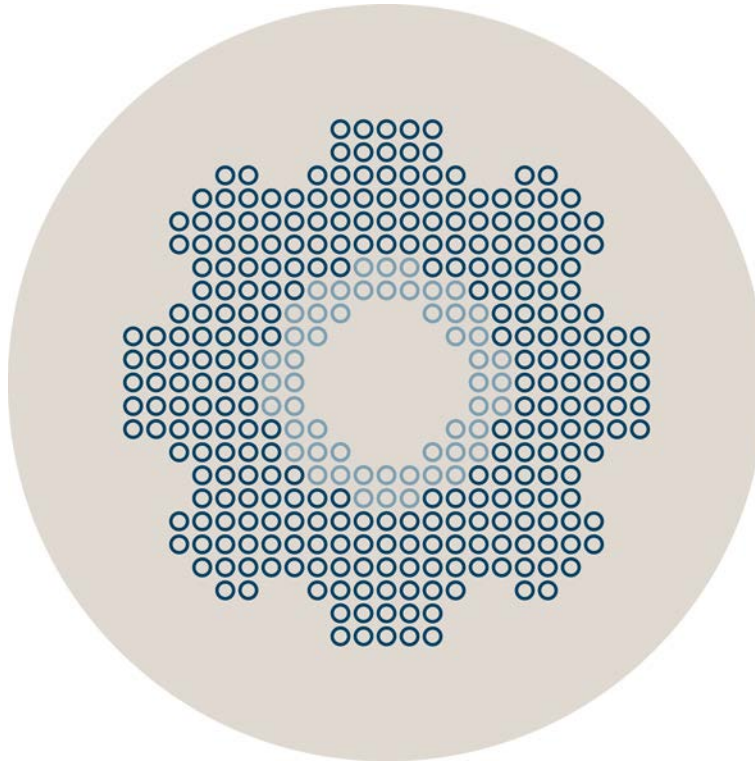


Stonesoft 5.5

Firewall/VPN 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:
www.stonesoft.com/en/support/eula.html

Third Party Licenses

The Stonesoft software includes several open source or third-party software packages. The appropriate software licensing information for those products can be found at the Stonesoft website:
www.stonesoft.com/en/customer_care/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) N:o 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/customer_care/support/

Replacement Service

The instructions for replacement service can be found at the Stonesoft website:
www.stonesoft.com/en/customer_care/support/rma/

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/customer_care/support/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, 1289202, 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.

Revision: SGFIG_20130624

Table of Contents

Introduction

Preparing for Installation

Configuring Firewalls

INSTALLING THE FIREWALL ENGINE

UPGRADING

APPENDICES

Introduction

In this section:

CHAPTER 1

USING STONESOFT DOCUMENTATION

This chapter describes how to use the *Firewall/VPN 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

The *Firewall/VPN 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

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

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.

Documentation Available

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

Guide	Description
Reference Guide	Explains the operation and features of the Stonesoft system 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.
Installation Guide	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.
Online Help	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.
Administrator's Guide	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.
User's Guide	Instructions for end-users. Available for the Stonesoft IPsec VPN Client and the Stonesoft Web Portal.
Appliance Installation Guide	Instructions for physically installing and maintaining Stonesoft appliances (rack mounting, cabling, etc.). Available for all Stonesoft hardware appliances.

PDF guides are available at http://www.stonesoft.com/en/customer_care/documentation/current/. The *Stonesoft 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 DVD.

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 web site at http://www.stonesoft.com/en/customer_care/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 at http://www.stonesoft.com/en/customer_care/kb/.

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 web site at http://www.stonesoft.com/.

Licensing Issues

You can view your current licenses at the License Center section of the Stonesoft web site 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 web site at http://www.stonesoft.com/en/customer_care/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.

Preparing for Installation

In this section:

CHAPTER 2

PLANNING THE 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, Master Engines, and Virtual Firewalls

A Stonesoft Firewall system consists of the Stonesoft Management Center and one or more Firewalls, Master Engines, and Virtual 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. A Master Engine is always a cluster that can include one to 16 nodes. A Virtual Firewall is always a Single Firewall.

The Firewalls, Master Engines, and Virtual 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. Anti-virus and anti-spam are not supported on Virtual Firewalls. Master Engines do not directly inspect traffic.
- 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 the *Stonesoft Management Center Installation Guide*. See the *Stonesoft Management Center Reference Guide* for more background information on the SMC, and the *Firewall/VPN Reference Guide* for more background information on Firewalls, Master Engines, and Virtual Firewalls.

Example Network Scenario

To get a better understanding of how the Stonesoft Firewall fits into a network, see the Example Network Scenario (page 181), which shows one way to deploy the Stonesoft Firewall.

Most of the 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 installation.

1. Install licenses for the engines. See Installing Licenses (page 21).
2. If network address translation (NAT) is applied to communications between system components and the Firewalls, define Contact Addresses. See Configuring NAT Addresses (page 25).
3. Define the Firewall, Master Engine, and Virtual Firewall element(s) in the Management Client. See the following sections:
   - Configuring Single Firewalls (page 33)
   - Configuring Firewall Clusters (page 55)
   - Configuring Master Engines and Virtual Firewalls (page 73).
4. Generate the initial configuration for the Firewall engines or Master Engines. See Saving the Initial Configuration (page 91). No initial configuration is needed for Virtual Firewalls.
5. Install and configure the Firewall engines or Master 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 Other Platforms (page 119).
   - No installation is needed for Virtual Firewalls.
6. Configure basic routing and install a policy on the engine. See Defining Routing and Basic Policies (page 99).

See the *Firewall/VPN Reference Guide* if you need more detailed background information on the operation of Firewalls, Master Engines, and Virtual Firewalls.

Supported Platforms

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

- Purpose-built Stonesoft Firewall appliances.
- Standard Intel-compatible servers. Search for the version-specific *Hardware Requirements* in the technical documentation search at http://www.stonesoft.com/en/customer_care/kb/
- Virtualization platforms that support the deployment of Open Virtual Format (OVF) templates. VMWare is officially supported. Other virtualization platforms may also be supported. There are some additional requirements and limitations when the Firewall is installed on a virtualization platform. See the Release Notes at http://www.stonesoft.com/en/customer_care/kb/ for more information. Detailed instructions can be found in Installing the Firewall Engine on a Virtualization Platform (page 123).

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

Firewall Clusters 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. The CVI allows other devices to communicate with the Firewall Cluster as a singly entity.
- *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. Master Engines only use NDIs.

Heartbeat Connection and State Synchronization in the Firewall Cluster

The nodes in a Firewall Cluster or a Master Engine 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. Make sure 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 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 Management Client *Online Help* or the *Stonesoft Administrator's Guide* 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 of a Firewall Cluster. *Packet Dispatch* mode is recommended for new installations. 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. 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 LICENSES

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

The following sections are included:

Overview to Firewall Licenses

Each Firewall and Master 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 Management Server *proof-of-license* (POL) code or the appliance *proof-of-serial* (POS) code.

Virtual Firewalls do not require a separate license. However, the Master Engine license limits the number of Virtual Resources that can be created. The limit for the number of Virtual Resources limits how many Virtual Firewalls can be created.

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

With Firewall appliances version 5.0 or newer, it is possible to download and install engine licenses automatically. For additional information on automatic downloading and installation of appliance licenses, see the *Stonesoft Administrator's Guide*.

If there is no connection between the Management Server and the Stonesoft License Center, appliance 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 using the Management Client.

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 25).
- 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, Master Engine, and Virtual Firewall element(s). Continue according to the element type:
  - Configuring Single Firewalls (page 33)
  - Configuring Firewall Clusters (page 55)
  - Configuring Master Engines and Virtual Firewalls (page 73)

Configuration Overview

The following steps are needed for installing licenses for Firewall engines and Master Engines.

1. Generate the licenses at the Stonesoft License Center. See Generating New Licenses (page 23).
2. Install the licenses in the Management Client. See Installing Licenses (page 23).

Generating New Licenses

You generate the licenses at the Stonesoft License Center based on your Management Server POL code, or the appliance POS code. Evaluation licenses are also available at the web site.

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 Stonesoft's online License Center at http://www.stonesoft.com/en/customer_care/licenses/.
2. To log in, enter the required code (POL or POS code) to identify a license you want to use and click **Submit**. The license page opens.
   - The proof-of-license (POL) code identifies a license. You can find it in the order delivery message sent by Stonesoft (usually by e-mail).
   - Stonesoft appliances additionally have a proof-of-serial number (POS) that you can find on a label attached to the appliance hardware.
3. Check which components are listed as included in this license and click **Register**. The license generation page opens.
4. Enter the POS code of the Stonesoft appliance or the Management Server's POL code. POS binding is always recommended when the option is available.
5. Click **Submit Request**. The license file is sent to you and also becomes available for download from the License Center.

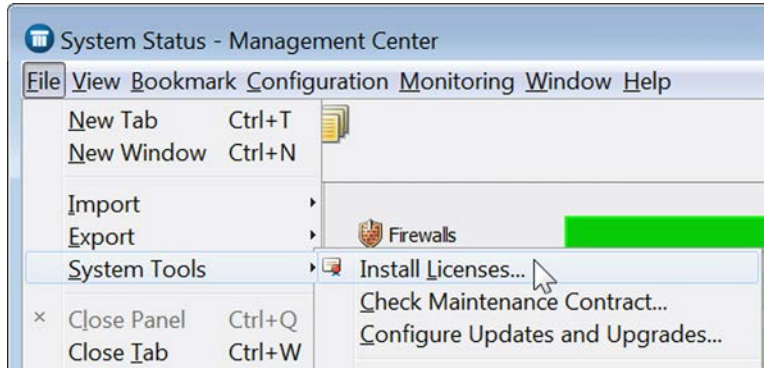
Note – Evaluation license orders may require manual processing. See the license page for current delivery times and details.

Installing Licenses

The license files must be available to the computer that you use to run the Management Client. You can install all of the licenses at the same time even though you have not yet defined all the elements the licenses will be bound to.

▼ To install licenses

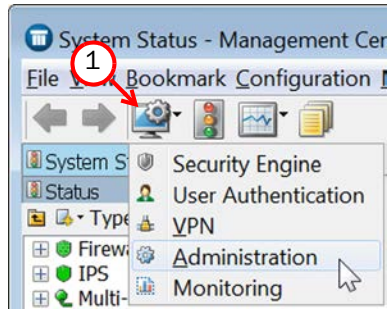
1. Select **File→System Tools→Install Licenses**.



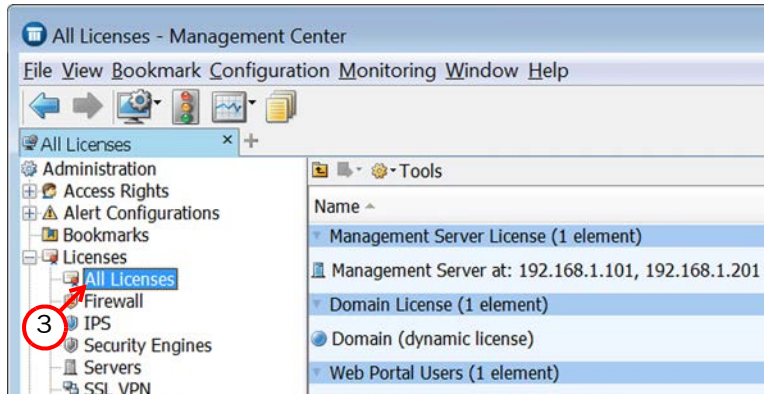
2. Select one or more license files to install in the dialog that opens and click **Install**.

▼ 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 or Master Engine node. 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 25).
- Otherwise, you are ready to define the Firewall element(s). Continue according to the element type:
  - Configuring Single Firewalls (page 33)
  - Configuring Firewall Clusters (page 55)
  - Configuring Master Engines and Virtual Firewalls (page 73)

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:

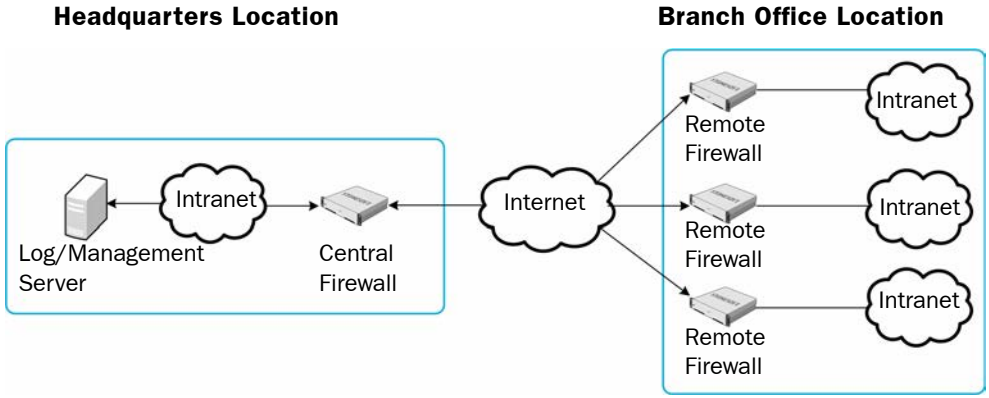
Getting Started with NAT Addresses

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 173).

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:

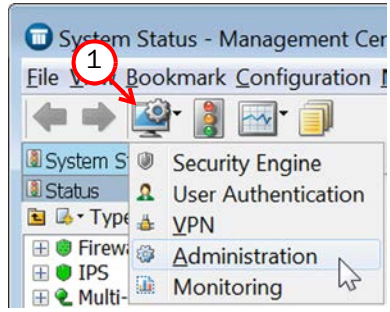
1. Define Location element(s). See Defining Locations.
2. Define contact addresses for the Management Server, and Log Server(s). See Adding SMC Server Contact Addresses (page 29).
3. Select the correct Location for firewalls and enter the contact address(es) for the firewalls when you create the Firewall elements. See Configuring Single Firewalls (page 33) and Configuring Firewall Clusters (page 55).

Defining Locations

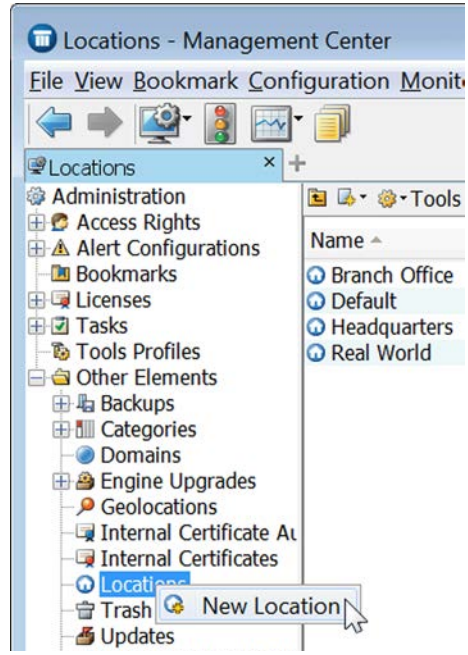
The first task is to group the system components into Location elements based on which components are on the same side of a NAT device. The elements that belong to the same Location element always use the primary IP address (defined in the Properties dialog of the element) when contacting each other.

▼ To create a new Location element

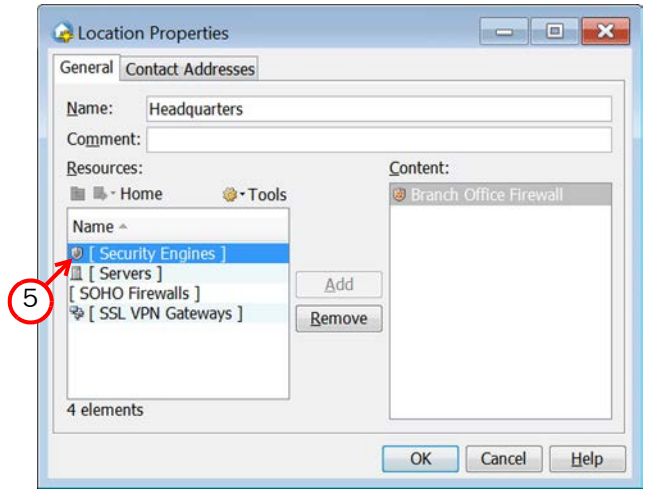
1. Click the **Configuration** icon in the toolbar, and select **Administration**. The Administration Configuration view opens.



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**.

Repeat to add other Locations as necessary.

What's Next?

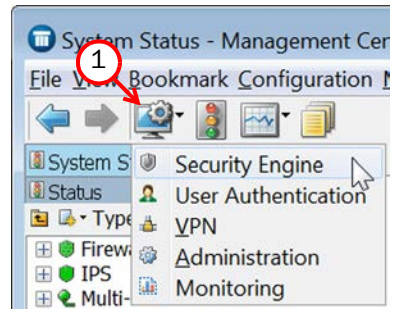
- If your Management Server or Log Server needs a contact address, proceed to Adding SMC Server Contact Addresses.
- If you plan to add contact addresses only for Single Firewall or Firewall Cluster elements, proceed to one of the following:
  - Configuring Single Firewalls (page 33)
  - Configuring Firewall Clusters (page 55)

Adding SMC Server Contact Addresses

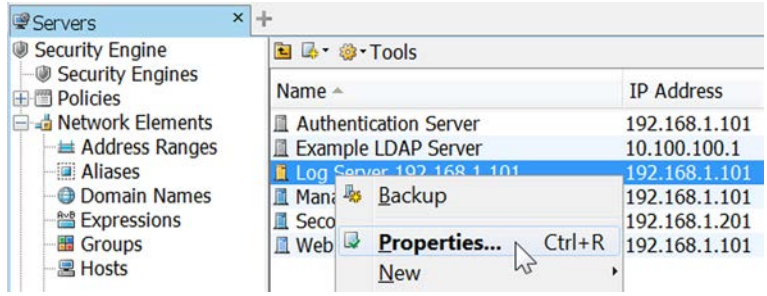
The Management Server and the Log Server can have more than one contact address for each Location. This allows you, for example, to define a contact address for each Internet link in a Multi-Link configuration for remotely managed components.

To define the Management Server and Log Server contact addresses

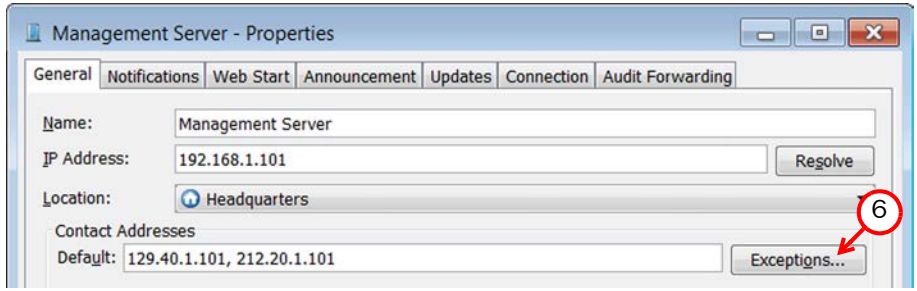
1. Click the **Configuration** icon in the toolbar, and select **Security Engine**. The Security Engine Configuration view opens.



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.



6. Click **Exceptions** and define Location-specific contact addresses if the Default Contact Address(es) are not valid from all other Locations.

Note – Elements grouped in the same Location element always use the primary IP address (defined in the 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 33).
- If you are installing a Firewall Cluster, proceed to Configuring Firewall Clusters (page 55).

Configuring Firewalls

In this section:

CHAPTER 5

CONFIGURING SINGLE FIREWALLS

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

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 36).
3. (*Optional*) Define the ADSL Interface. See Adding ADSL Interfaces (page 39).
4. (*Optional*) Define the Modem Interface(s). See Adding Modem Interfaces (page 50).
5. (*Optional*) Define the Wireless Interface. See Adding Wireless Interfaces (page 40).
6. Bind Management Server POL-bound licenses to specific Firewall elements. See Binding Engine Licenses to Correct Elements (page 52).

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 Management Client *Online Help* or the *Stonesoft Administrator's Guide*.

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 *Stonesoft Administrator's Guide*.

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.

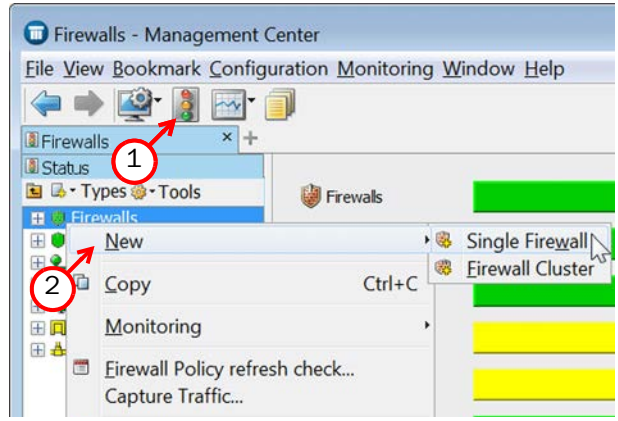
Creating a Single Firewall Element

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

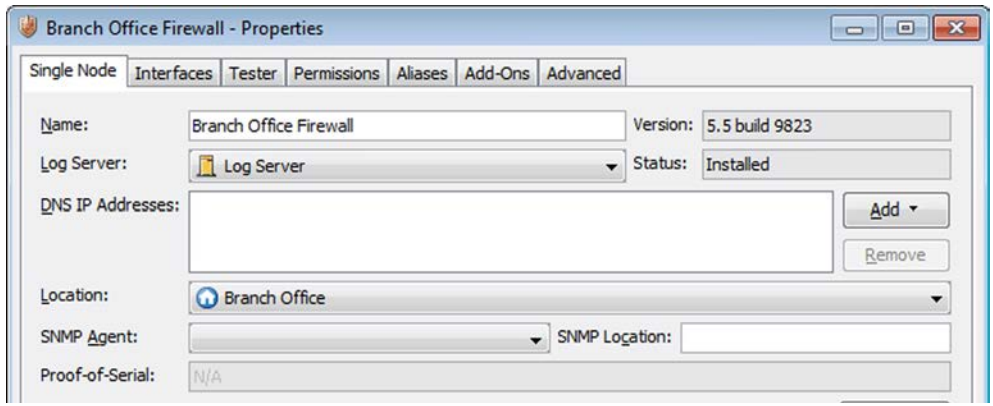
In the following tasks, the example values filled in the images refer to the example network's *Branch Office* Firewall settings (see the Example Network Scenario (page 181)).

▼ 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.



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 25)).
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 94) for more information.

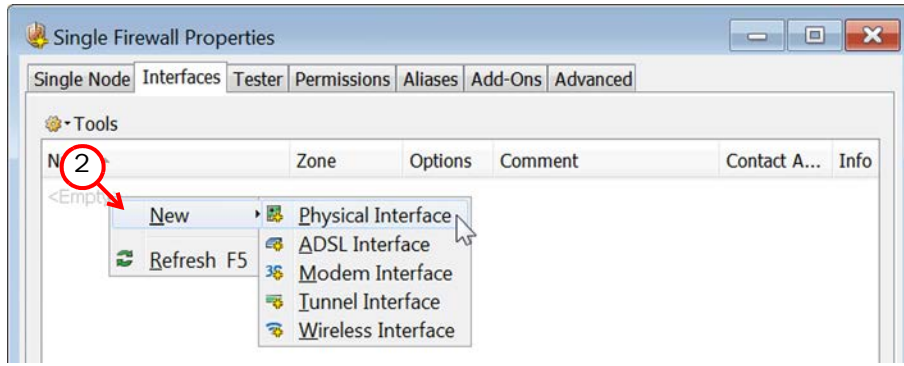
Adding Physical Interfaces

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

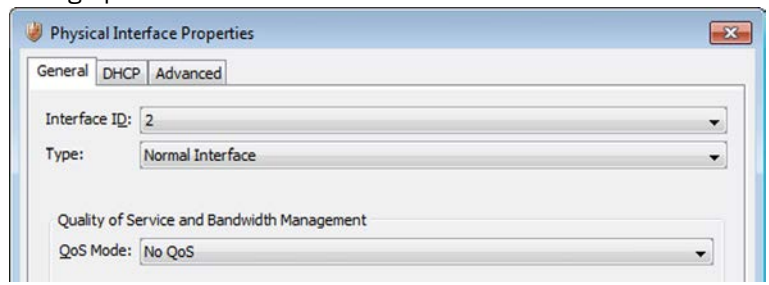
- A *Normal* interface corresponds to a single network interface on the Firewall engine.
- An *Aggregated Link in High-Availability Mode* represents two interfaces on the Firewall engine. Only the first interface in the aggregated link is actively used. The second interface becomes active only if the 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?

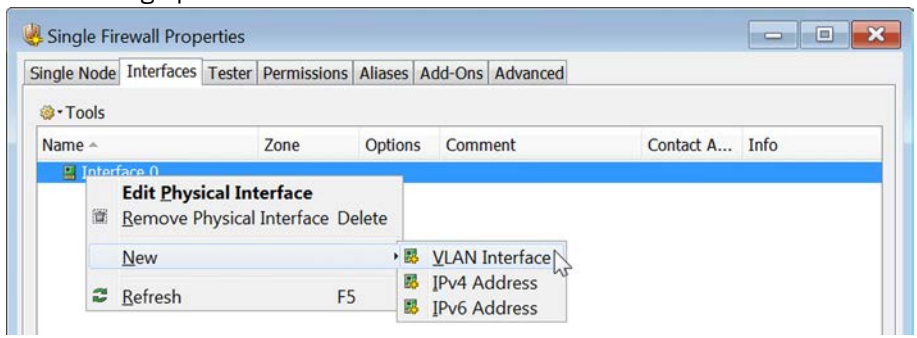
- If you want to divide any of the Physical Interfaces into VLANs, continue by Adding VLANs (page 38).
- If you want to define an ADSL Interface, continue by Adding ADSL Interfaces (page 39).
- If you want to define a Wireless Interface, continue by Adding Wireless Interfaces (page 40).
- If you want to define a Modem Interface, continue by Adding Modem Interfaces (page 50).
- Otherwise, proceed to Configuring IP Addresses for Physical, VLAN, ADSL, or SSID Interfaces (page 44).

Adding VLANs

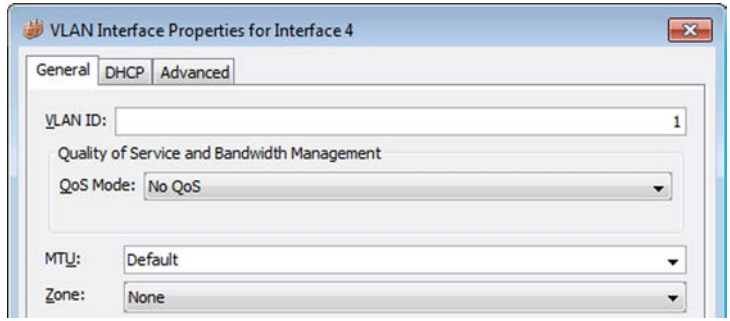
VLANs divide a single physical network link into several virtual links. You can add up to 4094 VLANS per interface.

▼ 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).



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?

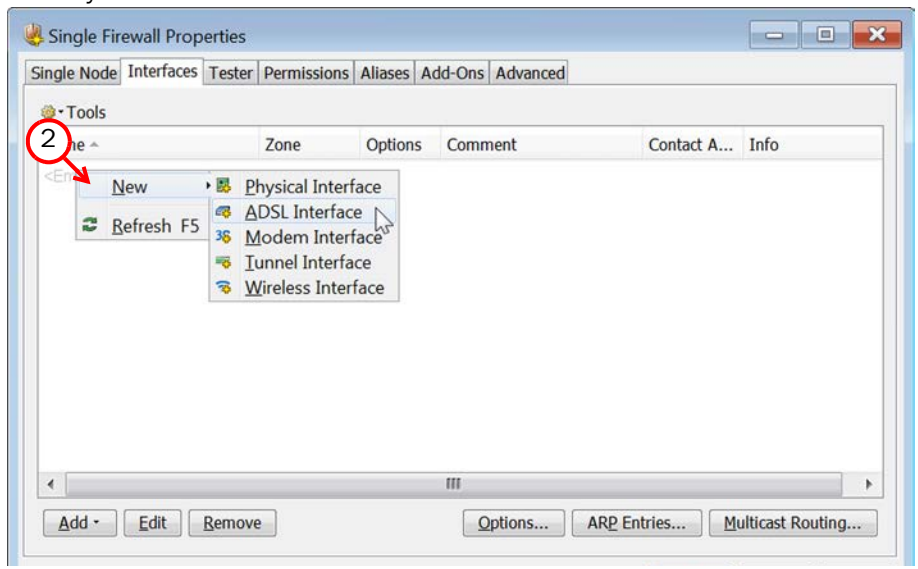
- If you want to define an ADSL Interface, continue by Adding ADSL Interfaces.
- If you want to define a Wireless Interface, continue by Adding Wireless Interfaces (page 40).
- If you want to define a Modem Interface, continue by Adding Modem Interfaces (page 50).
- Otherwise, proceed to Configuring IP Addresses for Physical, VLAN, ADSL, or SSID Interfaces (page 44).

Adding ADSL Interfaces

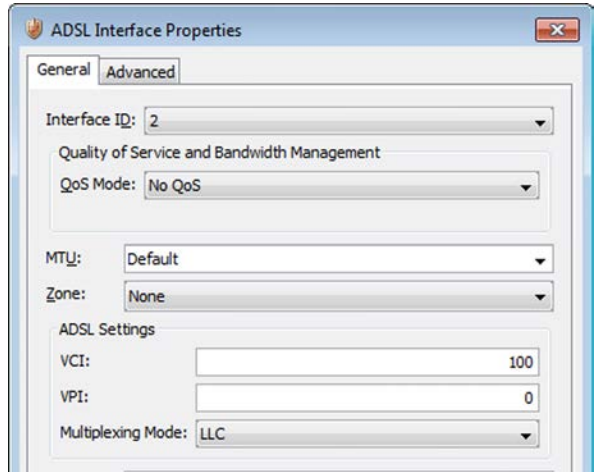
You can configure one ADSL Interface on a Single Firewall. ADSL is only supported on specific Stonesoft appliances that have an ADSL network interface card. The supported ADSL standards are ANSI T1.413 issue 2n, G.dmt, G.lite, ADSL2 DMT, ADSL2 G.lite, Annex A, and Annex B.

▼ 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. Define the ADSL Interface properties as explained in the table below.

Table 5.1 ADSL Interface Properties - General Tab

Option	Explanation
Interface ID	Select the number of the ADSL port on the appliance as the Interface ID. The Interface ID is automatically mapped to the ADSL port on the engine's ADSL card during the initial configuration of the engine.
VCI	Enter the **VCI** (Virtual Channel Identifier) value according to the configuration information provided by your ISP.
VPI	Enter the **VPI** (Virtual Path Identifier) value according to the configuration information provided by your ISP.
Multiplexing Mode	Select **LLC** (Logical Link Control) or **VC** (Virtual Circuit) according to the configuration information provided by your ISP.

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

What's Next?

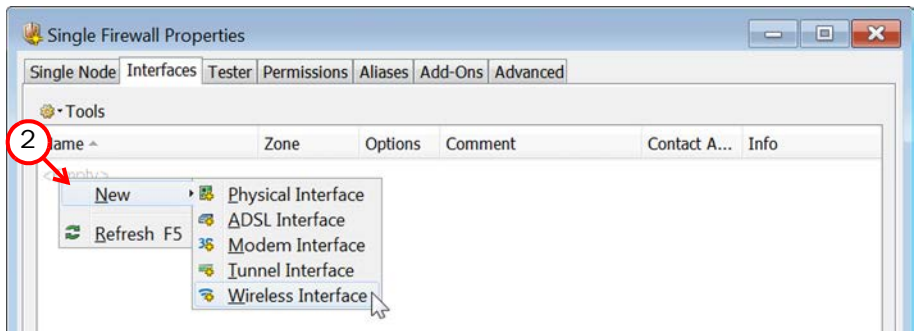
- If you want to define a Wireless Interface, continue by Adding Wireless Interfaces.
- If you want to define a Modem Interface, continue by Adding Modem Interfaces (page 50).
- Otherwise, proceed to Configuring IP Addresses for Physical, VLAN, ADSL, or SSID Interfaces (page 44).

Adding Wireless Interfaces

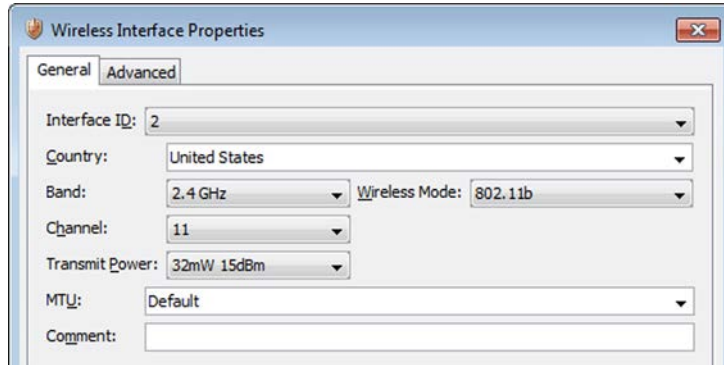
You can configure one Wireless Interface on a Single Firewall. Wireless Interfaces are only supported on specific Stonesoft appliances that have an integrated wireless network interface card.

▼ 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 5.2 Wireless Modes

Band	Wireless Mode	Description
2.4 GHz	802.11b	11 Mbit wireless-b only mode.
	802.11bg	54 Mbit wireless-b and g modes.
	802.11g	54 Mbit wireless-g only mode.
	802.11n	270 Mbit wireless-n only mode.
	802.11bgn	270 Mbit wireless-b, g, and n modes.
5 GHz	802.11a	11 Mbit wireless-a only mode.
	802.11an	270 Mbit wireless-a and n modes.
	802.11n	270 Mbit wireless-n only mode.

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 42).

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. (*Optional*) Select the maximum Transmit Power of the signal for transmitting the wireless traffic.
   - The power options are shown as milliwatts (mW) and as the power ratio in decibels of the measured power referenced to one milliwatt (dBm).
   - The values available depend on the regulatory limits for the selected Country and the Channel for the Wireless Interface.
   - If you are not sure what value to use, leave the default value selected.

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

What's Next?

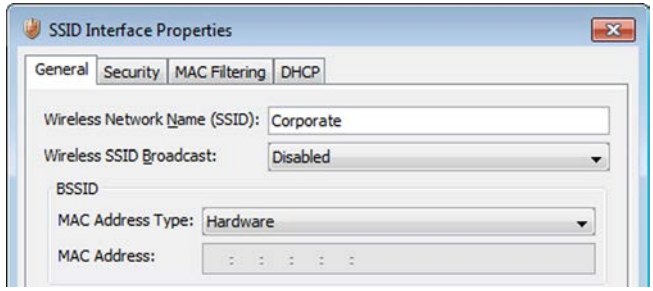
▶ Adding SSID Interfaces

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.

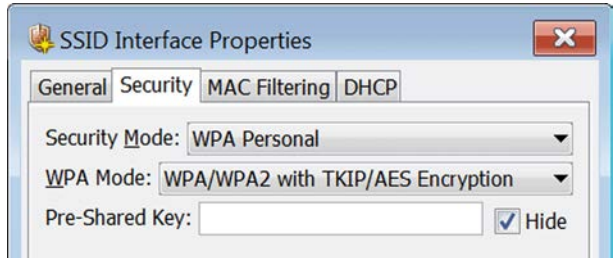
What's Next?

▶ Defining Security Settings for SSID Interfaces

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 5.3 Security Modes

Option	Explanation
Disabled	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.
WEP Open System	After the clients have connected to the Firewall, the wireless traffic is encrypted with a 40-bit or 104-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. **Note!** Some wireless clients do not support the 802.11n wireless mode with the WEP security mode.
WEP Shared Key	The connecting clients are authenticated using WEP (Wired Equivalent Privacy/ Wireless Encryption Protocol). The wireless traffic is encrypted with a 40-bit or 104-bit key. We do not recommend this security mode unless you must use WEP for compatibility reasons. **Note!** Some wireless clients do not support the 802.11n wireless mode with the WEP security mode.
WPA Personal	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.
WPA Enterprise	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.

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 Management Client *Online Help* or the *Stonesoft Administrator's Guide* for more information.

What's Next?

▶ Configuring IP Addresses for Physical, VLAN, ADSL, or SSID Interfaces (page 44)

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.

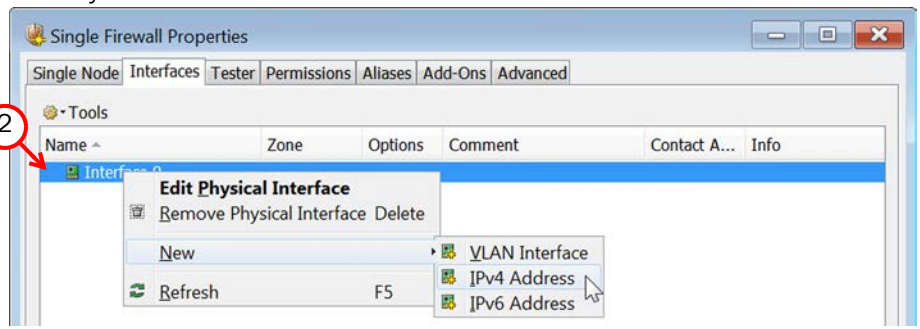
What's Next?

- To define a static IPv4 address, proceed to Adding Static IPv4 Addresses.
- To define a static IPv6 address, proceed to Adding Static IPv6 Addresses (page 47).
- To define a dynamic IP address, proceed to Configuring Dynamic IP Addresses (page 48).

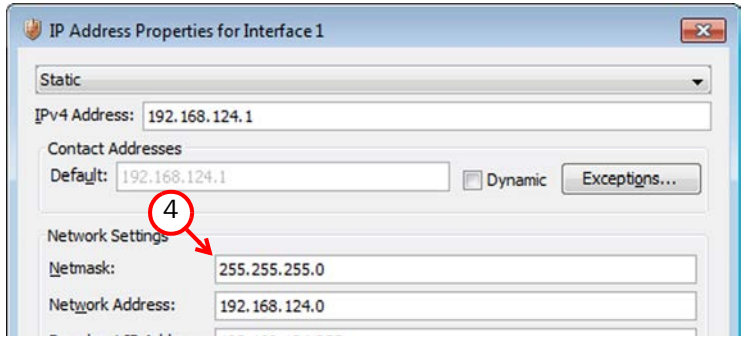
Adding Static IPv4 Addresses

▼ 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.



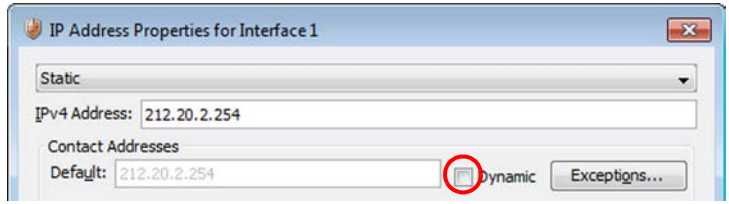
3. Enter the **IPv4 Address**.
4. Click **Netmask** and adjust the automatically added netmask if necessary. The Network Address and Broadcast IP Address are updated accordingly.

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 or VLAN Interface (page 46).
- 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 47).
- If you want to define Modem Interfaces, proceed to Adding Modem Interfaces (page 50).
- Otherwise, proceed to Setting Global Interface Options (page 51).

▼ 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.

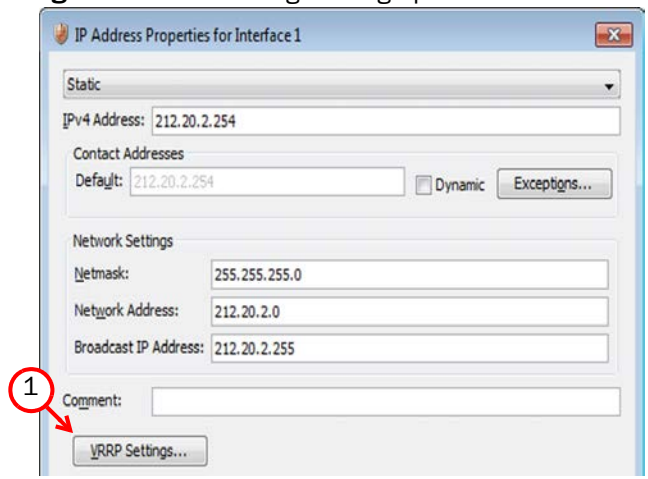
What's Next?

- If you want to use VRRP on a Physical, VLAN, or SSID Interface, proceed to the section Configuring a Virtual Router on a Physical or VLAN Interface (page 46).
- If you want to add IPv6 addresses to a Physical or VLAN Interface, proceed to Adding Static IPv6 Addresses (page 47).
- If you want to configure a Physical, VLAN, or ADSL Interface with a dynamic address, add the interface (see Adding Physical Interfaces (page 36), Adding VLANs (page 38), or Adding ADSL Interfaces (page 39)), and continue by Configuring Dynamic IP Addresses (page 48).
- If you want to define Modem Interfaces, proceed to Adding Modem Interfaces (page 50).
- Otherwise, proceed to Setting Global Interface Options (page 51).

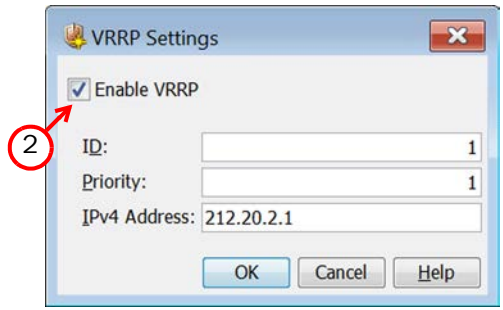
Configuring a Virtual Router on a Physical or VLAN Interface

▼ To configure VRRP

1. Click **VRRP Settings**. The VRRP Settings dialog opens.



2. Select **Enable VRRP**.



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

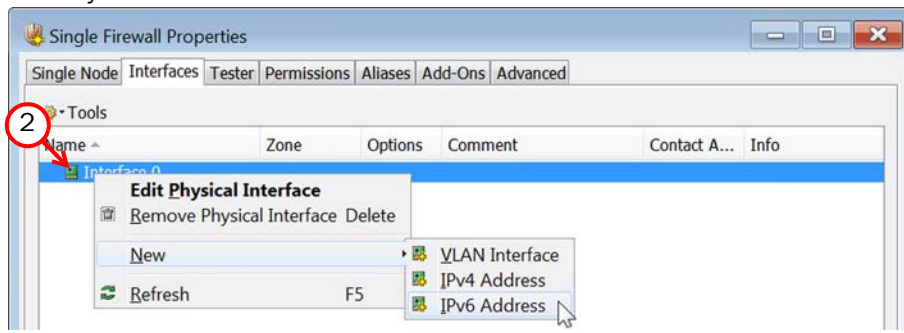
What's Next?

- If you want to configure a Physical, VLAN, or ADSL interface with a dynamic address, add the interface (see Adding Physical Interfaces (page 36), Adding VLANs (page 38), or Adding ADSL Interfaces (page 39)), and continue by Configuring Dynamic IP Addresses (page 48).
- If you want to define Modem Interfaces, proceed to Adding Modem Interfaces (page 50).
- If you are finished adding interfaces, proceed to Setting Global Interface Options (page 51).

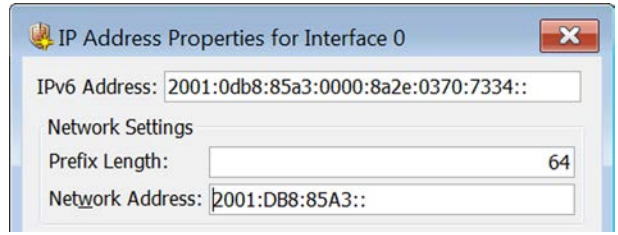
Adding Static IPv6 Addresses

▼ 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?

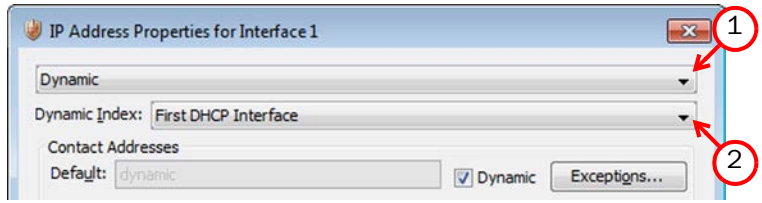
- If you want to define Modem Interfaces, proceed to Adding Modem Interfaces (page 50).
- Otherwise, proceed to Setting Global Interface Options (page 51).

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 50)).

▼ To define an interface for dynamic IP addressing

1. In the IP Address Properties, select **Dynamic**.



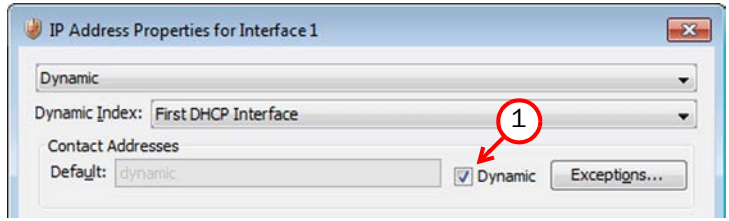
2. Select a **Dynamic Index**.

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 PPPoA or PPPoE, proceed to To set up PPP (page 49).
- 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 50).
- Otherwise, proceed to Setting Global Interface Options (page 51).

▼ To define a Contact Address for dynamic IP addressing

1. If the Default contact address is not dynamic, deselect **Dynamic** and enter the static contact address. It is used by default by components in a different Location.



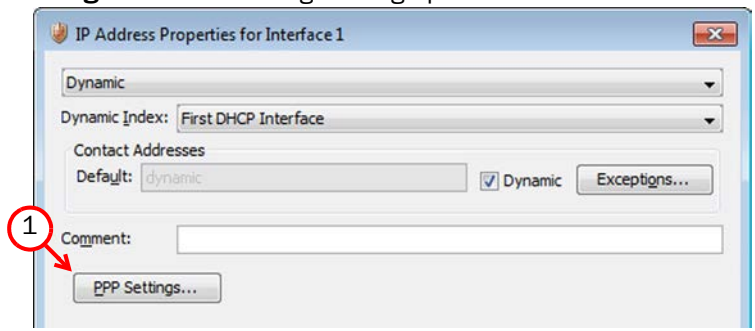
2. If components from some Locations must use a different IP address for contact, click **Exceptions** and define the Location-specific addresses.

What's Next?

- If the interface's dynamic IP address is assigned through PPPoA or PPPoE, proceed to To set up PPP (page 49).
- 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 50).
- Otherwise, proceed to Setting Global Interface Options (page 51).

▼ To set up PPP

1. Click **PPP Settings**. The PPP Settings dialog opens.



2. Select the **Mode** that the ADSL modem connected to the interface supports:
   - **PPPoE**: can be used with Physical Interfaces or ADSL Interfaces.
   - **PPPoA**: can be used with ADSL interfaces only.

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?

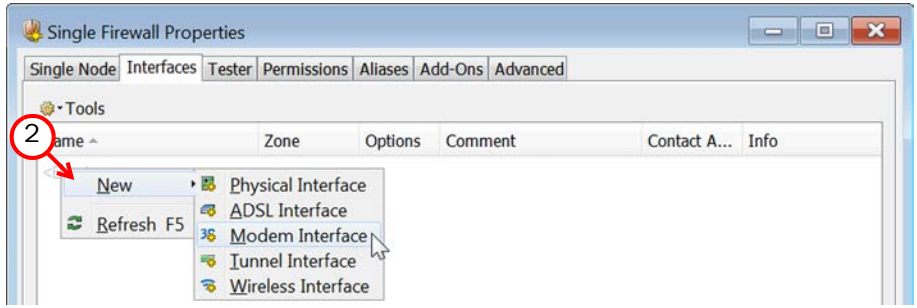
- If you are finished configuring the dynamic IP address properties, click **OK.**
- If you want to define Modem Interfaces, proceed to Adding Modem Interfaces (page 50).
- If you are finished adding interfaces, proceed to Setting Global Interface Options (page 51).

Adding Modem Interfaces

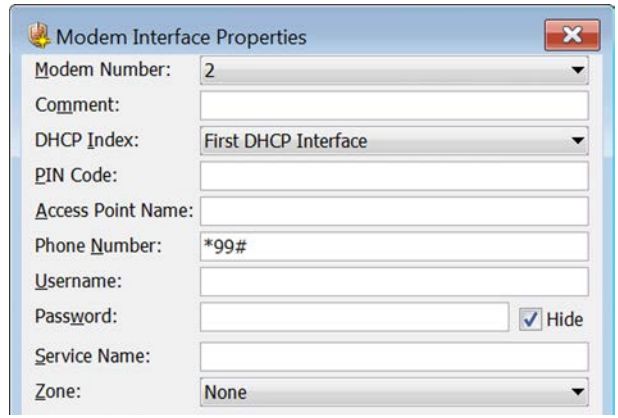
You can use 3G modem(s) with a Single Firewall to provide wireless link(s) for outbound connections.

▼ 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?

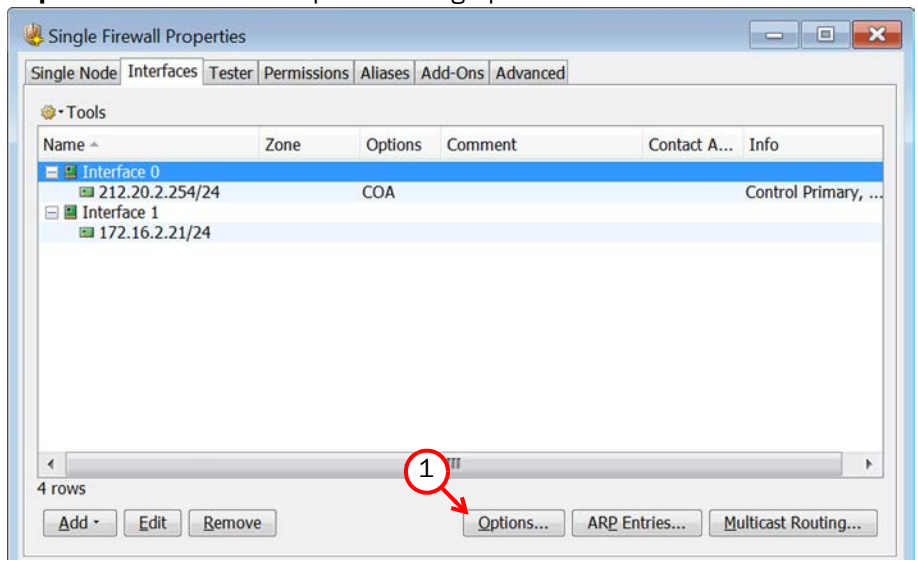
▶ Proceed to Setting Global Interface Options (page 51).

Setting Global Interface Options

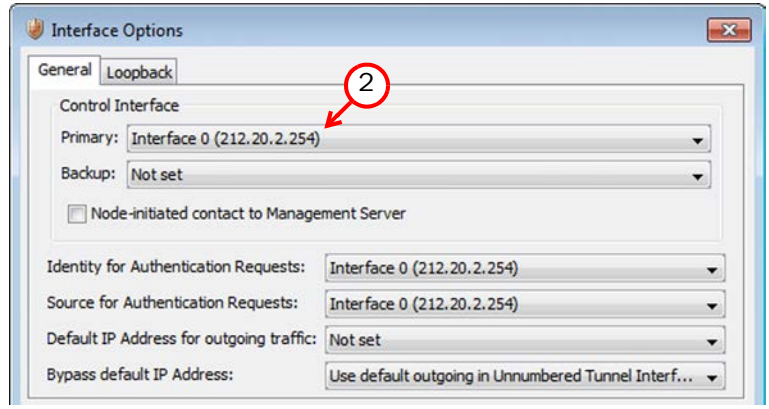
The interfaces you have defined are shown as a tree on the **Interfaces** tab. You must next select the roles that the IP addresses have in system communications. Only IPv4 addresses are used in system communications.

▼ To set global interface options for a single-node Firewall

1. Click **Options**. The Interface Options dialog opens.

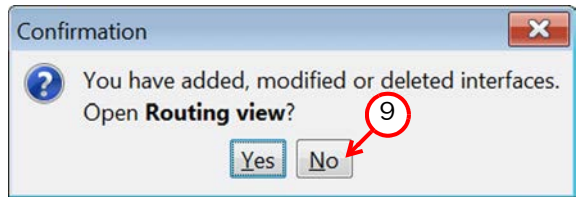


2. Set the interface that is used as the **Primary** interface for Management Server contact.



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 node does not have a static IP address on the Control Interface.
   - When this option is selected, the engine opens a connection to the Management Server and maintains connectivity.
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.

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.



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

What's Next?

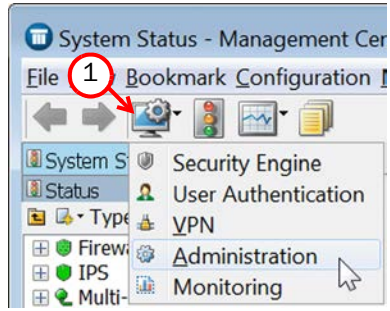
- If you have Firewall licenses that you generated based on the POL code of the Management Server (instead of the Firewall's IP address), proceed to Binding Engine Licenses to Correct Elements.
- Otherwise, you are ready to transfer the configuration to the physical Firewall engines. Proceed to Saving the Initial Configuration (page 91).

Binding Engine Licenses to Correct Elements

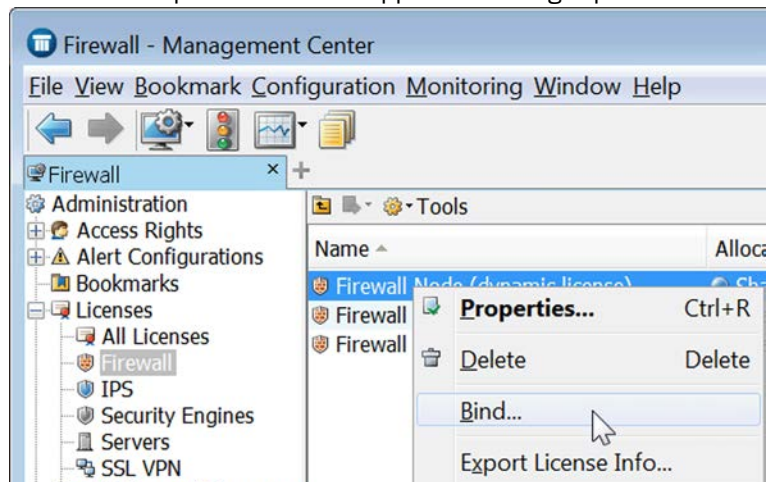
Licenses are created based on the Management Server's proof-of-license (POL) code or based on the appliance's proof-of-serial (POS) code. After you have configured the Firewall elements, you must manually bind Management Server POL-bound licenses to a specific Firewall element. POS-bound appliance licenses are automatically bound to the correct Firewall element when the engine is fully installed.

▼ To bind a Management Server POL-bound license to an engine

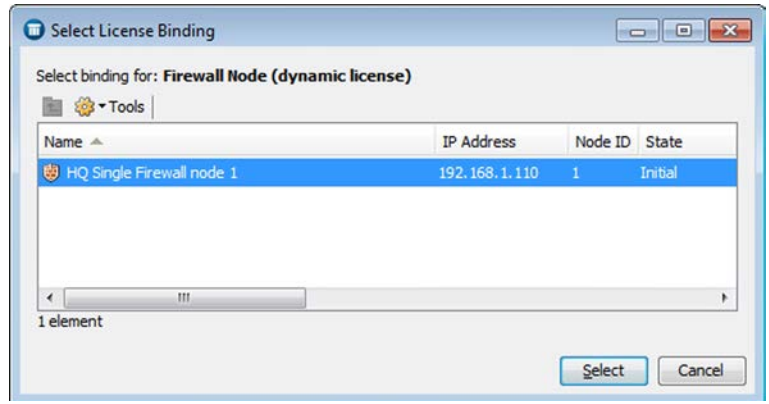
1. Click the Configuration icon in the toolbar and select **Administration.** The Administration Configuration view opens.



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 Server POL-bound license and select **Bind**. The Select License Binding dialog opens.



4. Select the Firewall and click **Select**. The license is now bound to the selected Firewall element.
   - If you bound the license to an incorrect element, right-click the license and select **Unbind**.

Caution – When you install or refresh the policy on the engine, the license is permanently bound to that engine. Permanently-bound licenses cannot be re-bound to another engine without re-licensing or deleting the engine element the license 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 91).

CHAPTER 6

CONFIGURING FIREWALL CLUSTERS

This chapter explains 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

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 58).
3. Define the physical interfaces and their properties. See Adding Physical Interfaces (page 59).
4. Bind Management Server POL-bound licenses to specific nodes in the Firewall Cluster. See Binding Engine Licenses to Correct Elements (page 70).

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 *a*t 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 185) 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 *Stonesoft Administrator's Guide*.

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.

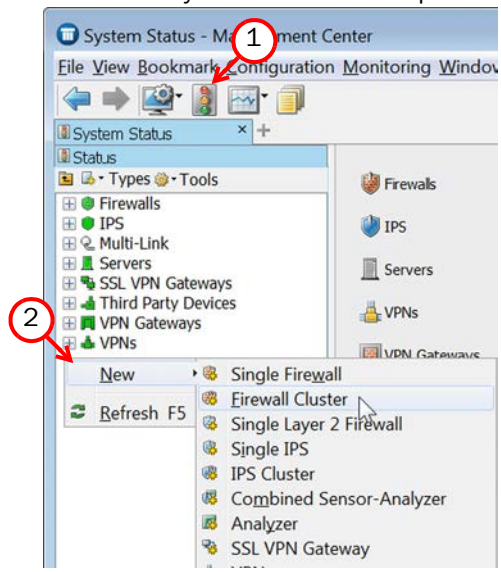
Creating a Firewall Cluster Element

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

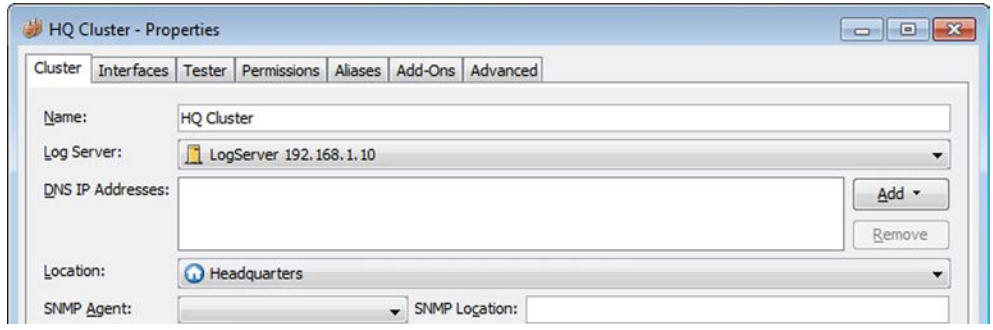
In the following tasks, the example values filled in the images refer to the example network's *Headquarters* Firewall Cluster settings. See the Example Network Scenario (page 181).

▼ 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**.

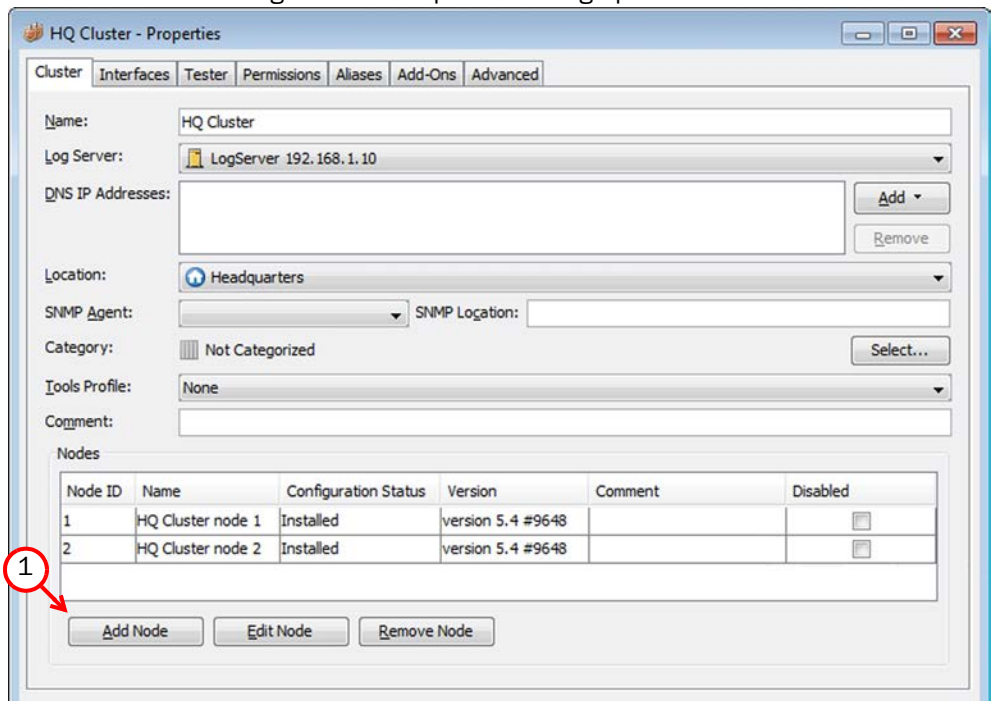
6. If required in your setup, select the **Location** (see Configuring NAT Addresses (page 25)).

Adding Nodes to a Firewall Cluster

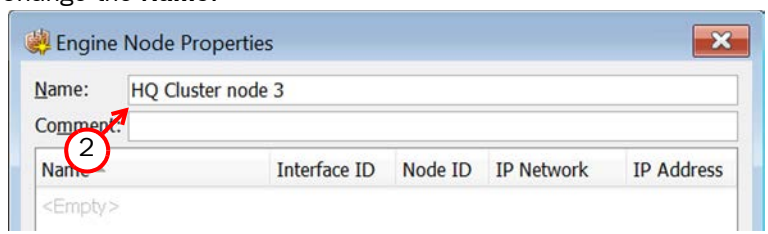
The Firewall Cluster properties have placeholders for two nodes when the element is created. A Firewall Cluster can have up to 16 nodes. Add all the nodes you plan to install before you begin configuring the interfaces.

▼ To add a node to a Firewall Cluster

1. Click **Add Node**. The Engine Node Properties dialog opens.



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.

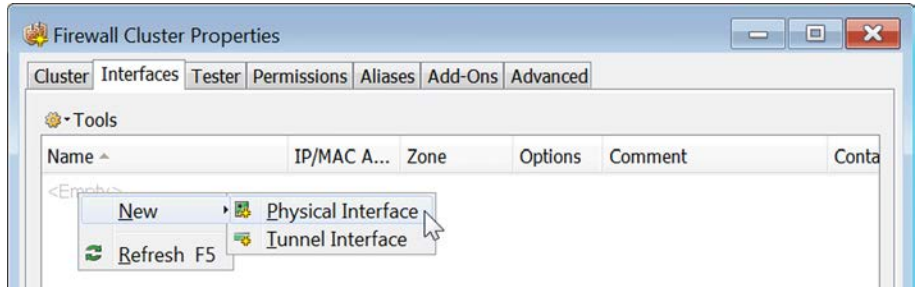
Adding Physical Interfaces

There are three types of Physical Interfaces on Firewall Clusters:

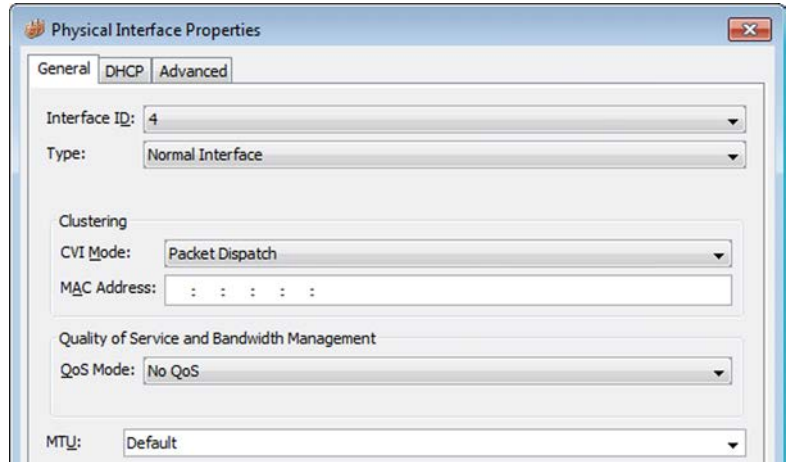
- A *Normal* interface corresponds to a single network interface on each node in the Firewall Cluster.
- An *Aggregated Link in High-Availability Mode* represents two interfaces on each node. Only the first interface in the aggregated link is actively used. The second interface becomes active only if 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.

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.

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?

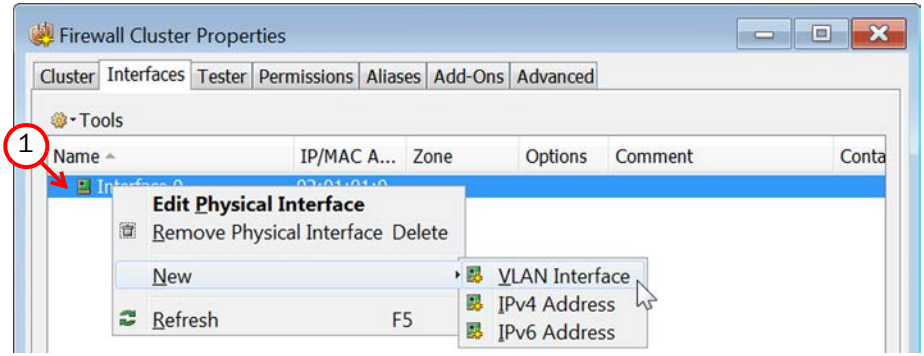
- If you want to divide any of the interfaces into VLANs, continue by Adding VLANs.
- Otherwise, proceed to Configuring IP Addresses for Cluster Interfaces (page 61).

Adding VLANs

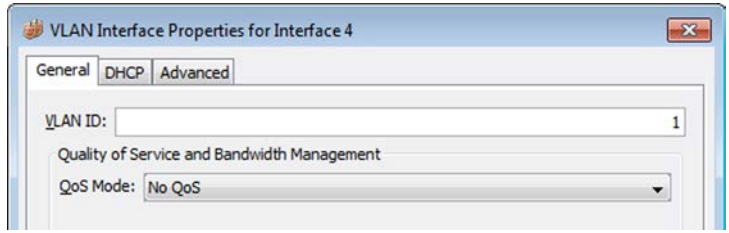
VLANs divide a single physical network link into several virtual links. You can add up to 4094 VLANs per physical interface.

▼ 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).



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.

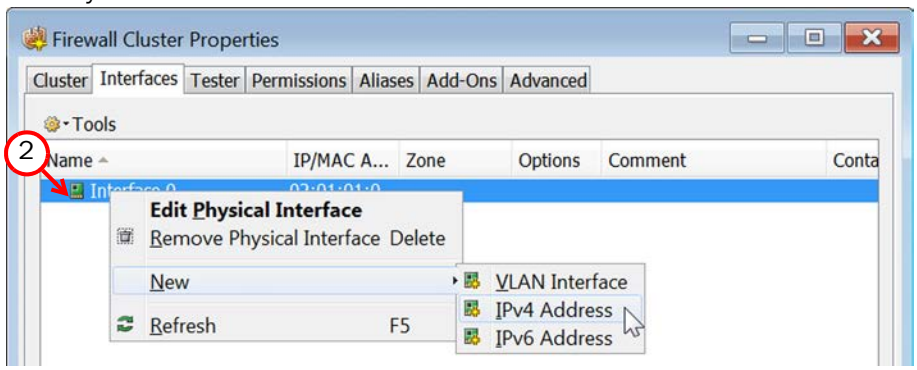
What's Next?

- To define an IPv4 address, proceed to Defining IPv4 Addresses (page 62).
- To define an IPv6 address, proceed to Defining IPv6 Addresses (page 63).

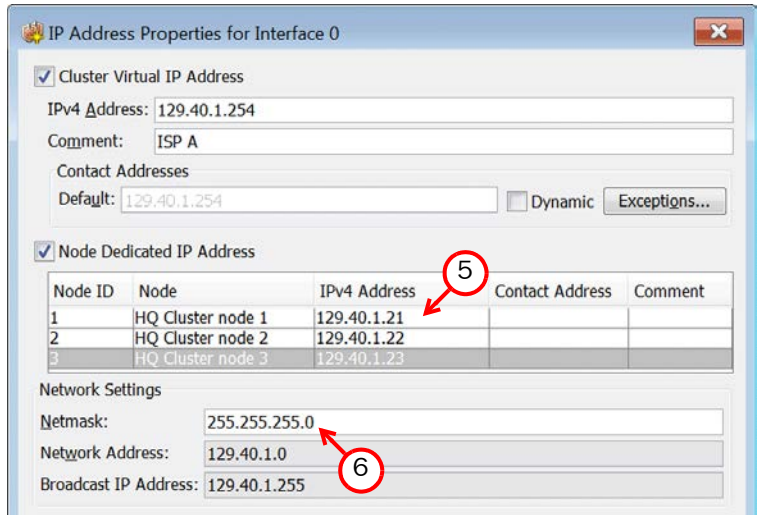
Defining IPv4 Addresses

▼ 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.

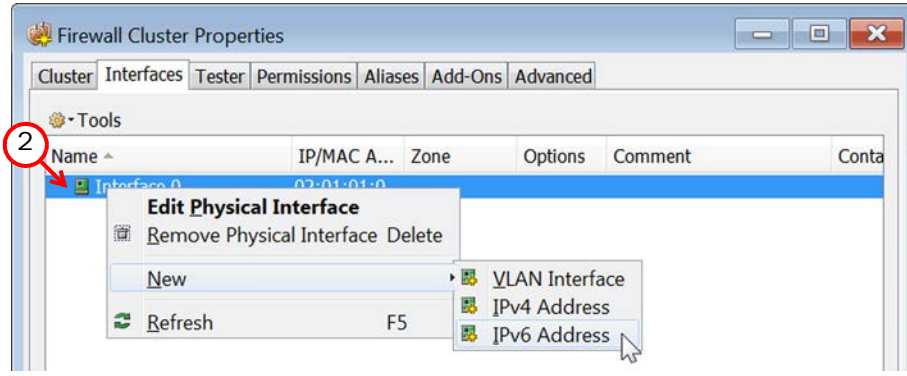
What's Next?

- If the interface(s) carry system communications and NAT is applied, complete the configuration in Defining Contact Addresses for Firewall Clusters (page 64).
- 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 66).

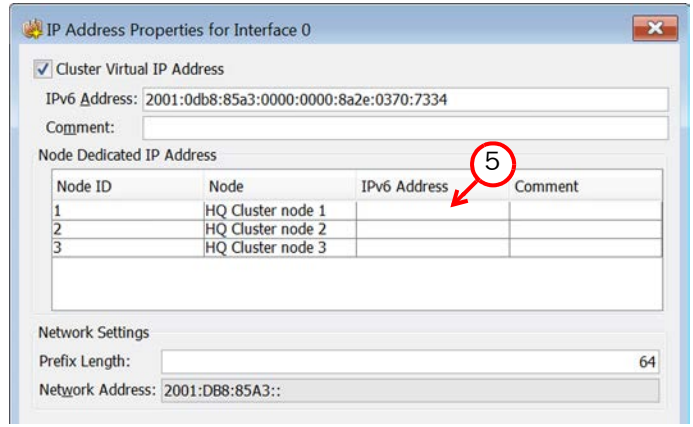
Defining IPv6 Addresses

▼ 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).

What's Next?

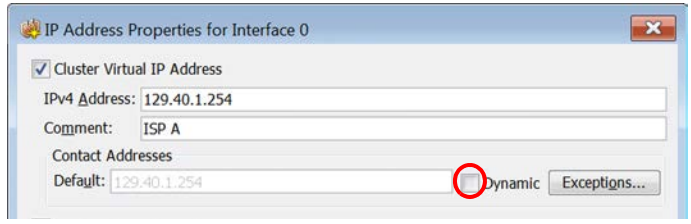
- If you are finished configuring the IPv6 address properties, click **OK**. Repeat the steps above if you want to add further IP addresses to this interface or other physical interfaces or VLAN interfaces.
- Otherwise, proceed to Setting Global Interface Options for Clusters (page 66).

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

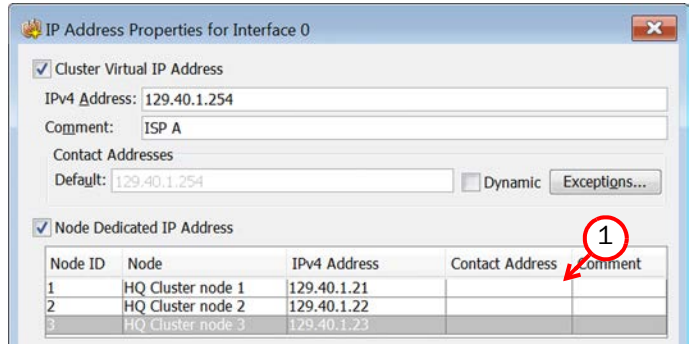
1. Enter the **Default** contact address or select **Dynamic** to define the translated IP address of this component. It is used by default by components in a different Location.



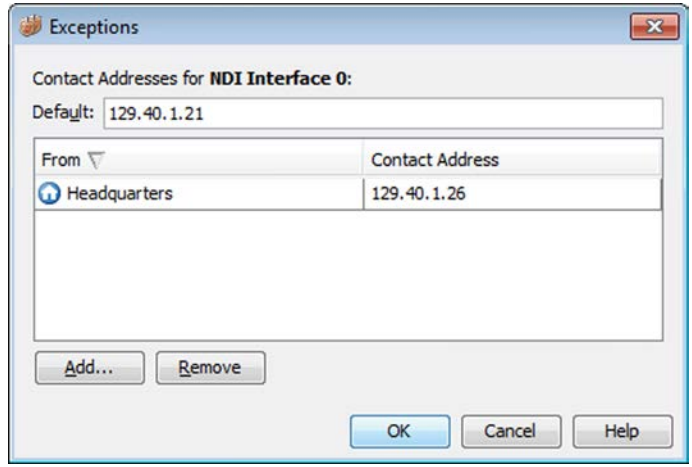
2. If components from some Locations must use a different IP address for contact, click **Exceptions** and define the Location-specific addresses.

▼ 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**.

Repeat the same steps to define contact addresses for other Cluster Virtual IP Addresses and/or Node Dedicated IP Addresses.

What's Next?

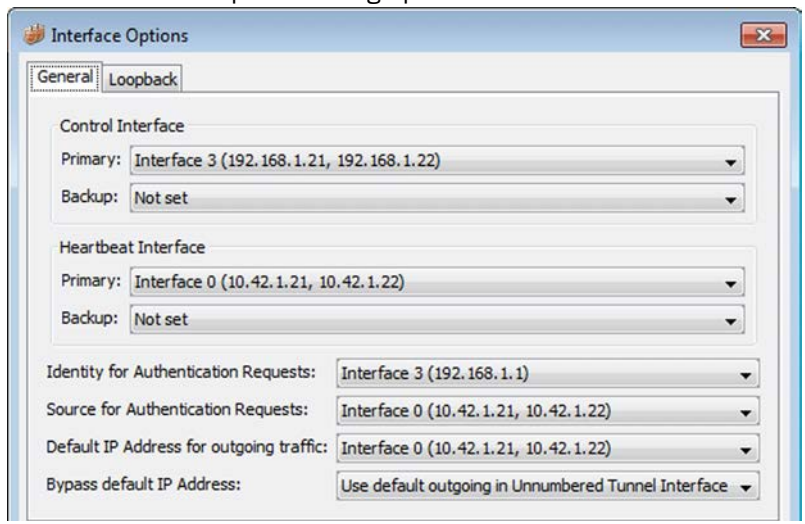
▶ If you are finished configuring cluster interfaces, click **OK** and proceed to Setting Global Interface Options for Clusters (page 66).

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

Option	Explanation
Control Interface	Select the **Primary** Control Interface for Management Server contact. This interface is used for communications with the Management Server.
	(*Optional*) Select a **Backup** Control Interface that is used if the Primary interface is not available.
Heartbeat Interface	Select the **Primary** Heartbeat Interface for communications between the nodes. We recommend that you use a Physical Interface, not a VLAN Interface. We strongly recommend that you do not direct any other traffic through this interface. A dedicated network helps ensure reliable and secure operation. **Caution!** 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 *Online Help* or the *Stonesoft Administrator's Guide*.

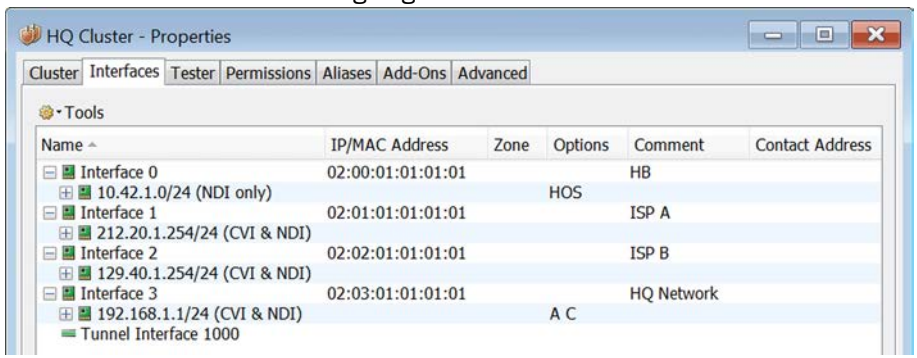
Table 6.1 Firewall Interface Options (Continued)

Option	Explanation
Heartbeat Interface (*cont.*)	Select a **Backup** 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. **Caution!** 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 *Online Help* or the *Stonesoft Administrator's Guide*.
Identity for Authentication Requests	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.
Source for Authentication Requests	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.
Default IP for Outgoing Traffic	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.

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):

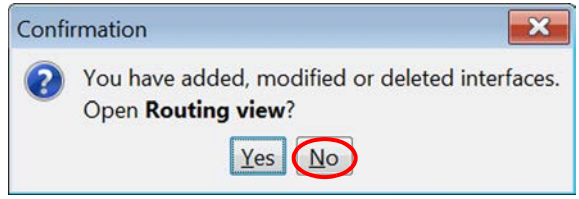
- "A" is the interface used as the identity for authentication requests
- "C" and "c" are the Primary and Secondary Control Interfaces
- "H" and "h" are the Primary and Secondary Heartbeat Interfaces
- "O" is the default IP address for outgoing connections



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 69). Otherwise, click **OK** to close the Firewall Cluster Properties.

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



What's Next?

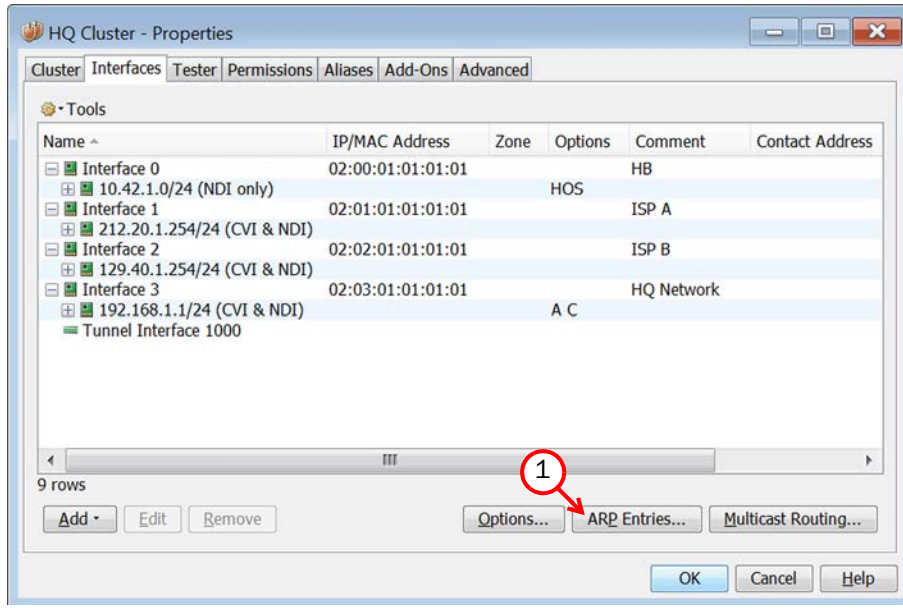
- If you generated Firewall licenses based on the POL code of the Management Server (instead of the Firewall's primary control IP address), proceed to Binding Engine Licenses to Correct Elements (page 70).
- Otherwise, you are now ready to transfer the configuration to the physical Firewall Cluster engines. Proceed to Saving the Initial Configuration (page 91).

Adding Manual ARP Entries

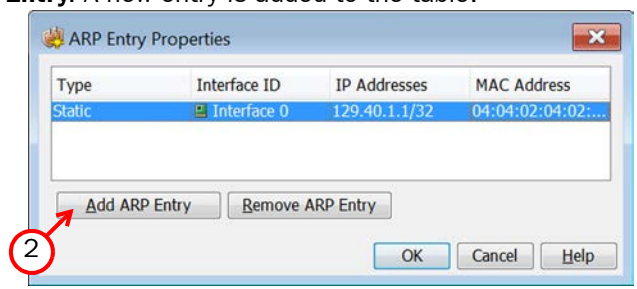
ARP entries are normally managed automatically based on the Firewall's routing configuration. However, you can also add manual ARP entries for the nodes. If an interface used for external connections has only a Cluster Virtual IP Address, you must add a static ARP entry that gives the node a permanent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

▼ To add manual ARP entries

1. Click **ARP Entries**. The ARP Entry Properties dialog opens.



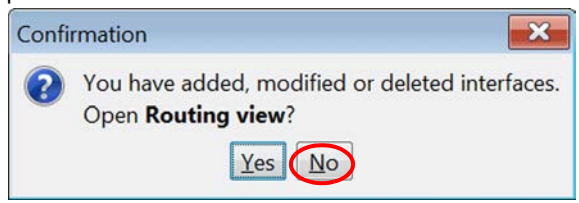
2. Click **Add ARP Entry**. A new entry is added to the table.



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?

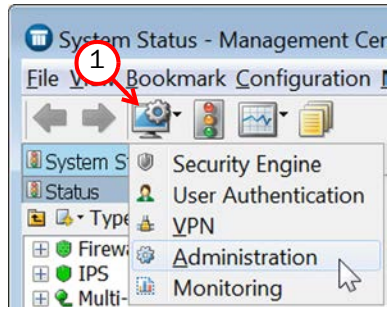
- If you generated Firewall licenses based on the POL code of the Management Server (instead of the Firewall's primary control IP address), proceed to Binding Engine Licenses to Correct Elements.
- Otherwise, you are now ready to transfer the configuration to the physical Firewall Cluster engines. Proceed to Saving the Initial Configuration (page 91).

Binding Engine Licenses to Correct Elements

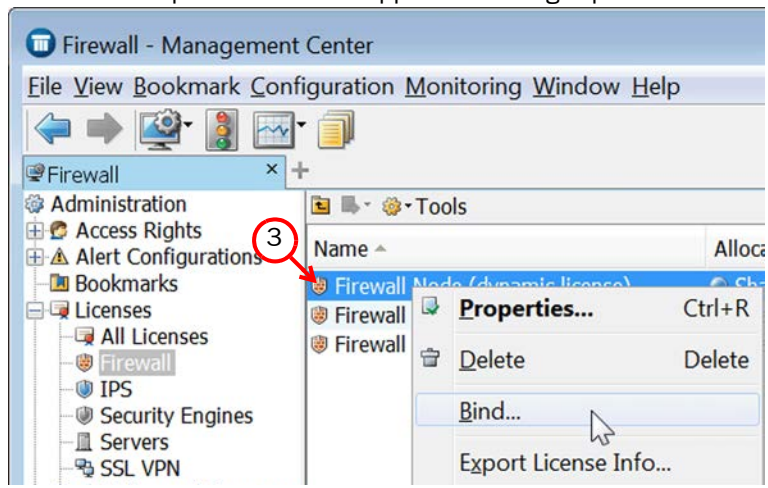
Licenses are created based on the Management Server's proof-of-license (POL) code or based on the appliance's proof-of-serial (POS) code. After you have configured the Firewall elements, you must manually bind Management Server POL-bound licenses to a specific Firewall element. POS-bound appliance licenses are automatically bound to the correct Firewall element when the engine is fully installed. Each engine is licensed separately even when the engines are clustered.

▼ To bind a Management Server POL-bound license to a node

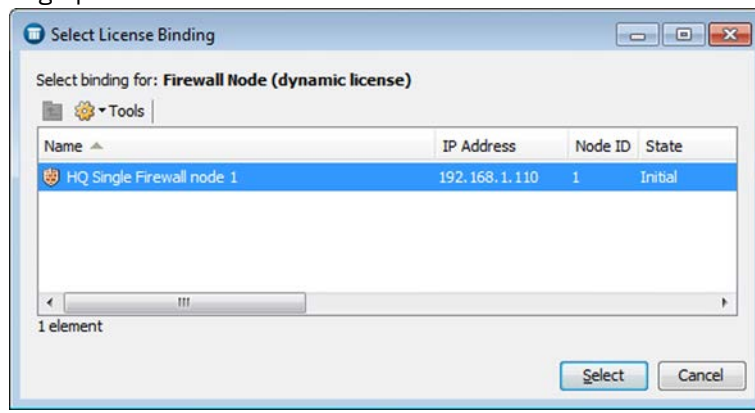
1. Click the Configuration icon in the toolbar and select **Administration.** The Administration Configuration view opens.



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 Server POL-bound license and select **Bind**. The Select License Binding dialog opens.



4. Select the node and click **Select**. The license is now bound to the selected Firewall element.
   - If you made a mistake, right-click the license and select **Unbind**.
   - Repeat the steps to bind the Management Server POL-bound licenses to all the nodes in the cluster.

Caution – When you install or refresh the policy on the engine, the license is permanently bound to that engine. Permanently-bound licenses cannot be re-bound to another engine without re-licensing or deleting the engine element the license 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 91).

CHAPTER 7

CONFIGURING MASTER ENGINES AND VIRTUAL FIREWALLS

This chapter contains the steps needed to complete the Master Engine and Virtual Firewall configuration that prepares the Management Center for a Master Engine and Virtual Firewall installation.

Very little configuration is done directly on the Master Engine. No installation or configuration is done on the Virtual Firewalls. 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

Virtual Firewalls are logically-separate Virtual Security Engines that run as virtual engine instances on a physical engine device. A Master Engine is a physical engine device that provides resources for Virtual Security Engines. One physical Master Engine can support multiple Virtual Security Engines.

The tasks you must complete are as follows:

1. Add a Master Engine element. See Adding a Master Engine Element.
2. Add a Virtual Resource element. See Adding a Virtual Resource Element (page 76).
3. Define Physical Interfaces and optionally VLAN Interfaces for the Master Engine, and assign Virtual Resources to the interfaces. See Adding Physical Interfaces for Master Engines (page 77) and Adding VLAN Interfaces for Master Engines (page 81).
4. Add a Virtual Firewall element. See Adding a Virtual Firewall Element (page 85).
5. Configure Physical Interfaces and optionally VLAN Interfaces for the Virtual Security Engine. See Configuring Physical Interfaces for Virtual Firewalls (page 86) and Adding VLAN Interfaces for Virtual Firewalls (page 87).
6. Bind Management Server POL-bound licenses to specific nodes in the Master Engine. See Binding Engine Licenses to Correct Elements (page 90).

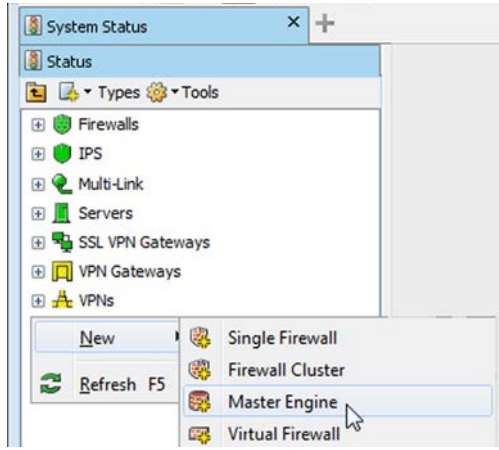
Adding a Master Engine Element

To introduce a new Master Engine to the Management Center, you must define a Master Engine element that stores the configuration information related to the Master Engine and Virtual Security Engines.

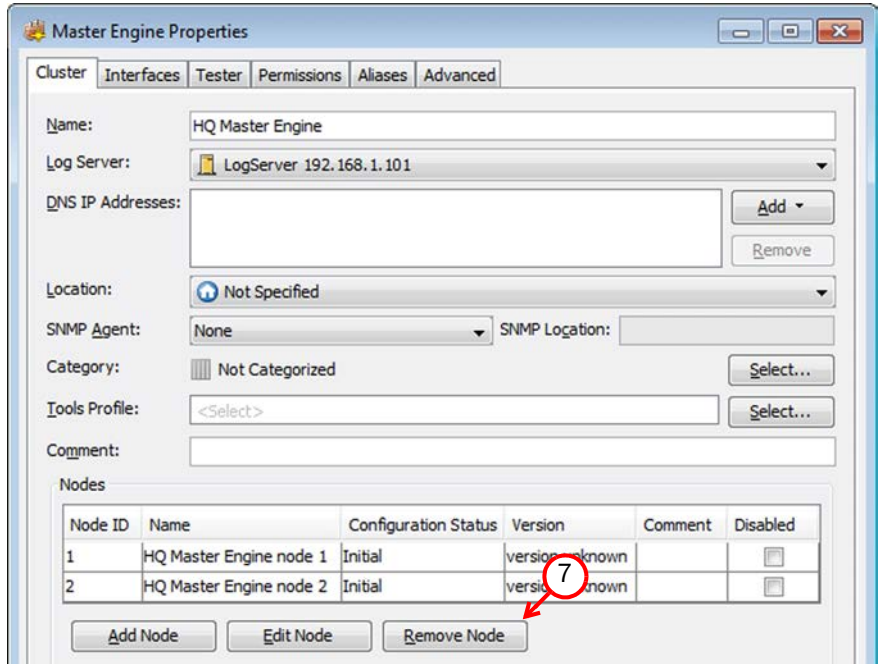
This section covers the basic configuration of a Master Engine element. For information on all the options, see the *Stonesoft Administrator's Guide* or the Management Client *Online Help*.

▼ To create a Master Engine element

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



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



3. Give the element a unique **Name**.
4. Select the **Log Server** to which the Master Engine sends its log data.
5. (*Optional*) Define one or more **DNS IP Addresses**. These are the IP addresses of the DNS server(s) that the Master Engine uses to resolve domain names. There are two ways to define IP addresses.
   - To enter a single IP address manually, click **Add** and select **IP Address**. Enter the IP address in the dialog that opens.
   - To define an IP address using a network element, click **Add** and select **Network Element**. Select an existing element, or click the New icon and define a new element.
6. Select the **Location** for this Master Engine if there is a NAT device between this Master Engine and other system components. See Defining Locations (page 80) for more information.
7. (*Optional*) If you do not need to use clustering on the Master Engine, select one of the nodes and click **Remove Node**. You are prompted to confirm that you want to delete the selected node. Click **Yes**.

What's Next?

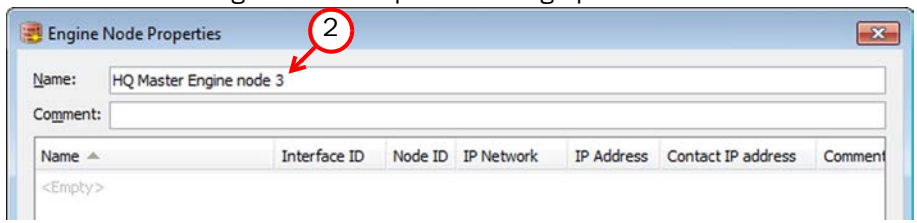
- If you want to add more nodes to the Master Engine, continue by Adding Nodes to a Master Engine (page 76).
- Otherwise, continue by Adding a Virtual Resource Element (page 76).

Adding Nodes to a Master Engine

The Master Engine properties have placeholders for two nodes when the element is created. A Master Engine 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 Master Engine

1. Click **Add Node**. The Engine Node Properties dialog opens.



2. (*Optional*) Modify the **Name**.
3. Click **OK**. The node is added to the Master Engine.

What's Next?

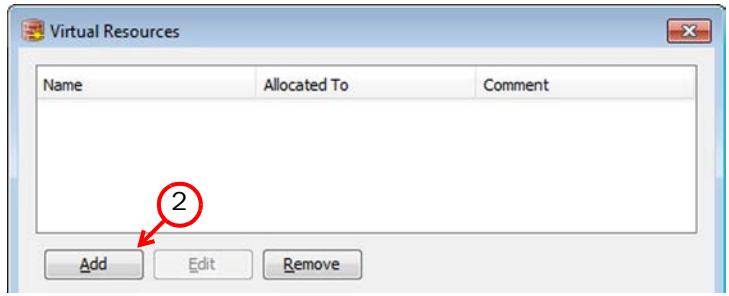
▶ Repeat these steps for each node that you want to add, then continue by Adding a Virtual Resource Element.

Adding a Virtual Resource Element

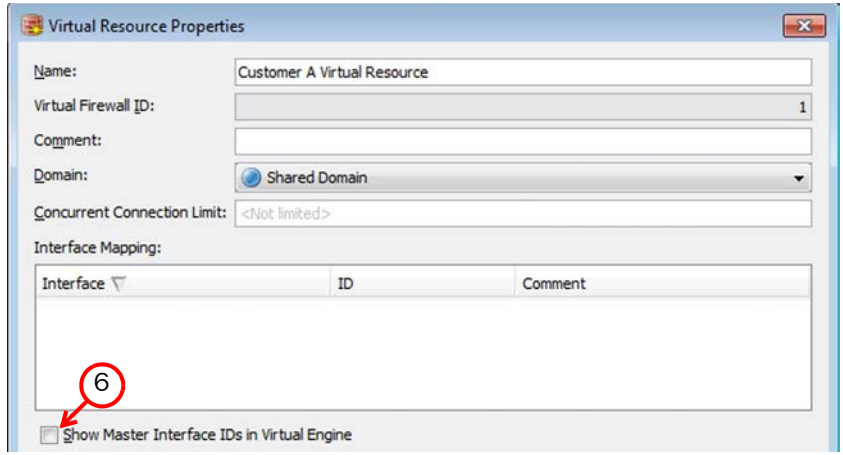
Virtual Resources define the set of resources on the Master Engine that are allocated to each Virtual Security Engine.

▼ To create a Virtual Resource element

1. Switch to the **Interfaces** tab of the Master Engine Properties and click **Virtual Resources**. The Virtual Resources dialog opens.



2. Click **Add**. The Virtual Resource Properties dialog opens.



3. Enter a unique **Name** for the Virtual Resource.
4. Select the **Domain** to which the Virtual Resource belongs.
5. (*Optional*) Enter the **Concurrent Connection Limit** to set a limit for connections from a single source and/or destination IP address. When the set number of connections is reached, the next connection attempts are blocked by the engine until a previously open connection is closed.
6. (*Optional*) Select **Show Master Interface IDs in Virtual Engine** if you want the Physical Interface IDs of the Master Engine to be shown in the Interface properties of the Virtual Security Engine.
7. Click **OK**. The Virtual Resource Properties dialog closes.
8. Click **OK**. The Virtual Resources dialog closes.

What's Next?

▶ Repeat these steps for all Virtual Resources that you want to add, then continue by Adding Physical Interfaces for Master Engines.

Adding Physical Interfaces for Master Engines

Master Engines can have two types of Physical Interfaces: interfaces for the Master Engine's own communications, and interfaces that are used by the Virtual Firewalls hosted on the Master Engine.

You must define at least one Physical Interface for the Master Engine's own communications. It is recommended to define at least two Physical Interfaces for the Master Engine:

- A *Control Interface* for communications between the Management Server and the Master Engine.
- A *Heartbeat Interface* for communications between the Master Engine nodes. The heartbeat traffic is critical to the functioning of the cluster, so it is highly recommended to have a dedicated Heartbeat Interface.

▼ To add a Physical Interface to a Master Engine

1. Switch to the **Interfaces** tab of the Master Engine Properties.
2. Right-click the empty space and select **New Physical Interface**. The Physical Interface Properties dialog opens.
3. (*Interface for Master Engine communications only*) Define the Physical Interface properties as explained in the table below.

Table 7.1 Physical Interface Properties for Master Engine Communications

Options		Explanation
Interface ID		The Interface ID automatically maps to a physical network port of the same number of the same number during the initial configuration of the engine, but the mapping can be changed as necessary through the engine's command line interface. Changes to the Master Engine interface mapping do not affect the Interface IDs that are defined for Virtual Security Engines in Virtual Resource elements.
Type	Normal Interface	Corresponds to a single network interface on the Master Engine appliance.
	Aggregated Link in High-Availability Mode	Represents two interfaces on the Master Engine appliance. Only the first interface in the aggregated link is actively used. The second interface becomes active only if the first interface fails. If you configure an Aggregated Link in High-Availability mode, connect the first interface to one switch and the second interface to another switch.
	Aggregated Link in Load-Balancing Mode	Represents two interfaces on the Master Engine appliance. Both interfaces in the aggregated link are actively used and connections are automatically balanced between the two interfaces. 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.
Second Interface ID (*Only if interface type is Aggregated Link*)		The second interface in the aggregated link.
Virtual Resource		Do not select a Virtual Resource for an interface that is used for the Master Engine's own communications.
Cluster MAC Address		The MAC address for the Master Engine. Do not use the MAC address of any actual network card on any of the Master Engine nodes.

Table 7.1 Physical Interface Properties for Master Engine Communications (Continued)

Options	Explanation
MTU (*Optional*)	The MTU (maximum transmission unit) size on the connected link. Either enter a value between 400-65535 or select a common MTU value from the list. The default value (also the maximum standard MTU in Ethernet) is 1500. Do not set a value larger than the standard MTU unless you know that all devices along the communications path support it.

4. (*Interface for hosted Virtual Firewall communications only*) Define the Physical Interface properties as explained in the table below.

Table 7.2 Physical Interface Properties for Hosted Virtual Engine Communications

Options		Explanation
Interface ID		The Interface ID automatically maps to a physical interface of the same number during the initial configuration of the engine, but the mapping can be changed as necessary through the engine's command line interface.
Type	Normal Interface	Corresponds to a single network interface on the Master Engine appliance.
	Aggregated Link in High-Availability Mode	Represents two interfaces on the Master Engine appliance. Only the first interface in the aggregated link is actively used. The second interface becomes active only if the first interface fails. If you configure an Aggregated Link in High-Availability mode, connect the first interface to one switch and the second interface to another switch.
	Aggregated Link in Load-Balancing Mode	Represents two interfaces on the Master Engine appliance. Both interfaces in the aggregated link are actively used and connections are automatically balanced between the two interfaces. 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.
Second Interface ID (*Only if interface type is Aggregated Link*)		The second interface in the aggregated link.

Table 7.2 Physical Interface Properties for Hosted Virtual Engine Communications (Continued)

Options	Explanation
Virtual Resource	The Virtual Resource associated with the interface. Select the same Virtual Resource in the properties of the Virtual Firewall element to add the Virtual Security Engine to the Master Engine. See Creating New Virtual Security Engines (page 457). Only one Virtual Resource can be selected for each Physical Interface. If you want to add multiple Virtual Resources, add VLAN Interfaces to the Physical Interface and select the Virtual Resource in the VLAN Interface properties as explained in Adding VLAN Interfaces for Master Engines (page 81).
Allow VLAN Definition in Virtual Engine (*Optional*)	Select this option to allow VLAN Interfaces to be added to the automatically created Physical Interfaces in the Virtual Security Engine that is associated with this interface.
Virtual Engine Interface ID	Select the Interface ID of the Physical Interface in the Virtual Security Engine that is associated with this interface.
Cluster MAC Address	The MAC address for the Master Engine. Do not use the MAC address of any actual network card on any of the Master Engine nodes.
Throughput (kbps) (*Optional*)	Enter the maximum throughput for Virtual Engines that use this interface as kilobits per second (for example, 2048). The same throughput is automatically applied to any VLANs created under this Physical Interface. See Adding VLAN Interfaces for Master Engines (page 81).
MTU (*Optional*)	The MTU (maximum transmission unit) size for Virtual Engines that use this interface. Either enter a value between 400-65535 or select a common MTU value from the list. The default value (also the maximum standard MTU in Ethernet) is 1500. Do not set a value larger than the standard MTU unless you know that all the devices along the communications path support it.

5. Click **OK**. The Physical Interface is added to the interface list.
6. Repeat from Step 2 to add any other Physical Interfaces.

What's Next?

- If you want to use VLANs on a Physical Interface, add the VLANs before adding IP addresses. Proceed to Adding VLAN Interfaces for Master Engines (page 81).
- Otherwise, add IP addresses directly to the Physical Interfaces used for Master Engine communications as instructed in Adding IPv4 Addresses for Master Engines (page 83).

Adding VLAN Interfaces for Master Engines

VLANs divide a single physical network link into several virtual links. The maximum number of VLANs for a single Physical Interface is 4094. The VLANs must also be defined in the configuration of the switch/router to which the interface is connected. Master Engines can have two types of VLAN Interfaces: interfaces for the Master Engine's own communications, and interfaces that are used by the Virtual Firewalls hosted on the Master Engine.

▼ To add a VLAN Interface to a Master Engine

1. Right-click a Physical Interface and select **New→VLAN Interface**. The VLAN Interface Properties dialog opens.
2. (*Interface for Master Engine communications only*) Define the VLAN Interface properties as explained in the table below.

Table 7.3 VLAN Interface Properties - General Tab

Option	Explanation
VLAN ID	Enter the VLAN ID (1-4094). The VLAN IDs you add must be the same as the VLAN IDs that are used in the switch at the other end of the VLAN trunk. Each VLAN Interface is identified as *Interface-ID.VLAN-ID*, for example *2.100* for Interface ID 2 and VLAN ID 100.
Virtual Resource	Do not select a Virtual Resource for an interface that is used for the Master Engine's own communications.
MTU (*Optional*)	The MTU (maximum transmission unit) size on the connected link. Either enter a value between 400-65535 or select a common MTU value from the list. **Caution!** The MTU for each VLAN Interface must not be higher than the MTU for the Physical Interface to which the VLAN Interface belongs. The default value (also the maximum standard MTU in Ethernet) is 1500. Do not set a value larger than the standard MTU unless you know that all the devices along the communications path support it.

3. (*Interface for hosted Virtual Firewall communications only*) Define the VLAN Interface properties as explained in the table below.

Table 7.4 VLAN Interface Properties - General Tab

Option	Explanation
VLAN ID	Enter the VLAN ID (1-4094). The VLAN IDs you add must be the same as the VLAN IDs that are used in the switch at the other end of the VLAN trunk. Each VLAN Interface is identified as *Interface-ID.VLAN-ID*, for example *2.100* for Interface ID 2 and VLAN ID 100.
Virtual Resource	The Virtual Resource associated with the interface. Select the same Virtual Resource in the properties of the Virtual Firewall element to add the Virtual Security Engine to the Master Engine. See Creating New Virtual Security Engines (page 457). Only one Virtual Resource can be selected for each VLAN Interface.

Table 7.4 VLAN Interface Properties - General Tab (Continued)

Option	Explanation
Throughput (*Optional*)	The maximum throughput for the Virtual Engines that use this VLAN Interface. Enter the throughput as kilobits per second (for example, 2048). If throughput is defined for the Physical Interface to which the VLAN Interface belongs, the throughput value is automatically inherited from the Physical Interface properties. **Caution!** The throughput for each VLAN Interface must not be higher than the throughput for the Physical Interface to which the VLAN Interface belongs. The throughput is for uplink speed (outgoing traffic) and typically must correspond to the speed of an Internet link (such as an ADSL line), or the combined speeds of several such links when they are connected to a single Physical Interface. **Caution!** Make sure you set the interface speed correctly. When the bandwidth is set, the Firewall always scales the total amount of traffic on this interface to the bandwidth you defined. This happens even if there are no bandwidth limits or guarantees defined for any traffic.
MTU (*Optional*)	The MTU (maximum transmission unit) size for Virtual Engines that use this interface. Either enter a value between 400-65535 or select a common MTU value from the list. **Caution!** The MTU for each VLAN Interface must not be higher than the MTU for the Physical Interface to which the VLAN Interface belongs. The default value (also the maximum standard MTU in Ethernet) is 1500. Do not set a value larger than the standard MTU unless you know that all the devices along the communications path support it.

4. Click **OK**. The specified VLAN ID is added to the Physical Interface.
5. Repeat from Step 2 to add further VLANs on the same or other Physical Interfaces.

What's Next?

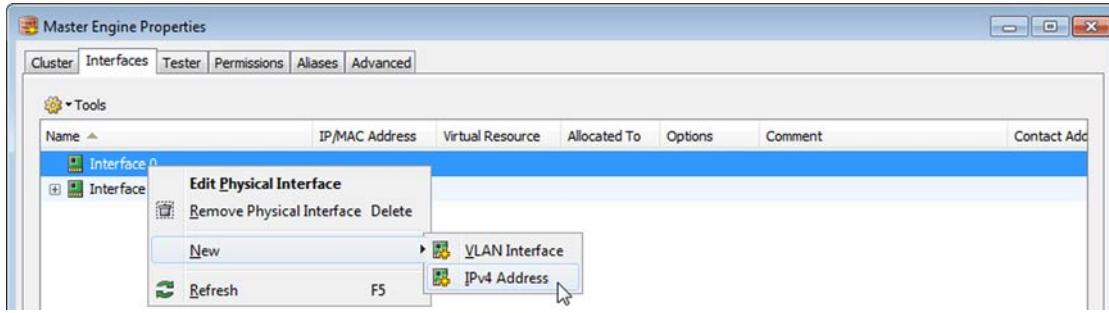
- Add IP addresses to the VLAN Interfaces used for Master Engine communications as instructed in Adding IPv4 Addresses for Master Engines (page 83).

Adding IPv4 Addresses for Master Engines

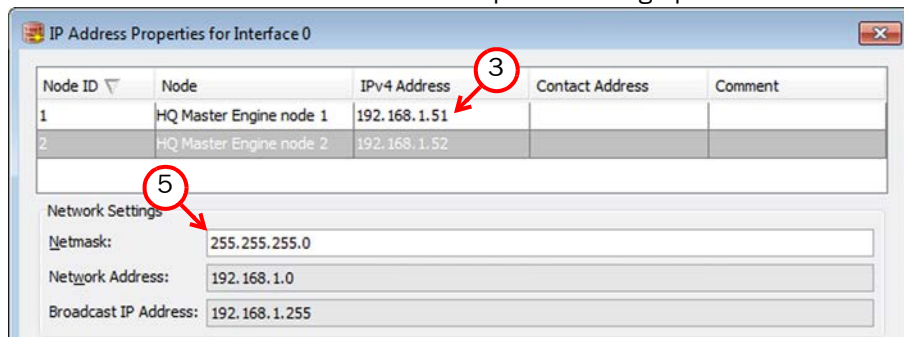
You can add several IPv4 addresses to each Physical Interface or VLAN Interface that does not have a Virtual Resource associated with it.

▼ To add IPv4 addresses for a Master Engine

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



2. Right-click a Physical Interface and select **New→IPv4 Address** or a VLAN Interface and select **New IPv4 Address**. The IP Address Properties dialog opens.



Note – If you use VLAN Interfaces, you must add the IPv4 Addresses to the VLAN Interfaces.

3. Enter the **IPv4 Address** for each node.
4. If necessary, double-click the **Contact Address** field and define the contact address(es).
   - Enter the **Default** contact address. The default contact address is used by default whenever a component that belongs to another Location connects to this interface.
   - If components from some Locations cannot use the Default contact address, click **Exceptions** to define Location-specific contact addresses.
5. Check the automatically filled-in **Netmask** and adjust it as necessary.
6. Click **OK**. Repeat from Step 2 to add IPv4 addresses to the same or other interfaces.

What's Next?

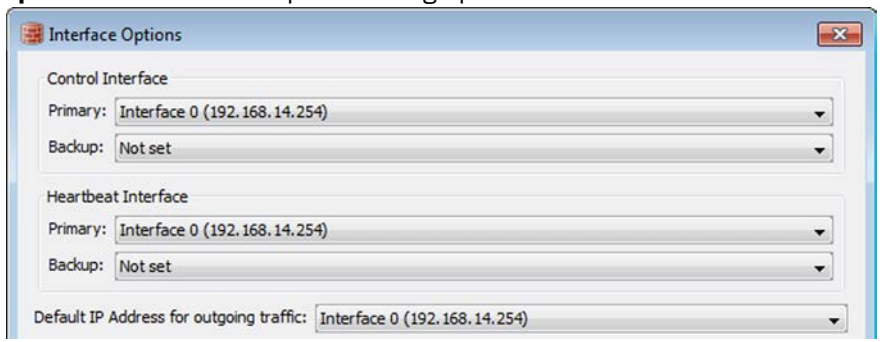
- If you want to change the roles the different interfaces have in the configuration, proceed to Setting Global Interface Options for Master Engines (page 84).
- Otherwise, proceed to Adding a Virtual Firewall Element (page 85).

Setting Global Interface Options for Master Engines

The Interface Options dialog contains the settings for selecting which IP addresses are used in particular roles in system communications (for example, in communications between the Master Engine and the Management Server). Only IPv4 addresses are used in system communications.

▼ To set global interface options for a Master Engine

1. Click **Options**. The Interface Options dialog opens.



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

Table 7.5 Master Engine Interface Options

Option	Explanation
Control Interface	Select the **Primary** Control Interface for Management Server contact.
	(*Optional*) Select a **Backup** Control Interface that is used if the Primary Control Interface is not available.
Heartbeat Interface	Select the **Primary** Heartbeat Interface for communications between the nodes. We recommend that you use a Physical Interface, not a VLAN Interface. We strongly recommend that you do not direct any other traffic through this interface. A dedicated network helps ensure reliable and secure operation. **Caution!** Primary and Backup Heartbeat networks exchange confidential information.
	Select a **Backup** Heartbeat Interface that is used if the Primary Heartbeat Interface is unavailable. It is not mandatory to configure a Backup Heartbeat Interface, 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. **Caution!** Primary and Backup Heartbeat networks exchange confidential information.
Default IP Address for Outgoing Traffic	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 IP Address. You must select an interface that has an IP address defined for all nodes.

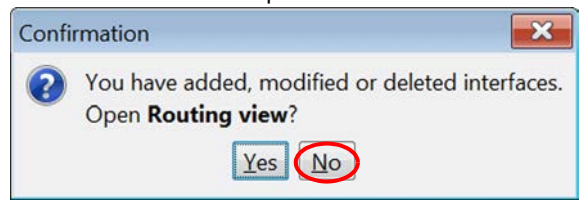
3. Click **OK**.

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

- "C" and "c" are the Primary and Secondary Control Interfaces
- "H" and "h" are the Primary and Secondary Heartbeat Interfaces
- "O" is the default IP address for outgoing traffic

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

4. Click **OK** to close the Firewall Cluster Properties. A Confirmation dialog opens. Click **No**.



What's Next?

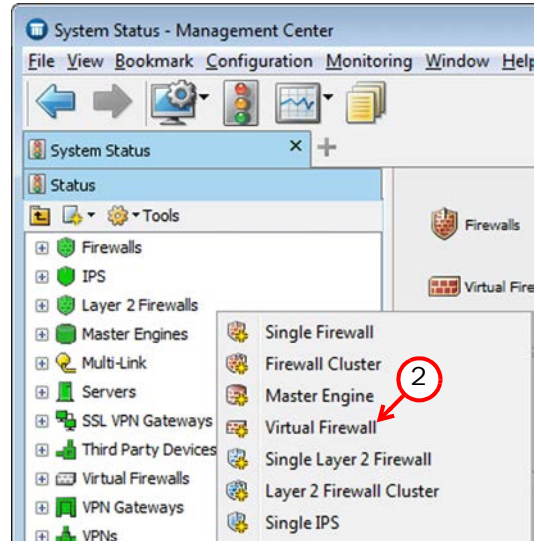
▶ Adding a Virtual Firewall Element

Adding a Virtual Firewall Element

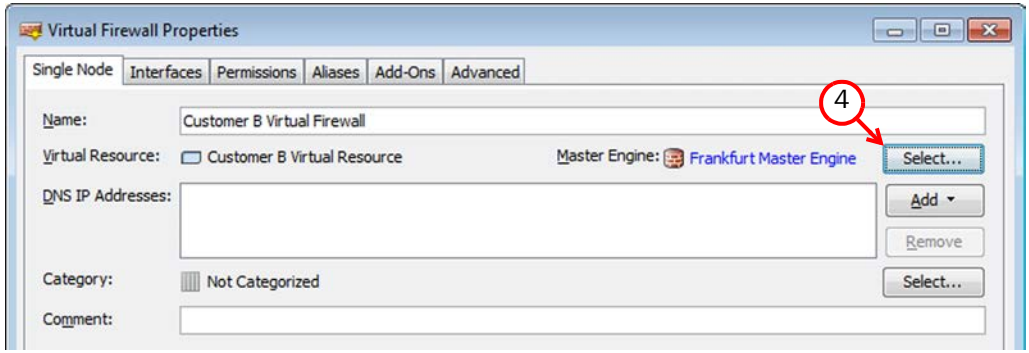
This section covers the basic configuration of a Virtual Firewall element. For information on all the options, see the *Stonesoft Administrator's Guide* or the Management Client *Online Help.*

▼ To create a Virtual Firewall element

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



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



3. Give the element a unique **Name**.
4. Click **Select** and select a Virtual Resource on the Master Engine to which you want to add the Virtual Firewall.

What's Next?

- If you want to modify the automatically-created Physical Interfaces, proceed to Configuring Physical Interfaces for Virtual Firewalls.
- If you want to divide any of the Physical Interfaces into VLANs, continue by Adding VLAN Interfaces for Virtual Firewalls (page 87).
- Otherwise, proceed to Configuring IP Addresses for Virtual Firewalls (page 88).

Configuring Physical Interfaces for Virtual Firewalls

Physical Interfaces for Virtual Security Engines represent interfaces allocated to the Virtual Security Engine in the Master Engine. When you select the Virtual Resource for the Virtual Security Engine, Physical Interfaces are automatically created based on the interface configuration in the Master Engine properties. The number of Physical Interfaces depends on the number of interfaces allocated to the Virtual Security Engine in the Master Engine. You cannot create new Physical Interfaces for Virtual Firewalls. You can optionally modify the automatically-created Physical Interfaces. For detailed instructions, see the *Stonesoft Administrator's Guide* or the Management Client *Online Help*.

The Interface ID of the Virtual Firewall Physical Interface automatically maps to a Physical Interface or VLAN Interface on the Master Engine. The mapping can optionally be changed in the properties of the Virtual Resource associated with the Virtual Security Engine.

What's Next?

- If you want to divide any of the Physical Interfaces into VLANs, continue by Adding VLAN Interfaces for Virtual Firewalls (page 87).
- Otherwise, proceed to Configuring IP Addresses for Virtual Firewalls (page 88).

Adding VLAN Interfaces for Virtual Firewalls

VLAN Interfaces can only be added for Virtual Firewalls if the creation of VLAN Interfaces for Virtual Firewalls is enabled in the Master Engine Properties. VLANs divide a single physical network link into several virtual links. The maximum number of VLANs for a single Physical Interface is 4094. The VLANs must also be defined in the configuration of the switch/router to which the interface is connected.

Note – You cannot add VLAN Interfaces on top of other VLAN Interfaces. Depending on the configuration of the Master Engine that hosts the Virtual Firewall, you may not be able to create valid VLAN Interfaces for the Virtual Firewall. See **Adding a Master Engine Element (page 74).**

▼ To add a VLAN Interface for a Virtual Firewall

1. Switch to the **Interfaces** tab.
2. Right-click a Physical Interface and select **New→VLAN Interface**. The VLAN Interface Properties dialog opens.
3. Enter the **VLAN ID** (1-4094). The VLAN IDs you add must be the same as the VLAN IDs that are used in the switch at the other end of the VLAN trunk.
   - Each VLAN Interface is identified as **`Interface-ID.VLAN-ID`**, for example **`2.100`** for Interface ID 2 and VLAN ID 100.
4. Click **OK**. The specified VLAN ID is added to the Physical Interface.
5. (*Optional*) Repeat the steps above to add further VLAN Interfaces.

What's Next?

▶ Proceed to Configuring IP Addresses for Virtual Firewalls (page 88).

Configuring IP Addresses for Virtual Firewalls

A Physical Interface or VLAN Interface on a Virtual Firewall can have multiple IPv4 and IPv6 addresses.

Adding IPv4 Addresses for Virtual Firewalls

▼ To add an IPv4 address for a Virtual Firewall

1. In the properties dialog for the Virtual Firewall, switch to the **Interfaces** tab.
2. Right-click a Physical Interface or VLAN Interface and select **New→IPv4 Address**. The IP Address Properties dialog opens.

Note – If you use VLAN Interfaces, you must add the IPv4 addresses to the VLAN Interfaces.

3. Enter the **IPv4 Address**.
4. If necessary, define the Contact Address information.
   - Enter the **Default** contact address that is used by when a component that belongs to another Location connects to this interface.
   - If components from some Locations cannot use the Default contact address, click **Exceptions** to define Location-specific contact addresses.
5. Check the automatically filled-in **Netmask** and adjust it as necessary.
6. Click **OK**. Repeat from Step 2 to add further IP addresses.

What's Next?

- ▶ To add IPv6 addresses, proceed to Adding IPv6 Addresses for Virtual Firewalls.
- ▶ Otherwise, proceed to Setting Global Interface Options for Virtual Firewalls (page 89).

Adding IPv6 Addresses for Virtual Firewalls

▼ To add IPv6 addresses for a Virtual Firewall

1. In the properties dialog for the Virtual Firewall, switch to the **Interfaces** tab.
2. Right-click a Physical Interface or VLAN Interface and select **New→IPv6 Address**. The IP Address Properties dialog opens.

Note – If you use VLAN Interfaces, you must add the IPv6 addresses to the VLAN Interfaces.

3. Enter the **IPv6 Address**.
4. Check the automatically filled-in **Prefix Length** and adjust it if necessary by entering a value between 0-128. The Network Address is automatically generated.
5. Click **OK**. Repeat from Step 2 to add further IPv6 addresses.

What's Next?

- ▶ Proceed to Setting Global Interface Options for Virtual Firewalls (page 89).

Setting Global Interface Options for Virtual Firewalls

The Interface Options dialog contains the settings for selecting which IP addresses are used in particular roles. All communication between Virtual Security Engines and the SMC is proxied by the Master Engine. Virtual Security Engines do not have any interfaces for system communications.

▼ To set global interface options for the Virtual Firewall

1. In the properties dialog for the Virtual Firewall, switch to the **Interfaces** tab.
2. Click **Options**. The Interface Options dialog opens.
3. Select the interface options as explained in the table below.

Table 7.6 Virtual Security Engine Interface Options

Option	Explanation
Identity for Authentication Requests	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 external authentication server. The IP address is used only as a parameter inside the authentication request payload to give a name to the request sender.
Source for Authentication Requests	By default, the source IP address for authentication requests is selected according to routing. If the authentication requests are sent to an external authentication server over VPN, select the interface that you want use for the authentication requests. If you use the 5.4 Authentication Server component for authenticating the users, this setting does not have any effect.
Default IP Address for Outgoing Traffic	This option defines the IP address that the nodes use if they have to initiate connections (system communications, ping, etc.).

4. Click **OK**.

What's Next?

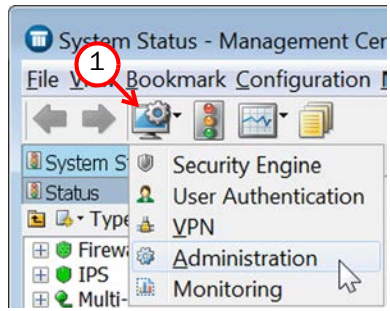
- If the Security Engine licenses for the Master Engine were generated based on the POL code of the Management Server (instead of the Master Engine's POS code), proceed to Binding Engine Licenses to Correct Elements (page 90).
- Otherwise, you are ready to transfer the configuration to the physical Master Engine nodes. Proceed to Saving the Initial Configuration (page 91).

Binding Engine Licenses to Correct Elements

Licenses are created based on the Management Server's proof-of-license (POL) code or based on the appliance's proof-of-serial (POS) code. You must manually bind Management Server POL-bound licenses to a specific Master Engine element. POS-bound appliance licenses are automatically bound to the correct Master Engine element when the engine is fully installed. Virtual Security Engines do not require a separate license.

▼ To bind a Management Server POL-bound license to a Master Engine Node

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



2. Browse to **Licenses→Security Engines**. All imported licenses appear in the right panel.
3. Right-click a Management Server POL-bound license 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 Server POL-bound licenses to all the Master Engine nodes.

Caution – When you install or refresh the policy on the engine, the license is permanently bound to that engine. Permanently-bound licenses cannot be re-bound to another engine without re-licensing or deleting the engine element the license 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 Master Engine nodes. Proceed to Saving the Initial Configuration (page 91).

CHAPTER 8

SAVING THE INITIAL CONFIGURATION

This chapter explains how to save a Firewall or Master Engine element configuration in the Management Center and how to transfer it to the physical engines. No initial configuration is needed for Virtual Firewalls.

The following sections are included:

Configuration Overview

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

You must complete the following steps:

1. Save the initial configuration in the Management Client. See Saving the Initial Configuration.
2. Transfer the initial configuration to the physical engines. See Transferring the Initial Configuration to the Engines (page 97).

Saving the Initial Configuration

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

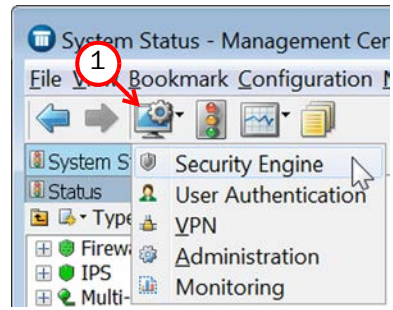
There are four ways to initialize your engines and establish contact between them and the Management Server:

- 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 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.

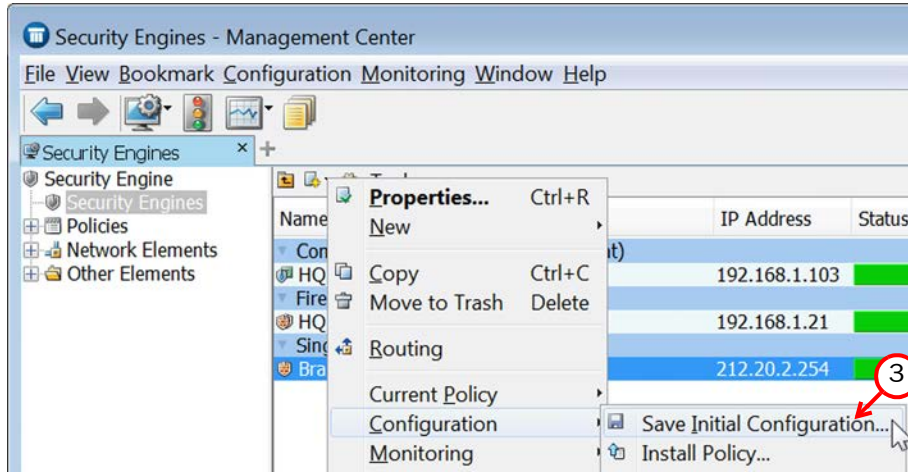
Note – Automatic configuration using a USB stick is primarily intended to be used with Stonesoft appliances, and may not work in all other environments. Uploading the initial configuration to the Stonesoft Installation Server can only be used with Stonesoft appliances and proof-of-serial codes.

▼ To save the initial configuration

1. Click the Configuration icon in the toolbar and select **Security Engine**. The Security Engine Configuration view opens.



2. Select **Security Engines**. A list of Security Engines opens.



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

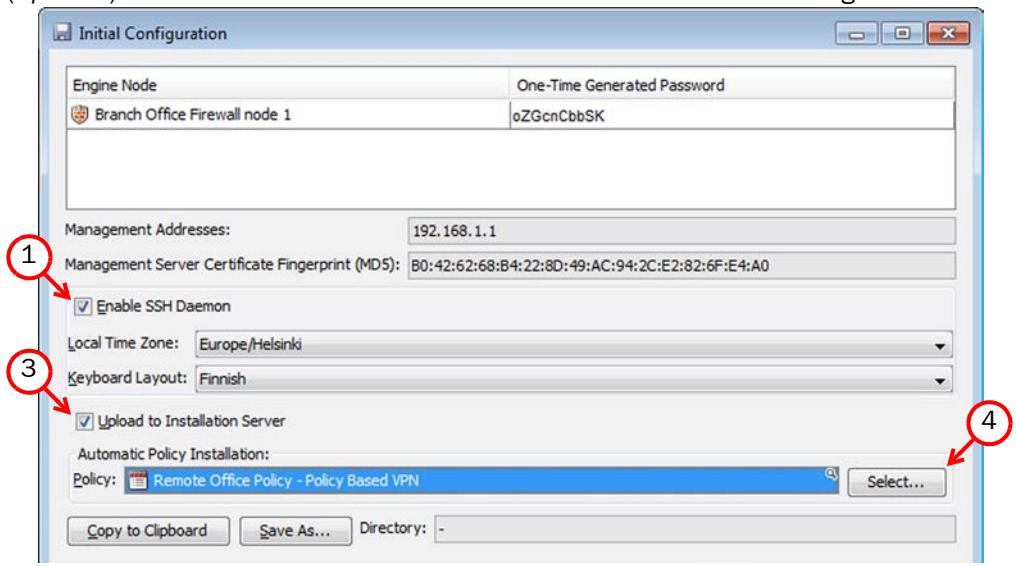
What's Next?

- If you want to use plug-and-play configuration, proceed to Preparing for Plug-and-Play Configuration (page 94).
- If you want to use automatic configuration, proceed to Preparing for Automatic Configuration (page 95).
- If you want to use the Configuration Wizard, proceed to Preparing for Configuration Using the Configuration Wizard (page 96).

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 engine is fully configured, SSH access can be set on or 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 finished. Make sure your Access rules allow SSH access to the engines from the administrators' IP addresses only.

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.

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 or Master Engine. The selected policy is automatically installed on the engine after the engine has contacted the Management Server.
5. Click **OK**.

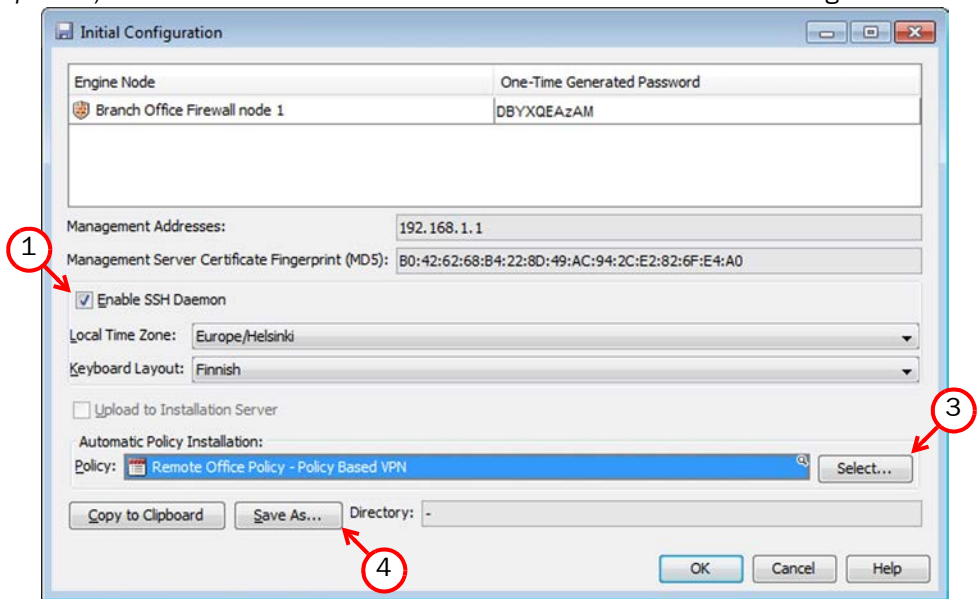
What's Next?

▶ Transferring the Initial Configuration to the Engines (page 97)

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 engine is fully configured, SSH access can be set on or 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 finished. Make sure your Access rules allow SSH access to the engines from the administrators' IP addresses only.

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.

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. *(Optional)* Click **Select** and select the appropriate policy if you already have a policy you want to use for the Firewall or Master Engine. The selected policy is automatically installed on the engine after the engine 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**.

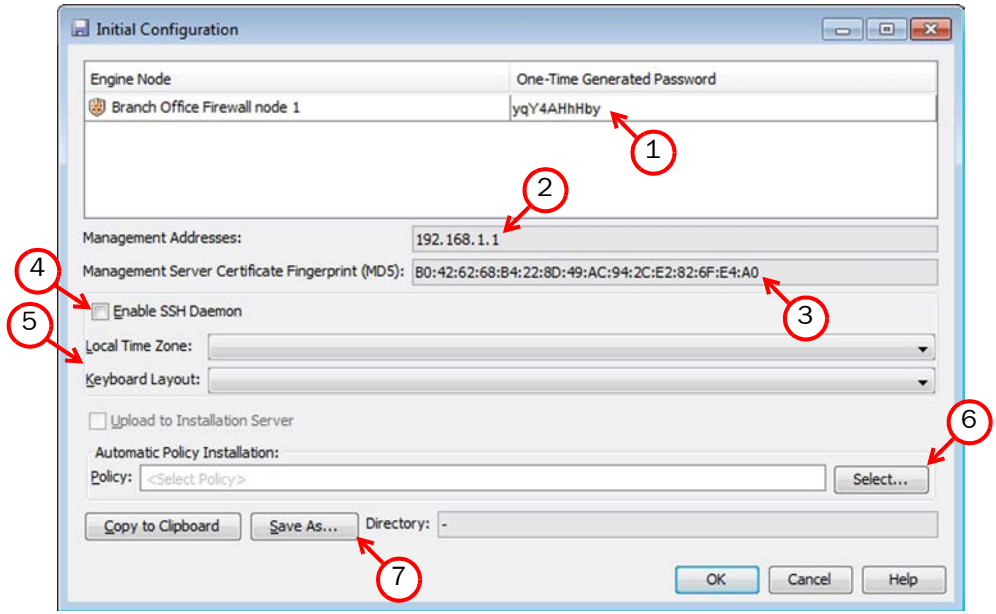
What's Next?

▶ Transferring the Initial Configuration to the Engines (page 97)

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.



2. If you plan to enter the information manually, write down or copy the **Management Addresses**.
3. (*Optional*) If you plan to enter the information manually, write down or copy the **Management Server Certificate Fingerprint** for additional security.
4. *(Optional)* If you plan to import the configuration in the Engine Configuration Wizard, 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 engine is fully configured, SSH access can be set on or 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 finished. Make sure your Access rules allow SSH access to the engines from the administrators' IP addresses only.

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. *(Optional)* If you plan to import the configuration in the Configuration Wizard, select the **Local Time Zone** and **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.
6. *(Optional)* Click **Select** and select the appropriate policy if you already have a policy you want to use for the Firewall or Master Engine. The selected policy is automatically installed on the engine after the engine has contacted the Management Server.
7. 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.

8. Click **OK**.

What's Next?

- Transferring the Initial Configuration to the Engines

Transferring the Initial Configuration to the Engines

You are now ready to install the 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 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 99) or see the more detailed instructions in the Management Client *Online Help* or the *Stonesoft Administrator's Guide*.
- If you want to use another type of device as the engine, proceed to Installing the Engine on Other Platforms (page 119).

CHAPTER 9

DEFINING ROUTING AND BASIC POLICIES

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

The following sections are included:

Defining Routing

Routing is configured entirely through the Management Client. For the most part, this information is automatically filled in according to the interfaces defined for each engine. You must add the following routes:

- The default route that packets to any IP addresses not specifically included in the routing configuration takes. The default route should always lead to the Internet if the site has Internet access.
- Routes through next-hop gateways to networks that are not directly connected to the engine.

Routing is most often configured using the following elements:

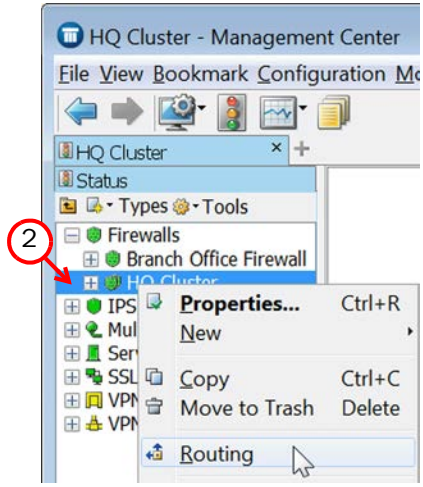
- **Network** elements: represent a group of IP addresses.
- **Router** elements: represent next-hop routers that are used for basic (non-Multi-Link) routing and to represent the ISP routers inside NetLink elements.
- **NetLink** elements: represent next-hop routers that are used for *Multi-Link* routing. 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.

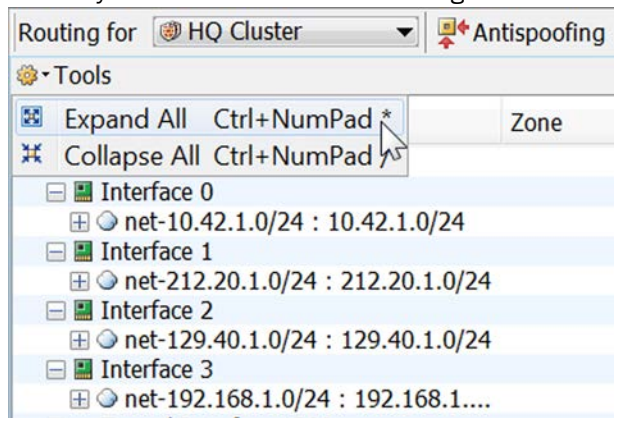
The engine's interfaces and their network definitions have been automatically added to the Routing view. As interfaces that belong to an aggregated link have the same network definitions, only the first interface selected for the aggregated link is shown in the list of interfaces.

▼ To access routing information

1. Select **Monitoring→System Status**.
2. Right-click the Firewall, Master Engine, or Virtual Firewall element and select **Routing**. The Routing view for the selected engine 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. 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 Policy defines which connections are allowed. All other connections are blocked.

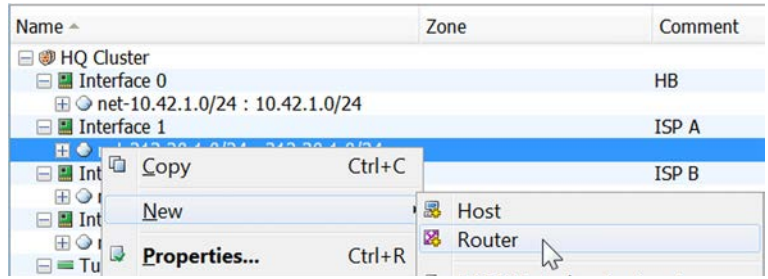
What's Next?

- 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 103).
- Otherwise, proceed to Adding a Default Route with a Single Network Link (page 102).

Adding a Default Route with a Single Network Link

▼ To add a router

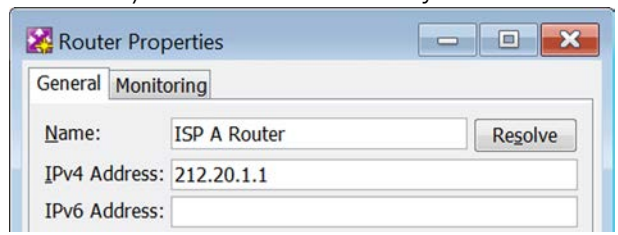
➥ Right-click the Network under the interface to be used as the default route and select **New→Router**.



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. If the interface has a fixed IP address, the Router Properties dialog opens, and you must define the Router properties as explained in the section To define a Router.

▼ To define a Router

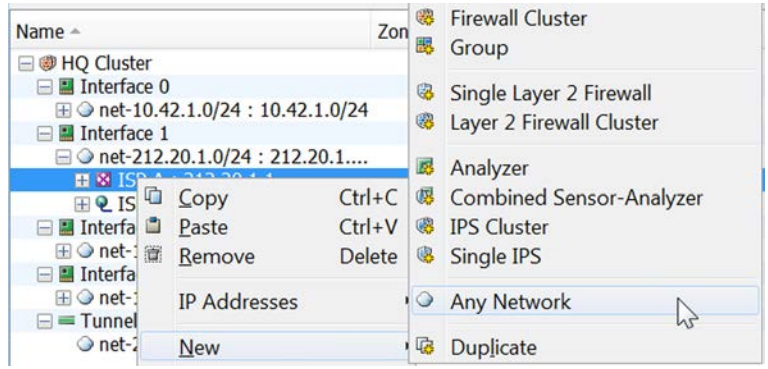
1. Enter a **Name** for the Router.
2. Enter the **IPv4 Address** and/or the **IPv6 Address** of your Internet router.



3. Click **OK**.

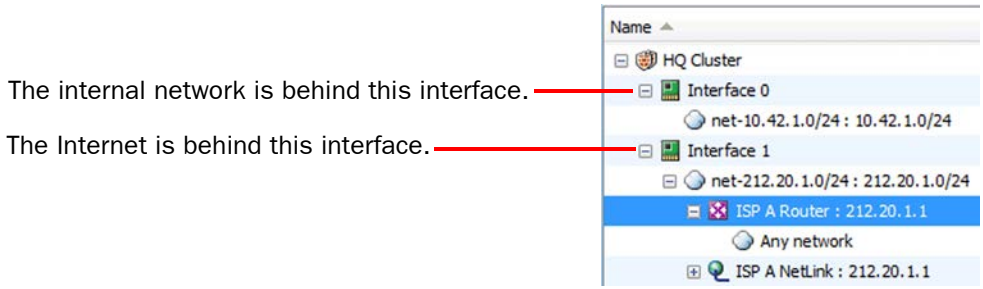
▼ To add the default route for a single network link

➥ 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 engine in the single-link configuration described here.

If you need to insert Any Network more than once, use a Multi-Link configuration instead (see Adding a Default Route With Multi-Link).

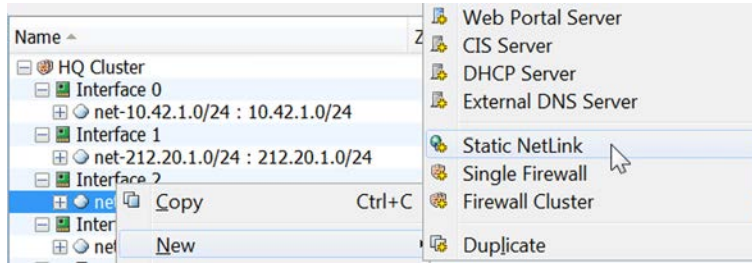


In the illustration above, one internal network is connected to the Internet through the Firewall. It makes no difference which interfaces are internal and which are external. The Firewall Policy defines which traffic is allowed.

Adding a Default Route With Multi-Link

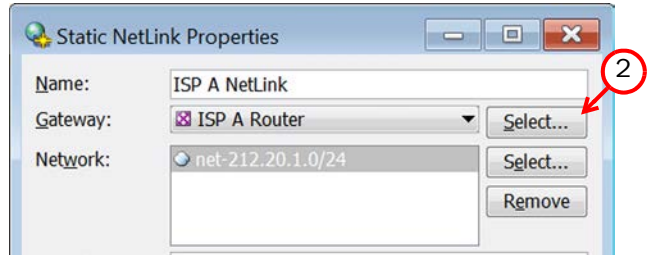
▼ To create a NetLink

➥ 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.

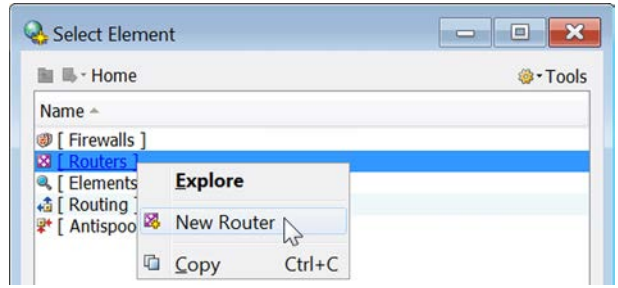


▼ To define a NetLink

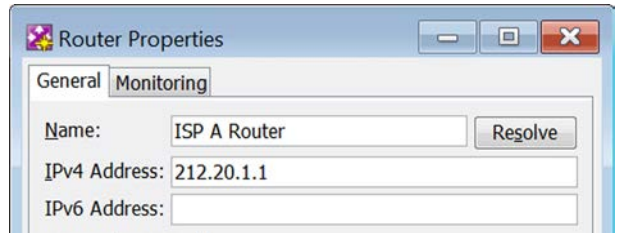
1. Enter a **Name** for the NetLink.
   - If you are defining a Dynamic NetLink, continue by defining the rest of the NetLink Properties as described in the section To define the remaining NetLink properties (page 106).



2. (*Static NetLink only*) Click **Select** for **Gateway**.

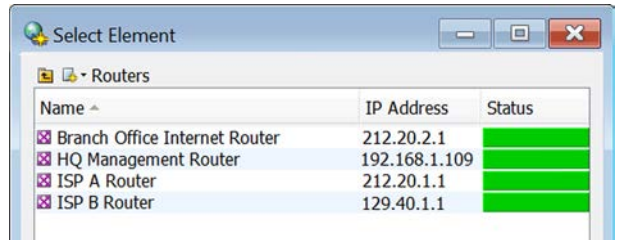


3. Right-click **Routers** and select **New Router**.



4. Enter a **Name** for the Router.
5. Enter the **IPv4 Address** and/or the **IPv6 Address** of the Internet router for this NetLink.
6. Click **OK**.

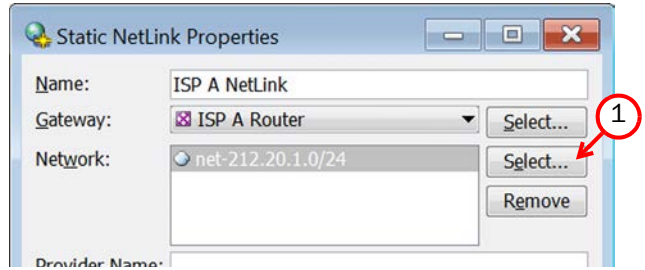
Create a **Router** element for all Static NetLinks in the same way, so that they are ready in the system when you create the other Static NetLinks.



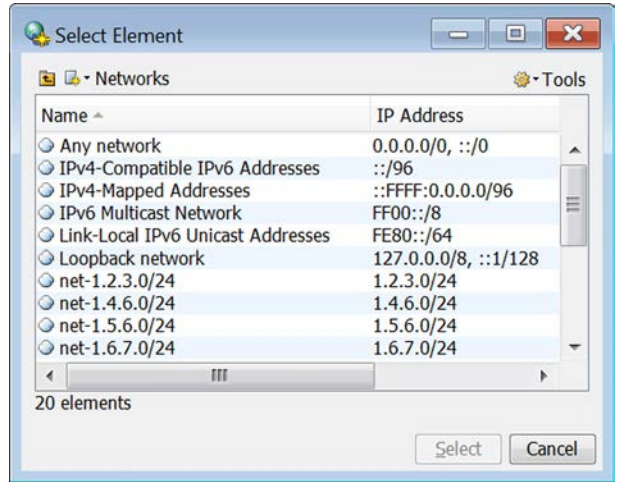
7. From the Router list that opens, select the correct Router and click **Select**.

▼ To add a Network

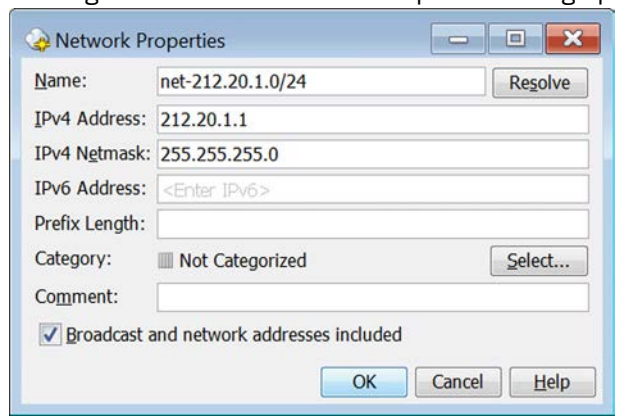
1. Click **Select** for **Network**.



2. Open **Networks**. The existing elements are listed.

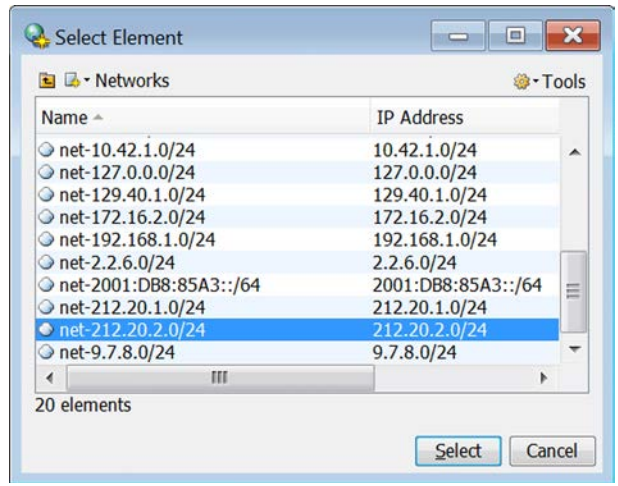


3. Select the correct Network(s) and proceed to the section To define the remaining NetLink properties (page 106).
   - If the correct Network(s) are not on the list, create a new Network element by clicking the New icon and selecting **Network**. The Network Properties dialog opens.



4. Enter a **Name** for the Network.
5. Enter the **IPv4 Address** and the **Netmask** and/or the **IPv6 Address** and the **Prefix Length** (0-128).
6. (*Optional*) Select **Broadcast and network addresses included** to include broadcast and network addresses in the Network.

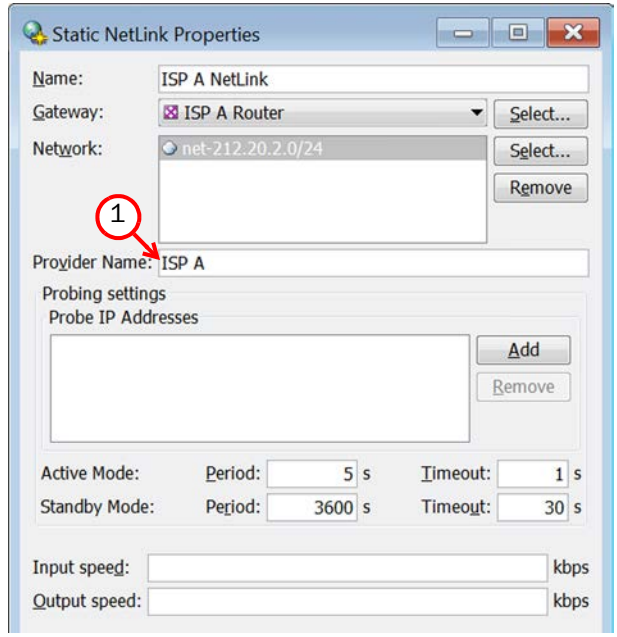
7. Click **OK**.



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.



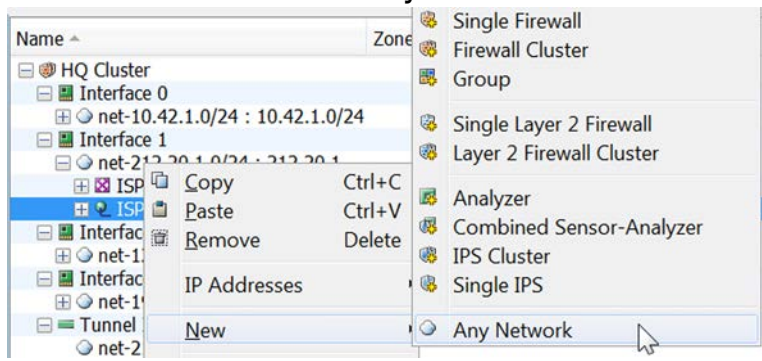
- **Probing Settings**, **Input Speed,** and **Output Speed** are used for specific Multi-Link features that are explained in the other guidebooks and the Management Client *Online Help*. Leave these empty for now.

2. Click **OK**.

Define all the necessary NetLinks in the same way, then use the NetLinks to define the default route to the Internet.

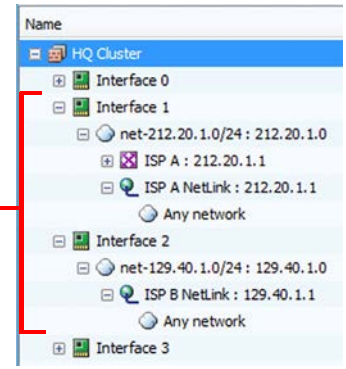
▼ To add the default route for Multi-Link

➥ 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”.

The Internet is behind these interfaces.



In the illustration above, internal networks are connected to the Internet using two Internet connections. It makes no difference which interfaces are internal and which are external. The Firewall Policy defines 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 *Stonesoft Administrator's Guide* or the Management Client *Online Help*.

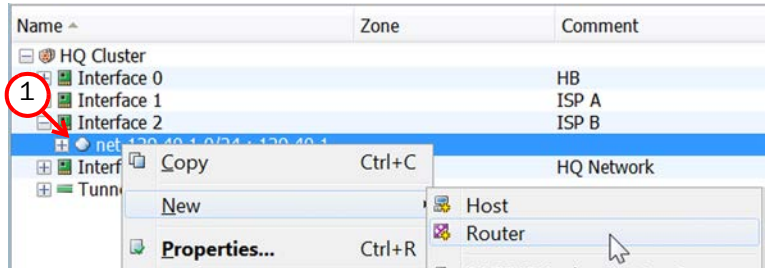
Defining Other Routes

The networks that are directly connected to the engine 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.

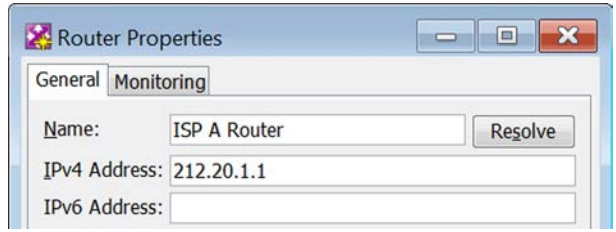
Usually, non-ISP routes use a single-link configuration, as explained below, but a Multi-Link configuration can be used instead if there are alternative links to the same network. If that is the case, add the routes using NetLinks instead of Router elements in a similar way as with the default route (see Adding a Default Route With Multi-Link (page 103)).

▼ 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.



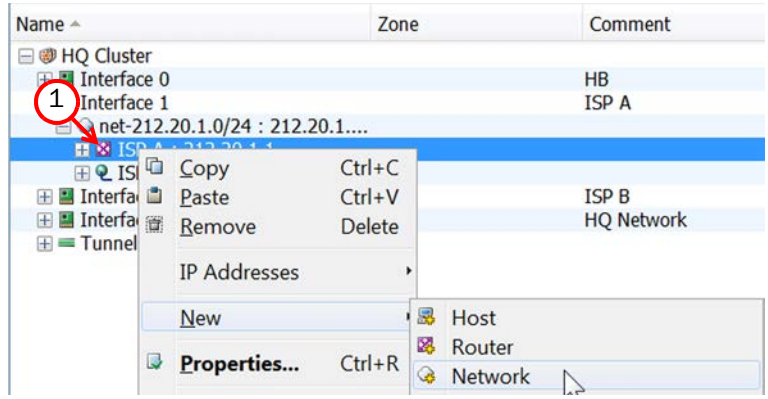
2. Enter a **Name** for the Router.
3. Enter the **IPv4 Address** and/or the **IPv6 Address** of the gateway device that connects the networks.



4. Click **OK**.

▼ To add networks

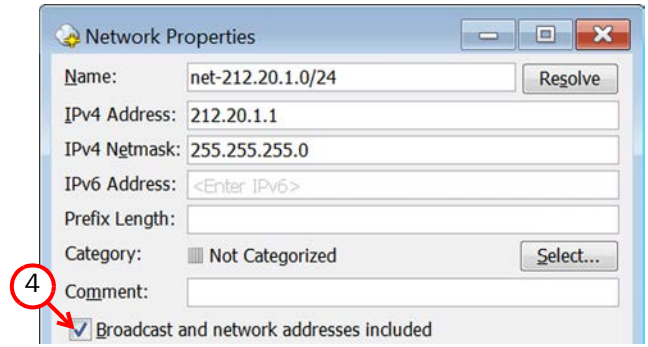
1. Right-click the Router you just added and select **New→Network**.



- 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 engines. 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 (page 110).

Using IP Address Count Limited Licenses

If you have a license that is based on a restriction of 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 engine.

▼ 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

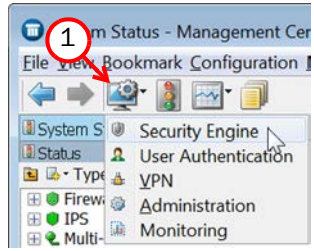
The final step in getting your engine up and running is creating the rules according to which the traffic is inspected. In addition to the rules in the policy, the other configuration information is also transferred to the engine when you install a policy on it (including the interface definitions and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

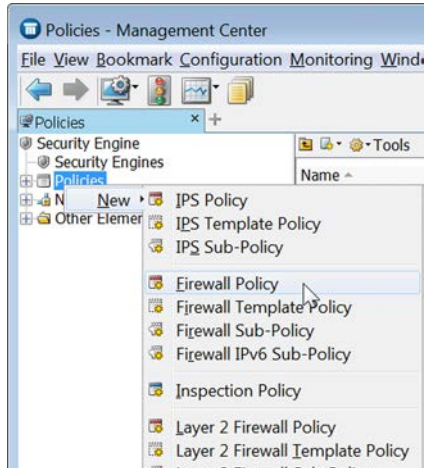
If you installed a policy automatically during the initial configuration, you can proceed directly to Commanding Engines Online (page 115).

▼ To create a policy

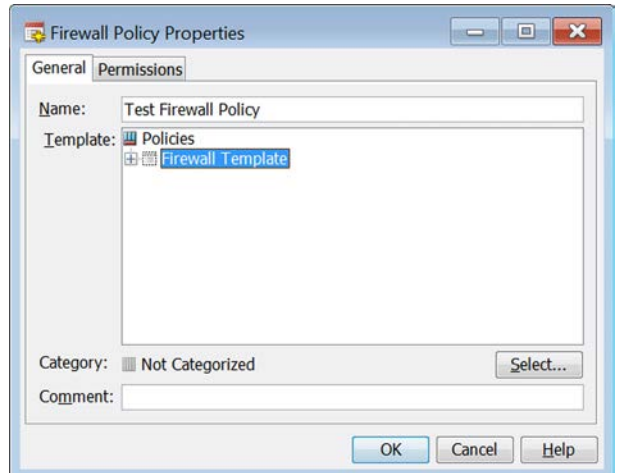
1. Click the Configuration icon in the toolbar and select **Security Engine**. The Security Engine Configuration view opens.



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



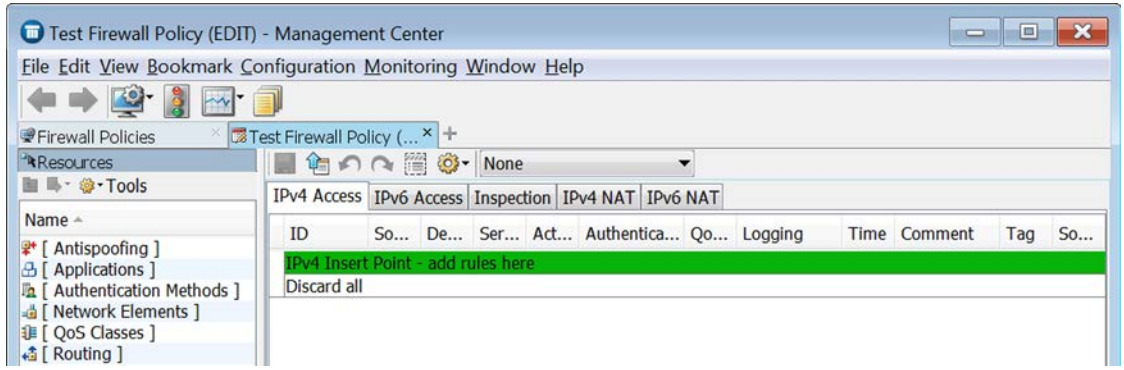
3. **Name** the new Policy.
4. Select a template. Only the **Firewall Template** is available, as you have not created your own templates yet.



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

▼ To add a rule

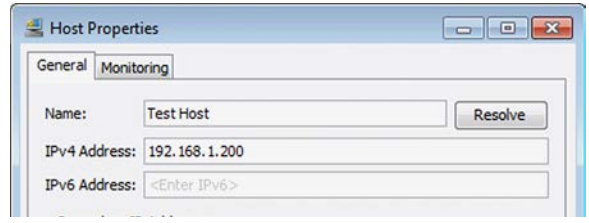
➥ Double-click the green row, or right-click the row and select **Rule→Add Rule**.



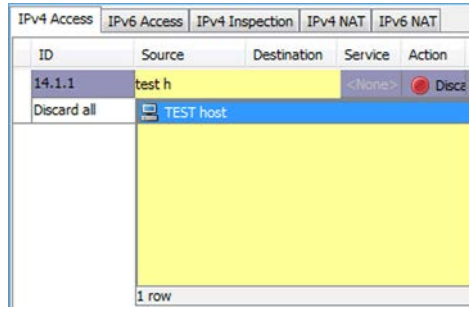
Note – Inherited rules are not editable in the policy that inherits the rules.

▼ To configure a ping rule

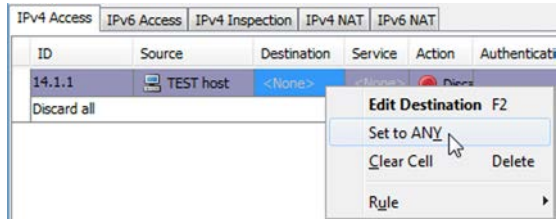
1. Right-click **Network Elements** and select **New→Host**. The Host Properties dialog opens.
2. Enter a **Name** and the **IPv4 Address** of the Host.



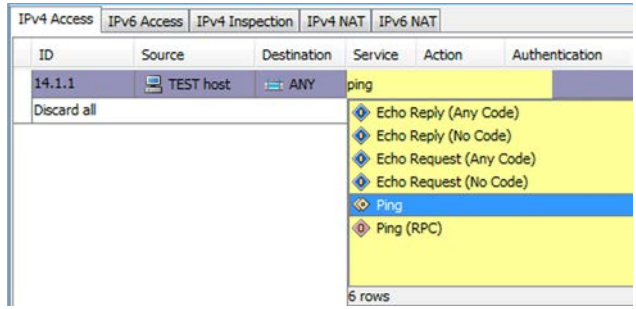
3. Click **OK**.



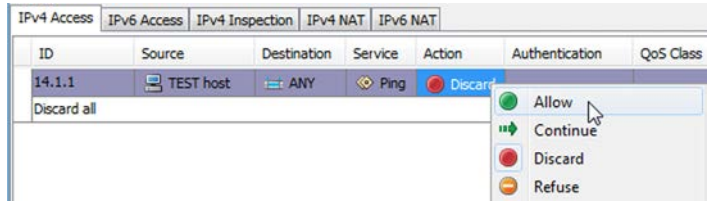
4. Click the Source cell and begin typing **TEST host**. When the correct element is found, select it from the list.



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 engine 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 engine, the connection is blocked.

What's Next?

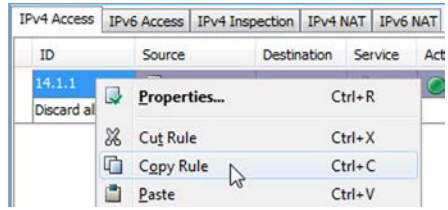
- If you want to ping between a private and a public IP address, add a rule on the **IPv4 NAT** tab to translate the IP address as explained in Adding a NAT Rule for the Example Ping Rule.
- If you do not want to create NAT rules now, proceed to Installing the Policy (page 114).

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

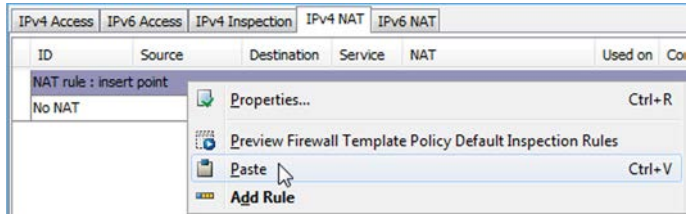
Adding a NAT Rule for the Example Ping Rule

To add a NAT rule

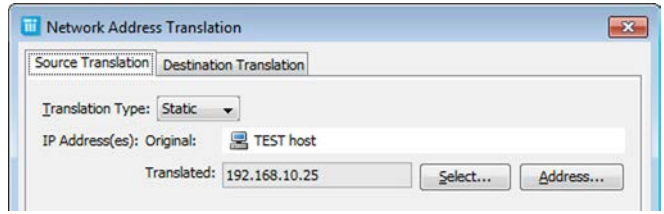
1. Right-click the IPv4 Access rule you just created and select **Copy Rule**.



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.

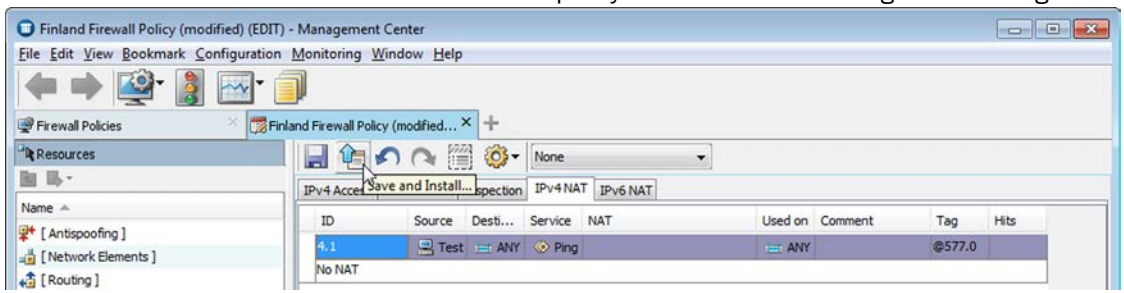
7. Click **OK**.

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.

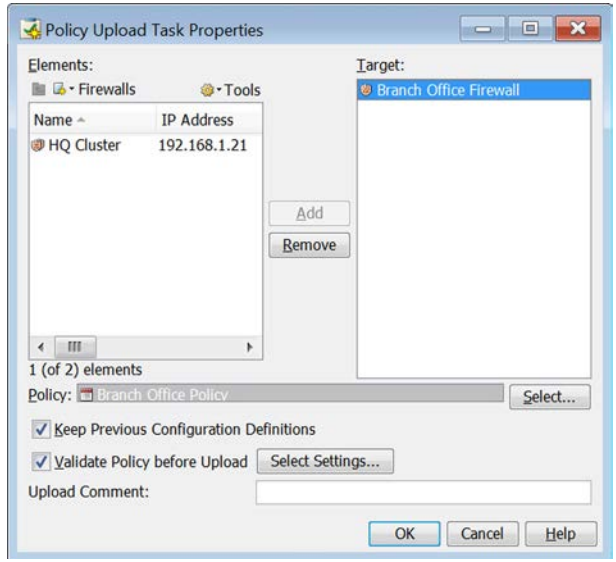
Installing the Policy

▼ To install the Firewall policy

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



2. Select the correct engine.
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 engine's other configuration information (including interface definitions and routing information) are transferred to the engine. If you validate the rules and the routing configuration at policy installation, the

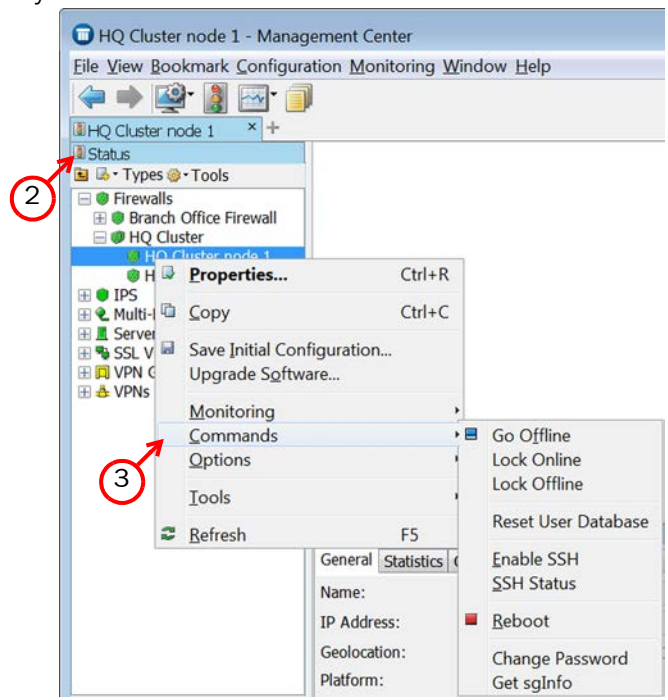
issues found in the policy are displayed in a separate panel in the tab that opens to show the progress of the policy installation. See the Management Client *Online Help* or the *Stonesoft Administrator's Guide* for more information on policy validation.

Commanding Engines Online

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

▼ To check system status and issue commands to engines

1. Switch to the System Status view.



2. Check the status of the engines and SMC on the **Status** tab.
   - You can select an element 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 engines at once.

This concludes the configuration instructions in this *Installation Guide*. To continue setting up your system, see the Management Client *Online Help* or the *Stonesoft Administrator's Guide*, 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:

CHAPTER 10

INSTALLING THE ENGINE ON OTHER PLATFORMS

This chapter describes how to install the Firewall/VPN engine on standard Intel or Intel-compatible platforms, or on a virtualization platform.

The following sections are included:

Installing the Firewall Engine on Intel-Compatible Platforms

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 DVDs. Depending on your order, you may have received ready-made Management Center and Firewall/VPN engine DVDs. If the DVDs 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 DVDs, obtain the files from the Stonesoft web site. See Downloading the Installation Files.
2. Start the installation and select the installation type. See Starting the Installation (page 122).
3. Configure the engines and establish contact with the Management Server. See Configuring the Engine in the Engine Configuration Wizard (page 125).

What's Next?

- If you have ready-made DVDs, proceed to Starting the Installation (page 122).
- Otherwise, start by Downloading the Installation Files.

Downloading the Installation Files

The engine installation files are available at the Stonesoft web site.

1. Go to the Downloads page at https://my.stonesoft.com/download.
2. Download the `.iso` image files.

What's Next?

- Continue by Checking File Integrity (page 121).

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 web site.

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
869aecd7dc39321aa2e0cfaf7fafdb8f sg_engine_1.0.0.1000.iso
```

4. Compare the displayed output to the checksum on the web site. 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.

What's Next?

▶ Continue by Creating the Installation DVD.

Creating the Installation DVD

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

What's Next?

▶ Continue by Starting the Installation (page 122).

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 91) 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 DVD

1. Insert the engine installation DVD 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 133).
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 after the installation finishes. Continue by Configuring the Engine Automatically with a USB Stick (page 124).
- Otherwise, remove the DVD 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 125).

Installing the Firewall Engine on a Virtualization Platform

The firewall engine can be installed on virtualization platforms that support the deployment of Open Virtual Format (OVF) templates. When the firewall engine is installed on a virtualization platform, the following requirements and restrictions apply:

- A minimum of one virtual network interface is required.
- Only Packet Dispatching CVI mode is supported for Firewall Clusters.
- Only Standby clustering mode is supported for Firewall Clusters.
- Heartbeat traffic for Firewall Clusters requires a dedicated non-VLAN-tagged interface.

The same Security Engine software can be used in the Firewall/VPN role, IPS role, or Layer 2 Firewall role. The engine role is selected during the initial configuration of the engine.

▼ To install the firewall engine on a virtualization platform

1. Install the Stonesoft Management Center as instructed in the *Stonesoft Management Center Installation Guide*.
2. (*Recommended*) Create the resource pool where you will import the virtual appliance package and configure it according to your requirements.
3. Download the license from the Stonesoft web site at https://my.stonesoft.com/managelicense.do.
4. Download the virtual appliance package from the Stonesoft web site at https://my.stonesoft.com/download.do.
   - The Stonesoft Security Engine virtual appliance package consists of two files: a compressed disk image file and an OVF file.
   - The OVF file specifies how the virtualization platform creates the appliance and connects it in the virtualized environment.
5. Extract the files from the virtual appliance package.
6. Deploy the OVF template according to the deployment procedure for your virtualization platform.
   - For detailed configuration instructions, see the product documentation for your virtualization platform.
7. Map the networks defined in the OVF template to the networks in your virtualized environment.

What's Next?

▶ Continue by Configuring the Engine in the Engine Configuration Wizard (page 125).

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.

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 Management Client *Online Help* or the *Stonesoft Administrator's Guide* for more information.

▼ 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 DVD 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.

What's Next?

▶ Continue as explained in After Successful Management Server Contact (page 132).

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 Configuration Wizard can be run at any time issuing the `sg-reconfigure` command on the engine command line.

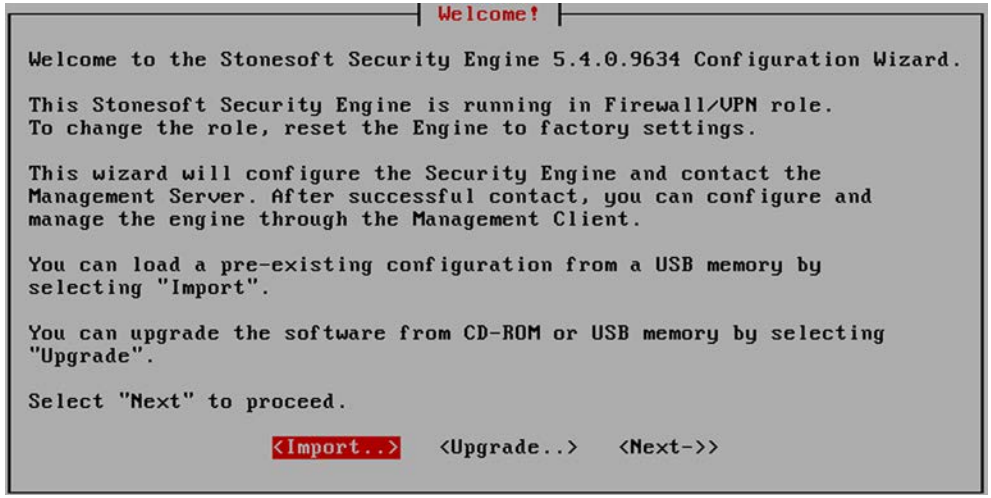
If you have stored the configuration on a USB memory stick, you can import it to reduce the need for typing in information. See Saving the Initial Configuration (page 91) for more information about saving the initial configuration.

▼ 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 126).



▼ 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.

What's Next?

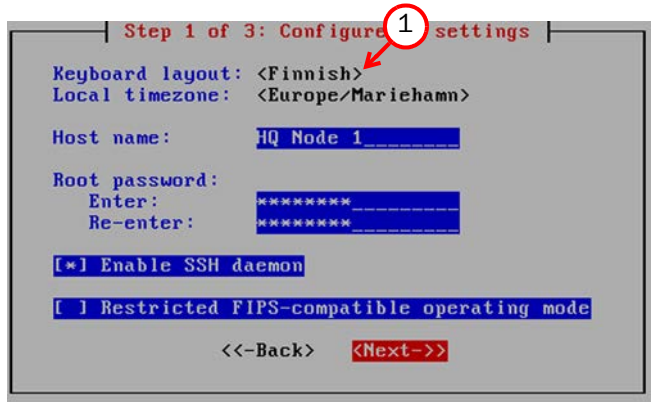
▶ Continue by Configuring the Operating System Settings.

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.

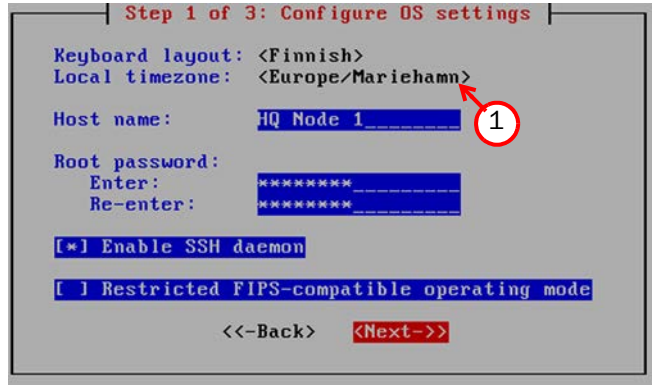


2. Highlight the correct layout and press Enter.
   - If the desired keyboard layout is not available, use the best-matching available layout, or select US_English.

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 – 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.

What's Next?

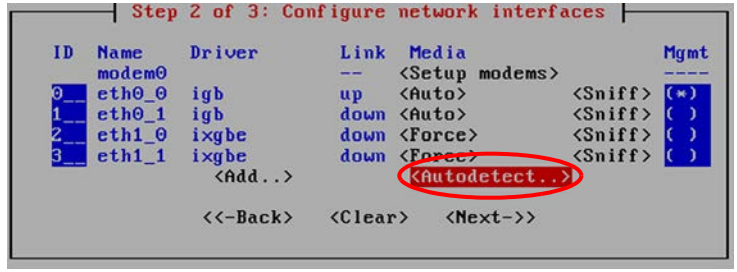
▶ Continue by Configuring the Network Interfaces (page 128).

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.



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

What's Next?

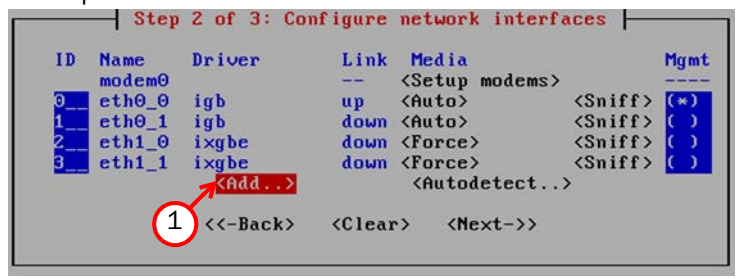
- If there are problems, add the network interfaces manually as explained in Defining Network Interface Drivers Manually (you can overwrite any autodetected setting).
- Otherwise, proceed to Mapping the Interfaces to Interface IDs (page 129).

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

Defining Network Interface Drivers Manually

▼ 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.

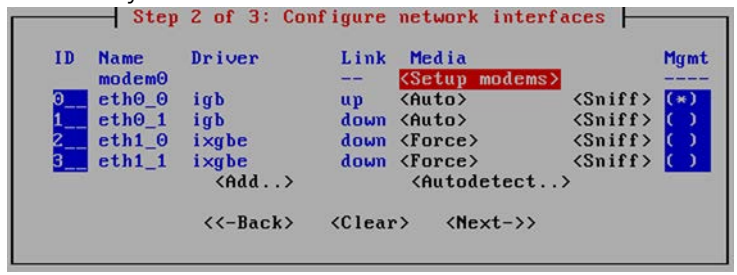
What's Next?

- Repeat as necessary, then map the interfaces to Interface IDs as explained in Mapping the Interfaces to Interface IDs (page 129).

Mapping the Interfaces to Interface IDs

▼ To map the interfaces to Interface IDs

1. Change the **ID**s 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.

Note – The Management interface must be the same interface that is configured as the primary control interface for the corresponding Firewall element in the Management Center. Otherwise the engine cannot contact the Management Center.

4. Highlight **Next** and press Enter to continue.

What's Next?

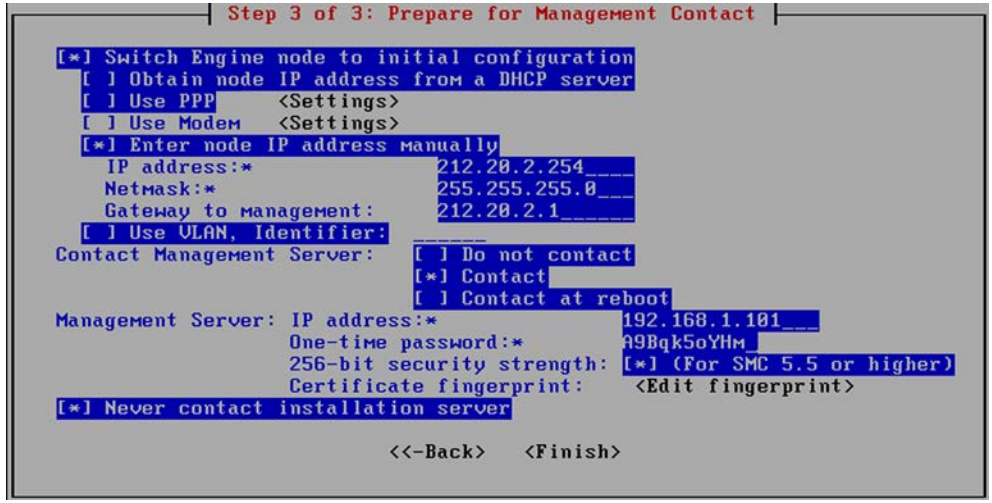
▶ Continue by Contacting the Management Server (page 130).

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 173) 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.

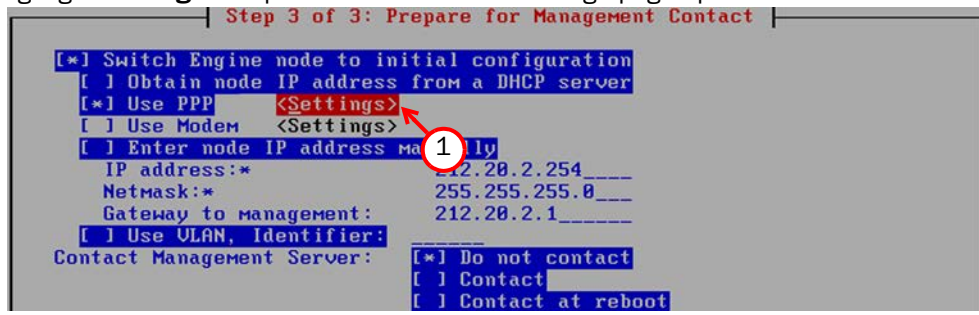


What's Next?

- 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 131).
- If the IP address of the control interface is assigned through PPPoE or PPPoA, select **Use PPP** and continue in To define PPP settings (page 131).
- 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 131).
- 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 PPP settings

1. Highlight **Settings** and press Enter. The PPP 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.

▼ To define modem settings

1. Highlight **Settings** and press Enter. The Modem 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.

▼ 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 (page 92).

1. Select **Contact** or **Contact at Reboot** and press the spacebar.

2. Enter the Management Server IP address and the one-time password.

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.

3. (*Optional*) Select **256-bit Security Strength** and press the spacebar to use 256-bit encryption for the connection to the Management Server. 256-bit encryption must also be enabled for the Management Server. See the *Stonesoft Management Center Installation Guide* for more information.

4. (*Optional*) Highlight **Edit Fingerprint** and press Enter. Fill in the Management Server's certificate fingerprint (also shown when you saved the initial configuration). Filling in the certificate fingerprint increases the security of the communications.
5. 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 173) 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.

What's Next?

▶ Continue as explained in After Successful Management Server Contact.

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 99).

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 DVD. See Installing the Firewall Engine on Intel-Compatible Platforms (page 120).

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 10.1 Partitions for the Engine

Partition	Flags	Partition Type	Filesystem Type	Size	Description
Engine root A	bootable	Primary	Linux	200 MB	The bootable root partition for the Firewall engine.
Engine root B		Primary	Linux	200 MB	Alternative root partition for the Firewall engine. Used for the engine upgrade.
Swap		Logical	Linux swap	Twice the size of physical memory.	Swap partition for the Firewall engine.
Data		Logical	Linux	500 MB or more	Used for the boot configuration files and the root user's home directory.
Spool		Logical	Linux	All remaining free disk space.	Used for spooling.

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.

Allocating Partitions

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

▼ 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 DVD from the machine and press Enter to reboot.

What's Next?

▶ Continue the configuration as described in Configuring the Engine Automatically with a USB Stick (page 124) or Configuring the Engine in the Engine Configuration Wizard (page 125).

UPGRADING

In this section:

Chapter 11

Upgrading

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

The following sections are included:

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. You can then apply it to selected engines through the Management Client. Alternatively, the upgrade can be done on the command line when it is more convenient (for example, for spare appliances in storage).

The engines have two alternative partitions for the engine software. When you install a new software version, the new version is installed on the inactive partition and the current version is preserved to allow rollback if the upgrade is unsuccessful. If the engine is not able to return to operation, the engine automatically rolls back to the previous software version at the next reboot. You can also use the **`sg-toggle-active`** command to roll back to the previous engine version. See Command Line Tools (page 151) for more information.

You can upload and activate the new software separately. For example, you can upload the upgrade during office hours and activate it later 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 communication ports are changed), the new version can use the existing configuration. Any potential version-specific adjustments are made when you refresh the policy after the upgrade.

Limitations

It is not possible to upgrade between 32-bit and 64-bit versions of the software. If you are running the software on a compatible standard server, you can reinstall the software using the other version. In clusters, 32-bit and 64-bit nodes cannot be online simultaneously. Stonesoft appliances support only the software architecture version that they are pre-installed with. Changing the architecture for third-party hardware using software licenses requires a full re-installation using a DVD.

You cannot upgrade Virtual Security Engines directly. To upgrade Virtual Security Engines, you must upgrade the Master Engine that hosts the Virtual Security Engines.

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 or generate a valid configuration for them. A newer Stonesoft Management Center version is compatible with several older engine versions. See the Release Notes at http://www.stonesoft.com/en/customer_care/kb/ 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**.

Before upgrading the engines, read the Release Notes for the new engine version.

Configuration Overview

Proceed as follows with the engine upgrade:

1. *(If automatic download of engine upgrades is not enabled)* Obtain the installation files and check the installation file integrity. See Obtaining Installation Files.
2. (*If you are upgrading engines locally)* Create the installation DVDs from the files with a DVD-burning application that can correctly read and burn the DVD-structure stored in the .iso images.
3. *(If automatic license updates are not enabled)* Update the licenses. See Upgrading or Generating Licenses (page 140).
4. Upgrade the engines one at a time. Confirm that the upgraded engine operates normally before upgrading the next engine. See Upgrading Engines Remotely (page 144) or Upgrading Engines Locally (page 146).

Obtaining Installation Files

If the Management Server is not set up to download engine upgrades automatically or if you want to upgrade engines locally, 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. Go to the Stonesoft Downloads page at https://my.stonesoft.com/download.do.
2. Enter the Proof-of-License (POL) or Proof-of-Serial (POS) code in the **License Identification** field and click **Submit**.
3. Click **Stonesoft Security Engine Downloads**. The Stonesoft Security Engine Downloads page opens.
4. Download the installation file. There are two types of packages available:
   - The .zip file 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 DVD.
   - The .iso download allows you to create a bootable installation DVD for a local upgrade on all supported platforms.
5. Change to the directory that contains the file(s) to be checked.
6. *(Linux only)* Generate a checksum of the file using the command **`md5sum`** *`filename`* or **`sha1sum`** *`filename`*, where *`filename`* is the name of the installation file.
   - For Windows, see the documentation for the third-party checksum program.

Example
```
$ md5sum sg_engine_1.0.0.1000.iso
869aecd7dc39321aa2e0cfaf7fafdb8f sg_engine_1.0.0.1000.iso
```

7. Compare the displayed output to the checksum on the web site.

Caution – Do not use files that have invalid checksums. If downloading the files again does not help, contact Stonesoft 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**.
2. Select the engine upgrade (`sg_engine_`*`version_platform`*`.zip`) file and click **Import**. The status bar at the bottom of the Management Client window shows the progress of the import.

▼ To prepare a downloaded .zip file for a local upgrade

➥ Copy the file to the root directory of a USB memory stick or a DVD.

▼ To prepare a downloaded .iso file for a local upgrade

➥ Create the installation DVD for the engines with a DVD-burning application that can correctly read and burn the DVD-structure stored in the .iso images. If the end result is a DVD file with the original .iso file on it, the DVD 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 144), or Upgrading Engines Locally (page 146) 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 engine up to that particular version. If the first two numbers in the old and the new versions 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). By default, licenses are regenerated and installed automatically. You can also upgrade the licenses at the Stonesoft web site. You can view and download your current licenses online at the Stonesoft License Center at www.stonesoft.com/en/customer_care/licenses/.

What's Next?

- If you do not need to upgrade licenses, proceed to Upgrading Engines Remotely (page 144) or Upgrading Engines Locally (page 146).
- If you need new licenses and you want to upgrade the licenses one at a time, proceed to Upgrading Licenses Under One Proof Code (page 141).
- If you need new licenses and you want to upgrade several licenses at once, Proceed to Upgrading Licenses Under Multiple Proof Codes (page 141).

Upgrading Licenses Under One Proof Code

A license file generated under one proof-of-license (POL) or proof-of-serial (POS) code can contain the license information for several components. You can also use the multi-upgrade form to upgrade the licenses. See Upgrading Licenses Under Multiple Proof Codes.

▼ To generate a new license

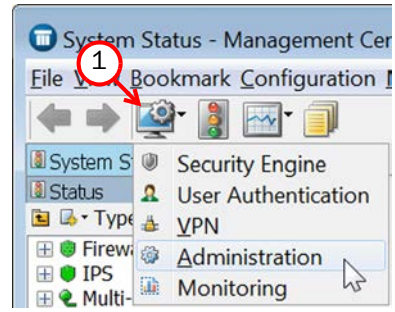
1. Go to the Stonesoft License Center at www.stonesoft.com/en/customer_care/licenses/.
2. Enter the POL or POS code in the **License Identification** field and click **Submit**. The License Center page opens.
3. Click **Update**. The License View page opens.
4. Follow the directions to upgrade the license.

Upgrading Licenses Under Multiple Proof Codes

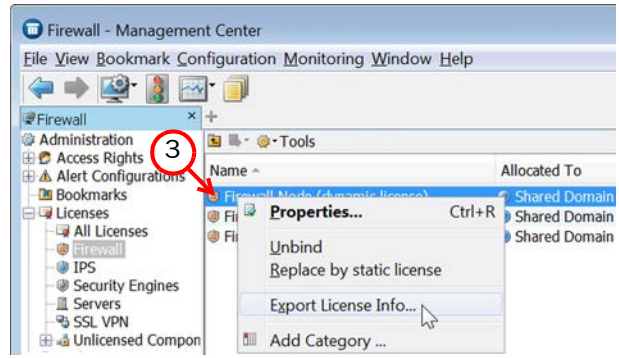
If you have several existing licenses with different proof-of-license (POL) or proof-of-serial (POS) codes that you need to upgrade, you can generate all of the new licenses at the same time.

▼ To upgrade multiple licenses

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

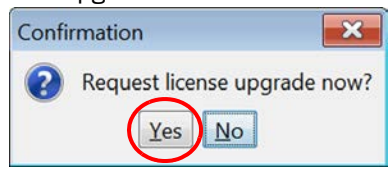


2. Browse to **Licenses→Firewall** or **Licenses→Security Engine** depending on the type of licenses you have.



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**. The Save License Upgrade Request dialog opens.

5. Select the location at which to save the license file in the dialog that opens. You are prompted to request a license upgrade.



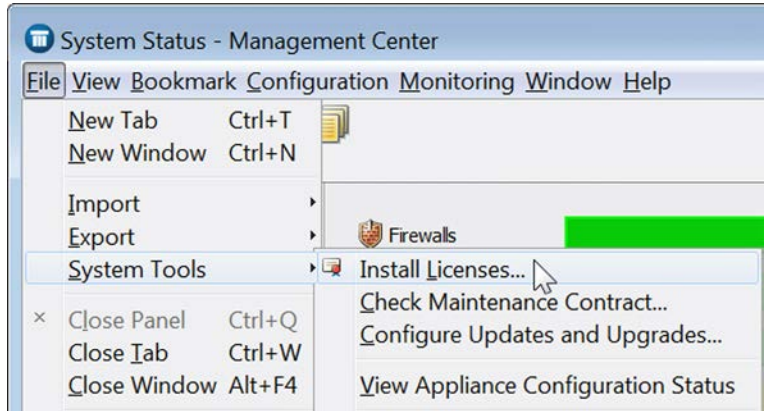
6. Click **Yes**. The Stonesoft web site opens.
7. Browse to **Customer Care→Licenses**.
8. Enter the POL or POS code in the **License Identification** field and click **Submit**. The License Center page opens.
9. Click the **Multi-Upgrade Licenses** link on the right. The Upload Multi-Upgrade Licenses page opens.
10. Enter the information needed for the upgrade request and select or upload the license file(s) to update.
11. Click **Submit** to upload the license request. A confirmation page opens, showing the details of your request. The upgraded licenses are e-mailed to you in a .zip file.

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**.



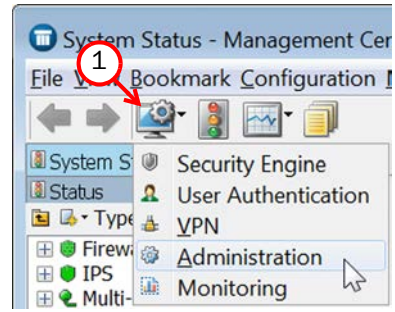
2. Select one or more license files and click **Install**. The new licenses are installed.

Checking the Licenses

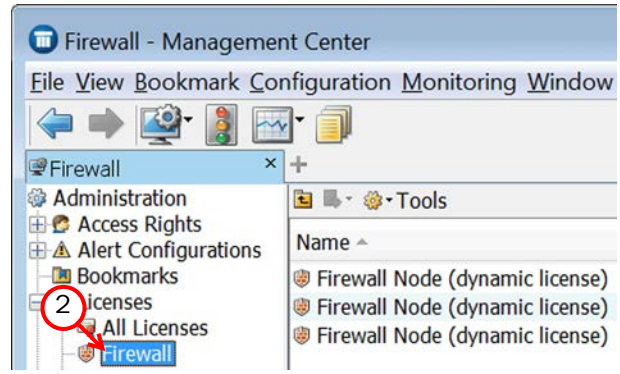
After installing the upgraded licenses, check the license information. When you upgrade licenses, the old licenses are automatically replaced with the new licenses.

▼ To check the licenses

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



2. Browse to **Licenses→Firewall** or **Licenses→Security Engine** depending on the type of licenses you have. The licenses and their status are displayed.



3. Verify that all of the engines are correctly licensed.
4. If any engines are not correctly licensed, you may need to upgrade or generate the licenses again. See Upgrading or Generating Licenses (page 140).

What's Next?

- If you want to upgrade the engines remotely through the Management Server, proceed to Upgrading Engines Remotely (page 144).
- If you want to upgrade the engines on the engine command line, proceed to Upgrading Engines Locally (page 146).

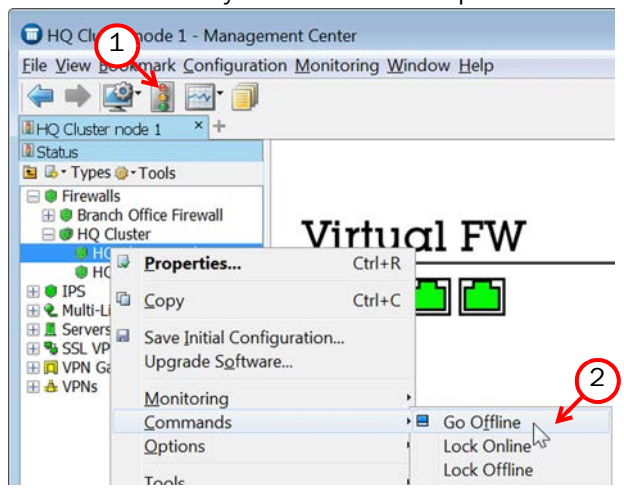
Upgrading Engines Remotely

You can upgrade the engines through the Management Server by importing the upgrade package manually or automatically. You can then activate the upgrade package or you can transfer the upgrade package to the engine and activate it separately later, for example, during a break in service. You can also create a scheduled Task for the remote upgrade as instructed in the *Stonesoft Administrator's Guide* or in the Management Client *Online Help*.

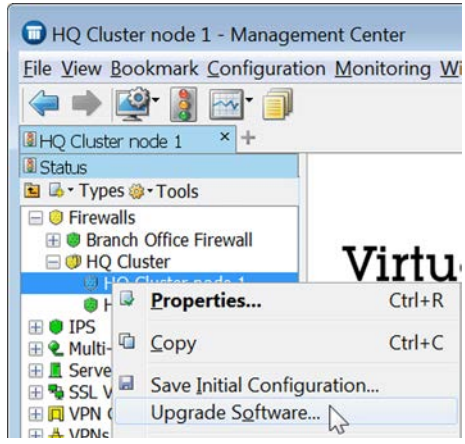
During a Firewall Cluster or Master Engine cluster upgrade, it is possible to have the upgraded nodes online and operational alongside the older version nodes. However, you must upgrade all the nodes to the same version as soon as possible, as prolonged use with mismatched versions is not supported.

▼ To upgrade the engine

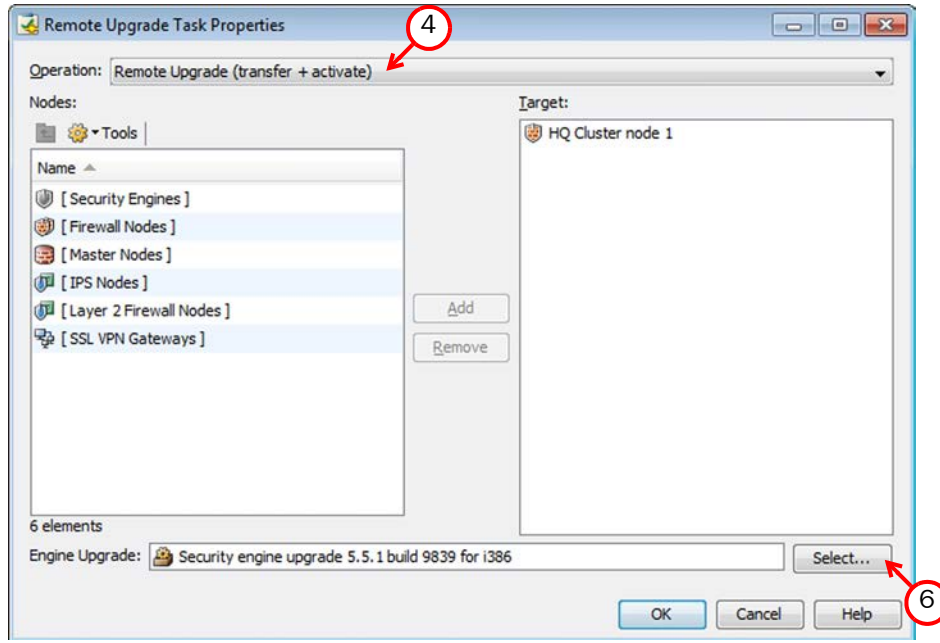
1. Click the System Status icon. The System Status view opens.



2. If you want to activate the new version immediately, right-click the engine node and select **Commands→Go Offline**.



3. Right-click the engine node and select **Upgrade Software**.



4. Select the type of **Operation** you want to perform:
   - **Remote Upgrade (transfer + activate)**: install the new software and reboot the node with the new version of the software.
   - **Remote Upgrade (transfer)**: install the new software on the node without an immediate reboot and activation. The node continues to operate with the currently installed version until you choose to activate the new version.
   - **Remote Upgrade (activate)**: reboot the node and activate the new version of the software that has been installed earlier.
5. Check the **Target** node selection and change it, if necessary.

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. Select the correct **Engine Upgrade** file and click **OK**. 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 engine and the network environment. Click **Abort** if you want to stop the upgrade.
7. Refresh the policy of the upgraded engine to make sure any possible changes specific to the new software version are transferred to the engine.

If you chose to activate the new configuration, the engine is automatically rebooted and the upgraded engine is brought to the online state once the engine is successfully upgraded.

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

What's Next?

- Upgrade any other engines in the same way.
- Otherwise, the upgrade is complete.

Upgrading Engines Locally

It is also possible to upgrade the engines on the engine command line 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 or Master Engine cluster upgrade, it is possible for the upgraded nodes to be online and operational side by side with the older version nodes. However, you must upgrade all the nodes to the same version as soon as possible, as prolonged use with mismatched versions is not supported.

What's Next?

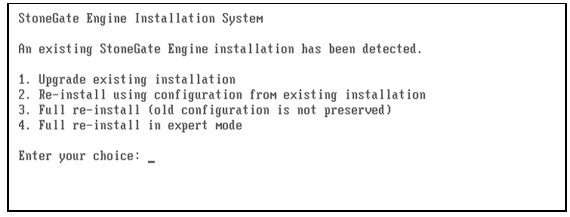
- If the hardware has a DVD drive (a USB DVD drive can be used) and you have an installation DVD, proceed to Upgrading From an Engine Installation DVD.
- If you want to upgrade from a .zip file on a USB stick or on a DVD, proceed to Upgrading From a .zip File (page 147).

Upgrading From an Engine Installation DVD

You can upgrade the engines to the latest version from a DVD that was shipped to you by Stonesoft, or from a DVD that you have created from an .iso image that you downloaded from the Stonesoft web site.

▼ To upgrade the engine from an engine installation DVD

1. Log in to the node as **root** with the password you set for the engine (you can set the password through the Management Client).
2. Insert the DVD into the engine's DVD drive.
3. Reboot the node from the DVD with the command **reboot** (*recommended*) or by cycling the power (if you cannot log in). You are promoted to select the upgrade type.



4. Enter **1** to upgrade the existing installation and press Enter to continue. The upgrade process starts.

5. When the process is finished, eject the DVD and press Enter to reboot.
   - If the Engine Configuration Wizard opens, configure the engine in the same way as after the first installation. See Configuring the Engine in the Engine Configuration Wizard (page 125) for instructions.
6. When the upgrade is finished, right-click the node in the Management Client and select **Commands→Go Online**.

If you are upgrading a Firewall Cluster or Master Engine cluster, we recommend beginning the upgrade on the next node only when the upgraded node is back online.

What's Next?

- Upgrade any other engines in the same way.
- Otherwise, the upgrade is complete.

Upgrading From a .zip File

Follow the instructions below if you want to use a .zip file to upgrade the engine software locally on the engine command line.

To upgrade the engine locally from a .zip file

1. 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 DVD.
3. Run the command `sg-reconfigure`. The Engine Configuration Wizard opens.
4. Select **Upgrade** 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.

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.

7. Select **OK**. The software is upgraded.
8. When prompted, press Enter. The engine reboots to the new version.

What's Next?

- Upgrade any other engines in the same way.
- Otherwise, the upgrade is complete.

APPENDICES

In this section:

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

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\Stonesoft\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\Stonesoft\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

Command	Description
sgArchiveExport [**host=**<*Management Server Address* [*Domain*]>] [**login**=<*login name*>] [**pass**=<*password*>] [**format**=**<*exporter format: CSV or XML*>**] **i=**<*input files and/or directories*> [**o=**<*output file name*>] [**f=**<*filter file name*>] [**e=**<*filter expression*>] [**-h** | **-help** | **-?**] [**-v**]	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`

Table A.1 Management Center Command Line Tools (Continued)

Command	Description
sgBackupAuthSrv [**pwd=**<*password*>] [**path=**<*destpath*>] [**nodiskcheck**] [**comment=**<*comment*>] [**-h** | **--help**]	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. **pwd** enables encryption. **path** defines the destination path. **nodiskcheck** ignores free disk check before creating the backup. **comment** allows you to enter a comment for the backup. The maximum length of a comment is 60 characters. **-h** or **--help** displays information on using the script. Also see **sgRestoreAuthBackup**.
sgBackupLogSrv [**pwd=**<*password*>] [**path=**<*destpath*>] [**nodiskcheck**] [**comment=**<*comment*>] [**nofsstorage**] [**-h** | **--help**]	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. **pwd** entering a password enables encryption. **path** defines the destination path. **nodiskcheck** ignores free disk check before creating the backup. **comment** allows you to enter a comment for the backup. The maximum length of a comment is 60 characters. **nofsstorage** creates a backup only of the log server configuration without the log data. **-h** or **--help** displays information on using the script. Also see **sgRestoreLogBackup**.
sgBackupMgtSrv [**pwd=**<*password*>] [**path=**<*destpath*>] [**nodiskcheck**] [**comment=**<*comment*>] [**-h** | **--help**]	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. **pwd** entering a password enables encryption. **path** defines the destination path. **nodiskcheck** ignores free disk check before creating the backup. **comment** allows you to enter a comment for the backup. The maximum length of a comment is 60 characters. **-h** or **--help** displays information on using the script. Also see **sgRestoreMgtBackup** and **sgRecoverMgtDatabase**.

Table A.1 Management Center Command Line Tools (Continued)

Command	Description
sgCertifyAuthSrv	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.
sgCertifyLogSrv [**host=**<*Management Server Address* [*Domain*]>]	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 into 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 [**host=**<*Management Server Address* [*Domain*]>]	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 into 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.

Table A.1 Management Center Command Line Tools (Continued)

Command	Description
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 [**host=***<Management Server Address [\Domain]>*] [**login**=*<login name>*] [**pass**=*<password>*] **file=***<file path and name>* [**type**=*<all|nw|ips|sv|rb|al>* [**name**= *<element name 1, element name 2, ...>*] [**recursion**] [**-system**] [**-h** | **-help** | -?]	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 into 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.

Table A.1 Management Center Command Line Tools (Continued)

Command	Description
sgHA [**host=**<*Management Server Address* [*Domain*]>] [**login**=<*login name*>] [**pass**=<*password*>] [**master**=<*Management Server used as master server for the operation*>] [**-set-active**] [**-set-standby**] [**-sync**] [**-fullsync**] [**-check**] [**-retry**] [**-isolate**] [**-force**] [**-restart**] [**-h**|**-help**|**-?**]	Controls 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 into 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 Management Server for the operation. **-set-active** activates and locks all administrative Domains. **-set-standby** deactivates and unlocks all administrative Domains. **-sync** performs full database replication. It replicates the database from the master Management Server to the specified Management Server. **-fullsync** performs full database replication with the master Management Server's backup. **-check** checks that the Management Server's database is in sync with the master Management 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. **-restart** restarts the specified Management Server. **-h**, **-help**, or **-?** displays information on using the script.

Table A.1 Management Center Command Line Tools (Continued)

Command	Description
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 into 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 into 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**: `sgImportExportUser login=admin pass=abc123 action=export file=c:\temp\exportedusers.ldif` **-h**, **-help**, or **-?** displays information on using the script.

Table A.1 Management Center Command Line Tools (Continued)

Command	Description
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 Management Server*>] [**standby-server=**<*name of additional Management Server*>] [**standby-server-address=**<*IP address of additional Management Server*>] [**-nodisplay**] [**-h**|**-help**|**-?**]	Replicates the Management Server's database from the active Management Server to an additional Management Server. The Management Server to which the database is replicated must be shut down before running this command. Restart the Management Server after running this command. **Note!** Use this script to replicate the database only if the additional Management Server's configuration has been corrupted, the additional 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 with the **sgHA** command or through the Management Client. See the *Stonesoft Administrator's Guide* for more information. **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 additional Management Server to which the Management database is replicated. **standby-server-address** option specifies the IP address of the additional 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.

Table A.1 Management Center Command Line Tools (Continued)

Command	Description
sgReinitializeLogServer	**Note!** This script is located in <*installation directory*>/bin/install. Creates a new Log Server configuration if the configuration file has been lost.
sgRestoreArchive <ARCHIVE_DIR>	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 <*installation directory*>/data/LogServerConfiguration.txt file: ARCHIVE_DIR_*xx*=*PATH*.
sgRestoreAuthBackup [**-pwd=**<*password*>] [**-backup=**<*backup file name*>] [**-nodiskcheck**] [**-h**|**-help**]	Restores the Authentication Server user information from a backup file in the <*installation directory*>/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.
sgRestoreLogBackup [**-pwd=**<*password*>] [**-backup=**<*backup file name*>] [**-nodiskcheck**] [**-overwrite-syslog-template**] [**-h**|**-help**]	Restores the Log Server (logs and/or configuration files) from a backup file in the <*installation directory*>/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.
sgRestoreMgtBackup [**-pwd**=<*password*>] [**-backup**=<*backup file name*>] [**-nodiskcheck**] [**-h**|**-help**]	Restores the Management Server (database and/or configuration files) from a backup file in the <*installation directory*>/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.

Table A.1 Management Center Command Line Tools (Continued)

Command	Description
sgRevert	**Note!** This script is located in <*installation directory*>/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.
sgShowFingerPrint	Displays the CA certificate's fingerprint on the Management Server.
sgStartAuthSrv	Starts the Authentication Server.
sgStartLogSrv	Starts the Log Server and its database.
sgStartMgtDatabase	Starts the Management Server's database. There is usually no need to use this script.
sgStartMgtSrv	Starts the Management Server and its database.
sgStartWebPortalSrv	Starts the Web Portal Server.
sgStopLogSrv	Stops the Log Server.
sgStopMgtSrv	Stops the Management Server and its database.
sgStopMgtDatabase	Stops the Management Server's database. There is usually no need to use this script.
sgStopWebPortalSrv	Stops the Web Portal Server.
sgStopRemoteMgtSrv [**host=<***Management Server Host Name***>**] [**login=<***login name***>**] [**pass=<***password***>**] [**-h**|**-help**|**-?**]	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.

Table A.1 Management Center Command Line Tools (Continued)

Command	Description
sgTextBrowser [**host=**<*Management Server address* [*Domain*]>] [**login**=<*login name*>] [**pass**=<*password*>] [**format**=<*CSV*|*XML*>] [**o=**<*output file*>] [**f=**<*filter file*>] [**e=**<*filter expression*>] [**m=**<*current*|*stored*>] [**limit=**<*maximum number of unique records to fetch*>] [**-h**|**-help**|**-?**]	Displays or exports current or stored logs. This command is available on the Log Server. Enclose the file and filter names in double quotes if they contain spaces. **host** defines the address of the Management Server used for checking the login information. If this parameter is not defined, Management Server is expected to be on the same host where the script is run. If Domains are in use, you can specify the Domain the Log Server belongs to. If `domain` is not specified, the Shared Domain is used. **login** defines the username for the account that is used for this export. If this parameter is not defined, the username `root` is used. **pass** defines the password for the user account used for this operation. **format** defines the file format for the output file. If this parameter is not defined, the XML format is used. **o** defines the destination output file where the logs will be exported. If this parameter is not defined, the output is displayed on screen. **f** defines the Stonesoft exported filter file that you want to use for filtering the log data. **e** defines the filter that you want to use for filtering the log data. Type the name as shown in the Management Client. **m** defines whether you want to view or export logs as they arrive on the Log Server (current) or logs stored in the active storage directory (stored). If this option is not defined, the current logs are used. **limit** defines the maximum number of unique records to be fetched. The default value is unlimited. **-h**, **-help**, or **-?** displays information on using the script.

Engine Commands

The commands in the following two tables can be run on the command line on Firewall, Virtual Firewall, Layer 2 Firewall, and/or IPS engines.

Note – All command line tools that are available in the Firewall role are also available for Virtual Firewalls. However, there is no direct access to the command line of Virtual Firewalls. Commands to Virtual Firewalls must be sent from the command line of the Master Engine using the `se-virtual-engine` command.

Table A.2 Stonesoft Engine Command Line Tools

Command	Engine Role	Description
se-virtual-engine **-l | --list** **-v <***virtual engine ID***>** **-e | --enter** **-E "<***command [options]***>"** **-h | --help**	Firewall (*Master Engine only*)	Used to send commands to Virtual Firewalls from the command line of the Master Engine. All commands that can be used for the Firewall role can also be used for Virtual Firewalls. **-l** or **--list** list the active Virtual Security Engines. **- v <virtual engine ID>** specifies the ID of the Virtual Security Engine on which to execute the command. **-e** or **--enter** enters the command shell for the Virtual Security Engine specified with the `-v` option. To exit the command shell, type `exit`. **-E "<***command [options]***>"** executes the specified command on the Virtual Security Engine specified with the `-v` option. **-h** or **--help** shows the help message for the se-virtual-engine command.

Table A.2 Stonesoft Engine Command Line Tools (Continued)

Command	Engine Role	Description

sg-blacklist
show [-v] [-f *FILENAME*] |
add [
[**-i** *FILENAME*] |
[**src** *IP_ADDRESS/MASK*]
[src6 *IPv6_ADDRESS/PREFIX*]
[dst *IP_ADDRESS/MASK*]
[dst6 *IPv6_ADDRESS/PREFIX*]
[**proto** *{tcp|udp|icmp|NUM}*]
[**srcport** *PORT{-PORT}*]
[**dstport** *PORT{-PORT}*]
[**duration** *NUM*]
] |
del [
[**-i** *FILENAME*] |
[**src** *IP_ADDRESS/MASK*]
[src6 *IPv6_ADDRESS/PREFIX*]
[dst *IP_ADDRESS/MASK*]
[dst6 *IPv6_ADDRESS/PREFIX*]
[**proto** *{tcp|udp|icmp|NUM}*]
[**srcport** *PORT{-PORT}*]
[**dstport** *PORT{-PORT}*]
[**duration** *NUM*]
] |
iddel *NODE_ID ID* |
flush
	Firewall, Layer 2 Firewall, IPS	Used to view, add, or delete active blacklist entries. The blacklist is applied as defined in Access Rules.
		Commands:
		show displays the current active blacklist entries in format: engine node ID | blacklist entry ID | (internal) | entry creation time | (internal) | address and port match | originally set duration | (internal) | (internal). Use the `-f` option to specify a storage file to view (`/data/blacklist/db_<number>`). The **-v** option adds operation's details to the output.
		add creates a new blacklist entry. Enter the parameters (see below) or use the **-i** option to import parameters from a file.
		del deletes the first matching blacklist entry. Enter the parameters (see below) or use the **-i** option to import parameters from a file.
		iddel *NODE_ID ID* removes one specific blacklist entry on one specific engine. `NODE_ID` is the engine's ID, `ID` is the blacklist entry's ID (as shown by the `show` command).
		flush deletes all blacklist entries.
		Add/Del Parameters:
		Enter at least one parameter. The default value is used for the parameters that you omit. You can also save parameters in a text file; each line in the file is read as one blacklist entry.
		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)

Command	Engine Role	Description
sg-bootconfig [**--primary-console**=*tty0*|*ttyS PORT,SPEED*] [**--secondary-console**= [*tty0*|*ttyS PORT,SPEED*]] [**--flavor**=*up*|*smp*] [**--initrd**=*yes*|*no*] [**--crashdump**=*yes*|*no*|*Y@X*] [**--append**=*kernel options*] [**--help**] **apply**	Firewall, Layer 2 Firewall, IPS	Used to edit boot command parameters for future bootups. **--primary-console**=*tty0*|*ttyS PORT,SPEED* parameter defines the terminal settings for the primary console. **--secondary-console**= [*tty0*|*ttyS PORT,SPEED*] parameter defines the terminal settings for the secondary console. **--flavor**=*up*|*smp* [*-kdb*] parameter defines whether the kernel is uniprocessor or multiprocessor. **--initrd**=*yes*|*no* parameter defines whether Ramdisk is enabled or disabled. **--crashdump**=*yes*|*no*|*Y@X* parameter defines whether kernel crashdump is enabled or disabled, and how much memory is allocated to the crash dump kernel (Y). The default is 24M. X must always be 16M. **--append**=*kernel options* parameter defines any other boot options to add to the configuration. **--help** parameter displays usage information. **apply** command applies the specified configuration options.
sg-clear-all	Firewall, Layer 2 Firewall, IPS	**Note! Use this only if you want to clear all configuration information from the engine.** 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.
sg-cluster [-v <*virtual engine ID*>] [status [-c *SECONDS*]] [versions] [online] [lock-online] [offline] [lock-offline] [standby] [safe-offline] [force-offline]	Firewall, Layer 2 Firewall, IPS	Used to display or change the status of the node. **-v <*virtual engine ID*>** (*Master Engine only*) option specifies the ID of the Virtual Security Engine on which to execute the command. **status** [**-c** *SECONDS*] command displays cluster status. When **-c** *SECONDS* is used, status is shown continuously with the specified number of seconds between updates. **version** command displays the engine software versions of the nodes in the cluster. **online** command sends the node online. **lock-online** command sends the node online and keeps it online even if another process tries to change its state. **offline** command sends the node offline. **lock-offline** command sends the node offline and keeps it offline even if another process tries to change its state. **standby** command sets an active node to standby. **safe-offline** command sets the node to offline only if there is another online node. **force-offline** command sets the node online regardless of state or any limitations. Also sets all other nodes offline.

Table A.2 Stonesoft Engine Command Line Tools (Continued)

Command	Engine Role	Description
sg-contact-mgmt	Firewall, Layer 2 Firewall, IPS	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.
sg-dynamic-routing **[start]** **[stop]** **[restart]** **[force-reload]** **[backup** *<file>*] **[restore** *<file>*] **[sample-config]** **[route-table]** **[info]**	Firewall	`start` starts the Quagga routing suite. `stop` stops the Quagga routing suite and flushes all routes made by zebra. `restart` restarts the Quagga routing suite. `force-reload` forces reload of the saved configuration. `backup` *<file>* backs up the current configuration to a compressed file. `restore` *<file>* restores the configuration from the specified file. `sample-config` creates a basic configuration for Quagga. `route-table` prints the current routing table. `info` displays the help information for the sg-dynamic-routing command, and detailed information about Quagga suite configuration with vtysh.
sg-ipsec -d [**-u** *<username[@domain]>* | **-si** *<session id>* | **-ck** *<ike cookie>* | **-tri** *<transform id>* **-ri** *<remote ip>* | **-ci** *<connection id>*]	Firewall	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 <username@domain> 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.

Table A.2 Stonesoft Engine Command Line Tools (Continued)

Command	Engine Role	Description
sg-logger **-f** *FACILITY_NUMBER* **-t** *TYPE_NUMBER* [**-e** *EVENT_NUMBER*] [**-i** *"INFO_STRING"*] [**-s**] [**-h**]	Firewall, Layer 2 Firewall, IPS	Used in scripts to create log messages with the specified properties. **-f** *FACILITY_NUMBER* parameter defines the facility for the log message. **-t** *TYPE_NUMBER* parameter defines the type for the log message. **-e** *EVENT_NUMBER* parameter defines the log event for the log message. The default is 0 (H2A_LOG_EVENT_UNDEFINED). **-i** *"INFO_STRING"* parameter defines the information string for the log message. **-s** parameter dumps information on option numbers to stdout **-h** parameter displays usage information.
sg-raid [**-status**] [**-add**] [**-re-add**] [**-force**] [**-help**]	Firewall, Layer 2 Firewall, IPS	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. **-status** option displays the status of the hard drive. **-add** options adds a new empty hard drive. Use **-add -force** if you want to add a hard drive that already contains data and you want to overwrite it. **-re-add** adds a hard drive that is already partitioned. This command prompts for the drive and partition for each degraded array. Use **-re-add -force** if you want to check all the arrays. **-help** option option displays usage information.
sg-reconfigure [**--boot**] [**--maybe-contact**] [**--no-shutdown**]	Firewall, Layer 2 Firewall, IPS	Used for reconfiguring the node manually. **--boot** option applies bootup behavior. Do not use this option unless you have a specific need to do so. **--maybe-contact** option contacts the Management Server if requested. This option is only available on firewall engines. **--no-shutdown** 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.
sg-selftest [**-d**] [**-h**]	Firewall	Runs cryptography tests on the engine. **-d** option runs the tests in debug mode. **-h** option displays usage information.
sg-status [**-l**] [**-h**]	Firewall, Layer 2 Firewall, IPS	Displays information on the engine's status. **-l** option displays all available information on engine status. **-h** option displays usage information.

Table A.2 Stonesoft Engine Command Line Tools (Continued)

Command	Engine Role	Description
sg-toggle-active *SHA1 SIZE* | **--force** [**--debug**]	Firewall, Layer 2 Firewall, IPS	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 `/var/run/stonegate` (**`ls -l /var/run/stonegate`**). The *SHA1 SIZE* 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 sg_engine_[version.build]_i386.zip file. **--debug** option reboots the engine with the debug kernel. **--force** option switches the active configuration without first verifying the signature of the inactive partition.
sg-upgrade	Firewall	Upgrades the node by rebooting from the installation DVD. Alternatively, the node can be upgraded remotely using the Management Client.
sg-version	Firewall, Layer 2 Firewall, IPS	Displays the software version and build number for the node.
sginfo [**-f**] [**-d**] [**-s**] [**-p**] [**--**] [**--help**]	Firewall, Layer 2 Firewall, IPS	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. **-f** option forces sgInfo even if the configuration is encrypted. **-d** option includes core dumps in the sgInfo file. **-s** option includes slapcat output in the sgInfo file. **-p** option includes passwords in the sgInfo file (by default passwords are erased from the output). **--** option creates the sgInfo file without displaying the progress **--help** option displays usage information.

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

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

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 A.4 Server Pool Monitoring Agent Commands

Command	Description
agent [-v *level*] [-c *path*] [test [*files*]] [syntax [*files*]]	(*Windows only*) Allows you to test different configurations before activating them. -v *level* Set the verbosity level. The default level is 5. Levels 6-8 are for debugging where available. -c *path* Use the specified path as the first search directory for the configuration. test [*files*] 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 -d option. syntax [*files*] Check the syntax in the configuration file. If no files are specified, the default configuration files are checked.
sgagentd [-d] [-v *level*] [-c *path*] [test [*files*]] [syntax [*files*]]	(*Linux only*) Allows you to test different configurations before activating them. -d Don't Fork as a daemon. All log messages are printed to stdout or stderr only. -v *level* Set the verbosity level. The default level is 5. Levels 6-8 are for debugging where available. -c *path* Use the specified path as the first search directory for the configuration. test [*files*] 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 -d option. syntax [*files*] 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 -d option.

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

Command	Description
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

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

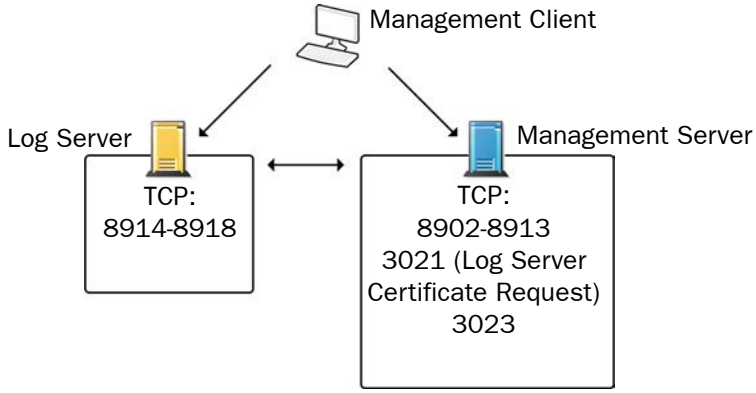
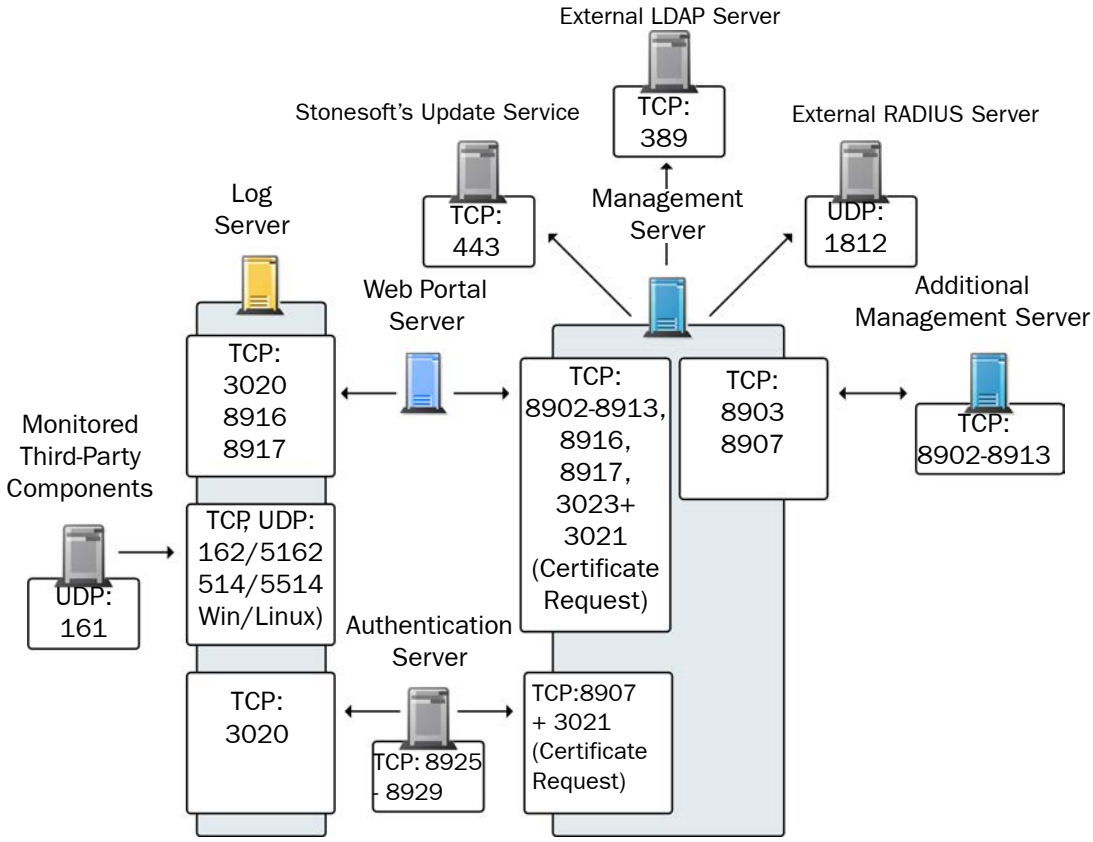


Illustration B.2 Default Destination Ports for Optional SMC Components and Features



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

Listening Host	Port/ Protocol	Contacting Hosts	Service Description	Service Element Name
Additional Management Servers	8902-8913/TCP	Management Server	Database replication (push) to the additional Management Server.	SG Control
Authentication Server	8925-8929/TCP	Management Server	Stonesoft Management Server commands to Authentication Server.	SG Authentication Commands
Authentication Server node	8988-8989/TCP	Authentication Server node	Data synchronization between Authentication Server nodes.	SG Authentication Sync
DNS server	53/UDP, 53/TCP	Management Client, Management Server, Log Server	DNS queries.	DNS (UDP)
LDAP server	389/TCP	Management Server	External LDAP queries for display/ editing in the Management Client.	LDAP (TCP)
Log Server	162/UDP, 5162/UDP	Monitored third-party components	SNMPv1 trap reception from third-party components. Port 162 is used if installed on Windows, port 5162 if installed on Linux.	SNMP (UDP)
Log Server	514/TCP, 514/UDP, 5514/TCP, 5514/UDP	Monitored third-party components	Syslog reception from third-party components. Port 514 is used if installed on Windows, port 5514 if installed on Linux.	Syslog (UDP) [*Partial match*]
Log Server	2055/UDP	Monitored third-party components	NetFlow or IPFIX reception from third-party components. Port 2055 is used in both Windows and Linux.	NetFlow (UDP)
Log Server	3020/TCP	Authentication Server, Log Server, Web Portal Server, Security Engines	Alert sending from the Authentication Server, Log Server, and Web Portal Server. Log and alert messages; monitoring of blacklists, connections, status, and statistics from Security Engines.	SG Log
Log Server	8914-8918/TCP	Management Client	Log browsing.	SG Data Browsing
Log Server	8916-8917/TCP	Web Portal Server	Log browsing.	SG Data Browsing (Web Portal Server)

Table B.1 Management Center Default Ports (Continued)

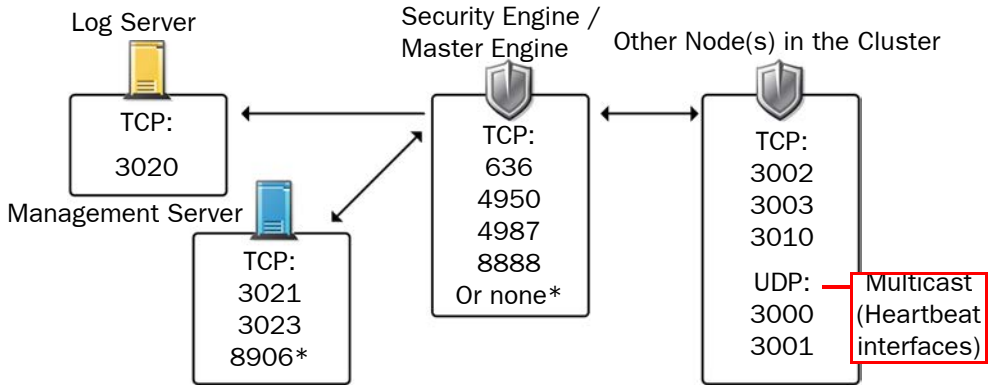
Listening Host	Port/ Protocol	Contacting Hosts	Service Description	Service Element Name
Management Server	3021/TCP	Log Server, Web Portal Server	System communications certificate request/renewal.	SG Log Initial Contact
Management Server	8902-8913/TCP	Management Client, Log Server, Web Portal Server	Monitoring and control connections.	SG Control
Management Server	3023/TCP	Additional Management Servers, Log Server, Web Portal Server	Log Server and Web Portal Server status monitoring. Status information from an additional Management Server to the active Management Server.	SG Status Monitoring
Management Server	8903, 8907/TCP	Additional Management Servers	Database replication (pull) to the additional Management Server.	SG Control
Management Server	8907/TCP	Authentication Server	Status monitoring.	SG Control
Monitored third-party components	161/UDP	Log Server	SNMP status probing to external IP addresses.	SNMP (UDP)
RADIUS server	1812/UDP	Management Server	RADIUS authentication requests for administrator logins. The default ports can be modified in the properties of the RADIUS Server element.	RADIUS (Authentication)
Stonesoft servers	443/TCP	Management Server	Update packages, engine upgrades, and licenses from update.stonesoft.com and smc.stonesoft.com.	HTTPS
Syslog server	514/UDP, 5514/UDP	Log Server	Log data forwarding to syslog servers. The default ports can be modified in the LogServerConfiguration.txt file.	Syslog (UDP) [*Partial match*]
Third-party components	2055/UDP	Log Server	NetFlow or IPFIX forwarding to third-party components. Port 2055 is used in both Windows and Linux.	NetFlow (UDP)

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.

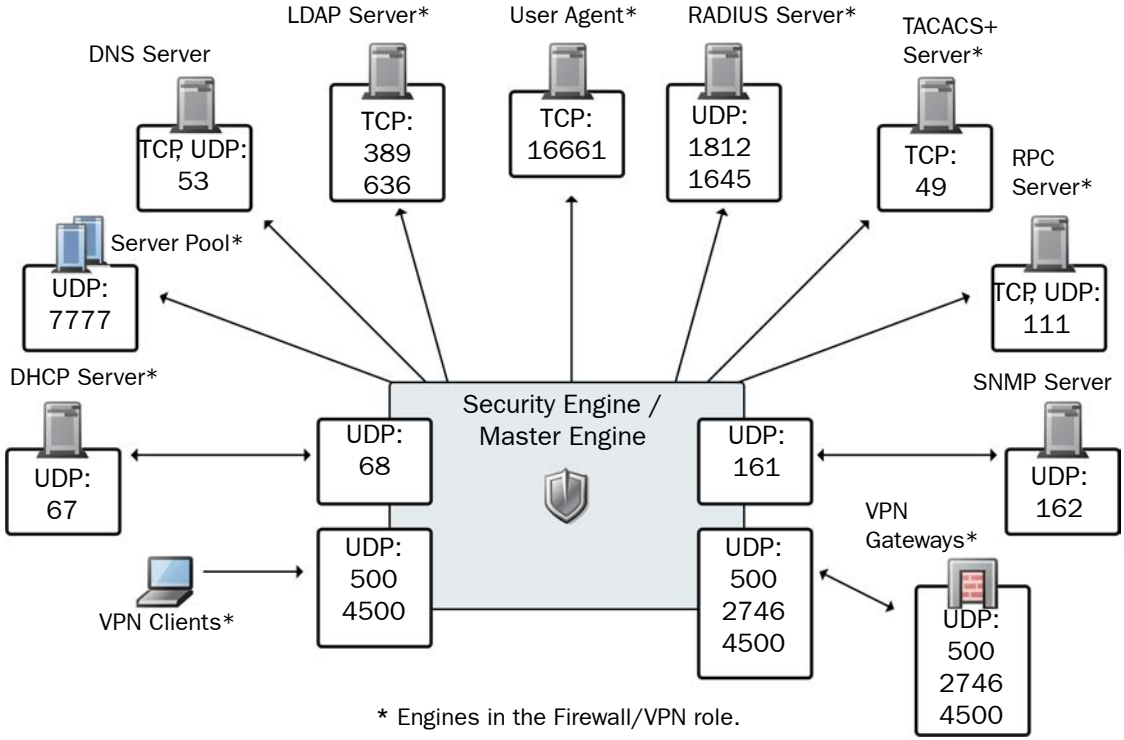
Note – Master Engines use the same default ports as clustered Security Engines. Virtual Security Engines do not communicate directly with other system components.

Illustration B.3 Destination Ports for Basic Security Engine Communications



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

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



* Engines in the Firewall/VPN role.

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 B.2 Security Engine and Master Engine Default Ports

Listening Host	Port/Protocol	Contacting Hosts	Service Description	Service Element Name
Anti-virus signature server	80/TCP	Firewall	Anti-virus signature update service.	HTTP
Authentication Server	8925-8929/ TCP	Firewall, Master Engine	User directory and authentication services.	LDAP (TCP), RADIUS (Authentication)
BrightCloud Server	2316/TCP	Firewall, Layer 2 Firewall, IPS, Master Engine	BrightCloud web filtering update service.	BrightCloud update
DHCP server	67/UDP	Firewall	Relayed DHCP requests and requests from a firewall that uses dynamic IP address.	BOOTPS (UDP)
DNS server	53/UDP, 53/TCP	Firewall, Master Engine	Dynamic DNS updates.	DNS (TCP)
Firewall	67/UDP	Any	DHCP relay on firewall engine.	BOOTPS (UDP)
Firewall	68/UDP	DHCP server	Replies to DHCP requests.	BOOTPC (UDP)
Firewall, Master Engine	500/UDP	VPN clients, VPN gateways	VPN negotiations, VPN traffic.	ISAKMP (UDP)
Firewall, Master Engine	636/TCP	Management Server	Internal user database replication.	LDAPS (TCP)
Firewall, Master Engine	2543/TCP	Any	User authentication (Telnet) for Access rules.	SG User Authentication
Firewall	2746/UDP	Stonesoft VPN gateways	UDP encapsulated VPN traffic (engine versions 5.1 and lower).	SG UDP Encapsulation
Firewall, Master Engine	4500/UDP	VPN client, VPN gateways	VPN traffic using NAT-traversal.	NAT-T
Firewall Cluster Node, Master Engine cluster node	3000-3001/ UDP 3002-3003, 3010/TCP	Firewall Cluster Node, Master Engine cluster node	Heartbeat and state synchronization between clustered Firewalls.	SG State Sync (Multicast), SG State Sync (Unicast), SG Data Sync
Firewall, Layer 2 Firewall, IPS, Master Engine	4950/TCP	Management Server	Remote upgrade.	SG Remote Upgrade

Table B.2 Security Engine and Master Engine Default Ports (Continued)

Listening Host	Port/Protocol	Contacting Hosts	Service Description	Service Element Name
Firewall, Layer 2 Firewall, IPS, Master Engine	4987/TCP	Management Server	Management Server commands and policy upload.	SG Commands
Firewall, Layer 2 Firewall, IPS	8888/TCP	Management Server	Connection monitoring for engine versions 5.1 and lower.	SG Legacy Monitoring
Firewall, Layer 2 Firewall, IPS, Master Engine	15000/TCP	Management Server, Log Server	Blacklist entries.	SG Blacklisting
Firewall, Layer 2 Firewall, IPS, Master Engine	161/UDP	SNMP server	SNMP monitoring.	SNMP (UDP)
IPS Cluster Node	3000-3001/ UDP 3002-3003, 3010/TCP	IPS Cluster Node	Heartbeat and state synchronization between clustered IPS engines.	SG State Sync (Multicast), SG State Sync (Unicast), SG Data Sync
LDAP server	389/TCP	Firewall, Master Engine	External LDAP queries, including StartTLS connections.	LDAP (TCP)
Layer 2 Firewall Cluster Node	3000-3001/ UDP 3002-3003, 3010/TCP	Layer 2 Firewall Cluster Node	Heartbeat and state synchronization between clustered Layer 2 Firewalls.	SG State Sync (Multicast), SG State Sync (Unicast), SG Data Sync
Log Server	3020/TCP	Firewall, Layer 2 Firewall, IPS, Master Engine	Log and alert messages; monitoring of blacklists, connections, status, and statistics.	SG Log
Management Server	3021/TCP	Firewall, Layer 2 Firewall, IPS, Master Engine	System communications certificate request/renewal (initial contact).	SG Initial Contact
Management Server	3023/TCP	Firewall, Layer 2 Firewall, IPS, Master Engine	Monitoring (status) connection.	SG Status Monitoring
Management Server	8906/TCP	Firewall, Layer 2 Firewall, IPS	Management connection for single engines with “Node-Initiated Contact to Management Server” selected.	SG Dynamic Control
RADIUS server	1812, 1645/ UDP	Firewall, Master Engine	RADIUS authentication requests.	RADIUS (Authentication), RADIUS (Old)

Table B.2 Security Engine and Master Engine Default Ports (Continued)

Listening Host	Port/Protocol	Contacting Hosts	Service Description	Service Element Name
RPC server	111/UDP, 111/TCP	Firewall, Master Engine	RPC number resolve.	SUNRPC (UDP), Sun RPC (TCP)
Server Pool Monitoring Agents	7777/UDP	Firewall, Master Engine	Polls to the servers' Server Pool Monitoring Agents for availability and load information.	SG Server Pool Monitoring
SNMP server	162/UDP	Firewall, Layer 2 Firewall, IPS, Master Engine	SNMP traps from the engine.	SNMP Trap (UDP)
TACACS+ server	49/TCP	Firewall, Master Engine	TACACS+ authentication requests.	TACACS (TCP)
User Agent	16661/TCP	Firewall, Master Engine	Queries for matching Users and User Groups with IP addresses.	SG Engine to User Agent
VPN gateways	500/UDP, 2746/UDP (Stonesoft gateways only), or 4500 UDP.	Firewall, Master Engine	VPN traffic. Ports 2746 and 4500 may be used depending on encapsulation options.	ISAKMP (UDP)

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.

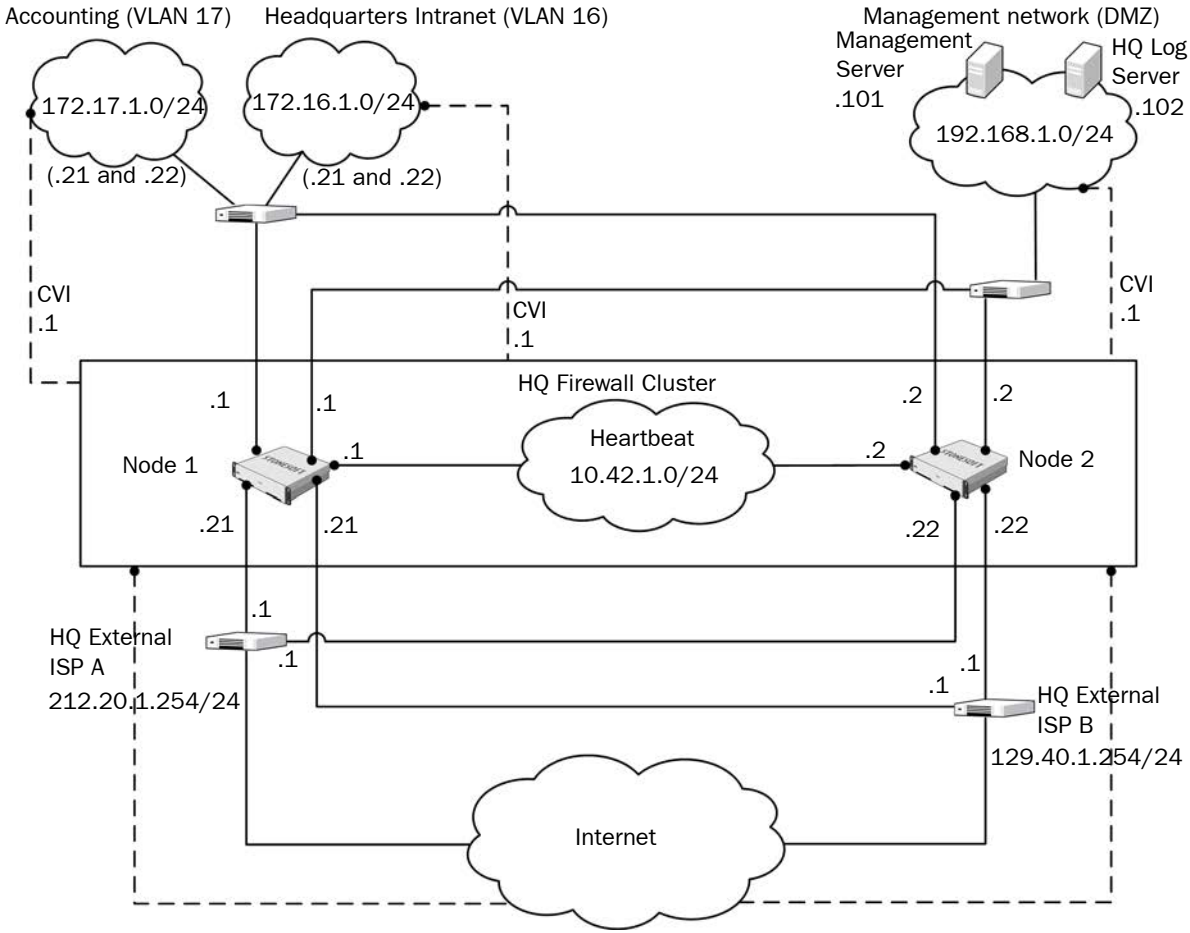
The following sections are included:

Overview of the Example Network

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

Network	Description
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

Management Center Component	Description
Management Server	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.
HQ Log Server	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.

Example Single Firewall

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

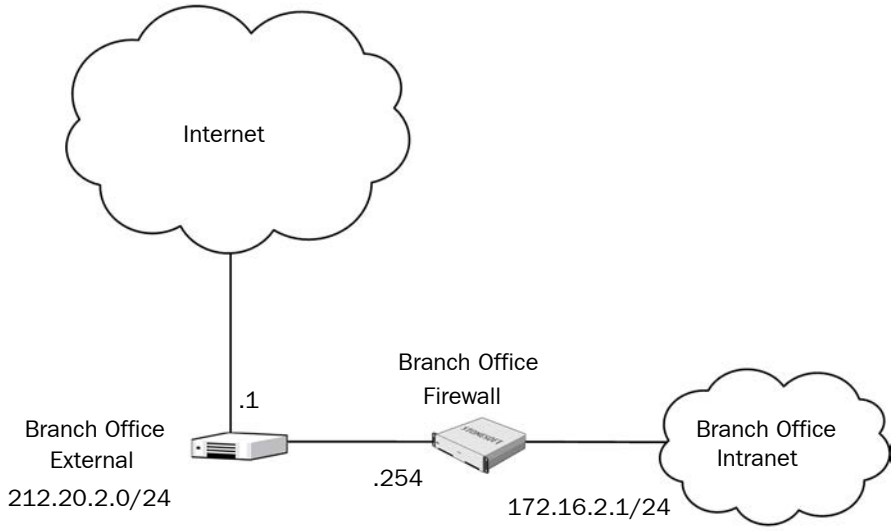


Table C.3 Single Firewall in the Example Network Scenario

Network	Description
External network	The Branch Office site is connected to the Internet through this link. **IP address**: 212.20.2.254. **Next hop router**: 212.20.2.1.
Internal network	The Branch Office has one internal network. **IP address**: 172.16.2.1.

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 D.1 Stonesoft Firewall Engine Interfaces

Inter face ID	Type	Mode*	IP Address	Netmask	MAC / IGMP IP Address	Comments
_____	CVI	U M I K A	_____ ._____._____._____	_____ ._____._____._____	MAC: ___ : ___ : ___ : ___ : ___ : ___ or IGMP IP: _____ ._____._____.____	
	NDI	H h C c D	_____ ._____._____._____	_____ ._____._____._____	MAC: ___ : ___ : ___ : ___ : ___ : ___	
_____	CVI	U M I K A	_____ ._____._____._____	_____ ._____._____._____	MAC: ___ : ___ : ___ : ___ : ___ : ___ or IGMP IP: _____ ._____._____.____	
	NDI	H h C c D	_____ ._____._____._____	_____ ._____._____._____	MAC: ___ : ___ : ___ : ___ : ___ : ___	
_____	CVI	U M I K A	_____ ._____._____._____	_____ ._____._____._____	MAC: ___ : ___ : ___ : ___ : ___ : ___ or IGMP IP: _____ ._____._____.____	
	NDI	H h C c D	_____ ._____._____._____	_____ ._____._____._____	MAC: ___ : ___ : ___ : ___ : ___ : ___	
_____	CVI	U M I K A	_____ ._____._____._____	_____ ._____._____._____	MAC: ___ : ___ : ___ : ___ : ___ : ___ or IGMP IP: _____ ._____._____.____	
	NDI	H h C c D	_____ ._____._____._____	_____ ._____._____._____	MAC: ___ : ___ : ___ : ___ : ___ : ___	
_____	CVI	U M I K A	_____ ._____._____._____	_____ ._____._____._____	MAC: ___ : ___ : ___ : ___ : ___ : ___ or IGMP IP: _____ ._____._____.____	
	NDI	H h C c D	_____ ._____._____._____	_____ ._____._____._____	MAC: ___ : ___ : ___ : ___ : ___ : ___	
_____	CVI	U M I K A	_____ ._____._____._____	_____ ._____._____._____	MAC: ___ : ___ : ___ : ___ : ___ : ___ or IGMP IP: _____ ._____._____.____	
	NDI	H h C c D	_____ ._____._____._____	_____ ._____._____._____	MAC: ___ : ___ : ___ : ___ : ___ : ___	

*)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 D.1 Stonesoft Firewall Engine Interfaces

Inter face ID	Type	Mode*	IP Address	Netmask	MAC / IGMP IP Address	Comments
______	CVI	U M I K A	_____ ._____._____._____	_____ ._____._____._____	MAC: ___ : ___ : ___ : ___ : ___ : ___ or IGMP IP: _____ ._____._____._____	
	NDI	H h C c D	_____ ._____._____._____	_____ ._____._____._____	MAC: ___ : ___ : ___ : ___ : ___ : ___	
______	CVI	U M I K A	_____ ._____._____._____	_____ ._____._____._____	MAC: ___ : ___ : ___ : ___ : ___ : ___ or IGMP IP: _____ ._____._____._____	
	NDI	H h C c D	_____ ._____._____._____	_____ ._____._____._____	MAC: ___ : ___ : ___ : ___ : ___ : ___	
______	CVI	U M I K A	_____ ._____._____._____	_____ ._____._____._____	MAC: ___ : ___ : ___ : ___ : ___ : ___ or IGMP IP: _____ ._____._____._____	
	NDI	H h C c D	_____ ._____._____._____	_____ ._____._____._____	MAC: ___ : ___ : ___ : ___ : ___ : ___	
______	CVI	U M I K A	_____ ._____._____._____	_____ ._____._____._____	MAC: ___ : ___ : ___ : ___ : ___ : ___ or IGMP IP: _____ ._____._____._____	
	NDI	H h C c D	_____ ._____._____._____	_____ ._____._____._____	MAC: ___ : ___ : ___ : ___ : ___ : ___	
______	CVI	U M I K A	_____ ._____._____._____	_____ ._____._____._____	MAC: ___ : ___ : ___ : ___ : ___ : ___ or IGMP IP: _____ ._____._____._____	
	NDI	H h C c D	_____ ._____._____._____	_____ ._____._____._____	MAC: ___ : ___ : ___ : ___ : ___ : ___	
______	CVI	U M I K A	_____ ._____._____._____	_____ ._____._____._____	MAC: ___ : ___ : ___ : ___ : ___ : ___ or IGMP IP: _____ ._____._____._____	
	NDI	H h C c D	_____ ._____._____._____	_____ ._____._____._____	MAC: ___ : ___ : ___ : ___ : ___ : ___	

*)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

L

M

N

O

P

R

S

T

U

V

W

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.

User's Guides - step-by-step instructions for end-users.

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