in your network is a two-step process: First you must create a rule that allows ospfd traffic. Then you must configure ospfd with the appropriate network information and processing options.

Creating a rule for ospfd

To enable access to the ospfd configuration file:

1 Select Policy > Rules.
2 Click New Rule.
3 Enter a name and description that quickly identified this as the rule that provides access to the ospfd server.
4 In the Service field, select ospfd.
5 Set both the Source Burb and the Destination Burb fields to Any.
6 Configure the other Source and Destination fields as necessary to enforce your OSPF security policy.
7 Save your changes.

For the appliance to pass OSPF traffic, you now need to configure the ospfd configuration file with the settings appropriate for your security policy. See the following section for the preferred method for enabling and disabling the ospfd server.
Configuring basic ospfd processing

There are several ways to configure ospfd on the Sidewinder appliance. They are:

- Telneting into the ospfd server on the appliance and using a command line interface (CLI).
- Using the Admin Console File Editor to edit the ospfd configuration file.
- Using a different file editor, such as vi, to edit the ospfd configuration file.

Because the CLI method provides ospfd help and validates commands as they are entered, the following sections focus on this method. The same commands and functionality described here are valid when using the other methods, but require different formatting. Be sure that you are familiar with ospfd formatting conventions before using those methods.

For additional documentation on OSPF processing, see the official Quagga web site at www.quagga.net.

To enable basic ospfd processing using a CLI:

1. Using a command line session, log into the appliance and switch to the Admn domain by entering:
   ```
   srole
   ```
2. Telnet into the Sidewinder ospfd server by entering:
   ```
   telnet localhost ospfd
   ```
   A password prompt appears.
3. Enter `zebra`.
   A `ospfd>` prompt appears.
4. Enable the full command set by entering:
   ```
   ospfd>en
   ```
   The prompt changes to `ospfd#` to indicate that the full command set is enabled.
5. Enable configuration mode by entering:
   ```
   (config)#conf t
   ```
   The prompt changes to `ospfd(conf)#` to indicate that configuration mode is enabled.
6 Enable ospfd and configure it to advertise routes, receive updates, and install routes in the local routing table by entering the following commands:

   (config)#router ospf
   (config-router)#network X.X.X.X/mask area n.n.n.n

where

   • X.X.X.X/mask is the subnet and network mask of the interface on which you are enabling OSPF. You can enter multiple network statements.
   • n.n.n.n is the area within the AS, such as 0.0.0.0 for the backbone area.

7 [Optional] To make changes persistent across reboots, write the changes to the configuration file by entering:

   (config)#write

ospfd is now enabled and is advertising, receiving, and creating routing information. See the following section for information on other configuration options.

To disable ospfd, follow step 1 through step 5 in the previous procedure, and then enter:

   (config)#no router ospf

ospfd is now disabled and will not participating in routing.

OSPF processing options

As with RIP, only administrators who are experienced with routing in general, and OSPF dynamic routing in particular, should configure ospfd.

These commands are presented as they are entered at a command line interface. They also assume that you have entered the appropriate network and area statements when you first accessed the ospfd server. Another option is to configure these options by using the Admin Console File Editor or other file editor to edit the configuration file directly. If you chose to modify the file directly, pay close attention to formatting. See the Quagga documentation at www.quagga.net for formatting assistance.

Important: Use the ospfd online help, available when using the CLI, for details on modifying the commands given here as well as other supported configurations. To access the ospfd online help, enter a mode (such as router ospf or route-map) and then enter ? or list. You must be currently running a mode to see its documentation.
In general, the OSPF configuration options are similar to the RIP configuration options, particularly the route-map, prefix-list, and redistribution commands. See “RIP processing options” on page 632 for details. However, the servers’ implementation differences of the `passive-interface` command is worth noting.

For both servers, the passive-interface command enables the routing protocol on all interfaces that are on the specified subnet. For ripd, the server receives updates and creates routes in the local routing table, but does not advertise routes. For ospfd, the server passively advertises the local interface information, but does not form adjacency with other routers over the specified interface.

For OSPF, use these commands to configure this option:

```
(config)#router ospf
(config-router)#passive-interface if_name
```

where `if_name` is the interface name of the burb that is to learn routes, but does not send HELLOs to other routers. Use `default` to set this configuration on all interfaces.
Viewing and comparing OSPF configurations

The Admin Console provides tools to help you manage your OSPF configuration. You can use these tools to quickly view the entire configuration file, compare different states of the configuration file, or list items such as the OSPF neighbors and routes. You can also use the OSPF area to edit the configuration file using the File Editor and to overwrite the configuration to be used the next time the ospfd restarts.

To use these tools, select Network > Routing > Dynamic Routing > OSPF or Policy > Rule Elements > Services > ospfd. The following window appears:

![Configuration file: Edit]

The OSPF service will be automatically restarted when the configuration file is saved.

Use this window to view and compare versions of the configuration file. The different versions are:

- **Starting configuration** — This is the version that is used when ospfd server restarts. The following events update this version:
  - An administrator makes changes using the CLI and saves the changes using the `write` command.
  - An administrator uses the Admin Console File Editor to save the configuration file or uses the `Overwrite` button.
  - An administrator saves changes using a file editor, such as `vi`, and then restarts ospfd.

- **Running configuration** — This is the version currently being used by the appliance. This may differ from the configuration file and the starting configuration if an administrator logs into the server using the CLI and makes changes, but does not issue the `write` command.

- **Configuration file** — This is the most recent saved configuration. If an administrator makes changes using a non-Admin Console file editor but does not restart ospfd, this version will be different from starting configuration file.
On this window, you can do the following:

- **Edit a configuration file.** Click **Edit** to open the configuration file using the Admin Console File Editor. Edit the file as needed and then save your changes. The appliance automatically restarts the ospfd server. See “Configuring basic ospfd processing” on page 644 for more information.

  **Note:** Remember to create a rule using ospfd in the Service field before attempting to pass OSPF traffic. See “Creating a rule for ospfd” on page 643.

- **View and compare files.** Select an option from the list and then click **Retrieve**. A pop-up window appears displaying the requested information. Close this pop-up to return to the main OSPF window.

- **Save the running configuration to the configuration file.** Click **Overwrite** to save the running configuration. The running configuration and the starting configuration are now the same.

---

**BGP on Sidewinder**

The Border Gateway Protocol (BGP) is an Exterior Gateway Protocol (EGP) used to pass routing information between Autonomous Systems (AS). Unlike OSPF, which is an Interior Gateway Protocol (IGP), BGP is used to connect to external routers, such as your ISP. It does, however, learn information from an interior network that it then passes to an external network.

Routers using BGP are commonly located at the perimeter of an AS, as shown in Figure 267.

**Figure 267: BGP areas**

![BGP areas](image)

Routers employing BGP use TCP connections to communicate with peer routers, known as *neighbors*. After a connection is established, routing information is exchanged. Traffic is passed on port 179. The connection is maintained using keep-alives that are sent by both neighbors at a default rate of every 60 seconds, with a 3 minute timeout.

On the Sidewinder appliance, BGP processing is done via a Sidewinder server process named **bgpd**. To implement BGP processing, a bgpd server process must be configured and there must be an active rule that allows BGP broadcasts. You can control which routers bgpd can communicate with by managing the source and destination endpoints in the bgpd rule. Each burb will have no more than a single bgpd instance to handle the network traffic for all interfaces assigned to the burb.

As with the other Sidewinder dynamic routing protocols, see the Quagga documentation for a list of supported features.
Configuring BGP (bgpd)

See the following section for information on configuring BGP processing.

These are the high level steps to set up BGP on the Sidewinder appliance.

1 Sketch a diagram showing your planned Sidewinder configuration (similar to the diagrams in “BGP areas” on page 648). Include the following items on your diagram:
   - configuration of the routers to which the appliance connects
   - BGP areas in the network(s)
   - the Sidewinder interfaces (burbs)

2 Define one or more netgroups for the routers to which the appliance connects. See “Creating network objects” on page 272.

3 Configure one or more rules for the BGP traffic. See “Creating a rule for bgpd” on page 649.

4 Configure the appropriate BGP parameters. See “BGP processing options” on page 651.

About basic bgpd configuration

Using BGP in your network is a two-step process: First you must create a rule that allows bgpd traffic. Then you must configure bgpd with the appropriate network information and processing options.

Creating a rule for bgpd

To enable access to the bgpd configuration file:

1 Select Policy > Rules.
2 Click New Rule.
3 Enter a name and description that quickly identified this as the rule that provides access to the bgpd server.
4 In the Service field, select bgpd.
5 Set both the Source Burb and the Destination Burb fields to Any.
6 Configure the other Source and Destination fields as necessary to enforce your BGP security policy.
7 Save your changes.

For the appliance to pass BGP traffic, you now need to configure the bgpd configuration file with the settings appropriate for your security policy. See the following section for the preferred method for enabling and disabling the bgpd server.
Configuring basic bgpd processing

There are several ways to configure bgpd on the Sidewinder appliance. They are:

- Telneting into the bgpd server on the appliance and using a command line interface (CLI).
- Using the Admin Console File Editor to edit the bgpd configuration file.
- Using a different file editor, such as vi, to edit the bgpd configuration file.

Because the CLI method provides bgpd help and validates commands as they are entered, the following sections focus on this method. The same commands and functionality described here are valid when using the other methods, but require different formatting. Be sure that you are familiar with bgpd formatting conventions before using those methods.

For additional documentation on BGP processing, see the official Quagga web site at www.quagga.net.

To enable basic bgpd processing using a CLI:

1. Using a command line session, log into the appliance and switch to the Admn domain by entering:
   
   `srole`

2. Telnet into the Sidewinder bgpd server by entering:
   
   `telnet localhost bgpd`
   
   A password prompt appears.

3. Enter `zebra`.
   
   A `bgpd>` prompt appears.

4. Enable the full command set by entering:
   
   `bgpd>en`
   
   The prompt changes to `bgpd#` to indicate that the full command set is enabled.

5. Enable configuration mode by entering:
   
   `(config)#conf t`
   
   The prompt changes to `bgpd(conf)#` to indicate that configuration mode is enabled.
6 Enable bgpd and configure it to advertise routes, receive updates, and install routes in the local routing table by entering the following commands:

(config)#router bgp
(config-router)#network X.X.X.X/mask

where X.X.X.X/mask is the subnet and network mask of the interface on which you are enabling BGP. You can enter multiple network statements.

7 [Optional] To make changes persistent across reboots, write the changes to the configuration file by entering:

(config)#write

bgpd is now enabled and is advertising, receiving, and creating routing information. See the following section for information on other configuration options.

To disable bgpd, follow step 1 through step 5 in the previous procedure, and then enter:

(config)#no router bgp

bgpd is now disabled and will not participating in routing.

---

### BGP processing options

As with RIP and OSPF, only administrators who are experienced with routing in general, and BGP dynamic routing in particular, should configure bgpd.

These commands are presented as they are entered at a command line interface. They also assume that you have entered the appropriate network and area statements when you first accessed the bgpd server. Another option is to configure these options by using the Admin Console File Editor or other file editor to edit the configuration file directly. If you chose to modify the file directly, pay close attention to formatting. See the Quagga documentation at [www.quagga.net](http://www.quagga.net) for formatting assistance.

---

**Important:** Use the bgpd online help, available when using the CLI, for details on modifying the commands given here as well as other supported configurations. To access the bgpd online help, enter a mode (such as `router bgp` or `route-map`) and then enter `?` or `list`. You must be currently running a mode to see its documentation.

In general, the BGP configuration options are similar to the RIP and OSPF configuration options, particularly the route-map, prefix-list, and redistribution commands. See “RIP processing options” on page 632 for details. However, instead of using interface names to identify the source and destination of routing information, BGP uses names of neighbors.
The Admin Console provides tools to help you manage your BGP configuration. You can use these tools to quickly view the entire configuration file, compare different states of the configuration file, or list items such as the BGP neighbors and routes. You can also use the BGP area to edit the configuration file using the File Editor and to manually overwrite the configuration to be used the next time the bgpd restarts.

To use these tools, select Network > Routing > Dynamic Routing > BGP or Policy > Rule Elements > Services > bgpd. The following window appears:

Use this window to view and compare versions of the configuration file. The different versions are:

- **Starting configuration** — This is the version that is used when bgpd server restarts. The following events update this version:
  - An administrator makes changes using the CLI and saves the changes using the `write` command.
  - An administrator uses the Admin Console File Editor to save the configuration file or uses the `Overwrite` button.
  - An administrator saves changes using a file editor, such as vi, and then restarts bgpd.

- **Running configuration** — This is the version currently being used by the appliance. This may differ from the configuration file and the running configuration if an administrator logs into the server using the CLI and makes changes, but does not issue the `write` command.

- **Configuration file** — This is the most recent saved configuration. If an administrator makes changes using a non-Admin Console file editor but does not restart bgpd, this version will be different from starting configuration file.
On this window, you can do the following:

- **Edit a configuration file.** Click **Edit** to open the configuration file using the Admin Console File Editor. Edit the file as needed and then save your changes. The appliance automatically restarts the bgpd server. See “About basic bgpd configuration” on page 649 for more information.

  *Note: Remember to create a rule using bgpd in the Service field before attempting to pass BGP traffic. See “Creating a rule for bgpd” on page 649*

- **View and compare files.** Select an option from the list and then click **Retrieve**. A pop-up window appears displaying the requested information. Close this pop-up to return to the main BGP window.

- **Save the running configuration to the configuration file.** Click **Overwrite** to save the running configuration. The running configuration and the starting configuration are now the same.
The Protocol Independent Multicast - Sparse Mode (PIM-SM) protocol is used to route traffic to multicast groups.

Multicast is communication between a single or multiple senders and multiple receivers on a network. The Sidewinder appliance uses a XORP routing package which contains IGMP and PIM-SM protocols to route multicast traffic:

- The Internet Group Management Protocol (IGMP) is used by hosts and adjacent routers to establish multicast group memberships. IGMP tells routers that a host wants to receive multicast traffic for the specified multicast group.

- The PIM-SM protocol sets up a multicast forwarding table in routers. Multicast traffic is directed to a rendezvous point (RP), which distributes it toward PIM-registered receivers.

When a host wants to join a multicast session, IGMP sends a join request to its gateway router for a multicast group. Since the gateway router doesn't have information about the source address, it will send a PIM join back to the rendezvous point, which will contain the source information.

The rendezvous point facilitates the route setup between the sender and receiver. The sending gateway router sends multicast data to a rendezvous point encapsulated in a unicast PIM packet.

Once a gateway router with direct connection to the receiver’s network has received traffic from the source, the gateway router might start a process to build a direct path from the sender to the source.
To configure a Sidewinder appliance to route multicast traffic using PIM-SM, you must perform the following procedures:

1. Create policy rules to enable the pimd service and allow multicast traffic and PIM traffic forwarding.
2. Configure the pimd (XORP server) service (see page 658).
3. Configure IGMP (see page 660).
4. Configure PIM-SM (see page 661).
5. Restart the pimd (XORP server) service (see page 664).

It is recommended that you make all of these configuration changes at one time, since you must restart the pimd service to initialize your changes.

**Note:** When making subsequent changes to PIM-SM, there are two types of changes that require different procedures. See “Exceptions to making PIM-SM changes” on page 664 for more information.

### Create policy rules

You must create these policy rules to allow multicast routing:

**Create a rule to enable the pimd (XORP server) service**

1. Select **Policy > Rules**.
2. Click **New Rule**.
3. Enter a name and description that quickly identifies this as the rule that enables the pimd (XORP server) service.
4. In the Service field, select **pimd** from the drop-down list.
5. Set both the Source Burb and the Destination Burb fields to **Any**.
6. Configure the other Source and Destination fields as necessary to enforce your PIM-SM security policy.
7. Save your changes.
Create a rule to enable PIM traffic forwarding to rendezvous points and bootstrap routers

1 Create a packet filter service for the rule:
   a Select Policy > Rule Elements > Services.
   b Click New Service. The New Service window appears.
   c Enter a name and description that easily identifies the service.
   d From the Agent drop-down list, select Other Protocol Packet Filter.
   e From the Protocol drop-down list, select 103 - pim.
   f Select Bi-directional.
   g Click Add and save your changes.

2 Create a rule using the service:
   a Select Policy > Rules.
   b Click New Rule.
   c Enter a name and description that quickly identifies this as the rule that enables PIM traffic forwarding.
   d In the Service field, select the new traffic forwarding service.
   e Set both the Source Burb and the Destination Burb fields to Any.
   f Configure the other Source and Destination fields as necessary to enforce your PIM-SM security policy. Include all rendezvous points and bootstrap routers within the PIM network.
   g Click Add and save your changes.
Create a rule to enable multicast traffic

1 Create a packet filter service for the rule:
   a Select Policy > Rule Elements > Services.
   b Click New Service. The New Service window appears.
   c Enter a name and description that easily identifies the service.
   d From the Agent drop-down list, select TCP/UDP Packet Filter.
   e In the UDP ports field, select the UDP ports your multicast applications will be using.
   f Select Bi-directional.
   g Make any other changes necessary for your site’s security policy.
   h Click Add and save your changes.

2 Create a rule using the service:
   a Select Policy > Rules.
   b Click New Rule.
   c Enter a name and description that quickly identifies this as the rule that enables multicast traffic forwarding.
   d In the Service field, select the new multicast traffic service.
   e Configure the Source and Destination fields as necessary to enforce your multicast security policy. Include the multicast groups in the Destination Endpoint field.
   f Click Add and save your changes.
Configure the pimd (XORP server) service

1. Select **Network > Routing > Dynamic Routing > PIMSM**.
2. Click **Edit**. The xorp configuration file opens in the File Editor.
3. Verify that the interface names in the file are correct.
4. Remove the comments for these parameters:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>PIM-SM Editor window</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interfaces you want to run multicast over.</td>
<td><img src="image1" alt="PIM-SM Editor window" /></td>
</tr>
<tr>
<td><code>default-system-config</code> causes pimd to use the interface configuration from the system kernel.</td>
<td><img src="image2" alt="PIM-SM Editor window" /></td>
</tr>
<tr>
<td><code>mfea4</code> identifies which interfaces are being used for multicast traffic.</td>
<td><img src="image1" alt="PIM-SM Editor window" /></td>
</tr>
<tr>
<td><code>register_vif</code> is necessary for XORP processing.</td>
<td><img src="image2" alt="PIM-SM Editor window" /></td>
</tr>
</tbody>
</table>

*More...*
### Parameters

**fea** tells pimd how to locate unicast routes.

```plaintext
fea {
  unicast-forwarding4 {
    disable: false
    forwarding-entries {
      retain-on-startup: false
      retain-on-shutdown: false
    }
  }
}
```

**fib2mrib** tells PIM-SM to use the unicast routing table to find a route to the rendezvous points and to the sender.

```plaintext
protocols {
  fib2mrib {
    disable: false
  }
}
```

* Note: fib2mrib is needed for multicast only if the unicast protocols
  * don't populate the MRIB with multicast-specific routes.

```plaintext
/*
 * See xorp/mibs/pimpscripts/README on how to configure Net-SNIPP in your host
 * before uncommenting the gmp section below.
 * Also check that the "bgp4_mib_1657.so" exists in the correct location.
 */

/*
protocols {
  gmp {
    module bgp4_mib_1657 {
      abc-path: "/usr/local/xorp/mibs/bgp4_mib_1657.so"
    }
  }
```

<table>
<thead>
<tr>
<th>Parameters</th>
<th>PIM-SM Editor window</th>
</tr>
</thead>
<tbody>
<tr>
<td>fea tells pimd how to locate unicast routes.</td>
<td><img src="image1.png" alt="PIM-SM Editor window" /></td>
</tr>
<tr>
<td>fib2mrib tells PIM-SM to use the unicast routing table to find a route to the rendezvous points and to the sender.</td>
<td><img src="image2.png" alt="PIM-SM Editor window" /></td>
</tr>
</tbody>
</table>
Configure IGMP

1. [If necessary] Select **Network > Routing > Dynamic Routing > PIMSM** and click **Edit** to open the xorp configuration file.

2. Add an IGMP clause to the configuration file, specifying the interfaces to networks where hosts are receiving multicast packets. See the example below.

3. Save your changes.

---

**Figure 272:** IGMP added to the xorp configuration file

```plaintext
{  
  protocol {  
    igmp {  
      disable: false  
      interface bc0 {  
        vif bc0 {  
          disable: false  
        }  
      }  
      pimsm4 {  
        disable: false  
        interface bc0 {  
          vif bc0 {  
            disable: false  
            dr-priority: 1  
          }  
        }  
      }  
    }  
  }  
}
```

**Note:** To disable IGMP, remove the `igmp` section, then restart the `pimd` service.
**Configure PIM-SM**

You need to perform two tasks for a dynamic PIM-SM configuration:

- Specify interfaces you expect to receive multicast traffic.
- Configure the rendezvous points for a dynamic or static configuration.

**Specify interfaces**

1. [If necessary] Select Network > Routing > Dynamic Routing > PIMSM and click Edit to open the xorp configuration file.

2. Configure the interfaces that will run PIM-SM.
   - For each interface, an interface statement within the `pimsm4` section of the config file must be included.
   - `register_vif` must be included.

3. Configure the rendezvous point information. There are two ways to configure the rendezvous point:
   - “Configure rendezvous points dynamically with a bootstrap router” on page 662.
   - “Configure rendezvous points using static configuration” on page 663.
Configure rendezvous points dynamically with a bootstrap router

The bootstrap (dynamic) protocol is useful for large networks.

- You can have multiple rendezvous points — if one rendezvous point goes away, another one is elected.
- You can specify whether you want to be a rendezvous point, and you can specify whether you want to communicate with another router that is a rendezvous point.
- You do not have to configure rendezvous points — rendezvous points are learned. You can specify which interfaces on your appliance can learn the rendezvous points.

1. [If necessary] Select **Network > Routing > Dynamic Routing > PIMSM** and click **Edit** to open the xorp configuration file.

**Note:** You cannot change the bsr-priority (bootstrap router priority) setting in this file. If you need to change this setting, see “Changing the bsr-priority setting” on page 665 for instructions.

![Figure 274: Bootstrap router parameters](image)
2 Remove the comments from the bootstrap router and rendezvous points.
   • `cand-bsr` is the bootstrap protocol that selects a bootstrap router. The
     bootstrap router tells all PIM-SM routers what the rendezvous points
     are.
   • `cand-rp` tells the bootstrap router that this router is a candidate to be a
     rendezvous point.
   • `switch-to-spt-threshold` lets you specify the data rate at which the router
     selects the shortest path between the sender and the receiver.
     • If you have a lot of multicast traffic and use multicast for a long time,
       finding a shortest path is useful.
     • If you don’t have much traffic, or if you use multicast for a short time,
       finding a shortest path isn’t necessary.
     See xorp documentation for more information.
   • `traceoptions` sends debug tracing to syslog.

3 Save your changes.

Configure rendezvous points using static configuration

Static PIM-SM is a simpler configuration that is useful for smaller networks, for
example, if you have only two PIM routers or if your ISP provides the
rendezvous point.

1 [If necessary] Select Network > Routing > Dynamic Routing > PIMSM and
   click Edit to open the xorp configuration file.

2 Add static-rps clause to the configuration file, specifying the rendezvous
   point for a range of group prefixes. See the example below.
   • If more than one rendezvous point is specified for a group, the
     rendezvous point with the lowest priority is used.
   • All PIM-SM routers must be configured with the same rendezvous
     points.

3 Save your changes.
Restart the pimd (XORP server) service

2. Select the rule that uses the pimd service and click Modify.
3. Clear the Enable box.
4. Click OK and save your changes.
5. Select the rule that uses the pimd service and click Modify.
6. Select the Enable box.
7. Click OK and save your changes.

Exceptions to making PIM-SM changes

The procedures in this document explain how to configure the XORP server using the Sidewinder Admin Console. To configure the XORP server through a command line interface, you use the XORP command shell xorpsh.

The Admin Console’s PIMSM window, xorpsh, and any file editor open the same config.boot file (/secureos/etc/xorp/config.boot). However, the PIMSM editor and xorpsh interact, which can cause conflicts.

To avoid conflicts, there are two types of changes to PIM-SM that require different procedures:

• Disabling and enabling PIM-SM
• Changing the bsr-priority setting

Disabling and enabling PIM-SM

You cannot use xorpsh to enable or disable PIM-SM. To avoid an error message, you must enable or disable the rule that uses the pimd service.

2. Select the rule that uses the pimd service and click Modify.
3. Make the appropriate action:
   • To disable the pimd (XORP server) service, clear the Enable box.
   • To enable the pimd (XORP server) service, select the Enable box.
4. Click OK and save your changes.
Changing the bsr-priority setting

You cannot change the bsr-priority (bootstrap) parameter using the Edit function on the PIMSM window. To avoid an error message, you must stop the XORP server, change the parameter, and restart the XORP server.

To change the bsr-priority parameter:

1  Stop the XORP server:
   a  Select Policy > Rules.
   b  Select the rule that uses the pimd service and click Modify.
   c  Clear the Enable box.
   d  Click OK and save your changes.

2  Change the bsr-priority parameter:
   a  Select Maintenance > File Editor and open the following firewall file:
      
      /secureos/etc/xorp/config.boot
   b  Make the desired change to the bsr-priority parameter.
   c  Save your changes and close the File Editor.

3  Start the XORP server:
   a  Select Policy > Rules.
   b  Select the rule that uses the pimd service and click Modify.
   c  Select the Enable box.
   d  Click OK and save your changes.
Use the PIM-SM window to view and configure PIM-SM routing parameters.

Select Network > Routing > Dynamic Routing > PIMSM or Policy > Rule Elements > Services > pimd. The PIMSM window appears.

You can view the following information:

- **MRIB information inside PIM** — Displays the unicast routes used to reach other PIM rendezvous points, bootstrap routers, and multicast source.
- **Bootstrap routers** — Displays current bootstrap router and the set of rendezvous points.
- **Groups** — Displays information regarding joined groups: source (sender), rendezvous point, and flags.
- **Interfaces** — Displays each network interface configured for PIM.
- **Neighbors** — Displays information on neighboring PIM routers: interface, priority, and address.
- **RPs** — Displays the current rendezvous point routers: IP address, type, priority, and group range.
- **Multicast Forwarding Cache** — Displays the kernel’s multicast forwarding table.

On this window, you can do the following:

- **Edit a configuration file.** Click Edit to open the configuration file using the Admin Console File Editor. Edit the file as needed and then save your changes. The appliance automatically restarts the bgpd server. See “Configuring PIM-SM (pimd)” on page 655 for more information.
- **View and compare files.** Select an option from the list and then click Retrieve. A pop-up window appears displaying the requested information. Close this pop-up to return to the main PIMSM window.
If you need to troubleshooting dynamic routing issues, you can use the following commands to enable debugging, and then either display or save the log files.

1. Using a command line session, log into the appliance and switch to the Admn domain by entering:
   
   `srole`

2. Telnet into the appropriate dynamic routing server by entering one of the following command:
   - To access ospfd, enter:
     
     `telnet localhost ospfd`
   - To access bgpd, enter:
     
     `telnet localhost bgpd`
   - To access ripd, enter:
     
     `telnet localhost_n ripd`

   where \( n \) = the burb index of the burb used as the source burb in the enabled ripd rule. Use `cf burb query` to look up a burb’s index. It is also listed on the Network > Burb Configuration window as the ID.

   A password prompt appears.

3. Enter `zebra`.
   
   A `ripd>` prompt appears.

   **Note:** The prompt will reflect the server you logged into.

4. Enable the full command set by entering:
   
   `ripd>en`

   The prompt changes to `ripd#` to indicate that the full command set is enabled.

   **Note:** Enabling debugging at this prompt turns debugging on temporarily. To making debugging persistent, enter the `conf t` command before entering the debug commands.

5. Set the debug parameters by entering one or more commands similar to these examples:
   
   `ripd#debug protocol event`
   
   `ripd#debug protocol packet [recv|send] [detail]`
   
   `ripd#debug protocol zebra`

   where protocol is rip (case sensitive).

   See the online help or Quagga documentation for ospf and bgp commands and for additional debugging flags.
6 View the log information in the current window by entering:

   ripd#term monitor

To stop writing debug statement to the current window, enter:

   ripd#term no monitor

7 [Optional] To save the log information to a log file, you can edit the configuration file directly and add this line:

   log file filename

   The default path for the log file is /var/run/quagga. To save the file in a different location, specify the entire path as part of the file name.

If you misconfigure your routing tables, you will need to disable ripd and make corrections to the tables and then restart ripd, either by writing the file changes or saving the configuration file using the Admin Console File Editor. Before restarting ripd, enter the following command at a UNIX prompt to flush the routing tables of all gateways.

   route flush
The SNMP Agent

In this chapter...

Understanding SNMP options ................................................................. 670
Overview of Sidewinder as a managed node ............................................ 671
Setting up the SNMP agent on Sidewinder .............................................. 676
Sending SNMP traffic through Sidewinder .............................................. 680
This section introduces Simple Network Management Protocol (SNMP) concepts and explains how to configure the Sidewinder SNMP agent. It also explains what needs to be done to allow the Sidewinder appliance to send or route SNMP messages to remote systems in an external network.

SNMP is the industry standard for network management. The Sidewinder appliance supports SNMP v1, SNMP v2c, and SNMP v3. The appliance can participate in SNMP management in two different ways:

- You can set up SNMP agent software that allows the appliance to be an SNMP-managed node. A node is monitored by SNMP-compliant network management stations located on one of the Sidewinder burbs.

- Using the SNMP proxy, you can configure the Sidewinder appliance to route SNMP messages from a management station through the appliance to an SNMP agent on a system in an external network.

Note: If you want your Sidewinder appliance to simultaneously act as an SNMP agent and pass SNMP traffic in the same burb, you will need to use a TCP/UDP Packet Filter service to pass the SNMP traffic. See “Creating and modifying services” on page 147.
Overview of Sidewinder as a managed node

The following sections describe how the Sidewinder appliance interacts with SNMP management stations:

- “Communicating with an SNMP management station” on page 671
- “About Sidewinder SNMP traps” on page 673
- “About Sidewinder SNMP MIBs” on page 673
- “About the management station” on page 675

Communicating with an SNMP management station

A network that is managed using SNMP involves two primary components: a manager (management station) and a number of managed nodes. The management station is typically a PC or UNIX workstation running network management software such as Hewlett-Packard’s OpenView® or the freeware Multi-Router Traffic Grapher (MRTG). Managed nodes are networking devices such as routers or Sidewinder appliances that contain an SNMP agent. Figure 279 shows a management station communicating with an SNMP node to obtain network configuration information.

The management station uses the management software to display a graphical representation of a network’s topology. In general, network managers can monitor SNMP nodes (including the Sidewinder appliance) by clicking icons that represent each node in the network’s topology.

A management station in an internal or external network can request information from a managed node’s SNMP agent. The SNMP management station sends a managed node `get` and `getnext` SNMP messages to retrieve node-specific parameters and variables, called `objects`. The message response from the managed system provides the SNMP administrator with information on a node’s device names, status, network connections, etc.

![Figure 279: Communication between a management station and a managed node](image)

---

**Important:** SNMP agents typically allow `Get`, `GetNext`, and `Set` requests from the management station. However, the Sidewinder SNMP agent does not support `Set` requests. This prevents a management system from sending commands to change variables or parameters in the appliance.
Each managed node can send an unsolicited event notification message, called a *trap*, to a management station when it detects certain system events. For example, you can configure the Sidewinder audit system to issue a trap whenever an unauthorized user tries to read, write, or execute a protected file on the appliance. (Refer to “Sidewinder SNMP traps” on page 418 for a list of all Sidewinder-supported traps.)

- When setting up SNMP management for SNMP v1 or SNMP v2c, a network administrator assigns the management station and the nodes it will manage a *community name*. As shown in the following figure, the community name is in the authentication header in each SNMP message exchanged between a management station and a managed node.

![Figure 280: Community name within an SNMP message](image)

<table>
<thead>
<tr>
<th>VERSION</th>
<th>COMMUNITY NAME</th>
<th>SNMP COMMAND: GET, GETNEXTREQUEST, ETC.</th>
</tr>
</thead>
</table>

The SNMP agent treats the community name like a password to validate the identity of a management station. For example, suppose a management station sends a *get* request to retrieve information from a managed node’s SNMP agent. If the community name within the *get* request is not also used by the SNMP agent, the agent will not return information to the management station.

**Caution:** To increase security on your network, do not use common default names such as “public” or “private,” which can be easily guessed.

- SNMP management in SNMP v3 requires a user name and password. The password is encrypted in SNMP messages, increasing the security.

Both the management station and the managed node also contain Management Information Bases (MIBs) that store information about the managed objects. Currently, the SNMP agent on the appliance supports standard MIB II objects, the Host Resources MIB (RFC 1514), and the Sidewinder-specific MIB objects. MIBs are discussed in greater detail in “About Sidewinder SNMP MIBs” on page 673.

**Note:** On the Sidewinder appliance, all Secure Computing Corporation MIB files are located in `/secureos/etc/snmp`.

If you need more information on SNMP, an excellent source is *Managing Internetworks with SNMP* by Mark A. Miller, P.E. (M&T Books).
About Sidewinder SNMP traps

An SNMP trap is an alert message that is sent as an unsolicited transmission of information from a managed node (router, Sidewinder appliance, etc.) to a management station. Most management stations can be configured to either: (1) display received traps in a pop-up window, or (2) automatically dial a phone number, such as a pager number.

The Sidewinder SNMP agent supports a basic trap, called the ColdStart trap, that is sent whenever Sidewinder’s SNMP agent is enabled. It is also sent if the Admin Console modifies the SNMP configuration file (/secureos/etc/snmp/snmpd.conf). You cannot disable the ColdStart trap.

You also have the option to configure the appliance to send audit alert SNMP traps when an audit event triggers a response. Additional information about requesting and configuring SNMP traps is available in “Sidewinder SNMP traps” on page 418.

About Sidewinder SNMP MIBs

Management Information Bases (MIBs) are associated with both the management station and the Sidewinder SNMP agent. The Sidewinder SNMP agent supports two MIB structures (as well as a Host MIB).

• **mib2** — This is a standard SNMP MIB as defined in RFC 1213.

• **sccMibSw** — This is a Sidewinder-specific MIB provided by Secure Computing Corporation. Figure 281, located on the following page, shows the location of the Sidewinder MIB structures within the SNMP root hierarchy.

**Note:** On the Sidewinder appliance, all Secure Computing Corporation MIB files are located in /secureos/etc/snmp.

Individual objects (parameters and variables) managed by an SNMP management station are part of an object group within an MIB. For example, the **swProxy** group stores information about currently-defined proxies on the system. The information might include the proxy name and the current status of the proxy.

When a management station requests information from the Sidewinder SNMP agent, the SNMP agent may or may not associate the returned information with a specific **burb**.
Figure 281: MIBs supported by the Sidewinder SNMP agent
About the management station

The administrator of the SNMP management station should be made aware of the following in order to retrieve information from the Sidewinder SNMP agent:

- **Sidewinder host name or IP address**
  This is needed to set up communication with the appliance. Note:
  - If the burb in which the SNMP agent is running contains more than one interface, specify the address of the first interface in the burb. The SNMP agent will only respond to the first interface in the burb.
  - If you are using High Availability (HA), specify the shared HA common IP address or host name, not the actual interface address or host name.

- **Community names configured in the Sidewinder SNMP agent**
  If you are using SNMP v1 or SNMP v2c, this is needed to allow the management station to retrieve MIB objects from the SNMP agent.

- **SNMP v3 user name and password**
  If you are using SNMP v3, you must configure the Sidewinder appliance with the user names and passwords established on the management station.

- **MIB information**
  This may be needed to properly translate the object identifications. Inform the administrator that the appliance supports the Host Resources MIB.
  On the Sidewinder appliance, all Secure Computing Corporation MIB files are located in the `/secureos/etc/snmp` directory and can be accessed directly. The files can also be downloaded via an FTP client or Web browser, The MIB files are `SCC-MIB.txt` and `SCC-SW-MIB.txt`.
  
  - To retrieve the files by FTP, from your FTP client log into `ftp.securecomputing.com`. The files are located in `/pub/mibs`.
  - To retrieve the files using a web browser, point the browser to `ftp://ftp.securecomputing.com/pub/mibs/`.
This section explains how to configure the SNMP agent on the Sidewinder appliance. It involves the following steps:

- Configure the SNMP agent (*Policy > Rule Elements > Services > SNMP Agent*).

- Create a rule allowing access from the management station to the Sidewinder SNMP agent (*Policy > Rules*).

**Note:** If you are configuring SNMP on an appliance that is part of an HA cluster, all Sidewinder queries must use the HA cluster address.

- Send custom traps (for example, from shell scripts) using the `snmptrap` command. See “Sidewinder SNMP traps” on page 418 and the `snmptrap` man page.

- Use the IPS Attack and System Event Responses (*Monitor > IPS Attack Responses/System Event Responses > Response* tab) to manage when the appliance sends SNMP traps to its management station. See Chapter 13, “IPS Attack and System Event Responses,” on page 399.

All of these steps play an important role in providing your SNMP management station with information.
Configuring the SNMP agent

To set up the SNMP agent, select Policy > Rule Elements > Services, then double-click snmpd and click Properties. The SNMP Agent Configuration window appears.

**Figure 282: SNMP Agent Configuration window**

Use this window to enter configuration information for the SNMP agent.

To set up the SNMP agent:

1. [Optional] In the Location field, type a description of the physical location of your appliance.
2. [Optional] In the Contact field, type an identifying name, such as your Sidewinder administrator user name or e-mail address.
3. In the Enable Authentication Failure Trap field, select Yes to enable authentication failure traps, or No to disable authentication failure traps. If you click Yes, the appliance will send authentication failure traps to all configured management stations whenever it detects an unauthenticated Get command.
4. In the Allowed Protocols area, select the versions of SNMP that incoming SNMP requests are allowed to use. SNMP message with versions that are not allowed are ignored.
5. From the Trap version drop-down list, select the SNMP version that the Sidewinder appliance should use when sending traps.

**Note:** This is a global setting that will affect all components that originate traps.
6 [Conditional] If you select trap version v3, click **v3 settings** and configure the security settings to use when sending traps:

- **Username** and **Password** — Enter the user name and password to use when sending traps. All trap destinations will use the same SNMP user when using SNMP v3. Enter the password again to confirm.

- **Security level** — From the drop-down list, select whether authentication and encryption should be used when sending traps:
  - noAuth — No authentication or encryption is required.
  - authNoPriv — A password is required. Payload encryption is not used.
  - authPriv — A password and payload encryption are required.

7 Click **OK** to return to the SNMP Agent Configuration window.

8 Use the SNMP v3 users list to view, create, and manage SNMP v3 users who can issue requests to the Sidewinder SNMP agent.

To configure SNMP v3 users who can issue requests to the Sidewinder SNMP agent, click **New** and enter the appropriate information:

- **Username** — Enter the user name established on the SNMP management station.

- **Description** — Optionally enter a description to easily identify this user.

- **Password** — Enter the password established on the SNMP management station. Enter the password again to confirm.

- **Minimum security level** — From the drop-down list, select whether authentication and encryption should be used when issuing requests:
  - noAuth — Any security level can be used.
  - authNoPriv — A password is required. Payload encryption is optional.
  - authPriv — A password and payload encryption are required.

9 Click **OK** to return to the SNMP Agent Configuration window.

10 In the Allowed Get Communities list, you can view all of the community names authorized to retrieve MIB information. The community name is part of the authentication header in all SNMP messages. The Sidewinder SNMP agent checks the community name in all v1 and v2c SNMP messages it receives to verify the identity of a manager.

To add, modify, or delete communities, use the **New**, **Modify**, and **Delete** buttons located directly beneath the list.

- The SNMP agent will not start unless a community name is specified. By default, if you do not specify an **Allowed Get Community** name, then only **Allowed Get Community** is “public.”

- Communities are ignored in SNMP v3.
In the Trap Destinations list, you can view all of the hosts that will receive traps generated by the Sidewinder SNMP agent.

To add, modify, or delete trap destinations, use the **New**, **Modify**, and **Delete** buttons located directly beneath the list.

- By default, if you do not specify a trap destination community name, the appliance uses the community name “public.”
- If the trap version selected is v3, the community name in Trap destinations is ignored.

Click **OK** to return to the SNMP Agent Configuration window.

Be sure to save your changes when you return to the main Services window. Once you create an enabled rule with the SNMP agent as the service, a ColdStart trap is issued to all configured trap destinations.

### Creating a rule to allow access to the SNMP agent

You must create a rule that allows SNMP queries to reach the Sidewinder’s SNMP agent. (For information on creating rules, see “Creating, modifying, and duplicating rules” on page 95.)

- If the management station is in a trusted, internal burb, create the following rule to allow traffic between the management station and the Sidewinder SNMP agent:

  **Table 45:** Key features in the SNMP agent rule

<table>
<thead>
<tr>
<th>Rule area</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service</td>
<td>SNMP agent</td>
</tr>
<tr>
<td>Source Burb</td>
<td>Must be a single burb and must match the destination burb. The SNMP agent will be enabled in the burb selected here.</td>
</tr>
<tr>
<td>Destination Burb</td>
<td>Must match the source burb.</td>
</tr>
</tbody>
</table>

- The SNMP agent can only be enabled in one burb. If you have management stations in other burbs that must reach the SNMP agent, see “Sending SNMP traffic through Sidewinder” on page 680 for information on creating rules for those situations.
You can route (or forward) SNMP messages between a management station behind the Sidewinder appliance and any SNMP managed node on the other side of the appliance. If your management station is in an untrusted burb, or you have multiple management stations in different burbs, you can also allow access to the Sidewinder SNMP agent using the SNMP proxy in a rule. This section describes three scenarios that use SNMP and provides guidance on how to set up the necessary rules.

The Sidewinder SNMP proxy sends SNMP requests and messages via UDP port 161. That proxy sends SNMP traps to an external management station via UDP port 162.

Figure 283 displays the following three scenarios:

1. Passing traffic from an internal SNMP management station through the appliance via the SNMP proxy to an external managed node (SNMP agent). Set the rule’s service to the SNMP proxy. The source and destination burbs will be different (for example, internal to external).

2. Passing traffic from a management station to the Sidewinder SNMP agent when both are located on the same burb. This scenario does not use the SNMP proxy. Set the rule’s service to SNMP agent. The source and destination burb must be the same (for example, internal to internal).

3. Passing traffic across burb boundaries to the SNMP agent. Although only one SNMP agent is allowed to operate on the appliance, access through other burbs is supported using the SNMP proxy. To allow SNMP management stations that reside in other burbs to connect to the SNMP agent, you must create an allow rule using the SNMP proxy. The source for this rule should consist of a network object group that contains only SNMP management station IP addresses. The destination should specify the destination IP address for the burb in which SNMP is running. Using redirection is common in this scenario (for example, external to external with redirection to the internal interface).
MAINTENANCE
In this chapter...

Setting the system date and time ................................................................. 684
Configuration file backup and restore ......................................................... 691
Activating the Sidewinder license ................................................................. 705
Protected host licensing and the Host Enrollment List ............................... 713
Software management ................................................................................ 716
Registering with CommandCenter ................................................................. 729
Enforcing FIPS ........................................................................................ 731
Setting the system date and time

You can use the Admin Console to set the date and time for the Sidewinder appliance, and to configure the NTP (Network Time Protocol) service to synchronize clocks.

Setting the date and time

To set the system date and time, select **Maintenance > Date and Time**. The Date and Time window appears.

Figure 284: Date and Time window

Use this window to set the date and time for the Sidewinder appliance, or to configure the NTP (Network Time Protocol) service to synchronize clocks.

**Note:** Applying changes to the date and time will cause the appliance to automatically reboot. Therefore, you should only modify date and/or time settings during off-hours.
Setting the date and time

To change the date and time:

1. Set the time zone: From the Time Zone drop-down lists, select the region, country, and time zone where the Sidewinder appliance is located. To use Greenwich Mean Time (also known as Coordinated Universal Time), select Use GMT (UTC).
2. Set the date and time: From the Date and Time fields, select the current date and time.
3. Save your changes.

Configuring NTP on a Sidewinder appliance

For a detailed explanation of NTP and the Sidewinder appliance, see “Understanding Network Time Protocol” on page 686.

Tip: For best results, set the Sidewinder appliance time as close as possible to the NTP server’s time. If the times are too far apart, it might take a long time for the NTP server to synchronize with the appliance.

To configure NTP:

1. In the Enable Network Time Protocol (NTP) on list, select the appliance burb that receives time updates from the NTP server. This enables the NTP service in the appropriate burb.
2. In the NTP Servers area, add one or more NTP servers:
   • To configure an NTP server that supplies time to the Sidewinder appliance, click New, then configure the server in the New NTP Server window.
     a. In the Server field, enter the IP address or the host name of the NTP server.
     b. From the Burb drop-down list, select the Sidewinder burb that communicates with the NTP server. This enables the NTP service in the appropriate burb.
     c. [Conditional] If you want this to be the preferred NTP server, select Preferred Server.
     d. Click Add.
   • To modify an existing NTP server, select the server in the list and click Modify, then make your changes in the Modify NTP Server window.
   • To delete an existing NTP server, select the server in the list and click Delete.
3. Save your changes.
Understanding Network Time Protocol

NTP provides a way to synchronize all clocks on a network, or to synchronize the clocks on one network with those on another network.

When you use NTP with a Sidewinder appliance:

- Time is set accurately.
- Synchronized network systems are useful for audit logs.
- You have a more accurate external time source when synchronizing your network for time-critical services.
- Cluster environments (High Availability, One-to-Many) benefit from synchronized time.

This release of the Sidewinder appliance is compatible with NTP versions 2, 3, and 4. Version 4 is the preferred version and is the default on the appliance.

NTP servers and clients

In NTP, a server is a system that sends a time feed to another system. (The server is also referred to as a host.) The receiving system — the one whose time is being set by the server — is an NTP client. The Sidewinder appliance can be set up as an NTP server or a client.

Figure 285 shows a simple configuration with an NTP time server and two NTP clients (A and B) in the same network. The NTP server supplies the time to NTP clients A and B. Using their own NTP software, each client system must also be set up to receive time from the server.

**Figure 285: NTP server-client relationship**

![NTP server-client relationship diagram](image-url)
The Sidewinder appliance as an NTP client

Figure 286 shows a common NTP setup. It is the recommended configuration, with the Sidewinder appliance configured as a client receiving time from a server labeled “Internal time source.” In this configuration, a server in the internal network (shown with an analog clock) is the designated time-setter for the rest of the network. The three other systems in the internal network are also NTP clients.

By means of NTP, the server automatically maintains the correct time on the appliance and also maintains the time on other workstations in the network.

The internal network does not rely on an external time server, so it is not exposed to any security breaches that could result. Since the Sidewinder appliance is not supplying time for other systems but is only receiving it, this setup has minimal effect on appliance performance.

• Do not configure the appliance to receive time from both an internal and external NTP server. It should receive time on only one burb. Input from the external time server cannot be reconciled with that from the internal server.

• For best results, set the Sidewinder appliance time as close as possible to the NTP server’s time. If the times are too far apart, it might take a long time for the NTP server to synchronize with the appliance.

To set up a Sidewinder appliance as an NTP client for an internal NTP server:

1. Select Maintenance > Date and Time.
2. In the Enable Network Time Protocol (NTP) on list, select the appliance burb that is used to communicate with the NTP server. This enables the NTP service in the appropriate burb.
3. In the NTP Servers area, click New. The New NTP Server window appears.
4. Enter the IP address of the NTP server (1.1.1.1 in the example above).
5. From the burb drop-down list, select the appliance burb that is used to communicate with the NTP server.

6. [Conditional] Identify this server as the preferred NTP server.

7. Click **Add**.

**The Sidewinder appliance as an NTP server**

You can also set up the Sidewinder appliance to be a time-setter for the rest of the network. The appliance can receive time from an external NTP server, then feed the time to an internal system, which in turn supplies time to your other workstations.

- Serving time directly from a Sidewinder appliance to several clients can slow the performance of the appliance.
- If the appliance is serving time (host), its clients should not receive time from any other NTP server.

In the figure below, the appliance is receiving time from NTP servers on an external network and passing the time on to the internal network. This would be advantageous if your company required constant and precise time updates to within microseconds of world standard time. In this scenario, the router must be able to handle NTP traffic.

---

**Important**: An external-to-internal NTP configuration may introduce security concerns to the appliance and thus to your network. Therefore, this configuration is only recommended for sites that need world standard time.
Configure the Sidewinder appliance to receive time from an NTP server and serve time to clients:

1 Select Maintenance > Date and Time.

2 In the Enable Network Time Protocol (NTP) on list, enable the NTP service in the appropriate burbs.
   • One burb communicates with external NTP servers.
   • One burb feeds time to the internal time server.

3 Add one or more external NTP servers:
   a In the NTP Servers area, click New. The New NTP Server window appears.
   b Enter the IP address of the external NTP server (1.1.1.1 in the example above).
   c From the burb drop-down list, select the external Sidewinder appliance burb that communicates with the NTP server.
   d [Optional] Select Preferred Server.
   e Click Add.

4 Add the Sidewinder appliance as a time server:
   a In the NTP Servers area, click New. The New NTP Server window appears.
   b Enter the following IP address: 127.127.1.0
   This tells the appliance to use the local hardware clock as its time source.
   c From the burb drop-down list, select the Sidewinder burb that communicates with the internal time server.
   d [Optional] Select Preferred Server.
   e Click Add.

5 Save your changes.
References

NTP is a complicated protocol with many options. There are numerous places where more information can be obtained. These include RFCs, Web sites, and local manual (man) pages. For more information about NTP, see the following sources:

Internet Request For Comments (RFC)

The following RFCs provide information on NTP:

• RFC 1119 Network Time Protocol (Version 2)
• RFC 1305 Network Time Protocol (Version 3)
• RFC 4330 Simple Network Time Protocol (Version 4)

Web Sites

Point your browser to the following Web site:

http://www.ntp.org/

On-line manual (man) pages

Type the following commands:

```bash
man cf_ntp
man ntpd
man ntpdc
man ntpdate
```
Configuration file backup and restore

Use the Configuration Backup feature to back up and restore Sidewinder configuration files. Backing up the configuration files lets you quickly restore an appliance to a previous operational state.

The figure below shows the three options for a configuration backup.

**Figure 288: Configuration file backup options**

- **Client system** — This option backs up configuration files to the Admin Console computer. This includes any location on your Admin Console hard drive; any removable media with a drive attached to the Admin Console computer, such as diskette or recordable CD; any network drive the Admin Console computer is connected to.

- **Local Sidewinder** — This option backs up configuration files to the appliance’s own hard drive, or to a USB flash drive. On the appliance, the backup files are stored in the /var/backups/repository; you can move them to another location using a file transfer mechanism such as FTP or SCP.

- **Remote system (SCP)** — This option backs up configuration files to a remote Sidewinder appliance or to another remote server.
  - You must have a rule on the remote appliance allowing SSH connections to the appropriate port.
  - A remote server needs SSH enabled (SCP) and a user created.

You can also use this feature to manage configuration backups and make a disaster recovery backup.

To back up or restore your configuration files, select **Maintenance > Configuration Backup**. The Configuration Backup window appears.

- To create and manage configuration backups, click the **Configuration Backup** tab. See “About the Configuration Backup: Configuration Backup tab” on page 692 for details.
- To restore configuration backups, click the **Configuration Restore** tab. See “About the Configuration Backup: Configuration Restore tab” on page 698 for details.
- To schedule automatic configuration backups, click the **Schedule** tab. See “About the Configuration Backup: Schedule tab” on page 703 for details.
Chapter 22: General Maintenance Tasks

Configuration file backup and restore

About the Configuration Backup: Configuration Backup tab

Use this tab to back up Sidewinder configuration files. You can also create a disaster recovery backup and manage local configuration backups.

Figure 289: Configuration Backup tab

You can perform the following actions:

- "Back up configuration files" on page 692
- "Create a disaster recovery backup" on page 696
- "Manage configuration backup files" on page 697

Back up configuration files

Use this feature to back up Sidewinder configuration files.

- You can back up configuration files to the Admin Console computer, the Sidewinder appliance, or a remote system.
- Only configuration files are backed up with this process. For example, the mail queues, the audit trail, the log files, or executable files will not be backed up in a configuration backup.

To back up more information, see “Create a disaster recovery backup” on page 696.

- The backup file must be at the same version as the system it is being restored to.
Backing up configuration files to the Admin Console computer

To back up configuration files to the Admin Console computer:

1. In the Backup Sidewinder Configuration area, select **Client System**.
2. Click **Backup now**. The Save Configuration Backup window appears.
3. Navigate to the location on the Admin Console computer where you want to save the configuration files. You can select any directory, media drive, or network available to the Admin Console computer.
4. [Optional] In the **File name** field, enter a name that can easily identify this configuration backup.
   
   A default name consisting of the appliance name plus the current date automatically populates this field.
5. Click **Save**. The Filename and encryption window appears.

![Figure 290: Filename and encryption window for Client System backup](image)

6. [Optional] Enter a key to encrypt the configuration backup file. Valid values include alphanumeric characters, periods (.), dashes(-), underscores (_), and spaces ( ).
   
   - This key will not be saved. You must remember it. You will not be able to restore the configuration file without this key.
   - You do not have to enter an encryption key. If you click **OK** without entering an encryption key, the backup continues.

   Enter the key again to verify.
7. Click **OK**.
   
   A “Configuration backup successful” message appears.
8. Click **OK**.

You have finished backing up a configuration file to the Admin Console computer.
Chapter 22: General Maintenance Tasks

Configuration file backup and restore

**Backing up configuration files to the Sidewinder appliance**

To back up configuration files to the appliance:

1. In the Backup Sidewinder Configuration area, select **Local Sidewinder**.
2. Click **Backup now**. The Filename and encryption window appears.

3. [Optional] In the **File name** field, enter a name that can easily identify this configuration backup.
   
   A default name consisting of the appliance name plus the current date automatically populates this field.

4. Select a location for the backup file:
   • To save the backup file on the appliance, select **Disk**.
   • To save the backup file on a flash drive inserted in the USB port on the appliance, select **USB Flash Drive**.
     • Insert the flash drive before performing the backup.
     • Do not remove the flash drive from the appliance until the “Configuration backup successful” message appears.

5. [Optional] Enter a key to encrypt the configuration backup file. Valid values include alphanumeric characters, periods (.), dashes(-), underscores (_), and spaces ( ).
   • This key will not be saved. You must remember it. You will not be able to restore the configuration file without this key.
   • You do not have to enter an encryption key. If you click **OK** without entering an encryption key, the backup continues.

   Enter the key again to verify.

6. Click **OK**. A “Configuration backup successful” message appears.

7. Click **OK**. The backup appears in the list of current local configuration backups.

You have finished backing up a configuration file to the appliance.
Chapter 22: General Maintenance Tasks
Configuration file backup and restore

Backing up configuration files to a remote system

Before performing this procedure:

• If backing up to a remote Sidewinder appliance, you must have a rule on the remote appliance allowing SSH connection to the appropriate burb.
• If backing up to another remote system, the remote system needs SSH enabled (SCP) and a user created.

To back up configuration files to a remote system:

1 In the Backup Sidewinder Configuration area, select **Remote System (SCP)**.

2 Define the remote system that is receiving the configuration backup files:
   • In the **Username** field, enter the user name of a user on the remote system. If the remote system is a Sidewinder appliance, this is an appliance administrator.
   • In the **Password** field, enter the password used to authenticate the user to the remote system.
   • **Note:** The appliance does not save the password.
   • In the **Hostname** field, enter the host name or the IP address of the remote system.
   • The **Port** field default is 22.
   • In the **Directory** field, enter the directory on the remote system where the configuration files are stored. If the remote system is a Sidewinder appliance, the administrator’s home directory is the default.

   This information is retained. You can change it at any time.

3 Click **Backup now**. The Filename and encryption window appears.

![Configuration Backup: Filename and encryption window for Remote System backup](image)

4 [Optional] In the **File name** field, enter a name that can easily identify this configuration backup.

   A default name consisting of the appliance name plus the current date automatically populates this field.
Chapter 22: General Maintenance Tasks

Configuration file backup and restore

5  [Optional] Enter a key to encrypt the configuration backup file. Valid values include alphanumeric characters, periods (.), dashes(-), underscores (_), and spaces ( ).

• This key will not be saved. You must remember it. You will not be able to restore the configuration file without this key.
• You do not have to enter an encryption key. If you click OK without entering an encryption key, the backup continues.

Enter the key again to verify.

6  Click OK. A “Configuration backup successful” message appears.

7  Click OK.

You have finished backing up a configuration file to a remote system.

Create a disaster recovery backup

Use this feature to create a disaster recovery backup. If you need to re-install your appliance, you can use this backup to restore the configuration.

• The disaster recovery backup saves configuration files, installed packages, and the Quick Start Wizard data file (qsw_datafile) to a USB flash drive plugged into the appliance.
• The backup can take several minutes to complete.

To create a disaster recovery backup file:

1  Insert a flash drive into the USB port of the Sidewinder appliance.

2  On the Admin Console, select Maintenance > Configuration Backup.

3  Click Create Disaster Recovery Backup. The Configuration Backup and Restore: Disaster Recovery window appears.

4  [Optional] Enter a key to encrypt the disaster recovery backup. Valid values include alphanumeric characters, periods (.), dashes(-), underscores (_), and spaces ( ).

• This key will not be saved. You must remember it. You will not be able to restore the disaster recovery backup without this key.
• You do not have to enter an encryption key. If you click OK without entering an encryption key, the backup continues.

Enter the key again to verify.

5  Click OK. A warning message appears.

6  Click Yes to confirm the backup.

A progress bar appears while the files are backed up to the flash drive.

**Note:** Do not remove the USB flash drive from the appliance until the “Disaster recovery successful” message appears.

When the backup is complete, a “successful” message appears.
7 Click OK.

8 Remove the flash drive from the appliance and store it in a safe place.

- You can restore the disaster recovery backup only during re-imaging. For more information, see “About the disaster recovery option via USB flash drive” on page 834.
- You can also create disaster recovery media using the Backup Builder, a standalone application available on the Sidewinder patch web site. See “Using the Backup Builder” on page 835 for information.

Manage configuration backup files

Use the Manage Sidewinder Configuration Backups area to move configuration backups between the Sidewinder appliance and the Admin Console computer, and to delete configuration backups.

Note: The Current local configuration backups list is also on the Configuration Restore tab. Any changes to this list on the Configuration Backup tab also appear on the Configuration Restore tab.

Delete a configuration backup from the appliance

1 Select a configuration backup from the list.

2 Click Delete. Click Yes to confirm the deletion.

Move a configuration backup file from the Admin Console to the appliance

1 Click Upload. The Upload Configuration Backup window appears.

2 Navigate to the location on the Admin Console computer where the configuration backup file is stored.

3 Select the configuration backup file and click Open. An “Upload successful” message appears when the upload is complete.

4 Click OK. The backup file appears in the list.

Move a configuration backup file from the appliance to the Admin Console

1 Select a configuration backup file from the list.

2 Click Download. The Save Configuration Backup window appears.

3 Navigate to the location on the Admin Console computer you want to copy the backup file to. This can include a directory on the hard drive, removable media with a drive attached to the Admin Console computer, or a network drive the Admin Console computer is connected to.

4 Click Save. A “Download successful” message appears when the download is complete.

5 Click OK.
Chapter 22: General Maintenance Tasks

Configuration file backup and restore

Chapter 22: General Maintenance Tasks

Configuration file backup and restore

About the Configuration Backup: Configuration Restore tab

Use this tab to restore a Sidewinder appliance to a previous operational state. You can also manage local configuration backups.

You can perform the following actions:

- “Restore configuration backups” on page 698
- "Manage configuration backup files" on page 702

Restore configuration backups

Use this feature to restore a Sidewinder appliance to a previous operational state.

- You can restore configuration files from the Admin Console computer, the Sidewinder appliance, or a remote system.
- Only configuration files are restored with this process. For example, the mail queues, the audit trail, the log files, or executable files will not be restored from a configuration backup.
- The backup file must be at the same version as the system it is being restored to.
Restoring configuration files from the Admin Console

**Note:** The appliance will reboot after the configuration files have been restored.

1. Select **Client System**.
2. Click **Browse...** and navigate to the location where the backup file is stored. Select the backup file and click **Open**. The backup file appears in the **Filename** field.
   
   You can also type the path and file name in the **Filename** field.
3. Click **Restore now**. A message appears stating that a system restore will cause a reboot of the appliance.
4. Click **Yes**. The Filename and encryption window appears.
5. [Optional] Enter an encryption key to restore the configuration backup file. Valid values include alphanumeric characters, periods (.), dashes (-), underscores (_), and spaces ( ). Enter the key again to verify.
   
   **Note:** If you did not enter an encryption key during the configuration backup, click **OK** to continue with the restore.
6. Click **OK**. When the restore is complete, a “Configuration restore successful” message appears.
7. Click **OK**. Your Admin Console is disconnected while the appliance reboots.

You have finished restoring a configuration backup from the Admin Console.
Restoring configuration files from the Sidewinder appliance

**Note:** *The appliance will reboot after the configuration files have been restored.*

1. Select **Local Sidewinder**.

2. From the list of configuration backups, select the configuration you want to restore to the appliance.

   If the configuration backup is on a flash drive, insert the flash drive in the appliance’s USB port, then click the **Refresh** button to see the configuration backup in the list.

3. Click **Restore now**. A message appears stating that a system restore will cause a reboot of the appliance.

4. Click **Yes**. The Filename and encryption window appears.

5. [Optional] Enter an encryption key to restore the configuration backup file. Valid values include alphanumeric characters, periods (.), dashes(-), underscores (_), and spaces ( ).

   Enter the key again to verify.

   **Note:** *If you did not enter an encryption key during the configuration backup, click OK to continue with the restore.*

6. Click **OK**. When the restore is complete, a “Configuration restore successful” message appears.

7. Click **OK**. Your Admin Console is disconnected while the appliance reboots.

You have finished restoring a configuration backup from the Sidewinder appliance.
Restoring configuration files from a remote system

**Note:** The appliance will reboot after the configuration files have been restored.

1. Select **Remote System (SCP)**.
2. In the **Filename** field, enter the name of the configuration backup file you are restoring.
3. Define the remote system that is receiving the configuration backup files:
   - In the **Username** field, enter the user name of a user on the remote system. If the remote system is a Sidewinder appliance, this is an appliance administrator.
   - In the **Password** field, enter the password used to authenticate the user to the remote system.
     **Note:** The appliance does not save the password.
   - In the **Hostname** field, enter the host name or the IP address of the remote system.
   - The **Port** field default is 22.
   - In the **Directory** field, enter the directory on the remote system where the configuration files are stored. If the remote system is a Sidewinder appliance, the administrator’s home directory is the default.

   This information is retained. You can change it at any time.

4. Click **Restore now**. A message appears stating that a system restore will cause a reboot of the appliance.
5. Click **Yes**. The Filename and encryption window appears.
6. [Optional] Enter the key you used to encrypt the configuration backup file. Valid values include alphanumeric characters, periods (.), dashes(-), underscores (_), and spaces ( ). Enter the key again to verify.
   **Note:** If you did not enter an encryption key during the configuration backup, click **OK** to continue with the restore.
7. Click **OK**. A warning message appears asking if you want to disconnect after starting the restore.
8. Click **Yes**. When the restore is complete, a “Configuration restore successful” message appears.
9. Click **OK**. Your Admin Console is disconnected while the appliance reboots.

You have finished restoring a configuration backup from a remote system.
Chapter 22: General Maintenance Tasks
Configuration file backup and restore

Manage configuration backup files

Use the Current local configuration backups list to move configuration backups between the Sidewinder appliance and the Admin Console computer, and to delete configuration backups.

**Note:** The Current local configuration backups list is also on the Configuration Backup tab. Any changes to this list on the Configuration Restore tab also appear on the Configuration Backup tab.

Delete a configuration backup from the appliance

1. Select **Local Sidewinder**.
2. Select a configuration backup from the list.
3. Click **Delete**. Click **Yes** to confirm the deletion.

Move a configuration backup file from the Admin Console to the appliance

1. Select **Local Sidewinder**.
2. Click **Upload**. The Upload Configuration Backup window appears.
3. Navigate to the location on the Admin Console computer where the configuration backup file is stored.
4. Select the configuration backup file and click **Open**. An “Upload successful” message appears when the upload is complete.
5. Click **OK**. The backup file appears in the list.

Move a configuration backup file from the appliance to the Admin Console

1. Select **Local Sidewinder**.
2. Select a configuration backup file from the list.
3. Click **Download**. The Save Configuration Backup window appears.
4. Navigate to the location on the Admin Console computer you want to copy the backup file to. This can include a directory on the hard drive, removable media with a drive attached to the Admin Console computer, or a network drive the Admin Console computer is connected to.
5. Click **Save**. A “Download successful” message appears when the download is complete.
6. Click **OK**.
About the Configuration Backup: Schedule tab

Use this tab to schedule automatic configuration backups. You can back up configuration files to the Sidewinder appliance, a USB flash drive, or a remote system.

![Schedule tab](image)

**Configuration Backup**

- **Enable scheduled configuration backups**
  - Configuration backups are currently scheduled daily at 1:00 am.

**Backup destination**

- **Local Sidewinder**
  - Location: Disk, USB flash drive
  - Maintain local configuration backups: Keep all backups, Keep the last backups

- **Remote system (SFTP)**
  - Username
  - Password
  - Hostname: Port 22
  - Directory

**Backup schedule**

- **Frequency**: Daily
- **Custom**
  - Minute: Hour: Day of month: Month: Day of week

**Command**: `cf config backup location=local`

**Description**: Run automated configuration backups
To schedule automatic configuration backups:

1 Select **Enable scheduled configuration backups**. If this check box is cleared, scheduled configuration backups will not occur.

2 Select the backup destination.
   - If you select **Local Sidewinder**:
     - To save the backup file on the appliance, select **Disk**.
     - To save the backup file on a flash drive inserted in the USB port on the appliance, select **USB Flash Drive**.
   - If you select **Remote System (SCP)**, define the remote system that is receiving the configuration backup files:
     - In the **Username** field, enter the user name of a user on the remote system. If the remote system is a Sidewinder appliance, this is an appliance administrator.
     - In the **Password** field, enter the password used to authenticate the user to the remote system. (The appliance does not save the password.)
     - In the **Hostname** field, enter the host name or IP address of the remote system.
     - The **Port** field default is 22.
     - In the **Directory** field, enter the directory on the remote system where the configuration files are stored. If the remote system is a Sidewinder appliance, the administrator’s home directory is the default.

   This information is retained. You can change it at any time.

3 Configure the backup schedule:
   - **Frequency** — From the drop-down list, select the frequency for exporting the file (hourly, daily, or weekly).
     - If you selected Hourly, enter the number of minutes after the hour.
     - If you selected Daily, enter the time for export.
     - If you selected Weekly, enter the time and day. You can select multiple days.
     - [Conditional] To define a custom frequency for exporting files, select **Custom** and complete the fields. Refer to man 5 crontab for options.
   - **Command** — Displays the backup that will be executed.
   - **Description** — A default description populates this field. If desired, enter a descriptive name for the task.
Activating the Sidewinder license

The Sidewinder license is automatically activated after running the Quick Start Wizard.

- When you first connect to a Sidewinder appliance using the Admin Console, a window appears displaying a list of features that are currently licensed for that appliance.

- To view a list of features currently available for the appliance and the status of each feature on your particular appliance, select Maintenance > License and click the Firewall tab. The Current Features pane displays the feature and license information.

For more information about each License window, see:
- “About the License: Contact tab” on page 709
- “About the License: Company tab” on page 709
- “About the License: Firewall tab” on page 710
- “About the License: Enrollment List tab” on page 712

If your appliance did not get licensed during initial configuration, the Sidewinder appliance will operate for seven days with a trial license. These features are licensed during the trial period:

- SecureOS
- Support
- VPN
- Failover
- Strong Cryptography

If you need to license or relicense your appliance, or if you need to license a feature after initial configuration, you can perform these procedures:

- “Licensing from an appliance connected to the internet” on page 706
- “Licensing from an appliance on an isolated network” on page 707

Note: If you relicense to a new firewall ID, you must call Secure Computing Customer Service.
Chapter 22: General Maintenance Tasks

Activating the Sidewinder license

Licensing from an appliance connected to the internet

If you are working on a Sidewinder appliance that is connected to the internet, perform this procedure to provide the necessary company information and obtain an activation key.

To license a Sidewinder appliance connected to the internet:

1 Locate the serial number for your appliance. The serial number should appear on your Activation Certificate.

2 In the Admin Console, select Maintenance > License. The License window appears.

3 Click the Contact tab and enter your company information. See “About the License: Contact tab” on page 709 for details.

4 Click the Company tab and enter your company information. See “About the License: Company tab” on page 709 for details.

5 Click the Firewall tab and enter the firewall information:

   a In the Serial Number field, type the 16-digit alpha-numeric serial number for this appliance. The serial number is located on your Sidewinder Activation Certificate.

   b In the Firewall ID field, accept the default. No selection is required. See “About the License: Firewall tab” on page 710 for details.

6 Click Submit Data. The license information is sent to the Secure Computing Corporation licensing web site using an encrypted HTTPS session. If the data is complete, the request is granted and a new activation key is written to the Activation Key field. The Current Features list updates with the new license information.
## Licensing from an appliance on an isolated network

If you are on an isolated network and do not have access to the Secure Computing activation server, perform this procedure to request an activation key.

To license an appliance on an isolated network:

1. Select **Maintenance > License**. The License window appears.
2. Click the **Firewall** tab.
3. In the **Serial Number** field, verify that it shows the 16-digit serial number located on the Activation Certificate or on your hardware platform.
4. In the **Firewall ID** field, accept the default. No selection is required.
5. [Conditional] If your Admin Console does not have web access, move to a computer that has web access. Bring a copy of the serial number and firewall ID with you.
6. Open a browser and go to the Sidewinder activation web page: https://www.securecomputing.com/cgi-bin/sidewinder-activation.cgi
7. Complete the form on the web site and click **Submit**. A confirmation screen appears.
8. Verify that the information you entered is correct. If it is not correct, use the **Back** button to return to the form and correct the information.
9. Click **Submit**. After a minute or so, a new web page appears displaying the activation key.
10. Using the on-screen instructions, save the activation key to a diskette.
   
   **Tip:** You may choose to continue following the on-screen instructions for importing the file via command line, or use the Admin Console instructions given here.

11. Insert the diskette into the Admin Console’s diskette drive.
12. Select **Maintenance > License**. The License window appears.
13. Click the **Firewall** tab.
14. Click the **Import Key...** button. The Import Key window appears.
15. Complete the Import Key window:
    - a. Select **Local File**.
    - b. In the **File** field, enter the name of the file that contains the activation key. If necessary, click **Browse...** and navigate to the file.
16. Click **OK**. The activation key is extracted from the file and appears in the **Activation Key** field.
   
   Your appliance software and any features you licensed are activated.
17 Enter information in the License windows to complete the licensing process:

a Click the **Contact** tab and enter your company information.
   See “About the License: Contact tab” on page 709 for details.

b Click the **Company** tab and enter your company information.
   See “About the License: Company tab” on page 709 for details.

c Save your changes.

---

**Configuring the Firewall License tabs**

To configure license information, select **Maintenance > License**. The License window appears. The License window contains four tabs used to collect various licensing information:

- **Contact** — See “About the License: Contact tab” on page 709 for details.
- **Company** — See “About the License: Company tab” on page 709 for details.
- **Firewall** — See “About the License: Firewall tab” on page 710 for details.
- **Enrollment List** — See “About the License: Enrollment List tab” on page 712 for details.
About the License: Contact tab

Use the Contact tab to enter contact information for the administrator of this Sidewinder appliance. This information is needed so that you can receive important customer bulletins and renewable support licenses.

To enter contact information:

1. In the **First Name** field, enter the first name of the Sidewinder administrator.
2. In the **Last Name** field, enter the last name of the Sidewinder administrator.
3. In the **Email** field, enter the e-mail address of the Sidewinder administrator.
4. In the **Primary Phone** field, enter the phone number of the Sidewinder administrator, including the area code.
5. [Optional] In the **Alternate Phone** field, enter an alternate phone number in case the first number is unavailable.
6. [Optional] In the **Fax** field, enter a fax number for your organization.
7. [Optional] In the **Job Title** field, enter the job title of the person responsible for administering this appliance.
8. [Optional] In the **Purchased From** field, enter the name of the company that sold you this appliance.
9. [Optional] In the **Comments** field, enter miscellaneous information about your site.
10. Save your changes.

About the License: Company tab

Use the Company tab to enter information about the company that has purchased this Sidewinder appliance.

To enter company information:

1. In the **Company Name** field, type the full name of the company that purchased this appliance.
2. In the **Industry Classification** drop-down list, select the classification that most closely matches your industry.
3. Fill in the requested address information fields on the Company Address tab and on the Billing Address tab. If the information is the same on both tabs, enter the information on the Company Address tab, then switch to the Billing Address tab and click **Copy From Company Address**.
4. Save your changes.
5 Click the **Firewall** tab to provide the information necessary to license your appliance. The Firewall tab appears.

![Firewall tab](image)

### About the License: Firewall tab

Use the Firewall tab to enter information about the Sidewinder appliance you are attempting to license, and to view the features available on the appliance and their licensing status.

- Do not edit the activation URL unless instructed to do so by Secure Computing Technical Support. The **Activation URL** field displays the URL of the web site to which the Sidewinder licensing information is sent.
- The Firewall ID is automatically selected. Do not change the Firewall ID unless instructed by Customer Service.
To enter Sidewinder appliance licensing information:

1  In the **Serial Number** field, type the 16-digit alpha-numeric serial number for this appliance. Include the dashes in your serial number.

   The serial number is located on your Sidewinder Activation Certificate.

2  Click **Submit Data...** to submit the license information to the Secure Computing Corporation licensing web site using an encrypted HTTPS session.

   If the data is complete, the request is granted and a new activation key is written to the **Activation Key** field. The Current Features list updates with the new license information.

3  In the **Current Features** pane, view the features currently available for the appliance and the licensing status of each feature.

   •  If a feature you want to use is currently not licensed, that feature’s window title in the Admin Console will include the words *Not Licensed*.

   •  If a feature you want to use is currently not licensed, you must obtain a different activation key in order to enable that feature.

4  [Optional] If you need to import an activation key that has been saved to a file, click **Import Key...**.

   You will typically use this button if your Sidewinder appliance or local network does not have access to the URL defined in the **Activation URL** field. See “Licensing from an appliance on an isolated network” on page 707 for instructions on obtaining a license in this situation.

5  Save your changes.
About the License: Enrollment List tab

Use the Enrollment List tab to view and modify the Host Enrollment List.

- You can identify which IP addresses are currently counted against your protected host license cap.
- You can delete IP address entries that you do not want counted against your host cap. For example, you might do this if a connection is initiated from a test system in your lab and you do not want that system to count against the host license cap.

**Note:** If you have an unlimited license, all license processing is bypassed.

To display and modify the contents of the Host Enrollment List, select Maintenance > License and click the Enrollment List tab.

You can perform the following actions:

- View the number of hosts authorized by your current Sidewinder license in the Licensed host limit field. This is your host license “cap.”
- View the current number of hosts listed in the Number of hosts in enrollment list field. This number is important because if it exceeds the number of hosts authorized by the Sidewinder license, you will be considered to be in violation of your license cap. If you have an unrestricted host license, the term Unlimited will appear in this field.
- Delete hosts from the Host Enrollment List by selecting the host and clicking Delete. To select multiple hosts to delete, hold the Shift key while selecting the hosts.
- Refresh the window to reflect updated information by clicking Refresh.

See “Protected host licensing and the Host Enrollment List” on page 713 for an in-depth explanation of the Host Enrollment List.
The Host Enrollment List is a dynamic list that is used to record each unique IP address (host) that makes an outbound connection to the Internet. The Sidewinder appliance uses this list to verify compliance with the IP address license “cap” — the portion of your Sidewinder license that dictates the number of hosts the appliance will support.

**Note:** You may ignore this section if you have an unlimited license. All license processing is bypassed if you have an unlimited license.

The Sidewinder appliance strictly enforces the maximum IP address (host) license number, meaning only the number of IP addresses authorized by the protected host license will be allowed to make connections through the appliance.

- If the number of IP addresses in the enrollment list exceeds 75% of the number allowed by your protected host license, an audit will occur informing you that you are approaching the maximum number of hosts. The audit will also display the current number of hosts and the maximum number of hosts that are allowed for your license.

- If the enrollment list becomes full:
  - Additional audits will occur each time a new IP address attempts to make a connection to the Internet, and only the IP addresses already contained in the enrollment list will be allowed to make a connection to the Internet.
  - A user attempting to make a connection using a browser will receive a standard policy denial message. A user attempting to make a connection using a non-browser application (for example, FTP), will simply be blocked and they will not receive an error message.

If you reach the host enrollment maximum and you want to allow access to additional hosts, you will need to do the following:

- Modify the host enrollment list to remove hosts entries that no longer need to be listed. See “Managing the Host Enrollment List” on page 715.

- Upgrade your license, or upgrade to a larger Sidewinder appliance.
How hosts are calculated

Any host that contains a unique IP address and that initiates a connection from a non-Internet burb is counted as a new host and added to the Host Enrollment List.

The manner in which remote hosts access the Sidewinder appliance may affect the host count. For example:

- Remote hosts that use dynamic addressing rather than static addressing may have multiple IP addresses added to the Host Enrollment List.

  **Note:** If you have control over the dynamic host server, you might want to control the range of IP addresses used for remote hosts, to minimize the impact of dynamic IP addresses on the enrollment list.

- Hosts accessing the appliance via a VPN will be added to the Host Enrollment List if the VPN uses proxies to move the traffic from a non-Internet burb to another burb. Figure 297 illustrates this idea.

![Figure 297: Determining which VPN clients count against the host license cap](image)

The appliance counts total hosts connecting to the Internet, not the number of hosts connecting to the Internet at one time. It is important to understand the distinction. Assume the following:

- You have a 25-host license.
- You have 30 hosts.
- No more than 20 hosts are online at any one time.

You will still exceed the license cap because each host that goes online has their IP address added to the Host Enrollment List. Eventually a 25th host will be added to the Host Enrollment List, and the 26th host will be detected by the appliance, putting you over the limit.
Managing the Host Enrollment List

Use the Enrollment List tab to view and modify the Host Enrollment List.

- You can identify which IP addresses are currently counted against your protected host license cap.
- You can delete IP address entries that you do not want counted against your host cap. For example, you might do this if a connection is initiated from a test system in your lab and you do not want that system to count against the host license cap.

To display and modify the contents of the Host Enrollment List, select Maintenance > License and click the Enrollment List tab.

You can perform the following actions:

- View the number of hosts authorized by your current Sidewinder license in the Licensed host limit field. This is your host license “cap.”
- View the current number of hosts listed in the Number of hosts in enrollment list field. This number is important because if it exceeds the number of hosts authorized by the Sidewinder license, you will be considered to be in violation of your license cap. If you have an unrestricted host license, the term Unlimited will appear in this field.
- Delete hosts from the Host Enrollment List by highlighting the host and clicking Delete. To select multiple hosts to delete, hold the Shift key while selecting the hosts.

**Note:** You can update the contents of the Host Enrollment List field by clicking Refresh.

Consider the following information when deleting entries from the enrollment list:

- If the host you delete has a current connection through the appliance, that connection will be preserved.
- If the host severs the connection and attempts a new connection, the new connection request may or may not be approved.
- A new connection request will be permitted only if there is still room available within the enrollment list.

You can use the System Responses window to configure to have e-mails sent when the enrollment list reaches the maximum number allowed: Select Monitor > System Responses, then select host license exceeded and click Modify. See “About the Modify System Responses: Event tab” on page 412 for more information.
Software management

The Sidewinder appliance comes installed with the latest software available at the time. Use the Software Management window to keep your appliance current with updates from Secure Computing. You can also uninstall updates or revert to a previous configuration.

Understanding software management

Updates can include improvements and enhancements to the Sidewinder software, as well as updates to optional features. The types of software updates are:

- **Base** — A major release with significant enhancements and added functionality.
- **Patch** — Released periodically and contains software fixes and/or new features. General release patches must be installed sequentially.
- **Vendor Patch** — Contains fixes, updates, or new features specific to the anti-virus or anti-spam add-on modules. Only install the patch if you have the feature enabled. Patches are to be installed sequentially.
- **Upgrade** — Brings your appliance to a new base version and includes significant new features.
- **Hotfix** — Contains an issue-specific fix, and should be installed only if it addresses a current problem.
- **Restricted** — Distribution is restricted to identified customer(s) to solve a particular defect.
- **E-Patch** — Sent to a particular customer on an as-needed basis to determine if the fix corrects an identified defect for a particular version of the product. If the fix works, it is then converted to a hotfix or incorporated into a full product release.

Software management includes these actions:

- “Loading and installing” on page 717
- “Uninstalling and rolling back” on page 717
- “Re-installing and re-imaging” on page 718
Loading and installing

Periodic software updates, called packages, are available on Secure Computing’s FTP site.

• **Load** — You load a package onto the appliance. This moves the package from the FTP site to the appliance, but does not install it.
  – Packages can be loaded manually, at automatic intervals, or at scheduled times using the Manage Packages and Load Packages tabs.
  – Secure Computing’s FTP site is the default location for software packages. You might configure a different location to load packages from if you have appliances on an isolated network, or to speed up downloads to several appliances.

• **Install** — Packages that are loaded on the appliance can then be installed on the appliance using the Manage Packages tab.
  – Packages can be installed manually or automatically at a scheduled time. Packages can be installed individually or several at a time.
  – Key package information is provided, such as dependencies with other packages, whether a reboot is required, and whether the package can be uninstalled.

Uninstalling and rolling back

If you are not satisfied with an update, you can uninstall the package or revert to the previous configuration.

• **Uninstall** — Package uninstalls are performed on the Manage Packages tab.
  – The Uninstallable column states if a package is uninstallable.
  – Any configuration changes you make after the package was installed remain after the package is uninstalled.
  – Packages can be uninstalled manually or automatically at a scheduled time. Packages can be uninstalled individually or several at a time.
  – Uninstalled packages remain loaded on the appliance.

• **Rollback** — Use the Rollback tab to restore the appliance to a previous state. Rolling back is an option if a package is not uninstallable.
  – Any configuration changes made after the package was installed are lost. A rollback reverts the appliance to the state just before the package was installed. Therefore, rolling back is a recommended recovery option for only a short time after a package installation.
  – A rollback can be performed manually or automatically at a scheduled time.
  – A rollback always requires a reboot.
  – The tab displays what patch level the appliance will roll back to and the date and time the patch was loaded.
Re-installing and re-imaging

More serious issues might require you to re-install or re-image your Sidewinder appliance.

- **Re-install from the virtual CD** — Use the virtual CD function to re-install the Sidewinder software. Re-installing from the virtual CD puts the appliance in its original unconfigured state.
  
  For information and instructions, see “Re-installing your appliance from the virtual CD” on page 830.

- **Re-install from a CD-ROM** — Re-installing from a CD-ROM erases the appliance’s hard drive and re-installs the software. Re-installing from a CD-ROM is a more disruptive procedure. It should be done only when other methods cannot fix the issue and only if instructed by Secure Computing Technical Support.
  
  For information and instructions, see “Re-installing your appliance from a CD-ROM” on page 832.

To manage Sidewinder software, select **Maintenance > Software Management**. The Software Management window appears. The Software Management window has three tabs:

- “About the Software Management: Manage Packages tab” on page 719.
- “About the Software Management: Load Packages tab” on page 725.
- “About the Software Management: Rollback tab” on page 727.
About the Software Management: Manage Packages tab

To manage software packages for the Sidewinder appliance, select Maintenance > Software Management. The following window appears:

Use this tab to load, install, and uninstall packages on the appliance.

You can perform these tasks:

- “Viewing available packages” on page 720
- “Sorting the Manage Packages table” on page 720
- “Loading, installing, and uninstalling packages now” on page 721
- “Scheduling automatic installs and uninstalls” on page 723
- “Viewing package information and activity logs” on page 723
- “Enabling e-mail notification” on page 724
**Viewing available packages**

To populate the table with packages that are available for downloading, click **Check for Updates**. Packages appear in the table with a status of Available. They are not yet installed.

Available packages are loaded from the Secure Computing FTP site, or from another site you designate on the Load Packages tab.

Use the Load Packages tab to configure automatic checking and loading, and to change the location where packages are downloaded from.

**Sorting the Manage Packages table**

To sort the table of packages:

- Select which package types and statuses appear in the table: Click **View Options** and make your selections in the pop-up window.
- Sort the Package Name column in ascending or descending order by clicking the column heading.
- Sort other columns by right-clicking a column heading and selecting a filter option from the pop-up list.
- Use the **Find** field to search for a specific element(s) in the list. Type your search criteria, and only packages with matching elements will appear in the list.
Loading, installing, and uninstalling packages now

Use the Manage Packages table to load, install, or uninstall packages immediately.

• The buttons that appear depend on the status of the package selected in the table:

  Download
  ![Download button](image)
  ![Find field](image)
  (Filtered View)

  Install
  ![Install button](image)
  ![Find field](image)
  (Filtered View)

  Uninstall
  ![Uninstall button](image)
  ![Find field](image)
  (Filtered View)

• You can select more than one package to manage.
  – The packages you select must have the same status.
  – Select several consecutive packages by selecting the first package, then pressing the **Shift** key while selecting the last package. To select several non-consecutive packages, press the **Ctrl** key as you select each desired package.
To download a package to the Sidewinder appliance:

1. Select a package in the table with the status of Available.
2. Click Download. A “successfully loaded” message appears and the package status changes to Loaded.

To install a package:

1. Select a package in the table with the status of Loaded.
2. Click Install. The Install window appears.
   
   If the package has dependencies, the dependencies appear in a lower table.
   
   • If a dependency is loaded, it is installed at the same time as the selected package. If you do not want to install the dependency, click Cancel. The selected package and dependency will not be installed.
   
   • If a dependency is not loaded, a message states that you must load the dependency before installing the selected package. Click Cancel to exit the Install window.

3. Select Install now.
4. [Optional] If the package requires a reboot, select whether you want the reboot to occur after installation.
   
   • If you select Activate packages after installation, the appliance will reboot after you click OK and the package is installed.
   
   • If you clear Activate packages after installation, the appliance will not reboot after you click OK and the package is installed. The installed package will not be active until the appliance is rebooted.

5. Click OK.

The package appears in the Manage Packages table with a status of Installed.

To uninstall a package:

1. Select a package in the table with the status of Installed.
2. Click Uninstall. The Uninstall window appears.
   
   If the package has a dependency, the dependency appears in a lower table and will be uninstalled at the same time as the selected package. If you do not want to uninstall the dependency, click Cancel. The selected package and dependency will not be uninstalled.

3. Select Uninstall now.
4. Click OK.

The package appears in the Manage Packages table with a status of Loaded.
Scheduling automatic installs and uninstalls

To schedule packages for automatic installs and uninstalls:

1. Click Schedule. The Schedule Install/Uninstall window appears.
   - Any package with a status of Loaded appears in the Select packages to install list.
   - Any package with a status of Installed appears in the Select packages to uninstall list. (If a package cannot be uninstalled, it does not appear.)
2. Select the packages you want to install or uninstall.
3. Select Schedule for and select a date and time for the action to take place.
4. Click OK.

The selected packages appears in the Manage Packages table with a status of Install scheduled on date or Uninstall scheduled on date.

To cancel a scheduled install or uninstall:

1. Click Schedule.
2. Select Unschedule All.
3. Click OK.

Viewing package information and activity logs

To view information and activity logs for a single package:

1. In the Manage Packages table, select a package.
2. Click View Package Details.

   View Package Details

   The Details window appears.
   - The Readme tab states what changes the package is making.
   - The Package Log tab shows all load, install, and uninstall activities for the package.

To view all package installation activities on this appliance:

Click View Log. The View Log window appears.

The View Log lists detailed histories of all package installs and uninstalls on the appliance, including programs run, package parameters, and errors.
Enabling e-mail notification

To enable e-mail notification of software management activities:

1  Select Enable e-mail notifications for install, uninstall, automatic load and rollback.
2  In the E-mail Address field, enter the e-mail address of the person who will be notified. The default address is the administrator of this appliance.
3  Save your changes.
About the Software Management: Load Packages tab

To manually or automatically load software packages onto the Sidewinder appliance, select **Maintenance > Software Management**, then click the **Load Packages** tab. The following window appears:

![Software Management: Load Packages tab](image)

Use this tab to automatically or manually load packages on the Sidewinder appliance. You can also configure a different site for the packages to be loaded from.

To configure your appliance to load packages automatically:

1. Select an automatic action:
   - **Automatically check for and load packages** — To find available packages and load them on the appliance, select this option. Packages appear in the Manage Packages table with a status of Loaded. They can be installed.
     This option works well if you regularly schedule package installations.
   - **Automatically check for available packages** — To find available packages, select this option. A list of packages appears in the Manage Packages table with a status of Available. They can be loaded.
     This option works well if downloading to your appliance is slow, or if you do not want to store and manage packages you will not use.
2 Identify the package site:
   • **Load using** — Select the protocol used to transport the package.
   • **Directory** — The path name on the site where the package is located.
   • **Host** — The host name or IP address of the site where the package is located.
   • **User Name** — The user account defined on the site.
   • **Port** — The number of the port used to access the site.
   • **Password** — The password to validate you to the site.
   • **Confirm Password** — Verify the password.

   *Note: To restore the system default values to these fields, click Restore Defaults.*

3 From the **Frequency** drop-down list, select how often you want the appliance to check for available packages.

   *Note: Use `cf crontab` to designate a specific time for the action to take place. See Appendix A, Command Line Reference.*

4 Save your changes.

To manually load a package:

1 Click **Perform Manual Load Now**. The Load Packages: Manual Load window appears.

2 Identify the package and its location:
   • **Load packages from** — Select the location of the package you are loading to the appliance. It can be an FTP or HTTPS site, a CD-ROM, or a file.
   • **Directory** — The path name where the package is stored.
   • **Packages** — The name of the package you are loading. If you are loading more than one package, separate each package name with a comma. Package names contain only alphanumeric characters. No spaces are allowed in package names.
   • **Host** — [Conditional] The host name of the FTP or HTTPS site where the package is located.
   • **User Name** — [Conditional] The user account defined on the FTP or HTTPS site.
   • **Port** — [Conditional] The number of the port used to access the FTP or HTTPS site.
   • **Password** — [Conditional] The password to authenticate to the FTP or HTTPS site.
   • **Confirm Password** — [Conditional] Verify the password.

3 Click **OK**. Click **Yes** to confirm the load.

The package appears in the Manage Packages tab with a status of Loaded. The package can be installed.
About the Software Management: Rollback tab

To roll back the Sidewinder appliance to a previous state, select **Maintenance > Software Management**, then click the **Rollback** tab. The following window appears:

![Rollback tab](image)

Use the Rollback tab to revert the Sidewinder appliance to a previous state. The table shows which packages will be on the appliance after the rollback.

- Any configuration changes made after the last package was installed are lost. A rollback reverts the appliance to the state just before the package was installed. Therefore, rolling back is a recommended recovery option for only a short time after a package installation.
- A rollback requires a reboot.
To roll back immediately:

1 Click **Rollback Now**. A warning message appears stating that configuration changes will be lost and that the appliance will reboot.

2 Click **Yes** to continue. The appliance reboots.

To schedule the rollback for a future time:

1 Select **Schedule rollback for** and select the desired date and time.

2 Save your changes. A warning message appears stating that configuration changes will be lost.

3 Click **Yes** to schedule the rollback.
Registering with CommandCenter

Use the CommandCenter Registration window to register this Sidewinder appliance to a CommandCenter Management Server.

- If you chose to auto-register to CommandCenter during initial configuration of this Sidewinder appliance, do not register with CommandCenter here. Use the Sign Up Firewalls dialog in the CommandCenter Configuration Tool to initiate rapid deployment.

- A Sidewinder administrator account named ccfwadmin is automatically created when you register with CommandCenter. If you already have an administrator account with that name, it will be overwritten.

To register this appliance with CommandCenter, select Maintenance > CommandCenter Registration. The CommandCenter Registration window appears.

![CommandCenter Registration window](image)

**Figure 301:** CommandCenter Registration window with Configure backup servers selected.

Use this window to register this Sidewinder appliance to a CommandCenter Management Server.

To register this appliance:

1. In the **FQDN** field, enter the fully qualified domain name of the Management Server that will manage this appliance. If you are also using backup servers, use the fully qualified domain name of the active Management Server.

2. In the **IP Address** field, enter the IP address of the Management Server.
3 [Optional] If you are using a High Availability Management Server configuration, select the **Configure backup servers** check box.

a In the **Backup Server # Name** fields, enter the fully qualified domain name of each Management Server acting as a backup to the active Management Server.

b In the **IP Address** fields, enter the IP address of the corresponding backup servers.

4 Click **Register with the CommandCenter Now**. Click **Yes** to confirm your changes. The Authentication window appears.

5 Enter the user name and password of the CommandCenter administrator, then click **OK**.

A “registration succeeded” message appears.

6 Click **OK**.

To complete registration, go to the Management Server Configuration Tool. See the *CommandCenter Administration Guide* for more information.
Federal Information Processing Standard (FIPS) 140-2 is a standard that describes the U.S. federal government requirements for a cryptographic module used in a security system. Select this option to configure settings that make a Sidewinder appliance FIPS 140-2 compliant. For more information on how enabling this option affects the Sidewinder appliance, see the FIPS application note at [www.securecomputing.com/goto/appnotes](http://www.securecomputing.com/goto/appnotes).

**Note:** This option is appropriate only for organizations that are explicitly required by the U.S. federal government to be FIPS 140-2 compliant.

**Figure 302: Enforcing FIPS**

To enable FIPS:

1. Select Maintenance > **FIPS**. The FIPS check box appears in the right pane.
2. Select **Enforce US Federal Information Processing Standard**.
3. Save the configuration change.
4. Select Maintenance > **System Shutdown** and reboot the appliance to the Operational kernel to activate the change.
CHAPTER 23

One-to-Many Clusters

In this chapter...

When to use One-to-Many ...........................................................734
Configuring a One-to-Many cluster ..............................................736
How to manage a One-to-Many cluster........................................742
Modifying an existing One-to-Many cluster ..............................744
The Sidewinder One-to-Many (OTM) configuration involves maintaining a synchronized policy on two to five appliances with management interfaces in the same subnet. This configuration is most common in large, high-volume networks that place their Sidewinder appliances behind load balancers. In OTM, changes you make to your primary appliance are automatically replicated to each secondary appliance immediately. From an administrative perspective, the primary and its secondaries can be managed as a single unit, or cluster.

A network diagram showing the typical placement of an OTM cluster is depicted in Figure 303.

**Note:** When implementing One-to-Many, the preferred setup is to configure each appliance with a dedicated cluster burb, allowing all communication between cluster members to be contained within its own burb.

In an OTM cluster, all of the appliances reside in the same network and are either backups of one another or are being used to share the network load. In this scenario, each appliance will have the same basic configuration, excluding host names and IP addresses.
In the following example, there are three appliances protecting a local network. Network traffic is load balanced across the appliances using a load-balancing tool, similar to the configuration depicted in the previous figure.

Because each appliance will be configured almost identically, the One-to-Many feature simplifies the management process. Any configuration changes you make to the primary will automatically be implemented on each of the secondaries, ensuring that all of your cluster members remain synchronized.

The typical scenario requires the following:

- A cluster Sidewinder appliances running at the same version (clusters can contain a minimum of two members and a maximum of five members)
- A load balancer
- The IP addresses used to access each appliance must all reside in a burb of the same name.

For example, in the sample network configuration shown in the following figure, if you are accessing the appliances from the internal network, all IP addresses used to access them must reside in a burb named *internal*.

Figure 304: Sample network configuration for One-to-Many

![Network Diagram](image-url)
Chapter 23: One-to-Many Clusters

Configuring a One-to-Many cluster

The following procedures explain how to initiate a One-to-Many relationship between multiple Sidewinder appliances.

What you should know before configuring One-to-Many

Note the following considerations when using One-to-Many:

- All participating cluster members must have matching configurations before they can join the cluster:
  - All appliances must be at the same version. (This does not include hotfixes or optional feature patches.)
  - All burb names must be identical.
  - DNS services must be configured identically.
  - Mail services must be configured identically.
  - The corresponding burbs and interfaces on each cluster member must all be on the same networks. For example:

<table>
<thead>
<tr>
<th>Burb</th>
<th>Primary A</th>
<th>Secondary B</th>
<th>Secondary C</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal</td>
<td>10.1.182.15</td>
<td>10.1.182.25</td>
<td>10.1.182.35</td>
</tr>
<tr>
<td>External</td>
<td>192.168.183.15</td>
<td>192.168.183.25</td>
<td>192.168.183.35</td>
</tr>
</tbody>
</table>

- Managing a cluster:
  - You can define only one primary for each cluster. Connect to this primary to configure all appliances in the One-to-Many cluster.

  **Note:** The only times you should connect directly to a secondary are to configure DNS and to promote that secondary to primary.

  - Most configuration details are synchronized, but a few features can be customized. For details on configuring non-synchronized areas for secondaries, see “How to manage a One-to-Many cluster” on page 742.
  - If you have VPNs configured, you must ensure that your load balancers are configured to send all traffic for a given VPN security association to a single appliance within the cluster instead of distributing it among the cluster members.

- One-to-Many clusters cannot participate in other multi-box configurations:
  - An appliance that is part of an HA cluster cannot participate in a One-to-Many cluster.
Chapter 23: One-to-Many Clusters

Configuring a One-to-Many cluster

Configuring a dedicated cluster burb for each appliance

Before configuring One-to-Many, Secure Computing strongly recommends configuring a dedicated cluster burb on each appliance that will join the cluster. Using a dedicated cluster burb separates traffic passing policy updates among cluster members from the appliance’s standard traffic. The IP addresses for the dedicated cluster burb must all be in the same subnet.

To add and configure the cluster burb:

1. Ensure that each appliance has an interface that can be dedicated to internal One-to-Many communication.

2. In the Admin Console, select Network > Burb Configuration and create a new burb. Note the following:
   - Select a name that makes it easily identifiable, such as cluster. The burb name for the cluster burb must be the same for each cluster member.
   - Select Respond to ICMP echo and timestamp. This is required for communication among the cluster members. The other connection options are optional.

   See “Configuring burbs” on page 452 for more information.

3. Click Save.

4. Go to Network > Interfaces to assign the cluster burb and an address to the appropriate interface. (Be sure to select Enable Interface.) All cluster burb address must be in the same subnet.

   See “Configuring interfaces” on page 456 for more information.

5. Click Save. You do not need to reboot at this time.

6. Repeat these steps for each appliance that will be participating in the One-to-Many cluster.

These burbs are now ready to be used for communicating status and policy information among the cluster. Verify that they are cabled correctly by pinging from one appliance to another.
Configuring the primary in a new One-to-Many cluster

The first step in creating a One-to-Many cluster is to establish a primary.

To configure your primary:

**Important:** It is recommended that you perform a system backup before configuring One-to-Many. See “Re-install and recovery options” on page 825 for details.

1. Start the Admin Console and log into the appliance that will become the primary.
2. Select **Maintenance > Cluster Wizard**.
3. Click **Launch Cluster Wizard**. The Welcome window appears.
4. Click **Next**.
5. Select **Create New Cluster** and click **Next**.
6. Select **One-to-Many Cluster** and click **Next**.
7. In the One-to-Many Communication Configuration window, do the following:
   a. In the **Cluster Burb** field, select the burb that will be used for intra-cluster policy communication. This is generally a dedicated burb. For information on creating a dedicated cluster burb, see “Configuring a dedicated cluster burb for each appliance” on page 737.
   b. In the **Primary IP Address** field, expand the drop-down list and select the IP address that corresponds to the cluster burb.

   **Note:** You will provide this IP address when you register your secondaries to this OTM cluster. You must have network connections from this IP address to the dedicated cluster burbs on your secondaries.

8. Click **Next**. The Cluster Wizard Summary window displays a list of the actions that will be performed when you click **Execute**.

   To change your configuration before executing, click **Back** to navigate to the appropriate window(s) and make the necessary changes.

   When you are satisfied with the summary of changes, click **Execute**. A progress bar appears while the configuration changes are made. If the transition is successful, the Success window appears displaying the new state.

9. Click **Finish**.

You now have a One-to-Many primary. The Admin Console refreshes and displays the new OTM tree layout, described in “How to manage a One-to-Many cluster” on page 742.

To add an additional cluster member, see the following section, “Adding a secondary”.

Adding a secondary

Once you have created a One-to-Many cluster with a primary, you can add one or more secondaries to be managed. Adding a secondary to a One-to-Many cluster is a two-step process:

1. Create a reservation for the secondary.
2. Use the Cluster Wizard to join the secondary to the cluster.

See the following sections for instructions.

Creating a secondary’s reservation

1. Connect to the primary One-to-Many cluster member, and then click **One To Many Management** in the Admin Console tree. The One To Many Management window appears.

   ![One To Many Management window](image1)

   **Figure 305:** One To Many Management window

   2. Click **New**. The Add Cluster Member window appears.

   ![Add Cluster Member window](image2)

   **Figure 306:** Add Cluster Member window
3 Enter the secondary’s fully-qualified domain name, cluster Burb IP address, and registration key.

**Note:** When you use the Cluster Wizard to join this secondary to the cluster, you will need to enter the host name and registration key exactly as you entered it here.

4 Click **Add** to save your changes.

You now have a reservation and can use the Cluster Wizard to join the secondary to this cluster.

You can also use the One-to-Many window to do the following:

- **View the status of a One-to-Many cluster** — To view the status of a One-to-Many cluster, click **Cluster Status**.

  **Note:** You must connect to a primary to view cluster status. Connecting to a secondary to check cluster status will not provide accurate information.

Information provided on the window includes:

- **Member Name** — This column lists the name of each appliance that is included in the One-to-Many cluster.

- **Registration State** — This column indicates whether the cluster member is **Registered** (synchronized and running), **Unregistered** (running but not registered and synchronized), or **Inactive** (registered, but has not yet been initially synchronized with the primary).

- **Communications** — This column indicates whether a remote cluster member is responding. A value of **Up** indicates that communication is available. A value of **Down** indicates that the cluster member is offline or otherwise not responding.

- **Policy State** — This column indicates if the secondary’s policy is synchronized with the primary. A value of **Up to date** indicates that the secondary is synchronized with the primary. A value of **Not up to date** indicates that the secondary is not synchronized with the primary.

- **Modify the primary IP address** — To change the primary IP address, click **Modify Primary Address**. The Modify Primary Address window appears. For information on modifying the IP address to determine which appliance is the primary, see “Changing the primary in a One-to-Many cluster” on page 746.
Using the Cluster Wizard to join the existing cluster

Once you finish adding the secondary’s reservation as described in the previous section, join the appliance to an existing One-to-Many cluster by following the steps below.

1. Connect the Admin Console to the appliance that will be joining the One-to-Many cluster as a secondary.
2. Select **Maintenance > Cluster Wizard**.
3. Click **Launch Cluster Wizard**. The Welcome window appears.
4. Click **Next**.
5. Select **Join Existing Cluster** and click **Next**.
6. Select **One-to-Many Cluster** and click **Next**.
7. In the Gathering information to join cluster window, configure the following fields:
   a. In the **Primary IP Address** field, type the IP address in the cluster burb of the primary to which you are registering the secondary. This is the same address you selected in step 7 on page 741.
   b. In the **Cluster Member Name** field, verify the host name of the secondary that you are registering. This must match the name you entered when you created the secondary’s reservation. This field is read-only
   c. In the **Registration Key** field, enter the registration key for this One-to-Many cluster. This is the unique, one-time key that you entered when you created the secondary’s reservation.
8. Click **Next**. The Cluster Wizard Summary window displays a list of the actions that will be performed when you click **Execute**.
   If you want to make changes to your configuration before executing, click **Back** to navigate to the appropriate window(s) and make the necessary changes.
   When you are satisfied with the summary of changes, click **Execute**. A progress bar appears while the configuration changes are made. If the transition is successful the Success window appears, displaying the new state. The secondary is now synchronized with the primary.
9. Select the new cluster member in any branch.
   “This firewall not registered” appears in the right pane.
10. Click **Check Now**.
    The new cluster member is registered as part of the OTM cluster and all branch contents are visible.

Add other secondaries using the same procedures. When the cluster is complete, see the following section, “How to manage a One-to-Many cluster”.
How to manage a One-to-Many cluster

The Admin Console tree structure is slightly different in a One-to-Many cluster environment. When you configure One-to-Many, all cluster members are managed within a single Admin Console connection to the primary. All the secondaries’ icons are removed from the tree.

Areas within the primary connection that are synchronized (that is, areas in which the information for all cluster members must be the same) will appear as a single tree option within the primary. When you modify information within those areas, it will automatically be applied to all of that cluster’s members.

Information specific to individual appliances within the One-to-Many cluster that cannot be synchronized among the cluster members (such as Configuration Backup and Audit) include a sub-folder within the primary that provides an icon for each cluster member. To modify these features, select the individual icon and make the changes. These changes will apply only to the cluster member that you have selected and will not be overwritten.

**Important:** DNS configuration is an exception to this structure. To configure this service on a secondary, you will need to add the secondary server icon and connect directly to that appliance. Also, use the Sidewinder File Editor to edit files. This ensures that changes will be synchronized. All other areas should be configured using the primary connection to avoid being overwritten.

The following figure demonstrates the difference between individually configured areas of the One-to-Many cluster (Configuration Backup and Date and Time) and a synchronized area of the One-to-Many cluster (Burb Configuration).

![Figure 307: Example of an individually configured area](image)

To modify individually configured information for a particular cluster member, simply select that member’s icon and make the desired changes. Changes to an individual member will be applied only to that appliance and will not be overwritten by changes made to the other cluster members.

The following tables summarize which features are synchronized and which features are configured individually in a One-to-Many cluster.
Chapter 23: One-to-Many Clusters

How to manage a One-to-Many cluster

Features that are *synchronized* in a One-to-Many cluster

- IPS Attack Responses
- System Responses
- Audit (health monitoring, filters)
- Rules
- Rule Elements
- Application Defenses
- Network Defenses
- Burb Configuration
- VPN Configuration
- Routing
- Administrator Accounts
- Reconfigure Mail/sendmail
- UPS

Features that are *configured individually* in a One-to-Many cluster

- Dashboard
- Service Status
- Interfaces
- DNS/Reconfigure DNS
- Configuration Backup
- Date and Time
- License
- Software Management
- System Shutdown
- File Editor

Note the following:

- Most areas are configured by connecting to the primary. The primary pushes the policy updates to its secondaries when there is a configuration change or a reboot.

- For audit, the health monitor setting is pushed from the primary to the other secondaries. Audit filters are also synchronized and should be created on the primary. However, to view real time audit using the Admin Console you must connect directly to each node to see its audit.

- The following areas require connecting directly to the secondary:
  - **Maintenance > Reconfigure DNS**
  - **Network > DNS**

All other features listed in the second table are configured using the primary connection.

To connect directly to the secondary, you will need to add the secondary to the Admin Console and then connect to the secondary using that new icon. (This is because the icon for the secondary is removed from the Admin Console tree branch when it is successfully added to a cluster.) For information on adding a Sidewinder appliance icon to the Admin Console, see “Adding an appliance to the Admin Console” on page 31.
Occasionally, changing network or hardware requirements will require you to make changes to your OTM cluster. You may need to remove members from the cluster or convert an existing secondary into the primary.

**Important:** Always use the Cluster Wizard to remove and add cluster members. Using any other method may have unexpected results.

### Removing members from a One-to-Many cluster

The following procedures allow you to delete one or more members from a One-to-Many cluster. The deleted cluster members are automatically converted to stand-alone appliances.

#### Removing a secondary from a One-to-Many cluster

Repeat this procedure on each secondary you want to remove.

To remove a secondary from a One-to-Many cluster:

1. Using the Admin Console, connect to the primary.
2. Select **One To Many Management**. The One To Many Cluster Management window appears.
3. In the One-to-Many Cluster Members list, select the secondary that you want to remove from the cluster, and click **Delete**. You will be prompted to confirm your decision. Click **Yes**.

The appliance is no longer a part of the One-to-Many cluster and must be managed by making a direct connection to that appliance. Changes are no longer replicated from the cluster to that appliance.

**Note:** To begin managing that stand-alone appliance, create a new Sidewinder appliance icon for it in the Admin Console tree. See “Adding an appliance to the Admin Console” on page 31 for more information.
Demoting the primary to a standalone

To demote the primary and change it to a standalone:

**Note:** You must remove all of the secondaries from the One-to-Many cluster before you can access the Cluster Wizard to demote the primary. If you remove a primary from a cluster without using the Cluster Wizard, you must re-install it before returning it to your network.

1. Connect to the One-to-Many cluster using the Admin Console.
2. Select the **One to Many Management** node.
3. Click **Change State to Standalone**. The Cluster Wizard Welcome window appears.
4. Click **Next**.
5. Select **Change To Standalone**.
6. Click **Next**. The Cluster Wizard Summary window displays a list of the actions that will be performed when you click **Execute**.

When you are satisfied with the summary of changes, click **Execute**. A progress bar appears while the configuration changes are made. If the transition is successful, the Success window appears displaying the new state.

When the primary is successfully demoted, it will be a standalone appliance.
Changing the primary in a One-to-Many cluster

Under certain circumstances, you may need to designate a secondary as the primary (for example, if the primary will be down indefinitely).

To transfer primary status to a secondary:

**Note:** When you change the primary, all of the secondaries will be rebooted.

1. In the Admin Console, add a new Sidewinder appliance icon for the secondary that you want to become the primary by clicking the New Appliance icon and entering the appropriate information. This is necessary because when you register a secondary to a One-to-Many cluster, the icon for the secondary is removed by default.

   **Note:** For information on adding a Sidewinder appliance to the Admin Console, see “Adding an appliance to the Admin Console” on page 31.

2. Connect directly to the secondary by clicking the icon that you added in the previous step. You will receive a warning message stating that you should only modify information on the primary. Ignore this message.

3. Select One To Many Management. The One To Many Management window appears.

4. In the One To Many Cluster Member window, select Modify Primary Address. The Modify Primary Address window appears.

5. In this window, expand the Cluster Burb drop-down list and select the cluster IP address for this appliance.

6. In the One to Many Primary IP Address drop-down list, select the cluster IP address for this appliance.

7. Click OK. You will be prompted to verify your decision. Click Yes to transfer primary status to this secondary.

The secondaries that will be managed by the new primary are rebooted at this time. When the secondaries finish rebooting, they will recognize the new primary.
In this chapter...

How High Availability works .......................................................... 748
HA configuration options .................................................................. 750
Configuring HA ........................................................................... 753
Understanding the HA cluster tree structure ................................ 765
Managing an HA cluster ............................................................... 766
How High Availability works

Two Sidewinder appliances configured for High Availability are known as an HA cluster. The clusters can be configured in either of these ways:

- Load-sharing, where both the primary and secondary appliance actively process traffic.
- Failover, where the standby does not process traffic unless called on to take over if the primary becomes unavailable.

As shown in Figure 308, configuring an HA cluster requires at least three burbs for each appliance: an internal burb, an external burb, and a heartbeat burb. A separate heartbeat burb allows all HA cluster-specific traffic (including the heartbeat message as well as any stateful session IP packet filter traffic) to pass between the HA cluster appliances in its own burb, and does not impact regular network traffic.

HA cluster appliances must have interfaces that reside in the same networks. The heartbeat burbs of the HA pair must be directly connected with a cross-over cable or a straight-through cable (if using em or bge interfaces).

*In a load-sharing HA cluster, the internal and external shared cluster addresses are shared between appliances.

In a failover HA cluster, they are assigned to the primary.

Figure 308: Basic HA configuration
To implement an HA cluster in your network, you will need one additional *shared cluster* address for each network. This address represents the cluster rather than an individual interface. The table below summarizes the IP addresses needed for this HA configuration.

<table>
<thead>
<tr>
<th>internal burb</th>
<th>external burb</th>
<th>heartbeat burb</th>
</tr>
</thead>
<tbody>
<tr>
<td>primary IP</td>
<td>aaa.aaa.aaa.1</td>
<td>bbb.bbb.bbb.1</td>
</tr>
<tr>
<td>secondary/standby IP</td>
<td>aaa.aaa.aaa.3</td>
<td>bbb.bbb.bbb.3</td>
</tr>
<tr>
<td>shared cluster address</td>
<td>aaa.aaa.aaa.5(^a)</td>
<td>bbb.bbb.bbb.5(^a)</td>
</tr>
</tbody>
</table>

\(^a\) In a load-sharing HA cluster, the internal and external shared cluster addresses are *shared* between Sidewinder appliances. In a failover HA cluster, they are assigned to the primary.

In this example, all users in the internal or external network must use the cluster address (aaa.aaa.aaa.5 or bbb.bbb.bbb.5, respectively) as its network gateway. Only system administrators should know about the other IP addresses. The same concept applies for DNS names.

**Tip:** When configuring an existing single Sidewinder configuration to become an HA cluster, consider using the existing interface addresses as the cluster addresses and getting new IP addresses for the actual NICs. This lessens the impact on your users, who will not have to change their perception of the “Sidewinder” address.
You can configure HA clusters in either of these ways:

- Load sharing, where both the primary and secondary appliance actively process traffic. See “Load-sharing HA” on page 750.
- Failover, where the standby does not process traffic unless called on to take over if the primary becomes unavailable. See “Failover HA” on page 751.

### Load-sharing HA

Load-sharing HA, also referred to as active-active HA, consists of two Sidewinder appliances that actively process traffic in a load-sharing capacity. When a secondary is registered to an HA cluster, synchronized areas will be overwritten to match the primary. (To determine which areas are synchronized, see “Managing an HA cluster” on page 766.)

Both Sidewinder network interfaces maintain their unique IP address, the shared cluster address, and any aliases assigned to the cluster. The appliances are then able to coordinate traffic processing on a single shared IP address using a multicast Ethernet address. Each connection (and the packets associated with that connection) is handled by the same appliance. The communication to coordinate load-sharing passes between appliances on the heartbeat burb. To configure load-sharing HA, both appliances must have the same hardware configuration (e.g., CPU speed, memory, active NICs).

In a load-sharing HA configuration, only the primary is assigned the cluster address for the heartbeat burb. The two appliances communicate on the heartbeat burb. An IPsec-authenticated heartbeat is sent by the primary and acknowledged by the standby. If one of the appliances becomes unavailable (that is, a heartbeat message or acknowledgement is not received by an appliance for the specified amount of time), the remaining appliance takes over and assumes responsibility for processing all traffic.

If one of the appliances unexpectedly becomes unavailable and the remaining appliance takes over processing all traffic, any active proxy sessions and non-stateful IP packet filter sessions that were assigned to the unavailable appliance will be lost. IP packet filter sessions that are configured for stateful session failover will not be lost.

If you know in advance that an appliance will need to be shut down, you can reduce the number of lost connections by scheduling the shutdown (rather than shutting down immediately). When a shutdown is scheduled for a later time, a soft shutdown will be performed to reduce the number of sessions that are lost. For information on soft shutdown, see “Scheduling a soft shutdown for a load-sharing HA cluster Sidewinder appliance” on page 775.
Certain connections in a load-sharing HA cluster will be assigned only to the primary. For example, connections that are used for Sidewinder management purposes (Admin Console, SSH) that are addressed to the shared cluster address will be assigned to the primary. In the event that the primary becomes unavailable, new connections will be assigned to the new primary, and existing connections will remain intact. SNMP messages that are addressed to the shared cluster address will also be assigned to the primary. Connections that are specifically addressed to an individual appliance address will be assigned to the specified appliance.

Failover HA

Failover HA consists of one appliance (the primary) actively processing traffic with the standby acting as a hot backup. When a standby appliance is registered to an HA cluster, synchronized areas will be overwritten by the HA cluster configuration. (To determine which areas are synchronized, see “Managing an HA cluster” on page 766.) Once registered, the standby monitors the primary through the heartbeat burb. An IPsec-authenticated heartbeat is sent by the primary and acknowledged by the standby. If the standby determines that the primary is unavailable, the standby takes over and assumes the role of the primary. When a standby takes over networking functions, any active proxy sessions through the primary are lost. IP Filter sessions that are configured for stateful session failover will not be lost.

You can configure failover HA in one of two ways:

- **peer-to-peer** — In a peer-to-peer HA cluster, both appliances are configured as standbys with the same takeover time. The first appliance to come online becomes the primary. If the primary becomes unavailable, the peer, currently acting as the standby, takes over as the primary and remains the primary until it becomes unavailable, at which time the peer again take over as the acting primary.

  This is the recommended failover HA configuration. However, to configure peer-to-peer HA, both appliances must have similar hardware configurations.

- **primary/standby** — In a primary/standby HA cluster, only the primary passes traffic. If the primary becomes unavailable, the standby takes over as the acting primary only until the primary becomes available again. When the primary becomes available, another takeover event occurs. This additional takeover event does not occur in a peer-to-peer configuration.

  This option is generally used if you have appliances that do not share the same hardware configuration.

*Note: When a takeover event occurs, there can be a number of netprobe events detected when connections take time to detect the switch of systems.*
When the primary is brought online, it activates its unique interface addresses, the cluster addresses, and any aliases assigned to the cluster. When the standby is brought online, it activates only its unique interface IP addresses.

If the standby does not receive a heartbeat signal for a number of seconds (based on the takeover setting of the standby), it sets the shared cluster addresses on its interfaces. In the process, the standby clears its address resolution protocol (ARP) cache and attempts to generate a gratuitous ARP. Most systems will immediately determine that the standby is now responsible for the addresses by which the primary is known, and new connections will be established through the new acting primary.

There may be a number of reasons why the gratuitous ARP is not received: a remote system may not recognize the message, the message may be blocked by certain switches, it may fail due to timing issues, etc. Often this can be resolved by flushing the ARP caches in the remote system. Many of these remote systems have ways to shorten the time that entries stay in the ARP cache; these should be set to time periods in the three to five minute range. You can also configure systems to communicate with the new ARP address by selecting the Force ARP Reset option on the High Availability Advanced Network Properties window when creating an HA cluster.
**Configuring HA**

This section provides the basic information you need to configure an HA cluster. Before you begin, sketch a diagram showing your planned configuration (similar to the diagram in Figure 308) for reference. Include the following items on your diagram:

- interfaces
- IP addresses
- HA shared cluster addresses
- burb names

Before you configure HA, the following conditions must be met:

- Both appliances must be at the same version.
- A dedicated heartbeat burb and interface must be configured on each appliance.

*Note:* For load-sharing HA, the interface used for the heartbeat burb must be at least as fast as the fastest load-sharing interfaces on your appliance. For information on configuring the heartbeat burb, see “Configuring the heartbeat burbs” on page 754.

- You can only assign one interface per burb when configuring load-sharing HA. (This includes VLANs.)
- The following areas *must* be configured identically on both appliances before you configure HA:
  - number and types of interfaces
  - number of burbs
  - burb names (burb names are case-sensitive)
- If static ARP entries are required on the HA cluster, you must add them to an *arp.conf* file. For details, see Knowledge Base article 8159 at [www.securecomputing.com/goto/kb](http://www.securecomputing.com/goto/kb).

*Note:* A configuration backup is automatically performed and stored on the Sidewinder appliance when creating an HA cluster.
Configuring the heartbeat burbs

You must configure a dedicated heartbeat burb and interface on each appliance before configuring an HA cluster. Follow the steps below for each appliance.

1. Ensure that the appliance has an interface that can be dedicated to HA traffic.
   • Do not use a VLAN for the heartbeat burb.
   • For load-sharing, the interface used for the heartbeat burb must be at least as fast as the fastest interface handling network traffic on your appliance.

2. In the Admin Console, connect to the appliance and create a heartbeat burb:
   a. Select Network > Burb Configuration.
   b. Click New.
   c. Type a name and optional description for the heartbeat burb.
   d. Select the Respond to ICMP echo and timestamp check box.

   **Note:** Do not select Hide port unreachables for a heartbeat burb.

   e. Click OK and save your changes.

3. Go to Network > Interface Configuration and assign the heartbeat burb and IP address to the appropriate interface. (Be sure to enable the interface.) See “Configuring interfaces” on page 456 for detailed information on configuring a new interface.

4. Save your changes. (You do not need to reboot at this time.)

5. Repeat these steps for each appliance that will be participating in the HA cluster.

6. Connect the heartbeat burbs with a crossover cable or a straight-through cable (if using em, bce, or bge interfaces).

7. Test the network connectivity between the two appliances for the heartbeat interface.

**Important:** Network connectivity must exist between the heartbeat burbs to successfully configure HA.
Configuring Sidewinder appliances for HA

Once you have configured a heartbeat burb for each Sidewinder appliance and have verified network connectivity between the appliances on the heartbeat interface, you can configure the appliances for HA. Perform these procedures to create an HA cluster:

- “Configure the first Sidewinder appliance in a new HA cluster” on page 755
- “Add a reservation in the HA cluster” on page 761
- “Join a Sidewinder appliance to an existing HA cluster” on page 762

Configure the first Sidewinder appliance in a new HA cluster

To configure the first appliance in a new HA cluster:

1. Connect to the appliance that will become the primary using the Admin Console.
2. Configure all functions and features other than HA.
3. Verify that you have a dedicated heartbeat burb and interface configured for HA on this appliance. See “Configuring the heartbeat burbs” on page 754 for instructions.
5. Click Launch Cluster Wizard. The Cluster Wizard window appears.
6. Click Next.
7. Select Create New Cluster and then click Next.
8. Select HA Cluster and then click Next.
Chapter 24: High Availability

Configuring HA

9 Select the HA configuration that you want to create, and then click **Next**.

*Note: To configure peer-to-peer HA or load-sharing HA, both appliances must have the same hardware configuration.*

- **Peer-To-Peer HA** — Select this button to create a peer-to-peer HA cluster. In a peer-to-peer HA cluster, both appliances are configured as standbys with the same takeover time. The first appliance to come online becomes the primary. Only the primary passes traffic. If the primary becomes unavailable, the peer, currently acting as the standby, takes over as the primary and remains the primary until it becomes unavailable, at which time the peer again take over as the acting primary. Failing over using this configuration requires fewer reboots than the primary/standby configuration.

- **Load-Sharing HA** — Select this button to create a load-sharing HA cluster. Load-sharing HA consists of two appliances that actively process traffic in a load-sharing capacity. This is the recommended configuration.

  See “Load-sharing HA” on page 750 for more information.

- **Primary/Standby HA** — Select this button to create a primary/standby HA cluster. In a primary/standby HA cluster, only the primary passes traffic. If the primary becomes unavailable, the standby takes over as the acting primary only until the primary becomes available again. This option is generally used if you have appliances that do not share the same hardware configuration.

  For more information on primary/standby HA, see “Failover HA” on page 751.

10 [Conditional] In the High Availability Takeover Time window, specify the number of seconds that the primary must be unavailable before the secondary/standby will begin the takeover process. The default value is 13 seconds.

*Note: This window does not appear if you selected the primary-standby HA option. For primary-standby HA, the takeover time is 3 seconds for the primary and 13 seconds for the secondary by default and cannot be modified in the Cluster Wizard.*

Click **Next**. The High Availability Shared Cluster Addresses window appears.
The High Availability Shared Cluster Addresses window allows you to configure the shared cluster addresses for the interfaces in your HA cluster. It also allows you to specify the heartbeat burb, which is responsible for sending and receiving heartbeats. Do the following, and then click Next:

a. Select the interface row that you want to configure, and click **Configure**. The High Availability Aliases window appears.

b. In the **Shared cluster IP address** field, type the shared cluster IP address for the interface that will be shared between appliances within the HA cluster.

   **Note:** The cluster address is the address most systems should use to communicate with or through the appliance, meaning that DNS, default routes, etc. need to be aware of this address.

c. Click **OK**.

d. Repeat step a through step c for each interface that will use HA.

e. In the **Heartbeat Burb** drop-down list, select the burb that HA will use to send or receive heartbeats. (A heartbeat is a short message that is sent out at specific intervals to verify whether a Sidewinder appliance is operational.) This must be a dedicated burb.

f. [Optional] If you want to skip the advanced configuration windows and use the default values, select the **Use default advanced High Availability properties and skip advanced screens** check box.

   If you select this check box, the following configuration options will be made automatically:
   - IPsec authentication password and authentication type will be automatically selected.
   - HA identification cluster ID and multicast address will be automatically assigned.
   - Remote test configuration options will not be configured.

   If you want to modify or configure any of these properties, clear the **Use default advanced High Availability properties and skip advanced screens** check box and click **Next** to access the Advanced General Properties and Advanced Network Properties windows.
12 [Conditional] The High Availability Advanced General Properties window allows you to configure IPsec Authentication values and High Availability identification values. Modify any of the following values:

**Note:** This window does not appear if you selected the Use default advanced High Availability properties and skip advanced screens check box in the High Availability Shared Cluster Addresses window.

- **High Availability Password** — Type the password to be used to generate the authentication key for IPsec. This password must be the same for both appliances because they share the same virtual firewall ID.
- **Authentication Type** — Select one of the following:
  - **SHA1** — Select this option if using HMAC-SHA1 authentication.
  - **MD5** — Select this option if using HMAC-MD5 authentication.
- **Cluster ID** — Select an ID that will be assigned to the HA cluster. This allows you to distinguish between and manage multiple HA clusters, if needed. Each appliance within an HA cluster must be assigned the same cluster ID. Valid values are 1–255.
- **Multicast Address** — This field displays the address of the multicast group used for HA purposes in the heartbeat burb. The default address is 239.255.0.1. To modify the address, click **Edit Address**.

When you have finished configuring this window, click **Next**.
13 [Conditional] The High Availability Advanced Network Properties window allows you to configure interface testing and force ARP reset properties. To configure interface testing and/or ARP reset properties, do the following and then click Next.

This window does not appear if you selected the **Use default advanced High Availability properties and skip advanced screens** check box in the High Availability Shared Cluster Addresses window.

*Note: For more information on interface testing with HA, see “Interface configuration issues with HA” on page 856.*

a In the Interface Test area, configure remote test IP addresses that you want to monitor:

*Note: If you specify 255.255.255.255 in this field, HA will only test the status of the interface rather than send data to verify that the appliance is up. This functionality is not intended for use in the heartbeat burb.*

- Select the network row that you want to modify, and click **Modify**. The Remote Test window appears.
- In the **Remote Test IP** field, enter the IP address that the Sidewinder appliance will periodically ping. The remote address must be a highly reliable system that is directly attached to the Sidewinder network, but does not belong to either cluster member.

For example, if you use a VRRP (Virtual Router Redundancy Protocol) cluster, you can specify the VRRP address of the router as your remote ping address. (However, some VRRP routing clusters will only respond to pings if the configured primary router is currently acting as the primary. If you are using this type of VRRP routing cluster, you should use an alternative remote address.)

For load-sharing HA, if remote ping fails on one of the two cluster members, that member will become unavailable until the remote interface is again detected. If there is only one active cluster member and a remote ping failure is detected, that member will audit the failure and remain in the cluster until another member joins the cluster (without a ping failure), or until the remote system is detected.

- Click **OK** to return to the High Availability Advanced Network Properties window.

b In the **Ping the Remote Test IP every** field, specify how often (in seconds) the HA cluster will ping the remote address to ensure that an interface and path are operational.

c In the **Consecutive ping failures before takeover** field, specify the number of failed ping attempts that must occur before a secondary/standby takes over as the primary.

If the remote test IP host becomes unavailable immediately after a ping attempt has been issued, the time it takes for a secondary/standby to take over will be slightly longer (this is because it will take close to an entire test interval before the first failure is detected).
[Conditional] The Force ARP Reset area lists the IP address and burb of each system that you determine needs to update its ARP cache with the new cluster alias IP. Use this area to list all systems that are known to ignore gratuitous ARPs, but that need to know the new cluster alias.

**Note:** This area is not available if you are configuring load-sharing HA.

- To define a system to be included in the Force ARP Reset list, click **New**. The Force ARP Reset window appears. Enter the IP Address and select the burb for the system, and then click **OK**.
- To modify an entry, select the appropriate entry and click **Modify**.
- To delete an IP address from the list, select the address and click **Delete**.

The Cluster Wizard Summary window displays a list of the actions that will be performed when you click **Execute**.

14 Review the Cluster Wizard Summary window.

If you want to make changes to your configuration before executing, click **Back** to navigate to the appropriate window(s) and make the necessary changes.

**Important:** Carefully review the changes, as changes you make after executing the cluster will require an additional reboot.

15 When you are satisfied with the summary of changes, click **Execute**.

A progress bar appears while the configuration changes are made. If the transition is successful, the Success window appears displaying the new state.

16 Click **Finish**. The Admin Console disconnects.

The IP address on the connection window changes to the shared cluster address. Connect the Admin Console to the HA cluster using the shared cluster address.

To add an additional cluster member, see “Join a Sidewinder appliance to an existing HA cluster” on page 762.
Chapter 24: High Availability
Configuring HA

Add a reservation in the HA cluster

Before joining a Sidewinder appliance to an existing HA cluster, you must make a reservation for that appliance in the Common Parameters tab of the HA cluster. Once you have added the appliance to the HA cluster, you will need to join the appliance to the HA cluster using the Cluster Wizard.

To add a reservation for the new appliance in the existing HA cluster:

1. Connect to the HA cluster using the Admin Console using the cluster IP address.
2. In the Admin Console tree, select High Availability. The High Availability Common Parameters tab appears.
3. In the Pair Members area, click New. The Add New Firewall window appears.
4. In the Hostname field, enter the name of the appliance you are adding to the HA cluster. The name must be a fully qualified host name in the same domain as the primary.
5. [Conditional] If you selected the Primary/Standby HA mode, in the Takeover Time field, select the number of seconds that the primary must be unavailable before the secondary/standby will begin the takeover process. The default value is 13 seconds.

   Note: This field does not appear if you selected Primary/Standby HA.

6. In the IP Address in Heartbeat Burb field, enter the individual IP address (in the heartbeat burb) of the appliance that you are adding to the HA cluster.
7. In the Registration Key field, create the registration key for this HA cluster. The key must be at least one character long and may consist of alphanumeric characters, hyphens (-), and underscores (_).

   Important: You will need the registration key when you join the appliance to the HA cluster using the Cluster Wizard.

8. Click Add to add the appliance to the HA cluster.

You can now join the Sidewinder appliance to the HA cluster using the Cluster Wizard. See “Join a Sidewinder appliance to an existing HA cluster” on page 762.
Join a Sidewinder appliance to an existing HA cluster

To join an appliance to an existing HA cluster:

1. Using the Admin Console, connect to the appliance that will be joining the HA cluster.
2. Select Maintenance > Cluster Wizard.
3. Click Launch Cluster Wizard. The Welcome window appears.
4. Click Next.
5. Select Join Existing Cluster and then click Next.
6. Select HA Cluster and then click Next.
7. In the Gathering information to join cluster window, configure the following fields:
   - **Partner’s Heartbeat Burb IP Address** — Enter the heartbeat IP address of the HA partner.
   - **Cluster Member Name** — This is the name of the appliance that you are joining to the HA cluster (the name you entered when you added this appliance to the HA cluster). This field is read-only.
   - **Registration Key** — Enter the registration key for the HA cluster (the key that you created when you added this appliance to the HA cluster in step 7 on page 761).
8. Click Next. The Cluster Summary window displays a list of the actions that will be performed.
9. Review the Cluster Wizard Summary window.
   If you want to make changes to your configuration before executing, click Back to navigate to the appropriate window(s) and make the necessary changes.

   **Important:** Carefully review the changes, as changes you make after executing the cluster will require an additional reboot.
10. When you are satisfied with the summary of changes, click Execute, then click Yes to confirm.
    A progress bar appears while the configuration changes are made. If the transition is successful, the Success window appears displaying the new state.
11. Click Finish.
    The firewall icon you just joined to the cluster disappears from the Admin Console tree.
12. Select the new cluster member in any branch.
    “This firewall not registered” appears in the right pane.
13. Click Check Now.
    The new cluster member is registered as part of the HA cluster and all branch contents are visible.
Enabling and disabling load-sharing for an HA cluster

If you have an HA cluster configured and want to enable or disable load-sharing, follow the steps below. For more information on load-sharing HA, see “Load-sharing HA” on page 750.

For more information on load-sharing HA, see “Load-sharing HA” on page 750.

1 Connect to the HA cluster and select **High Availability**.
2 Click the plus sign (+) in front of the High Availability branch to display the individual icons for each appliance that is part of the HA cluster.
3 Select the primary icon. The Common Parameters tab appears.
4 In the **Cluster Mode** area, enable or disable load-sharing by selecting the appropriate cluster mode as follows:
   - **Designate as part of a Load Sharing High Availability Cluster** — Select this option if you want to enable load-sharing for the HA cluster (both appliances actively process traffic).
   - **Designate as part of a Primary/Standby High Availability Cluster** — Select this option if you want to disable load-sharing HA and convert the HA cluster to a failover HA cluster (only one appliance processes traffic, with the other appliance acting as a hot backup).
   - **Primary** — Select this option to make the selected icon the primary member of the cluster.
   - **Standby** — Select this option to make the selected icon the standby member of the cluster.
5 Save your changes.
6 Wait 60 seconds to allow the appliances to synchronize.
7 Shut down the secondary/standby:
   a Select **Maintenance > System Shutdown > secondary icon**.
   b Select **Halt System**.
   c Select **Shutdown Immediately**.
   d Click **Perform Shutdown**.
8 Shut down the primary:
   a Select **Maintenance > System Shutdown > primary icon**.
   b Select **Reboot to Operational Kernel**.
   c Select **Shutdown Immediately**.
   d Click **Perform Shutdown**.
9 When the primary is finished rebooting, start up the secondary/standby.

**Important:** If you do not begin the reboot process for the second appliance before the primary finishes rebooting, it will detect that the second appliance is configured for a different cluster mode, and the HA cluster will not function properly. If this happens, you will need to reboot each appliance to synchronize the HA cluster.
Removing a Sidewinder appliance from an HA cluster

To remove a secondary/standby from an HA cluster, follow the steps below.

**Removing a secondary/standby from an HA cluster**

1. Connect to the HA cluster and select **High Availability** in the Admin Console tree. The Common Parameters window appears.
2. In the **Pair Members** table, select the secondary/standby and then click **Delete**.

   When the appliance is removed from the HA cluster, it will restart in a standalone state.

   To connect to the removed appliance, you must add it to the Admin Console tree:
   a. From the **File** menu, select **New Firewall**. The Add Firewall window appears.
   b. Enter the appliance name and IP address, then click **Add**.

**Removing the primary from an HA cluster**

You must remove the secondary/standby from the HA cluster before you can remove the primary from the HA cluster. Once you have removed the secondary/standby from an HA cluster, follow the steps below to remove the primary from the HA cluster:

1. From the Admin Console, connect to the primary using the cluster address.
2. In the Admin Console tree, select **High Availability**. The Common Parameters window appears.
3. In the Pair Members area, click **Change State to Standalone**. The Cluster Wizard Welcome window appears.
4. Click **Next**.
5. Select **Change To Standalone**, and then click **Next**.

   The Cluster Wizard Summary window appears.
6. Review the summary. When you are satisfied with the summary of changes, click **Execute**. Click **Yes** to confirm the reboot.

   A progress bar appears while the configuration changes are made. If the transition is successful, the Success window appears displaying the new state.
7. Click **Finish**. The Admin Console disconnects. The appliance will restart in a standalone state.
Understanding the HA cluster tree structure

The Admin Console tree structure is slightly different for an HA cluster. As explained above, when you configure an HA cluster, both appliances are managed within a single Admin Console connection.

Areas of the HA cluster that are synchronized (that is, areas in which the information for both appliances must be the same and remains in sync) will appear with a single tree option. When you modify information within those areas, the information will automatically be updated for both appliances.

Information specific to individual appliances within the HA cluster (such as configuration backup and restore) includes a sub-folder (indicated by a plus [+] sign) that contains an icon for each appliance that is part of the HA cluster. To modify information within these areas, expand the tree branch, select the appropriate appliance, and make the desired changes. Non-synchronized modifications to an individual appliance will be applied only to that appliance and will not be overwritten by changes made to the other appliance.

The License window is further split in an HA cluster: The Contact and Company tabs appear when you select License in the tree; the Firewall and Enrollment List tabs appear when you select a Sidewinder license.

The figure below demonstrates the difference between an individually configured area of the HA cluster (Reports) and a synchronized area of the HA cluster (Burb Configuration).

**Figure 309:** Example of an individually configured area

Auditing is configured on an individual appliance basis.

Burb Configuration is synchronized, and does not allow you to select an individual appliance.

The High Availability and Interface Configuration areas within the HA cluster tree include some areas that are synchronized and some areas that are configured on an individual appliance basis, as shown in the figure below.

**Figure 310:** Special HA and Interface Configuration options

Synchronized HA information is configured by selecting the main HA option.

Synchronized information is configured by selecting the main Interfaces option.

HA information specific to a single appliance is configured by selecting an appliance.

Interface information specific to a single appliance is configured by selecting that appliance.
The following lists summarize the features that are synchronized and the features that are configured individually in an HA cluster.

Features that are synchronized within an HA cluster

- High Availability
- IPS Attack Responses
- System Responses
- Audit (health monitoring, filters)
- Rules
- Rule Elements
- Application Defenses
- Configuration Backup
- Network Defenses
- Burb Configuration
- VPN Configuration
- DNS
- sendmail
- Routing
- Administrator Accounts
- UPS
- Interface Aliases

Features that are configured individually within an HA cluster

- Dashboard
- Service Status
- Interfaces
- Configuration Backup
- Date and Time
- License
- Software Management
- System Shutdown
- File Editor

**Note:** For audit, the health monitor setting is pushed from the primary to the other secondaries. Audit filters are also synchronized and should be created on the primary.

Managing an HA cluster

Once you have configured an HA cluster, the HA cluster will be represented in the Admin Console tree by a one combined firewall icon. When you connect to the HA cluster, you will use the HA shared cluster address that you created when you configured HA. This allows you to manage both appliances by connecting to the HA cluster.

**Caution:** If you modify your hardware interface configuration, you may need to re-add the cluster address for that interface. A reboot is required if you make this change.
Modifying HA common parameters

Use the Common Parameters tab to configure properties that are common to the HA cluster. To configure common HA parameters, connect to the HA cluster using the Admin Console and select **High Availability**. The following window appears:

![Common Parameters tab](image_url)
To configure the Common Parameters tab:

1. In the **High Availability Identification** area, do the following:
   a. In the **Cluster ID** field, select an ID that is assigned to the HA cluster. This allows you to distinguish between and manage multiple HA clusters, if needed. Each appliance with an HA cluster must be assigned the same cluster ID. Valid values are 1–255.
   b. The **Multicast Group Address** field displays the address of the multicast group used for HA purposes on the heartbeat burb. The default address is 239.255.0.1. To modify the address, click **Edit address**. See “Changing the multicast address” on page 771 for details on modifying the multicast group address.
   c. In the **Heartbeat Burb** drop-down list, select the burb that HA will use to send or receive a heartbeat. A **heartbeat** is a short message that is sent out at specific intervals to verify whether a Sidewinder appliance is operational. The heartbeat, session information, and configuration information are also transferred between the heartbeat burbs. This must be a dedicated heartbeat burb.
   d. In the **Heartbeat Verification Burb** drop-down list, select the burb that HA will use to send or receive a mini-heartbeat. This should be a burb that regularly passes traffic, such as the internal burb.

   This mini-heartbeat helps protect against false failover events by doing the following:
   - If the appliance does not detect the heartbeat but does detect the mini-heartbeat, the HA cluster does not fail over. An audit message is generated, alerting the administrator to check the heartbeat burbs’ connectivity.

   **Note:** The switch must be able to pass IGMP (with an IP protocol number of 2) and must not decrement time to live (TTL) of the HA heartbeat.

   **Important:** Loss of communications on the heartbeat burb causes diminished HA services. For load-sharing, the active secondary no longer shares the session load; it goes to a standby state. For non-load sharing, the standby cannot receive updated information about new ipfilter sessions established on the primary. Maintain high availability service to your network by troubleshooting the heartbeat burbs’ communication problems as soon as possible.

   - If the appliance does not detect either the heartbeat or the mini-heartbeat, the HA cluster fails over.

Additional information on heartbeat verification is available in knowledge base article 3848.
2 In the **IPsec Authentication** area, do the following:

   a In the **Authentication Type** field, select the type of IPsec authentication to use for HA:
      • SHA1 — Select this option if using HMAC-SHA1 authentication.
      • MD5 — Select this option if using HMAC-MD5 authentication

   b In the **Password** field, type the password that will be used to generate the authentication key for IPsec. This password must be the same for both appliances because they share the same virtual firewall ID.

3 [Conditional] The **Pair Members** table lists the Sidewinder appliances that have been added to the HA cluster.

   • To add an appliance to the **Pair Members** table, see “Add a reservation in the HA cluster” on page 761.
   • To view the status of the cluster, click **Cluster Status**. A pop-up window will appear displaying the status of each appliance. (When just one HA member is in the table, this button reads **Change State to Standalone**.)
   • To close the status information window, click **OK**.

   This table is not available until you successfully promote a primary. Once the primary has been promoted, you can add a second appliance to the HA cluster. However, you must join the second appliance before it will become functional within the HA cluster. See “Join a Sidewinder appliance to an existing HA cluster” on page 762 for information on registering an appliance to an HA cluster.

4 [Conditional] To define a system that requires ARP cache updates, in the **Force ARP Reset** area, click **New** and see “Configuring an entry in the Force ARP Reset area” on page 771. (This option is not used for load-sharing HA.)

   The Force ARP Reset area lists the IP address and burb of each system that you determine needs to update its ARP cache with the new cluster alias IP. Use this area to list all systems that are known to ignore gratuitous ARPs, but that need to know the new cluster alias. (To delete an IP address from the list, highlight the address and click **Delete**.)

5 In the **Interface Test** area, do the following:

   a In the **Time Between Tests** field, specify how often (in seconds) the HA cluster will ping the remote address to ensure that an interface and path are operational.

   b In the **Consecutive Failures** field, specify the number of failed ping attempts that must occur before a secondary/standby takes over as the primary.

   If the remote host becomes unavailable immediately after a ping attempt has been issued, the time it takes for a secondary/standby to take over will be slightly longer (this is because it will take close to an entire test interval before the first failure is detected).

   **Note:** The **Auto-Recover On Reconnect** option is not currently functional.
6 The Interfaces table identifies the burb, cluster address, network address, remote test IP address, and cluster MAC address for each interface.

The Cluster MAC column is a read-only column that displays the MAC address for each cluster interface that is defined. Depending on the type of router you are using, this address may be required to configure the router if you have load-sharing HA configured. The Cluster MAC is used for all shared cluster addresses and aliases on that interface.

You must define a shared IP address for each interface being backed up via HA. To define a new interface, click New. To modify an HA shared cluster address, highlight the interface you want to modify, and click Modify. See "Modifying an entry in the Interfaces table" on page 772 for details. To delete an interface, highlight the interface and click Delete.

**Important:** All non-HA alias IP addresses are defined in the Aliases tab of the Interfaces window.

7 When you are finished configuring the HA parameters for this appliance, save your changes.

8 Select Maintenance > System Shutdown and reboot to the operational kernel. Your changes will not take effect until the reboot completes.
Changing the multicast address

The Edit Multicast Group window allows you to specify different multicast addresses for an HA cluster. Do not specify an address that conflicts with other multicast groups on the heartbeat burb. Addresses in the range of 239.192.0.0 to 239.255.255.255 have been reserved by RFC 2365 for locally administered multicast addresses. Boundary routers should be configured to not pass your selected address if such a feature exists.

To restore the default address (239.255.0.1), click **Restore Default**.

---

**Important:** If the default is not used, you should change the reverse lookup files in DNS to allow DNS reverse resolution of the multicast address. Refer to the `/etc/namedb.u/failover.rev` file.

Configuring an entry in the Force ARP Reset area

The Force ARP Reset window allows you to specify the IP address and its associated burb for each system that would ignore the gratuitous ARP containing the new cluster MAC address.

To add this information, follow the steps below.

---

**Note:** The Force ARP Reset area is not used for load-sharing HA because the MAC address does not change during failover.

---

1. In the **IP Address** field, enter the system’s IP address.
2. In the **Burb** field, select the burb that connects to that system’s network.
3. Click **Add** to save the information, or click **Close** to close the window without saving your changes.
Modifying an entry in the Interfaces table

The Common IP window allows you to specify the shared cluster address for your interfaces. You will need to configure a shared cluster address for each interface that uses HA. Follow the steps below.

**Note:** Be sure to add the shared cluster address and the associated domain name to your DNS service.

1. In the Burb drop-down list, select the appropriate burb.

2. In the Common IP Address field, type the shared cluster address for that burb.

   The cluster address is the address most systems should use to communicate with or through the appliance, meaning that DNS, default routes, etc. need to know this address.

3. [Optional] In the Remote Test IP field, specify the address that the appliance will periodically ping.

   The remote address must be a highly reliable system that is directly attached to the Sidewinder network. For example, if you use a VRRP (Virtual Router Redundancy Protocol) cluster, you can specify the VRRP address of the router as your remote ping address. (However, some VRRP routing clusters will only respond to pings if the configured primary router is currently acting as the primary. If you are using this type of VRRP routing cluster, you should use an alternative remote address.)

   For load-sharing HA, if remote ping fails on one of the two cluster members, that member will become unavailable until the remote interface is again detected. If there is only one active cluster member and a remote ping failure is detected, that member will audit the failure and remain in the cluster until another member joins the cluster (without a ping failure), or until the remote system is detected.

   **Note:** If you specify 255.255.255.255 in this field, HA will test the status of the appliance interface rather than a remote system.

4. Click OK to save the cluster address information and return to the Local Parameters tab. (To exit the window without saving your changes, click Cancel.)
Modifying HA local parameters

To configure local HA parameters, connect to the appliance using the Admin Console and select **Firewall Administration > High Availability**. (If you have already configured HA, the **High Availability** option will appear directly beneath the appliance icon.) Select the **Local Parameters** tab. The following window appears:

![Local Parameters tab](image)

The Local Parameters tab specifies the parameters that are unique to a particular appliance in your HA configuration. Follow the steps below.

1. In the **Cluster Mode** area, select one of the following options:
   - **Designate as part of a Load Sharing High Availability Cluster** — Select this option if you want to configure load-sharing HA (both appliances actively process traffic).
   - **Designate as part of a Primary/Standby High Availability Cluster** — Select this option if you want to configure failover HA (only one appliance processes traffic, with the other appliance acting as a hot backup).

   **Note**: To configure load-sharing HA or peer-to-peer failover HA, the appliances must have the same hardware configuration. For more information on each HA configuration option, see “HA configuration options” on page 750.
2 [Conditional] If you selected Primary-Standby in the previous step, select one of the following options in the Cluster Mode area:
   • **Primary** — Select this option if this will be the primary in your network. (This option is only used for the dedicated primary-standby HA configuration.)
   • **Standby** — Select this option if this appliance is a standby in your network, or if you are configuring peer-to-peer HA.

   **Note:** For peer-to-peer HA, you must configure each appliance as a standby.

3 In the Control field, select Enabled to enable HA for this appliance. (To disable HA, select Disabled.)

   **Note:** You must reboot both appliances before the HA configuration will take effect.

4 [Conditional] In the Takeover Time field specify the number of seconds that the primary must be unavailable before the secondary/standby will begin the takeover process.

   **Note:** If the primary in an HA cluster goes into failure mode and the secondary/standby is not available, the primary will remain as the primary, but the Takeover Time value for that appliance will change to one, ensuring that if a secondary/standby becomes available, it can take over as the primary.

   The secondary/standby Takeover Time value will differ depending on the type of HA configuration you are using:

   • **Load sharing Takeover Time** — The takeover time for load-sharing HA cluster appliances must be the same for EACH appliance that is participating in the HA configuration. The default value is 13 seconds for load-sharing configurations.
   • **Peer-to-peer Takeover Time** — The takeover time for load-sharing HA cluster appliances must be the same for EACH appliance that is participating in the HA configuration. The default value is 13 seconds for load-sharing configurations.
   • **Primary-standby Takeover Time** — The takeover time for the primary is 3 seconds by default and cannot be modified. This value ensures that the designated primary will become the actual primary when it is activated. The default for the standby is 13.

   **Note:** If you assign a standby Takeover Time value that is too close to 3 seconds, the standby may attempt to take over as the primary during periods when the primary is too busy processing data traffic to send the heartbeat.
Scheduling a soft shutdown for a load-sharing HA cluster Sidewinder appliance

When a Sidewinder appliance that belongs to an HA cluster is shutdown by an administrator (for example, to perform scheduled maintenance), a soft shutdown will automatically occur (assuming the shutdown time is not immediate). A soft shutdown provides a buffer period before the actual shutdown occurs, allowing the appliance to stop accepting new connections, while allowing most existing connections to complete before the appliance actually shuts down. IP packet filter processing is also transferred to the remaining appliance.

**Note:** A peer must be available in order to perform a soft shutdown.

By default, the soft shutdown process will begin 30 minutes prior to a scheduled shutdown. If the shutdown is scheduled to occur in less than 30 minutes, the soft shutdown process will begin immediately and will remain in effect until the actual shutdown time occurs. You can also manually increase or decrease the length of the soft shutdown period.

For example, suppose you configure the appliance to shutdown in two hours using the default soft shutdown of 30 minutes. The appliance will continue to accept and process connections for 1.5 hours. When the appliance is 30 minutes from the shutdown time, it will stop accepting new connections and existing connections will have 30 minutes to complete. After the soft shutdown period completes, the appliance will shut down and will be unavailable until it is rebooted.
The soft shutdown feature is specified via command line. If you schedule a shutdown using the Admin Console, the default soft shutdown time will be applied. The following bullets provide examples of configuring an HA cluster appliance for shutdown:

- If you want the soft shutdown process to begin immediately, use the following command (the appliance must be shut down or manually rebooted once the soft shutdown process is complete):

  ```shell
cf failover softshutdown
  ```

- To configure soft shutdown to occur for a specific amount of time, as follows:

  ```shell
  shutdown -s [soft_shutdown_time] [shutdown_time]
  ```

  The `soft_shutdown_time` specifies that amount of time that soft shutdown will occur. The `shutdown_time` specifies the time at which the actual shutdown will occur. Each variable can be specified either as a number of minutes or as an exact date and time. If you are specifying the number of minutes, you must include a plus (+) sign in front of the minutes.

  For example, if you want the appliance to shut down on Saturday, June 12, 2004 at 11:00 am with a 15 minute soft shutdown period, you would enter the following command:

  ```shell
  shutdown -s +15 0406121100
  ```

  In this case, the soft shutdown process would begin at 10:45 am, and the appliance would shutdown at 11:00 am on the specified day.

  If you want the appliance to begin the soft shutdown at 6:00 am with an actual shutdown at 6:20 am, you would enter the following command:

  ```shell
  shutdown -s 0600 0620
  ```

  **Note:** For a complete listing of shutdown options, refer to the `shutdown` man page.

You can cancel a scheduled shutdown at anytime prior to the final 30 minute period by entering the `shutdown -c` command. However, once the appliance has entered soft shutdown mode, this command will no longer cancel the soft shutdown process. When the soft shutdown process is complete, you will need to reboot the appliance before it will properly function as part of the HA cluster.
Re-establishing an HA cluster if a cluster member fails

If a member of an HA cluster is no longer functional and must be re-installed, you can re-establish the cluster by restoring a configuration backup. You can use the configuration backup from either the failed cluster member or the remaining cluster member.

To re-establish an HA cluster:

1. Re-install the failed appliance or install a new system with the same host name.
2. Add the new or re-imaged appliance to the Admin Console tree.
3. Use the Admin Console to connect to the new or re-imaged appliance.
4. Restore the configuration file to the new system: Select Maintenance > Configuration Backup.

The Local Parameters window appears. The appliance is part of the HA cluster.
Managing an HA cluster
## Appendix A: Command Line Reference

### In this appendix...

- Frequently used commands ................................................................. 782
- List of cf areas .................................................................................. 794
- Monitoring Sidewinder status ............................................................ 807
- About automatic (cron) jobs ............................................................... 812
- Working with files on the appliance .................................................. 814
Frequently used commands

The command line interface can play an important role in troubleshooting problems. A list of the most frequently used commands is provided in the following table. The commands are grouped by topic, and the topics are listed alphabetically. Some commands are basic UNIX commands. Other commands are specific to the Sidewinder appliance. Additional information about Sidewinder-specific commands is available in the next section.

**Caution:** Some of these commands disconnect existing sessions or can change policy. Therefore, you should only use these commands if you are an advanced administrator or when working with Secure Computing Technical Support.

- “Administrator accounts” on page 782 • “Policy” on page 788
- “Audit” on page 783 • "Routing" on page 789
- “Backups” on page 784 • “Sendmail” on page 790
- “Burbs and burb groups” on page 784 • “Spam filter” on page 790
- “DNS” on page 785 • “Shutdown” on page 790
- “Emergency Maintenance Mode (EMM)” on page 786 • “System” on page 791
- “File system” on page 786 • “tcpdump” on page 791
- “High Availability and One-to-Many clusters” on page 786 • “Technical Support” on page 792
- “License pages” on page 787 • “Text editors and viewers” on page 792
- “Manual pages” on page 787 • “TrustedSource” on page 792
- “Network” on page 787 • “Type Enforcement” on page 793
- “NTP” on page 788 • “VPN” on page 793
- “Packages and software” on page 788

Table 46: Administrator accounts

<table>
<thead>
<tr>
<th>Administrator accounts commands</th>
<th>Description of use</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>man cf_adminuser</strong></td>
<td>Man page for cf adminuser</td>
</tr>
<tr>
<td><strong>cf adminuser add</strong></td>
<td>Create admin users</td>
</tr>
<tr>
<td><strong>cf adminuser delete</strong></td>
<td>Delete admin users</td>
</tr>
<tr>
<td><strong>cf adminuser modify user=</strong></td>
<td>Change an administrator account password at the command line</td>
</tr>
<tr>
<td><strong>auth=password password=newpassword</strong></td>
<td></td>
</tr>
<tr>
<td><strong>cf adminuser query</strong></td>
<td>Lists the Sidewinder administrator user database</td>
</tr>
</tbody>
</table>
# Appendix A: Command Line Reference

## Frequently used commands

### Table 47: Audit

<table>
<thead>
<tr>
<th>Audit commands</th>
<th>Description of use</th>
</tr>
</thead>
</table>
| `cf acl set loglevel=[1-4]` | Set the audit output level for the rule set  
  1 = lowest, fatal errors only  
  2 = default, fatal and major errors, and denied rules  
  3 = level 2 audit and allowed rules  
  4 = verbose, troubleshooting only  
  **Tip:** See the Policy area for commands about rules. |
| `acat audit.raw > /var/tmp/audit.txt` | Convert audit to ascii readable and write to file `audit.txt`                                                                                     |
| `tail -1000 /var/log/audit.raw | acat > /tmp/audit.txt` | Convert the last 1000 lines of audit to readable ascii and write to file `audit.txt` in the `/tmp` directory                                  |
| `acat -k` | Show all audits in real time                                                                                                                      |
| `acat_acls -d` | Show real time audit for policy denies                                                                                                            |
| `acat_acls -a` | Show real time audit for policy allows                                                                                                             |
| `acat -c` | Review all the possible options for a `sacap_filter`                                                                                           |
| `showaudit -kp` | Show netprobes in real time                                                                                                                     |
| `showaudit -kH x.x.x.x` | Show real time audits pertaining to x.x.x.x                                                                                                      |
| `rollaudit -R d -w` | Roll log files (such as `audit.raw`)                                                                                                               |
| `cf daemond enable agent=auditsql` | Enable the audit database. Enable this first, then enable the auditdbd server.                                                                |
| `cf daemond enable agent=auditdbd` | After enabling auditsql, enable the audit server. `cf reports` will not generate output until the auditsql database and auditdbd server are enabled. |
| `cf reports run_report report_name=report_name` | View a report from the command line                                                                                                                |
| `gen_reports -l` | List all the available reports                                                                                                                   |

### Table 48: Anti-virus

<table>
<thead>
<tr>
<th>Anti-virus commands</th>
<th>Description of use</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>cf antivirus query</code></td>
<td>Show AV configuration</td>
</tr>
<tr>
<td><code>cf daemond restart agent=virus-scan</code></td>
<td>Restart the anti-virus engine</td>
</tr>
<tr>
<td><code>cf antivirus engine applyavpatch patch=patch_name</code></td>
<td>Install an AV engine patch without having to reboot</td>
</tr>
<tr>
<td><code>cf antivirus engine download</code></td>
<td>Download the latest IDE files for the AV engine</td>
</tr>
</tbody>
</table>
Table 49: Backups

<table>
<thead>
<tr>
<th>Backup commands</th>
<th>Description of use</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>cf config backup loc=local filename=filename</code></td>
<td>Create a configuration backup that is saved locally in <code>/var/backups/repository</code></td>
</tr>
<tr>
<td><code>cf config backup loc=location filename=filename</code></td>
<td>Save configuration backup; specify local, remote, or USB</td>
</tr>
<tr>
<td><code>cf config restore loc=location filename=filename</code></td>
<td>Restore a configuration backup; specify local, remote, or USB</td>
</tr>
<tr>
<td><code>cf config restore loc=local filename=filename</code></td>
<td>Restore a local configuration backup from <code>/var/backups/repository</code></td>
</tr>
<tr>
<td><code>less /secureos/etc/config.conf</code></td>
<td>View include and exclude lists (cannot exclude directories)</td>
</tr>
<tr>
<td><code>find / -name &quot;*.core&quot; -print</code></td>
<td>Find core files that could make the backup large</td>
</tr>
</tbody>
</table>

Table 50: Burbs and burb groups

<table>
<thead>
<tr>
<th>Burb and burb group commands</th>
<th>Description of use</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>cf burb query</code></td>
<td>Show burb configuration</td>
</tr>
<tr>
<td><code>cf burb delete burb=burbname</code></td>
<td>Delete a burb; the burb cannot be deleted if referenced by any active policy</td>
</tr>
<tr>
<td><code>cf burb add burb=burbname region</code></td>
<td>Add a new burb</td>
</tr>
<tr>
<td><code>cf burbgroup query</code></td>
<td>Show burb group configuration</td>
</tr>
<tr>
<td><code>cf burbgroup delete name=name</code></td>
<td>Delete a burb group; the burb group cannot be deleted if reference by any active policy</td>
</tr>
<tr>
<td><code>cf burbgroup add name=name</code></td>
<td>Add a new burb group</td>
</tr>
<tr>
<td><code>cf burbgroup modify name=name members=names</code></td>
<td>Add new burbs to a burb group</td>
</tr>
</tbody>
</table>
## DNS

<table>
<thead>
<tr>
<th>DNS commands</th>
<th>Description of use</th>
</tr>
</thead>
<tbody>
<tr>
<td>cf dns query</td>
<td>Check if configuration is split/single/transparent</td>
</tr>
<tr>
<td>cf daemond restart agent=named-internet</td>
<td>Restart only the internet DNS server</td>
</tr>
<tr>
<td>cf daemond restart agent=named-unbound</td>
<td>Restart only the unbound DNS server</td>
</tr>
<tr>
<td>cf dns reload</td>
<td>Reloads DNS zone and configuration files</td>
</tr>
<tr>
<td>cf dns dumpdb</td>
<td>Dumps current DNS database in memory</td>
</tr>
<tr>
<td>cf dns trace</td>
<td>Enables debug tracing by one 'bump' in the named(s). logged to /var/run/named.run.i and /var/run/named.run.u</td>
</tr>
<tr>
<td>cf dns notrace</td>
<td>Turns off tracing</td>
</tr>
<tr>
<td>hostname</td>
<td>View the firewall hostname</td>
</tr>
<tr>
<td>named-checkconf named.conf.u</td>
<td>Check configuration file syntax</td>
</tr>
<tr>
<td>named-checkzone zone file.db</td>
<td>Check zone file for correct syntax</td>
</tr>
<tr>
<td>dig host.domain.tld</td>
<td>Query the DNS server on burb index ‘x’ for host info</td>
</tr>
<tr>
<td>dig zone MX</td>
<td>Query for an MX record</td>
</tr>
<tr>
<td>dig –x X.X.X.X</td>
<td>Query for the PTR record</td>
</tr>
<tr>
<td>tail -f /var/log/daemon.log</td>
<td>View current logs pertaining to DNS updated in real time</td>
</tr>
<tr>
<td>tail -f /var/log/daemon.log</td>
<td>grep named</td>
</tr>
<tr>
<td>less /etc/named.conf.#</td>
<td>View conf file for Internet/Unbound DNS</td>
</tr>
<tr>
<td>ls /etc/namedb.#</td>
<td>List the directory containing Internet/Unbound zones (.db)</td>
</tr>
</tbody>
</table>
### Table 52: Emergency Maintenance Mode (EMM)

<table>
<thead>
<tr>
<th>EMM commands</th>
<th>Description of use</th>
</tr>
</thead>
<tbody>
<tr>
<td>shutdown now</td>
<td>Reboot the appliance to the emergency maintenance mode (EMM)</td>
</tr>
<tr>
<td>cf policy restore_console_access</td>
<td>Run in EMM to add Admin Console and login console rule</td>
</tr>
<tr>
<td>mount -a</td>
<td>Mounts all filesystems in /etc/fstab</td>
</tr>
<tr>
<td>fsck</td>
<td>Check all filesystems listed in /etc/fstab</td>
</tr>
<tr>
<td>less /var/run/dmesg.boot</td>
<td>View log file of system messages from the kernel</td>
</tr>
</tbody>
</table>

### Table 53: File system

<table>
<thead>
<tr>
<th>File system commands</th>
<th>Description of use</th>
</tr>
</thead>
<tbody>
<tr>
<td>df</td>
<td>Display disk free space</td>
</tr>
<tr>
<td>du -a /</td>
<td>sort -nr</td>
</tr>
<tr>
<td>find / -type f -name &quot;*name&quot;</td>
<td>Find a file with 'name' in the name of the file</td>
</tr>
</tbody>
</table>

### Table 54: High Availability and One-to-Many clusters

<table>
<thead>
<tr>
<th>HA and OTM commands</th>
<th>Description of use</th>
</tr>
</thead>
<tbody>
<tr>
<td>man cf_failover</td>
<td>Man page for cf failover commands</td>
</tr>
<tr>
<td>cf failover status</td>
<td>Displays current state of failover</td>
</tr>
<tr>
<td>cf cluster status</td>
<td>Displays current policy for primary and peer</td>
</tr>
<tr>
<td>cf failover query</td>
<td>Shows failover configuration</td>
</tr>
<tr>
<td>cf failover reset</td>
<td>Resets any indicators, such as a failed interface</td>
</tr>
<tr>
<td>cf failover stop</td>
<td>Stops the failover process</td>
</tr>
<tr>
<td>cf failover restart</td>
<td>Restarts the failover process</td>
</tr>
<tr>
<td>tcpdump -p</td>
<td>Run tcpdump on a load-sharing HA cluster</td>
</tr>
</tbody>
</table>
### Appendix A: Command Line Reference

#### Frequently used commands

<table>
<thead>
<tr>
<th>License commands</th>
<th>Description of use</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>cf license features</code></td>
<td>Prints a list of the currently licensed features</td>
</tr>
<tr>
<td><code>cf license q</code></td>
<td>Show the current license configuration</td>
</tr>
<tr>
<td><code>cf license get</code></td>
<td>Retrieves master key based on license configuration</td>
</tr>
<tr>
<td><code>cf license host list</code></td>
<td>Show list of internal hosts being counted against your license</td>
</tr>
<tr>
<td><code>cf license firewallid</code></td>
<td>Lists the firewall ID used for licensing</td>
</tr>
<tr>
<td><code>cf license read file=filename</code></td>
<td>Read the license from a file for manual activation</td>
</tr>
</tbody>
</table>

### Table 56: Manual pages

<table>
<thead>
<tr>
<th>Man page commands</th>
<th>Description of use</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>man cf_command</code></td>
<td>Use underscores in cf commands to retrieve their man pages</td>
</tr>
<tr>
<td><code>man -k term</code></td>
<td>Shows all man pages that include the specified term; does not return cf commands</td>
</tr>
<tr>
<td><code>apropos term</code></td>
<td>Shows all man pages that are related to the specified term; does not return cf commands</td>
</tr>
</tbody>
</table>

### Table 57: Network

<table>
<thead>
<tr>
<th>Network commands</th>
<th>Description of use</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>netstat -in</code></td>
<td>Show interfaces/ips/networks; see <code>man netstat</code> for additional flags</td>
</tr>
<tr>
<td><code>netstat -I interface -w 5</code></td>
<td>Show live statistics for interface updated every 5 seconds</td>
</tr>
<tr>
<td><code>ifconfig -a</code></td>
<td>Show current network interface parameters</td>
</tr>
<tr>
<td><code>cf interface q</code></td>
<td>Show network interface configuration</td>
</tr>
<tr>
<td><code>cf interface detect</code></td>
<td>Detects new or removed network devices</td>
</tr>
<tr>
<td><code>ping x.x.x.x</code></td>
<td>Ping the specified IP from the appliance</td>
</tr>
</tbody>
</table>
### Table 58: NTP

<table>
<thead>
<tr>
<th>NTP commands</th>
<th>Description of use</th>
</tr>
</thead>
<tbody>
<tr>
<td>cf ntp query</td>
<td>Summary of NTP configuration</td>
</tr>
<tr>
<td>cf server restart ntp burb=burname</td>
<td>Restart a specific NTP server</td>
</tr>
<tr>
<td>ntpdate -bu time_serverIP</td>
<td>Force immediate synchronization with server</td>
</tr>
<tr>
<td>tcpdump -npi interface udp port 123</td>
<td>Packet capture for port 123 (NTP) traffic</td>
</tr>
<tr>
<td>ntpdc</td>
<td>Special NTP query program; see man ntpdc for details</td>
</tr>
</tbody>
</table>

### Table 59: Packages and software

<table>
<thead>
<tr>
<th>Packages and software commands</th>
<th>Description of use</th>
</tr>
</thead>
<tbody>
<tr>
<td>man cf_package</td>
<td>Man page for cf package</td>
</tr>
<tr>
<td>cf package list</td>
<td>Show summary of installed/loaded packages (/var/spool/packages)</td>
</tr>
<tr>
<td>cf package load source=source packages=package_name</td>
<td>Download package</td>
</tr>
<tr>
<td>cf package install package=package_name</td>
<td>Install package (only works in admin kernel)</td>
</tr>
<tr>
<td>cf package uninstall packages=package_name</td>
<td>Uninstall a patch</td>
</tr>
<tr>
<td>cf package load source=cdrom package=package_name</td>
<td>Load a package from a patch CD</td>
</tr>
<tr>
<td>uname -r</td>
<td>Shows the Sidewinder version and patch level</td>
</tr>
</tbody>
</table>

### Table 60: Policy

<table>
<thead>
<tr>
<th>Policy commands</th>
<th>Description of use</th>
</tr>
</thead>
<tbody>
<tr>
<td>man cf_policy</td>
<td>Man page for cf policy</td>
</tr>
<tr>
<td>cf policy q</td>
<td>less</td>
</tr>
<tr>
<td>cf service query</td>
<td>View all services</td>
</tr>
<tr>
<td>cf proxy query</td>
<td>View all proxies</td>
</tr>
<tr>
<td>cf server query</td>
<td>View all servers</td>
</tr>
<tr>
<td>cf appfilter query</td>
<td>Shows all the application defenses</td>
</tr>
</tbody>
</table>

More...
## Frequently used commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description of use</th>
</tr>
</thead>
<tbody>
<tr>
<td>`cf nss query</td>
<td>grep enable`</td>
</tr>
<tr>
<td>`cf nss query</td>
<td>grep service`</td>
</tr>
<tr>
<td><code>ipfilter -v</code></td>
<td>View the ipfilter database currently used by the kernel</td>
</tr>
<tr>
<td><code>ipfilter -x</code></td>
<td>Print the current ipfilter NAT rewrite port range</td>
</tr>
<tr>
<td><code>cf policy reload</code></td>
<td>Reload the ipfilter database being used by the kernel. Active sessions will be dropped</td>
</tr>
</tbody>
</table>

### Policy commands

Table 61: Routing

<table>
<thead>
<tr>
<th>Routing commands</th>
<th>Description of use</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>netstat -nr</code></td>
<td>Show routing table</td>
</tr>
<tr>
<td><code>route -n get x.x.x.x</code></td>
<td>Show route used to get to the specified IP address</td>
</tr>
<tr>
<td><code>route -n get default</code></td>
<td>Show default route</td>
</tr>
<tr>
<td><code>traceroute -n x.x.x.x</code></td>
<td>Shows the route traveled for a destination</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: traceroute is not allowed through the appliance. Follow the route to the appliance and then resume the traceroute from there.</td>
</tr>
<tr>
<td><code>less /etc/route.default</code></td>
<td>View file where default gateway is stored</td>
</tr>
<tr>
<td><code>less /etc/gateways</code></td>
<td>View where routes are stored</td>
</tr>
<tr>
<td></td>
<td><em>(sh /etc/gateways – to load)</em></td>
</tr>
<tr>
<td><code>arp -a</code></td>
<td>Show arp tables</td>
</tr>
<tr>
<td><code>arp -s hostname link_addr</code></td>
<td>Add a static arp entry to the appliance</td>
</tr>
<tr>
<td><code>arp -d hostname</code></td>
<td>Clear arp entry from the appliance</td>
</tr>
<tr>
<td><code>route add host mask gateway</code></td>
<td>Add a route to the appliance</td>
</tr>
<tr>
<td><code>route add default ipaddr</code></td>
<td>Add a default route at the command line</td>
</tr>
<tr>
<td><code>route delete hostname</code></td>
<td>Delete a route. Use ‘default’ as the name for default route</td>
</tr>
<tr>
<td><code>gdc dump</code></td>
<td>Shows OSPF routing information, including neighbors, if gated is running</td>
</tr>
</tbody>
</table>
Table 62: Sendmail

<table>
<thead>
<tr>
<th>Sendmail commands</th>
<th>Description of use</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>cf sendmail flush queue=burb</code></td>
<td>Flushes the mail queue for the specified burb</td>
</tr>
<tr>
<td><code>cf sendmail rebuild</code></td>
<td>Re-hash mailertable; accesstable; etc.</td>
</tr>
<tr>
<td><code>cf daemond restart agent=sendmail</code></td>
<td>Restart the sendmail server</td>
</tr>
<tr>
<td><code>cf server status sendmail</code></td>
<td>Verify if sendmail is running and in which burbs</td>
</tr>
<tr>
<td><code>mailq</code></td>
<td>List the mail queues</td>
</tr>
<tr>
<td><code>tail -f /var/log/maillog</code></td>
<td>Shows the mail log in real time</td>
</tr>
<tr>
<td>`netstat -na</td>
<td>grep LISTEN</td>
</tr>
<tr>
<td><code>ls /var/spool/mqueue.#</code></td>
<td>View directory for queued mail</td>
</tr>
<tr>
<td><code>newaliases</code></td>
<td>Re-hash <code>/etc/aliases</code> file</td>
</tr>
<tr>
<td><code>telnet x.x.x.x 25</code></td>
<td>Telnet to a mail server's IP address on port 25 to test</td>
</tr>
<tr>
<td></td>
<td>SMTP connectivity</td>
</tr>
<tr>
<td>`pss sendmail</td>
<td>grep -c sendmail`</td>
</tr>
<tr>
<td><code>pss sendmail</code></td>
<td>Shows if sendmail is accepting connections</td>
</tr>
</tbody>
</table>

Table 63: Spam filter

<table>
<thead>
<tr>
<th>Spam filter commands</th>
<th>Description of use</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>cf daemond restart agent=spamfilter</code></td>
<td>Restart the spamfilter server</td>
</tr>
<tr>
<td><code>pss spamfilter</code></td>
<td>Show the spamfilter process</td>
</tr>
<tr>
<td>`cf server q</td>
<td>grep spamfilter`</td>
</tr>
</tbody>
</table>

Table 64: Shutdown

<table>
<thead>
<tr>
<th>Shutdown commands</th>
<th>Description of use</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>shutdown -r now</code></td>
<td>Reboot the appliance immediately</td>
</tr>
<tr>
<td><code>shutdown -h now</code></td>
<td>Halt the appliance</td>
</tr>
<tr>
<td><code>shutdown -p now</code></td>
<td>Power off the appliance remotely</td>
</tr>
<tr>
<td><code>shutdown -s now</code></td>
<td>Activate soft shutdown on a load-sharing HA pair to</td>
</tr>
<tr>
<td></td>
<td>direct all connections to one member before shutting</td>
</tr>
<tr>
<td></td>
<td>down the other member</td>
</tr>
<tr>
<td><code>shutdown now</code></td>
<td>Reboot into the emergency maintenance mode</td>
</tr>
<tr>
<td><code>setconsole serial</code></td>
<td>Set booting to the serial console as the default</td>
</tr>
</tbody>
</table>
## Frequently used commands

### System commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description of use</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>top</strong></td>
<td>Display top CPU processes</td>
</tr>
<tr>
<td><strong>man netstat</strong></td>
<td>Man page for netstat</td>
</tr>
<tr>
<td>**netstat -na</td>
<td>grep string**</td>
</tr>
<tr>
<td><strong>netstat -nap tcp</strong></td>
<td>Show open tcp ports</td>
</tr>
<tr>
<td><strong>netstat -m</strong></td>
<td>Display memory management information</td>
</tr>
<tr>
<td><strong>netstat -naf inet</strong></td>
<td>Show all TCP and UDP open ports</td>
</tr>
<tr>
<td>**netstat -Ana</td>
<td>grep LISTEN**</td>
</tr>
<tr>
<td><strong>uptime</strong></td>
<td>Show system uptime since last reboot</td>
</tr>
<tr>
<td><strong>vmstat</strong></td>
<td>Show virtual memory statistics</td>
</tr>
<tr>
<td><strong>connect_mon</strong></td>
<td>Show number of current connections by service</td>
</tr>
<tr>
<td>**pss -axd</td>
<td>more**</td>
</tr>
<tr>
<td><strong>pss process_name</strong></td>
<td>Find a specific process and its process ID (PID)</td>
</tr>
<tr>
<td><strong>dmesg</strong></td>
<td>Display system/hardware information from the system buffer</td>
</tr>
<tr>
<td><strong>kill -HUP pid#</strong></td>
<td>Restart a process but keep the same process ID</td>
</tr>
<tr>
<td><strong>kill pid#</strong></td>
<td>Kill the process with specified process ID</td>
</tr>
<tr>
<td><strong>kill -9 pid#</strong></td>
<td>Force kill of process specified process ID</td>
</tr>
<tr>
<td><strong>cf hostname set name=newhostname</strong></td>
<td>Used in changing the appliance’s host name. See the Knowledge Base for complete procedure.</td>
</tr>
</tbody>
</table>

### tcpdump commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description of use</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>man tcpdump</strong></td>
<td>Man page for tcpdump. See also <a href="http://www.tcpdump.org">www.tcpdump.org</a>.</td>
</tr>
<tr>
<td><strong>tcpdump -npi em0 host X.X.X.X</strong></td>
<td>Show packets on specified interface from/to specified host</td>
</tr>
<tr>
<td><strong>tcpdump -npi em0 -Xs 1500 port y</strong></td>
<td>Show data content of packets for specified port on specified interface</td>
</tr>
<tr>
<td><strong>tcpdump -npi em0 -w filename</strong></td>
<td>Write raw dump to file (can read it with <strong>r</strong> flag or Ethereal). Puts file in current directory named <strong>filename</strong></td>
</tr>
<tr>
<td><strong>tcpdump -p</strong></td>
<td>Run tcpdump on a load-sharing HA cluster</td>
</tr>
</tbody>
</table>
### Table 67: Technical Support

<table>
<thead>
<tr>
<th>Technical Support commands</th>
<th>Description of use</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>scp</code> <code>filename</code></td>
<td>Secure copy a file into Technical Support's incoming directory. Contact Technical Support for password. Be sure to include the ticket number.</td>
</tr>
<tr>
<td><code>scp@scp.support.securecomputing.com:</code> <code>/incoming/</code> <code>ticket#-filename</code></td>
<td></td>
</tr>
<tr>
<td><code>ktrace -p pid#</code></td>
<td>Start a trace of the process with the specified process ID</td>
</tr>
<tr>
<td><code>ktrace -C pid#</code></td>
<td>Stop a process trace; send ktrace results to Technical Support</td>
</tr>
<tr>
<td><code>kill -6 pid#</code></td>
<td>Kill a process and dump a core file of the process; scp file to Technical Support</td>
</tr>
<tr>
<td><code>sysctl -w kern.corefile='%N.core.%P'</code></td>
<td>Include the process ID in the file name of the core; allows multiple core files, which can be examined by Technical Support for troubleshooting purposes</td>
</tr>
<tr>
<td>Use <code>sysctl -w kern.corefile='%N.core'</code> to return to previous operating mode</td>
<td></td>
</tr>
</tbody>
</table>

### Table 68: Text editors and viewers

<table>
<thead>
<tr>
<th>Text editor and viewer commands</th>
<th>Description of use</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vi</code></td>
<td>Powerful but complex screen-based text editor</td>
</tr>
<tr>
<td><code>emacs</code></td>
<td>Another customizable text editor</td>
</tr>
<tr>
<td><code>more</code></td>
<td>View files that contain more lines than can be displayed in terminal</td>
</tr>
<tr>
<td><code>less</code></td>
<td>Similar to ‘more’ but allows for moving backwards in a file, even after reaching the end</td>
</tr>
<tr>
<td><code>view</code></td>
<td>A ‘read-only’ version of vi</td>
</tr>
<tr>
<td><code>cat</code></td>
<td>Create and display short files</td>
</tr>
</tbody>
</table>

### Table 69: TrustedSource

<table>
<thead>
<tr>
<th>TrustedSource command</th>
<th>Description of use</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>blackhole dump</code></td>
<td>List IP addresses currently blackholed by TrustedSource</td>
</tr>
</tbody>
</table>
Table 70: Type Enforcement

<table>
<thead>
<tr>
<th>Type Enforcement commands</th>
<th>Description of use</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ls -alZ</code></td>
<td>Show TE and list files in currently directory</td>
</tr>
<tr>
<td><code>ps -ald</code></td>
<td>Show TE domain information</td>
</tr>
<tr>
<td><code>chtype creator:type filename</code></td>
<td>Change the type enforcement for a file</td>
</tr>
</tbody>
</table>

Table 71: VPN

<table>
<thead>
<tr>
<th>VPN commands</th>
<th>Description of use</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>cf ipsec q</code></td>
<td>Show all configured VPNs</td>
</tr>
<tr>
<td><code>cf ipsec policydump</code></td>
<td>Show active VPNs</td>
</tr>
<tr>
<td><code>cf ipsec reload [flush=1]</code></td>
<td>Flush all existing keys and policy, then reload the VPNs</td>
</tr>
<tr>
<td><code>cf pool q</code></td>
<td>Show client address pools</td>
</tr>
<tr>
<td><code>showaudit -vk</code></td>
<td>Show real time audits on VPN information</td>
</tr>
<tr>
<td>`netstat -na</td>
<td>grep 500`</td>
</tr>
<tr>
<td><code>tcpdump -npi int udp port 500 or proto 50 or proto 51</code></td>
<td>Packet capture for ISAKMP, ESP (IP Proto 50), or AH (IP Proto 51) traffic</td>
</tr>
<tr>
<td><code>tcpdump -npi int udp port 4500</code></td>
<td>Packet capture for NAT-T traffic</td>
</tr>
</tbody>
</table>
List of cf areas

The cf (configure firewall) command makes it possible for you to configure various Sidewinder areas (rules, burbs, DNS, etc.) directly from the UNIX command line. You can use the cf command as an alternative to the Admin Console (the Sidewinder graphical user interface) for performing most system administration tasks.

There are several situations when you may want to use the cf command interface instead of the Admin Console to perform configuration activities. With cf, you can automate repetitive configuration tasks by using scripts. For example, you can use a script to add many similar rules. Also, cf is useful under circumstances when the Admin Console cannot be used, such as performing Sidewinder configuration from a text-only terminal. Another benefit of cf is that it provides a quick and easy way to see how a certain area of your Sidewinder appliance is currently configured.

The following table lists all cf areas, showing the primary commands available for each area. This table does not show the keywords available for each Sidewinder area.

The online manual entry (man page) for cf provides a full description of all areas available in the cf command and the keywords/options associated with each area.

- To display the man page listing for the cf command, enter:
  
  ```
  man cf
  ```

- To display the man page listing for a specific cf area, enter:

  ```
  man cf_command
  ```

  For example, man cf_policy or man cf_interface.

- To display all commands related to a specific command, enter:

  ```
  apropos command
  ```
<table>
<thead>
<tr>
<th>Sidewinder cf area</th>
<th>Commands</th>
<th>Area description</th>
</tr>
</thead>
<tbody>
<tr>
<td>acl</td>
<td>flushcache</td>
<td>Use this area to maintain the access control list (acl) daemon.</td>
</tr>
<tr>
<td></td>
<td>query</td>
<td>• Flush the cache to clear the stored DNS query responses. This is mostly commonly needed after making changes to the DNS database.</td>
</tr>
<tr>
<td></td>
<td>set loglevel</td>
<td>• Query displays the loglevel and caching status.</td>
</tr>
<tr>
<td></td>
<td>set cache</td>
<td>• Set the loglevel to the increase audit message log level during troubleshooting. This shows what rules matched (or did not match) a connection. Always set back to lower level when done, as too much audit can overflow the hard drive.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Set acl response caching to on or off. Having caching set to on increases efficiency and is the default.</td>
</tr>
<tr>
<td>adminuser</td>
<td>add</td>
<td>Use this area to configure the Sidewinder administrator accounts.</td>
</tr>
<tr>
<td></td>
<td>delete</td>
<td></td>
</tr>
<tr>
<td></td>
<td>modify</td>
<td></td>
</tr>
<tr>
<td></td>
<td>set</td>
<td></td>
</tr>
<tr>
<td></td>
<td>query</td>
<td></td>
</tr>
<tr>
<td>agent</td>
<td>modify</td>
<td>Use this area to display and configure proxy, server and filter global agent attributes.</td>
</tr>
<tr>
<td></td>
<td>query</td>
<td></td>
</tr>
<tr>
<td>antivirus</td>
<td>engine set</td>
<td>Use this area to configure the anti-virus scan engine and the Sidewinder’s virus scanning service.</td>
</tr>
<tr>
<td></td>
<td>engine version</td>
<td></td>
</tr>
<tr>
<td></td>
<td>engine download</td>
<td></td>
</tr>
<tr>
<td></td>
<td>engine applyavpatch</td>
<td></td>
</tr>
<tr>
<td></td>
<td>engine undo avpatch</td>
<td></td>
</tr>
<tr>
<td></td>
<td>scanner set</td>
<td></td>
</tr>
<tr>
<td></td>
<td>scanner add</td>
<td></td>
</tr>
<tr>
<td></td>
<td>scanner modify</td>
<td></td>
</tr>
<tr>
<td></td>
<td>scanner delete</td>
<td></td>
</tr>
<tr>
<td></td>
<td>query</td>
<td></td>
</tr>
<tr>
<td>Sidewinder cf area</td>
<td>Commands</td>
<td>Area description</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------</td>
<td>------------------</td>
</tr>
<tr>
<td>appfilter</td>
<td>add</td>
<td>Use this area to configure individual Application Defenses and Application Defense groups.</td>
</tr>
<tr>
<td></td>
<td>delete</td>
<td></td>
</tr>
<tr>
<td></td>
<td>modify</td>
<td></td>
</tr>
<tr>
<td></td>
<td>purge</td>
<td></td>
</tr>
<tr>
<td></td>
<td>set</td>
<td></td>
</tr>
<tr>
<td></td>
<td>defaultgroup</td>
<td></td>
</tr>
<tr>
<td></td>
<td>query</td>
<td></td>
</tr>
<tr>
<td>audit</td>
<td>add</td>
<td>Use this area to configure audit, including auditbot (response), e-mail, and filter options. This area also includes network defenses.</td>
</tr>
<tr>
<td></td>
<td>auditbot</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ad filter</td>
<td></td>
</tr>
<tr>
<td></td>
<td>delete</td>
<td></td>
</tr>
<tr>
<td></td>
<td>auditbot</td>
<td></td>
</tr>
<tr>
<td></td>
<td>delete</td>
<td></td>
</tr>
<tr>
<td></td>
<td>filter</td>
<td></td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>modify</td>
<td></td>
</tr>
<tr>
<td></td>
<td>query</td>
<td></td>
</tr>
<tr>
<td></td>
<td>set</td>
<td></td>
</tr>
<tr>
<td>auth</td>
<td>add</td>
<td>Use this area to manage authenticators.</td>
</tr>
<tr>
<td></td>
<td>delete</td>
<td></td>
</tr>
<tr>
<td></td>
<td>flush</td>
<td></td>
</tr>
<tr>
<td></td>
<td>list</td>
<td></td>
</tr>
<tr>
<td></td>
<td>modify</td>
<td></td>
</tr>
<tr>
<td></td>
<td>query</td>
<td></td>
</tr>
<tr>
<td></td>
<td>set</td>
<td></td>
</tr>
<tr>
<td>burb</td>
<td>add</td>
<td>Use this area to configure burbs.</td>
</tr>
<tr>
<td></td>
<td>modify</td>
<td>Burbs, in general, cannot be deleted if they are currently being used by an active rule. The exception is if the burb is a member of a burb group in an active rule; then the burb can be deleted.</td>
</tr>
<tr>
<td></td>
<td>delete</td>
<td></td>
</tr>
<tr>
<td></td>
<td>start</td>
<td></td>
</tr>
<tr>
<td></td>
<td>query</td>
<td></td>
</tr>
<tr>
<td>burbgroup</td>
<td>add</td>
<td>Use this area to configure burb groups.</td>
</tr>
<tr>
<td></td>
<td>modify</td>
<td></td>
</tr>
<tr>
<td></td>
<td>delete</td>
<td></td>
</tr>
<tr>
<td></td>
<td>query</td>
<td></td>
</tr>
<tr>
<td>Sidewinder cf area</td>
<td>Commands</td>
<td>Area description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>catgroups</td>
<td>add delete modify query</td>
<td>Use this area to manage IPS signatures categories groups.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cert</td>
<td>add delete getcert getkey getcrl modify updatedbs view query</td>
<td>Use this area to manage all certificates, private keys and certificate identities on the Sidewinder appliance.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cluster</td>
<td>status register</td>
<td>Use this area to display the current status and connection state of your Sidewinder cluster and to register a secondary/standby to an HA or OTM cluster.</td>
</tr>
<tr>
<td>cmd</td>
<td>set query</td>
<td>Use this area to configure global settings for the certificate management server on the appliance.</td>
</tr>
<tr>
<td>config</td>
<td>backup restore set list query delete</td>
<td>Use this area to configure the Sidewinder configuration backup and restore process. This does not back up/restore the entire hard disk.</td>
</tr>
<tr>
<td>crontab</td>
<td>set query</td>
<td>Use this area to configure status (enabled/disabled) and frequency of the available cron jobs. The default cron jobs are listed in “Monitoring Sidewinder status” on page 807.</td>
</tr>
<tr>
<td>Sidewinder \n\n\n\ncf area</td>
<td>Commands</td>
<td>Area description</td>
</tr>
<tr>
<td>--------</td>
<td>----------</td>
<td>------------------</td>
</tr>
</tbody>
</table>
| daemond | query    | Use this area to view or configure daemond, and to stop or restart agents.  
\n**Note:** Disabled agents remain stopped until the next policy apply. A policy apply occurs every time a change to rules, rule elements, or the system clock, is saved. |
|         | restart agent=\textit{agentname} |  
|         | set      |  
|         | enable agent=\textit{agentname} |  
|         | disable agent=\textit{agentname} |  |
| dns     | add      | Use this area to configure Sidewinder DNS.  
\n**Note:** When configuring DNS files, do not switch between the Admin Console and a command line editor. The Admin Console will always overwrite any changes made using the command line. |
|         | delete   |  
|         | dumpdb   |  
|         | query    |  
|         | querylog |  
|         | reload   |  
|         | set      |  
|         | status   |  
|         | stats    |  
|         | trace    |  
|         | notrace  |  |
| domain  | add      | Use this area to configure domain network objects. |
|         | delete   |  
|         | modify   |  
|         | purge    |  
|         | query    |  |
| entrelayd | reload | Use this area to reload the entrelayd server’s configuration files and view its connection state and policy status.  
\n**Note:** The preferred method of viewing policy status is \texttt{cf cluster status}. |
<p>|         | status   |  |</p>
<table>
<thead>
<tr>
<th>Sidewinder cf area</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>export</td>
<td>add</td>
</tr>
<tr>
<td></td>
<td>all</td>
</tr>
<tr>
<td></td>
<td>delete</td>
</tr>
<tr>
<td></td>
<td>disable</td>
</tr>
<tr>
<td></td>
<td>enable</td>
</tr>
<tr>
<td></td>
<td>ftp</td>
</tr>
<tr>
<td></td>
<td>modify</td>
</tr>
<tr>
<td></td>
<td>query</td>
</tr>
<tr>
<td></td>
<td>set</td>
</tr>
<tr>
<td></td>
<td>cleanup</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>failover</td>
<td>add</td>
</tr>
<tr>
<td></td>
<td>delete</td>
</tr>
<tr>
<td></td>
<td>query</td>
</tr>
<tr>
<td></td>
<td>reload</td>
</tr>
<tr>
<td></td>
<td>reset</td>
</tr>
<tr>
<td></td>
<td>restart</td>
</tr>
<tr>
<td></td>
<td>set</td>
</tr>
<tr>
<td></td>
<td>softshutdown</td>
</tr>
<tr>
<td></td>
<td>start</td>
</tr>
<tr>
<td></td>
<td>status</td>
</tr>
<tr>
<td></td>
<td>stop</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>fips</td>
<td>set</td>
</tr>
<tr>
<td></td>
<td>query</td>
</tr>
<tr>
<td></td>
<td>verify</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>fwregisterd</td>
<td>set</td>
</tr>
<tr>
<td></td>
<td>unregister</td>
</tr>
<tr>
<td></td>
<td>query</td>
</tr>
</tbody>
</table>

**Area description**

Use this area to configure the audit export utility.

Use this area to configure the failover (High Availability) service.

This area is used to enable/disable FIPS 140-2 compliance mode and to examine the default_SSL_cert to ensure FIPS 140-2 compliance.

Use this area to configure cluster registration on either the cluster manager or the cluster client.
<table>
<thead>
<tr>
<th>Sidewinder cf area</th>
<th>Commands</th>
<th>Area description</th>
</tr>
</thead>
<tbody>
<tr>
<td>gated</td>
<td>set</td>
<td>Use this area to configure the gated daemon.</td>
</tr>
<tr>
<td></td>
<td>add</td>
<td></td>
</tr>
<tr>
<td></td>
<td>modify</td>
<td></td>
</tr>
<tr>
<td></td>
<td>delete</td>
<td></td>
</tr>
<tr>
<td></td>
<td>validate</td>
<td></td>
</tr>
<tr>
<td></td>
<td>query</td>
<td></td>
</tr>
<tr>
<td>host</td>
<td>add</td>
<td>Use this area to configure host network objects.</td>
</tr>
<tr>
<td></td>
<td>delete</td>
<td></td>
</tr>
<tr>
<td></td>
<td>modify</td>
<td></td>
</tr>
<tr>
<td></td>
<td>purge</td>
<td></td>
</tr>
<tr>
<td></td>
<td>query</td>
<td></td>
</tr>
<tr>
<td>hostname</td>
<td>set</td>
<td>Use this to view or change the appliance’s host name.</td>
</tr>
<tr>
<td></td>
<td>query</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> Changing the host name affects DNS configuration, the Sendmail configuration, and entries in all /etc/resolv.conf* files. Make sure to manually change all affected entries. Reboot the appliance after changing the host name.</td>
</tr>
<tr>
<td>ids</td>
<td>add</td>
<td>Use this area to configure the shunning service. Available settings include IDS entries that specify an IP address of an IDS (Intrusion Detection Server), a shared password, and a timeout value that identifies the amount of seconds to shun an IP address. This area is also used to remove IPs from the shunned list.</td>
</tr>
<tr>
<td></td>
<td>delete</td>
<td></td>
</tr>
<tr>
<td></td>
<td>modify</td>
<td></td>
</tr>
<tr>
<td></td>
<td>query</td>
<td></td>
</tr>
<tr>
<td>ikmpd</td>
<td>set</td>
<td>Configure global settings for the ISAKMP server.</td>
</tr>
<tr>
<td></td>
<td>query</td>
<td></td>
</tr>
</tbody>
</table>

*More...*
<table>
<thead>
<tr>
<th>Sidewinder cf area</th>
<th>Commands</th>
<th>Area description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>add, modify, delete, detect, up, down, set, status, swap, query</td>
<td>Use this area to configure the Sidewinder network interfaces.</td>
</tr>
<tr>
<td>ipaddr</td>
<td>add, delete, modify, purge, query</td>
<td>Use this area to configure IP address network objects.</td>
</tr>
<tr>
<td>iprange</td>
<td>add, delete, modify, purge, query</td>
<td>Use this area to configure IP range network objects.</td>
</tr>
<tr>
<td>ips</td>
<td>list, set, reload</td>
<td>Use this area to specify parameters for IPS signature downloads, show attack categories or service categories from a downloaded signature package, or to activate current signature package.</td>
</tr>
</tbody>
</table>
| ipsresponse        | add, delete, modify, purge | Use this area to specify how the appliance responds if its signature-based IPS inspection detects an intrusion.  
  
  **Note:** This is different from IPS Attack Responses, which are controlled using cf audit. |
<table>
<thead>
<tr>
<th>Sidewinder cf area</th>
<th>Commands</th>
<th>Area description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipsec</td>
<td>add</td>
<td>Use this area to configure IPsec parameters and view the VPN status, the IPsec SADB table, and the IPsec SPD table.</td>
</tr>
<tr>
<td></td>
<td>delete</td>
<td></td>
</tr>
<tr>
<td></td>
<td>keydump</td>
<td></td>
</tr>
<tr>
<td></td>
<td>modify</td>
<td></td>
</tr>
<tr>
<td></td>
<td>policydump</td>
<td></td>
</tr>
<tr>
<td></td>
<td>query</td>
<td></td>
</tr>
<tr>
<td></td>
<td>reload</td>
<td></td>
</tr>
<tr>
<td></td>
<td>status</td>
<td></td>
</tr>
<tr>
<td>lca</td>
<td>add</td>
<td>Use this area to configure the local (on-box) certification authority. This feature is not widely used.</td>
</tr>
<tr>
<td></td>
<td>modify</td>
<td></td>
</tr>
<tr>
<td></td>
<td>delete</td>
<td></td>
</tr>
<tr>
<td></td>
<td>query</td>
<td></td>
</tr>
<tr>
<td></td>
<td>list</td>
<td></td>
</tr>
<tr>
<td></td>
<td>revoke</td>
<td></td>
</tr>
<tr>
<td></td>
<td>gencrl</td>
<td></td>
</tr>
<tr>
<td></td>
<td>getcrl</td>
<td></td>
</tr>
<tr>
<td></td>
<td>getcacert</td>
<td></td>
</tr>
<tr>
<td></td>
<td>gencert</td>
<td></td>
</tr>
<tr>
<td>license</td>
<td>check</td>
<td>Use this area to license this Sidewinder and any premium features.</td>
</tr>
<tr>
<td></td>
<td>features</td>
<td></td>
</tr>
<tr>
<td></td>
<td>firewallID</td>
<td></td>
</tr>
<tr>
<td></td>
<td>get</td>
<td></td>
</tr>
<tr>
<td></td>
<td>read</td>
<td></td>
</tr>
<tr>
<td></td>
<td>set</td>
<td></td>
</tr>
<tr>
<td></td>
<td>query</td>
<td></td>
</tr>
<tr>
<td>netgroup</td>
<td>add</td>
<td>Use this area to configure network object groups (netgroups).</td>
</tr>
<tr>
<td></td>
<td>delete</td>
<td></td>
</tr>
<tr>
<td></td>
<td>modify</td>
<td></td>
</tr>
<tr>
<td></td>
<td>purge</td>
<td></td>
</tr>
<tr>
<td></td>
<td>query</td>
<td></td>
</tr>
<tr>
<td>Sidewinder cf area</td>
<td>Commands</td>
<td>Area description</td>
</tr>
<tr>
<td>--------------------</td>
<td>----------</td>
<td>-----------------</td>
</tr>
<tr>
<td>netmap</td>
<td>add, delete, modify, purge, query</td>
<td>Use this area to configure netmap network objects.</td>
</tr>
<tr>
<td>nss</td>
<td>query</td>
<td>Use this area to display current service configuration information as viewed by NSS for a particular service or for all services.</td>
</tr>
<tr>
<td>ntp</td>
<td>add, config, delete, modify, enable, disable, set, restart, query</td>
<td>Use this area to configure network time protocol (NTP).</td>
</tr>
</tbody>
</table>
| package            | list, query, log, description, readme, load, install, uninstall, rollback, rollback_time, autorun, autoload | Use this area to configure the package download system.  
**Caution:** Avoid using autorun and autoload, as they require specific parameters to run. Use install, uninstall, and rollback instead. |
## Sidewinder cf area

<table>
<thead>
<tr>
<th>Sidewinder cf area</th>
<th>Commands</th>
<th>Area description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policy</td>
<td>add</td>
<td>Use this area to manage rules and rule groups, and to export rule elements. Use restore_console_access if the login and Admin Console rules were altered and no longer permit logging into the appliance. The reload command only reloads the filter rule set.</td>
</tr>
<tr>
<td></td>
<td>delete</td>
<td></td>
</tr>
<tr>
<td></td>
<td>export</td>
<td></td>
</tr>
<tr>
<td></td>
<td>modify</td>
<td></td>
</tr>
<tr>
<td></td>
<td>query</td>
<td></td>
</tr>
<tr>
<td></td>
<td>purge</td>
<td></td>
</tr>
<tr>
<td></td>
<td>reload</td>
<td></td>
</tr>
<tr>
<td></td>
<td>repair</td>
<td></td>
</tr>
<tr>
<td></td>
<td>restore_console_access</td>
<td></td>
</tr>
<tr>
<td>pool</td>
<td>add</td>
<td>Use this area to manage client address pools used in IPsec VPN definitions for dynamic client addressing.</td>
</tr>
<tr>
<td></td>
<td>delete</td>
<td></td>
</tr>
<tr>
<td></td>
<td>modify</td>
<td></td>
</tr>
<tr>
<td></td>
<td>query</td>
<td></td>
</tr>
<tr>
<td>proxy</td>
<td>query</td>
<td>Use this area to display Sidewinder proxies configuration data.</td>
</tr>
<tr>
<td>reports</td>
<td>add</td>
<td>Use this area to define, store, and run audit reports.</td>
</tr>
<tr>
<td></td>
<td>delete</td>
<td></td>
</tr>
<tr>
<td></td>
<td>modify</td>
<td></td>
</tr>
<tr>
<td></td>
<td>query</td>
<td></td>
</tr>
<tr>
<td></td>
<td>run</td>
<td></td>
</tr>
<tr>
<td></td>
<td>show</td>
<td></td>
</tr>
<tr>
<td>routed</td>
<td>add</td>
<td>Use this area to configure RIP processing.</td>
</tr>
<tr>
<td></td>
<td>delete</td>
<td></td>
</tr>
<tr>
<td></td>
<td>query</td>
<td></td>
</tr>
<tr>
<td></td>
<td>restart</td>
<td></td>
</tr>
<tr>
<td></td>
<td>set</td>
<td></td>
</tr>
<tr>
<td></td>
<td>start</td>
<td></td>
</tr>
<tr>
<td></td>
<td>stop</td>
<td></td>
</tr>
<tr>
<td>sendmail</td>
<td>flush</td>
<td>Use this area to rebuild the sendmail database files.</td>
</tr>
<tr>
<td></td>
<td>rebuild</td>
<td></td>
</tr>
<tr>
<td>Sidewinder cf area</td>
<td>Commands</td>
<td>Area description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------------</td>
<td>--------------------------------------------------------</td>
</tr>
<tr>
<td>server</td>
<td>status</td>
<td>Use this area to display Sidewinder server state data.</td>
</tr>
<tr>
<td></td>
<td>query</td>
<td></td>
</tr>
<tr>
<td>service</td>
<td>add</td>
<td>Use this area to display and configure Sidewinder proxy,</td>
</tr>
<tr>
<td></td>
<td>delete</td>
<td>server, and filter service attributes.</td>
</tr>
<tr>
<td></td>
<td>modify</td>
<td></td>
</tr>
<tr>
<td></td>
<td>query</td>
<td></td>
</tr>
<tr>
<td>servicegroup</td>
<td>add</td>
<td>Use this area to display and configure Sidewinder service</td>
</tr>
<tr>
<td></td>
<td>delete</td>
<td>group attributes.</td>
</tr>
<tr>
<td></td>
<td>modify</td>
<td></td>
</tr>
<tr>
<td></td>
<td>query</td>
<td></td>
</tr>
<tr>
<td></td>
<td>set</td>
<td></td>
</tr>
<tr>
<td>snmp</td>
<td>add</td>
<td>Use this area to configure simple network management</td>
</tr>
<tr>
<td></td>
<td>delete</td>
<td>protocol (SNMP).</td>
</tr>
<tr>
<td></td>
<td>modify</td>
<td></td>
</tr>
<tr>
<td></td>
<td>query</td>
<td></td>
</tr>
<tr>
<td></td>
<td>set</td>
<td></td>
</tr>
<tr>
<td>ssl</td>
<td>query</td>
<td>Use this area to assign certificates used for SSL</td>
</tr>
<tr>
<td></td>
<td>set</td>
<td>communications for administrative sessions to the appliance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(for example, Admin Console connections).</td>
</tr>
<tr>
<td>static</td>
<td>query</td>
<td>Use this area to manage static network routes.</td>
</tr>
<tr>
<td>subnet</td>
<td>add</td>
<td>Use this area to configure subnet network objects.</td>
</tr>
<tr>
<td></td>
<td>delete</td>
<td></td>
</tr>
<tr>
<td></td>
<td>modify</td>
<td></td>
</tr>
<tr>
<td></td>
<td>purge</td>
<td></td>
</tr>
<tr>
<td></td>
<td>query</td>
<td></td>
</tr>
<tr>
<td>swede</td>
<td>repair</td>
<td>Use this area to repair the Sidewinder enterprise database.</td>
</tr>
<tr>
<td>timeperiod</td>
<td>add</td>
<td>Use this area to configure time period objects.</td>
</tr>
<tr>
<td></td>
<td>delete</td>
<td></td>
</tr>
<tr>
<td></td>
<td>modify</td>
<td></td>
</tr>
<tr>
<td></td>
<td>purge</td>
<td></td>
</tr>
<tr>
<td></td>
<td>query</td>
<td></td>
</tr>
<tr>
<td>Sidewinder cf area</td>
<td>Commands</td>
<td>Area description</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------</td>
<td>------------------</td>
</tr>
<tr>
<td>timezone</td>
<td>set</td>
<td>Use this area to configure the appliance’s time zone.</td>
</tr>
<tr>
<td></td>
<td>query</td>
<td></td>
</tr>
<tr>
<td></td>
<td>list</td>
<td></td>
</tr>
<tr>
<td>udb</td>
<td>add</td>
<td>Use this area to manage the authentication user database.</td>
</tr>
<tr>
<td></td>
<td>delete</td>
<td></td>
</tr>
<tr>
<td></td>
<td>modify</td>
<td></td>
</tr>
<tr>
<td></td>
<td>purge</td>
<td></td>
</tr>
<tr>
<td></td>
<td>query</td>
<td></td>
</tr>
<tr>
<td>ups</td>
<td>query</td>
<td>Use this area to configure the use of an uninterruptible power supply with the appliance.</td>
</tr>
<tr>
<td></td>
<td>set</td>
<td></td>
</tr>
<tr>
<td>usergroup</td>
<td>add</td>
<td>Use this area to configure user groups that are stored in the Sidewinder user database.</td>
</tr>
<tr>
<td></td>
<td>delete</td>
<td></td>
</tr>
<tr>
<td></td>
<td>modify</td>
<td></td>
</tr>
<tr>
<td></td>
<td>purge</td>
<td></td>
</tr>
<tr>
<td></td>
<td>query</td>
<td></td>
</tr>
<tr>
<td>whitelist</td>
<td>add</td>
<td>Use this area to configure the spam filter whitelist.</td>
</tr>
<tr>
<td></td>
<td>modify</td>
<td></td>
</tr>
<tr>
<td></td>
<td>delete</td>
<td></td>
</tr>
<tr>
<td></td>
<td>query</td>
<td></td>
</tr>
</tbody>
</table>
Monitoring Sidewinder status

In addition to the features available on the dashboard, you can use the following commands to check the Sidewinder appliance’s system and network status, and basic DNS information. As always, more information is available in the related man pages.

## Checking system status

You can use the commands in the following sections to display information on the current status of your network connections and view what is happening on the system.

### CPU usage

CPU usage allows you to obtain information on system performance. To view CPU usage information, enter each of the following commands at a Sidewinder command prompt:

```
vmstat
uptime
top
```

### Process status

To view the status of all processes currently running on the appliance, enter either of these commands at a Sidewinder command prompt:

```
ps -axd
pss processname
```

This information is useful for tasks such as determining which processes are using excessive CPU time. The `ps` command allows you to look at information about the processes running on the system. This command is a variation on the standard UNIX process status command in that it includes information on the Sidewinder domains. To display process information, enter:

```
ps -d
```

This command list process information as well as information on the domains in which processes are operating.
In addition to the standard information displayed with the `ps` command, the `-d` switch provide the following additional information:

<table>
<thead>
<tr>
<th>LABEL</th>
<th>PID</th>
<th>TT</th>
<th>STAT</th>
<th>TIME</th>
<th>COMMAND</th>
</tr>
</thead>
<tbody>
<tr>
<td>secureos/Dmnd</td>
<td>189</td>
<td>con</td>
<td>Ss+</td>
<td>0:01.30</td>
<td>/usr/libexec daemond</td>
</tr>
<tr>
<td>secureos/Admn</td>
<td>1360</td>
<td>p0</td>
<td>R+</td>
<td>0:02.05</td>
<td>ps -d</td>
</tr>
</tbody>
</table>

where:

- **LABEL** — domain name
- **PID** — process identification number
- **TT** — terminal line from which the process was initiated
- **STAT** — current status of the process
- **TIME** — total amount of CPU time used by the process
- **COMMAND** — command line used to start the process

**Disk usage**

To view statistics about the amount of free disk space on a file system, enter the following command at a Sidewinder command prompt:

```
 df
```

This information is useful to determine which file systems are using the most disk space.

**Viewing administrator activity**

To view which administrators are currently logged onto your Sidewinder appliance, enter the following command at a Sidewinder command prompt:

```
 who
```

When you use this utility, you can see the administrator's login name, console name, the date and time of their login, and their host name if it is not a local host.

```plaintext
lloyd  tty??  Feb 23 22:11  (a.example.com)
lloyd  ttyp0  Feb 23 21:34  (10.1.1.1)
```
Checking network status

You can use the commands in the following sections to display information on the status of your network connections, routing tables, and network utilities. These commands can provide snapshots of different aspects of your system with command line outputs.

**Note:** Output for `netstat -i` queries will display shared addresses with a plus (+) sign.

**ping**

The `ping` command checks whether an Internet system is running by sending packets that the remote system should echo back. As output, `ping` lists how much time it took for the message to travel to the other system and back, the total number of packets sent and received, the percent of packets lost, and the average and maximum time it took for a round trip. To view this information, enter:

```
  ping -c 5 ipaddress
```

**traceroute**

The `traceroute` command provides information on the gateways an IP packet must pass through to get to a destination. As input, the command needs the host name or IP address of the destination system. It then sends these IP packets from your Sidewinder appliance to that address. As output, it lists the host names and IP addresses of each system the packets were handed off to and how long it took to send each packet back and forth.

To view this information, enter:

```
  traceroute -m 50 -p 33500 ipaddress
```

To run traceroute that crosses burb boundaries, follow it to the appliance and then initiate a second traceroute from the appliance itself.

**Important:** Traceroute is not allowed through the firewall. In addition to security risks, NAT prevents most sites from getting a return from the external network (Internet) because of non-routable addresses.

**Active listens**

To view the status of all active listens, enter:

```
  netstat -na|grep LISTEN
```
To view the status of all open connections, enter:

```bash
netstat -na|grep ESTAB
```

To view the status of all connections waiting for a termination request, enter:

```bash
netstat -na|grep FIN_WAIT_1
```

To view the status of all connections waiting for enough time to pass to be sure the remote TCP received the acknowledgment of its connection termination request, enter:

```bash
netstat -na|grep TIME
```

**Network interfaces**

To view the status of network interfaces on the appliance, enter:

```bash
netstat -in
```

To view statistics of network interfaces on the appliance, enter:

```bash
netstat -s
```

**Routing tables**

To view the status of the Operational kernel’s available routes and their status, enter the following command at a Sidewinder command prompt:

```bash
netstat -r
```

For the same results without DNS data, enter:

```bash
netstat -nr
```

**route get**

The `route get` command looks up the route for a destination and displays the route in the window. To view this information, enter the following command at a Sidewinder command prompt:

```bash
route get ipaddress
```

The following shows sample output for this command:

```
route to: www.example.com
destination: default
mask: default
gateway: host_a
interface: bge0
region: 1
flags: <UP, GATEWAY, DONE, STATIC>
recpipe sendpipe ssthresh rtt,msce rttvar hopcount mtu expire
0 0 0 0 0 0 0 0 1500 0
```
DNS

You can use the dig command to display DNS information.

**dig**

The **dig** (Domain Information Groper) command gathers information from DNS based on a hostname or an IP address. The command queries servers based on type (NS for name servers, MX for mail servers, etc.) and has many advanced options. This command is more powerful than **nslookup**.

```plaintext
dig hostname

dig -x ipaddress
```

Here is an example of dig output:

```
; <<>> DiG 9.3.2 <<>> securecomputing.com
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15043
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0
;; QUESTION SECTION:
;securecomputing.com.           IN      A
;; ANSWER SECTION:
securecomputing.com.    86400   IN      A       66.45.10.76
;; AUTHORITY SECTION:
securecomputing.com.    3600    IN      NS      stpdc02.scur.com.
;; Query time: 7 msec
;; SERVER: 10.65.240.246#53(10.65.240.246)
;; WHEN: Mon Jan  8 19:06:52 2007
;; MSG SIZE  rcvd: 80
```
About automatic (cron) jobs

The appliance contains jobs that perform routine maintenance tasks such as rotating files, cleaning out old files, and controlling software and signature file updates. These jobs are run by the `cron` daemon. The status and frequency of the cron jobs can be configured using `cf crontab`. New automated jobs can also be added using the `cf crontab` command.

Default cron jobs

Many of the default cron jobs are enabled when you enable the corresponding feature in the Admin Console. For example, if you license the anti-spam service and create an enabled rule with anti-spam filtering configured, the appliance automatically enables the `spamfilter_download` cron job. The following table lists the default cron jobs and their functions. Use `cf crontab query` to view additional details about each job.

**Table 73: Default cron jobs**

<table>
<thead>
<tr>
<th>Cron job name</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>audit export</td>
<td>Runs the <code>cf export</code> utility.</td>
</tr>
<tr>
<td>roll audit</td>
<td>Daily rollover of log files.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> See “The roll audit cron job” on page 813 for more information on this cron job.</td>
</tr>
<tr>
<td>roll auditdbd</td>
<td>Daily rollover of report database</td>
</tr>
<tr>
<td>log status</td>
<td>Hourly check of the log files.</td>
</tr>
<tr>
<td>log check</td>
<td>Checks system audit partition utilization hourly. If a partition is 100% full, the appliance stops processing traffic.</td>
</tr>
<tr>
<td>cert</td>
<td>Automatically retrieves updated Certificate Revocation Lists (CRL) and new signed certificates.</td>
</tr>
<tr>
<td>package_run</td>
<td>Installs or rollbacks software updates as schedule in the Software Management area.</td>
</tr>
<tr>
<td>package_download</td>
<td>Downloads any available patches from the designated FTP server.</td>
</tr>
<tr>
<td>licensed host check</td>
<td>Checks for exceeded protected host limits and notifies the administrator via e-mail so that they can take steps to resolve the problem by upgrading the protected host license.</td>
</tr>
<tr>
<td>license expiration check</td>
<td>Checks the license status and notifies the administrator via e-mail when a license is going to expire.</td>
</tr>
</tbody>
</table>
The roll audit cron job

The roll audit cron job serves an important function in monitoring available disk space. There are two `rollaudit` jobs. The first job checks the size of various audit and log files daily at 2:00 a.m. The second job runs each hour and rotates files found to be growing too quickly. When these jobs run, they check the `/secureos/etc/rollaudit.conf` configuration file to see which files should be rotated. The following files are checked by `rollaudit`:

- `/var/log/audit.raw` (The appliance generates reports when these files are rolled.)
- `/var/log/auditd.log`
- `/var/log/cron`
- `/var/log/daemon.log`
- `/var/log/daemond.log`
- `/var/log/messages`
- `/var/log/maillog` (This file is rotated once a week. The output is used for the mail traffic reports described in Chapter 12, "Auditing," on page 359.)
- `/var/log/SF.log`
- `/var/log/snmpd.log`

You can edit the `/secureos/etc/rollaudit.conf` file to specify how large files are allowed to get before they are rotated and the maximum amount of time that should elapse between rotations. See the `rollaudit` man page for details on editing this file.

⚠️ **Caution:** To avoid serious system problems, do not allow the `/var/log` partition to become full. The `/sbin/logcheck` job will generate an e-mail message warning you if the `/var/log` partition becomes 85% full and then again if it becomes 100% full.
Working with files on the appliance

You have several choices for editing files on the appliance:

- The File Editor is an easy-to-use text editor that is available directly from the Admin Console (Maintenance > File Editor). The File Editor simplifies the editing process, which enables you to perform virtually every necessary editing task from the Admin Console instead of command line.

Refer to “Using the Admin Console File Editor” on page 48 for details.

- The appliance also supports typical UNIX editors, including vi and emacs.

In general, use the Admin Console for configuration changes. If you do not have much command line experience, only edit files manually when instructed to do so by the documentation or Technical Support. If you have experience using the command line, remember that files may have been altered for security reasons and therefore may not behave as you expect. For all administrators, create a backup file before making changes so that you can, if necessary, quickly return your appliance to a functional configuration.

About editing Sidewinder files

Sidewinder files are not protected against simultaneous editing by two individuals. Whoever saves the file last usually prevails. In some cases, file corruption occurs.

**Caution:** An administrator should take care not to make changes to a file when another administrator is working on it.

For example, if an administrator is editing the server.conf configuration file using the Admin Console’s File Editor while someone else is using a text editor to change that file, there may be undesirable results. If two people try editing the same file and both are using vi or both are using emacs, however, the editor will warn the users about the situation.

A frequent error to be aware of when manually editing the Sidewinder configuration files (server.conf, roles.conf, etc.) is the misuse of special characters that are used to format commands within these files. Special characters include double quotes, single quotes, brackets ([ ]), the pound symbol (#), and parenthesis ( ). Inadvertently placing special characters in the configuration files will render the files unreadable to the appliance. Enter `man sidewinder.conf` at a command prompt for details.

**Important:** Save any scripts you create for the appliance in the /usr/local/bin directory. During software upgrades, the upgrade procedure will automatically save any scripts that reside in that directory.
Checking file and directory permissions (ls command)

Standard Unix permits access to files based on a process’ user and group identifiers and the file’s permissions (mode bits that indicate who can read, write, or execute a file). As described in Chapter 1, Sidewinder's Type Enforcement mandatory security policy is the ultimate authority on if, and when, a given process may access files and it overrides standard UNIX permissions. A Sidewinder file that appears to be accessible based on standard UNIX permissions can be denied by the Type Enforcement policy.

To check Type Enforcement, enter the following commands and switches:

- for files: `/bin/ls -alZ filename`
- for directories: `/bin/ls -dlZ directory_name`

You will see output similar to the following:

```
secureos/Slog:logs 3965 Feb 23 23:55 cron
```

<table>
<thead>
<tr>
<th>File or directory name</th>
<th>Time stamp</th>
<th>File size</th>
<th>Type (diry for directory, and exec, file, conf, etc. for files)</th>
<th>Creating Domain (such as Admn, $Sys, mtac)</th>
</tr>
</thead>
</table>

Changing a file’s type (chtype command)

Type Enforcement assigns each file and directory a type. In general, you should not, and cannot, change this type. In the rare situation where you need to change the type, use the chtype command.

To change type on a file or directory:

1. At a command prompt, log in and enter the following command to switch to the Admn role:
   ```
srole
   ```

2. Copy the file or directory you want to change:
   ```
cp file1 newfile
   ```

3. Delete the original file:
   ```
rm file1
   ```

4. Change the new file to the target domain and/or file type:
   ```
chtype domain:filetype newfile
   ```

5. Rename the file or directory:
   ```
mv newfile file1
   ```
Creating your own scripts

While operating in either the User or Admn domains, you can create your own scripts for use on the appliance. Scripts created in the User domain are executable by the Admn and User domain but no other domain. Scripts created in the Admn domain cannot be executed by anyone until the type is changed to Admn:scrp using the chtype command.
In this chapter...

Troubleshooting rules ........................................................................................................ 818
Troubleshooting logging in ............................................................................................... 823
Re-install and recovery options ....................................................................................... 825
Re-installing without a CD-ROM drive ............................................................................ 838
Troubleshooting licensing problems .............................................................................. 850
Troubleshooting High Availability .................................................................................. 851
Troubleshooting NTP ...................................................................................................... 857
Troubleshooting VPNs .................................................................................................... 860
Troubleshooting rules

The following sections provide information on troubleshooting basic rule problems. For additional information on troubleshooting rules, refer to the `cf_service` man page.

- “Failed connection requests” on page 818
- “Monitoring allow and deny rule audit events” on page 820
- “Active rules and DNS” on page 822

Failed connection requests

If the appliance rejects a connection request that you think should have succeeded, you can take steps to determine why the connection was rejected. Use the following steps to locate and correct rule configuration errors. They will also help you gain a better understanding of how your rules work.

1. **Verify that the rule is configured correctly:** Select Policy > Rules.
   Verify that the rule in question specifies the correct source and destination burbs and endpoints. If the source burb is incorrect, the service will not listen for incoming connections on the correct network. Check all attributes closely, particularly port settings, application defense settings, and assigned authentication method.

2. **Verify the position of the rules within the Active Rules window:** Select Policy > Rules, and then click Active Rules.
   The order of the rules in the Active Rules window is important. The attributes of a connection request sometimes may match multiple rules. If the traffic is inadvertently matching a similar rule, move the correct rule before the incorrect rule or adjust some of the properties on the incorrect rule.

3. **Check the audit log information.**
   If the connection still fails, scan the audit log to determine which rule denied the connection. See Chapter 12, "Auditing," on page 359 for details on viewing audit.

   The below displays a common scenario, a connection that failed to match a rule:

   Feb 1 16:57:40 2007 CST  f_telnet_proxy a_proxy t_attack p_major
   pid: 44770 ruid: 0 euid: 0 pgid: 44770 logid: 0 cmd: 'tnauthp'
   domain: Atnx edomain: Atnx hostname: a.example.com
   category: policy_violation event: ACL deny attackip: 10.10.1.155
   attackburb: internal srcip: 10.10.1.155 srcport: 4584 srcburb:
   internal dstip: 1.2.3.4 dstport: 23 dstburb: external protocol: 6
   service_name: all-tcpudp user_name: (null) auth_method: (null)
   acl_id: Deny All cache_hit: 0 reason: Access Control List denial
   message
4 Turn on verbose auditing of rule (ACL) checks.

To determine why no proxy rule matched the connection request, type the following command to turn on verbose auditing of rule checks:

```
cf acl set loglevel=4
```

This increases the level of rule audits from the default level 2 (minor) to level 4 (major).

When the next connection attempt is rejected, the service will generate a more verbose audit message as shown below:

```
Feb 1 16:45:28 2007 CST f_ssh_server a_aclquery t_info p_trivial
pid: 44689 ruid: 0 euid: 0 pgid: 44689 logid: 0
cmd: 'sshd' domain: ssh2 edomain: ssh2 hostname: a.example.com
Skip 'ssh to 1.2.3.4': dest IP addr 10.10.1.15 did not match ('ipaddr', '1.2.3.4').
Skip 'ssh from 10.10.1.15': source IP addr 10.10.1.155 did not match ('ipaddr', '10.10.1.150').
Skip 'ssh to DMZ': query dest burb internal != rule's: DMZ.
Skip 'ssh to securecomputing.com': query dest burb internal != rule's: external.
AUTHENTICATION REQUIRED: Access tentatively allowed by rule 'ssh-internal'.
```

Use this output to determine why each rule failed to match the connection request. Locate the rule that you thought should have matched. Then inspect and correct the rule.

5 When you are done troubleshooting, type the following command to lower the level of rule audits back to the default:

```
cf acl set loglevel=2
```

**Important:** If you do not set the loglevel back to 2, you may run out of disk space.

The traffic should now match the correct rule.
Monitoring allow and deny rule audit events

Another troubleshooting tool is the rule monitoring tool (acat_acls). This real time monitoring tool enables you to display allow and deny rule audit events as they occur on the Sidewinder. Because the rule audit events are displayed in real time, this tool provides a Sidewinder administrator a unique window by which to view Sidewinder rule activity. You can use the tool to determine if your rule database is properly configured, or to simply view how your rules are being used on a live system.

For example:

• If you are not certain whether your Telnet rule is properly configured, you can start the monitoring tool, attempt your Telnet connection and see (in real time) whether the connection is allowed or denied.

• If you want to see (in real time) which rules are currently the most heavily used, start the monitoring tool and watch as the current rule audit events scroll by within a command window.

The remainder of this section provides information on using the monitoring tool. Information can also be found by typing `man acat_acls` at a Sidewinder command prompt.

Starting the rule monitoring tool (acat_acls)

To start the rule monitoring tool, enter the following commands at a Sidewinder command prompt:

```bash
acat_acls -a -d
```

where:

• `-a` = display allow rule audit events
• `-d` = display deny rule audit events

If you want to view only allow rule audit events or only deny rule audit events, simply omit the undesired option (`-a` or `-d`).
**Viewing the output from the rule monitoring tool**

Each rule audit event is displayed on a single 80-character line. The source burb and the destination burb fields display the burb index number, not the burb name. The following example shows both an allow rule audit event and a deny rule audit event:

<table>
<thead>
<tr>
<th>Action</th>
<th>Date</th>
<th>Time</th>
<th>Source burb</th>
<th>Source IP</th>
<th>Dest. burb</th>
<th>Dest. IP</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>DENY</td>
<td>02/05/07</td>
<td>02:41:04</td>
<td>2</td>
<td>192.168.179.76</td>
<td>1</td>
<td>192.168.180.87</td>
<td>ping</td>
</tr>
<tr>
<td>ALLOW</td>
<td>02/05/07</td>
<td>02:42:32</td>
<td>2</td>
<td>192.168.179.76</td>
<td>1</td>
<td>192.168.180.87</td>
<td>telnet</td>
</tr>
</tbody>
</table>

**Adjusting rule monitoring tool output**

If the output from the monitoring tool is scrolling by too quickly, you can temporarily halt the output by pressing the following key combination:

**Ctrl+S**

To resume output, press the following key combination:

**Ctrl+Q**

You can also add `|more` or `|less` to a command to control how much output to view at a glance, or redirect the output to a file to view at another time.

**Stopping the rule monitoring tool**

To stop the rule monitoring tool, press the following key combination:

**Ctrl+C**
Active rules and DNS

If you create a proxy rule that contains a host name or a domain name, that rule will consult the Domain Name System (DNS) in order to translate the name to its corresponding IP address. Because of this, there are some facts related to DNS that you should consider when setting up your security policy.

The Sidewinder can be configured to use transparent DNS, one DNS server (known as single or unbound DNS), or two DNS servers (known as split DNS). The split DNS scenario is the most secure, as one DNS server is dedicated to your Internet burb and the second DNS server services your remaining burbs. This essentially isolates the two DNS servers from each other, protecting your non-Internet burbs from attacks by malicious persons on the Internet.

However, it is theoretically possible for attackers on the Internet to feed false information to your Internet DNS server. Therefore, you should be careful when using rules to allow or deny access to specific hosts on the Internet.

When dealing with outside connections, there are steps that you can take to increase the level of assurance:

1. Use IP addresses in your rule instead of host names or domain names. This avoids having to depend on external DNS.
2. Make the rule demand strong authentication (for example, SafeWord).
3. Make the rule demand encryption of the connection (for example, VPN).

Tip: For additional protection, you should do a combination of the above.
Troubleshooting logging in

If you forget your administrator password, you can boot the appliance into emergency maintenance mode (EMM) and reset your password.

**Important:** By default, the EMM does not require authentication. However, if you have configured your system to require authentication to enter that mode, you will need to temporarily disable EMM authentication before you can enter that mode and change your password. For information on disabling EMM when you have forgotten your password, see “Changing authentication requirements for emergency maintenance mode” on page 824.

Restoring access to the appliance

If an administrator accidentally alters the rule set in a way that prevents an administrator from logging into the appliance (for example, moving the Deny All rule to the first position or deleting certain access rules), use this procedure to restore access.

To regain access to both the local console and the Admin Console:

1. At the local console, reboot the appliance.
2. At the Sidewinder boot menu, select **2. Boot in Emergency Maintenance Mode**. A prompt appears stating:

   Enter full pathname of shell or RETURN for /bin/sh:

4. Restore console access by entering the following:
   ```
   cf policy restore_console_access
   ```
   This command recreates the default local console and the Admin Console rules. The rules are added to the beginning of the rule set.
5. Reboot to the Operational kernel by entering the following:
   ```
   shutdown -r now
   ```

You can now log in at the local console or with an Admin Console session initiated on the appliance’s internal burb.
Changing a forgotten password

You must be at the Sidewinder local console to run this procedure.

To change your administrator account password:

1 Reboot the system.
2 At the Sidewinder boot menu, select Emergency Maintenance Mode.
3 Press Enter when asked what shell patch to use. The system prompt appears.
4 Enter the following command to change your password:
   \[ \text{cf adminuser modify user=\_name password=\_newpassword} \]
5 Reboot to the Operational kernel by entering the following command:
   \[ \text{shutdown -r now} \]

You can now log into the appliance using your new password.

Manually clearing an authentication failure lockout

If you have enabled the authentication failure lockout option and are locked out of your system, have another administrator log using the Admin Console and clear the lock (see “Configuring an authenticator” on page 301).

However, if you do not have another administrator who can clear your lock for you, you can still manually clear your lock by successfully logging in at the appliance’s local console. When you successfully log in, the lock automatically clears and you can now log into the Admin Console as usual.

Changing authentication requirements for emergency maintenance mode

To change authentication for entering the emergency maintenance mode:

1 Log into the Admin Console, and select Maintenance > File Editor.
2 Click Start File Editor.
3 Select File > Open.
4 In the Source field, select Firewall File.
5 In the File field, type /etc/\_ttys and click OK.
6 Edit the following line:
   \[ \text{console none unknown off secure} \]
   • To require authentication, change the value to insecure.
   • To disable authentication, change the value to secure.
7 Save your changes and close the file editor.

The authentication requirements are now changed.
There are several options available for when your appliance experiences a severe software or hardware problem. Recovery options range from a rollback to a previous restore point to fix short-term problems to re-installing a full backup onto new hardware. The overview section describes the recovery options and when to use them. The procedures are in the following sections:

- “Overview of recovery options” on page 825
- “Re-installing your appliance from the virtual CD” on page 830
- “Re-installing your appliance from a CD-ROM” on page 832
- “About the disaster recovery option via USB flash drive” on page 834
- “Re-installing without a CD-ROM drive” on page 838

**Overview of recovery options**

Occasionally, you may experience a situation where you need to restore your appliance to a working configuration. The Sidewinder appliance has several recovery options to fit different severities and types of situations. Do the following to maximize recovery success:

- Create configuration backups on a regular basis.
- Create disaster recovery backups after installing a new patch.
- When selecting a recovery option, always attempt the least disruptive option first and determine if that solves your problem.

The following sections describe the available recovery options.

**Configuration restore**

The policy configuration restore replaces the appliance’s current policy with a saved configuration file. Create configuration backups frequently to ensure you have an up-to-date configuration backup from when the policy was known to be configured correctly.

Use this option when misconfiguration or data corruption renders the current policy unacceptable, or to return to a recent configuration after completing a re-install.

See “Configuration file backup and restore” on page 691 for this procedure.
Uninstall
The uninstall option removes a patch but maintains the current configuration. Patches can be uninstalled individually or several at a time. Patches that can be uninstalled are listed with an Uninstall status of Yes. They are often smaller patches that do not include features or substantial changes, such as vendor patches and hotfixes.

Use this option when a newly installed uninstallable patch fails to install or introduces behavior that is incompatible with your policy.

This procedure is an option in the Maintenance > Software Management area. See “About the Software Management: Manage Packages tab” on page 719 for information on uninstalling patches.

Rollback
The rollback option reverts your appliance to the previous restore point, which is a snapshot of the patch level and policy configuration just before the most recent patch was installed. If multiple patches were installed at the same time, then the restore point is before the earliest patch.

Use this option when a newly installed patch fails to install or introduces unexpected behavior that is incompatible with your policy. With the rollback option, all configuration changes made between when the problematic patch was installed and when the rollback was initiated are lost.

This procedure is an option in the Maintenance > Software Management area. See “About the Software Management: Rollback tab” on page 727 for information on scheduling and initiating a rollback.

Re-install
The re-install option is to be used when the appliance has experienced a serious hardware failure, such as a failed hard drive, or when the appliance is to be repurposed, such as moving it from one network to another. You can re-install your appliance from its virtual CD or from the Sidewinder Installation - Disk Imaging CD. With the virtual CD, you can individually select which patches to install. When using the physical CD, you can automatically install all previously installed patches using disaster recovery media.

- Re-installing from the virtual CD (VCD)
  The re-install option restores your appliance using the virtual CD (VCD). During the re-install process, you select which patches to install from a list of packages that were available on the appliance before starting the re-install procedure. This option provides flexibility in what version the appliance will be after the recovery. Make sure you know which patches need to be installed to match the configuration backup you intend to restore.

  **Note:** Using this option with disaster recovery media is not recommended, as there is a chance that the selected patches will not match the patches in the disaster recovery media.

  See “Re-installing your appliance from the virtual CD” on page 830 for this procedure.
Appendix B: Basic Troubleshooting
Re-install and recovery options

- **Re-installing from a CD-ROM**
  You must insert the Sidewinder CD into the appliance or use the PXE boot re-installing process to install the Sidewinder software on the appliance. This option is less flexible than restoring from the VCD, but requires less interaction with the appliance.

  If your appliance has a CD drive, see “Re-installing your appliance from a CD-ROM” on page 832. If your appliance does not have a CD drive, see “Re-installing without a CD-ROM drive” on page 838.

  Consult Technical Support to ensure that re-installing is your best remaining option.

**Disaster recovery restore**

The disaster recovery restore option restores your appliance to a previous patch level and configuration by restoring files from a USB flash drive containing a disaster recovery backup. This backup includes all installed patches, an initial configuration, and the standard configuration backup files. This option is an efficient way to return your appliance to its previous patch level and a known configuration. If you have a configuration backup that is more recent than the one on your disaster recovery media, you may want to restore that after the recovery completes.

Use this option to recover after replacing a hard disk or entire system, or if the policy becomes seriously misconfigured or corrupt.

Note the following:

- Disaster recovery backups can only be saved on a USB flash drive. See “About the disaster recovery option via USB flash drive” on page 834.
- Do not alter the disaster recovery backup file.
- The disaster recovery files are intended to be restored on the same hardware as when they were created. If you attempt to restore the backup to different hardware, expect to make significant adjustments.

⚠️ **Caution:** Failure to follow the guidelines listed above could corrupt the disaster recovery backup.
There are two options for creating disaster recovery media:

- Create the disaster recovery media using the Backup Builder. The Backup Builder is a standalone application available on the Sidewinder patch website. It combines a Quick Start Wizard data file, a configuration backup, and the base and patches required for that configuration backup and saves the combined backup to a USB flash drive. See “Using the Backup Builder” on page 835 for information.

- Create disaster recovery media using the Create Disaster Recovery Media option on the Configuration Backup window (Maintenance > Configuration Backup). This recovery media includes the configuration and installed patches that were on the appliance when the recovery media was made. See “About the Configuration Backup: Configuration Backup tab” on page 692 for information on creating a configuration backup.

For the disaster recovery restore procedure, see “About the disaster recovery option via USB flash drive” on page 834.
Summary of options

The following table lists common problems and their recommended recovery solution.

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patch upgrade failed or caused unexpected behavior.</td>
<td>Use the uninstall or rollback option.</td>
</tr>
<tr>
<td>Software or configuration disaster.</td>
<td>Select the least disruptive option: configuration restore, uninstall or rollback, or re-install.</td>
</tr>
<tr>
<td>Repurpose system in some way, such as moving an appliance from one network to another.</td>
<td>Re-install and create a new configuration.</td>
</tr>
<tr>
<td>Hard disk failure or system replacement.</td>
<td>Re-install and restore an existing configuration.</td>
</tr>
</tbody>
</table>

Before re-installing, determine which process can best create the final configuration that meets your needs. See the following table for options.

<table>
<thead>
<tr>
<th>Re-install process</th>
<th>Recovery options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Re-install from the virtual CD</td>
<td>• Load or create an initial configuration and restore a configuration backup.</td>
</tr>
<tr>
<td></td>
<td>• Load or create an initial configuration and create a new policy.</td>
</tr>
<tr>
<td>Re-install from the physical CD</td>
<td>• Restore from a disaster recovery backup created using the Create Disaster Recovery Backup option or the Backup Builder. You may also want to restore a recent configuration backup.</td>
</tr>
<tr>
<td></td>
<td>• Load or create an initial configuration, download and install the necessary patches, and restore a configuration backup.</td>
</tr>
<tr>
<td></td>
<td>• Load or create an initial configuration, and create a new policy.</td>
</tr>
</tbody>
</table>
Re-installing your appliance from the virtual CD

Use this procedure to re-install your Sidewinder appliance from the virtual CD, which contains a copy of all installed patches. Re-installing from the VCD is appropriate when the appliance needs to be repurposed or needs to recover from a software or configuration disaster, and the hard drive is still functional. This option gives you the opportunity to select which packages to install.

Note the following:

• This method does not require the Sidewinder Disk Imaging - Installation CD.

• Plan your restore method before you begin. Options include:
  – Load or create an initial configuration, and create a new policy.
  – Load or create an initial configuration and restore a configuration backup. Know which patches need to be installed to match the configuration backup you intend to restore.

• If you are using a serial terminal for this procedure, use the hot keys to make selections. Using the arrow keys may have unexpected results.

To re-install from the virtual CD:

1 Power on or reboot the appliance.
   After the standard boot information completes, a menu similar to the following appears:
   
   Secure Computing
   F1 Virtual CD
   F2 Alternate Slice
   F3 Operational Slice
   
   F3 Default

2 Press F1 to enter the Virtual CD.
   The “Welcome to Sidewinder!” menu for the virtual CD appears.

3 Select a Sidewinder boot option:
   • To accept the default installation option, press Enter.
   • If you intend to use a serial console, type 4 and press Enter.

   Note: The Emergency Maintenance Mode option, the Boot with ACPI option, and the Escape to Loader Prompt option are generally only to be used on instruction from Technical Support and are not appropriate for this procedure.

The VCD Sidewinder Main Menu appears, displaying the following options:

Select and Install — Select and install Sidewinder Packages
Maintenance Shell — VCD Maintenance Shell Menu
Advanced Menus — Advanced Install Menus
[RTN To select] X Exit Install
4 Press S to select Select and Install, and then press Enter.
   A menu appears listing all available packages.

5 [Conditional] If selecting packages:
   • Use the hot keys or the up and down arrows to move among the packages. (If using a serial connection, only use the hot keys.)
   • Use the space bar to select a package or clear a previous selection.
   • Press O for OK when ready to install the selected packages.
   • Press C to cancel and return to the previous menu.

6 [Conditional] After pressing O for OK, you are prompted to confirm your selection. Press Y.
   The packages install. When installation is complete, the VCD Main Menu appears again.

7 Press X to exit. You are prompted to confirm your decision and reminded to remove all media from the floppy and CD drives.

8 Press Y. The appliance reboots.

9 At the Secure Computing menu, accept the default, which is the Operational System.

10 At the Welcome to Sidewinder! boot menu, select a boot method.

11 Provide the appropriate initial configuration using one of these methods:
   • Insert a USB flash drive containing a disaster recovery backup. (See License information is included in the backup file.
   • Run your chosen Quick Start method. (See the Sidewinder Startup Guide for more information.)
   The appliance tries to send the license activation request for one minute. If the activation is not successful in that time, you must activate your appliance using the Admin Console.

12 Connect to your appliance using the Admin Console.

13 [Conditional] If you need to restore a configuration backup, select Maintenance > Configuration Backup and restore your Sidewinder configuration data. See “Configuration file backup and restore” on page 691 for more information.

Your appliance is now re-installed.
Re-installing your appliance from a CD-ROM

Use this procedure to re-install your Sidewinder appliance from the Sidewinder Installation - Disk Imaging CD. This procedure should only be used as a last resort, such as when the appliance has had a hardware failure or has been completely replaced. Generally, you should only run this procedure under guidance from Technical Support.

Note the following:

• Plan your restore method before you begin. Options include:
  – Restore a disaster recovery backup from a USB flash drive. You may also want to restore a recent configuration backup.
  – Load or create an initial configuration, download and install the necessary patches, and restore a configuration backup.
  – Load or create an initial configuration, and create a new policy.

• You will need your Sidewinder Installation–Disk Imaging CD. All Sidewinder software on the CD will be installed on the appliance.

To re-install from a CD:

1 Boot the appliance from the Sidewinder Installation - Disk Imaging CD:
   • If the appliance is on, insert the CD and then reboot.
   • If the appliance is off, power it on and then quickly insert the CD.
   The appliance boots from the CD and displays standard boot-up information.

2 [Conditional] By default, the boot order is set to check the CD drive first. If the boot order has been altered and does not check the CD drive first, reboot and enter the BIOS to adjust the boot order accordingly.

3 At the Secure Computing menu, accept the default, which is the Operational System.

4 Then the “Welcome to Sidewinder!” boot menu appears.

5 Select a Sidewinder boot option:
   • To accept the default installation option, press Enter.
   • If you intend to use a serial console, type 4 and press Enter.

**Note:** The Emergency Maintenance Mode option, the Boot with ACPI option, and the Escape to Loader Prompt option are generally only to be used on instruction from Technical Support and are not appropriate for this procedure.

The appliance loads and installs the Sidewinder packages.

6 When the “Installation complete” message appears, remove the CD from its drive.
Appendix B: Basic Troubleshooting
Re-install and recovery options

7 Press R to reboot the appliance, and then press Enter. The appliance boots and displays standard boot-up information.

8 At the Secure Computing menu, accept the default, which is the Operational System.

9 At the Welcome to Sidewinder! boot menu, select a boot method.

10 Provide the appropriate initial configuration using one of these methods:
   • Insert a USB flash drive containing a disaster recovery backup.
     License information is included in the backup file.
   • Run your chosen Quick Start method. (See the Sidewinder Startup Guide for more information.)
     The appliance tries to send the license activation request for one minute. If the activation is not successful in that time, you must activate your appliance using the Admin Console. If the system cannot retrieve its license key, the appliance comes up with a temporary license. You must obtain your license within 7 days.

11 Connect to your appliance using the Admin Console.

12 [Conditional] If you need to install additional patches, select Maintenance > Software Management. See “Software management” on page 716 for more information.

13 [Conditional] If you need to restore a configuration backup, select Maintenance > Configuration Backup and restore your Sidewinder configuration data. See “Configuration file backup and restore” on page 691 for more information.

Your appliance is now re-installed.
About the disaster recovery option via USB flash drive

This option automatically saves the necessary configuration information and patches to a USB flash drive. Use this option when recovering from a failed hard drive or when configuring a replacement appliance. Save backups often to ensure that you can quickly return to the correct patch level and configuration.

Selecting a USB flash drive

Your USB flash drive must meet the following requirements:

- Supported USB flash drive sizes are 1 GB, 2 GB, 4 GB, and 8 GB. The flash drive must be large enough to hold the configuration and patches. In general, a 1 GB flash drive should be sufficient for most appliances. Configurations with large home directories may require a larger size.

- Supported brands are:
  - 1 GB Secure Computing branded
  - 1 GB PQI® “Mr Flash U172”
  - 1 GB “PNY Attache™”
  - 2 GB “SanDisk Cruzer® Titanium”
  - 2 GB “A-DATA® PD2 My Flash”
  - 4 GB “Super Talent™ Ultra Flash”
  - 4 GB “A-DATA PD2”
  - 8 GB “Transcend JetFlash™”
  - 8 GB “A-DATA PD2”

Other brands may work, but have not been tested.

- Your flash drive must be formatted in MS-DOS.

- The Sidewinder appliance’s USB port must be enabled in the BIOS settings.

Saving the disaster recovery backup

There are two options for creating disaster recovery media:

- **Using the Maintenance > Configuration Backup window**
  
  This recovery media includes the configuration and installed patches that were on the appliance when the recovery media was made.

  To save a disaster recovery backup:

  1. Insert a USB flash drive in the appliance’s USB port.
    
    **Caution:** This process will overwrite anything on the flash drive, including previous disaster recovery backups.

  2. Select Maintenance > Configuration Backup.

  3. Click Create Disaster Recovery Backup. The Configuration Backup and Restore: Disaster Recovery window appears.
4 [Optional] Enter a key to encrypt the disaster recovery backup. Valid values include alphanumeric characters, periods (.), dashes(-), underscores (_), and spaces ( ).
   • This key will not be saved. You must remember it. You will not be able to restore the disaster recovery backup without this key.
   • You do not have to enter an encryption key. If you click OK without entering an encryption key, the backup continues.

Enter the key again to verify.

5 Click OK. A warning message appears.

6 Click Yes to confirm the backup.

A progress bar appears while the files are backed up to the flash drive.

**Note:** Do not remove the USB flash drive from the appliance until the “Disaster recovery successful” message appears.

When the backup is complete, a “successful” message appears.

7 Click OK.

8 The disaster recovery file is saved to the USB flash drive.

• **Using the Backup Builder**

Create the disaster recovery media using the Backup Builder. The Backup Builder is a standalone application available on the Sidewinder patch web site. It combines a Quick Start Wizard data file, a configuration backup, and the base and patches required for that configuration backup and saves the combined backup to a USB flash drive.

To download the Backup Builder:

1 Go to [www.securecomputing.com/goto/updates](http://www.securecomputing.com/goto/updates) and click Sidewinder 7.0 Upgrades and Patches.

2 Enter your Sidewinder serial number and click Submit.

3 In the Sidewinder 7.0 Upgrades area, select Sidewinder 7 Backup Builder.

4 Follow the on-screen instructions to download the Backup Builder.

To create a disaster recovery media using the Backup Builder:

1 Verify you have the necessary tools:
   • the Backup Builder
   • a USB flash drive
   • Access to the necessary patches. The first time you use the Backup Builder, you will need the Sidewinder 7 base from the Sidewinder 7 Installation - Disk Imaging CD and additional patches from a network connection or CD. Once the Backup Builder downloads a patch, it saves it in a local package directory.
2 Create a Quick Start Wizard configuration file:
   a Select **Start > Programs > Secure Computing > Sidewinder 7 Admin Console > Quick Start Wizard**.
   b Run the Quick Start Wizard. If you need more information, see the online help or the *Sidewinder Startup Guide*.
   c On the Quick Start Summary window, save the file as a text file or without an extension, and then close the Quick Start Wizard.

3 Go to **Start > Programs > Secure Computing > Sidewinder 7 Backup Builder > Sidewinder 7 Backup Builder**.
   The Backup Builder opens.

4 In the Sidewinder 7 Configuration Backup field, click **Browse** and browse to the 7.0-compatible backup you created in Procedure 2.

5 In the Quick Start Wizard Configuration File field, click **Browse** and browse to the file you created in step 2 of this procedure.

6 In the Required Packages area, retrieve the required packages:
   • To download packages from the Secure Computing HTTP activation server select the package or packages and click **Download Now**.
   • To import packages from a specified location, select the package or packages and click **Import**.

7 Insert the USB flash drive into a USB port on this computer and check its drive mapping. Verify that the Backup Builder’s removable media drive matches this drive.

8 Click **Create Combined Backup**.
   The backup containing the configuration backup, the Quick Start Wizard configuration file, and the required patches is saved to the USB flash drive.
Appendix B: Basic Troubleshooting
Re-install and recovery options

Restoring the backup

To restore the disaster recovery configuration:

1 Verify you have the necessary tools:
   • Sidewinder Disk Installation - Imaging CD
   • USB flash drive containing the disaster recovery backup
   • If the appliance does not have a CD drive:
     • a Windows XP computer installed with the VMware Player and the
       PXE Imaging Server for Sidewinder
     • a cross-over cable

2 Insert the USB flash drive into the appliance’s USB port.

3 Follow the appropriate re-installing method:
   • If the appliance has a CD drive, see “Re-installing your appliance from a
     CD-ROM” on page 832.
   • If the appliance does not have a CD drive, see “Re-installing without a
     CD-ROM drive” on page 838.

4 Immediately after the re-install completes, remove the CD from the drive.

5 Leave the USB flash drive in its port until the recovery is complete. You can
   remove the drive after the Admin prompt appears, or leave the USB drive in
   the appliance for future use.

The appliance is now restored to the patch level and configuration saved in that
backup.
Re-installing without a CD-ROM drive

This section explains how to re-install Sidewinder software on an appliance that does not have a CD-ROM drive.

How CD-less re-installing works

To re-install a Sidewinder appliance that does not have a CD-ROM drive, you create an imaging server on a separate computer and use a cross-over cable to connect the imaging server to the appliance.

**Note:** Re-installing a Sidewinder appliance over a network is not supported.

1 Download and install VMware Player® on a Windows® XP computer. This allows you to run a virtual machine on the Windows computer.

2 Download and install the Sidewinder 7 PXE Imaging Server software on the Windows computer. This creates a virtual machine — the PXE Imaging Server — on the Windows computer.

**Note:** Some appliances were shipped with the PXE Imaging Server software on a CD.

3 Install the Sidewinder Installation-Disk Imaging software on the Sidewinder 7 PXE Imaging Server.

4 Re-install the appliance over a cross-over cable.

After the re-installing is complete, your appliance will be in one of these states:

- If you use this procedure in conjunction with a USB device containing a disaster recovery backup file, you will restore the appliance to the patch level and configuration stored in that backup.

- If you use this procedure without a disaster recovery backup, optional patches, such as hotfixes, engineering patches, anti-virus, or anti-spam patches, are not included in Sidewinder re-installing software. You may install any optional patches after re-installing your appliance.
System requirements

The computer you use to re-install the appliance must meet the following requirements:

**Operating system:**

Windows XP Professional or Home Edition with Service Pack 1 or 2

**System requirements for VMware Player:**

- Processor speed — 400 MHz or faster (500 MHz or faster recommended)
- Memory — 128 MB minimum, 256 MB recommended
  You must have enough memory to run the host operating system, plus the memory required for each guest operating system and for applications on the host and guest. See your guest operating system and application documentation for their memory requirements.
- Hard disk — At least 700 MB free disk space for the PXE Imaging Server
  For installation, VMware Player requires approximately 150 MB.

**Other requirements:**

- Internet connection
- Cross-over cable
- VGA console or serial console
- Sidewinder Installation-Disk Imaging CD (version 7.0.0.xx only)
Re-installing the Sidewinder

Perform these four procedures to re-install an appliance without a CD drive:

- “Procedure 1 – Download and install VMware Player” on page 840
- “Procedure 2 – Download and install the Sidewinder 7 PXE Imaging Server software” on page 841
- “Procedure 3 – Install the Sidewinder re-installation software” on page 842
- “Procedure 4 – Re-installing the Sidewinder appliance” on page 845

Procedure 1 – Download and install VMware Player

Download the free VMware Player software and install it on your Windows XP computer.

Note: The VMware Player software is free.

1. Open a browser and go to www.vmware.com/products/player. The VMware Player page appears.

2. Follow the on-screen instructions to download the VMware Player. You will be asked to complete an on-line registration form. When the installation is finished, click Yes at the prompt to reboot your computer.

3. Disable VMware Player virtual interfaces:
   b. Right-click VMware Network Adapter VMnet1 and select Disable from the pop-up menu.

   c. Right-click VMware Network Adapter VMnet8 and select Disable from the pop-up menu.

   d. Close the Network Connections window.

Continue with “Procedure 2 – Download and install the Sidewinder 7 PXE Imaging Server software” on page 841.
Appendix B: Basic Troubleshooting

Re-installing without a CD-ROM drive

Procedure 2 – Download and install the Sidewinder 7 PXE Imaging Server software

Perform this procedure to download the Sidewinder 7 PXE Imaging Server software and install it on the Windows XP computer.

- This download is over 500 MB. You can request a CD version of the software using the Product Upgrade and CD Request form. Use your Sidewinder serial number and enter "Sidewinder 7 PXE Imaging Server" in the Requested Version field.
- Some appliances were shipped with the PXE Imaging Server software on a CD.

To download and install the Sidewinder 7 PXE Imaging Server software:

1. Open a browser and go to www.securecomputing.com/goto/updates.
2. Click Sidewinder 7.0.0 Upgrades and Patches.
3. Type your Sidewinder serial number, then click Submit.
4. In the Contents box on the left, click 7.0.0 Re-imaging Tools.
5. Right-click Sidewinder 7 PXE Imaging Server and save it to your Windows XP desktop.
6. On the desktop of the Windows XP computer, double-click the SW7_PXE_200.exe icon.
   Follow the on-screen prompts to install the Sidewinder 7 PXE Imaging Server software.

To install the Sidewinder 7 PXE Imaging Server software from a CD:

1. Insert the CD into your Window’s XP computer’s CD-ROM drive.
2. Navigate to the CD’s contents and double-click SW7_PXE_200.exe.
3. Follow the on-screen prompts to install the Sidewinder 7 PXE Imaging Server software.

The PXE Imaging Server is now installed on the VMware Player on the Windows XP computer.
**Procedure 3 – Install the Sidewinder re-installation software**

Perform this procedure to install the Sidewinder re-installation software on the Sidewinder 7 PXE Imaging Server. You need the Sidewinder Installation-Disk Imaging CD for this procedure.

1. **[Conditional] If you use dynamic addressing (DHCP), you must assign a static IP address in order for the re-installation process to work properly.**

   Open the Internet Protocol (TCP/IP) Properties window and select **Use the following IP address**, then enter an IP address and subnet mask.

   ![Internet Protocol (TCP/IP) Properties window](image)
2 On the Windows XP computer, open the Sidewinder 7 PXE Imaging Server:

   a Click **Start > Programs > VMware > VMware Player**. The Browse for virtual machine configuration file window appears.

   b Navigate to `C:\Documents and Settings\user\My Documents\My Virtual Machines\SW7PXELImagingServer`.

   c Select **FreeBSD.vmx** and click **Open**.

A message appears stating that the location of the configuration file has changed.

**Note:** This message appears only the first time you open the Sidewinder 7 PXE Imaging Server. It will not appear in subsequent uses.
d Verify or select **Create**, then click **OK**.

The Sidewinder 7 PXE Imaging Server (SW7PXEImagingServer) boots FreeBSD, then screen text appears telling you to insert Sidewinder media in the CD-ROM drive.

3 Insert the Sidewinder Installation-Disk Imaging CD into the CD-ROM drive. “Copying files...” text appears while files are copied from the CD to the imaging server.

“Done” appears when the files are copied, then a login prompt appears. You do not need to log in.

4 Remove the Sidewinder Installation-Disk Imaging CD.

You are finished installing the Sidewinder re-installation software. Continue with “Procedure 4 – Re-installing the Sidewinder appliance” on page 845.
Appendix B: Basic Troubleshooting

Re-installing without a CD-ROM drive

Procedure 4 – Re-installing the Sidewinder appliance

Perform this procedure to re-install the appliance using the Sidewinder 7 PXE Imaging Server software on the Windows XP computer.

1 Disconnect all network cables from the Sidewinder.

---

Important: The re-install may fail if network cables are not disconnected.

---

2 Using a cross-over cable, physically connect the Windows XP computer to the Sidewinder.

3 Connect a VGA console or serial console to the Sidewinder. If you use a serial console, you can use a terminal emulator such as HyperTerminal.

   If you are connecting with a terminal or terminal emulator, you will need to set the parameters listed below:

<table>
<thead>
<tr>
<th>Port settings</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>COM1</td>
</tr>
<tr>
<td>Bits per second</td>
<td>9600</td>
</tr>
<tr>
<td>Data bits</td>
<td>8</td>
</tr>
<tr>
<td>Parity</td>
<td>None</td>
</tr>
<tr>
<td>Stop bits</td>
<td>1</td>
</tr>
<tr>
<td>Flow control</td>
<td>None</td>
</tr>
</tbody>
</table>

   Windows XP — If you are connecting with a terminal or terminal emulator on a Windows XP computer, set the parameters in the Device Manager of that computer:

   a Click Start > Control Panel.

   b Double-click System (in Category view, click Performance and Maintenance, then System). The System Properties window appears.

   c Click the Hardware tab.

   d Click the Device Manager button.

   e Expand Ports (COM & LPT).

   f Double-click Communications Port (COM1).

   g Click the Port Settings tab.

   h Select the appropriate port settings from the drop-down lists.

   i Click OK, then close the open windows.
4 Configure the Sidewinder to boot from the ethernet card. The method to boot from the ethernet card varies by model. You might need to do any of the following:
   • Enter the BIOS settings and enable the ethernet card option.
   • Enter the BIOS settings and change the boot order.
   • Press a key during startup to initiate booting from the ethernet card.

5 Reboot the Sidewinder from the ethernet card.

The appliance restarts from the Sidewinder 7 PXE Imaging Server and the re-installation process begins. You do not need to take any action while the Sidewinder is re-installed.

When the re-installation is complete:
   • Disconnect the cross-over cable from the appliance and the Windows XP computer.
   • [If necessary] Enter the BIOS settings of the appliance and configure it to boot from the hard drive.
   • Turn off the Sidewinder 7 PXE Imaging Server on the Windows XP computer: From the Player drop-down menu, select Troubleshoot > Power Off and Exit.
   • [If necessary] Re-assign dynamic addressing (DHCP) on the Windows XP computer through the Internet Protocol (TCP/IP) Properties window.
   • Re-connect the network cables to the appliance.

Refer to the Sidewinder Startup Guide to configure the appliance.
Updating the image on the Sidewinder 7 PXE Imaging Server

Perform this procedure to update the Sidewinder re-imaging software currently installed on the Sidewinder 7 PXE Imaging Server.

Important information:

• **Do not perform this procedure unless required.** The Sidewinder 7 PXE Imaging Server needs to be updated only for hardware-related issues. This will typically happen if you need to re-install a Sidewinder appliance that is not supported by the version of re-imaging software you previously installed on the Sidewinder 7 PXE Imaging Server.

• Do not install optional patches, such as hotfixes, engineering patches, or anti-virus patches, on the Sidewinder 7 PXE Imaging Server. After re-installing, you can re-install any optional patches on the appliance.

• Patches must be installed on the Sidewinder 7 PXE Imaging Server via CD.
  - If a patch CD is mailed to you, go to “Install the patch” on page 848.
  - If a patch is downloaded from the Secure Computing web site, you must first perform the procedure “[Conditional] Create a patch CD” below.

[Conditional] Create a patch CD

Patches must be installed on the Sidewinder 7 PXE Imaging Server via CD. Perform this procedure if you download a Sidewinder patch from the Secure Computing web site.

*Note:* You need a computer with a recordable CD drive and CD-writing software in order to create a patch CD from the download file.

1. Insert a recordable CD into the Windows XP CD-ROM drive.

2. On the Windows XP computer, create a folder on the desktop called \packages.


4. Right-click the desired patch link and select Save Target As… from the pop-up menu. The Save As window appears.

5. From the Save in drop-down list, select Desktop\packages, then click Save.

6. Using your CD-creation software, select the ISO 9660 file system format and burn the \packages folder onto the CD.

7. Remove the patch CD from the CD drive.

You are done creating a patch CD.
Install the patch

On the Windows XP computer that contains the Sidewinder 7 PXE Imaging Server:

1. Make sure no CD is in the CD drive. Have your patch CD ready but do not insert it until instructed.

2. Open the Sidewinder 7 PXE Imaging Server (SW7PXIEImagingServer):

   Note: If the PXE Imaging Server is already open, it must be reset: From the Player drop-down menu, select Troubleshoot > Reset. Wait for the “insert Sidewinder media” message, then go to step 3.

   a. Click Start > Programs > VMware > VMware Player. The Browse for virtual machine configuration file window appears.

   b. Navigate to C:\Documents and Settings\user\My Documents\My Virtual Machines\SW7PXIEImagingServer.

   c. Select FreeBSD.vmx and click Open.
FreeBSD boots on the Sidewinder 7 PXE Imaging Server, then screen text appears telling you to insert Sidewinder media in the CD-ROM drive in 30 seconds.

3 Insert the patch CD into the CD-ROM drive. “Copying files...” text appears while files are copied from the CD to the virtual server.

“Done” appears when the files are copied, then a login prompt appears. You do not need to log in.

4 Remove the patch CD from the CD-ROM drive.

You are finished updating the Sidewinder image on the Sidewinder 7 PXE Imaging Server. Refer to “Procedure 4 – Re-installing the Sidewinder appliance” on page 845 for Sidewinder re-installation instructions.
Appendix B: Basic Troubleshooting

Troubleshooting licensing problems

If the appliance comes up in failure mode because it did not license during the reboot, check the following:

- Try to obtain the license by entering:
  ```
  cf license get
  ```
- Verify that there is a default route by entering:
  ```
  netstat -nr
  ```
  If there is not a default route, add it back with
  ```
  route add default aaa.bbb.ccc.ddd
  ```
  where `aaa.bbb.ccc.ddd` is the next hop router for the default route.
- Verify that DNS is resolving by entering:
  ```
  dig www.securecomputing.com
  ```
- Obtain the license by doing one of the following:
  - If DNS is resolving, enter `cf license get`.
  - If DNS is not resolving, you will need to get the license using the Secure Computing activation server’s IP address by entering the following on a single line:
    ```
    cf license get activation_url=https://66.45.10.76/cgi-bin/sidewinder-activation.cgi
    ```
- Reboot the appliance again by entering:
  ```
  shutdown -r now
  ```

The appliance should now be correctly licensed and fully functional.
Troubleshooting High Availability

This section provides information to determine whether High Availability is functioning properly.

**Viewing configuration-specific information**

The `cf failover query` command gives you configuration-specific information, as shown in the following example:

```bash
failover set heartbeat_burb=heartbeat ping_wait=1 interval_time=1 \ interface_test_failures=3 priority=245 multicast_group=239.255.0.1 \ firewall_id=20 interface_test_time=30 load_sharing=off enabled=on
failover set password=1ff130fdb0 type=SHA1
failover add address alias=10.65.249.20 network=10.65.249.0 burb=external
failover add address alias=10.65.248.20 network=10.65.248.0 burb=internal
failover add address alias=10.65.247.20 network=10.65.247.0 burb=heartbeat
```
The `cf cluster status` command gives an overview of the whole cluster, as shown in the following example:

```
HA Cluster Status Information
-------------------------------
Primary Host:      myprimary.example.net
Primary IPAddress: 10.65.247.2
Cluster Burb:      'heartbeat'
Cluster CERT:      'Default_Enterprise_Certificate'
Cluster CA:        'Default_Enterprise_CA'

Member Name          State         IP address
==================== ============= ===============
mysecondary.example. ne registered    10.65.247.3
myprimary.example.ne registered   10.65.247.2

Policy and Peer Connection Status
---------------------------------
mysecondary.example.net (peer)
-------------------------------
Connection State : Currently Connected
Policy Version    : 25-1172343142.61-1172343140
FW Version        : 70000
Status            : Ready

myprimary.example.net (primary)
-------------------------------
Connection State : Localhost
Policy Version    : 25-1172343142.61-1172343140
FW Version        : 70000
Status            : Up to date - Current
```
Viewing status information

The `cf failover status` command gives you information on whether or not HA is active, what state the system is in (primary or secondary/standby), and useful statistical information.

Viewing status information for a primary

The following example shows sample results for a primary in a peer-to-peer HA configuration:

This system is operating in load sharing mode as primary.

This system is node 0.
The secondary is node 1 (10.65.247.3).
Failover is running in burb 3
shared cluster address 10.65.249.20 assigned to interface fxp0
shared cluster address 10.65.248.20 assigned to interface xl0

Failover interface status:
  Interface em0 not monitored
  Interface fxp0 not monitored
  Interface xl0 not monitored

IP Filter tracking state as load sharing peer

Active firewall list:
  node  address
  1  10.65.247.3        (secondary)

A backup heartbeat interface is not configured

Statistics for failover

Failover running since Sat Feb 24 14:06:48 2007
Primary since Sat Feb 24 14:16:47 2007

Failover allowing 3 seconds for interface swap (default)

Number of advertisements sent = 1078
Number of received advertisements = 498
Number of rcvd advertisements since primary = 498
Number of times this system has become primary = 2
Number of release messages received = 0
Number of release messages sent = 0
Number of failed takeover attempts = 0
Number of possible duplicate primary messages = 0
Appendix B: Basic Troubleshooting

Troubleshooting High Availability

Number of heartbeat ack messages received = 501
Number of heartbeat ack messages sent = 0
Number of messages received with errors = 0
Number of same priority advertisements rcvd = 0
Number of pings received on interface em0 = 0
Number of pings received on interface fxp0 = 0
Number of pings received on interface xl0 = 0
Viewing status information for a secondary

The following example shows sample results for a secondary that is configured for load-sharing HA:

This system is operating in load sharing mode as secondary.

This system is node 1.
The primary is node 0 (10.65.247.2).
Failover is running in burb 3
cluster heartbeat address 10.65.247.20 assigned to interface em0
shared cluster address 10.65.249.20 assigned to interface fxp0
shared cluster address 10.65.248.20 assigned to interface xl0

Failover interface status:
  Interface em0 not monitored
  Interface fxp0 not monitored
  Interface xl0 not monitored

IP Filter tracking state as load sharing peer

Active firewall list:
  node  address
  0  10.65.247.2        (primary)

A backup heartbeat interface is not configured

Statistics for failover

Failover running since Sat Feb 24 14:16:43 2007

Failover allowing 3 seconds for interface swap (default)

Number of advertisements sent                    = 0
Number of received advertisements                = 291
Number of rcvd advertisements since primary      = 291
Number of times this system has become primary   = 0
Number of release messages received              = 0
Number of release messages sent                   = 0
Number of failed takeover attempts               = 0
Number of possible duplicate primary messages    = 0
Number of heartbeat ack messages received         = 0
Number of heartbeat ack messages sent             = 291
Number of messages received with errors           = 0
Number of same priority advertisements rcvd       = 0
Number of pings received on interface  em0        = 0
Number of pings received on interface  fxp0       = 0
Number of pings received on interface  xl0        = 0
Identifying load-sharing addresses in netstat and ifconfig

Output for netstat -i queries will display load sharing addresses with a plus (+) sign. The following example displays the results for the netstat -i command with load sharing enabled.

<table>
<thead>
<tr>
<th>Name</th>
<th>Mtu</th>
<th>Network</th>
<th>Address</th>
<th>Ipvts</th>
<th>Ierrs</th>
<th>Opkts</th>
<th>Oerrs</th>
<th>Coll</th>
</tr>
</thead>
<tbody>
<tr>
<td>fxp0</td>
<td>1500</td>
<td>&lt;Link#1&gt;</td>
<td>00:a0:c9:9d:99:a1</td>
<td>3059</td>
<td>0</td>
<td>2869</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>fxp0</td>
<td>1500</td>
<td>10.65.249/2410.65.249.20</td>
<td>129</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fxp0</td>
<td>1500</td>
<td>10.65.249/24a</td>
<td>98</td>
<td></td>
<td></td>
<td></td>
<td>77</td>
<td></td>
</tr>
<tr>
<td>x10</td>
<td>1500</td>
<td>&lt;Link#2&gt;</td>
<td>00:10:5a:98:51:26</td>
<td>0</td>
<td>0</td>
<td>10</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>x10</td>
<td>1500</td>
<td>10.65.248/2410.65.248.20</td>
<td>0</td>
<td></td>
<td></td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>x10</td>
<td>1500</td>
<td>10.65.248/24a.example.com</td>
<td>0</td>
<td></td>
<td></td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>em0</td>
<td>1500</td>
<td>&lt;Link#3&gt;</td>
<td>00:0c:f1:c7:ba:ea</td>
<td>506253</td>
<td>0</td>
<td>356438</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>em0</td>
<td>1500</td>
<td>10.65.247/2410.65.247.20</td>
<td>95</td>
<td></td>
<td></td>
<td>642</td>
<td></td>
<td></td>
</tr>
<tr>
<td>em0</td>
<td>1500</td>
<td>10.65.247/2410.65.247.2</td>
<td>611</td>
<td></td>
<td></td>
<td>248</td>
<td></td>
<td></td>
</tr>
<tr>
<td>lo0</td>
<td>16384</td>
<td>&lt;Link#4&gt;</td>
<td>7478</td>
<td></td>
<td>0</td>
<td>7478</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>lo0</td>
<td>16384</td>
<td>127</td>
<td>localhost</td>
<td>3951</td>
<td></td>
<td>7478</td>
<td></td>
<td></td>
</tr>
<tr>
<td>lo2</td>
<td>16384</td>
<td>&lt;Link#5&gt;</td>
<td>114</td>
<td></td>
<td>0</td>
<td>114</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>lo2</td>
<td>16384</td>
<td>127</td>
<td>localhost_2</td>
<td>57</td>
<td></td>
<td>114</td>
<td></td>
<td></td>
</tr>
<tr>
<td>lo1</td>
<td>16384</td>
<td>&lt;Link#6&gt;</td>
<td>0</td>
<td></td>
<td>0</td>
<td>0</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>lo1</td>
<td>16384</td>
<td>127</td>
<td>localhost_1</td>
<td>0</td>
<td></td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>lo3</td>
<td>16384</td>
<td>&lt;Link#7&gt;</td>
<td>0</td>
<td></td>
<td>0</td>
<td>0</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>lo3</td>
<td>16384</td>
<td>127</td>
<td>127.3.0.1</td>
<td>0</td>
<td></td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Interface configuration issues with HA

If you modify your interface configuration, your HA configuration will not function until you update the HA Interfaces table (in the Admin Console, select High Availability > Common Parameters tab) to match the modified interface configuration. When you are finished updating the interface information, reboot the appliances.

Troubleshooting remote interface test failover for peer-to-peer HA

If you have a peer-to-peer HA cluster configured and the remote host used for interface testing becomes unavailable, the primary will report an interface failure after the specified number of failed ping attempts is reached, and failover will occur. When this happens, the new primary receives the interface failure status from the former primary, and interface failure testing is disabled. In this state, the standby takes over for the primary only if the primary becomes unavailable.

Once the remote host is restored, issue the cf failover reset command on the current standby, and then issue the cf failover reset command on the current primary, in order to reset and re-enable the interface failover indicators.
Troubleshooting NTP

Use the commands in this section to verify that NTP traffic is passing as expected. If NTP is experiencing problems, use the following commands to help determine the cause.

Verify that NTP is running and using the correct time

- Check the NTP daemon is running on the time server that is serving time to the Sidewinder appliance:
  
  `ps -df |grep ntpd`

  If ntpd is not running, correct this problem before proceeding.

  Run the `ntpd` command to show that the NTP daemon is responding to the request:

  `ntpd -q -u server_ip`

  where `server_ip` is the IP address of the time server. This command also reports if the queried server time is different from the appliance’s system time. To check the time on a Sidewinder-hosted NTP server, use the IP address of the burb where the NTP server is running.

  **Note:** To run the above commands, you need command line access to the NTP server.

- Check the process to see that the Sidewinder NTP server is enabled and running:

  `pss ntpd`

  `cf server status ntp`

- If you have NTP properly configured and enabled, you should be able to monitor NTP packets being sent/received on the appropriate Sidewinder interfaces. To do so, enter the following commands:

  `tcpdump -npi if_name udp port 123`

  where `if_name` is the interface and number that you are troubleshooting (for example `em0`, `em1`, etc.)

  In the `tcpdump` output, check to make sure that NTP packets are being both sent and received. If traffic is not flowing both ways, verify the routing connectivity between your Sidewinder appliance and the NTP server.

- To check the appliance’s exact system time, enter the `date` command and compare it to a known good clock source (for example, www.time.gov).
Troubleshooting NTP when the Sidewinder is an NTP client

Here is an example of the output of the `ntpd` command, where the Sidewinder is configured as an NTP client and the IP address 100.1.1.199 is the IP address of the Sidewinder’s interface that is running NTP:

```
fw:Admn {1} % ntpdc -s 100.1.1.199
remote           local      st poll reach  delay   offset    disp
===========================================================
*  cisco1-mhk.kans 100.1.1.199  2  128  377 0.06488  0.013563 0.00798
.  triangle.kansas 100.1.1.199  2  128  377 0.06522  0.013999 0.00902
.  ns.nts.umn.edu   100.1.1.199  16 128  377 0.07059  0.002498 0.00983
```

This is a list of the time servers that the Sidewinder appliance is configured to query for time. The stratum field will tell you whether the appliance is able to communicate properly with the time servers. In this case, the first two entries have a stratum of 2, while the third has a stratum of 16. A stratum of 16 always indicates that the appliance is not synchronizing successfully with a time server. In this case, the appliance was able to communicate properly with the first two servers, but not with the third.

Troubleshooting NTP when the Sidewinder is an NTP server

Here is an example of the output of the `ntpd` command when the Sidewinder appliance is configured as an NTP server and the IP address 100.100.2.200 is the IP address of the Sidewinder’s interface that is running NTP:

```
Fw2:Admn {1} % ntpdc -s 100.1.2.200
remote      local      st poll reach  delay   offset    disp
===========================================================
  100.1.2.50 100.1.2.200  3  128  377 0.06488  0.013563 0.00798
```

This is a list of the NTP clients that are configured to get time from the Sidewinder appliance. The stratum field will tell you if the appliance is able to communicate properly with the NTP clients. In this case, the client 100.1.2.50 has a stratum of 2, which means it is communicating properly. A stratum of 16 would indicate that the client was not synchronizing successfully with the appliance.

In most situations, you can look at the stratum to determine whether or not NTP is configured properly and working. There is additional information in the `ntpd` output that may be useful in troubleshooting NTP issues. However, that information is out of the scope of this document.
**Synchronization problems**

If you are having synchronization problems, enter the following command:

```
ntpdc
```

Use `man ntpdc` to see detailed information.

**Possible reason NTP stopped**

NTP is designed to automatically quit whenever the client’s time deviates from the server’s signal by more than 15 minutes. When a deviation of this magnitude occurs, NTP writes a message to file `/var/log/messages` before quitting.

To restart NTP, first set the Sidewinder’s clock manually (refer to “Setting the system date and time” on page 684) and then follow the directions in the next section for restarting NTP.

**Restarting NTP from a command line prompt**

If the NTP process stops, you can restart the NTP process by doing the following:

1. To start the NTP time server, enter the following command:
   ```
   cf daemond restart agent=ntp
   ```
2. [Optional] Verify the state of the NTP servers by entering the following command:
   ```
   cf server status ntp
   ```
In addition to standard logging, the appliance also performs auditing of certain system events which allows you to generate information on VPN connections. Table 74 shows some useful commands you can use to track VPN connections in real time mode and check VPN settings/configuration.

**Table 74: Basic Sidewinder VPN troubleshooting commands**

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>tcpdump -npi ext_if port 500 or proto 50 or proto 51</code></td>
<td>Show IPsec, ESP, and AH traffic arriving at the appliance.</td>
</tr>
<tr>
<td><code>tcpdump -npi if_name udp port 4500</code></td>
<td>Show NAT-T traffic arriving at the appliance.</td>
</tr>
<tr>
<td><code>cf ipsec q</code></td>
<td>Review VPN policies.</td>
</tr>
<tr>
<td><code>cf ipsec policydump</code></td>
<td>Determine if VPN is active. The presence of SPI and transform numbers indicates the secure connection is functioning.</td>
</tr>
<tr>
<td><code>showaudit -vk</code></td>
<td>Show detailed audit trace information for VPN in real time.</td>
</tr>
</tbody>
</table>

To enable a more detailed auditing level, adjust the ISAKMP server’s audit level:

1. In the Admin Console, select **Policy > Rule Elements > Services**.
2. Select **isakmp**, and click **Properties**.
3. Set the audit level to **Verbose**.
4. Click **OK** on both windows.
5. Save your changes.
<table>
<thead>
<tr>
<th><strong>activation</strong></th>
<th>The process by which a customer’s licensed software becomes active.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>activation key</strong></td>
<td>A string of numbers and characters that allows the operation of the software.</td>
</tr>
<tr>
<td><strong>ActiveX</strong></td>
<td>Microsoft’s name for certain object-oriented programming technologies and tools. ActiveX is often downloaded and executed on a local system when browsing the Internet, and may require specific port restrictions. Consult Microsoft’s documentation for more information.</td>
</tr>
<tr>
<td><strong>Admin Console</strong></td>
<td>The graphic user interface (GUI) used to configure and manage the Sidewinder appliance. The Admin Console runs on Windows-based platforms.</td>
</tr>
<tr>
<td><strong>Admin Console tree</strong></td>
<td>The hierarchical layout in the left–hand panel of the Admin Console.</td>
</tr>
<tr>
<td><strong>Admn domain</strong></td>
<td>The physical and logical resources within the UNIX operating system that has access to most of the other domains.</td>
</tr>
<tr>
<td><strong>admin role</strong></td>
<td>The role is assigned to administrators authorized to work in the Admn domain with full privileges. An administrator assigned the admin role can use all menus and commands in the Admin Console. This includes adding or removing users, backing up and restoring the system, and using all other system functions and commands.</td>
</tr>
<tr>
<td><strong>adminRO role</strong></td>
<td>The read–only role assigned to administrators authorized to access and view, but not modify, information. The AdminRO role is essentially an auditor role, allowing the administrator to view system and audit information, as well as generate reports.</td>
</tr>
<tr>
<td><strong>agent</strong></td>
<td>The process responsible for managing a service’s traffic. The transport layer information includes elements such as the protocol, the ports, and the connection or session timeouts. Agents can be type proxy, filter, or server. Each type consists of several different agents, such as the Generic Proxy, the TCP/UDP Packet Filter Agent, and the SNMP Agent.</td>
</tr>
<tr>
<td><strong>alarm event</strong></td>
<td>A Sidewinder feature used to monitor your network for potentially threatening activity, such as an attempted attack or an audit overflow. When an alarm event is generated, an appropriate event response is issued.</td>
</tr>
<tr>
<td><strong>alias</strong></td>
<td>An arbitrary name that a system administrator can assign to a network element.</td>
</tr>
</tbody>
</table>
Application Defenses™: A feature that is incorporated in rules to configure application-specific properties for each service on a per-rule basis. Properties include application-specific permissions, as well as anti-virus/spyware, anti-spam/fraud, SSL decryption, and Web services management for key proxies.

application-layer proxy: Also known as an intelligent proxy. Application-layer proxies check application-layer data as it comes into the Sidewinder appliance. If the data is compliant with that application's standard, the appliance initiates a new connection on its opposite side and passes on the data. If the data is not compliant, the appliance drops the data.

ARP (address resolution protocol): A protocol used to map an IP address to a MAC address. A gratuitous ARP is a system broadcasting its own information, often after an address change, so other devices can update their ARP caches.

auditing: A method of collecting and storing information that can be used to track system activity, such as authentication attempts, configuration modifications, stopping and starting of services, etc.

authentication: A process that verifies the authenticity of a person or system before allowing access to a network system or service.

authenticator: A device or mechanism used to verify the identity of an individual logging onto a network, application, or computer.

BIND (Berkeley Internet Name Domain): A standard program which implements the domain name system (DNS).

burb: Refers to an interface and all the systems it connects. The systems in a burb are to be treated the same from a system security policy point of view.

certificate: See digital certificate.

Certificate Authority (CA): A highly trusted entity, that issues and revokes certificates for a set of subjects, and is ultimately responsible for their authenticity.

cipher key: In order for encryption to be unique, it uses a random set of characters, called a cipher key. Encrypting data using two different keys will produce two completely different results. All authenticators contain at least one key that they use to generate passwords.

client: A program or user that requests network service(s) from a server.

cluster: Two or more Sidewinder appliances in a High Availability or One-to-Many configuration. Appliances in a cluster serve as backups for each other or share the network load.

Cluster Wizard: A Sidewinder wizard used for creating and taking apart One-to-Many and High Availability clusters.

configuration backup: A process that saves policy information, user account information, and home directory contents to a single backup file. You can use a configuration backup file to quickly restore an appliance to a previous operational state.
**console**
Refers to any monitor and keyboard attached directly to a Sidewinder appliance. Can also refer to the Admin Console, the graphical user interface used to manage the appliance.

**daemon**
A software routine within UNIX that runs in the background, performing system-wide functions.

**daemond**
(Pronounced daimon-dee) A powerful Sidewinder component process that enhances overall security by monitoring and controlling all of the appliance’s major software components. It also detects and audits some classes of attacks against the appliance.

**DHCP (dynamic host configuration protocol)**
A protocol for dynamically assigning IP addresses to networked devices. In a dynamic environment, IP addresses may change frequently. Using DHCP addressing requires the device be on a network with a DHCP server.

**digital certificate**
A data structure that is digitally signed by a CA, or a signature source that users can trust. The certificate contains a series of values, such as the certificate name and usage, information identifying the owner of the public key, the public key itself, an expiration date, and the name of the CA that generated the certificate.

**disaster recovery media**
A system backup saved to a USB flash drive that contains all installed patches, a configuration backup, and initial configuration information.

**DMZ (demilitarized zone)**
A network buffer zone that generally hosts services that require interaction with Internet traffic, while still protecting internal systems. On the Sidewinder appliance, the DMZ is generally a burb for hosting Web servers and other hosts that receiving large volumes of external, untrusted traffic.

**DNS (domain name system)**
A TCP/IP service that maps domain and host names to IP addresses, IP addresses to domain and host names, and provides information about services and points of contact in a network or the Internet. A set of connected name servers and resolvers allows users to use a host name rather a 32-bit Internet address.

**domain**
(1) Relative to networking, the portion of an Internet address that denotes the name of a computer network. For instance, in the e-address jones@example.sales.com, the domain is example.sales.com.  (2) Relative to Type Enforcement, an attribute applied to a process running on SecureOS that determines which system operation the process may perform.

**DoS (Denial of Service)**
Event in which a network experiences a loss of a service, like e-mail or a Web server, that is expected to be available. This event is generally caused by a malicious attack, but may also happen accidentally.

**dynamic password**
The unique one–time response to a log in challenge or special code presented by an authentication server. Each password is obtained using a software or hardware authenticator that communicates with a password generator.
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>editor</td>
<td>A program that can be used to create or modify text files. See also <em>File Editor</em>.</td>
</tr>
<tr>
<td>Emergency Maintenance Mode (EMM)</td>
<td>An operating state that allows you to do repair work with other services turned off. The appliance does not pass traffic. You must connect a local console to the appliance to work with it. Similar to the single-user mode in UNIX systems.</td>
</tr>
<tr>
<td>encryption</td>
<td>Data encryption uses a secret code to scramble information so that it can be read only by computers using the same code or encryption technology. While encryption reduces the risk of unauthorized access, it does not create a totally safe networking environment on its own.</td>
</tr>
<tr>
<td>end user</td>
<td>See <em>user</em>.</td>
</tr>
<tr>
<td>event response</td>
<td>A response to an alarm event that includes notifying the administrator and/or performing a Strikeback.</td>
</tr>
<tr>
<td>extended authentication (XAUTH)</td>
<td>An extension of the IKE protocol. It provides a mechanism to employ an administrator–selected authentication mechanism in addition to the existing IKE authentication (that is, in addition to certificate based or pre-shared key authentication). It initiates after the existing IKE authentication mechanism is successful. XAUTH enables use of strong authentication (sometimes referred to as legacy authentication) in VPN configurations.</td>
</tr>
<tr>
<td>external DNS</td>
<td>External DNS provides a limited external view of the organizational domain. No internal information is available to the external DNS and only the external DNS can communicate with the outside. Therefore, no internal naming information can be obtained by anyone on the outside. The external DNS cannot query the internal DNS or any other DNS server inside the Sidewinder appliance.</td>
</tr>
<tr>
<td>failover</td>
<td>See <em>high availability</em>.</td>
</tr>
<tr>
<td>failure mode</td>
<td>See <em>safe mode</em>.</td>
</tr>
<tr>
<td>File Editor</td>
<td>The program available directly in the Admin Console that can be used to create or modify text files. The File Editor communicates with the Sidewinder appliance using a secured connection.</td>
</tr>
<tr>
<td>filter</td>
<td>A software agent that is used to create packet filter services. The filter agent handles traffic at the network layer or the transport layer of the network stack.</td>
</tr>
<tr>
<td>FIPS</td>
<td>Federal Information Processing Standard 140-2 is a standard that describes the U.S. federal government requirements for a cryptographic module used in a security system.</td>
</tr>
<tr>
<td>firewall</td>
<td>A network component that filters traffic between a designated “protected network” and external networks. A firewall ensures that the protected network is safe from unauthorized entry and file manipulation.</td>
</tr>
<tr>
<td>firewall ID</td>
<td>An automatically generated number used to identify your Sidewinder appliance. The firewall ID is used when activating your appliance.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>------</td>
<td>------------</td>
</tr>
<tr>
<td><strong>fixed password</strong></td>
<td>A string of characters of varying lengths and composition (text and/or numerics) used to identify a user attempting to access a service. Fixed passwords remain unchanged unless given a finite life span. Fixed passwords are also known as memorized passwords.</td>
</tr>
<tr>
<td><strong>FTP (file transfer protocol)</strong></td>
<td>A protocol used on the Internet for transferring files.</td>
</tr>
<tr>
<td><strong>FTP site</strong></td>
<td>An Internet site that hosts directories and files that you can browse and copy to your system using the file transfer protocol (FTP).</td>
</tr>
<tr>
<td><strong>gatekeeper</strong></td>
<td>A system that typically provides services such as authentication, authorization, alias resolution, billing, and call routing for H.323 traffic, and sits between that traffic’s source and destination endpoints.</td>
</tr>
<tr>
<td><strong>gateway</strong></td>
<td>A network component used to connect two or more networks that may use dissimilar protocols and data transmission media.</td>
</tr>
<tr>
<td><strong>group</strong></td>
<td>Logical groupings of two or more users, identified by a single name. See rule groups, user groups.</td>
</tr>
<tr>
<td><strong>hardware authenticator</strong></td>
<td>Also referred to as tokens. Hardware authenticators are hand-held devices that use an internally held cryptographic variable to generate a dynamic (single-use) passcode.</td>
</tr>
<tr>
<td><strong>heartbeat</strong></td>
<td>A message and acknowledgement between HA cluster members to confirm that they are operational. Also refers to a heartbeat burb, which allows all HA cluster-specific traffic to pass between the HA cluster appliances in its own burb without impacting regular network traffic.</td>
</tr>
<tr>
<td><strong>high availability</strong></td>
<td>A licensed feature that allows a second Sidewinder appliance to be configured either in a load sharing capacity or in “hot backup” mode.</td>
</tr>
<tr>
<td><strong>host</strong></td>
<td>Any computer connected to a network; for example, a workstation, router, Sidewinder appliance, or server.</td>
</tr>
<tr>
<td><strong>HTML (hypertext markup language)</strong></td>
<td>A simple programming language used to create Web documents. Hypertext uses special links that you can click to jump from one related topic to another.</td>
</tr>
<tr>
<td><strong>HTTP (hypertext transfer protocol)</strong></td>
<td>An agreed-upon format (protocol) that requests and transfers HTML documents on the World Wide Web.</td>
</tr>
<tr>
<td><strong>HTTPS (hypertext transfer protocol-secure)</strong></td>
<td>An agreed-upon format (protocol) that requests and transfers HTML documents on the World Wide Web in a secured manner.</td>
</tr>
<tr>
<td><strong>ICANN (Internet Corporation for Assigned Names and Numbers)</strong></td>
<td>A U.S. non-profit organization designated to allocate IP address space, assign protocol parameters, perform domain name system management, and maintain root server systems. Other domain registration companies are available.</td>
</tr>
<tr>
<td><strong>IETF (Internet Engineering Task Force)</strong></td>
<td>The organization that developed the IPSec standard which protects data on unprotected (or untrusted) networks such as the Internet.</td>
</tr>
</tbody>
</table>
IKE (Internet key exchange)  A key management protocol standard which automates the implementations of other protocols (ISAKMP, Oakley, etc.) used in a VPN connection.

interface  A shared boundary through which information can be exchanged. An interface may be a shared portion of computer software accessed by two or more programs, a hardware component linking two devices, or a device or program allowing a user to communicate and use the computer or program.

internal DNS  Manages DNS information only available to internal machines. The internal name server cannot receive queries from external hosts since it cannot communicate directly with the external network. Resolution of external DNS information both for the appliance itself and to handle internal queries for external information are handled by the internal name server. Although it is unable to communicate directly with external hosts, it is able to send queries and receive the responses via the external DNS.

IP address  For IPv4, a 32-bit address that uses standard dotted quad notation assigned to TCP/IP network devices. An IP address is unique to each machine on the Internet. An IP address contains a network and host field. For IPv6, the address is 128 bits and is normally written as eight groups of four hexadecimal digits.

IPS (Intrusion Prevention System)  A system for identifying attacks before they pass through the appliance. The Sidewinder appliance has a signature-based IPS feature that is configurable on packet filter, proxy, and server rules, and has an IPS Attack Response feature that sends alerts based on audit events.

IPSec (Internet Protocol Security)  A set of standards created to provide data integrity and confidentiality at the IP layer of the network stack.

ISAKMP (internet security association and key management protocol)  A protocol framework which sets the parameters for a VPN connection by defining the payload format, how the key exchange protocol will be implemented, and how the security association will be negotiated.

ISP (Internet Service Provider)  A company that provides individuals and other companies access to the Internet and other related services such as Web site building and virtual hosting. An ISP has the equipment and the telecommunication line access required to have a point-of-presence (POP) on the Internet for the geographic area served.

kernel  Manages all physical resources, including scheduling of processes, virtual memory, file system management, reading and writing files to disk or tape, printing, and network communications.

key pair  The reference to a private key and a mathematically-related public key. The private key is safeguarded by the owner, and known only to them. The public key can be distributed to anyone. This allows one key to be used for encryption, and the other key to be used for decryption.

key pair generation  The process of generating mathematically-related public/private key pairs.
| **LDAP (Lightweight Directory Access Protocol)** | An internet standard for directory services that run over TCP/IP. |
| **login ID** | When used in conjunction with a password, a means of authentication to start a session with a computer system. |
| **MAC (media access control)** | A unique address assigned to network interface card hardware as a means of identification. |
| **mail server** | A network computer that serves as an intermediate station for electronic mail transfers. |
| **man page** | Short for manual page, refers to the online help that is available within the UNIX operating system. For example, entering `man ls` at the UNIX prompt displays a description of the UNIX `ls` command. |
| **MAT (multiple address translation)** | The ability for a single Sidewinder interface to support multiple external IP addresses so that inbound connections can be directed based on IP addresses and service. MAT allows proxies to be directed to different destinations for the same service by the IP address to which it was connected. |
| **MIB (management information base)** | Within SNMP architecture, a database that stores information about managed objects. These objects are used in the management of networks. |
| **MIME (Multi-purpose Internet Mail Exchange)** | Allows a mail client or Web browser to send and receive non-textual information, such as graphics, audio, video, and spreadsheets. |
| **MX (mail exchanger) records** | Entries in DNS that define where e-mail addresses within domain names get delivered. |
| **name resolution** | The process in which name servers supply address and hostname information to hosts. |
| **name server** | A network computer that maintains a relationship between IP addresses and corresponding domain names. |
| **NAT (network address translation)** | Rewriting the source address of a packet to a new IP address specified by the administrator. The term NAT is often applied when the appliance rewrites the source address. See redirection for when the appliance rewrites the destination address. |
| **NAT Traversal (NAT-T)** | A solution that allows multiple VPN users behind a NAT device to access a VPN tunnel. |
| **nested rule group** | A nested rule group is a rule group that you place within another rule group. |
| **network-layer proxy** | Network-layer proxies check data at the transport and session (TCP/IP) layers to verify that the data packet complies with expected standards. |
| **NIC (network interface controller)** | Hardware, like a computer circuit board, that contains a port or a jack that enables a computer to connect to network wiring, such as an ethernet cable, a phone line, etc. |
node  (1) Any network device such as a workstation or server. (2) The connection point for devices in a network.

non-anonymous FTP  An FTP site that can only be accessed by individuals who enter a valid user name and password.

NSS (network service sentry)  Manages servers and proxy services on the Sidewinder appliance.

NTP (network time protocol)  A protocol that provides a way to synchronize all clocks on a network, or to synchronize the clocks on one network with those on another network.

object  Generally an item that you can individually select and manipulate, including shapes and pictures that appear on a display screen, as well as less tangible software entities.

off-line  State of a computer when it is not connected to another device.

on-line  State of a computer when it is connected to another device.

OS (Operating System)  The master control program that keeps everything flowing inside your computer.

OSPF (Open Shortest Path First)  A routing protocol that dynamically updates changes to routing table information. This protocol is an enhancement over previous protocols that required entire tables to be updated instead of changed data only.

packet filter  Provides the ability to specify rules for IP-based traffic to flow through the appliance at the network layer or the transport layer of the network stack. For example, traffic may pass through the application without being passed to the application proxies. Packet filtering can be used for tracking TCP session states.

Passport  An authentication process (also known as single sign-on) that works in conjunction with a specified authentication method to allow access to multiple services with a single successful authentication to the appliance.

password  The most common form of authentication security. Some networks require multiple levels of passwords to gain access to various servers or databases. Passwords become weak links when they are shared among colleagues, stolen, written down or created in such a way that they can be easily guessed.

PIN (Personal Identification Number)  A number known only by an individual for the purpose of helping identify a person during a computer-based authentication process. PINs should be memorized by the individual.

ping  A command that sends an ICMP message from a host to another host over a network to test connectivity and packet loss.
<table>
<thead>
<tr>
<th><strong>Glossary</strong></th>
<th><strong>Definition</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PKI (Public Key Infrastructure)</strong></td>
<td>System for distributing public cryptographic keys within a community of interested users. The predominant model (based on X.509) makes use of digital certificates generated by certificate authorities. A PKI enables secure remote communication in a number of network application areas.</td>
</tr>
<tr>
<td><strong>port</strong></td>
<td>The number that identifies the destination application process for transmitted data. Port numbers range from 1 to 65535. For example, Telnet typically uses port 23, DNS uses 53, etc.</td>
</tr>
<tr>
<td><strong>primary name server</strong></td>
<td>The DNS server for a domain where the name information is stored and maintained.</td>
</tr>
<tr>
<td><strong>private key</strong></td>
<td>The private key is used to decrypt messages that were encrypted with the corresponding public key. A private key can also be used to digitally sign messages. The recipient can use the corresponding public key to verify the authenticity of the message.</td>
</tr>
<tr>
<td><strong>protocol</strong></td>
<td>A set of rules by which one entity communicates with another, especially over a network. This is important when defining rules by which clients and servers talk to each other over a network. Important protocols become published, standardized, and widespread.</td>
</tr>
<tr>
<td><strong>proxy</strong></td>
<td>A software agent that acts on behalf of a user requesting a network connection through the Sidewinder appliance. The proxy agent accepts a connection from a user, make a decision as to whether or not the user or client IP address is permitted to use the proxy, optionally does additional authentication, and then completes a connection on behalf of the user to a remote destination.</td>
</tr>
<tr>
<td><strong>public key</strong></td>
<td>A public key is used to encrypt messages that only the holder of the corresponding private key can decrypt. Public keys can also be used to verify the authenticity of digitally-signed documents.</td>
</tr>
<tr>
<td><strong>public key cryptography</strong></td>
<td>A class of cryptographic methods that employ a pair of keys for encrypting and decrypting messages. A message encrypted with the public key can only be decrypted with the corresponding private key. Within a public key cryptography system, the public key may be made public without compromising the encrypted data. Public key cryptography enables encryption and digital signatures, and simplifies cryptographic key distribution through the use of a public key infrastructure.</td>
</tr>
<tr>
<td><strong>Quick Start Wizard</strong></td>
<td>A Windows-based program that allows you to initially configuration your Sidewinder appliance.</td>
</tr>
<tr>
<td><strong>RAID (redundant array of individual disks)</strong></td>
<td>Stores information on multiple hard disks to provide redundancy. Using RAID can improve performance and fault-tolerance.</td>
</tr>
</tbody>
</table>
redirection Network address translation where that the Sidewinder appliance rewrite the destination address. The originating host sends the traffic to one destination, such as the appliance’s external interface, and then the appliance redirects the connection to another address based on specifications in the corresponding rule.

reference implementation An IETF term. It is the particular implementation of the protocol or standard that is referred to and used in the associated RFC.

registration The process of authenticating one Sidewinder to an HA cluster or One-To-Many cluster. This process establishes an encrypted, trusted connection between the two systems.

remote management The ability to administer a system from a remote location.


RIP (Routing Information Protocol) A protocol that updates routing tables.

role A login mode used for administrating the Sidewinder. The Sidewinder separates administrator access into two roles: admin (write privileges) or adminro (read-only privileges).

rollback A software management option that restores an appliance to a previous state.

root In UNIX, a user name that gives special privileges to a person who logs onto the system using that name and the correct password. The root user name allows the user to have access to all of the systems files. **The Sidewinder appliance does not allow root privileges.**

root servers The highest level DNS servers.

router A network device that forwards data between two or more networks, delivering them to their final destination or to another router.

rule A rule is a mini policy which contains criteria that is used to inspect incoming or outgoing traffic. Rules determine whether that traffic will be allowed to continue to its destination. There are three distinct rules types that you can configure on the Sidewinder appliance: packet filter rules, proxy rules, and server rules.

rule group An organized set of rules. A rule group can consist of both rules and nested rule groups.

safe mode Also known as failure mode, a Sidewinder operating state that allows system administration while not allowing network traffic to pass through. A Sidewinder can enter this mode under conditions that include: (a) after a failed license check, (b) after a reboot during which the system failed to start a critical service, or (c) after the audit partition has overflowed.
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>secondary name server</td>
<td>DNS servers that download and record a backup copy of domain information from a primary DNS server.</td>
</tr>
<tr>
<td>SecureOS™</td>
<td>The UNIX-based operating system used in a Sidewinder system. SecureOS is built upon BSD/OS and includes Type Enforcement security mechanisms.</td>
</tr>
<tr>
<td>SEF (Sidewinder Export Format)</td>
<td>A Secure Computing proprietary format that can be used when exporting Sidewinder audit data.</td>
</tr>
<tr>
<td>service</td>
<td>Associates a traffic’s transport layer with a specific agent that is responsible for managing the service’s traffic. It consists of an agent, transport-layer properties, and, depending on the agent, agent-specific properties.</td>
</tr>
<tr>
<td>server</td>
<td>A computer system that provides services (such as FTP) to a network, or a program running on a host that offers a service to other hosts on a network.</td>
</tr>
<tr>
<td>session</td>
<td>The time period during which a terminal user logs on the system until they log off the system.</td>
</tr>
<tr>
<td>SIP (Session Initiation Protocol)</td>
<td>An application-layer protocol for that manages some Internet telephone calls, multimedia distribution, and multimedia conferences with one or more participants.</td>
</tr>
<tr>
<td>SMTP (simple mail transport protocol)</td>
<td>The TCP/IP protocol that transfers e-mail as it moves through the system.</td>
</tr>
<tr>
<td>SNMP (simple network management protocol)</td>
<td>The industry standard protocol used for network management.</td>
</tr>
<tr>
<td>SNMP agent</td>
<td>A server that communicates with SNMP management stations to provide information and status for a network node.</td>
</tr>
<tr>
<td>SOA (Start of Authority)</td>
<td>A record found in every DNS zone that contains information about which DNS server is the primary name server, in addition to other administrative information about the zone.</td>
</tr>
<tr>
<td>srole</td>
<td>A Sidewinder UNIX command used to change to a different domain (User, Admn, or AdmRO).</td>
</tr>
<tr>
<td>SSO (single sign-on)</td>
<td>See Passport.</td>
</tr>
<tr>
<td>standalone</td>
<td>Refers to a device or software program that is self-contained; one that does not require any other device or software program to function. Also indicate a Sidewinder appliance that is not part of a cluster configuration or centrally managed.</td>
</tr>
<tr>
<td>standard password authentication</td>
<td>A UNIX mechanism that requires someone logging into a network server to enter a password in order to prove they have a valid login account.</td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>stateful inspection</td>
<td>Method of checking a data packet’s source and destination. The information is recorded in a dynamic state table. New packets from the same session are checking against the table to ensure that they are valid. Invalid packets are dropped.</td>
</tr>
<tr>
<td>Strikeback®</td>
<td>A Sidewinder feature that can be configured to gather information about detected network access violations, or ignore packets from a particular host for a specified period of time.</td>
</tr>
<tr>
<td>strong authentication</td>
<td>A login process that requires a user to enter a unique, one-time response to a login challenge or special code presented by an authentication server. The authentication server resides somewhere in the internal network and sends a log in challenge to a user when he or she attempts to log in. The user must make the proper response to the challenge using a special hardware or software token.</td>
</tr>
<tr>
<td>subnet</td>
<td>A network addressing scheme that separates a single network into a number of smaller physical networks to simplify routing.</td>
</tr>
<tr>
<td>syntax</td>
<td>Refers to the spelling and grammar of a programming language. Computers are inflexible machines that only understand what you type if you type it in the exact form (syntax) that the computer expects.</td>
</tr>
<tr>
<td>TCP/IP (transmission control protocol/internet protocol)</td>
<td>A networking protocol suite created for use in the Internet.</td>
</tr>
<tr>
<td>Telnet</td>
<td>A TCP/IP protocol that directs the exchange of character-oriented data during a client-to-server session.</td>
</tr>
<tr>
<td>traceroute</td>
<td>A UNIX command that shows all of the routing steps between a host and another host.</td>
</tr>
<tr>
<td>trap</td>
<td>An SNMP alert message sent as an unsolicited transmission of information from a managed node (router, Sidewinder appliance, etc.) to an SNMP management station.</td>
</tr>
<tr>
<td>TrustedSource™</td>
<td>A reputation service that filters incoming mail connections and then provides precise information about an e-mail sender's reputation based on its IP address. The purpose of this service is to reduce spam.</td>
</tr>
<tr>
<td>Type Enforcement®</td>
<td>Secure Computing’s patented security technology that protects against intruders by preventing someone from taking over the UNIX operating system within the Sidewinder appliance and accessing critical files or doing other damage.</td>
</tr>
<tr>
<td>UDP (user datagram protocol)</td>
<td>A connectionless protocol that transfers data across a network with no reliability checking or error checking.</td>
</tr>
<tr>
<td>UNIX</td>
<td>A powerful operating system used in high-end workstations and computer systems on the Internet. It allows a single computer to operate multiple programs and be accessed by other computers, all at the same time.</td>
</tr>
</tbody>
</table>
URL (universal resource locator)  Provides the address of specific documents on the Web. Every Internet file has a unique URL; they indicate the name of the server, the directory, and the specific document. The form of a URL is protocol://pathname. For example, ftp://www.website.com; http://www.website.com. Also known as URI (universal resource identifier).

URL filtering  See Web filtering.

user (end user)  A collection of specific data elements that identify the user to the system, define the resources to which they have access, the administrative group to which they belong, and their role within a network structure.

user domain  The domain that allows access to all nonsensitive files.

user groups  A logical grouping of two or more users, identified by a single name.

VLAN interface  An interface that allows administrators to segment a LAN into different broadcast domains regardless of the physical location. To use VLAN interfaces on the Sidewinder appliance, the neighboring network switches and routers must be able to decipher VLAN traffic.

virtual CD  An area where installed patches are copied in order to be easily accessible in case the appliance requires a re-install and still has a functioning hard drive.

VPN (virtual private network)  A method of authenticating and encrypting data transmissions between the machines (Sidewinder-to-Sidewinder, Sidewinder-to-client) via the Internet. VPN makes it appear as though the networks on the internal side of the Sidewinders are connected to each other via a pair of routers with a leased line between them.

VoIP (Voice over IP)  A technology that allows voice information to be transmitted over networks. Some common protocols used to deliver VoIP services include H.323, T.120, and SIP.

VPN tunnel  A secure route via the Internet between two machines (Sidewinder-to-Sidewinder, Sidewinder-to-client, etc.) that use authentication and encryption to transfer data.

weak authentication  A login process that merely requires a user to enter the same password each time he or she logs in. The “standard” UNIX password process is considered a weak authentication method. If someone “sniffs” the password off the phone line or network as it is transmitted, they can conceivably use that password to break into the system. Because your internal network is thought to be “trusted,” this type of authentication is generally used for authenticating internal-to-external proxy connections.

Web filtering  Managing access to Web content, such as blocking certain pages or domains based on a combination of how the Web content’s URL is categorized in a database and the site’s Web access policy. The Sidewinder appliance is interoperable with the SmartFilter Web filtering application.
| **Web farm** | A group of computers that host multiple Web servers for one Web site or a group of Web sites belonging to the same company. Load balancing is often used to distribute traffic among the servers to handle shifts in demand. |
| **XAUTH** | An abbreviation of Extended Authentication. |
A

A record (address record) 522, 525
acat 395
acat_acls 820
accept certificate 32
Access Table mail file 487
account
  administrator 44
  changing password 48
activation process 705
Active Directory 296
active policy 94
add-on modules
  anti-spam 20, 185, 261
  anti-virus 19, 251
  IPS 20, 234
  SmartFilter 17, 267
  SSL 21
  SSL decryption 167
  TrustedSource 18, 257
address pools 603
Admin Console
  about 24
  adding an appliance 31
  administration options 25
  exiting 27
  File Editor 48
  logging in 32
  restoring access to 786
  server 143, 154
  setting system date and time 684
  starting 26
  tips when using 29
  valid port values 425
admin role
  file access 6
  tasks 44
administration
  remote via SSH 54
  remote via telnet 62
administration options 11
administration tool 24
administrator
  account 44
  cautions when editing UNIX files 814
  administrator accounts
    commands 782, 795
    monitoring activity 808
adminro role 44
Admn domain 6
alarms see IPS Attack Responses and System Event Responses
algorithms with VPN 571
alias
  mail 494
  NAT 85, 97, 106
  redirection 86
  root 495
allow traffic 96
allowed get communities 677
allowed header and regular expression entries, spam filtering 262
allowed host entries, spam filtering 262
allow-query option 512, 517
allow-transfer option 512, 517
allow-update option 517
analysis see SecurityReporter
anomaly detection 443
  see also attacks
anti-relay controls 480
Anti-spam filtering
  see also spam filtering
  overview 20, 479
Anti-virus filtering
  see also virus scanning
  for FTP 204–208
  for Mail 191
  for Web 175
  overview 19, 478
aol proxy 121
Application Defense Defense groups 73
Application Defenses
about 10
Citrix 200
commands 796
FTP 202–208
groups 228
H.323 212
HTTP and HTTPS 163–183
IIOP 209
in rules 99
Mail (sendmail) 184–195
Oracle 215
Packet Filter 225
selecting in rules 109
SIP 223
SMTP proxy 196–199
SNMP 219
SOCKS 217
T.120 210
application notes xviii
ARP
force reset and HA 759
gratuitous 752
Network Defense 353
attack audits
ICMP 351
IP 347
IPsec 355
TCP 345
UDP 349
attack protection tools 10, 240
attack responses 400
attacks by service 446
audit
*.gz files 363
*.raw files 363
about 360–364
acat 395
adjusting 96, 342, 364
attack responses 400
commands 783, 796
configuring 400
cron job 812
dashboard 443–447
events 361
IPS Attack Responses 400
levels in rules 96
One-to-Many and 743
SecurityReporter 392
sending SNMP traps 418, 673
sending to syslog 390
SNMP traps 673
supported formats 393
System Event Responses 400
understanding messages 388
viewing 392, 445
viewing a service’s audit errors 430
viewing syslog messages 391
Audit Management
Audit Options pane 382
Crontab Editor 386
export entry 383
exporting log files 386
exporting on request 387
LogFile Options pane 383
rolling log files 386
rolling on request 387
schedule export 386
schedule rolling 386
signing export files 385
statistics 383
window 382
Audit Options pane 382
audit records 447
Audit Viewing 365
custom filters 378
deleting filters 374
exporting data 370
filter examples 380
filter fields 378
filter syntax 378
filtering 371–381
ordering the event table 369
predefined filters 374
saving audit events 369
saving filters 373
viewing mode 365–368
audit.raw file 361, 534
auditbotd 361
auditd 361, 390
auditdbd 361
authentication
alternate methods 299
clear locks 824
commands 796
LDAP 295, 296, 311
Passport 295, 304
password 295, 309
RADIUS 297, 320–321
SafeWord 297, 322
selecting in rules 100, 111
SNMP message header 672
SSH login 55
Windows Domain 296, 317–319
with VPN 537
authentication failure lockout 338, 824
authentication failure traps 677

B
backup
configuration files 693–696
disaster recovery 696
BGP
configuring 649–653
bibliography xix
bi-directional filter rules 151
binary characters 189
BIND 505
blackhole 409
as IPS Attack Response 407
list of blocked IP addresses 792
with signature-based IPS 235
blackhole list 486
blackholed IPs
managing 438, 440
TrustedSource and 260
with signature-based IPS 244
Boot with ACPI 830, 832
broadcast address 609
burb groups
about 72
commands 784, 796
burbs
cluster 737
commands 784, 796
configuring 452–455
network stack separation 7
viewing services enabled in 428

c
ccmd server 143
certificate accept window 32
Certificate Authority (CA)
checking 590, 593
defined 540
definition 577
public versus private 583
certificate server 577
certificates
commands 797
configuring 589
cron job 812
defined 577
exporting 586
remote 592, 599
cf commands
command syntax 794
displaying the man page listing 794
list 794–806
overview 794
cf export 396
change password server 143, 154, 325
changing admin password 48
chtype command 815
Citrix
Application Defense 200
proxy (ICA) 122
class types 235, 241, 243
client address pools 603
cluster burbs 737
cluster status 740, 786
CNAME record 525, 526
command line interface 24, 25
commands
cf areas 794–806
dig 811
frequently used 782–794
mail queues 490
netstat 810
ping 809
process 807
route 810
showaudit 363, 860
tcpdump 857, 860
top 807
traceroute 809
uptime 807
vmstat 807
community names 672
configuration
auditing 400
DNS 498, 502
files 814
mail host 476
Strikeback 400
configuration backup commands 784, 797
configuration files
backing up 693–696
Index

restoring 699–701
connection type 149
contact information iv
Control List, SmartFilter 268
conventions used in this guide xx
copying rules 95
CPU, time by process 807
creating an alternate policy 89
CRL 585
cron 797, 812
Crontab Editor window 387
Crontab Editor, Audit Management 386
Custom LDAP 296
customizing the Rules window 93

d
daemon 422, 798
dashboard
  about 432–433
  audit 443–447
  device information 434–437
  HA management 766
  monitor 432
  network traffic 438–442
  summary of statistics 443–447
date (setting) 684
decryption 538
default route 624–626
Deny All rule 87, 88
deny traffic 96
destination burb 98
dig command 811
disaster recovery
  creating a backup 696, 834
  creating an alternate policy 89
  re-installing 827
disk use information 437, 808
Distinguished Names 580–582
DNS
  A record (address record) 522, 525, 526
  active rules and 822
  advanced server options 511
  advanced zone options 517
  BIND 505
  CNAME record 525, 526
  commands 785, 798
  configuration 498, 502, 506, 507
  configuration utility 528
  disabling servers 503
  editing configuration files 498
  enabling servers 503
  file types 533
  forward zones 514
  forwards 509
  HINFO 525, 526
  hosts 523
  if turned off 503
  logging 534
  mail exchanger records 522
  master zone 515
  master zone attributes 518
  master zone contents 523
  MX record 504, 525, 526
  name servers table 522
  One-to-Many and 742, 743
  proxy 121
  query 504
  reconfigure 528
  reverse zones 514
  rules 88
  serial number 519
  servers for VPNs 607
  Sidewinder Hosted 500
  Sidewinder hosted 507
  slave zone 515
  SOA record 518
  split DNS mode 501, 503
  sub-domain 522
  transparent 499, 506
  TTL value 520
  zone 513
documentation xvii
domain definition table 6
domain object 275
domains
  access 5
  Admn 6
  creator 815
  defined 4
  file access 6
  mail 476
drop traffic 96
duplicating rules 95
dynamic IP addressing
  see also DHCP
  Adding a new VPN 560
  interface configuration 458
Index

E

 editing UNIX files 814
 editors
 Admin Console File Editor 48
 emacs 814
 vi 814
 emacs editor
 commands 814
 using 814
 Emergency Maintenance Mode 40, 830, 832
 encrypted files, scanning for viruses 256
 encryption, with VPN 537
 endpoint
 destination 99
 in rules 106–108
 source 97
 entrelayd 143, 154, 798
 Escape to Loader prompt 830, 832
 etc/sidewinder/daemond.conf 422
 etc/syslog.conf file 389
 evalutaing SmartFilter 268
 evalutaing TrustedSource 257
 event analysis 432
 see also SecurityReporter
 executables, installing 6
 expected connections 117, 152
 export
 audit data 370
 commands 799
 cron job 812
 with a signature 397
 export entry, Audit Management 383
 Export File window 384, 387
 exporting log files 386
 signature 385
 Extended Authentication 542

F

 failed connection request 818
 failover see High Availability
 failure mode see safe mode
 fast path sessions 119, 149
 Federal Information Processing Standard 731
 File Editor 48–53
 file editors 792
 file permissions 815
 file size range, virus scanning 255
 file system commands 786
 file type
 checking 815
 DNS files 533
 files
 configuration 814
 rotating 812
 filter rules, direction 151
 filter syntax 378
 filtering
 mail 184
 Web 175
 filters
 about 134
 access control 9
 commands 789
 general properties 150
 global properties 114
 reloading 789
 reserved port range 153
 session maximums 153
 with stateful packet inspection 135–136
 without stateful packet inspection 138
 finger proxy 121
 FIPS 731, 799
 firewall certificate 589
 firewall license 705
 fixed IP 609
 forward zones 514
 fraud 265
 FTP
 command filtering 203
 proxy 121
 server response configuration 133
 virus/spyware filtering 204
 fwregisterd server 143, 154, 799
 fwregisterp proxy 121

G

 gated
 server 143, 154, 800
 gatekeeper 128–131
 gdc dump 789
 general system information 432
 getting started 14
 global properties 114, 151
gopher proxy 121
### H

<table>
<thead>
<tr>
<th>Page</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>H.323</td>
<td>Application Defense 212</td>
</tr>
<tr>
<td>H.323</td>
<td>gatekeeper 128–131</td>
</tr>
<tr>
<td>H.323</td>
<td>NetMeeting 131</td>
</tr>
<tr>
<td>H.323</td>
<td>overview 127</td>
</tr>
<tr>
<td>H.323</td>
<td>proxy 121</td>
</tr>
</tbody>
</table>

### halt system
- Page 40

### halting services
- Page 426–430

### hardware, warranty
- Page 2

### header stripping
- Page 484

### heartbeat burb
- Page 748, 750, 754

### help (online)
- Page xix

### High Availability
- basic steps 16
- commands 786, 797, 799
- configuration options 750
- configuring 753
- heartbeat burb 748, 750, 754
- load sharing 750
- peer-to-peer 751
- primary-standby 751
- SNMP considerations 675
- statefule session failover 142
- tcpdump and 786
- troubleshooting 851–856

### HINFO
- Page 525, 526

### Host Enrollment List
- Page 713

### host name
- Page 800

### host object
- Page 276

### Host Resources MIB
- Page 675

### hosted DNS
- on firewall 507
- single 500
- split server 500

### HTTP and HTTPS Application Defenses
- Page 163–183

### HTTP proxy
- Page 121

### HTTPS proxy
- Page 122

---

### identity theft
- Page 265

### IDS
- Page 235, 243, 248

### IETF
- Page 537

### IIOP Application Defense
- Page 209

### IIOP proxy
- Page 122

### IKE
- Page 538

### IKEv1
- Page 538, 569

### IKEv2
- Page 538, 569

### imap proxy
- Page 122

### importing SecureClient certificates
- Page 600

### in-addr-arpa
- Page 514

### inbound rules
- Page 70

### inetd
- Page 422, 425

### inoffensive, TrustedSource
- Page 260

### Installation-Disk Imaging CD
- Page 830

### installing executables
- Page 6

### interface status
- commands 787
- viewing in the dashboard 439

### interfaces report
- Page 810

### interfaces, configuring
- Page 456–461

### Internet Key Exchange
- Page 538

### Internet server
- Page 503

### intra-burb forwarding
- Page 153

### IP address object
- Page 278, 279

### IP Network Defense
- Page 347

### IP sniffing
- Page 2

### IP spoofing
- Page 2

### iPlanet
- Page 295

### IPS
- about 11
- about signature-based inspection 234–237
- and IPS Attack Responses 240
- basic steps 20
- commands 797, 801
- cron job 813
- response mappings 241–244
- selecting in rules 100, 110, 237
- signature file updates 239, 249
- signature groups 245–248

### IPS Attack Responses
- about 11, 400
- and signature-based IPS 240
- attack descriptions 404–406
- ignoring network probe attempts 417
- managing 401–408
- response settings 409
- TrustedSource and 260

### IPsec

---
commands 793, 802, 804
defined 537
Network Defense 355
troubleshooting 860

irc proxy 122
Ironmail proxies 122
ISAKMP
commands 800
server 143
ISAKMP server 154, 574, 574–576

K
keys (VPN)
defined 538
ever encryption and decryption 538
generating 538
keyword search 479
Knowledge Base xviii

L
LDAP
authentication 311
Certificate Authorities 577
proxy 123
license
commands 787
cron job 812
Host Enrollment List 713
how to 705
troubleshooting 850
listens 809
load balancers and OTM 734
load sharing HA 750
locked out 823–824
locked out of appliance 786
log check 812
log in, Admin Console 32
logcheck 360
Logfile Options pane 383
Logfile Options, toolbar 383
logging 389
logging DNS 534
Login Console 143, 154
loglevel 783, 819
loopback address 514
lotus proxy 123
ls -yalZ command 815

M
M4 Config File 493
M4 config file 484–488, 491
m4 macros 480
mail
advanced configuration 484–488
aliases 494
collection basics 480–483
domains 476
internal server 476
local delivery 477
local program 477
local server 476
mailertables 482
One-to-Many and 743
postmaster 476
reconfiguring 474
redirecting 494
rules for transparent 475
servers 476
SMTP 473
SMTP hosted 472
transparent SMTP 472
Type Enforcement restrictions 477
viewing mail on the appliance 495
mail exchanger records 504, 518, 521, 522
mail filtering
anti-spam filtering 185
keyword search filter 185
MIME/Anti-Virus filter 185
size filter 185, 186
mail host 476
mail host configuration 476
mail queues
about 478
commands 790
managing 491–493
viewing 490
mailertable files 482
maintenance 812
man pages, about 787, 794
management information base (MIB) 672–675
manuals xvii
masquerade_domain 488
master zone
about 515
attributes 518
contents (DNS) 523
messages
  audit 388
  DNS 534
  in mail queues 490
  log 389
  postmaster 476
mib2 673
MIME filtering
  for mail 191
  for Web 175
monitor 432
monitoring
  attacks 443, 445
  network traffic 438, 442
  system events 443
  system resources 434–439
  system status 432
  using SecurityReporter 392
  VPN status 441, 558
msn proxy 123
mssql proxy 123
mta domains 476
mtac domain 476
Multicast Group Address 768
Multiple Address Translation (MAT) 461
multiple instantiations of a proxy 117, 152
MX record 504, 525, 526

N
name servers table 522
name servers, configuring 502
NAT
  about 85
  in filter rules 139
  selecting in rules 97
NAT Traversal (NAT-T) 572
NetBIOS proxy 123
netmap
  defining 280
  member 280
netmask 458
netstat
  listens 809
  live statistics 787
  load-sharing 856
  ports and 791
  routing and 789
  sendmail and 790
  VPN and 793
network address translation (NAT) 500
Network Defenses
  about 10, 342–344
  ARP 353
  ICMP 351
  IP 347
  IPsec 355
  TCP 345
  UDP 349
network interfaces 456
network interfaces report 810
network objects
  commands 798, 800
  creating 272
  network probe attempts 417
networks
  interfaces report 810
  process status 807
  routing tables 810
  services 425
  stack separation 7
neutral, TrustedSource 260
NNTP proxy 123
non-transparent
  connection type 149
  rules for non-transparent mail 475
non-transparent proxies 118
notify option 511, 517
NSS 425
NTP
  about 686–690
  commands 788, 803
  proxy 123
  reasons for having stopped 859
  references 690
  restarting 859
  servers and clients 686
  troubleshooting 856
  version number 686

O
OID, editing 221
One-to-Many
  about 734–735
  basic steps 16
  becoming a standalone 745
  before you configure 736
  changing the primary 746
  commands 786, 797
Index

883

defining additional secondary firewalls 738
deleting a member 744
making a primary 738
making a secondary 739–741
promoting a secondary 746
synchronized areas 742
online help xix
OpenLDAP 296
Oracle
  Application Defense 215
  proxy 123
ordering your rules 71
OSPF
  configuring 643–648
  overview 640–642
  processing 642–648
outbound rules 71

P

packages
  commands 788
  cron job 812
downloading 722
installing 717, 722
loading 717
scheduling installs and uninstalls 723
types 716
uninstall 717, 722
viewing available 720
viewing current version 434
Packet Filter Application Defense 225
packet filters
  see also filters
  about 134
Passport 88, 295, 304–310
Passport authenticator
  server 144, 155
password
  authentication 295
  changing 48, 324, 325
  how users change their own 326
  if you forget 824
password authentication 309
patches
  see also packages
  commands 803
performance report 807
phishing 265
PIM-SM
  configuring 655
  overview 654
  ping 123, 809
PKCS7 signature 397
policy
  commands 788
  planning guidelines 71
policy planning guidelines 87
POP proxy 123
port redirection 99, 108
ports
  address translation and 98, 106, 108, 139–140
  restricting source 150
  selecting in filter services 150
  selecting in proxy services 149
  valid values 425
  viewing configurations for services 428
postmaster 476
powering down 40
preserve source port 98, 106, 140
pre-shared password, defined 540
primary name server 501
primary-standby HA 751
printer proxy 123
process
  CPU time 807
  displaying information 807
  domain 807
  domain access 5
  file access 6
  report 807
  status 807
process command 807
process use information 436
protocol anomaly detection, see anomaly detection
proxies
  about 116–119
  commands 788
  expected connections 152
  general properties 149
  initial set-up 120
  list of defaults 121–125
  multiple instantiation 117, 152
  non-transparent 118
  overview 9
  transparent 118
proxy agents
expected connections 117
  global properties 114
proxy connection information 441
ps command 807
PXE boot and the appliance 838–849

Q

Quality of Service
  enabling 459
  overview 462
  profiles 464
  queues 465
  scenarios 469
queue interval 493
quick deployment tips 14
Quick Start Wizard
  configurations set during 35
  Management Tools CD 24

R

RADIUS authentication 297, 320–321
read-only administrators 29, 44
real time audit 366
RealMedia 124
RealTime Blackhole List 486
rebooting 40
reconfigure
  DNS 528
  mail 474
recovery options 825–829
redirection
  about 86
  in filter rules 139
  in rules 99
reference material
  online help xix
  RFCs xix
re-installing
  from the product CD 832–833
  from the VCD 830–831
  options 826
  using a USB flash drive 834–837
  using PXE boot 838–849
remote administration
  via SSH 54
  via telnet 62
remote certificate 592
Remote Identities, defined and configuring
  587
reporting
  exporting data 389, 393–396
  SecurityReporter 392
reports
  3rd party tools 393
  commands 804
  mail queues 490
  network interfaces 810
  routing tables 810
reputation classes, TrustedSource 259
reserved port range 153
response mappings 241–244
responses see IPS Attack Responses and System Event Responses 400
restarting services 426–430
restoring configuration files 699–701
restoring console access 786, 823
reverse zones 514
RFCs xix
RIP
  see also routed
  see also routed
  configuring 629–639
  overview 627–628
  processing 629–637
  trace and log information 667
rlogin proxy 124
roles
  about 44
  admin 6
rollaudit 813
rollaudit.conf file 813
rollback 717, 727
rolling log files 386
root 4, 6
rotating files 389, 812
route commands 789, 805, 810
routed
  see also RIP
  see also RIP
  commands 804
  configuring 629–639
  flushing filter routes 668
  RIP processing 627, 629–639
  server 144, 154
routes
  default 624–626
  static 624–626
routing tables report 810
RSH proxy 124
RTSP proxy 124
rule groups
  about 73–74
  managing 90, 102
rules
  about the Rules window 89–94
  default policy 88
  displaying 93
  example of 77
  failed connection request 818
  IPS and 237
  managing 95–101
  monitoring tool 820
NAT 85
  order 75–77
  overview 82–84
  redirection 86
  troubleshooting 817
  types of 70
  viewing the active policy 94

S
sacap filters 373, 378, 390
safe mode 424
SafeWord authentication 297, 322
scan buffer size, virus scanning 256
scanners, virus scanning 255
scanning encrypted files 256
SCC MIB files 675
sccMibSw 673
SCEP 585, 590, 593, 594
schedule, exporting log files 386
schedule, rolling log files 386
scripts
  creating your own 816
  cron 812
SCSR see SecurityReporter
secondary name server 501
Secure Manager Server 143
secure shell (SSH) 54
SecureClient certificates, importing 600
SecureOS 2, 7
Security Parameters Index (SPI), using
  manual key exchange 571
SecurityReporter 392
SEF
  and SecurityReporter 392
  and syslog 390
  converting using the Admin Console 370
  exporting in 393–396
sendmail
  see also SMTP
advanced configuration 484–488
allow/deny mail on a user basis 487
commands 790, 804
configuration basics 480–483
header stripping 484
m4 macros 480
masquerade_domain 488
One-to-Many and 743
RealTime Blackhole list 486
server 144, 154
version 480
serial number (DNS) 519
server agents, global properties 114
server response configuration, FTP 133
server rules 71
server.conf file 667, 814
servers
  about 142
  access control 10
  commands 788, 805
  DNS 503
  list of 143
  managing 154
  sendmail 476
telnet 62
service groups
  about 72
  commands 805
  managing 156–157
service status 426–430
services
  see also proxies, filters, and servers
  commands 795
  filter general properties 150
  managing 145–153
  overview 114–115
  proxy general properties 149
  selecting in rules 96, 103
session maximums 153
sfadmin server 144, 267
sfadminserver 155
sfredirect server 144, 267
sftp 54
showaudit command 363, 860
shutdown 40, 42, 790
Sidewinder 7 PXE imaging server 838–849
Sidewinder appliance, about 2
Sidewinder Export Format see SEF
Sidewinder Hosted DNS 500
sighup command 424
signature categories 235, 245
signature groups 245–248
signature-based IPS see IPS
signing export files 385
SIP
  Application Defense 223
    proxy 124, 132
size filter 186
slave zone 515
SmartFilter
  about 267
  basic steps 17
  configuring 269–270
  Control List 268
  evaluating 268
  servers 144, 155
SMTP
  mail queues 490–493
  proxy 124
  secure split servers 472
  transparent mail 472
snapshot audit 366
SNMP
  agent 144, 155, 670
  allowed get communities 677
  Application Defense 219
  authentication header 672
  commands 805
  community names 672
  configuration agents 676–679
  configuring rules 679
  High Availability and 675
  management information base (MIB) 672–675
  options on Sidewinder 670
  passing to and through the appliance 680
  proxy 124, 670
  response trap 673
  trap destinations 678
  traps 407, 415, 418
snmptrap 671–673
SOA record 518
SOCKS Application Defense 217
SOCKS proxy 124
SoftRemote 541, 596
software management
  commands 788, 803
  rollback 826
  uninstall 826
source burb 97, 106
spam filtering
  see also TrustedSource
  about 261, 479
  basic steps 20
  commands 790, 806
  cron job 813
  licensing 261
  spamcatcher.conf 265–266
  whitelist configuration 262–264
spam, TrustedSource 260
spamcatcher.cfg for spam filtering 265
SPI (Security Parameters Index), using manual key exchange 571
split DNS 501, 503
SSH
  client 59
  configuring 54
  proxy 124
  server 144, 155
SSL acceleration 21
SSL decryption 164
ssod server 144, 155
stacks 7
State Change Wizard
  HA cluster 755, 762
  One-to-Many 738–741
  starting 738, 745
stateful inspection 9
stateful packet inspection 150
stateful session failover 150
static route 624–626
statistics, Audit Management 383
status process 807
status reports, routing tables 810
streamworks proxy 124
Strikeback 400
Strong Cryptography 167
sub-domain (DNS) 522
subnet object 282
sunrcp proxy 124
super-user 4, 6
support for multiple networks 3
supported audit formats 393
suspicious, TrustedSource 260
syslog
about 389
audit messages 390
configuration file 389
syslogd 389
system calls 5
System Event Responses
about 400
managing 411–415
response settings 416
system resources 434, 437, 439

T

T.120
Application Defense 210
proxy 125, 126
TCP
checksum offload 456
Network Defense 345
state information 442
tcpdump 791, 857, 860
TE see Type Enforcement
Technical Support 792
Telnet
defined 62
proxy 125
server 62, 144, 154
temporarily disabling services 426–430
text editors 792
time (setting) 684
time periods
commands 805
creating 288
in rules 97
selecting in rules 104
time zones, commands 806
timeouts 149, 150
toolbar, Logfile Options 383
top command 807
traceroute 123, 789, 809
traffic basics 70
transparent
connection type 149
DNS 499, 506
mail (SMTP) 472
proxies 118
rules for transparent mail 475
tunnel mode 541, 561
trap destinations 678
traps 407, 418, 671–673, 677
troubleshooting
no admin access 823
NTP 856
rules 817
TrustedSource
see also spam filtering
about 257–258
basic steps 18
commands 792
 configuring 259–260
reputation classes 259
subscription 257, 259
Web site 260
TTL value (DNS) 520
tunnel mode 541, 561
TXT record 522, 525, 526
Type Enforcement
about 4
defined 4
effects 6
file types 815
how it works 4
restore 6
sendmail 477
types of traffic 70

U

UDP
checksum 150
Network Defense 349
unbound DNS server 503
uni-directional filter rules 151
Unified Threat Management 2
UNIX
editing files 814
security 4
text editors 814
unverified, TrustedSource 260
updates
IPS signature files 239, 249
virus scanning signature files 252–254
UPS
commands 806
configuring 64
uptime command 807
uptime statistics 434, 791
URL filtering see SmartFilter
USB flash drive 827
user database commands 806
Index

user groups
  commands 806
  displaying 330
  selecting in rules 111
users
  changing password 48
  displaying 330
users and user groups 330–339
UTM (Unified Threat Management) 2

V

var/log/audit.raw file 534
var/log/daemon.log file 534
var/spool/mqueue.X 478, 490
vi editor
  commands 814
  using 814
viewing items 29, 44
virtual burb 545
virtual CD 826, 830–831
virus scanning
  about 251, 478
  advanced features 255–256
  basic steps 19
  commands 783, 795
cron job 813
  engine updates 252–254
  file size range 255
  signature file updates 252–254
VLAN
  configuring 460
  interface configuration 457
vmstat command 807
VPN
  AH keys 571
  algorithms 571
  authentication 543
  basic steps 16
  certificate authority 577
certificate server 577
  client 541
  client address pools 603
  commands 793, 860
  definitions 555–573
  Extended Authentication 542
  firewall certificate 589
  fixed IP 609
  IKE keys 571
  ISAKMP server 574
  key types 538
  local authentication 569
  NAT Traversal (NAT-T) 572
  public CA server 583
  remote authentication 564
  remote certificate 592
  Remote Identities 587
  scenarios 611–621
  SPI 571
  status of active 441
  transport mode 541
  troubleshooting 860
  tunnel mode 541
  understanding 536
XAUTH 564

W

wais proxy 125
warranty 2
Web filtering see SmartFilter
Web sites
  activation 707
  application notes xviii
  Knowledge Base xviii
  Secure Computing xviii
  SmartFilter 268
  TrustedSource 260
whitelist configuration for spam filtering 262–264
whois command 125
whois proxy 125
Windows Domain authentication 296, 317–319
Windows XP 845
wins proxy 125
WINS server 607

X

XAUTH 564
Xwindows proxy 125

Z

zones 513
**Web Gateway** – Comprehensive protection against malware, viruses, data leakage and Internet misuse, while ensuring policy enforcement, regulatory compliance, and a productive application environment.

**Messaging Gateway** – Inbound defense against spam, viruses, denial-of-service and intrusions; outbound protection against data leaks and policy violations.

**Network Gateway** – World’s strongest firewall appliance contains the most comprehensive set of security solutions consolidated in one appliance and automatically discards huge volumes of unwanted traffic from known “bad” entities.

**Identity & Access Management** – Providing safe access to applications, data and resources through policy-driven security and strong authentication.