Stonesoft 5.4

Firewall Installation Guide

Firewall
Virtual Private Networks

STONESOFT
Legal Information

End-User License Agreement
The use of the products described in these materials is subject to the then current end-user license agreement, which can be found at the Stonesoft website:

Third Party Licenses
The Stonesoft software includes several open source or third-party software packages. The appropriate software licensing information for those products at the Stonesoft website:
www.stonesoft.com/en/support/third_party_licenses.html

U.S. Government Acquisitions
If Licensee is acquiring the Software, including accompanying documentation on behalf of the U.S. Government, the following provisions apply. If the Software is supplied to the Department of Defense ("DoD"), the Software is subject to "Restricted Rights", as that term is defined in the DoD Supplement to the Federal Acquisition Regulations ("DFAR") in paragraph 252.227-7013(c) (1). If the Software is supplied to any unit or agency of the United States Government other than DoD, the Government’s rights in the Software will be as defined in paragraph 52.227-19(c) (2) of the Federal Acquisition Regulations ("FAR"). Use, duplication, reproduction or disclosure by the Government is subject to such restrictions or successor provisions.

Product Export Restrictions
The products described in this document are subject to export control under the laws of Finland and the European Council Regulation (EC) No.1334/2000 of 22 June 2000 setting up a Community regime for the control of exports of dual-use items and technology (as amended). Thus, the export of this Stonesoft software in any manner is restricted and requires a license by the relevant authorities.

General Terms and Conditions of Support and Maintenance Services
The support and maintenance services for the products described in these materials are provided pursuant to the general terms for support and maintenance services and the related service description, which can be found at the Stonesoft website:
www.stonesoft.com/en/support/view_support_offering/terms/

Replacement Service
The instructions for replacement service can be found at the Stonesoft website:
www.stonesoft.com/en/support/view_support_offering/return_material_authorization/

Hardware Warranty
The appliances described in these materials have a limited hardware warranty. The terms of the hardware warranty can be found at the Stonesoft website:
www.stonesoft.com/en/support/view_support_offering/warranty_service/

Trademarks and Patents
The products described in these materials are protected by one or more of the following European and US patents: European Patent Nos. 1065844, 1189410, 1231538, 1231754, 1259028, 1271283, 1289183, 1292002, 1304830, 1304849, 1313290, 1326393, 1361724, 1379037, and 1379046 and US Patent Nos. 6,650,621; 6,856,621; 6,912,200; 6,996,573; 7,099,284; 7,127,739; 7,130,266; 7,130,305; 7,146,421; 7,162,737; 7,234,166; 7,260,843; 7,280,540; 7,325,248; 7,360,242; 7,386,525; 7,406,534; 7,461,401; 7,573,823; 7,721,084; and 7,739,727 and may be protected by other EU, US, or other patents, or pending applications. Stonesoft, the Stonesoft logo and StoneGate, are all trademarks or registered trademarks of Stonesoft Corporation. All other trademarks or registered trademarks are property of their respective owners.

Disclaimer
Although every precaution has been taken to prepare these materials, THESE MATERIALS ARE PROVIDED "AS-IS" and Stonesoft makes no warranty to the correctness of information and assumes no responsibility for errors, omissions, or resulting damages from the use of the information contained herein. All IP addresses in these materials were chosen at random and are used for illustrative purposes only.

Copyright © 2012 Stonesoft Corporation. All rights reserved. All specifications are subject to change.

Revision: SGFIG_20120830
# Table of Contents

## Introduction

<table>
<thead>
<tr>
<th>Chapter 1</th>
<th>Using Stonesoft Documentation</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>How to Use This Guide</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>Documentation Available</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>Product Documentation</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>Support Documentation</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>System Requirements</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>Supported Features</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>Contact Information</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>Licensing Issues</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>Technical Support</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>Your Comments</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>Other Queries</td>
<td>10</td>
</tr>
</tbody>
</table>

## Preparing for Installation

<table>
<thead>
<tr>
<th>Chapter 2</th>
<th>Planning the Firewall Installation</th>
<th>13</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Introduction to Stonesoft Firewalls</td>
<td>14</td>
</tr>
<tr>
<td></td>
<td>Overview to the Installation Procedure</td>
<td>15</td>
</tr>
<tr>
<td></td>
<td>Important to Know Before Installation</td>
<td>16</td>
</tr>
<tr>
<td></td>
<td>Supported Platforms</td>
<td>16</td>
</tr>
<tr>
<td></td>
<td>Date and Time Settings</td>
<td>16</td>
</tr>
<tr>
<td></td>
<td>Firewall Cluster IP Addresses</td>
<td>16</td>
</tr>
<tr>
<td></td>
<td>Heartbeat Connection and State</td>
<td>17</td>
</tr>
<tr>
<td></td>
<td>Synchronization in the Firewall Cluster</td>
<td>17</td>
</tr>
<tr>
<td></td>
<td>Firewall Cluster Modes</td>
<td>17</td>
</tr>
</tbody>
</table>

## Configuring Firewalls

<table>
<thead>
<tr>
<th>Chapter 3</th>
<th>Installing Firewall Licenses</th>
<th>19</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Overview to Firewall Licenses</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>Configuration Overview</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>Generating New Licenses</td>
<td>21</td>
</tr>
<tr>
<td></td>
<td>Installing Licenses</td>
<td>21</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 4</th>
<th>Configuring NAT Addresses</th>
<th>23</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Getting Started with NAT Addresses</td>
<td>24</td>
</tr>
<tr>
<td></td>
<td>Configuration Overview</td>
<td>25</td>
</tr>
<tr>
<td></td>
<td>Defining Locations</td>
<td>25</td>
</tr>
<tr>
<td></td>
<td>Adding SMC Server Contact Addresses</td>
<td>27</td>
</tr>
</tbody>
</table>

## Configuring Single Firewalls

<table>
<thead>
<tr>
<th>Chapter 5</th>
<th>Configuring Single Firewalls</th>
<th>31</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Configuration Overview</td>
<td>32</td>
</tr>
<tr>
<td></td>
<td>Adding a Single Firewall Element</td>
<td>32</td>
</tr>
<tr>
<td></td>
<td>Selecting Interface Numbers</td>
<td>32</td>
</tr>
<tr>
<td></td>
<td>Creating a Single Firewall Element</td>
<td>33</td>
</tr>
<tr>
<td></td>
<td>Adding Physical Interfaces</td>
<td>35</td>
</tr>
<tr>
<td></td>
<td>Adding VLANS</td>
<td>36</td>
</tr>
<tr>
<td></td>
<td>Adding ADSL Interfaces</td>
<td>38</td>
</tr>
<tr>
<td></td>
<td>Adding Wireless Interfaces</td>
<td>39</td>
</tr>
<tr>
<td></td>
<td>Adding SSID Interfaces</td>
<td>40</td>
</tr>
<tr>
<td></td>
<td>Defining Security Settings for SSID Interfaces</td>
<td>41</td>
</tr>
<tr>
<td></td>
<td>Configuring IP Addresses for Physical, VLAN, ADSL, or SSID Interfaces</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td>Adding Static IPv4 Addresses</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td>Configuring a Virtual Router on a Physical, VLAN, or SSID Interface</td>
<td>44</td>
</tr>
<tr>
<td></td>
<td>Adding Static IPv6 Addresses</td>
<td>45</td>
</tr>
<tr>
<td></td>
<td>Configuring Dynamic IP Addresses</td>
<td>46</td>
</tr>
<tr>
<td></td>
<td>Adding Modem Interfaces</td>
<td>48</td>
</tr>
<tr>
<td></td>
<td>Setting Global Interface Options</td>
<td>49</td>
</tr>
<tr>
<td></td>
<td>Binding Engine Licenses to Correct Elements</td>
<td>51</td>
</tr>
</tbody>
</table>

## Configuring Firewall Clusters

<table>
<thead>
<tr>
<th>Chapter 6</th>
<th>Configuring Firewall Clusters</th>
<th>53</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Configuration Overview</td>
<td>54</td>
</tr>
<tr>
<td></td>
<td>Adding a Firewall Cluster Element</td>
<td>54</td>
</tr>
<tr>
<td></td>
<td>Selecting Interface Numbers</td>
<td>54</td>
</tr>
<tr>
<td></td>
<td>Creating a Firewall Cluster Element</td>
<td>55</td>
</tr>
<tr>
<td></td>
<td>Adding Nodes to a Firewall Cluster</td>
<td>56</td>
</tr>
<tr>
<td></td>
<td>Adding Physical Interfaces</td>
<td>57</td>
</tr>
<tr>
<td></td>
<td>Adding VLANS</td>
<td>58</td>
</tr>
<tr>
<td></td>
<td>Configuring IP Addresses for Cluster Interfaces</td>
<td>59</td>
</tr>
<tr>
<td></td>
<td>Defining IPv4 Addresses</td>
<td>60</td>
</tr>
<tr>
<td></td>
<td>Defining IPv6 Addresses</td>
<td>61</td>
</tr>
<tr>
<td></td>
<td>Defining Contact Addresses for Firewall Clusters</td>
<td>62</td>
</tr>
<tr>
<td></td>
<td>Setting Global Interface Options for Clusters</td>
<td>64</td>
</tr>
<tr>
<td></td>
<td>Adding Manual ARP Entries</td>
<td>67</td>
</tr>
<tr>
<td></td>
<td>Binding Engine Licenses to Correct Elements</td>
<td>68</td>
</tr>
</tbody>
</table>
CHAPTER 7
Saving the Initial Configuration .... 71
  Configuration Overview ......... 72
  Saving the Initial Configuration for Firewall Engines .... 72
  Preparing for Plug-and-Play Configuration ... 74
  Preparing for Automatic Configuration .... 75
  Preparing for Configuration Using the Configuration Wizard .... 76
  Transferring the Initial Configuration to Firewall Engines .... 77

CHAPTER 8
Defining Routing and Basic Policies .... 79
  Defining Routing .......... 80
  Adding a Default Route with a Single Network Link .... 82
  Adding a Default Route With Multi-Link .... 83
  Defining Other Routes .... 88
  Antispoofing .... 90
  Using IP Address Count Limited Licenses .... 90
  Defining Basic Policies .... 91
  Adding a NAT Rule for the Example Ping Rule .... 94
  Installing the Policy .... 95
  Commanding Engines Online .... 96

INSTALLING THE FIREWALL ENGINE

CHAPTER 9
Installing the Engine on Intel-Compatible Platforms .... 99
  Installing the Firewall Engine .... 100
  Configuration Overview .... 100
  Obtaining Installation Files .... 101
  Downloading the Installation Files .... 101
  Checking File Integrity .... 101
  Creating the Installation CD-ROM .... 101
  Starting the Installation .... 102
  Configuring the Engine .... 103
  Configuring the Engine Automatically with a USB Stick .... 103
  Configuring the Engine in the Engine Configuration Wizard .... 103
  Configuring the Operating System Settings .... 105
  Configuring the Network Interfaces .... 106
  Contacting the Management Server .... 107
  After Successful Management Server Contact .... 110
  Installing the Engine in Expert Mode .... 110
  Partitioning the Hard Disk Manually .... 110
  Allocating Partitions .... 111

UPGRADING

CHAPTER 10
Upgrading .... 115
  Getting Started with Upgrading Firewalls .... 116
  Configuration Overview .... 117
  Obtaining Engine Upgrade Files .... 117
  Upgrading or Generating Licenses .... 118
  Upgrading Licenses Under One Proof Code .... 119
  Upgrading Licenses Under Multiple Proof Codes .... 119
  Installing Licenses .... 120
  Checking the Licenses .... 121
  Upgrading Engines Remotely .... 122
  Upgrading Engines Locally .... 124
  Upgrading From an Engine Installation CD-ROM .... 124
  Upgrading From a ZIP Archive File .... 126

APPENDICES

APPENDIX A
Command Line Tools .... 129
  Management Center Commands .... 130
  Engine Commands .... 140
  Server Pool Monitoring Agent Commands .... 147

APPENDIX B
Default Communication Ports .... 149
  Management Center Ports .... 150
  Security Engine Ports .... 153

APPENDIX C
Example Network Scenario .... 157
  Overview of the Example Network .... 158
  Example Firewall Cluster .... 159
  Example Management Center .... 160
  Example Single Firewall .... 160

APPENDIX D
Installation Worksheet for Firewall Clusters .... 163
  Index .... 167
In this section:

Using Stonesoft Documentation - 7
This chapter describes how to use the *Firewall Installation Guide* and lists other available documentation. It also provides directions for obtaining technical support and giving feedback.

The following sections are included:

- How to Use This Guide (page 8)
- Documentation Available (page 9)
- Contact Information (page 10)
How to Use This Guide

The *Firewall Installation Guide* is intended for the administrators of a Stonesoft Firewall/VPN installation. It describes step by step how to install Stonesoft Firewall engine(s). The chapters in this guide are organized in the general order you should follow when installing the system.

Most tasks are explained using illustrations that include explanations on the steps you need to complete in each corresponding view in your own environment. The explanations that accompany the illustrations are numbered when the illustration contains more than one step for you to perform.

Typographical Conventions

The following conventions are used throughout the documentation:

**Table 1.1 Typographical Conventions**

<table>
<thead>
<tr>
<th>Formatting</th>
<th>Informative Uses</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User Interface text</strong></td>
<td>Text you see in the User Interface (buttons, menus, etc.) and any other interaction with the user interface are in <strong>bold-face</strong>.</td>
</tr>
<tr>
<td><strong>References, terms</strong></td>
<td>Cross-references and first use of acronyms and terms are in <strong>italics</strong>.</td>
</tr>
<tr>
<td><strong>Command line</strong></td>
<td>File names, directories, and text displayed on the screen are <strong>monospaced</strong>.</td>
</tr>
<tr>
<td><strong>User input</strong></td>
<td>User input on screen is in <strong>monospaced bold-face</strong>.</td>
</tr>
<tr>
<td><strong>Command parameters</strong></td>
<td>Command parameter names are in <strong>monospaced italics</strong>.</td>
</tr>
</tbody>
</table>

We use the following ways to indicate important or additional information:

- **Note** – Notes prevent commonly-made mistakes by pointing out important points.
- **Caution** – Cautions prevent breaches of security, information loss, or system downtime. Cautions always contain critical information that you must observe.
- **Tip** – Tips provide additional helpful information, such as alternative ways to complete steps.
- **Example** Examples present a concrete scenario that clarifies the points made in the adjacent text.
Stonesoft documentation is divided into two main categories: Product Documentation and Support Documentation. Each Stonesoft product has a separate set of manuals.

**Product Documentation**

The table below lists the available product documentation.

### Table 1.2  Product Documentation

<table>
<thead>
<tr>
<th>Guide</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reference Guide</td>
<td>Explains the operation and features of Stonesoft comprehensively. Demonstrates the general workflow and provides example scenarios for each feature area. Available as separate guides for Stonesoft Management Center and Stonesoft Firewall/VPN, and as a combined guide for Stonesoft IPS and Stonesoft Layer 2 Firewall.</td>
</tr>
<tr>
<td>Installation Guide</td>
<td>Instructions for planning, installing, and upgrading a Stonesoft system. Available as separate guides for Stonesoft Management Center and Stonesoft Firewall/VPN, and as a combined guide for Stonesoft IPS and Stonesoft Layer 2 Firewall.</td>
</tr>
<tr>
<td>Online Help</td>
<td>Describes how to configure and manage the system step-by-step. Accessible through the Help menu and by using the Help button or the F1 key in any window or dialog. Available in the Stonesoft Management Client and the Stonesoft Web Portal. An HTML-based system is available in the Stonesoft SSL VPN Administrator through help links and icons.</td>
</tr>
<tr>
<td>Administrator’s Guide</td>
<td>Describes how to configure and manage the system step-by-step. Available as a combined guide for Stonesoft Firewall/VPN, Stonesoft IPS, and Stonesoft Layer 2 Firewall, and as separate guides for Stonesoft SSL VPN and Stonesoft IPsec VPN Client.</td>
</tr>
<tr>
<td>Appliance Installation Guide</td>
<td>Instructions for physically installing and maintaining Stonesoft appliances (rack mounting, cabling, etc.). Available for all Stonesoft hardware appliances.</td>
</tr>
</tbody>
</table>

PDF guides are available at [http://www.stonesoft.com/support/](http://www.stonesoft.com/support/). The Administrator’s Guide, and the Reference Guides and Installation Guides for Stonesoft Management Center, Stonesoft Firewall/VPN, Stonesoft IPS, and Stonesoft Layer 2 Firewall are also available as PDFs on the Management Center CD-ROM.
Support Documentation

The Stonesoft support documentation provides additional and late-breaking technical information. These technical documents support the Stonesoft Guide books, for example, by giving further examples on specific configuration scenarios.

The latest Stonesoft technical documentation is available on the Stonesoft website at http://www.stonesoft.com/support/.

System Requirements

The certified platforms for running Stonesoft engine software can be found at the product pages at http://www.stonesoft.com/en/products/fw/Software_Solutions/.

The hardware and software requirements for the version you are running can also be found in the Release Notes available on the software download page at the Stonesoft website.

Supported Features

Not all features are supported on all platforms. See the Appliance Software Support Table at the Stonesoft Support Documentation pages for more information.

Contact Information

For street addresses, phone numbers, and general information about Stonesoft products and Stonesoft Corporation, visit our website at http://www.stonesoft.com/.

Licensing Issues

You can view your current licenses at the License Center section of the Stonesoft website at https://my.stonesoft.com/managelicense.do.

For license-related queries, e-mail order@stonesoft.com.

Technical Support

Stonesoft offers global technical support services for Stonesoft’s product families. For more information on technical support, visit the Support section at the Stonesoft website at http://www.stonesoft.com/support/.

Your Comments

We want to make our products fulfill your needs as well as possible. We are always pleased to receive any suggestions you may have for improvements.

- To comment on software and hardware products, e-mail feedback@stonesoft.com.
- To comment on the documentation, e-mail documentation@stonesoft.com.

Other Queries

For queries regarding other matters, e-mail info@stonesoft.com.
CHAPTER 2

PLANNING THE FIREWALL INSTALLATION

This chapter provides important information to take into account before beginning the installation, including an overview to the installation.

The following sections are included:

► Introduction to Stonesoft Firewalls (page 14)
► Example Network Scenario (page 15)
► Overview to the Installation Procedure (page 15)
► Important to Know Before Installation (page 16)
Introduction to Stonesoft Firewalls

A Stonesoft Firewall system consists of the Stonesoft Management Center and one or more Firewalls. A Stonesoft Firewall is either a **Single Firewall** with only one physical device or a **Firewall Cluster** that can include up to 16 physical devices that work as a single virtual entity. The Firewalls are managed centrally through the Stonesoft Management Center (SMC).

The main features of Stonesoft Firewalls include:

- **Advanced traffic inspection**: Multi-Layer packet and connection verification process ensures maximum security without compromising system throughput. An anti-virus scanner, and anti-spam and web filtering complement the standard traffic inspection features when the Firewall is licensed for the UTM (unified threat management) feature.
- **Built-in Load Balancing and High-Availability**: The clustering of the Firewall engines is integrated. The Firewall engines dynamically load-balance individual connections between the cluster nodes.
- **Multi-Link technology**: Multi-Link allows configuring redundant network connections without the more complex traditional solutions that require redundant external routers and switches. It provides high-availability for inbound, outbound, and VPN connections.
- **QoS and bandwidth management**: You can set up the minimum and maximum bandwidth value and the priority value for different types of traffic.
- **Reporting tools**: Stonesoft Management Center provides extensive reporting tools for generating statistical reports based on logs, alerts, and operating statistics.
- **Virtual Private Networks**: The Firewall provides fast, secure, and reliable VPN connections with the added benefits of the clustering and Multi-Link technologies that provide load balancing and failover between ISPs and VPN gateways.
- **Unified Stonesoft Management Center and integration with other Security Engines**: You can configure and monitor the Stonesoft Firewall/VPN and the other Security Engines through the same Management Center and the same graphical user interface.

You must have an SMC configured before you can proceed with installing the firewalls. The SMC can be used to manage a large number of different Stonesoft products. The SMC installation is covered in a separate guide. See the **SMC Reference Guide** for more background information on the SMC, and **Firewall/VPN Reference Guide** for more background information on the Firewall.

It is possible to download and install licenses for Firewall Appliances automatically. For additional information on automatic downloading and installation of Firewall Appliance licenses, refer to the **Administrator’s Guide**.
Example Network Scenario

To get a better understanding of how the Stonesoft Firewall fits into a network, see the Example Network Scenario (page 157), which shows one way to deploy the Stonesoft Firewall.

All illustrations of the software configuration in this Installation Guide are filled in according to this example scenario; this way, you can always compare how the settings in the various dialogs relate to the overall network structure.

Overview to the Installation Procedure

After installing the Management Center, proceed as follows with the Firewall installation.

1. Install licenses for the Firewall engines. See Installing Firewall Licenses (page 19).
2. If network address translation (NAT) is applied to communications between system components and the Firewalls, define Contact Addresses. See Configuring NAT Addresses (page 23).
3. Define the Firewall element(s) in the Management Client. See Configuring Single Firewalls (page 31), and Configuring Firewall Clusters (page 53).
4. Generate the initial configuration for the Firewall engine(s). See Saving the Initial Configuration (page 71).
5. Install and configure the Firewall engines.
   • For hardware installation and initial configuration of Stonesoft appliances, see the Appliance Installation Guide that is delivered with each appliance.
   • For software installations, see Installing the Engine on Intel-Compatible Platforms (page 99).
6. Configure basic routing and install a policy on the Firewall. See Defining Routing and Basic Policies (page 79).
Important to Know Before Installation

Consult the Firewall/VPN Reference Guide if you need more detailed background information on the operation of the Firewall than what is offered in this chapter.

Supported Platforms

Firewall engines can be run on the following general types of platforms:

- Purpose-built Stonesoft Firewall appliances.
- As a VMWare virtual host. There are some additional requirements and limitations when the Firewall is run as a virtual host. See the release notes for more information. Detailed instructions can be found in Installing and Activating Stonesoft Firewall/VPN in VMWare ESX Server in the Stonesoft Technical Documentation database.

The Firewalls have an integrated, hardened Linux operating system that is always a part of the engine software, eliminating the need for separate operating system installation, configuration, and patching.

Date and Time Settings

Make sure that the Date, Time, and Time zone settings are correct on any computer you use as a platform for any Management Center component, including the workstations used for the Management Client. The time settings of the engines do not need to be adjusted, as they are automatically synchronized with the Management Server’s time setting. For this operation, the time is converted to UTC time according to the Management Server’s time zone setting. The system always uses UTC internally.

Firewall Cluster IP Addresses

Because of their dual role as members of a common virtual entity and as separate physical devices, Firewall engines in a cluster have two types of IP addresses:

- **Cluster Virtual IP Address (CVI):** IP address that is used to handle traffic routed through the cluster for inspection. This is an IP address that is shared by all nodes in a cluster, in effect making the node appear as a single entity for the outside network behind the IP address.
- **Node Dedicated IP Address (NDI):** IP address that is used to handle traffic from or to a single node in a cluster. These IP addresses are used for the heartbeat connections between the engines in a cluster, for control connections from the Management Server, etc.

You can configure several CVIs and/or NDIs on the same physical interface.
Heartbeat Connection and State Synchronization in the Firewall Cluster

The nodes in a Firewall Cluster use a Heartbeat connection to keep track of the other nodes’ operation and to synchronize their state tables so that the connections can fail-over from a non-operational node to the remaining nodes when necessary.

The heartbeat connection is essential for the operation of the cluster. Take special care to ensure that the heartbeat network works correctly and reliably. Make sure that you are using the correct type of network cables (after testing that they work), that the network interface cards’ duplex and speed settings match, and that any network devices in between the nodes are correctly configured. Problems in the heartbeat network may seriously degrade the performance of the cluster.

If you have a two-node Firewall Cluster, it is recommended to use a crossover cable without any intermediary devices between the nodes. If you use a switch or a router between the nodes, make sure that portfast is enabled on the switch or the router and that the speed/duplex settings of the switch/router and the Firewall devices are set to Auto. The Firewall must also be set to forward multicast traffic (see the Online Help or the Administrator’s Guide PDF for more information). It is possible to authenticate and encrypt the heartbeat traffic.

Firewall Cluster Modes

There are several operating modes for the Physical Interfaces. The Packet Dispatch mode is recommended for new installations as it requires no special switch or router configuration. The other modes are provided for backward compatibility. See the Firewall/VPN Reference Guide for more information on the other operating modes.

In Packet Dispatch mode, even though several cluster nodes can process the traffic, there is only one contact MAC address for each Physical Interface. This MAC address is controlled by a dispatcher node that forwards the packets to the correct Firewall nodes for processing. The dispatcher node is chosen separately for each Cluster Virtual IP Address, so different nodes may be selected as dispatcher nodes for different Cluster Virtual IP Addresses.

The packet dispatcher for any given Cluster Virtual IP Address is changed when the dispatcher goes offline, for example. When the dispatcher changes, the Firewall sends an ARP message to the switch or router. The switch or router has to update its address table without significant delay when the packet dispatcher MAC address is moved to another Firewall node. This is a standard network addressing operation where the switch or router learns that the MAC address is located behind a different port. Then, the switch or router forwards traffic destined to the Cluster Virtual IP Address to this new packet dispatcher.
CHAPTER 3

INSTALLING FIREWALL LICENSES

This chapter instructs how to generate and install licenses for Firewall engines.

The following sections are included:

- Overview to Firewall Licenses (page 20)
- Generating New Licenses (page 21)
- Installing Licenses (page 21)
Overview to Firewall Licenses

Each Firewall engine must have its own license. Some engines use a Security Engine Node license. Other engines use Firewall-specific licenses. The correct type of license for each engine is generated based on your proof-of-license (POL) or proof-of-serial-number (POS).

With Firewall appliance version 5.0 or newer, it is possible to download and install engine licenses automatically. This is possible if the Generate and Install New Licenses Automatically option has been selected in the SMC and there is a working Internet connection between the Management Server and the Stonesoft License Center.

If there is no connection between the Management Server and the Stonesoft License Center, the Firewall appliance (version 5.0 or newer) can be used without a license for 30 days. After this you must generate the license(s) manually at the Stonesoft License Center Web page and install them on the Management Server using the Management Client before you can bring your system fully operational.

All firewalls can have a management-bound license, which is bound to the POL (proof-of-license) code of the Management Server. New appliance models can alternatively be bound to the POS (proof-of-serial number) code of the appliance. POS binding is always recommended if the option is shown as available when you generate a license for your appliance.

The Management Server’s license may also be limited to managing only a certain number of firewalls.

What's Next?
- If you need new licenses, proceed as explained in the overview below.
- If you do not need new licenses for the firewalls and NAT is applied to communications between any system components, proceed to Configuring NAT Addresses (page 23).
- If you do not need new licenses for the firewalls and NAT is not applied to the communications, you are ready to define the Firewall element(s). Continue according to the Firewall type:
  - Configuring Single Firewalls (page 31)
  - Configuring Firewall Clusters (page 53)

Configuration Overview

The following steps are needed for installing licenses for Firewall engines.

1. Generate the licenses at the Stonesoft License Center. See Generating New Licenses (page 21).
2. Install the licenses in the Management Client. See Installing Licenses (page 21).
Generating New Licenses

You generate the licenses at the Stonesoft License Center based on your proof-of-license (POL, for software, included in the order confirmation message sent by Stonesoft) or proof of serial number (POS, for appliances, printed on a label attached to the appliance hardware). Evaluation licenses are also available at the website.

If you are licensing several components of the same type, remember to generate one license for each component.

▼ To generate a new license
1. Go to the Stonesoft License Center at www.stonesoft.com/license/.
2. Enter the required code (proof-of-license or proof-of-serial number) in the correct field and click Submit. The license page opens.
3. Click Register. The license generation page opens.
4. Enter the Management Server’s proof-of-license code for the engines that you want to license.
   • The Management Server’s proof-of-license can be found in the e-mail you received detailing your licenses. Later on, this information is shown in the Management Client for all licenses imported into the system.
5. Click Submit Request. The license file is sent to you in a moment. It will also become available for download at the license page.

Note – Evaluation license orders may need manual processing. See the license page for current delivery times and details.

Installing Licenses

To install licenses, the license files must be available to the computer that you use to run the Management Client. All licenses can be installed even though you have not yet defined all the elements the licenses will be bound to.

▼ To install licenses

2. Select one or more license files to install in the dialog that opens and click Install.
To check that the licenses were installed correctly

1. Click the Configuration icon and select Administration from the menu. The Administration Configuration view opens.

2. Expand the Licenses branch of the tree.

3. Select All Licenses in the list.

You should see one license for each Firewall engine. You must bind management-bound engine licenses manually to the correct engines once you have configured the engine elements. POS-bound engine licenses are attached to the correct engines once the engine is fully installed.

What’s Next?

- If NAT is applied to communications between the firewalls and other system components, proceed to Configuring NAT Addresses (page 23).
- Otherwise, you are ready to define the Firewall element(s). Continue according to the Firewall type:
  - Configuring Single Firewalls (page 31)
  - Configuring Firewall Clusters (page 53)
CHAPTER 4

CONFIGURING NAT ADDRESSES

This chapter contains the steps needed to configure Locations and contact addresses when a NAT (network address translation) operation is applied to the communications between the Firewall and other system components.

The following sections are included:

- Getting Started with NAT Addresses (page 24)
- Defining Locations (page 25)
- Adding SMC Server Contact Addresses (page 27)
Getting Started with NAT Addresses

If there is network address translation (NAT) between communicating system components, the translated IP address may have to be defined for system communications. All communications between the system components are presented as a table in Default Communication Ports (page 149).

You use Location elements to configure system components for NAT. There is a Default Location to which all elements belong if you do not assign them a specific Location. If NAT is applied between two system components, you must separate them into different Locations and then add a contact address for the component that needs to be contacted.

You can define a Default contact address for contacting a component (defined in the Properties dialog of the corresponding element). The component’s Default contact address is used in communications when components that belong to another Location contact the component and the component has no contact address defined for their Location.

Illustration 4.1  An Example Scenario for Using Locations

In the illustration above, there are several remote firewalls that are managed through Management and Log Servers at a central site. NAT is typically applied at the following points:

- The central site Firewall or an external router may provide the SMC servers external IP addresses on the Internet. The external addresses must be defined as contact addresses so that the remote firewalls can contact the servers across the Internet.
- The central Firewall’s IP address may be translated by an external router. The external IP address must be defined as a contact address to allow VPN connections from the remote firewalls to the central site using that address.
- NAT may also be applied at the remote sites (by external equipment) to translate the remote firewalls’ IP address. In this case, you must define contact addresses for the remote firewalls so that the Management Server can contact them. The communications between the remote firewalls and the Management Server may also be reversed, so that the remote firewalls open the connections to the Management Server and maintain the connections open while waiting for commands.
When contact addresses are needed, a single Location to group all remote sites may be enough. The SMC servers’ and the central Firewall’s definitions must include a contact address for the “Remote Firewalls” Location. However, if VPN communications between firewalls from different remote sites are allowed, it is necessary to create a Location for each remote Firewall and to add further contact addresses for the firewalls.

Configuration Overview
To add contact addresses, proceed as follows:

1. Define Location element(s). See Defining Locations.
2. Define contact addresses for the Management Server, and Log Server(s). See Adding SMC Server Contact Addresses (page 27).
3. Select the correct Location for firewalls and enter the contact address(es) for the firewalls when you create the Firewall elements. See Configuring Single Firewalls (page 31) and Configuring Firewall Clusters (page 53).

Defining Locations

The first task is to group the system components into Location elements based on which components are on the same side of a NAT device. The elements that belong to the same Location element always use the primary IP address (defined in the main Properties dialog of the element) when contacting each other.

▼ To create a new Location element
1. Click the Configuration icon in the toolbar, and select Administration. The Administration Configuration view opens.
2. Expand the **Other Elements** branch in the tree.

3. Right-click **Locations** and select **New Location**. The Location Properties dialog opens.

4. Enter a **Name**.

5. Select element(s) to add to the Location and click **Add**.

6. Repeat Step 5 until all necessary elements are added.

7. Click **OK**.
Adding SMC Server Contact Addresses

The Management Server and the Log Server can have more than one contact address for each Location. This allows you, for example, to define a contact address for each Internet link in a Multi-Link configuration for remotely managed components.

To define the Management Server and Log Server contact addresses

2. Expand the Network Elements branch in the tree and select Servers.

3. Right-click a server and select Properties. The Properties dialog for that server opens.
4. Select the Location of this server.
5. Enter the Default contact address. If the server has multiple alternative IP addresses, separate the addresses with commas.

Repeat to add other Locations as necessary.

What’s Next?
- If your Management Server or Log Server needs a contact address, proceed to Adding SMC Server Contact Addresses (page 27).
- If you plan to add contact addresses only for Single Firewall or Firewall Cluster elements, proceed to one of the following:
  - Configuring Single Firewalls (page 31)
  - Configuring Firewall Clusters (page 53)
6. Click **Exceptions** and define Location-specific contact addresses if the Default Contact Address(es) are not valid from all other Locations.

![Server Properties](image)

6

Note – Elements grouped in the same Location element always use the primary IP address (defined in the main Properties dialog of the element) when contacting each other. All elements not specifically put in a certain Location are treated as if they belonged to the same Location.

7. Click **OK** to close the server properties. You can define the contact addresses for other servers in the same way.

What’s Next?
- If you are installing a Single Firewall, proceed to Configuring Single Firewalls (page 31).
- If you are installing a Firewall Cluster, proceed to Configuring Firewall Clusters (page 53).
CONFIGURING FIREWALLS

In this section:

Configuring Single Firewalls - 31
Configuring Firewall Clusters - 53
Saving the Initial Configuration - 71
Defining Routing and Basic Policies - 79
This chapter contains the steps needed to complete the Single Firewall configuration that prepares the Management Center for a Firewall installation.

Very little configuration is done directly on the engines. Most of the configuration is done using the Management Client, so the engines cannot be successfully installed before defining them in the Management Client as outlined in this chapter.

The following sections are included:

- Configuration Overview (page 32)
- Adding a Single Firewall Element (page 32)
- Adding Physical Interfaces (page 35)
- Adding VLANs (page 36)
- Adding ADSL Interfaces (page 38)
- Adding Wireless Interfaces (page 39)
- Configuring IP Addresses for Physical, VLAN, ADSL, or SSID Interfaces (page 42)
- Adding Modem Interfaces (page 48)
- Binding Engine Licenses to Correct Elements (page 51)
Configuration Overview

Once you have the Stonesoft Management Center (SMC) installed and running, you can configure the Firewalls. This chapter explains the tasks you must complete before you can install and configure the physical firewalls.

The tasks you must complete are as follows:

1. Add Firewall element(s). See Adding a Single Firewall Element.
2. Define the Physical Interfaces and their properties. See Adding Physical Interfaces (page 35).
3. (Optional) Define the ADSL Interface. See Adding ADSL Interfaces (page 38).
4. (Optional) Define the Modem Interface(s). See Adding Modem Interfaces (page 48).
5. (Optional) Define the Wireless Interface. See Adding Wireless Interfaces (page 39).
6. Bind management-bound licenses to specific Firewall elements. See Binding Engine Licenses to Correct Elements (page 51).

Adding a Single Firewall Element

To add a new single-node Firewall to the Management Center, you must define a Single Firewall element that stores the configuration information related to the Firewall. You can also define several Single Firewall elements at the same time by using the Create Multiple Single Firewalls wizard. For more information on creating several Single Firewall elements at the same time, see the Online Help of the Management Client or the Administrator’s Guide PDF.

Only one interface is needed to install the Firewall: the Control Interface that is used for communications between the Management Server and the Firewall/VPN engine. Although you can configure more interfaces at any later time, it is simplest to add more interfaces right away, so that traffic can also be routed through the Firewall.

Selecting Interface Numbers

There are five types of interfaces on single firewalls:

- A Physical Interface represents an Ethernet port of a network interface card on the engine.
- An ADSL Interface represents the ADSL port of a pre-installed Stonesoft appliance. Only certain Stonesoft appliances have an integrated ADSL network interface card with an ADSL port.
- A Wireless Interface represents a wireless network interface card of a pre-installed Stonesoft appliance. Only certain Stonesoft appliances have an integrated wireless network interface card.
- A Modem Interface represents a 3G modem connected to a USB port on a pre-installed Stonesoft appliance. The Modem Interfaces are identified with Modem Numbers in the Management Center. A Modem Number is mapped to the modem’s IMEI (international mobile equipment identity) number, and each modem is assigned a unique ID when you connect the modem to the Firewall engine.
- A Tunnel Interface is a logical interface that is used as an end-point for tunnels in the Route-Based VPN. For detailed information about configuring Tunnel Interfaces and the Route-Based VPN, see the Management Client Online Help or the Administrator’s Guide PDF.
Physical Interfaces, ADSL Interfaces, and Wireless Interfaces have their own numbering system in the Management Center called Interface ID. The Modem numbers of Modem Interfaces and the Interface IDs of Physical Interfaces, ADSL Interfaces, and Wireless Interfaces in the Management Center are mapped to the corresponding network interfaces on the physical engine when the engine is initialized. Tunnel Interfaces are numbered with Tunnel Interface ID numbers. The Tunnel Interface IDs are automatically mapped to the physical network interfaces on the engine according to the routing configuration.

Check the correct interface numbers in the Appliance Installation Guides delivered with each appliance. If necessary, you can change the Interface ID and Modem number mapping after the initial configuration using the command line tools on the engine.

There are four ways to initialize single firewalls and establish contact between them and the Management Server.

- You can use plug-and-play configuration, in which you upload the initial configuration from the Management Client to the Stonesoft Installation Server and the Firewall engines download it from the Installation Server.
- You can save the initial configuration on a USB memory stick and use the memory stick to automatically configure the engine without using the command line Configuration Wizard.
- You can save the configuration on a USB memory stick to import some of the information in the command line Configuration Wizard on the engines.
- You can write down the one-time password and enter all information manually in the command line Configuration Wizard on the engines.

Creating a Single Firewall Element

This section covers the basic configuration of a Single Firewall element. For more information on configuring the Firewall, see the Online Help of the Management Client (click the help button in the dialogs to see help specific to that dialog) or the Administrator's Guide PDF.

In the following tasks, the example values filled in the images refer to the example network's Branch Office Firewall settings (see the Example Network Scenario (page 157)).

To create a Single Firewall element

1. Click the System Status icon. The System Status view opens.
2. Right-click **Firewalls** and select **New → Single Firewall**. The Single Firewall Properties dialog opens.

![Branch Office Firewall - Properties](image)

3. Enter a **Name**.

4. Select a **Log Server** for storing this Firewall’s logs.

5. **(Optional)** Define one or more **DNS IP Addresses**. These are the IP addresses of the DNS server(s) that the Firewall uses to resolve virus signature mirrors, domain names, and web filtering categorization services (which are defined as URLs). There are two ways to define IP addresses.
   - To enter a single IP address manually, click **Add** and select **Add IP Address**. Enter the IP address in the dialog that opens.
   - To define an IP address by using a Network element, click **Add** and select **Add Network Element**.

6. If required in your setup, select the **Location** (see **Configuring NAT Addresses** (page 23)).

7. **(Optional)** If you have a Stonesoft appliance, copy-and-paste the proof-of-serial (POS) code delivered with the appliance to the **Proof of Serial** field. Using the POS code allows you to configure the Firewall engine using plug-and-play configuration. See **Preparing for Plug-and-Play Configuration** (page 74) for more information.
Adding Physical Interfaces

To route traffic through the Firewall, you must define at least two physical network interfaces. There are three types of Physical Interfaces:

• A Normal interface corresponds to a single network interface on the Firewall engine.
• An Aggregated Link in High-Availability Mode represents two interfaces on the Firewall engine. Only the first interface in the aggregated link is actively used. The second interface becomes active only if the first interface fails.
• An Aggregated Link in Load-Balancing Mode also represents two interfaces on the Firewall engine. Both interfaces in the aggregated link are actively used and connections are automatically balanced between the two interfaces.

To add a Physical Interface

1. Switch to the Interfaces tab.

2. Right-click the empty space and select New → Physical Interface. The Physical Interface Properties dialog opens.

3. Select an Interface ID. This maps to a physical interface during the initial configuration of the engine.

4. Select the Type and also the Second Interface ID if the Type is Aggregated Link.
   • Link aggregation in the load-balancing mode is implemented based on the IEEE 802.3ad Link Aggregation standard. If you configure an Aggregated Link in Load-Balancing Mode,
connect both interfaces to a single switch. Make sure that the switch supports the Link Aggregation Control Protocol (LACP) and that LACP is configured on the switch.

• If you configure an Aggregated Link in High-Availability mode, connect the first interface in the link to one switch and the second interface to another switch.

5. Click OK.

The Physical Interface is added to the interface list. Add the necessary number of Physical Interfaces in the same way.

**What's Next?**

- If you want to divide any of the Physical Interfaces into VLANs, continue by Adding VLANs.
- If you want to define an ADSL Interface, continue by Adding ADSL Interfaces (page 38).
- If you want to define a Wireless Interface, continue by Adding Wireless Interfaces (page 39).
- If you want to define a Modem Interface, continue by Adding Modem Interfaces (page 48).
- Otherwise, proceed to Configuring IP Addresses for Physical, VLAN, ADSL, or SSID Interfaces (page 42).

## Adding VLANs

VLANs divide a single physical network link into several virtual links. You can add up to 4094 VLANs per interface.

**To add a VLAN Interface to a Physical Interface**

1. Right-click a Physical Interface and select New→VLAN Interface. The VLAN Interface Properties dialog opens.
2. Enter the **VLAN ID** (1-4094).

![VLAN Interface Properties for Interface 0]

3. Click **OK**.

The specified VLAN ID is added to the Physical Interface. Repeat the steps above to add further VLANs to the interface.

Note – The **VLAN ID** must be the same VLAN ID used in the switch at the other end of the VLAN trunk.

The VLAN Interface is now ready to be used as a network interface. The VLAN interface is identified as `Interface-ID.VLAN-ID`, for example `2.100` for Interface ID 2 and VLAN ID 100.

**What's Next?**
- If you want to define an ADSL Interface, continue by Adding ADSL Interfaces (page 38).
- If you want to define a Wireless Interface, continue by Adding Wireless Interfaces (page 39).
- If you want to define a Modem Interface, continue by Adding Modem Interfaces (page 48).
- Otherwise, proceed to Configuring IP Addresses for Physical, VLAN, ADSL, or SSID Interfaces (page 42).
**Adding ADSL Interfaces**

You can configure one ADSL Interface on a Single Firewall. ADSL is only supported on specific Stonesoft appliances that have an ADSL network interface card. The supported ADSL standards are ANSI T1.413 issue 2n, G.dmt, G.lite, ADSL2 DMT, ADSL2 G.lite, Annex A, and Annex B.

**To add an ADSL Interface**

1. Make sure you are on the Interfaces tab.

2. Right-click the empty space and select **New → ADSL Interface**. The ADSL Interface Properties dialog opens.

3. Select the **Interface ID**. This maps to the ADSL port during the initial configuration of the engine.

4. Click **OK** to close the ADSL Interface properties.

**What's Next?**

- If you want to define a Wireless Interface, continue by **Adding Wireless Interfaces** (page 39).
- If you want to define a Modem Interface, continue by **Adding Modem Interfaces** (page 48).
- Otherwise, proceed to **Configuring IP Addresses for Physical, VLAN, ADSL, or SSID Interfaces** (page 42).
Adding Wireless Interfaces

You can configure one Wireless Interface on a Single Firewall. Wireless Interfaces are only supported on specific Stonesoft appliances that have an integrated wireless network interface card.

To add a Wireless Interface

1. Make sure you are on the Interfaces tab.
2. Right-click the empty space and select New → Wireless Interface. The Wireless Interface Properties dialog opens.
3. Select the Interface ID. This maps to the Wireless port during the initial configuration of the engine.
4. Select the Country where the Firewall is used as a wireless access point.
5. Select the Band for the wireless interface access point.
6. Select the Wireless Mode for transmitting the wireless traffic according to the capabilities of the connecting clients.

Table 5.1 Wireless Modes

<table>
<thead>
<tr>
<th>Band</th>
<th>Wireless Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11b</td>
<td>11 Mbit wireless-b only mode.</td>
<td></td>
</tr>
<tr>
<td>802.11bg</td>
<td>54 Mbit wireless-b and g modes.</td>
<td></td>
</tr>
<tr>
<td>802.11g</td>
<td>54 Mbit wireless-g only mode.</td>
<td></td>
</tr>
<tr>
<td>802.11n</td>
<td>270 Mbit wireless-n only mode.</td>
<td></td>
</tr>
<tr>
<td>802.11bgn</td>
<td>270 Mbit wireless-b, g, and n modes.</td>
<td></td>
</tr>
</tbody>
</table>
7. Select the Channel for transmitting the wireless traffic. If there are other wireless access points nearby, use channels that are as far apart as possible to avoid interference.

8. Click OK. The Wireless Interface is added to the interface list.

Adding SSID Interfaces

An SSID (service set identifier) interface represents an 802.11 wireless LAN. You can define several SSID Interfaces for the Wireless Interface.

To add an SSID Interface

1. Right-click the Wireless Interface and select New SSID Interface. The SSID Interface Properties dialog opens.

2. Enter the Wireless Network Name (SSID). It identifies the network to the end-users.

3. Select if Wireless SSID Broadcast is Enabled (the wireless network name is broadcast to anyone in range) or Disabled (users must type the name to connect).

4. Select the MAC Address Type.
   - Hardware: The MAC address of the Firewall appliance’s wireless card. The first SSID interface that you define is automatically assigned the MAC address of the wireless card.
   - Custom: A custom MAC address. Enter the MAC Address in the field below.

What’s Next?
► Defining Security Settings for SSID Interfaces (page 41)

<table>
<thead>
<tr>
<th>Band</th>
<th>Wireless Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 GHz</td>
<td>802.11a</td>
<td>11 Mbit wireless-a only mode.</td>
</tr>
<tr>
<td></td>
<td>802.11an</td>
<td>270 Mbit wireless-a and n modes.</td>
</tr>
<tr>
<td></td>
<td>802.11n</td>
<td>270 Mbit wireless-n only mode.</td>
</tr>
</tbody>
</table>

Note – Some wireless clients do not support the 802.11n wireless mode with the WEP security mode. See Defining Security Settings for SSID Interfaces (page 41).
## Defining Security Settings for SSID Interfaces

**To define security settings for SSID Interfaces**

1. Switch to the **Security** tab in the SSID Interface Properties.

2. Select the Security Mode settings as explained in the table below.
   - When you select the security mode, the options particular for that mode are enabled. We recommend using one of the WPA security modes.

<table>
<thead>
<tr>
<th>Option</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disabled</td>
<td>Wireless traffic is not encrypted. Anyone within range can freely use and intercept traffic from this wireless network. We do not recommend using this setting.</td>
</tr>
<tr>
<td>WEP Open System</td>
<td>After the clients have connected to the Firewall, the wireless traffic is encrypted with a 40-bit, 104-bit, or 128-bit WEP (Wired Equivalent Privacy/Wireless Encryption Protocol) key. We do not recommend this security mode. If you must use WEP for compatibility reasons, use WEP Shared Key. Not! Some wireless clients do not support the 802.11n wireless mode with the WEP security mode.</td>
</tr>
<tr>
<td>WEP Shared Key</td>
<td>The connecting clients are authenticated using WEP (Wired Equivalent Privacy/Wireless Encryption Protocol). The wireless traffic is encrypted with a 40-bit, 104-bit, or 128-bit key. We do not recommend this security mode unless you must use WEP for compatibility reasons. Not! Some wireless clients do not support the 802.11n wireless mode with the WEP security mode.</td>
</tr>
<tr>
<td>WPA Personal</td>
<td>Wireless traffic is encrypted using the WPA or WPA2 protocol. Three encryption modes are available: either TKIP (Temporal Key Integrity Protocol) or AES (Advanced Encryption Standard) or both TKIP and AES are used.</td>
</tr>
<tr>
<td>WPA Enterprise</td>
<td>Same as above, but RADIUS-based authentication methods provided by an external authentication server or the Authentication Server component are used to authenticate the users. This is the most secure option offered, and it is recommended if an external RADIUS service is available.</td>
</tr>
</tbody>
</table>
3. Fill in the options for the selected security mode:
   • For WEP Open System and WEP Shared Key, select the Key Length and the Default Key, and enter 1 to 4 encryption keys.
   • For WPA Personal, select the WPA Mode and enter a Pre-Shared Key of 8 to 64 ASCII characters.
   • For WPA Enterprise, first select the WPA Mode and then click Select to choose the RADIUS Authentication Method that authenticates the users. See the Online Help of the Management Client or the Administrator’s Guide PDF for more information.

Configuring IP Addresses for Physical, VLAN, ADSL, or SSID Interfaces

A Single Firewall’s Physical Interface, VLAN Interface, or ADSL Interface can have one or more static IPv4 addresses or a dynamic IPv4 address. A Physical Interface or a VLAN Interface can also have one or more IPv6 addresses. An SSID Interface can have a single IPv4 or IPv6 address. Only IPv4 addresses are used in system communications.

What’s Next?
▶ Configuring IP Addresses for Physical, VLAN, ADSL, or SSID Interfaces

Adding Static IPv4 Addresses

To add an IPv4 address for a Physical, VLAN, ADSL, or SSID Interface
1. Make sure you are on the Interfaces tab.
2. Right-click a Physical, VLAN, or SSID Interface and select New IPv4 Address, or right-click an ADSL Interface and select New IPv4 Address. The IP Address Properties dialog opens.  

![IP Address Properties](image)

3. Enter the IPv4 Address.

4. Click Netmask and adjust the automatically added netmask if necessary. The Network Address and Broadcast IP Address are updated accordingly.

**What’s Next?**

- If the interface carries system communications and NAT is applied, proceed to To define a Contact Address for static IPv4 addressing.
- If you want to configure VRRP for a Physical or VLAN Interface, proceed to the section Configuring a Virtual Router on a Physical, VLAN, or SSID Interface (page 44).
- If you are finished configuring the static IPv4 address properties, click OK. Repeat the steps above if you want to add further IPv4 addresses to this interface or other Physical or VLAN Interfaces.
- If you want to add IPv6 addresses to a Physical, VLAN, or SSID Interface, proceed to Adding Static IPv6 Addresses (page 45).
- If you want to define Modem Interfaces, proceed to Adding Modem Interfaces (page 48).
- Otherwise, proceed to Setting Global Interface Options (page 49).

**To define a Contact Address for static IPv4 addressing**

1. Enter the Default contact address or select Dynamic to define the translated IP address of this component. It is used by default by components in a different Location.
2. If components from some Locations must use a different IP address for contact, click **Exceptions** and define the Location-specific addresses.

**What’s Next?**
- If you want to use VRRP on a Physical, VLAN, or SSID Interface, proceed to the section **Configuring a Virtual Router on a Physical, VLAN, or SSID Interface**.
- If you want to add IPv6 addresses to a Physical or VLAN Interface, proceed to **Adding Static IPv6 Addresses** (page 45).
- If you want to configure a Physical, VLAN, or ADSL Interface with a dynamic address, add the interface (see **Adding Physical Interfaces** (page 35), **Adding VLANs** (page 36), or **Adding ADSL Interfaces** (page 38)), and continue by **Configuring Dynamic IP Addresses** (page 46).
- If you want to define Modem Interfaces, proceed to **Adding Modem Interfaces** (page 48).
- Otherwise, proceed to **Setting Global Interface Options** (page 49).

**Configuring a Virtual Router on a Physical, VLAN, or SSID Interface**

- **To configure VRRP**
  1. Click **VRRP Settings**. The VRRP Settings dialog opens.

![VRRP Settings](image)

2. Select **Enable VRRP**

3. Enter the **ID**, **Priority**, and **IPv4 Address** according to the configuration of the virtual router.
4. Click **OK**.

**What’s Next?**
- If you want to configure a Physical, VLAN, or ADSL interface with a dynamic address, add the interface (see Adding Physical Interfaces (page 35), Adding VLANs (page 36), or Adding ADSL Interfaces (page 38)), and continue by Configuring Dynamic IP Addresses (page 46).
- If you want to define Modem Interfaces, proceed to Adding Modem Interfaces (page 48).
- If you are finished adding interfaces, proceed to Setting Global Interface Options (page 49).

### Adding Static IPv6 Addresses

**▸ To add an IPv6 address to a Firewall interface**

1. Make sure you are on the **Interfaces** tab.

2. Right-click a Physical, VLAN, or SSID Interface and select **New → IPv6 Address**. The IP Address Properties dialog opens.

3. Enter the **IPv6 Address**.
4. Enter the **Prefix Length** (0-128).
5. Click **OK**.

Repeat the steps above to define more static IPv6 addresses for this or other interfaces.

**What’s Next?**
- If you want to define Modem Interfaces, proceed to Adding Modem Interfaces (page 48).
- Otherwise, proceed to Setting Global Interface Options (page 49).
Configuring Dynamic IP Addresses

You can configure dynamic IPv4 addresses for Physical, VLAN, and ADSL Interfaces. Dynamic IPv6 addresses are not supported. The interfaces with a dynamic IPv4 address are identified by a DHCP Index, which is used for identification in other parts of the configuration (such as Firewall Policies) to represent the possibly changing IP address. A Modem Interface always has a dynamic IP address (see Adding Modem Interfaces (page 48)).

❖ To define an interface for dynamic IP addressing
  ➥ In the IP Address Properties, select Dynamic and a DHCP Index.

What's Next?
❖ If the interface carries system communications and NAT is applied, proceed to To define a Contact Address for dynamic IP addressing.
❖ If the interface’s dynamic IP address is assigned through PPPoE, proceed to To set up PPPoE (page 47).
❖ If you are finished configuring the dynamic IP address properties, click OK.
❖ If you want to define Modem Interfaces, proceed to Adding Modem Interfaces (page 48).
❖ Otherwise, proceed to Setting Global Interface Options (page 49).

❖ To define a Contact Address for dynamic IP addressing
  1. If the Default contact address is not dynamic, disable Dynamic and enter the static contact address. It is used by default by components in a different Location.

  2. If components from some Locations must use a different IP address for contact, click Exceptions and define the Location-specific addresses.

What's Next?
❖ If the interface’s dynamic IP address is assigned through PPPoE, proceed to To set up PPPoE (page 47).
❖ If you are finished configuring the dynamic IP address properties, click OK.
❖ If you want to define Modem Interfaces, proceed to Adding Modem Interfaces (page 48).
❖ Otherwise, proceed to Setting Global Interface Options (page 49).
To set up PPPoE
1. Click **PPPoE Settings**. The PPPoE Settings dialog opens.

2. Select **Enable PPPoE**.

3. Fill in the **User Name**, **Password**, and (optional) **Service Name**. If you do not have these, contact your service provider.
   - Select **Hide** to hide the input password characters.

4. Click **OK**.

**What's Next?**
- If you are finished configuring the dynamic IP address properties, click **OK**.
- If you want to define Modem Interfaces, proceed to **Adding Modem Interfaces** (page 48).
- If you are finished adding interfaces, proceed to **Setting Global Interface Options** (page 49).
Adding Modem Interfaces

You can use 3G modem(s) with a Single Firewall to provide wireless link(s) for outbound connections.

▼ To add a Modem Interface

1. Make sure you are on the Interfaces tab.

2. Right-click the empty space and select **New → Modem Interface**. The Modem Interface Properties dialog opens.

3. Select the **Modem Number** that is mapped to the modem’s IMEI (international mobile equipment identity) number.

4. Select the **DHCP index**. It is used to distinguish different DHCP Interfaces from one another.

5. Enter the **PIN** code if it is needed for the modem’s SIM card and the modem’s **Phone Number** if it differs from the default phone number.

6. Enter the rest of the information (**Access Point Name**, **Username**, **Password**, **Service Name**, and **Zone**) according to the instructions that you have received from your service provider.

7. Click **OK**. The Modem Interface is added to the interface list.
Add the necessary number of Modem Interfaces. Two active 3G modems are currently supported on Stonesoft appliances.

What's Next?
- Proceed to Setting Global Interface Options.

Setting Global Interface Options
The interfaces you have defined are shown as a tree on the Interfaces tab. You must next select the roles that the IP addresses have in system communications. Only IPv4 addresses are used in system communications.

To set global interface options for a single-node Firewall
1. Click Options. The Interface Options dialog opens.

2. Set the interface that is used as the Primary interface for Management Server contact.

3. (Optional, recommended) Select a Backup interface for Management Server contact (used if the Primary fails).

4. Select Node-initiated contact to Management Server if the control IP of the node is dynamically NATed.
5. Select the interface used as **Identity for Authentication Requests**.
   • This has no effect on routing; the address identifies the Firewall to external authentication servers.
   • The address is also shown in the default authentication prompt in Telnet-based authentication.

6. *(Optional)* Select the interface used as **Source for Authentication Requests**.
   • This has no effect on routing; the address identifies the Firewall when it sends an authentication request to an external authentication server over a VPN.

7. Click **OK**.

8. Click **OK** to close the Firewall Properties. You should see the notification shown in the illustration below.

![Confirmation](image)

9. Click **No** and proceed as explained below.

**What’s Next?**

- If you have Firewall licenses that you generated based on the POL code of the Management Server (instead of the Firewall’s IP address), proceed to **Binding Engine Licenses to Correct Elements** (page 51).
- Otherwise, you are ready to transfer the configuration to the physical Firewall engines. Proceed to **Saving the Initial Configuration** (page 71).
Binding Engine Licenses to Correct Elements

Licenses are created based on the Management Server’s POL code or based on a Firewall appliance’s POS code. After you have configured the Firewall elements in the Management Center, management-bound licenses must be manually bound to a specific Firewall element, because they contain no information that would automatically bind them to the correct Firewall. POS-bound appliance licenses are automatically attached to the correct engine when the engine is fully installed.

To bind a management-bound license to an engine

1. Click the Configuration icon in the toolbar and select Administration. The Administration Configuration view opens.

2. Browse to Licenses → Security Engine or Licenses → Firewall depending on the type of licenses you have. All imported licenses appear in the right panel.
3. Right-click a management-bound license (a license that states *Dynamic* in place of an IP address) and select **Bind**. The Select License Binding dialog opens.

4. Select the correct Firewall from the list.
5. Click **Select**.

The license is now bound to the selected Firewall element. If you made a mistake, right-click the license and select **Unbind**.

![Select License Binding dialog](image)

**Caution** – When you make a configuration change on the engine (policy upload or refresh), the license is permanently bound to that engine. Such licenses cannot be re-bound to some other engine without re-licensing or deleting the engine element it is bound to; until you do that, the unbound license is shown as Retained.

**What’s Next?**
- You are now ready to transfer the configuration to the physical Firewall engines. Proceed to *Saving the Initial Configuration* (page 71).
This chapter contains the steps needed to complete the Firewall Cluster configuration that prepares the Management Center for a Firewall Cluster installation.

Very little configuration is done directly on the engines. Most of the configuration is done using the Management Client, so the engines cannot be successfully installed before defining them in the Management Client as outlined in this chapter.

The following sections are included:

- Configuration Overview (page 54)
- Adding a Firewall Cluster Element (page 54)
- Adding Nodes to a Firewall Cluster (page 56)
- Adding Physical Interfaces (page 57)
- Adding VLANs (page 58)
- Configuring IP Addresses for Cluster Interfaces (page 59)
- Binding Engine Licenses to Correct Elements (page 68)
Configuration Overview

Once you have the Stonesoft Management Center (SMC) installed and running, you can configure the firewalls. This is mostly done through the Management Client. This chapter explains the tasks you must complete before you can install and configure the physical firewalls.

The tasks you must complete are as follows:

1. Add a Firewall Cluster element. See Adding a Firewall Cluster Element.
2. Add the necessary number of nodes to the Firewall Cluster. See Adding Nodes to a Firewall Cluster (page 56).
3. Define the physical interfaces and their properties. See Adding Physical Interfaces (page 57).
4. Bind management-bound licenses to specific nodes in the Firewall Cluster. See Binding Engine Licenses to Correct Elements (page 68).

Adding a Firewall Cluster Element

To introduce a new Firewall Cluster to the Management Center, you must define a Firewall Cluster element that stores the configuration information related to the firewalls.

You must define at least two interfaces for the Firewall Cluster:

- A Control Interface for communications between the Management Server and the Firewall/VPN engine.
- A Heartbeat Interface for communications between the cluster nodes. The heartbeat traffic is critical to the functioning of the cluster, so it is highly recommended to have a dedicated heartbeat interface.

You must also define a Cluster Virtual IP Address (CVI) that is shared by all the nodes in the cluster and is used for routing traffic through the Firewall.

Although you can configure more interfaces at any later time, it is simplest to add more interfaces right away, so that traffic can also be routed through the Firewall. You can use the Installation Worksheet for Firewall Clusters (page 163) to document the interfaces.

Selecting Interface Numbers

There are two types of interfaces on Firewall Clusters:

- A Physical Interface represents an Ethernet port of a network interface card on the engine.
- A Tunnel Interface is a logical interface that is used as an end-point for tunnels in the Route-Based VPN. For detailed information about configuring Tunnel Interfaces and the Route-Based VPN, see the Management Client Online Help or the Administrator's Guide PDF.

Physical Interfaces have their own numbering in the Management Center called Interface ID, which is independent of the operating system interface numbering on the Firewall engine. However, if you install and configure the engine automatically with a USB memory stick, the Interface IDs in the Firewall Cluster element are mapped to match the current physical interface numbering in the operating system (eth0 is mapped to Interface ID 0 and so on). You can change the Interface ID mapping using command line tools on the engine.
Tunnel Interfaces are numbered with Tunnel Interface ID numbers. The Tunnel Interface IDs are automatically mapped to the physical network interfaces on the engine according to the routing configuration.

Creating a Firewall Cluster Element

This section covers the basic configuration of a Firewall Cluster element. For information on all the options, see the Online Help of the Management Client (click the Help button in the dialogs) or the Administrator's Guide PDF.

In the following tasks, the example values filled in the images refer to the example network's Headquarters Firewall Cluster settings (see the Example Network Scenario (page 157)).

▼ To create a Firewall Cluster element

1. Click the System Status icon. The System Status view opens.

2. Right-click the empty space and select New → Firewall Cluster. The Firewall Cluster Properties dialog opens.

3. Enter a Name.

4. Select a Log Server for storing this Firewall Cluster’s logs.

5. (Optional) Define one or more DNS IP Addresses. These are the IP addresses of the DNS server(s) that the Firewall Clusters use to resolve virus signature mirrors, domain names,
and web filtering categorization services (which are defined as URLs). There are two ways to define IP addresses.

- To enter a single IP address manually, click Add and select Add IP Address. Enter the IP address in the dialog that opens.
- To define an IP address by using a Network element, click Add and select Add Network Element.

6. If required in your setup, select the Location (see Configuring NAT Addresses (page 23)).

### Adding Nodes to a Firewall Cluster

The Firewall Cluster properties have placeholders for two nodes when the element is created. A Firewall Cluster can have up to 16 nodes. Add all the nodes you plan to install before you begin configuring the interfaces.

**To add a node to a Firewall Cluster**


2. (Optional) Change the Name.

3. Click OK.

The node is added to the Firewall Cluster. Repeat these steps for each node you want to add.
**Adding Physical Interfaces**

There are three types of Physical Interfaces on Firewall Clusters:

- A *Normal* interface corresponds to a single network interface on each node in the Firewall Cluster.
- An *Aggregated Link in High-Availability Mode* represents two interfaces on each node. Only the first interface in the aggregated link is actively used. The second interface becomes active only if the first interface fails.
- An *Aggregated Link in Load-Balancing Mode* also represents two interfaces on each node. Both interfaces in the aggregated link are actively used and connections are automatically balanced between the two interfaces.

▼ **To add a physical interface**

1. Switch to the *Interfaces* tab.

2. Right-click the empty space and select *New Physical Interface*. The Physical Interface Properties dialog opens.

3. Select an *Interface ID*. This maps to a physical interface during the initial configuration of the engine.

4. Select the *Type* and also the *Second Interface ID* if the Type is Aggregated Link.
   - Link aggregation in the load-balancing mode is implemented based on the IEEE 802.3ad Link Aggregation standard. If you configure an Aggregated Link in Load-Balancing Mode, connect both interfaces to a single switch. Make sure that the switch supports the Link Aggregation Control Protocol (LACP) and that LACP is configured on the switch.
   - If you configure an Aggregated Link in High-Availability mode, connect the first interface in the link to one switch and the second interface to another switch.
5. Leave **Packet Dispatch** selected as the **CVI Mode** and add a **MAC Address** with an even number as the first octet. This MAC address must not belong to any actual network card on any of the nodes.

- Packet Dispatch is the primary clustering mode in new installations. See the *Firewall/VPN Reference Guide* for information on the other clustering modes.
- Different CVI modes can be used for different interfaces of a Firewall Cluster without limitations.

6. *(Optional)* Adjust the **MTU** if this link requires a lower MTU than the Ethernet-default 1500.

7. Click **OK**.

To route traffic through the Firewall, you must define at least two different physical network interfaces.

**What’s Next?**
- If you want to divide any of the interfaces into VLANs, continue by Adding VLANs.
- Otherwise, proceed to Configuring IP Addresses for Cluster Interfaces (page 59).

### Adding VLANs

VLANs divide a single physical network link into several virtual links. You can add up to 4094 VLANs per physical interface.

#### To add a VLAN to a physical interface

1. Right-click a physical interface and select **New → VLAN Interface**. The VLAN Interface Properties dialog opens.

2. Enter the **VLAN ID** (1-4094).

---

**Note** – All Cluster Virtual IP Addresses that are defined for the same physical network interface must use the same unicast MAC address. The dispatcher nodes use the MAC address you define here. Other nodes use their network card’s MAC address.
3. Click **OK**.

The specified VLAN ID is added to the physical interface. Repeat the steps to add further VLANs to the interface.

**Note** – The VLAN ID must be the same VLAN ID used in the switch at the other end of the VLAN trunk.

The VLAN interface is now ready to be used as a network interface. The VLAN interface is identified as `Interface-ID.VLAN-ID`, for example `2.100` for Interface ID 2 and VLAN ID 100.

### Configuring IP Addresses for Cluster Interfaces

There are two types of IP addresses for Firewall Cluster interfaces:

- A **Cluster Virtual IP Address (CVI)** is used for traffic that is routed through the Firewall for inspection. It is shared by all the nodes in the cluster.
- A **Node Dedicated IP Address (NDI)** is used for traffic that the nodes themselves send or receive (such as communication between the nodes and the Management Server or between the nodes in the cluster). Each node in the cluster has a specific IP address that is used as the Node Dedicated IP Address.

You can define more than one Cluster Virtual IP Address and/or Node Dedicated IP Address for the same physical interface or VLAN interface. To route traffic through the Firewall, you must define at least two IP Addresses. For a working cluster, you also need at least two Node Dedicated IP Addresses (one for management connections and one for the heartbeat traffic between the nodes).

A physical interface or a VLAN interface may have just a Cluster Virtual IP Address or a Node Dedicated IP Address. A Cluster Virtual IP Address is needed only if traffic that the Firewall inspects is routed to/from the interface. We recommend that you define a Node Dedicated IP Address for each interface that has a Cluster Virtual IP Address, if practical, as some features may not work reliably without a Node Dedicated IP Address.

IPv6 addresses are supported on Firewall Clusters with dispatch clustering mode. IPv6 and IPv4 addresses can be used together on the same Firewall Cluster. Only IPv4 addresses are used in system communications.

**What’s Next?**

- To define an IPv4 address, proceed to Defining IPv4 Addresses (page 60).
- To define an IPv6 address, proceed to Defining IPv6 Addresses (page 61).
Defining IPv4 Addresses

To add IPv4 addresses for a Firewall Cluster

1. Make sure you are on the Interfaces tab.

2. Right-click a physical interface or VLAN interface and select New → IPv4 Address. The IP Address Properties dialog opens.

3. Select the types of IP addresses that you want to add using the Cluster Virtual IP Address and Node Dedicated IP Address options. By default, both are selected.
   - If the interface does not receive or send traffic that the Firewall examines, there is no need to define a Cluster Virtual IP Address.
   - We recommend that you add a Node Dedicated IP Address for each (sub)network that is located behind the physical interface.

4. If you are adding a Cluster Virtual IP Address, enter the IPv4 Address that is used as the Cluster Virtual IP Address.

5. If you are adding a Node Dedicated IP Address for the nodes, set the IPv4 Address for each node by double-clicking the field.

6. (Optional) Modify the Netmask value as necessary.
What’s Next?

- If the interface(s) carry system communications and NAT is applied, complete the configuration in Defining Contact Addresses for Firewall Clusters (page 62).
- If you are finished configuring the IPv4 address properties, click OK. Repeat the steps above if you want to add further IP addresses to this interface or other physical interfaces or VLAN interfaces.
- If you want to add IPv6 addresses to a physical or VLAN interface, proceed to Defining IPv6 Addresses.
- Otherwise, proceed to Setting Global Interface Options for Clusters (page 64).

Defining IPv6 Addresses

To add IPv6 addresses for a Firewall Cluster

1. Make sure you are on the Interfaces tab.

2. Right-click a Physical interface or a VLAN and select New→IPv6 Address. The IP Address Properties dialog opens.
3. Select the types of IP addresses that you want to add using the **Cluster Virtual IP Address** and **Node Dedicated IP Address** options. By default, both are selected.
   • If the interface does not receive or send traffic that the Firewall examines, there is no need to define a Cluster Virtual IP Address.
   • We recommend that you add a Node Dedicated IP Address for each (sub)network that is located behind the physical interface.

4. If you are adding a Cluster Virtual IP Address, enter the **IPv6 Address** that is used as the Cluster Virtual IP Address.

5. If you are adding a Node Dedicated IP Address for the nodes, set the **IPv6 Address** for each node by double-clicking the field.

6. *(Optional)* Modify the **Prefix Length** *(0-128).*

---

**Defining Contact Addresses for Firewall Clusters**

It is necessary to define a Contact Address for a Firewall Cluster, for example, if the Firewall Cluster is used as a VPN gateway.

**To define a contact address for a Cluster Virtual IP Address**

1. Enter the **Default** contact address or select **Dynamic** to define the translated IP address of this component. It is used by default by components in a different Location.

2. If components from some Locations must use a different IP address for contact, click **Exceptions** and define the Location-specific addresses.
To define a contact address for a Node Dedicated IP Address

1. To define a contact address for the node-specific IP addresses, double-click the node’s Contact Address cell. The Exceptions dialog opens.

2. Enter the Default contact address to define the translated IP address of this engine. It is used by default by components in a different Location.

3. (Optional) Click Add to define a different contact address for contacting this engine from some specific Location.

4. Repeat as necessary, then click OK.

What’s Next?

- If you are finished configuring cluster interfaces, click OK and proceed to Setting Global Interface Options for Clusters (page 64).
Setting Global Interface Options for Clusters

The interfaces you have defined are shown as a tree on the Interfaces tab. You must next select the roles that the IP addresses have in system communications. Only IPv4 addresses are used in system communications.

To set global interface options

1. Click Options. The Interface Options dialog opens.

2. Select the interface options as explained in the table below.

Table 6.1  Firewall Interface Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Interface</td>
<td>Select the Primary Control Interface for Management Server contact. This interface is used for communications with the Management Server.</td>
</tr>
<tr>
<td></td>
<td><em>(Optional)</em> Select a Backup Control Interface that is used if the Primary interface is not available.</td>
</tr>
</tbody>
</table>
Configuring IP Addresses for Cluster Interfaces

3. Click **OK**.

The interfaces you have defined are shown as a tree-table on the **Interfaces** tab. Global interface options have codes in the tree-table (also note the Info column):

- “A” is the interface used as the identity for authentication requests
- “C” and “c” are the Primary and Secondary Control Interfaces
- “H” and “h” are the Primary and Secondary Heartbeat Interfaces

### Table 6.1  Firewall Interface Options (Continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Heartbeat Interface</td>
<td>Select a <strong>Backup</strong> Heartbeat Interface that is used if the Primary Heartbeat Interface is unavailable. It is not mandatory to configure a backup heartbeat, but we strongly recommend it. If heartbeat traffic is not delivered, the cluster cannot operate and traffic will be disturbed. We strongly recommend that you use a dedicated interface for the backup heartbeat as well. Note that the Backup Heartbeat interface has constant light activity for testing the link even when the Primary heartbeat is active. <strong>Caution!</strong> Primary and Backup Heartbeat networks exchange confidential information. If dedicated networks are not possible, configure the cluster to encrypt the exchanged information. See the Management Client <strong>Online Help</strong> or the <strong>Administrator's Guide</strong> PDF.</td>
</tr>
<tr>
<td>Identity for Authentication Requests</td>
<td>The IP address of the selected interface is used when an engine contacts an external authentication server and it is also displayed (by default) to end-users in Telnet-based authentication. This option does not affect the routing of the connection with the authentication server. The IP address is used only as a parameter inside the authentication request payload to give a name to the request sender.</td>
</tr>
<tr>
<td>Source for Authentication Requests</td>
<td>The IP address of the interface that has a Node Dedicated IP address that is used when an engine sends an authentication request to an external authentication server over VPN. This option does not affect the routing of the connection with the authentication server.</td>
</tr>
<tr>
<td>Default IP for Outgoing Traffic</td>
<td>This option defines the IP address that the nodes use if they have to initiate connections (system communications, ping, etc.) through an interface that has no Node Dedicated IP Address. You must select an interface that has an IP address defined for all nodes.</td>
</tr>
</tbody>
</table>
“0” is the default IP address for outgoing connections

Double-click to edit the interface. Make sure you do this at the correct level for the properties you want to edit.

If an interface used for external connections has only a Cluster Virtual IP Address, you must add manual ARP entries for the nodes as instructed in Adding Manual ARP Entries (page 67). Otherwise, click **OK** to close the Firewall Cluster Properties.

A Confirmation dialog opens. Click **No**.

**What’s Next?**
- If you generated Firewall licenses based on the POL code of the Management Server (instead of the Firewall’s primary control IP address), proceed to Binding Engine Licenses to Correct Elements (page 68).
- Otherwise, you are now ready to transfer the configuration to the physical Firewall Cluster engines. Proceed to Saving the Initial Configuration (page 71).
Adding Manual ARP Entries

ARP entries are normally managed automatically based on the Firewall’s routing configuration. However, you can also add manual ARP entries for the nodes. If an interface used for external connections has only a Cluster Virtual IP Address, you must add a static ARP entry that gives the node a permanent reference to an IP address/MAC address.

To add manual ARP entries
1. Click ARP Entries. The ARP Entry Properties dialog opens.

2. Click Add ARP Entry. A new entry is added to the table.

3. Click Type and select Static.
4. Click Interface ID and select the interface on which the ARP entry is applied.
5. Double-click IP Address and MAC Address and enter the IP address and MAC address information.
6. Repeat as necessary, then click OK.

If you are finished configuring the interfaces, click OK to close the Firewall Cluster Properties.
A Confirmation dialog opens. Click No.

What's Next?

- If you generated Firewall licenses based on the POL code of the Management Server (instead of the Firewall’s primary control IP address), proceed to Binding Engine Licenses to Correct Elements.
- Otherwise, you are now ready to transfer the configuration to the physical Firewall Cluster engines. Proceed to Saving the Initial Configuration (page 71).

Binding Engine Licenses to Correct Elements

Licenses are created based on the Management Server’s POL code or based on a Firewall appliance’s POS code. After you have configured the Firewall elements in the Management Center, management-bound licenses must be manually bound to specific Firewall engines, because they contain no information that would automatically bind them to the correct engine. POS-bound appliance licenses are automatically attached to the correct engine when the engine is fully installed. Each engine is licensed separately even when the engines are clustered.

To bind a management-bound license to a node

1. Click the Configuration icon in the toolbar and select Administration. The Administration Configuration view opens.
2. Browse to Licenses→Security Engine or Licenses→Firewall depending on the type of licenses you have. All imported licenses appear in the right panel.

3. Right-click a management-bound license (a license that states Dynamic in place of an IP address) and select Bind. The Select License Binding dialog opens.

4. Select the node and click Select.
The license is now bound to the selected node. If you made a mistake, right-click the license and select Unbind.

Repeat the steps to bind the management-bound licenses to all the nodes in the cluster.

Caution – When you make a configuration change on the engine (policy upload or refresh), the license is permanently bound to that engine. Such licenses cannot be re-bound to some other engine without re-licensing or deleting the engine element it is bound to; until you do that, the unbound license is shown as Retained.

What’s Next?
▶ You are now ready to transfer the configuration to the physical Firewall Cluster engines. Proceed to Saving the Initial Configuration (page 71).
CHAPTER 7

SAVING THE INITIAL CONFIGURATION

This chapter explains how to save a Firewall element configuration in the Management Center and how to transfer it to the physical Firewall engines.

The following sections are included:

- Configuration Overview (page 72)
- Saving the Initial Configuration for Firewall Engines (page 72)
- Transferring the Initial Configuration to Firewall Engines (page 77)
Configuration Overview

Once you have configured the Firewall elements in the Management Client, you must transfer the configuration information to the physical Firewall engines.

You must complete the following steps:

1. Save the initial configuration in the Management Client. See Saving the Initial Configuration for Firewall Engines.
2. Transfer the initial configuration to the physical Firewall engines. See Transferring the Initial Configuration to Firewall Engines (page 77).

Saving the Initial Configuration for Firewall Engines

The initial configuration sets some basic parameters for the Firewall and creates the one-time passwords needed to establish a connection with the Management Server.

There are four ways to initialize your Firewall engines and establish contact between them and the Management Server.

- If you are using a plug-and-play installation, you can upload the initial configuration from the Management Server to the Stonesoft Installation Server using the Management Client. When the initial configuration is uploaded to the Installation Server, the Firewall engines contact the Installation Server when they are plugged in and fetch the initial configuration. After this, the engines establish contact with the Management Server.
- You can save the initial configuration on a USB memory stick and use the memory stick to automatically configure the engine without using the command line Configuration Wizard.
- You can save the configuration on a USB memory stick to import some of the information in the command-line Configuration Wizard on the engines.
- You can write down the one-time password and enter all information manually in the command-line Configuration Wizard on the engines.

Note – Automatic configuration using a USB stick is primarily intended to be used with Stonesoft appliances, and may not work in all other environments. Uploading the initial configuration to the Stonesoft Installation Server can only be used with Stonesoft appliances and proof-of-serial codes.

To save the initial configuration


![Security Engine Configuration view](image)
2. Select **Security Engines**. A list of Security Engines opens.

![Security Engines Management Center](image)

3. Right-click the Firewall whose initial configuration you want to save and select **Configuration → Save Initial Configuration**. The Initial Configuration dialog opens.

**What’s Next?**
- If you want to use plug-and-play configuration, proceed to Preparing for Plug-and-Play Configuration (page 74).
- If you want to use automatic configuration, proceed to Preparing for Automatic Configuration (page 75).
- If you want to use the Configuration Wizard, proceed to Preparing for Configuration Using the Configuration Wizard (page 76).
Preparing for Plug-and-Play Configuration

To prepare for plug-and-play configuration

1. (Optional) Select **Enable SSH Daemon** to allow remote access to the engine command line.

- Enabling SSH in the initial configuration gives you remote command line access in case the configuration is imported correctly, but the engine fails to establish contact with the Management Server.
- Once the Firewall is fully configured, SSH access can be set on and off using the Management Client. We recommend that you enable the SSH access in the Management Client when needed and disable the access again when you are done. Make sure your Access rules allow SSH access to the engines from the administrators’ IP addresses only.

2. Select the **Local Time Zone** and the **Keyboard Layout**.

- The time zone selection is used only for converting the UTC time that the engines use internally for display on the command line. All internal operations use UTC time, which is synchronized with the Management Server’s time once the engine is configured. For external operations, engines use the time zone of their geographical location.

3. Select **Upload to Installation Server** to upload the initial configuration automatically to the Stonesoft Installation Server.

4. (Optional) Click **Select** and select the appropriate policy if you already have a policy you want to use for the Firewall. The selected policy is automatically installed on the Firewall after the Firewall has contacted the Management Server.

Caution – If you enable SSH, set the password for command line access after the initial configuration either through the Management Client or by logging in to the command line. When the password is not set, anyone with SSH access to the engine can set the password.
5. Click **OK**.

**What's Next?**

- Transferring the Initial Configuration to Firewall Engines (page 77)

### Preparing for Automatic Configuration

**To prepare for automatic configuration**

1. *(Optional)* Select **Enable SSH Daemon** to allow remote access to the engine command line.

- Enabling SSH in the initial configuration gives you remote command line access in case the configuration is imported correctly, but the engine fails to establish contact with the Management Server.
- Once the Firewall is fully configured, SSH access can be set on and off using the Management Client. We recommend that you enable the SSH access in the Management Client when needed and disable the access again when you are done. Make sure your Access rules allow SSH access to the engines from the administrators’ IP addresses only.

2. Select the **Local Time Zone** and the **Keyboard Layout**.

- The time zone selection is used only for converting the UTC time that the engines use internally for display on the command line. All internal operations use UTC time, which is synchronized with the Management Server's time once the engine is configured. For external operations, engines use the time zone of their geographical location.
- The **Name** and **Country** are only for your reference. Fill in the other settings according to information supplied by your service provider. **Type** (supported encapsulation method) must be Ethernet over ATM.

---

**Caution – If you enable SSH, set the password for command line access after the initial configuration either through the Management Client or by logging in to the command line. When the password is not set, anyone with SSH access to the engine can set the password.**

---
3. *(Optional)* Click **Select** and select the appropriate policy if you already have a policy you want to use for the Firewall. The selected policy is automatically installed on the Firewall after the Firewall has contacted the Management Server.

4. Click **Save As** and save the configuration to the **root** directory of a USB memory stick, so that the system can boot from it.

```
Caution – Handle the configuration files securely. They include the one-time password that allows establishing trust with your Management Server.
```

5. Click **OK**.

```
What’s Next?
► Transferring the Initial Configuration to Firewall Engines (page 77)
```

**Preparing for Configuration Using the Configuration Wizard**

▼ **To prepare for configuration using the Configuration Wizard**

1. If you plan to enter the information manually, write down or copy the **One-Time Password** for each engine. Keep track of which password belongs to which engine node.

![Configuration Wizard](image)

2. *(Optional)* If you plan to enter the information manually, write down or copy the **Management Server SSL Fingerprint** for additional security.

3. *(Optional)* Click **Select** and select the appropriate policy if you already have a policy you want to use for the Firewall. The selected policy is automatically installed on the Firewall after the Firewall has contacted the Management Server.

4. If you plan to import the configuration in the Configuration Wizard, click **Save As** and save the configuration on a USB memory stick.

```
Caution – Handle the configuration files securely. They include the one-time password that allows establishing trust with your Management Server.
```
5. Click **OK**.

**What’s Next?**
- Transferring the Initial Configuration to Firewall Engines

---

**Transferring the Initial Configuration to Firewall Engines**

You are now ready to install the Firewall engine(s). The initial configuration is transferred to the engines during the installation.

**What’s Next?**
- If you selected the plug-and-play configuration method and automatic policy installation, the system takes care of the installation procedures once you plug in the cables of the Firewall engine(s) and power the engine(s) on.
- If you have a Stonesoft appliance but you did not use the plug-and-play configuration method, see the installation and initial configuration instructions in the *Appliance Installation Guide* that was delivered with the appliance. After this, return to this guide to set up basic routing and policies. See *Defining Routing and Basic Policies* (page 79) or see the more detailed instructions in the *Online Help* of the Management Client or the *Administrator's Guide PDF*.
- If you want to use another type of device as the Firewall engine, proceed to *Installing the Engine on Intel-Compatible Platforms* (page 99).
CHAPTER 8

DEFINING ROUTING AND BASIC POLICIES

After successfully installing the Firewall and establishing contact between the Firewall engine(s) and the Management Server, the Firewall is left in the initial configuration state. Now you must define basic routing and policies to be able to use the Firewall for access control. Both of these tasks are done using the Management Client.

The following sections are included:

► Defining Routing (page 80)
► Defining Basic Policies (page 91)
► Commanding Engines Online (page 96)
Defining Routing

Routing is configured entirely through the Management Client. Most often only one or two simple tasks are needed to define routing information for Firewall elements:

- Define the default route. This is the route packets to any IP addresses not specifically included in the routing configuration should take. The default route should always lead to the Internet if the site has Internet access.
- Add routes to internal networks that are not directly connected to the Firewall if there are any. Directly connected networks are added automatically based on the IP addresses you defined for the Firewall’s interfaces.

Routing is most often configured using the following elements:

- **Network** elements: represent a group of IP addresses.
- **Router** elements: represent next-hop routers that are used for basic (non-Multi-Link) routing and to represent the ISP routers inside NetLink elements.
- **NetLink** elements: represent next-hop routers that are used for Multi-Link routing. In Multi-Link routing, traffic is automatically distributed between two or more (usually Internet) connections.

Note – When you define routing for an Aggregated Link in Load-Balancing Mode, make sure that the router supports the Link Aggregation Control Protocol (LACP) and that LACP is configured on the router.

The Firewall’s interfaces and their network definitions have been automatically added to the Routing view. As interfaces that belong to an aggregated link have the same network definitions, only the first interface selected for the aggregated link is shown in the list of interfaces.

▼ To access routing information

1. Select **Monitoring→System Status** from the menu.
2. Right-click the Firewall element and select **Routing**. The Routing view for the selected Firewall opens.
3. Expand the routing tree to view routing information for the interfaces. Click the Tools icon and select Expand All if you want to view the full routing information for all the interfaces.

First, you must add a default route. This is done using the Any Network element as explained on the next pages. Routing decisions are done from the most specific to the least specific route. The Any Network element (which covers all IP addresses) is always the last route that is considered. In other words, only packets that have a destination IP address that is not included anywhere else in your routing configuration are forwarded to the interface with the Any Network element.

Note – Adding a Network in the Routing tree makes that network routable, but does not allow any host in that network to make connections. The Firewall's policy defines which connections are allowed. All other connections are blocked.

What's Next?
- If you have more than one Internet connection and you use either an aggregated link or two or more network interfaces as the default route, proceed to Adding a Default Route With Multi-Link (page 83).
- Otherwise, proceed to Adding a Default Route with a Single Network Link (page 82).
Adding a Default Route with a Single Network Link

**To add a router**
- Right-click the Network under the interface to be used as the default route and select **New → Router**.

If this interface receives its IP address from a DHCP server or a PPP daemon, a special Router named **Gateway (DHCP Assigned)** is now added to the Routing tree. If that is the case, add the default route as described in the section **To add the default route for a single network link** (page 82). If the interface has a fixed IP address, the Router Properties dialog opens, and you must define the Router properties as explained in the next illustration.

**To define a Router**
1. Enter a **Name** for the Router.
2. Enter the **IPv4 Address** and/or the **IPv6 Address** of your Internet router.
3. Click **OK**.

**To add the default route for a single network link**
- Right-click the Router you just created and select **New → Any Network**.

You are not actually creating a new element in this case, but just inserting the existing default element “Any Network”. The Any Network element must appear in the Routing tree only once for each Firewall in the single-link configuration described here. If you need to insert Any Network
more than once, use the Multi-Link configuration instead (see Adding a Default Route With Multi-Link).

The internal network is behind this interface.

The Internet is behind this interface.

In the illustration above, one internal network is connected to the Internet through the Firewall. Note that it makes no difference to the Firewall which interfaces are internal and which are external. The configuration you create for the Firewall is the only deciding factor for which traffic is allowed and which is not.

**Adding a Default Route With Multi-Link**

**To create a NetLink**

Right-click the Network under an interface that is used as one of the default routes (to the Internet) and select **New**→**Static NetLink** or **New**→**Dynamic NetLink**. The Static NetLink Properties dialog opens.

**To define a NetLink**

1. Enter a **Name** for the NetLink.
   * If you are defining a Dynamic NetLink, continue by defining the rest of the NetLink Properties as described in the section To define the remaining NetLink properties (page 86).
2. (For Static NetLink only) Click Select for Gateway.


4. Enter a Name for the Router.
5. Enter the IPv4 Address of the Internet router for this NetLink.
6. Click OK.

Create a Router element for all Static NetLinks in the same way, so that they are ready in the system when you create the other Static NetLinks.

7. From the Router list that opens, select the correct Router and click Select.

To add a Network
1. Click Select for Network.
2. Open **Networks**. The existing elements are listed.

![Select Element](image)

3. Select the correct Network(s) and proceed to the section **To define the remaining NetLink properties** (page 86).
   - If the correct Network(s) are not on the list, create a new Network element by clicking the New icon and selecting **Network**. The Network Properties dialog opens.

![Network Properties](image)

4. Enter a **Name** for the Network.
5. Enter the **IPv4 Address** and the **Netmask**.
6. (Optional) Select **Broadcast and network addresses included** to include broadcast and network addresses in the Network.
7. Click **OK**.

8. Select the correct Network and click **Select**.

    ▼ To define the remaining NetLink properties

    1. (Optional) Enter the name of the service provider for your own reference.

    • **Probing Settings**, **Input Speed**, and **Output Speed** are used for specific Multi-Link features that are explained in the other guidebooks and the **Online Help**. Leave these empty for now.

    2. Click **OK**.

Define all the necessary NetLinks in the same way, then use the NetLinks to define the default route to the Internet.
To add the default route for Multi-Link

- Right-click the NetLink and select **New**→**Any Network**.

You are not actually creating a new element in this case, but just inserting the existing default element “Any Network”.

In the illustration above, internal networks are connected to the Internet using two Internet connections. Note that it makes no difference to the Firewall which interfaces are internal and which are external. The configuration you create for the Firewall is the only deciding factor for which traffic is allowed.

Caution – The configuration outlined above is only a part of the Multi-Link configuration. For additional steps required for a fully featured Multi-Link configuration, see the Management Client Online Help.
Defining Other Routes

The networks that are directly connected to the Firewall are automatically added to the Routing view. However, you may also need to route traffic to networks that are not directly connected. In that case, you must manually add the networks to the Routing view. You must also add the Router elements that represent the next-hop routers for routing traffic to those networks.

Usually, non-ISP routes use a single-link configuration, as explained below, but a Multi-Link configuration can be used instead if there are alternative links to the same network. If that is the case, add the routes using NetLinks instead of Router elements in a similar way as with the default route (see Adding a Default Route With Multi-Link (page 83)).

▼ To create a router

1. Right-click the Network that is the correct route to some other network and select New → Router. The Router Properties dialog opens.

2. Enter a Name for the Router.

3. Enter the IPv4 Address and/or the IPv6 Address of the gateway device that connects the networks.

4. Click OK.
To add networks

1. Right-click the Router you just added and select New → Network.

   You can add existing Networks by dragging and dropping them from the panel on the left.

2. Enter a Name for the Network.

3. Enter the IPv4 Address and the Netmask and/or the IPv6 Address and the Prefix Length (0-128).

4. (Optional) Select Broadcast and Network Addresses Included to include broadcast and network addresses in the Network.

5. Click OK.

Add as many Networks as you need to the Router element.
Antispoofing

Spoofing an IP address means that someone uses the IP address of some legitimate (internal) host to gain access to protected resources. Spoofing can be prevented with antispoofing rules.

Antispoofing is automatically configured based on the routing information of firewalls. By default, connection attempts with a source IP address from a certain internal network are only allowed through if they are coming from the correct interface as defined in the Routing tree. As the routing entry is usually needed for the communications to work, antispoofing rarely needs additional modifications.

If you need to make exceptions to the antispoofing configuration generated automatically, you can add individual Host elements in the Antispoofing view behind interfaces through which they are allowed to make transmissions. For more information, see the Management Client Online Help.

What's Next?

- If you have a license that is based on a restriction on the number of IP addresses in your networks, proceed to Using IP Address Count Limited Licenses.
- If you have an unlimited license or a throughput-based license, proceed to Defining Basic Policies.

Using IP Address Count Limited Licenses

If you have a license that is based on a restriction on the number of IP addresses in your networks, you must exclude the Internet interface from the IP address counting. Otherwise, addresses on the Internet are counted towards the license restriction and some of your internal hosts may not be allowed to connect through the Firewall.

To exclude an interface from IP address counting

- Right-click the Internet interface in the Routing tree and select Exclude from IP Counting.

Only one interface can be excluded from IP address counting.

Note – If you want to use Multi-Link with an IP address limited license, all network links must be made accessible through a single interface. See more information at www.stonesoft.com/support.
Defining Basic Policies

The final step in getting your Firewall up and running is creating the rules according to which the traffic is inspected. In addition to the rules in the policy, the other configuration information is also transferred to the Firewall when you install a policy on it (including the interface definitions and routing information).

To walk you through the basics of rule editing, the following illustrations show you an example of how to create a simple IPv4 Access rule that allows pinging from one host in your internal network to any address.

If you installed a policy automatically during the initial configuration, you can proceed directly to Commanding Engines Online (page 96).

To create a policy


2. Right-click Policies and select New → Firewall Policy.

3. Name the new Policy.
4. Select a template. Only the **Firewall Template** is available, as you have not created your own templates yet.

![Firewall Policy Properties](image)

5. Click **OK**. The Policy opens for editing.

**To add a rule**

- Double-click the green row, or right-click the row and select **Rule→Add Rule**.

![Test Firewall Policy (EDIT) - Management Center](image)

**Note – Inherited rules are not editable in the policy that inherits the rules.**

**To configure a ping rule**

1. Right-click **Network Elements** and select **New→Host**. The Host Properties dialog opens.
2. Enter a **Name** and the **IPv4 Address** of the Host.

![Host Properties](image)
3. Click **OK**.

4. Click the Source cell and begin typing **TEST host**. When the correct element is found, select it from the list.

5. Right-click the **Destination** cell and select **Set to ANY**.

6. Click the **Service** cell and type **Ping**. When the correct element is found, select it from the list.

7. Right-click the **Action** cell and select **Allow**.

If you want to add more rules, right-click the rule and select either **Rule → Add Rule Before** or **Rule → Add Rule After**.

By default, the Firewall maintains connection tracking information on connections allowed by a rule. As one result, you only have to add rules for allowing the opening of connections. Once the connection is opened, reply packets that belong to that connection are then allowed through as long as they are appropriate for the state of that particular connection. A second rule is only needed if connection opening needs to be allowed from the other end as well.
In the case of the ping rule in this example, the replies to pings made by the Test host are allowed through without any modification to the rules. However, if someone else tries to ping the Test host through the Firewall, the connection is blocked.

What's Next?
- If you want to ping between a private and a public IP address, add a rule on the IPv4 NAT tab to translate the IP address as explained in Adding a NAT Rule for the Example Ping Rule.
- If you do not want to create NAT rules now, proceed to Installing the Policy (page 95).

Adding a NAT Rule for the Example Ping Rule

To add a NAT rule
1. Right-click the IPv4 Access rule you just created and select Copy Rule.

2. Switch to the IPv4 NAT tab.

3. Right-click the green row and select Paste to add a NAT rule with the same Source, Destination, and Service as the IPv4 Access rule.

4. Right-click the NAT cell and select Edit NAT. The Network Address Translation dialog opens.

5. Select Static as the Translation Type.

6. Click Address and enter the public IP address of the Test host.
   - The original IP address is the contents of the Source cell in the NAT rule, since we are defining source address translation.

Note – Multi-Link Load balancing requires additional configuration and a specific type of NAT rule. See Outbound Traffic Management in the Online Help or in the Administrator’s Guide PDF for information on these additional steps.
7. Click **OK**.

The NAT rule is now finished. Again, there is no need to specify that the destination address in the reply packets must be translated back to the Test host’s private IP address. This return translation is done automatically. The static translation used in this rule is only practical for a small number of hosts. Dynamic translation is more suitable for a large number of translations, such as for Internet access for the whole office network.

### Installing the Policy

**To install the Firewall policy**

1. Click the Save and Install icon to save the policy and transfer the changes to the Firewall.

2. Select the correct Firewall.

3. Click **Add**.

4. Leave **Validate Policy Before Upload** selected if you want to validate the rules in the policy.

5. Click **OK**.

When the policy is installed, all the rules in the policy as well as all the Firewall’s other configuration information (including interface definitions and routing information) are transferred to the Firewall. If you validate the rules and the routing configuration at policy installation, the
issues found in the policy are displayed in a separate panel in the tab that opens to show the progress of the policy installation. See the Online Help or the Administrator's Guide PDF for more information on policy validation.

**Commanding Engines Online**

After a successful policy installation on Firewall engines, your system is ready to process traffic. You can control the firewalls using the right-click menu as shown in the illustration below.

▼ To check system status and issue commands to firewalls

1. Switch to the System Status view.

2. Check the status of the firewalls and SMC on the Status tab.
   - You can select a Firewall or server to view more information about it in the Info panel.

3. Use the Commands submenu to command engines Online/Offline. Only nodes in Online mode process traffic.
   - Depending on the selection in the Status tree, you can give commands individually for each node, for a selected group of nodes, for a whole cluster, or several firewalls at once.

This concludes the configuration instructions in this Installation Guide. To continue setting up your system, consult the Online Help (or the Administrator's Guide PDF), particularly the Getting Started section.

You can access the Online Help by pressing the F1 key, by selecting Help→Help Topics in the main menu, or by clicking the Help button in a dialog. Depending on which window is currently active, you see either a help topic that is related to the current window or the front page of the help system.
INSTALLING THE FIREWALL ENGINE

In this section:

Installing the Engine on Intel-Compatible Platforms - 99
CHAPTER 9

INSTALLING THE ENGINE ON INTEL-COMPATIBLE PLATFORMS

This chapter instructs how to install the Firewall/VPN engine on any standard Intel or Intel-compatible platform, such as AMD.

The following sections are included:

► Installing the Firewall Engine (page 100)
► Obtaining Installation Files (page 101)
► Starting the Installation (page 102)
► Configuring the Engine (page 103)
► Installing the Engine in Expert Mode (page 110)
Installing the Firewall Engine

Stonesoft hardware appliances are delivered with pre-installed software. If you are using a Stonesoft appliance, configure the software as instructed in the Appliance Installation Guide delivered with the appliance.

On other systems, the software is installed from CD-ROMs. Depending on your order, you may have received ready-made Management Center and Firewall/VPN engine CD-ROMs. If the CD-ROMs are not included in the order, you will first have to create them.

Caution – Check that the Automatic Power Management (APM) and Advanced Configuration and Power Interface (ACPI) settings are disabled in BIOS. Otherwise, the engine may not start after installation or may shut down unexpectedly.

Note – The engines must be dedicated to the Firewall. No other software can be installed on them.

Configuration Overview

1. If you do not have ready-made installation CD-ROMs, obtain the files from the Stonesoft website. See Obtaining Installation Files (page 101).
2. Start the installation and select the installation type. See Starting the Installation (page 102).
3. Configure the engines and establish contact with the Management Server. See Configuring the Engine (page 103).

What’s Next?
• If you have ready-made CD-ROMs, proceed to Starting the Installation (page 102).
• Otherwise, start by Obtaining Installation Files (page 101).
Obtaining Installation Files

Downloading the Installation Files
The engine installation files are available at the Stonesoft website.

2. Download the .iso image files.

Checking File Integrity
Before installing the Firewall/VPN engine from downloaded files, check that the installation files have not become corrupt or been modified. Using corrupt files may cause problems at any stage of the installation and use of the system. File integrity is checked by generating an MD5 or SHA-1 file checksum of the downloaded files and by comparing the checksum with the checksum on the download page at the Stonesoft website.

Windows does not have MD5 or SHA-1 checksum tools by default, but there are several third party programs available.

▼ To check MD5 or SHA-1 file checksum
1. Look up the correct checksum at https://my.stonesoft.com/download/.
2. Change to the directory that contains the file(s) to be checked.
3. Generate a checksum of the file using the command `md5sum filename` or `sha1sum filename`, where `filename` is the name of the installation file.

Example $ md5sum sg_engine_1.0.0.1000.iso
869aecd7dc39321aa2e0cfa7fadb8f sg_engine_1.0.0.1000.iso

4. Compare the displayed output to the checksum on the website. They must match.

Caution – Do not use files that have invalid checksums. If downloading the files again does not help, contact Stonesoft technical support to resolve the issue.

Creating the Installation CD-ROM
Once you have checked the integrity of the installation files, create the installation CD-ROMs from the files. Use a CD-burning application that can correctly read and burn the CD-structure stored in the .iso images. If the end result is a CD-ROM file with the original .iso file on it, the CD-ROM cannot be used for installation.
Starting the Installation

Before you start installing the firewalls, make sure you have the initial configuration and a one-time password for management contact for each Firewall engine. These are generated in the Management Center. See Saving the Initial Configuration (page 71) for more information.

What you see on your screen may differ from the illustrations in this guide depending on your system configuration.

Caution – Installing the Firewall/VPN engine software deletes all existing data on the hard disk.

To install the Firewall/VPN engine from a CD-ROM
1. Insert the engine installation CD-ROM into the drive and reboot the machine. The License Agreement appears.
2. Type YES and press Enter to accept the license agreement and continue with the configuration.
3. Select the type of installation: Full Install or Full Install in expert mode.
   • Type 1 for the normal Full Install.
   • Type 2 for the Full Install in expert mode if you want to partition the hard disk manually.
4. Enter the number of processors:
   • For a uniprocessor machine, type 1 and press Enter.
   • For a multiprocessor machine, type 2 and press Enter.
   • If you selected Full Install in expert mode in the previous step, continue in Installing the Engine in Expert Mode (page 110)
5. Type YES and press Enter to accept automatic hard disk partitioning. The installation process starts.

What's Next?
▶ If you want to use the automatic configuration method, do not reboot once the installation finishes. Continue by Configuring the Engine Automatically with a USB Stick (page 103).
▶ Otherwise, remove the CD-ROM and press Enter to reboot when prompted to do so. The Configuration Wizard starts. Continue in Configuring the Engine in the Engine Configuration Wizard (page 103).
Configuring the Engine

During the initial configuration, the operating system settings, network interfaces, 3G modem settings (single firewalls only), and the Management Server connection are defined.

Configuring the Engine Automatically with a USB Stick

The automatic configuration is primarily intended to be used with Stonesoft appliances, and may not work in all environments when you use your own hardware. If the automatic configuration does not work, you can still run the Configuration Wizard as explained in the next section and import or enter the information manually.

When automatic configuration is used, Interface IDs are mapped to physical network interfaces in sequential order: Physical Interface ID 0 is mapped to eth0, Physical Interface ID 1 is mapped to eth1, and so on. The Modem Numbers of Modem Interfaces defined for single firewalls are mapped to the IMEI (international mobile equipment identity) number that each modem has. Each modem connected to the engine is also automatically assigned a unique modem ID when the engine is configured.

1. To install and configure the engine with a USB stick
   1. Make sure you have a physical connection to the appliance using a monitor and keyboard or a serial cable.
   2. Insert the USB stick.
   3. Remove the CD-ROM and press Enter at the installation finished prompt. The engine reboots, imports the configuration from the USB stick, and makes the initial contact to the Management Server.
      • If the automatic configuration fails, and you do not have a display connected, you can check for the reason in the log (sg_autoconfig.log) written on the USB stick.
      • If you see a “connection refused” error message, ensure that the Management Server IP address is reachable from the node.

   The configuration is complete when the appliance successfully contacts the Management Server and reboots itself.

Configuring the Engine in the Engine Configuration Wizard

The Firewall engine’s settings (for example, network card settings, the mapping of Interface IDs to physical interfaces on the engine, and the modem IDs of 3G modems connected to a Single Firewall) can be configured in the Configuration Wizard. The wizard can be run at any time issuing the sg-reconfigure command on the engine command line.

If you have stored the configuration on a USB memory stick (see Saving the Initial Configuration (page 71)), you can import it to reduce the need for typing in information.

Note – The imported configuration does not contain a password for the root account, so you must set the password manually in the Management Client before you can log in for command line access to the engine. See the Online Help of the Management Client or the Administrator’s Guide PDF for more information.
To select the role and the configuration method

1. Highlight **Role** and press **Enter** to select the role for the Security Engine.

2. Highlight **Firewall/VPN** and press **Enter**. The role-specific Configuration Wizard starts.

3. Select one of the following configuration methods:
   - Highlight **Import** and press **Enter** to import a saved configuration.
   - Highlight **Next** and press **Enter** to manually configure the Firewall engine's settings.

Proceed to Configuring the Operating System Settings (page 105).

To import the configuration

1. Select **USB Memory** and press **Enter**.

2. Select the correct configuration file. Remember that these are specific to each individual Firewall engine node.

3. Highlight **Next** and press **Enter** to continue.
Configuring the Operating System Settings

The Configure OS Settings screen is displayed. Some of the settings may be filled in if you imported a configuration as explained above (depending on the type of configuration imported).

▼ To set the keyboard layout

1. Highlight the entry field for **Keyboard Layout** and press **Enter**. The Select Keyboard Layout page opens.

2. Highlight the correct layout and press **Enter**.
   - If the desired keyboard layout is not available, use the best-matching available layout, or select US_English.

**Tip** – Type the first letter of the desired keyboard layout to move forward more quickly.

▼ To set the engine’s timezone

1. Highlight the entry field for **Local Timezone** and press **Enter**. The Select Timezone page opens.

2. Select the timezone from the list in the same way you selected the keyboard layout.

The timezone setting affects only the way the time is displayed on the engine command line. The actual operation always uses UTC time. The engine’s clock is automatically synchronized with the Management Server’s clock.

▼ To set the rest of the operating system settings

1. Type in the name of the Firewall.
2. Enter and confirm the password for the user root. This is the only account for command line access to the engine.

3. (Optional) Highlight Enable SSH Daemon and press the spacebar to allow remote access to the engine command line using SSH.

   ![Note](image)

   Note – Unless you have a specific need to enable SSH access to the engine command line, we recommend leaving it disabled.

4. Highlight Next and press Enter. The Configure Network Interfaces page is displayed.

**Configuring the Network Interfaces**

The configuration utility can automatically detect which network cards are in use. You can also add interfaces manually if necessary. If the list is not populated automatically, you can launch the autodetect as explained in the illustration below.

**To define the network interface drivers automatically**

- Highlight Autodetect and press Enter.

![Image]

Check that the autodetected information is correct and that all interfaces have been detected.

**What’s Next?**

- If there are problems, add the network interfaces manually as explained in To define the network interface drivers manually (page 107) (you can overwrite any autodetected setting).
- Otherwise, proceed to To map the interfaces to Interface IDs (page 106).

**Tip** – You can use the Sniff option for troubleshooting the network interfaces. Select Sniff on an interface to run network sniffer on that interface.

**To map the interfaces to Interface IDs**

1. Change the IDs as necessary to define how the interfaces are mapped to the Interface IDs and Modem Numbers you defined in the Firewall element.
2. If necessary, highlight the Media column and press Enter to change settings to match those used by the device at the other end of the link.

3. Highlight the Mgmt column and press the spacebar on your keyboard to select the correct interface for contact with the Management Server.

4. Highlight Next and press Enter to continue. Proceed to Contacting the Management Server (page 107).

To define the network interface drivers manually
1. Highlight Add and press Enter.

2. Select the correct driver for your network card and press Enter.

What’s Next?
➢ Repeat as necessary, then map the interfaces to Interface IDs as explained above.

Contacting the Management Server
The Prepare for Management Contact page opens. If the initial configuration was imported from a USB memory stick, most of this information is filled in.

Note – If there is an intermediate firewall between this firewall and the Management Server, make sure that the intermediate firewall's policy allows the initial contact and all subsequent communications. See Default Communication Ports (page 149) for a listing of the ports and protocols used.
Before the engine can make initial contact with the Management Server, you activate an initial configuration on the engine. The initial configuration contains the information that the engine needs to connect to the Management Server for the first time.

- To define PPPoE settings
  1. Highlight **Settings** and press **Enter**. The PPPoE Settings page opens.
  2. Fill in the account details according to the information you have received from your service provider.
  3. Highlight **OK** and press **Enter**.

What’s Next?

- If the IP address of the control interface is assigned by a DHCP server, select **Obtain Node IP address from a DHCP server** and continue in To fill in the Management Server information (page 109).
- If the IP address of the control interface is assigned through PPPoE, select **Use PPPoE** and continue in To define PPPoE settings (page 108).
- If you have selected a Modem Interface as the control interface on a Single Firewall, the **Use Modem** option is automatically selected. Continue in To define modem settings (page 109).
- If the IP address of the control interface is static, select **Enter node IP address manually** and fill in the **IP address** and **Netmask** (always), and **Gateway to management** (if the Management Server is not in a directly connected network).
To define modem settings

2. Fill in the account details according to the information you have received from your service provider.
3. Highlight Ok and press Enter.

To fill in the Management Server information

In the second part of the configuration, you define the information needed for establishing a trust relationship between the engine and the Management Server.

If you do not have a one-time password for this engine, see Saving the Initial Configuration for Firewall Engines (page 72).

1. Select Contact or Contact at Reboot and press the spacebar.
2. Enter the Management Server IP address and the one-time password.
3. (Optional) Fill in the Key fingerprint (also shown when you saved the initial configuration). Filling it in increases the security of the communications.
4. Highlight Finish and press Enter. The engine now tries to make initial Management Server contact. The progress is displayed on the command line.
   • If you see a “connection refused” error message, ensure that the one time password is correct and the Management Server IP address is reachable from the node. Save a new initial configuration if you are unsure about the password.
   • If there is another firewall between the engine and the Management Server or Log Server, make sure that the firewall’s policy allows the initial contact and the subsequent communications. See Default Communication Ports (page 149) for a list of the ports and protocols used.

If the initial management contact fails for any reason, the configuration can be started again with the sg-reconfigure command.

Note – The one-time password is engine-specific and can be used only for one initial connection to the Management Server. Once initial contact has been made, the engine receives a certificate from the Management Center for identification. If the certificate is deleted or expires, you need to repeat the initial contact using a new one-time password.
After Successful Management Server Contact

After you see a notification that Management Server contact has succeeded, the Firewall engine installation is complete and the Firewall is ready to receive a policy. The Firewall element’s status changes in the Management Client from Unknown to No Policy Installed, and the connection state is Connected, indicating that the Management Server can connect to the node.

What’s Next?

► To finish your Firewall configuration, proceed to Defining Routing and Basic Policies (page 79).

Installing the Engine in Expert Mode

In expert mode, you partition the hard disk manually. If you are unfamiliar with partitioning hard disks in Linux, we recommend that you use the normal installation process.

Caution – When using the command prompt, use the reboot command to reboot and halt command to shut down the node. Do not use the init command. You can also reboot the node using the Management Client.

To start the installation, reboot from the CD-ROM (see Installing the Firewall Engine (page 100)).

Partitioning the Hard Disk Manually

Typically, you need five partitions for an engine as explained in the table below.

Caution – Partitioning deletes all the existing data on the hard disk.

► To partition the hard disk

1. If you are asked whether you want to create an empty partition table, type y to continue.
2. When prompted, press Enter to continue. The partition table is displayed.
3. Create the partitions for the engine as follows:

Table 9.1 Partitions for the Engine

<table>
<thead>
<tr>
<th>Partition</th>
<th>Flags</th>
<th>Partition Type</th>
<th>Filesystem Type</th>
<th>Size</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Engine root A</td>
<td>bootable</td>
<td>Primary</td>
<td>Linux</td>
<td>200 MB</td>
<td>The bootable root partition for the Firewall engine.</td>
</tr>
<tr>
<td>Engine root B</td>
<td>Primary</td>
<td>Linux</td>
<td>200 MB</td>
<td></td>
<td>Alternative root partition for the Firewall engine. Used for the engine upgrade.</td>
</tr>
<tr>
<td>Swap</td>
<td>Logical</td>
<td>Linux swap</td>
<td>Twice the size of physical memory.</td>
<td></td>
<td>Swap partition for the Firewall engine.</td>
</tr>
</tbody>
</table>
### Allocating Partitions

After partitioning the hard disk, the partitions are allocated for the Firewall engine.

<table>
<thead>
<tr>
<th>Partition</th>
<th>Flags</th>
<th>Partition Type</th>
<th>Filesystem Type</th>
<th>Size</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data</td>
<td>Logical</td>
<td>Linux</td>
<td>500 MB or more</td>
<td></td>
<td>Used for the boot configuration files and the root user's home directory.</td>
</tr>
<tr>
<td>Spool</td>
<td>Logical</td>
<td>Linux</td>
<td>All remaining free disk space.</td>
<td></td>
<td>Used for spooling.</td>
</tr>
</tbody>
</table>

4. Check that the partition table information is correct.
5. Select **Write** to commit the changes and confirm by typing **yes**.
6. Select **Quit** and press **Enter**.

#### To allocate the partitions

1. Check that the partition table is correct. Type **yes** to continue.
2. Using the partition numbers of the partition table, assign the partitions for the engine, for example:
   • For the engine root A partition, type 1.
   • For the engine root B partition, type 2.
   • For the swap partition, type 5.
   • For the data partition, type 6.
   • For the spool partition, type 7.
3. Check the partition allocation and type **yes** to continue. The engine installation starts.
4. When installation is complete, remove the CD-ROM from the machine and press **Enter** to reboot.
5. Continue the configuration as described in **Configuring the Engine** (page 103).
UPGRADING

In this section:

Upgrading - 115
CHAPTER 10

UPGRADING

This chapter explains how you can upgrade your Firewall engines. When there is a new version of the Firewall engine software, you should upgrade as soon as possible.

The following sections are included:

► Getting Started with Upgrading Firewalls (page 116)
► Obtaining Engine Upgrade Files (page 117)
► Upgrading or Generating Licenses (page 118)
► Upgrading Engines Remotely (page 122)
► Upgrading Engines Locally (page 124)
Getting Started with Upgrading Firewalls

How Engine Upgrades Work

The primary way to upgrade engines is a remote upgrade through the Management Server. The upgrade package is imported on the Management Server manually or automatically. Then, you apply it to selected engines through the Management Client. Alternatively, the upgrade can be done locally when it is more convenient (for example, for spare appliances in storage).

Firewall engines have two alternative partitions for the engine software. When you install a new software version, it is installed on the inactive partition and the current version is preserved to allow rollback to the previous version in case the installation is interrupted or some other problems arise. If the engine is not able to return to operation, it automatically returns to the previous software version at the next reboot. You can also switch the active partition manually.

You can upload and activate the new software separately, for example, to upload the upgrade during office hours but activate it during a service window.

The currently installed working configuration (routing, policies, etc.) is stored separately and is not changed in an upgrade or a rollback. Although parts of the configuration may be version-specific (for example, if system communications ports are changed), the new version can use the existing configuration. Possible version-specific adjustments are made when you refresh the policy after the upgrade.

Limitations

It is not possible to upgrade between 32-bit version and a 64-bit version of the software. If you are running the software on a compatible standard server, you can reinstall the software using the other version (note that in clusters, 32-bit and 64-bit nodes cannot be online simultaneously). Stonesoft appliances do not support this type of architecture change.

What Do I Need to Know before I Begin

The Management Center must be up to date before you upgrade the engines. An old Management Center version may not be able to recognize the new engine versions and generate a valid configuration for them. Several older versions of engines can be controlled by any newer Management Center versions. See the Release Notes for version-specific compatibility information.

During a cluster upgrade, it is possible to have the upgraded nodes online and operational side by side with the older version nodes. This way, you can upgrade the nodes one by one while the other nodes handle the traffic. However, you must upgrade all the nodes to the same version as soon as possible, as prolonged use with mismatched versions is not supported.

To check the current engine software version, select the engine in the System Status view. The engine version is displayed on the General tab in the Info panel. If the Info panel is not shown, select View→Info.

Configuration Overview

Proceed as follows with the engine upgrade:

1. *(If automatic download has not been configured for engine upgrades)* Obtain the installation files and check the installation file integrity (see Obtaining Engine Upgrade Files). See the Management Client Online Help for information on configuring automatic download for engine upgrades.

2. *(If you are upgrading engines locally)* Create the installation CD-ROMs from the files with a CD-burning application that can correctly read and burn the CD-structure stored in the .iso images.

3. *(If automatic updates have not been configured for licenses)* Update the licenses (see Upgrading or Generating Licenses (page 118)). See the Management Client Online Help for information on configuring automatic updates for licenses.

4. Upgrade the Firewall engines one by one. Confirm that the upgraded engine operates normally before upgrading the next engine (see Upgrading Engines Remotely (page 122) or Upgrading Engines Locally (page 124)).

Obtaining Engine Upgrade Files

If the Management Server is not set up to download engine upgrades automatically or if you want to perform a local upgrade, you must download the installation files manually and check the installation file integrity using the MD5 or SHA-1 file checksums. Windows does not have MD5 or SHA-1 checksum programs by default, but there are several third party programs available.

▼ To manually download an engine upgrade file

1. Download the installation file from www.stonesoft.com/download/. There are two types of packages available:
   - The .zip package is used in the remote upgrade on all supported platforms. It can also be used for a local upgrade from a USB memory stick or a non-bootable CD-ROM.
   - The .iso download allows you to create a bootable installation CD-ROM for a local upgrade on all supported platforms.

2. Change to the directory that contains the file(s) to be checked.

3. Generate a checksum of the file using the command `md5sum` filename or `sha1sum` filename, where filename is the name of the installation file.

Example

```
$ md5sum sg_engine_1.0.0.1000.iso
869aeced7dc39321aa2e0cfa7f8f68f sg_engine_1.0.0.1000.iso
```

4. Compare the displayed output to the checksum on the website.

Caution – Do not use files that have invalid checksums. If downloading the files again does not help, contact Stonesoft technical support to resolve the issue.
To prepare a downloaded ZIP file for a remote upgrade
1. Log in to the Management Client and select File→Import→Import Engine Upgrades from the top menu.
2. Select the engine upgrade (sg_engine_version_platform.zip file) and click Import. The import takes a while. You can see the related messages in the status bar at the bottom of the Management Client window.

To prepare a downloaded ZIP file for a local upgrade
- Copy the file to the root directory of a USB memory stick or on a CD-ROM.

To prepare a downloaded ISO file for a local upgrade
- Create the installation CD-ROM for the engines with a CD-burning application that can correctly read and burn the CD-structure stored in the .iso images. If the end result is a CD-ROM file with the original .iso file on it, the CD-ROM cannot be used for installation.

What's Next?
- If you are sure you do not need to upgrade your licenses, you are ready to upgrade the Firewall engines. Continue by Upgrading Engines Remotely (page 122), or Upgrading Engines Locally (page 124) depending on whether you are going to upgrade the engines remotely through the Management Server or locally at the engine site.
- Otherwise, continue by Upgrading or Generating Licenses.

Upgrading or Generating Licenses
When you installed the engine software for the first time, you installed licenses that work with all versions of the Firewall up to that particular version. If the first two numbers in the old and the new version are the same, the upgrade can be done without upgrading licenses (for example, when upgrading from 1.2.3 to 1.2.4). When either of the first two numbers in the old version and the new version are different, you must first upgrade your licenses (for example, when upgrading from 1.2.3 to 1.3.0). Licenses are regenerated and installed automatically by default. You can also upgrade the licenses at the Stonesoft website. See the Management Client Online Help for information on upgrading the licenses automatically.

What's Next?
- If you need new licenses and want to upgrade the licenses one by one, proceed to Upgrading Licenses Under One Proof Code.
- If you need new license and want to upgrade one or more licenses at once, proceed to Upgrading Licenses Under Multiple Proof Codes (page 119).
Upgrading Licenses Under One Proof Code
A license file generated under one POL or POS code contains the license information for several components. You can also always use the multi-upgrade form to upgrade the licenses (see Upgrading Licenses Under Multiple Proof Codes (page 119)).

To generate a new license
1. Go to the Stonesoft License Center website at www.stonesoft.com/license/.
2. Enter the required code (proof-of-license or proof-of-serial number) in the correct field and click Submit. The license page opens.
3. Click Update. The license upgrade page opens.
4. Follow the directions on the page that opens to upgrade the license.

Upgrading Licenses Under Multiple Proof Codes
If you have several existing licenses with different POL or POS codes that you need to upgrade, you can make the work easier by generating the new licenses all at once.

To upgrade multiple licenses
1. Click the Configuration icon and select Administration. The Administration Configuration view opens.
2. Expand the Licenses branch and select Firewall. All Firewall licenses appear in the right panel.
3. Ctrl-select or Shift-select the licenses you want to upgrade.
4. Right-click one of the selected items and select Export License Info.
5. Select the location where the license file is saved in the dialog that opens. You are prompted to request a license upgrade.

![Confirmation Dialog](image)

6. *(Optional)* Click **Yes** in the message to launch the Stonesoft License Center website’s multi-upgrade form in your default browser.

Next, upload the license upgrade request file to the Stonesoft License Center website at [www.stonesoft.com/license/](http://www.stonesoft.com/license/) using the multi-upgrade form. The upgraded licenses are sent to you.

You can view and download your current licenses at the license website (log in by entering the proof-of-license or proof-of-serial number code at the License Center main page).

### Installing Licenses

After you have generated the licenses for the upgrade as described above, you install the license file in the Management Client.

- **To install licenses**
  1. Select **File**→**System Tools**→**Install Licenses**.

![System Status - Management Center](image)

  2. Select one or more license files for installing in the dialog that opens.
Checking the Licenses
After installing the upgraded licenses, check the license information. When you upgrade licenses, the old licenses are automatically replaced with the new licenses.

▼ To check the licenses
1. Click the Configuration icon and select Administration. The Administration Configuration view opens.

2. Expand the Licenses branch and select Security Engine or Firewall depending on the type of licenses you have.

What's Next?
► If you are upgrading the engines remotely through the Management Client, proceed to Upgrading Engines Remotely (page 122).
► If you are upgrading the engines using a physical connection to the engine, proceed to Upgrading Engines Locally (page 124).
Upgrading Engines Remotely

The remote upgrade has two separate parts, transfer and activation. You can choose to do both parts consecutively, or you can choose to transfer the configuration now and launch a separate task for the activation at a later time. You can also create a scheduled Task for the remote upgrade as instructed in the Management Client Online Help.

Note – Clusters operate normally throughout the upgrade when the upgrade is done in stages, but upgrade all nodes in the cluster to the same version as soon as possible. Prolonged use with mismatched versions is not supported. However, it is not possible to have 32-bit and 64-bit engines online in the cluster at the same time.

To upgrade the engine
1. Click the System Status icon. The System Status view opens.

2. (If you plan to activate the new software right away) Right-click the node you wish to upgrade and select Commands → Go Offline.
3. Right-click the node and select **Upgrade Software**.

4. Select the upgrade **Operation**:
   - transfer and activate the upgrade now
   - transfer the upgrade for later activation
   - activate an upgrade.

5. Check the node selection in the **Target** field and change it, if necessary.

![Remote Upgrade Task Properties](image)

Caution – To avoid an outage, do not activate the new configuration simultaneously on all the nodes of a Firewall Cluster. Activate the new configuration one node at a time, and proceed to the next node only after the previous node is back online.

6. Check the **Engine Upgrade** version for the upgrade and change it, if necessary.

7. Click **OK**.

   If you chose to activate the new configuration, you now need to acknowledge a warning that the node will be rebooted. A new tab opens showing the progress of the upgrade.

   - The time it takes to upgrade the node varies depending on the performance of your machine and the network environment. Click **Abort** if you want to stop the upgrade.
   - If you chose to activate the new configuration, once the engine is successfully upgraded, the machine is automatically rebooted and the upgraded engine is brought to online state.

If you are upgrading a Firewall Cluster, begin the upgrade on the next node only after the upgraded node is back online.

The upgrade overwrites the inactive partition and then switches the active partition. To undo the upgrade, use `sg-toggle-active` command or the engine's boot menu to switch back to the previous software version on the other partition. See **Command Line Tools** (page 129) for more information. This switch may also happen automatically at the next reboot if the engine is not able to successfully return to operation when it boots up after the upgrade.

**What's Next?**

- When the upgrades are finished, refresh the policy of upgraded engines to make sure any possible changes specific to the new software version are transferred to the engines.
Upgrading Engines Locally

Instead of upgrading the Firewall engines remotely from the Management Server, it is possible to upgrade the engines locally as described in this section. Upgrading locally requires a physical connection to the engine using a monitor and keyboard or a serial cable. During a Firewall Cluster upgrade, it is possible to have the upgraded nodes online and operational side by side with the older version nodes.

Note – Clusters operate normally throughout the upgrade when the upgrade is done in stages, but upgrade all nodes in the cluster to the same version as soon as possible. Prolonged use with mismatched versions is not supported. However, it is not possible to have 32-bit and 64-bit engines online in the cluster at the same time.

What’s Next?
- Upgrading From an Engine Installation CD-ROM
- Upgrading From a ZIP Archive File (page 126)

Upgrading From an Engine Installation CD-ROM

Follow the procedure below to upgrade Firewall engines to the latest version locally from a CD-ROM that you have created from an .iso image downloaded from the Stonesoft website or shipped to you by Stonesoft.

Caution – To avoid an outage, do not activate the new configuration simultaneously on all the nodes of a Firewall Cluster. Activate the new configuration one node at a time, and proceed to the next node only after the previous node is back online.

▼ To upgrade the Firewall locally from an installation CD-ROM
1. (Recommended) Log in to the node as root with the password set for the engine (you can set the password through the Management Client).
2. Insert the engine installation CD-ROM into the engine’s CD-ROM drive.
3. Reboot the node from the CD-ROM with the command reboot (recommended) or by cycling the power (if you cannot log in). You are prompted to select the upgrade type.

```
Stonewall Engine Installation System
No existing Stonewall Engine installation has been detected.
1. Upgrade existing installation
2. Re-install using configuration from existing installation
3. Full re-install (old configuration is not processed)
4. Full re-install in expert mode
Enter your choice: 
```
4. Select 1 to upgrade the previous installation and press ENTER to continue. The upgrade process starts.

```
Upgrading existing StoneGate installation:

PREFIX: /gs
ACTIVE: /dev/disk0s2
INACTIVE: /dev/disk0s1
BMP: /dev/disk0s2
SPR: /dev/disk0s1
defsys: 1
Inactive partition will be upgraded.
```

Extracting StoneGate image...
Upgrade finished! Remove CDROM disc and press Enter to reboot.

5. When the process is finished, remove the CD-ROM and press ENTER to reboot.
   - If the Configuration Wizard opens, configure the engine in the same way as after the first installation: refer to Configuring the Engine (page 103) for instructions on how to make the engine operational again.

6. When the upgrade is finished, right-click the node in the Management Client and select Go Online to command the node online. The node can also be brought online with the command `sg-cluster online` on the node.

   If you are upgrading a Firewall Cluster, begin the upgrade on the next node only after the upgraded node is back online.

   The upgrade overwrites the inactive partition and then switches the active partition. To undo the upgrade, use the `sg-toggle-active` command or the engine’s boot menu to switch back to the previous software version on the other partition. See Command Line Tools (page 129) for more information. This switch may also happen automatically at the next reboot if the engine is not able to successfully return to operation when it boots up after the upgrade.

What’s Next?

- When the upgrades are finished, refresh the policy of upgraded engines to make sure any possible changes specific to the new software version are transferred to the engines.
Upgrading From a ZIP Archive File

Follow the instructions below if you do not want to use the remote upgrade, but you want to use a .zip archive to upgrade the Firewall software.

Caution – To avoid an outage, do not activate the new configuration simultaneously on all the nodes of a Firewall Cluster. Activate the new configuration one node at a time, and proceed to the next node only after the previous node is back online.

To upgrade the engine locally from an archive file

1. (Recommended) Log in to the node as root with the password set for the engine (you can set the password through the Management Client).
2. Insert the USB stick or the CD-ROM.
3. Run the command `sg-reconfigure`. The engine Configuration Wizard opens.
4. Select Upgrade using the arrow keys and press ENTER.
5. Select the source media where the upgrade file is located.
6. (Optional) If you have not already done so, select Calculate SHA1 to calculate the checksum. The calculation takes some time. The calculated checksum must be identical to the one from the .zip file.
7. Select OK. The software is upgraded.
8. When prompted, press ENTER. The Firewall reboots to the new version.

If you are upgrading a Firewall Cluster, begin the upgrade on the next node only after the upgraded node is back online.

The upgrade overwrites the inactive partition and then switches the active partition. To undo the upgrade, use the `sg-toggle-active` command or the engine’s boot menu to switch back to the previous software version on the other partition. See Command Line Tools (page 129) for more information. This switch may also happen automatically at the next reboot if the engine is not able to successfully return to operation when it boots up after the upgrade.

Caution – Do not use files that have invalid checksums. Select Cancel if the checksum does not match and acquire a new copy of the upgrade file.

What’s Next?

- When the upgrades are finished, refresh the policy of upgraded engines to make sure any possible changes specific to the new software version are transferred to the engines.
In this section:

- Command Line Tools - 129
- Default Communication Ports - 149
- Example Network Scenario - 157
- Installation Worksheet for Firewall Clusters - 163
- Index - 167
APPENDIX A

COMMAND LINE TOOLS

This appendix describes the command line tools for Stonesoft Management Center and the engines.

Note – Using the Management Client is the recommended configuration method, as most of the same tasks can be done through it.

The following sections are included:

- Management Center Commands (page 130)
- Engine Commands (page 140)
- Server Pool Monitoring Agent Commands (page 147)
Management Center Commands

Management Center commands include commands for the Management Server, Log Server, Web Portal Server, and Authentication Server. Most of the commands are found in the `<installation directory>/bin/` directory. In Windows, the command line tools are `*.bat` script files. In Linux, the files are `*.sh` scripts.

Note – If you installed the Management Server in the `C:\Program Files\Stonsoft\Management Center` directory in Windows, some of the program data is stored in the `C:\ProgramData\Stonesoft\Management Center` directory. Command line tools may be found in the `C:\Program Files\Stonsoft\Management Center\bin` and/or the `C:\ProgramData\Stonesoft\Management Center\bin` directory.

Commands that require parameters must be run through the command line (cmd.exe in Windows). Commands that do not require parameters can alternatively be run through a graphical user interface, and may be added as shortcuts during installation.

Caution – login and password parameters are optional. Giving them as Command Line parameters may pose a security vulnerability. Do not enter login and password information unless explicitly prompted to do so by a Command Line tool.
Table A.1  Management Center Command Line Tools

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| sgArchiveExport   | Displays or exports logs from archive. This command is only available on the Log Server. The operation checks privileges for the supplied administrator account from the Management Server to prevent unauthorized access to the logs. Enclose details in double quotes if they contain spaces.  
  
  **Host** specifies the address of the Management Server. If the parameter is not defined, the loopback address (localhost) is used.  
  
  **login** defines the username for the account that is used for this operation. If this parameter is not defined, the username root is used.  
  
  **pass** defines the password for the user account.  
  
  **format** defines the file format for the output file. If this parameter is not defined, the XML format is used.  
  
  **i** defines the source from which the logs will be exported. Can be a folder or a file. The processing recurses into subfolders.  
  
  **o** defines the destination file where the logs will be exported. If this parameter is not defined, the output is displayed on screen.  
  
  **f** defines a file that contains the filtering criteria you want to use for filtering the log data. You can export log filters individually in the Management Client through Tools → Save for Command Line Tools in the filter’s right-click menu.  
  
  **e** allows you to type in a filter expression manually (using the same syntax as exported filter files).  
  
  **-h**, **-help**, or **-?** displays information on using the script.  
  
  **-v** displays verbose output on the command execution.  
  
  **Example** (exports logs from one full day to a file using a filter):  
  sgArchiveExport login=admin pass=abc123 i=c:/stonesoft/Stonesoft/data/archive/firewall/year2011/month12./sgB.day01/ f=c:/stonesoft/Stonesoft/export/MyExportedFilter.flp format=CSV o=MyExportedLogs.csv |
### sgBackupAuthSrv

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[pwd=&lt;password&gt;]</td>
<td>Enables encryption.</td>
</tr>
<tr>
<td>[path=&lt;destpath&gt;]</td>
<td>Defines the destination path.</td>
</tr>
<tr>
<td>[nodiskcheck]</td>
<td>Ignores free disk check before creating the backup.</td>
</tr>
<tr>
<td>[comment=&lt;comment&gt;]</td>
<td>Allows you to enter a comment for the backup. The maximum length of a comment is 60 characters.</td>
</tr>
<tr>
<td>[-h</td>
<td>--help]</td>
</tr>
</tbody>
</table>

This script creates a backup of Authentication Server user information. The backup file is stored in the `<installation directory>/backups/` directory. Backing up the Authentication only backs up Users, not the configuration of the Authentication Server. The Authentication Server configuration is included in the Management Server backup.

### sgBackupLogSrv

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[pwd=&lt;password&gt;]</td>
<td>Enables encryption.</td>
</tr>
<tr>
<td>[path=&lt;destpath&gt;]</td>
<td>Defines the destination path.</td>
</tr>
<tr>
<td>[nodiskcheck]</td>
<td>Ignores free disk check before creating the backup.</td>
</tr>
<tr>
<td>[comment=&lt;comment&gt;]</td>
<td>Allows you to enter a comment for the backup. The maximum length of a comment is 60 characters.</td>
</tr>
<tr>
<td>[nofsstorage]</td>
<td>Creates a backup only of the log server configuration without the log data.</td>
</tr>
<tr>
<td>[-h</td>
<td>--help]</td>
</tr>
</tbody>
</table>

This script creates a backup of Log Server configuration data. The backup file is stored in the `<installation directory>/backups/` directory. Twice the size of log database is required on the destination drive. Otherwise, the operation fails.

### sgBackupMgtSrv

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[pwd=&lt;password&gt;]</td>
<td>Enables encryption.</td>
</tr>
<tr>
<td>[path=&lt;destpath&gt;]</td>
<td>Defines the destination path.</td>
</tr>
<tr>
<td>[nodiskcheck]</td>
<td>Ignores free disk check before creating the backup.</td>
</tr>
<tr>
<td>[comment=&lt;comment&gt;]</td>
<td>Allows you to enter a comment for the backup. The maximum length of a comment is 60 characters.</td>
</tr>
<tr>
<td>[-h</td>
<td>--help]</td>
</tr>
</tbody>
</table>

This script creates a complete backup of the Management Server (including both the local configuration and the stored information in the configuration database). The backup file is stored in the `<installation directory>/backups/` directory. Twice the size of the Management Server database is required on the destination drive. Otherwise, the operation fails.
Table A.1  Management Center Command Line Tools (Continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sgCertifyAuthSrv</td>
<td>Contacts the Management Server and creates a new certificate for the Authentication Server to allow secure communications with other system components. Renewing an existing certificate does not require changing the configuration of any other system components.</td>
</tr>
</tbody>
</table>
| sgCertifyLogSrv      | Contacts the Management Server and creates a new certificate for the Log Server to allow secure communications with other system components. Renewing an existing certificate does not require changing the configuration of any other system components.  
  
  host specifies the address of the Management Server. If the parameter is not defined, the loopback address (localhost) is used.  
  
  Domain specifies the administrative Domain the Log Server belongs to if the system is divided in administrative Domains. If the Domain is not specified, the Shared Domain is used.  
  
  The Log Server needs to be shut down before running this command. Restart the server after running this command. |
| sgCertifyMgtSrv      | Creates a new certificate for the Management Server to allow secure communications between the Stonesoft system components. Renewing an existing certificate does not require changes on any other system components.  
  
  The Management Server needs to be shut down before running this command. Restart the server after running this command. |
| sgCertifyWebPortalSrv| Contacts the Management Server and creates a new certificate for the Web Portal Server to allow secure communications with other system components. Renewing an existing certificate does not require changing the configuration of any other system components.  
  
  host specifies the address of the Management Server. If the parameter is not defined, the loopback address (localhost) is used.  
  
  Domain specifies the administrative Domain the Web Portal Server belongs to if the system is divided in administrative Domains. If the Domain is not specified, the Shared Domain is used.  
  
  The Web Portal Server needs to be shut down before running this command. Restart the server after running this command. |
| sgChangeMgtIPOnAuthSrv<IP address> | Changes the Management Server’s IP address in the Authentication Server’s local configuration to the IP address you give as a parameter. Use this command if you change the Management Server’s IP address.  
  
  Restart the Authentication Server after running this command. |
### sgChangeMgtIPOnLogSrv <IP address>
Changes the Management Server's IP address in the Log Server's local configuration to the IP address you give as a parameter. Use this command if you change the Management Server's IP address. Restart the Log Server service after running this command.

### sgChangeMgtIPOnMgtSrv <IP address>
Changes the Management Server's IP address in the local configuration to the IP address you give as a parameter. Use this command if you change the Management Server's IP address. Restart the Management Server service after running this command.

### sgClient
Starts a locally installed Stonesoft Management Client.

### sgCreateAdmin
Creates an unrestricted (superuser) administrator account. The Management Server needs to be stopped before running this command.

### sgExport
Exports elements stored on the Management Server to an XML file. Enclose details in double quotes if they contain spaces. 
- **host** specifies the address of the Management Server. If the parameter is not defined, the loopback address (localhost) is used.
- **Domain** specifies the administrative Domain for this operation if the system is divided in administrative Domains. If the Domain is not specified, the Shared Domain is used.
- **login** defines the username for the account that is used for this operation. If this parameter is not defined, the username root is used.
- **pass** defines the password for the user account.
- **file** defines the name and location of the export ZIP file.
- **type** specifies which types of elements are included in the export file:
  - **all** for all exportable elements
  - **nw** for network elements
  - **ips** for IPS elements
  - **sv** for services
  - **rb** for security policies
  - **al** for alerts
  - **vpn** for VPN elements.
- **name** allows you to specify by name the element(s) that you want to export.
- **recursion** includes referenced elements in the export, for example, the network elements used in a policy that you export.
- **-system** includes any system elements that are referenced by the other elements in the export.
- **-h**, **-help**, or **-?** displays information on using the script.
sgHA

[host=<Management Server Address>]
[\{Domain\}]
[login=<login name>]
[pass=<password>]
[master=<management server>]
[-set-active]
[-set-standby]
[-sync]
[-fullsync]
[-check]
[-retry]
[-isolate]
[-force]
[-h|-help|-?]

Controls highly available (active and standby) Management Servers.

**host** specifies the address of the Management Server. If the parameter is not defined, the loopback address (localhost) is used.

**Domain** specifies the administrative Domain for this operation if the system is divided in administrative Domains. If the Domain is not specified, the Shared Domain is used.

**login** defines the username for the account that is used for this operation. If this parameter is not defined, the username root is used.

**pass** defines the password for the user account.

**master** defines the Management Server used as a master server for the operation.

-**set-active** activates and locks all domains.
-**set-standby** deactivates and unlocks all domains.

**sync** performs full database replication. This functions differently on a standby Management Server and an active Management Server. If you run it on an active Management Server, it replicates the active database to every standby Management Server that has the Include in Database Replication option selected in its properties. If you run it on a standby Management Server, it replicates the active database from the active Management Server only to this standby Management Server (regardless of whether the Include in Database Replication option is selected in the standby Management Server’s properties).

-**fullsync** performs full database replication with active server backup.

-**check** checks that the database is in sync with the active server.

-**retry** retries replication if this has been stopped due to a recoverable error.

-**isolate** isolates the management server from database replication. This is an initial requirement for synchronization.

-**force** enforces the operation even if all Management Servers are not in sync. Note that using this option may cause instability if used carelessly.

-**h**, **-help**, or **-?** displays information on using the script.
**sgImport**

[host=<Management Server Address>]
[\Domain>]
[login=<login name>]
[pass=<password>]
file=<file path and name>
[-replace_all]
[-h|-help|-?]

Imports Stonesoft Management Server database elements from a Stonesoft XML file. When importing, existing (non-default) elements are overwritten if both the name and type match.

- **host** specifies the address of the Management Server. If the parameter is not defined, the loopback address (localhost) is used.
- **Domain** specifies the administrative Domain for this operation if the system is divided in administrative Domains. If the Domain is not specified, the Shared Domain is used.
- **login** defines the username for the account that is used for this operation. If this parameter is not defined, the username root is used.
- **pass** defines the password for the user account.
- **file** defines the ZIP file whose contents you want to import.
- **-replace_all** ignores all conflicts by replacing all existing elements with new ones.
- **-h**, **-help**, or **-?** displays information on using the script.

**sgImportExportUser**

[host=<Management Server Address>]
[\Domain>]
[login=<login name>]
[pass=<password>]
action=<import|export>
file=<file path and name>
[-h|-help|-?]

Imports and exports a list of Users and User Groups in an LDIF file from/to a Stonesoft Management Server’s internal LDAP database. To import User Groups, all User Groups in the LDIF file must be directly under the stonesoft top-level group (dc=stonesoft).

- **The user information in the export file is stored as plaintext.** Handle the file securely.
- **host** specifies the address of the Management Server. If the parameter is not defined, the loopback address (localhost) is used.
- **Domain** specifies the administrative Domain for this operation if the system is divided in administrative Domains. If the Domain is not specified, the Shared Domain is used.
- **login** defines the username for the account that is used for this operation. If this parameter is not defined, the username root is used.
- **pass** defines the password for the user account.
- **action** defines whether users are imported or exported.
- **file** defines the file that is used for the operation.

**Example:**

```bash
sgImportExportUser login=admin
case=abc123 action=export
case=c:\temp\exportedusers.ldif
-h, -help, or -? displays information on using the script.
```
sgInfo

SG_ROOT_DIR FILENAME

[fast] [-nolog] [-client]
[-h|-help|-?]

Creates a ZIP file that contains copies of configuration files and
the system trace files. The resulting ZIP file is stored in the
logged in user's home directory. The file location is displayed on
the last line of screen output. Provide the generated file to
Stonesoft support for troubleshooting purposes.

SG_ROOT_DIR Stonesoft Management Center installation
directory.
FILENAME name of output file.
-nolog extended log server information is NOT collected.
-client collects traces only from the Management Client.
-h, -help, or -? displays information on using the script.

sgOnlineReplication

[login=<login name>]
[pass=<password>]
[active-server=<name of active server>]
[standby-server=<name of standby server>]
[standby-server-address=<IP address of standby server>]
[-nodisplay]
[-h|-help|-?]

Replicates the Management Server's database from the active
Management Server to the standby Management Server.

Note! Use this script only if the secondary Management Server's
configuration has been corrupted, the secondary Management
Server's certificate has expired, or in new SMC installations if
the automatic database replication between the Management
Servers has not succeeded. Otherwise, synchronize the
database through the Management Client (see Synchronizing
Management Databases Manually (page 375) or use the sgHA
command.

pass defines the password for the user account.
active-server option specifies the IP address of the active
Management Server from which the Management database is
replicated.
standby-server option specifies the name of the standby
Management Server to which the Management database is
replicated.
standby-server-address option specifies the IP address
of the standby Management Server to which the Management
database is replicated.
-nodisplay sets a text only console.
-h, -help, or -? displays information on using the script.
The return values are:
0 OK
8 sgOnlineReplication.sh failed to initialize properly
9 login failed
11 unknown error
12 bad command line arguments
13 replication canceled by user.

sgReinitializeLogServer

Note! This script is located in <installation directory>/
bin/install.

Creates a new Log Server configuration if the configuration file
has been lost.

Table A.1 Management Center Command Line Tools (Continued)
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sgRestoreArchive</td>
<td>Restores logs from archive files to the Log Server. This command is available only on the Log Server. ARCHIVE_DIR is the number of the archive directory (0 – 31) from where the logs will be restored. By default, only archive directory 0 is defined. The archive directories can be defined in the &lt;installation directory&gt;/data/LogServerConfiguration.txt file: ARCHIVE_DIR_xx=PATH.</td>
</tr>
<tr>
<td>sgRestoreAuthBackup</td>
<td>Restores the Authentication Server user information from a backup file in the &lt;installation directory&gt;/backups/directory. Apply the Authentication Server’s configuration after this command. -pwd defines a password for encrypted backup. -backup defines a name for the backup file. -nodiskcheck ignores free disk check before backup restoration. -h or -help displays information on using the script.</td>
</tr>
<tr>
<td>sgRestoreLogBackup</td>
<td>Restores the Log Server (logs and/or configuration files) from a backup file in the &lt;installation directory&gt;/backups/directory. Apply the Authentication Server’s configuration after this command. -pwd defines a password for encrypted backup. -backup defines a name for the backup file. -nodiskcheck ignores free disk check before backup restoration. -overwrite-syslog-template overwrites a syslog template file if found in the backup. -h or -help displays information on using the script.</td>
</tr>
<tr>
<td>sgRestoreMgtBackup</td>
<td>Restores the Management Server (database and/or configuration files) from a backup file in the &lt;installation directory&gt;/backups/directory. -pwd defines a password for encrypted backup. -backup defines a name for the backup file. -nodiskcheck ignores free disk check before backup restoration. -h or -help displays information on using the script.</td>
</tr>
<tr>
<td>sgRevert</td>
<td>Note! This script is located in &lt;installation directory&gt;/bin/uninstall. Reverts to the previous installation saved during the upgrade process. The previous installation can be restored at any time, even after a successful upgrade.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>sgShowFingerPrint</td>
<td>Displays the CA certificate’s fingerprint on the Management Server.</td>
</tr>
<tr>
<td>sgStartAuthSrv</td>
<td>Starts the Authentication Server.</td>
</tr>
<tr>
<td>sgStartLogSrv</td>
<td>Starts the Log Server and its database.</td>
</tr>
<tr>
<td>sgStartMgtDatabase</td>
<td>Starts the Management Server's database. There is usually no need to use this script.</td>
</tr>
<tr>
<td>sgStartMgtSrv</td>
<td>Starts the Management Server and its database.</td>
</tr>
<tr>
<td>sgStartWebPortalSrv</td>
<td>Starts the Web Portal Server.</td>
</tr>
<tr>
<td>sgStopLogSrv</td>
<td>Stops the Log Server.</td>
</tr>
<tr>
<td>sgStopMgtSrv</td>
<td>Stops the Management Server and its database.</td>
</tr>
<tr>
<td>sgStopMgtDatabase</td>
<td>Stops the Management Server's database. There is usually no need to use this script.</td>
</tr>
<tr>
<td>sgStopWebPortalSrv</td>
<td>Stops the Web Portal Server.</td>
</tr>
<tr>
<td>sgStopRemoteMgtSrv</td>
<td>Stops the Management Server service when run without arguments. To stop a remote Management Server service, provide the arguments to connect to the Management Server. host is the Management Server’s host name if not localhost. login is a Stonesoft administrator account for the login. pass is the password for the administrator account. -h, -help, or -? displays information on using the script.</td>
</tr>
</tbody>
</table>
Appendix A  Command Line Tools

Engine Commands

The commands in the following two tables can be run on the command line on Firewall, Layer 2 Firewall, and/or IPS engines.
### Table A.2 Stonesoftware Engine Command Line Tools

<table>
<thead>
<tr>
<th>Command</th>
<th>Engine Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>sg-blacklist</code></td>
<td></td>
<td>Can be used to view, add, or delete active blacklist entries. The blacklist is applied as defined in Access Rules.</td>
</tr>
<tr>
<td><code>show</code> [-v][-f FILENAME]</td>
<td></td>
<td>Displays the current active blacklist entries in format: engine node ID</td>
</tr>
<tr>
<td><code>add</code> [-i FILENAME]</td>
<td></td>
<td>Creates a new blacklist entry. Enter the parameters (see below) or use the <code>-i</code> option to import parameters from a file.</td>
</tr>
<tr>
<td><code>del</code> [-i FILENAME]</td>
<td></td>
<td>Deletes the first matching blacklist entry. Enter the parameters (see below) or use the <code>-i</code> option to import parameters from a file.</td>
</tr>
<tr>
<td><code>iddel</code> NODE_ID ID</td>
<td></td>
<td>Removes one specific blacklist entry on one specific engine. <code>NODE_ID</code> is the engine's ID, <code>ID</code> is the blacklist entry's ID (as shown by the <code>show</code> command).</td>
</tr>
<tr>
<td><code>flush</code></td>
<td></td>
<td>Deletes all blacklist entries.</td>
</tr>
</tbody>
</table>

### Add/Del Parameters:

- **src IP_ADDRESS/MASK** defines the source IP address and netmask to match. Matches any IP address by default.
- **src6 IPv6_ADDRESS/PREFIX** defines the source IPv6 and prefix length to match. Matches any IPv6 address by default.
- **dst IP_ADDRESS/MASK** defines the destination IP address and netmask to match. Matches any IP address by default.
- **dst6 IPv6_ADDRESS/PREFIX** defines the destination IPv6 address and prefix length to match. Matches any IPv6 address by default.
- **proto {tcp|udp|icmp|NUM}** defines the protocol to match by name or protocol number. Matches all IP traffic by default.
- **srcport PORT[-PORT]** defines the TCP/UDP source port or range to match. Matches any port by default.
- **dstport PORT[-PORT]** defines the TCP/UDP destination port or range to match. Matches any port by default.
- **duration NUM** defines in seconds how long the entry is kept. Default is 0, which cuts current connections, but is not kept.

### Examples:

- `sg-blacklist add src 192.168.0.2/32 proto tcp dstport 80 duration 60`
- `sg-blacklist add -i myblacklist.txt`
- `sg-blacklist del dst 192.168.1.0/24 proto 47`
### Table A.2  Stonesoft Engine Command Line Tools (Continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Engine Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sg-bootconfig</td>
<td></td>
<td>Can be used to edit boot command parameters for future bootups.</td>
</tr>
<tr>
<td>[--primary-console=tty0</td>
<td>ttyS PORT,SPEED]</td>
<td>[--primary-console=tty0</td>
</tr>
<tr>
<td>[--secondary-console=</td>
<td></td>
<td>[--secondary-console=[tty0</td>
</tr>
<tr>
<td>--flavor=up</td>
<td>smp]</td>
<td>[--flavor=up</td>
</tr>
<tr>
<td>[--initrd=yes</td>
<td>no]</td>
<td>[--initrd=yes</td>
</tr>
<tr>
<td>[--crashdump=yes</td>
<td>no</td>
<td>Y@X]</td>
</tr>
<tr>
<td>[--append=kernel options]</td>
<td>[--append=kernel options] parameter defines any other boot options to add to the configuration.</td>
<td></td>
</tr>
<tr>
<td>apply</td>
<td></td>
<td>apply command applies the specified configuration options.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note! Use this only if you want to clear all configuration information from the engine.</strong></td>
</tr>
<tr>
<td>sg-clear-all</td>
<td></td>
<td>This command resets all configuration information from the engine. It does not remove the engine software. After using this command, you must reconfigure the engine using the sg-reconfigure command.</td>
</tr>
<tr>
<td>sg-cluster</td>
<td></td>
<td>Used to display or change the status of the node.</td>
</tr>
<tr>
<td>[status [-c SECONDS]]</td>
<td></td>
<td>status [-c SECONDS] command displays cluster status. When -c SECONDS is used, status is shown continuously with the specified number of seconds between updates.</td>
</tr>
<tr>
<td>[online]</td>
<td></td>
<td>online command sends the node online.</td>
</tr>
<tr>
<td>[lock-online]</td>
<td></td>
<td>lock-online command sends the node online and keeps it online even if another process tries to change its state.</td>
</tr>
<tr>
<td>[offline]</td>
<td></td>
<td>offline command sends the node offline.</td>
</tr>
<tr>
<td>[lock-offline]</td>
<td></td>
<td>lock-offline command sends the node offline and keeps it offline even if another process tries to change its state.</td>
</tr>
<tr>
<td>[standby]</td>
<td></td>
<td>standby command sets an active node to standby.</td>
</tr>
<tr>
<td>[safe-offline]</td>
<td></td>
<td>safe-offline command sets the node to offline only if there is another online node.</td>
</tr>
<tr>
<td>sg-contact-mgmt</td>
<td></td>
<td>Used for establishing a trust relationship with the Management Server as part of engine installation or reconfiguration (see sg-reconfigure below). The engine contacts the Management Server using the one-time password created when the engine’s initial configuration is saved.</td>
</tr>
<tr>
<td>Command</td>
<td>Engine Role</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>sg-dynamic-routing</td>
<td>Firewall</td>
<td><em>start</em> starts the Quagga routing suite. <em>stop</em> stops the Quagga routing suite and flushes all routes made by zebra. <em>restart</em> restarts the Quagga routing suite. <em>force-reload</em> forces reload of the saved configuration. <em>backup &lt;file&gt;</em> backs up the current configuration to a compressed file. <em>restore &lt;file&gt;</em> restores the configuration from the specified file. <em>sample-config</em> creates a basic configuration for Quagga. <em>route-table</em> prints the current routing table. <em>info</em> displays the help information for the sg-dynamic-routing command, and detailed information about Quagga suite configuration with vtysh.</td>
</tr>
<tr>
<td>sg-ipsec -d</td>
<td>Firewall</td>
<td>Deletes VPN-related information (use vpninfo command to view the information). Option -d (for delete) is mandatory. -u deletes the VPN session of the named VPN client user. You can enter the user account in the form <a href="mailto:username@domain">username@domain</a> if there are several user storage locations (LDAP domains). -si deletes the VPN session of a VPN client user based on session identifier. -ck deletes the IKE SA (Phase one security association) based on IKE cookie. -tri deletes the IPSEC SAs (Phase two security associations) for both communication directions based on transform identifier. -ri deletes all SAs related to a remote IP address in gateway-to-gateway VPNs. -ci deletes all SAs related to a connection identifier in gateway-to-gateway VPNs.</td>
</tr>
<tr>
<td>sg-logger</td>
<td>Firewall, Layer 2, Layer 3, IPS</td>
<td>Can be used in scripts to create log messages with the specified properties. -f <em>FACILITY_NUMBER</em> parameter defines the facility for the log message. -t <em>TYPE_NUMBER</em> parameter defines the type for the log message. -e <em>EVENT_NUMBER</em> parameter defines the log event for the log message. The default is 0 (H2A_LOG_EVENT_UNDEFINED). -i &quot;INFO_STRING&quot; parameter defines the information string for the log message. -s parameter dumps information on option numbers to stdout -h parameter displays usage information.</td>
</tr>
</tbody>
</table>
Table A.2  Stonesoft Engine Command Line Tools (Continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Engine Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>sg-raid</strong></td>
<td>Firewall,</td>
<td>Configures a new hard drive. This command is only for Stonesoft appliances that support RAID (Redundant Array of Independent Disks) and have two hard drives.</td>
</tr>
<tr>
<td>[-status] [-add]</td>
<td>Layer 2</td>
<td>- <strong>status</strong> option displays the status of the hard drive.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use <strong>add -force</strong> if you want to add a hard drive that already contains data and you want to overwrite it.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>re-add</strong> adds a hard drive that is already partitioned. This command prompts for the drive and partition for each degraded array.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use <strong>re-add -force</strong> if you want to check all the arrays.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>-help</strong> option displays usage information.</td>
</tr>
<tr>
<td><strong>sg-reconfigure</strong></td>
<td>Firewall,</td>
<td>Used for reconfiguring the node manually.</td>
</tr>
<tr>
<td>[---boot]</td>
<td>Layer 2</td>
<td><strong>--boot</strong> option applies bootup behavior. Do not use this option unless you have a specific need to do so.</td>
</tr>
<tr>
<td>[---maybe-contact]</td>
<td>IPS</td>
<td><strong>--maybe-contact</strong> option contacts the Management Server if requested. This option is only available on firewall engines.</td>
</tr>
<tr>
<td>[---no-shutdown]</td>
<td></td>
<td><strong>--no-shutdown</strong> option allows you to make limited configuration changes on the node without shutting it down. Some changes may not be applied until the node is rebooted.</td>
</tr>
<tr>
<td><strong>sg-selftest</strong></td>
<td>Firewall</td>
<td>Runs cryptography tests on the engine.</td>
</tr>
<tr>
<td>[-d] [-h]</td>
<td></td>
<td><strong>-d</strong> option runs the tests in debug mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>-h</strong> option displays usage information.</td>
</tr>
<tr>
<td><strong>sg-status</strong></td>
<td>Firewall,</td>
<td>Displays information on the engine’s status.</td>
</tr>
<tr>
<td>[-l] [-h]</td>
<td>Layer 2</td>
<td><strong>-l</strong> option displays all available information on engine status.</td>
</tr>
<tr>
<td></td>
<td>IPS</td>
<td><strong>-h</strong> option displays usage information.</td>
</tr>
</tbody>
</table>
### Table A.2 Stonesoft Engine Command Line Tools (Continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Engine Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>sg-toggle-active</strong></td>
<td>Firewall, Layer 2 Firewall, IPS</td>
<td>Switches the engine between the active and the inactive partition. This change takes effect when you reboot the engine. You can use this command, for example, if you have upgraded an engine and want to switch back to the earlier engine version. When you upgrade the engine, the active partition is switched. The earlier configuration remains on the inactive partition. To see the currently active (and inactive) partition, see the directory listing of <code>/var/run/stonegate</code> (<code>ls -l /var/run/stonegate</code>). The <code>SHA1 SIZE</code> option is used to verify the signature of the inactive partition before changing it to active. If you downgrade the engine, check the checksum and the size of the earlier upgrade package by extracting the signature and size files from the <code>sg_engine_[version.build]_i386.zip</code> file. The <code>--debug</code> option reboots the engine with the debug kernel. The <code>--force</code> option switches the active configuration without first verifying the signature of the inactive partition.</td>
</tr>
<tr>
<td><strong>sg-upgrade</strong></td>
<td>Firewall</td>
<td>Upgrades the node by rebooting from the installation CD-ROM. Alternatively, the node can be upgraded remotely using the Management Client.</td>
</tr>
<tr>
<td><strong>sg-version</strong></td>
<td>Firewall, Layer 2 Firewall, IPS</td>
<td>Displays the software version and build number for the node.</td>
</tr>
<tr>
<td><strong>sginfo</strong></td>
<td>Firewall, Layer 2 Firewall, IPS</td>
<td>Gathers system information you can send to Stonesoft support if you are having problems. Use this command only when instructed to do so by Stonesoft support. The <code>--f</code> option forces sginfo even if the configuration is encrypted. The <code>--d</code> option includes core dumps in the sginfo file. The <code>--s</code> option includes slapcat output in the sginfo file. The <code>--p</code> option includes passwords in the sginfo file (by default passwords are erased from the output). The <code>--</code> option creates the sginfo file without displaying the progress. The <code>--help</code> option displays usage information.</td>
</tr>
</tbody>
</table>
The table below lists some general Linux operating system commands that may be useful in running your engines. Some commands can be stopped by pressing Ctrl+c.

### Table A.3 General Command Line Tools on Engines

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dmesg</td>
<td>Shows system logs and other information. Use the -h option to see usage.</td>
</tr>
<tr>
<td>halt</td>
<td>Shuts down the system.</td>
</tr>
<tr>
<td>ip</td>
<td>Displays IP address information. Type the command without options to see usage. <strong>Example:</strong> type <code>ip addr</code> for basic information on all interfaces.</td>
</tr>
<tr>
<td>ping</td>
<td>Tests connectivity with ICMP echo requests. Type the command without options to see usage.</td>
</tr>
<tr>
<td>ps</td>
<td>Reports the status of running processes.</td>
</tr>
<tr>
<td>reboot</td>
<td>Reboots the system.</td>
</tr>
<tr>
<td>scp</td>
<td>Secure copy. Type the command without options to see usage.</td>
</tr>
<tr>
<td>sftp</td>
<td>Secure FTP. Type the command without options to see usage.</td>
</tr>
<tr>
<td>ssh</td>
<td>SSH client (for opening a terminal connection to other hosts). Type the command without options to see usage.</td>
</tr>
<tr>
<td>tcpdump</td>
<td>Gives information on network traffic. Use the -h option to see usage. You can also analyze network traffic by creating tcpdump files from the Stonesoft Management Client GUI with the Traffic Capture feature. See <em>Taking a Traffic Capture</em> (page 141).</td>
</tr>
<tr>
<td>top</td>
<td>Displays the top CPU processes taking most processor time. Use the -h option to see usage.</td>
</tr>
<tr>
<td>traceroute</td>
<td>Traces the route packets take to the specified destination. Type the command without options to see usage.</td>
</tr>
<tr>
<td>vpninfo</td>
<td>Displays VPN information and allows you to issue some basic commands. Type the command without options to see usage.</td>
</tr>
</tbody>
</table>
**Server Pool Monitoring Agent Commands**

You can test and monitor the Server Pool Monitoring Agents on the command line with the commands described in the table below.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>agent</strong></td>
<td><code>(Windows only) Allows you to test different configurations before activating them.</code></td>
</tr>
<tr>
<td><code>-v level</code></td>
<td><code>-v level</code> Set the verbosity level. The default level is 5. Levels 6-8 are for debugging where available.</td>
</tr>
<tr>
<td><code>-c path</code></td>
<td><code>-c path</code> Use the specified path as the first search directory for the configuration.</td>
</tr>
<tr>
<td><code>[test [files]]</code></td>
<td>Run in the test mode - status queries do not receive a response. If you specify the files, they are used for reading the configuration instead of the default files. The output is directed to syslog or eventlog instead of the console where the command was run unless you use the <code>-d</code> option.</td>
</tr>
<tr>
<td><code>[syntax [files]]</code></td>
<td>Check the syntax in the configuration file. If no files are specified, the default configuration files are checked.</td>
</tr>
<tr>
<td><strong>sgagentd</strong></td>
<td><code>(Linux only) Allows you to test different configurations before activating them.</code></td>
</tr>
<tr>
<td><code>-d</code></td>
<td><code>-d</code> Don’t Fork as a daemon. All log messages are printed to stdout or stderr only.</td>
</tr>
<tr>
<td><code>-v level</code></td>
<td><code>-v level</code> Set the verbosity level. The default level is 5. Levels 6-8 are for debugging where available.</td>
</tr>
<tr>
<td><code>-c path</code></td>
<td><code>-c path</code> Use the specified path as the first search directory for the configuration.</td>
</tr>
<tr>
<td><code>[test [files]]</code></td>
<td>Run in the test mode - status queries do not receive a response. If you specify the files, they are used for reading the configuration instead of the default files. The output is directed to syslog or eventlog instead of the console where the command was run unless you use the <code>-d</code> option.</td>
</tr>
<tr>
<td><code>[syntax [files]]</code></td>
<td>Check the syntax in the configuration file. If no files are specified, the default configuration files are checked. The output is directed to syslog or eventlog instead of the console where the command was run unless you use the <code>-d</code> option.</td>
</tr>
</tbody>
</table>
### sgmon

**Command**: `sgmon`  
**Parameters**:
- `[status|info|proto] [-p port] [-t timeout] [-a id] host`  

Sends a UDP query to the specified host and waits for a response until received, or until the timeout limit is reached. The request type can be defined as a parameter. If no parameter is given, `status` is requested. The commands are:
- `status` - query the status.
- `info` - query the agent version.
- `proto` - query the highest supported protocol version.
- `-p port` Connect to the specified port instead of the default port.
- `-t timeout` Set the timeout (in seconds) to wait for a response.
- `-a id` Acknowledge the received log messages up to the specified id. Each response message has an id, and you may acknowledge more than one message at a given time by using the id parameter. Note that messages acknowledged by sgmon will no longer appear in the firewall logs.
- `host` The IP address of the host to connect to. To get the status locally, you may give `localhost` as the host argument. This parameter is mandatory.

**Return value**:
- 0 if the response was received
- 1 if the query timed out
- -1 in case of an error

---

**Table A.4 Server Pool Monitoring Agent Commands (Continued)**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| `sgmon` [status|info|proto] [-p port] [-t timeout] [-a id] host | Sends a UDP query to the specified host and waits for a response until received, or until the timeout limit is reached. The request type can be defined as a parameter. If no parameter is given, `status` is requested. The commands are: `status` - query the status. `info` - query the agent version. `proto` - query the highest supported protocol version. `-p port` Connect to the specified port instead of the default port. `-t timeout` Set the timeout (in seconds) to wait for a response. `-a id` Acknowledge the received log messages up to the specified id. Each response message has an id, and you may acknowledge more than one message at a given time by using the id parameter. Note that messages acknowledged by sgmon will no longer appear in the firewall logs. `host` The IP address of the host to connect to. To get the status locally, you may give `localhost` as the host argument. This parameter is mandatory. **Return value**:  
  - 0 if the response was received  
  - 1 if the query timed out  
  - -1 in case of an error |
APPENDIX B

DEFAULT COMMUNICATION PORTS

This chapter lists the default ports used in connections between Stonesoft components and the default ports Stonesoft components use with external components.

The following sections are included:

- Management Center Ports (page 150)
- Security Engine Ports (page 153)
The illustrations below present an overview to the most important default ports used in communications between the Stonesoft Management Center (SMC) components and from the SMC to external services. See the table below for a complete list of default ports.

**Illustration B.1  Destination Ports for Basic Communications Within SMC**

**TCP:**
- 8914-8918 (Log Server Management Server)
- 8902-8913, 3021 (Log Server Certificate Request)
- 3023 (Management Client)

**TCP:**
- 3020, 8916, 8917

**UDP:**
- 161 (Monitored Third Party Components)
- 1812 (Additional Management Server)

**TCP:**
- 3020

**TCP:**
- 389

**UDP:**
- 162/5162, 514/5514 (Win/Linux)

**TCP:**
- 8925, 8929

**TCP:**
- 8902-8913, 8916, 8917, 3023+ (Certificate Request)

**TCP:**
- 8907 + 3021 (Certificate Request)

**TCP:**
- 8902-8913, 3021 (Certificate Request)

**TCP:**
- 443

**UDP:**
- 162/5162, 514/5514 (Win/Linux)

**TCP:**
- 8903, 8907

**TCP:**
- 8903, 389

**TCP:**
- 8907 + 3021 (Certificate Request)

**TCP:**
- 8925, 8929

**TCP:**
- 8902-8913, 3021 (Certificate Request)

**TCP:**
- 389

**TCP:**
- 8903, 8907
The table below lists all default ports SMC uses internally and with external components. Many of these ports can be changed. The name of corresponding default Service elements are also included for your reference. For information on communications between SMC components and the engines, see the separate listings.

Table B.1 Management Center Default Ports

<table>
<thead>
<tr>
<th>Listening Host</th>
<th>Port/Protocol</th>
<th>Contacting Hosts</th>
<th>Service Description</th>
<th>Service Element Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Additional Management Servers</td>
<td>8902-8913/TCP</td>
<td>Management Server</td>
<td>Database replication (push) to the additional Management Server.</td>
<td>SG Control</td>
</tr>
<tr>
<td>Authentication Server</td>
<td>8925-8929/TCP</td>
<td>Management Server</td>
<td>Stonesoft Management Server commands to Authentication Server.</td>
<td>SG Authentication Commands</td>
</tr>
<tr>
<td>Authentication Server node</td>
<td>8988-8989/TCP</td>
<td>Authentication Server node</td>
<td>Data synchronization between Authentication Server nodes.</td>
<td>SG Authentication Sync</td>
</tr>
<tr>
<td>DNS server</td>
<td>53/UDP, 53/TCP</td>
<td>Management Client, Management Server, Log Server</td>
<td>DNS queries.</td>
<td>DNS (UDP)</td>
</tr>
<tr>
<td>LDAP server</td>
<td>389/TCP</td>
<td>Management Server</td>
<td>External LDAP queries for display/editing in the Management Client.</td>
<td>LDAP (TCP)</td>
</tr>
<tr>
<td>Log Server</td>
<td>162/UDP, 5162/UDP</td>
<td>Monitored third party components</td>
<td>SNMPv1 trap reception from third party components. Port 162 is used if installed on Windows, port 5162 if installed on Linux.</td>
<td>SNMP (UDP)</td>
</tr>
<tr>
<td>Log Server</td>
<td>514/TCP, 514/UDP, 5514/TCP, 5514/UDP</td>
<td>Monitored third party components</td>
<td>Syslog reception from third party components. Port 514 is used if installed on Windows, port 5514 if installed on Linux.</td>
<td>Syslog (UDP) [Partial match]</td>
</tr>
<tr>
<td>Log Server</td>
<td>8914-8918/TCP</td>
<td>Management Client</td>
<td>Log browsing.</td>
<td>SG Data Browsing</td>
</tr>
<tr>
<td>Log Server</td>
<td>8916-8917/TCP</td>
<td>Web Portal Server</td>
<td>Log browsing.</td>
<td>SG Data Browsing (Web Portal Server)</td>
</tr>
<tr>
<td>Management Server</td>
<td>3021/TCP</td>
<td>Log Server, Web Portal Server</td>
<td>System communications certificate request/renewal.</td>
<td>SG Log Initial Contact</td>
</tr>
<tr>
<td>Listening Host</td>
<td>Port/Protocol</td>
<td>Contacting Hosts</td>
<td>Service Description</td>
<td>Service Element Name</td>
</tr>
<tr>
<td>----------------</td>
<td>---------------</td>
<td>------------------</td>
<td>--------------------------------------------------------------------------------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>Management Server</td>
<td>8902-8913/TCP</td>
<td>Management Client, Log Server, Web Portal Server</td>
<td>Monitoring and control connections.</td>
<td>SG Control</td>
</tr>
<tr>
<td>Management Server</td>
<td>8903, 8907/TCP</td>
<td>Additional Management Servers</td>
<td>Database replication (pull) to the additional Management Server.</td>
<td>SG Control</td>
</tr>
<tr>
<td>Management Server</td>
<td>8907/TCP</td>
<td>Authentication Server</td>
<td>Status monitoring.</td>
<td>SG Control</td>
</tr>
<tr>
<td>Monitored Third Party Components</td>
<td>161/UDP</td>
<td>Log Server</td>
<td>SNMP status probing to external IP addresses.</td>
<td>SNMP (UDP)</td>
</tr>
<tr>
<td>RADIUS server</td>
<td>1812/UDP</td>
<td>Management Server</td>
<td>RADIUS authentication requests for administrator logins. The default ports can be modified in the properties of the RADIUS Server element.</td>
<td>RADIUS (Authentication)</td>
</tr>
<tr>
<td>Stonesoft servers</td>
<td>443/TCP</td>
<td>Management Server</td>
<td>Update packages, engine upgrades, and licenses from update.stonesoft.com and smc.stonesoft.com.</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Syslog Server</td>
<td>514/UDP, 5514/UDP</td>
<td>Log Server</td>
<td>Log data export to syslog servers. The default ports can be modified in the LogServerConfiguration.txt file.</td>
<td>Syslog (UDP) Partial match</td>
</tr>
</tbody>
</table>
Security Engine Ports

The illustrations below present an overview to the most important default ports used in communications between Security Engines and the SMC and between clustered Security Engine nodes. See the table below for a complete list of default ports for the engines.

Illustration B.3  Destination Ports for Basic Security Engine Communications

Log Server

TCP: 3020

Management Server

TCP: 3021
3023
8906*

TCP: 3020

Security Engine

TCP: 636
4950
4987
8888
Or none*

Other Node(s) in the Cluster

TCP: 3002
3003
3010
UDP: 3000
3001
Multicast (Heartbeat interfaces)

* Single engines with “Node-initiated Contact to Management Server” selected.

Illustration B.4  Default Destination Ports for Security Engine Service Communications

DNS Server

TCP, UDP: 53

LDAP Server*

TCP: 389
636

User Agent*

TCP: 16661

RADIUS Server*

UDP: 1812
1645

Server Pool*

UDP: 7777

DHCP Server*

UDP: 67

VPN Clients*

UDP: 68

UDP: 500
4500

TCP, UDP: 111

RPC Server*

TCP: 49

UDP: 161

UDP: 500
2746
4500

UDP: 162

UDP: 500
2746
4500

* Engines in the Firewall/VPN role only.
The table below lists all default ports the Security Engines use internally and with external components. Many of these ports can be changed. The name of corresponding default Service elements are also included for your reference.

<table>
<thead>
<tr>
<th>Listening Host</th>
<th>Port/Protocol</th>
<th>Contacting Hosts</th>
<th>Service Description</th>
<th>Service Element Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anti-virus signature server</td>
<td>80/TCP</td>
<td>Firewall</td>
<td>Anti-virus signature update service.</td>
<td>HTTP</td>
</tr>
<tr>
<td>Authentication Server</td>
<td>8925-8929/TCP</td>
<td>Firewall</td>
<td>User directory and authentication services.</td>
<td>LDAP (TCP), RADIUS (Authentication)</td>
</tr>
<tr>
<td>BrightCloud Server</td>
<td>2316/TCP</td>
<td>Firewall, Layer 2 Firewall, IPS</td>
<td>BrightCloud web filtering update service.</td>
<td>BrightCloud update</td>
</tr>
<tr>
<td>DHCP server</td>
<td>67/UDP</td>
<td>Firewall</td>
<td>Relayed DHCP requests and requests from a firewall that uses dynamic IP address.</td>
<td>BOOTS (UDP)</td>
</tr>
<tr>
<td>DNS server</td>
<td>53/UDP, 53/TCP</td>
<td>Firewall</td>
<td>Dynamic DNS updates.</td>
<td>DNS (TCP)</td>
</tr>
<tr>
<td>Firewall</td>
<td>67/UDP</td>
<td>Any</td>
<td>DHCP relay on firewall engine.</td>
<td>BOOTS (UDP)</td>
</tr>
<tr>
<td>Firewall</td>
<td>68/UDP</td>
<td>DHCP server</td>
<td>Replies to DHCP requests.</td>
<td>BOOTPC (UDP)</td>
</tr>
<tr>
<td>Firewall</td>
<td>500/UDP</td>
<td>VPN clients, VPN gateways</td>
<td>VPN negotiations, VPN traffic.</td>
<td>ISAKMP (UDP)</td>
</tr>
<tr>
<td>Firewall</td>
<td>636/TCP</td>
<td>Management Server</td>
<td>Internal user database replication.</td>
<td>LDAPS (TCP)</td>
</tr>
<tr>
<td>Firewall</td>
<td>2543/TCP</td>
<td>Any</td>
<td>User authentication (Telnet) for Access rules.</td>
<td>SG User Authentication</td>
</tr>
<tr>
<td>Firewall</td>
<td>2746/UDP</td>
<td>Stonesoft VPN gateways</td>
<td>UDP encapsulated VPN traffic.</td>
<td>SG UDP Encapsulation</td>
</tr>
<tr>
<td>Firewall</td>
<td>4500/UDP</td>
<td>VPN client, VPN gateways</td>
<td>VPN traffic using NAT-traversal.</td>
<td>NAT-T</td>
</tr>
<tr>
<td>Firewall Cluster Node</td>
<td>3000-3001/UDP</td>
<td>Firewall Cluster Node</td>
<td>Heartbeat and state synchronization between clustered Firewalls.</td>
<td>SG State Sync (Multicast), SG State Sync (Unicast), SG Data Sync</td>
</tr>
<tr>
<td>Firewall, Layer 2 Firewall, IPS</td>
<td>4950/UDP</td>
<td>Management Server</td>
<td>Remote upgrade.</td>
<td>SG Remote Upgrade</td>
</tr>
<tr>
<td>Firewall, Layer 2 Firewall, IPS</td>
<td>4987/UDP</td>
<td>Management Server</td>
<td>Management Server commands and policy upload.</td>
<td>SG Commands</td>
</tr>
<tr>
<td>Listening Host</td>
<td>Port/Protocol</td>
<td>Contacting Hosts</td>
<td>Service Description</td>
<td>Service Element Name</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>---------------</td>
<td>---------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>-------------------------------------------</td>
</tr>
<tr>
<td>Firewall, Layer 2</td>
<td>8888/TCP</td>
<td>Management Server</td>
<td>Connection monitoring for old engine versions (5.1 and earlier).</td>
<td>SG Legacy Monitoring</td>
</tr>
<tr>
<td>Firewall, Layer 2</td>
<td>15000/TCP</td>
<td>Management Server, Log</td>
<td>Blacklist entries.</td>
<td>SG Blacklisting</td>
</tr>
<tr>
<td>Firewall, Layer 2</td>
<td>161/UDP</td>
<td>SNMP server</td>
<td>SNMP monitoring.</td>
<td>SNMP (UDP)</td>
</tr>
<tr>
<td>IPS Cluster Node</td>
<td>3000-3001/UDP</td>
<td>IPS Cluster Node</td>
<td>Heartbeat and state synchronization between clustered IPS engines.</td>
<td>SG State Sync (Multicast), SG State Sync (Unicast), SG Data Sync</td>
</tr>
<tr>
<td>Layer 2 Firewall Cluster Node</td>
<td>3000-3001/UDP</td>
<td>Layer 2 Firewall Cluster Node</td>
<td>Heartbeat and state synchronization between clustered Layer 2 Firewalls.</td>
<td>SG State Sync (Multicast), SG State Sync (Unicast), SG Data Sync</td>
</tr>
<tr>
<td>Log Server</td>
<td>3020/TCP</td>
<td>Firewall, Layer 2 Firewall, IPS</td>
<td>Log and alert messages; monitoring of blacklists, connections, status, and statistics.</td>
<td>SG Log</td>
</tr>
<tr>
<td>Management Server</td>
<td>3021/TCP</td>
<td>Firewall, Layer 2 Firewall, IPS</td>
<td>System communications certificate request/renewal (initial contact).</td>
<td>SG Initial Contact</td>
</tr>
<tr>
<td>Management Server</td>
<td>3023/TCP</td>
<td>Firewall, Layer 2 Firewall, IPS</td>
<td>Monitoring (status) connection.</td>
<td>SG Status Monitoring</td>
</tr>
<tr>
<td>Management Server</td>
<td>8906/TCP</td>
<td>Firewall, Layer 2 Firewall, IPS</td>
<td>Management connection for single engines with &quot;Node-Initiated Contact to Management Server&quot; selected.</td>
<td>SG Dynamic Control</td>
</tr>
<tr>
<td>RADIUS server</td>
<td>1812, 1645/UDP</td>
<td>Firewall</td>
<td>RADIUS authentication requests.</td>
<td>RADIUS (Authentication), RADIUS (Old)</td>
</tr>
<tr>
<td>RPC server</td>
<td>111/UDP, 111/TCP</td>
<td>Firewall</td>
<td>RPC number resolve.</td>
<td>SUNRPC (UDP), Sun RPC (TCP)</td>
</tr>
<tr>
<td>Server Pool Monitoring Agents</td>
<td>7777/UDP</td>
<td>Firewall</td>
<td>Polls to the servers’ Server Pool Monitoring Agents for availability and load information.</td>
<td>SG Server Pool Monitoring</td>
</tr>
<tr>
<td>Listening Host</td>
<td>Port/Protocol</td>
<td>Contacting Hosts</td>
<td>Service Description</td>
<td>Service Element Name</td>
</tr>
<tr>
<td>----------------</td>
<td>--------------</td>
<td>------------------</td>
<td>---------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>SNMP server</td>
<td>162/UDP</td>
<td>Firewall, Layer 2 Firewall, IPS</td>
<td>SNMP traps from the engine.</td>
<td>SNMP Trap (UDP)</td>
</tr>
<tr>
<td>TACACS+ server</td>
<td>49/TCP</td>
<td>Firewall</td>
<td>TACACS+ authentication requests.</td>
<td>TACACS (TCP)</td>
</tr>
<tr>
<td>User Agent</td>
<td>16661/TCP</td>
<td>Firewall</td>
<td>Queries for matching Users and User Groups with IP addresses.</td>
<td>SG Engine to User Agent</td>
</tr>
<tr>
<td>VPN gateways</td>
<td>500/UDP, 2746/UDP (Stonesoft gateways only), or 4500 UDP</td>
<td>Firewall</td>
<td>VPN traffic. Ports 2746 and 4500 may be used depending on encapsulation options.</td>
<td>ISAKMP (UDP)</td>
</tr>
</tbody>
</table>
APPENDIX C

EXAMPLE NETWORK SCENARIO

To give you a better understanding of how Stonesoft Firewall fits into a network, this section outlines a network with two firewalls: a single firewall at a branch office and a firewall cluster at headquarters.

The following sections are included:

- Overview of the Example Network (page 158)
- Example Firewall Cluster (page 159)
- Example Management Center (page 160)
- Example Single Firewall (page 160)
Overview of the Example Network

The illustration below shows you an example network. In the example network scenario, *Headquarters Cluster* is located in the Headquarters network. The cluster consists of two cluster nodes: *Node 1* and *Node 2*.

The different components of this configuration are explained in detail in the sections that follow.

Illustration C.1  The Example Network Scenario
## Example Firewall Cluster

Below is the list of Firewall Cluster interfaces in the example network scenario.

### Table C.1  Firewall Cluster in the Example Network Scenario

<table>
<thead>
<tr>
<th>Network</th>
<th>Description</th>
</tr>
</thead>
</table>
| Heartbeat network        | The heartbeat and cluster synchronization goes through the heartbeat network.  
                          | **CVI**: no CVI defined.  
                          | **NDI**: 10.42.1.1 (Node 1) and 10.42.1.2 (Node 2).                                                                                                                                                  |
| Management network (DMZ) | The management network interface is used for the control connections from the Management Server and for connecting to the HQ Log Server.  
                          | **CVI**: 192.168.10.1.  
                          | **NDI**: 192.168.10.21 (Node 1) and 192.168.10.22 (Node 2).                                                                                                                                 |
| ISP A external network   | This is one of the two Internet connections from the Headquarters site. It is provided by ISP A.  
                          | **CVI**: 212.20.1.254.  
                          | **NDI**: 212.20.1.21 (Node 1) and 212.20.1.22 (Node 2).  
                          | **Next hop router**: 212.20.1.1.                                                                                                           |
| ISP B external network   | This is the other of the two Internet connections from the Headquarters site. It is provided by ISP B.  
                          | **CVI**: 129.40.1.254.  
                          | **NDI**: 129.40.1.21 (Node 1) and 129.40.1.22 (Node 2).  
                          | **Next hop router**: 129.40.1.1.                                                                                                           |
| HQ intranet              | This VLAN (VLAN ID 16) is connected to the same network interface on the firewall with the HQ Accounting VLAN.  
                          | **CVI**: 172.16.1.1.  
                          | **NDI**: 172.16.1.21 (Node 1) and 172.16.1.22 (Node 2).                                                                                                                                                 |
| HQ Accounting network    | This VLAN (VLAN ID 17) is connected to the same network interface on the firewall with the HQ Intranet VLAN.  
                          | **CVI**: 172.17.1.1.  
                          | **NDI**: 172.17.1.21 (Node 1) and 172.17.1.22 (Node 2).                                                                                                                                                 |
**Example Management Center**

In the example scenario the Management Server and the HQ Log Server are at the headquarters site, in DMZ.

**Table C.2 Management Center in the Example Network Scenario**

<table>
<thead>
<tr>
<th>Management Center Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management Server</td>
<td>This Management Server manages all the Stonesoft firewalls and Log Servers of the example network. The Management Server in the Headquarters’ Management Network (DMZ) with the IP address 192.168.1.101.</td>
</tr>
<tr>
<td>HQ Log Server</td>
<td>This Log Server receives log data from the firewalls. The server is located in the Headquarters’ Management Network (DMZ) with the IP address 192.168.1.102.</td>
</tr>
</tbody>
</table>

**Example Single Firewall**

The *Branch Office Firewall* is a single firewall located in the Branch Office network.

**Illustration C.2 Branch Office Firewall**
Table C.3  Single Firewall in the Example Network Scenario

<table>
<thead>
<tr>
<th>Network</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>External network</td>
<td>The Branch Office site is connected to the Internet through this link.</td>
</tr>
<tr>
<td></td>
<td><strong>IP address</strong>: 212.20.2.254.</td>
</tr>
<tr>
<td></td>
<td><strong>Next hop router</strong>: 212.20.2.1.</td>
</tr>
<tr>
<td>Internal network</td>
<td>The Branch Office has one internal network.</td>
</tr>
<tr>
<td></td>
<td><strong>IP address</strong>: 172.16.2.1.</td>
</tr>
</tbody>
</table>
APPENDIX D

INSTALLATION WORKSHEET FOR FIREWALL CLUSTERS

For planning the configuration of network interfaces for the engine nodes, use the worksheet in Table D.1:

• In **Interface ID**, write the Interface ID (and the VLAN ID, if VLAN tagging is used)
• On the CVI line, write the Interface ID’s CVI information (if any) and on the NDI line, write the interfaces NDI information (if any). Use multiple lines for an Interface ID if it has multiple CVIs/NDIs defined.
• For **Mode**, mark all the modes that apply for this Interface ID.
• In **IP Address** and **Netmask**, define the CVI or NDI network address.
• In **MAC/IGMP IP Address**, define the MAC address used, or if the interface’s CVI Mode is Multicast with IGMP, define the multicast IP address used for generating automatically the multicast MAC address.
• In **Comments**, define for example a name of the connected network, or how the NDI addresses differ between the nodes, or a management interface’s contact address if different from the interface’s IP address.

Interface modes are explained below the table. These same character codes are displayed in the firewall element interface properties of the Management Client.
<table>
<thead>
<tr>
<th>Interface ID</th>
<th>Type</th>
<th>Mode*</th>
<th>IP Address</th>
<th>Netmask</th>
<th>MAC / IGMP IP Address</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVI</td>
<td>U</td>
<td>M I K A</td>
<td>___ . . . . . . . . .</td>
<td>___ . . . . . . . . .</td>
<td>MAC: ___ : ___ : ___ : ___ : ___</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>or IGMP IP: ___ . . . . . . . . .</td>
<td></td>
</tr>
<tr>
<td>NDI</td>
<td>H h</td>
<td>C c D</td>
<td>___ . . . . . . . . .</td>
<td>___ . . . . . . . . .</td>
<td>MAC: ___ : ___ : ___ : ___ : ___</td>
<td></td>
</tr>
<tr>
<td>CVI</td>
<td>U</td>
<td>M I K A</td>
<td>___ . . . . . . . . .</td>
<td>___ . . . . . . . . .</td>
<td>MAC: ___ : ___ : ___ : ___ : ___</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>or IGMP IP: ___ . . . . . . . . .</td>
<td></td>
</tr>
<tr>
<td>NDI</td>
<td>H h</td>
<td>C c D</td>
<td>___ . . . . . . . . .</td>
<td>___ . . . . . . . . .</td>
<td>MAC: ___ : ___ : ___ : ___ : ___</td>
<td></td>
</tr>
<tr>
<td>CVI</td>
<td>U</td>
<td>M I K A</td>
<td>___ . . . . . . . . .</td>
<td>___ . . . . . . . . .</td>
<td>MAC: ___ : ___ : ___ : ___ : ___</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>or IGMP IP: ___ . . . . . . . . .</td>
<td></td>
</tr>
<tr>
<td>NDI</td>
<td>H h</td>
<td>C c D</td>
<td>___ . . . . . . . . .</td>
<td>___ . . . . . . . . .</td>
<td>MAC: ___ : ___ : ___ : ___ : ___</td>
<td></td>
</tr>
<tr>
<td>CVI</td>
<td>U</td>
<td>M I K A</td>
<td>___ . . . . . . . . .</td>
<td>___ . . . . . . . . .</td>
<td>MAC: ___ : ___ : ___ : ___ : ___</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>or IGMP IP: ___ . . . . . . . . .</td>
<td></td>
</tr>
<tr>
<td>NDI</td>
<td>H h</td>
<td>C c D</td>
<td>___ . . . . . . . . .</td>
<td>___ . . . . . . . . .</td>
<td>MAC: ___ : ___ : ___ : ___ : ___</td>
<td></td>
</tr>
<tr>
<td>CVI</td>
<td>U</td>
<td>M I K A</td>
<td>___ . . . . . . . . .</td>
<td>___ . . . . . . . . .</td>
<td>MAC: ___ : ___ : ___ : ___ : ___</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>or IGMP IP: ___ . . . . . . . . .</td>
<td></td>
</tr>
<tr>
<td>NDI</td>
<td>H h</td>
<td>C c D</td>
<td>___ . . . . . . . . .</td>
<td>___ . . . . . . . . .</td>
<td>MAC: ___ : ___ : ___ : ___ : ___</td>
<td></td>
</tr>
<tr>
<td>CVI</td>
<td>U</td>
<td>M I K A</td>
<td>___ . . . . . . . . .</td>
<td>___ . . . . . . . . .</td>
<td>MAC: ___ : ___ : ___ : ___ : ___</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>or IGMP IP: ___ . . . . . . . . .</td>
<td></td>
</tr>
<tr>
<td>NDI</td>
<td>H h</td>
<td>C c D</td>
<td>___ . . . . . . . . .</td>
<td>___ . . . . . . . . .</td>
<td>MAC: ___ : ___ : ___ : ___ : ___</td>
<td></td>
</tr>
</tbody>
</table>

*CVI modes: U=Unicast MAC, M=Multicast MAC, I=Multicast with IGMP, K=Packet Dispatch, A=Interface's IP address used as the identity for authentication requests
NDI modes: H=Primary heartbeat, h=Backup heartbeat, C=Primary control IP address, c=Backup control IP address, D=Default IP address for outgoing connections
<table>
<thead>
<tr>
<th>Interface ID</th>
<th>Type</th>
<th>Mode*</th>
<th>IP Address</th>
<th>Netmask</th>
<th>MAC / IGMP IP Address</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVI</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NDI</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CVI</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NDI</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CVI</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NDI</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CVI</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NDI</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*CVI modes: U=Unicast MAC, M=Multicast MAC, I=Multicast with IGMP, K=Packet Dispatch, A=Interface's IP address used as the identity for authentication requests
NDI modes: H=Primary heartbeat, h=Backup heartbeat, C=Primary control IP address, c=Backup control IP address, D=Default IP address for outgoing connections
# Index

A
- ADSL interfaces, 38
- advanced configuration and power interface (ACPI), 100
- aggregated links
  - for firewall clusters, 57
  - for single firewalls, 35
- antispoofing, 90
- ARP entries, 67
- automatic power management (APM), 100

B
- BIOS settings, 100

C
- checking
  - engine version, 116
  - file integrity, 101, 117
- checksums, 101
- cluster virtual IP addresses, see CVI
- command line tools, 129
- commanding engines, 96
- commands
  - engine, 140
  - log server, 130
  - management server, 130
- compatibility, 16
- configuration
  - automatic, 75
  - manual, 76
  - plug-and-play, 74
- configuring engine on Intel or compatible, 103
- contact addresses
  - for firewall clusters, 62
  - for log servers, 28
  - for management servers, 27
- contact information, 10
- customer support, 10
- CVI, 16, 59

D
- date and time settings, 16
- defining
  - firewall clusters, 54
  - single firewalls, 32
- defining basic policies, 91–94
- deployment example, 157
- documentation available, 9

E
- example network scenario, 15, 157

F
- file integrity checking, 101, 117
- fingerprint of certificates, 139
- firewall clusters
  - contact addresses for, 62
  - defining VLAN IDs, 59
  - interface options for, 64
  - IP address types for, 16
  - modes for, 17
  - physical interfaces for, 57
  - VLAN tagging for, 58
- firewalls
  - defining clusters, 54
  - defining single, 32
  - engine commands, 96
  - IP address types for, 16
  - plug-and-play, 74
  - saving initial configuration, 72

G
- generating licenses, 21, 120

H
- hardware requirements, 10
- heartbeat connection, 17

I
- importing
  - licenses, 120
- initial configuration
  - automatic, 75
  - manual, 76
  - plug-and-play, 74
  - saving, 71
- transferring to engines, 77
- installation files, 100
- installing
  - engine on Intel or compatible, 99
  - files for, 100
  - licenses, 21
  - overview to, 15
  - policies, 95
- integrity of files, 101
- interface IDs, 32, 54
- interface options
  - for firewall clusters, 64
  - for single firewalls, 49
- IP addresses
  - for firewall clusters, 16, 59
  - for single firewalls, 42
L
licenses, 19–22
installing, 120
management-bound, 20, 51, 68
retained, 52, 69
upgrading, 118, 119–120
locations, 24–27
log server contact addresses, 28

M
management server contact addresses, 27
management-bound licenses, 20, 51, 68
MD5 checksum, 101
modem interfaces, 48
modem numbers, 32

N
NAT (network address translation), 24–27
NDI, 16, 59
node dedicated IP addresses, see NDI

O
one-time passwords on Intel and compatible, 109
overview to the installation, 15

P
packet dispatch mode, 17
partitioning engine hard disk on Intel or compatible, 110
physical interfaces
for firewall clusters, 57
for single firewalls, 35
platforms supported, 16
plug-and-play, 74
policies, 91–94
policy installation, 95
PPPoE, 47

R
requirements for running stonegate, 10
restart engine configuration on Intel and compatible, 110
retained licenses, 52, 69
routing, 80–90
default route with multi-link, 83
default route with single link, 82

S
saving initial configuration, 71
SHA-1 checksum, 101
single firewalls
ADSL interfaces for, 38
defining VLAN IDs, 37
interface options for, 49
modem interfaces for, 48
physical interfaces for, 35
SSID interfaces for, 40
VLAN tagging for, 37
wireless interfaces for, 39
sniffing network interfaces on Intel and compatible, 106
SSID interfaces, 40
state synchronization, 17
stonegate architecture, 14
support services, 10
supported platforms, 16
system architecture, 14
system requirements, 10

t
technical support, 10
transferring initial configuration to engines, 77
typographical conventions, 8

U
upgrading, 115–126
engines locally, 124
licenses, 118, 119–120

V
VLAN IDs
defining on firewall clusters, 59
defining on single firewalls, 37
VLAN tagging
for firewall clusters, 58
for single firewalls, 37
VRRP, 44

W
wireless interfaces, 39
Stonesoft Guides

Administrator’s Guides - step-by-step instructions for configuring and managing the system.

Installation Guides - step-by-step instructions for installing and upgrading the system.

Reference Guides - system and feature descriptions with overviews to configuration tasks.


For more documentation, visit
www.stonesoft.com/support/

Stonesoft Corporation
Itälahdenkatu 22 A
FI-00210 Helsinki
Finland

Tel. +358 9 476 711
Fax +358 9 4767 1349

Stonesoft Inc.
1050 Crown Pointe Parkway
Suite 900
Atlanta, GA 30338
USA

Tel. +1 770 668 1125
Fax +1 770 668 1131

Copyright 2012 Stonesoft Corporation. All rights reserved. All specifications are subject to change.