



STONEGATE 5.2

SOHO FIREWALL INSTALLATION GUIDE

SMALL OFFICE/HOME OFFICE FIREWALL

STONESOFT

Secure Information Flow

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 StoneGate software includes several open source or third-party software packages. The appropriate software licensing information for those products at the Stonesoft website:

www.stonesoft.com/en/support/third_party_licenses.html

U.S. Government Acquisitions

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

Product Export Restrictions

The products described in this document are subject to export control under the laws of Finland and the European Council Regulation (EC) 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/support/view_support_offering/terms/

Replacement Service

The instructions for replacement service can be found at the Stonesoft website:

www.stonesoft.com/en/support/view_support_offering/return_material_authorization/

Hardware Warranty

The appliances described in these materials have a limited hardware warranty. The terms of the hardware warranty can be found at the Stonesoft website:

www.stonesoft.com/en/support/view_support_offering/warranty_service/

Trademarks and Patents

The products described in these materials are protected by one or more of the following European and US patents: European Patent Nos. 1065844, 1189410, 1231538, 1259028, 1271283, 1289183, 1289202, 1304849, 1313290, 1326393, 1379046, 1330095, 1317111, 1317937 and 1443729 and US Patent Nos. 6,650,621; 6,856,621; 6,885,633; 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; 7,302,480; 7,386,525; 7,406,534; 7,461,401; 7,721,084; and 7,739,727 and may be protected by other EU, US, or other patents, or pending applications. Stonesoft, the Stonesoft logo and StoneGate, are all trademarks or registered trademarks of Stonesoft Corporation. All other trademarks or registered trademarks are property of their respective owners.

Disclaimer

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

Copyright © 2010 Stonesoft Corporation. All rights reserved. All specifications are subject to change.

TABLE OF CONTENTS

CHAPTER 1	
Using StoneGate Documentation	5
How to Use This Guide	6
Typographical Conventions	6
Documentation Available	7
Product Documentation	7
Support Documentation	7
System Requirements	8
Contact Information	8
Licensing Issues	8
Technical Support	8
Your Comments	8
Other Queries	8
CHAPTER 2	
Preparing for Installation	9
Introduction to StoneGate SOHO Firewalls	10
Overview to the Installation Procedure	10
Important to Know Before Installation	11
System Communications and NAT	11
Internal Clients and NAT	11
Licensing	11
Pre-Installed Firmware	11
RADIUS Server for Wireless User Authentication	11
Selecting a Wireless Access Mode	12
CHAPTER 3	
Configuring NAT Addresses	13
Configuration Overview	14
Defining Locations	15
Adding SMC Server Contact Addresses	17
Adding the Central Firewall Contact Address	18
CHAPTER 4	
Creating SOHO Firewall Elements	21
Configuration Overview	22
Creating New SOHO Firewall Elements	22
Defining Basic Properties	25
Selecting Interface Types	26
Configuring External Interfaces	27
Configuring an External Interface for ADSL or PPPoE	27
Configuring an External Interface for Standard Ethernet	29
Defining DNS Servers for the External and Guest Interfaces	30
Configuring Corporate and Guest Interfaces	31
Defining DNS Servers for the Corporate Interface	32
Defining Security Settings for Wireless Access	34
Defining a RADIUS Server for WPA Enterprise	36
Defining General Wireless Settings	38
Finishing the SOHO Firewall Configuration	39
CHAPTER 5	
Configuring a VPN	41
Overview to Configuring a VPN	42
Creating an Internal Gateway Element	43
Creating a SOHO Gateway Group	45
Creating a VPN Element	46
Creating VPN Access Rules for the Central Firewall	48
CHAPTER 6	
Initializing SOHO Firewall Appliances	51
Allowing SOHO Communications Through a Central Firewall	52
Saving the Initial Configuration	52
CHAPTER 7	
Upgrading	55
Getting Started with Upgrading	56
Configuration Overview	56
Upgrading the SOHO Firewall Engines	56
Checking File Integrity	56
Manually Importing an Upgrade File	57
Upgrading a SOHO Firewall Appliance	57
APPENDIX A	
Default Communication Ports	59
Management Center Ports	60
Firewall/VPN Engine Ports	62
Index	67

CHAPTER 1

USING STONEGATE DOCUMENTATION

Welcome to StoneGate™ SOHO Firewall and VPN solution by Stonesoft Corporation. This chapter describes how to use this *Installation Guide* and lists other available documentation. It also provides directions for obtaining technical support and giving feedback.

The following sections are included:

- ▶ [How to Use This Guide](#) (page 6)
- ▶ [Documentation Available](#) (page 7)
- ▶ [Contact Information](#) (page 8)

How to Use This Guide

This *Installation Guide* is intended for the administrators of StoneGate SOHO firewalls. It describes step by step how to configure the StoneGate SOHO firewall appliances. To configure and install your SOHO firewall appliance, you must have a working StoneGate Management Center (SMC). The chapters in this guide are organized in the general order you should follow when installing the SOHO firewall.

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 instructions that accompany the illustrations are numbered when there is more than one step for you to perform.

Typographical Conventions

The following typographical conventions are used throughout the guide:

Table 1.1 Typographical Conventions

Formatting	Informative Uses
Normal text	This is normal text.
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 .
<i>References, terms</i>	Cross-references and first use of acronyms and terms are in <i>italics</i> .
Command line	File names, directories, and text displayed on the screen are monospaced.
User input	User input on screen is in monospaced bold-face .
<i>Command parameters</i>	Command parameter names are in <i>monospaced italics</i> .

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



Note – Notes provide important information that prevents mistakes or helps you complete a task.



Caution – Cautions provide critical information that you must take into account to prevent breaches of security, information loss, or system downtime.

Tip – Tips provide information that is not crucial, but may still be helpful.

Documentation Available

StoneGate documentation is divided into two main categories: [Support Documentation](#) and [Support Documentation](#). The *Administrator's Guide* and the Online Help system cover all products; the other guidebooks are product-specific.

Product Documentation

The table below lists the available product documentation. PDF guides are available on the Management Center CD-ROM and at <http://www.stonesoft.com/support/>.

Table 1.2 Product Documentation

Guide	Description
Reference Guide	Explains the operation and features of StoneGate comprehensively. Demonstrates the general workflow and provides example scenarios for each feature area. Available for StoneGate Management Center, Firewall/VPN, and StoneGate IPS.
Installation Guide	Instructions for planning, installing, and upgrading a StoneGate system. Available for StoneGate Management Center, Firewall/VPN, IPS, and SOHO firewall products.
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 StoneGate Management Client and the StoneGate Web Portal. An HTML-based system is available in the StoneGate 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 both StoneGate Firewall/VPN and StoneGate IPS, and as separate guides for StoneGate SSL VPN and StoneGate IPsec VPN Client.
User's Guide	Instructions for end-users. Available for the StoneGate IPsec VPN Client and the StoneGate Web Portal.
Appliance Installation Guide	Instructions for physically installing and maintaining StoneGate appliances (rack mounting, cabling, etc.). Available for all StoneGate hardware appliances.

Support Documentation

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

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

System Requirements

The system requirements for running StoneGate, including the approved network interfaces, supported operating systems, and other such hardware and software requirements for StoneGate engines and the Management Center can be found at http://www.stonesoft.com/en/products_and_solutions/products/fw/Software_Solutions/.

The hardware and software requirements for the version of StoneGate you are running can also be found in the *Release Notes* available at the Stonesoft website.

Contact Information

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

Licensing Issues

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

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

Technical Support

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

Your Comments

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

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

Other Queries

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

CHAPTER 2

PREPARING FOR INSTALLATION

This chapter provides important information to take into account before the installation can begin. This chapter also includes an overview to the installation process.

The following sections are included:

- ▶ [Introduction to StoneGate SOHO Firewalls](#) (page 10)
- ▶ [Overview to the Installation Procedure](#) (page 10)
- ▶ [Important to Know Before Installation](#) (page 11)
- ▶ [Selecting a Wireless Access Mode](#) (page 12)

Introduction to StoneGate SOHO Firewalls

StoneGate SOHO firewalls are primarily meant for connecting a small branch office or a home office to the general corporate network. SOHO firewalls have an integrated ADSL modem and they work as a wireless access point. Otherwise, they have a reduced feature set compared to other StoneGate firewalls. The SOHO firewall's main features include:

- **Simplified configuration:** the configuration is optimized for a remote office. Traffic filtering, NAT, and routing are set up simply by assigning a function to each interface.
- **Wireless LAN:** the appliances can be used as a wireless base station for 802.11b and 802.11g compatible clients. Different access profiles separate internal users from visitors.
- **IPsec VPN:** the appliances can establish an IPsec VPN to transparently provide the end-users secure access to corporate resources at a central location.
- **Integrated DHCP server:** the SOHO firewall can assign IP addresses to local clients.

StoneGate firewalls are always managed centrally through the StoneGate Management Center (SMC). You must have an SMC configured before you can proceed with installing the SOHO firewall appliances. The SMC can be used to manage a large number of different StoneGate products. The SMC installation is covered in a separate guide.

More background information on the SOHO firewalls and the SMC can be found in the *StoneGate Firewall/VPN Reference Guide*.

Overview to the Installation Procedure

You must have a working Management Center before you can start installing SOHO firewalls. The SOHO firewall installation proceeds as follows:

1. If network address translation (NAT) is applied to communications between the SOHO firewall and the Management Server and/or Log Server, define Contact Addresses. This is explained in [Configuring NAT Addresses](#) (page 13).
2. Define the SOHO Firewall element(s) in the Management Client. This is explained in [Creating SOHO Firewall Elements](#) (page 21).
3. Configure a VPN to encrypt traffic between the SOHO firewalls' protected network and other internal networks. This is explained in [Configuring a VPN](#) (page 41).
4. Generate the initial configuration file for the SOHO firewall appliance(s). This is explained in [Saving the Initial Configuration](#) (page 52).
5. Install and configure the SOHO firewall appliances. This is explained in the *Appliance Installation Guide* that is delivered with each appliance.

The chapters of this guide are organized in the order outlined above.

System Communications and NAT

If NAT (network address translation) is applied to the SOHO firewall's communications with the Management Server and/or Log Server, you must define the public IP address (contact address) for the servers to allow system communications. If the public address is missing, the SOHO firewall is not able to establish contact with the Management Center.

Internal Clients and NAT

The SOHO firewall applies NAT (network address translation) to any communications from its protected hosts to the Internet. The SOHO firewall's own external IP address is used in this dynamic NAT operation. This operation is fully automatic and needs no manual configuration. Communications must be transported over the TCP or UDP transport protocols (or encapsulated) to connect to the Internet directly, since TCP and UDP ports are required to track dynamically translated connections. Internet connections from company-internal clients may alternatively be relayed through a central StoneGate Firewall/VPN gateway to avoid local NAT at the SOHO firewall.

Licensing

SOHO firewall engines do not require a separate license file for licensing each individual SOHO firewall. However, the Management Server license may be limited to a certain number of managed engine components. Each five SOHO firewalls are counted together as just one managed unit.

Pre-Installed Firmware

StoneGate hardware appliances are pre-installed at the factory with the versions available at the time of manufacture. If you wish to upgrade to a new version, use the remote upgrade feature after the firewall is fully configured.

RADIUS Server for Wireless User Authentication

SOHO firewalls support the WPA Enterprise security mode. You can use any authentication server that supports the RADIUS protocol to authenticate wireless users (for example, Microsoft IAS or RSA Authentication Manager). The server must be configured to accept standard RADIUS wireless (WiFi) authentication requests from the SOHO firewall using the protected EAP (PEAP) mode.

Selecting a Wireless Access Mode

If you want to allow wireless access, decide on the level of security you want to provide for internal and/or visitor access. The security modes are explained in [Table 2.1](#).

Table 2.1 Security Modes

Security Mode	Name	Description
Disabled	None	Traffic is not encrypted. Anyone within range can freely use the access point and intercept any of the transferred data. This mode is not recommended, but it may be appropriate for guest access. We recommend you always encrypt internal communications.
WEP	WEP 40	Traffic is encrypted with a 40-bit WEP (Wired Equivalent Privacy/Wireless Encryption Protocol) key. Users must enter the pre-shared key for access. This mode is not recommended, but it may be appropriate for guest access or if using it is necessary for compatibility reasons. WEP 104 is more secure than WEP 40.
	WEP 104	Traffic is encrypted with a 104-bit WEP key. Users must enter the pre-shared key for access. This mode may be appropriate for guest access or if using it is necessary for compatibility reasons. WEP 104 is more secure than WEP 40.
WPA-PSK	WPA (with TKIP encryption)	Traffic is encrypted with TKIP (Temporal Key Integrity Protocol) encryption. Users must enter the pre-shared key for access. AES is more secure than TKIP.
	WPA2 (with AES encryption)	Traffic is encrypted with AES (Advanced Encryption Standard) encryption. Users must enter the pre-shared key for access. AES is more secure than TKIP.
	WPA and WPA2	Traffic is encrypted with TKIP or AES depending on client capabilities. Users must enter the pre-shared key for access.
WPA Enterprise	WPA (with TKIP encryption)	An external RADIUS server is used to authenticate the users. Traffic is encrypted with TKIP. AES is more secure than TKIP.
	WPA2 (with AES encryption)	An external RADIUS server is used to authenticate the users. Traffic is encrypted with AES. This security mode is currently considered the most secure of the options available.
	WPA and WPA2	An external RADIUS server is used to authenticate the users. Traffic is encrypted with TKIP or AES depending on client capabilities.

CHAPTER 3

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 from the SOHO firewall to the Management Center components and/or a remote VPN gateway.

The following sections are included:

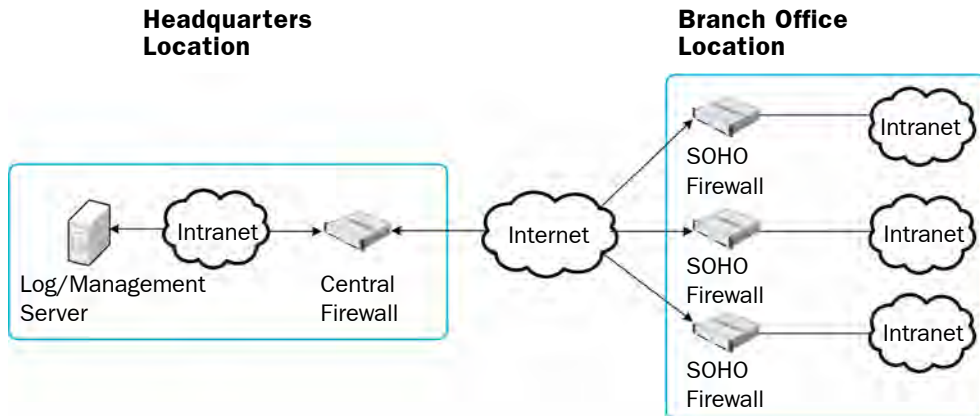
- ▶ [Configuration Overview](#) (page 14)
- ▶ [Defining Locations](#) (page 15)
- ▶ [Adding SMC Server Contact Addresses](#) (page 17)
- ▶ [Adding the Central Firewall Contact Address](#) (page 18)

Configuration Overview

If there is *network address translation* (NAT) between communicating system components, the translated IP address may have to be defined for system communications and VPN connectivity. You use *Location* elements to configure StoneGate components for NAT. If NAT is applied between two system components, you separate them into different Locations.

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 3.1 A Scenario for Using Locations



In the illustration above, several remote SOHO firewalls are managed through SMC Servers at a central site. NAT is typically applied at one or more of 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 SOHO 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 VPNs from the SOHO firewalls to the central site using that address.
- NAT may also be applied at a remote site (by external equipment) to translate the IP address of a SOHO firewall. In this case, a contact address is not needed because other components do not open connections to SOHO firewalls.

When contact addresses are needed, a single Location to group all SOHO firewalls is usually enough. The Management Server, Log Server, and central firewall can be left in their current Location. The SMC servers' and the central firewall's definitions must include a contact address for the SOHO Firewalls' Location. Proceed as follows:

1. Define Location element(s). See [Defining Locations](#) (page 15).
2. Define contact addresses for the Management Server(s) and Log Server(s). See [Adding SMC Server Contact Addresses](#) (page 17).
3. If NAT is applied to a central firewall's VPN endpoint IP address, define a contact address for the firewall interface in question. See [Adding the Central Firewall Contact Address](#) (page 18).
4. Select the correct Location for SOHO firewalls when you create the SOHO Firewall elements. See [Creating SOHO Firewall Elements](#) (page 21).

Defining Locations

The first task is to classify the components with Location elements based on which components are on the same side of a NAT device. There is a Default Location to which all elements belong if you do not assign them a specific Location.

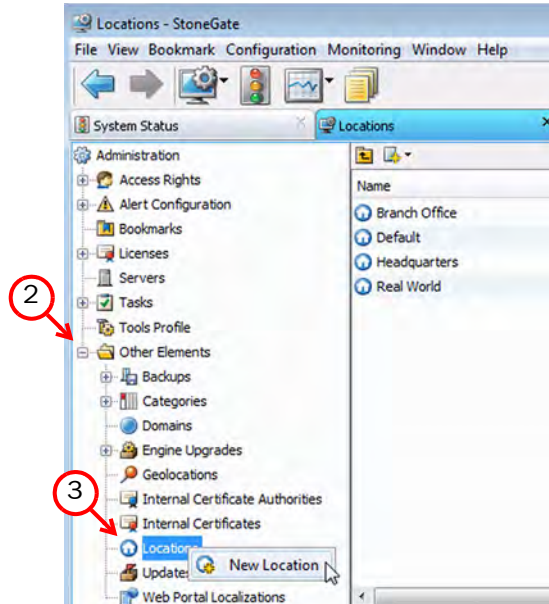
The steps below instruct you to create a new Location element that can be used for all SOHO firewalls. The Management Center components can stay in their current Location (Default or something else you have defined). If there are previously configured Locations in the system, you may be able to reuse an existing Location instead of creating a new one. Some configurations may require additional Locations.

▼ To create a new Location for SOHO firewalls

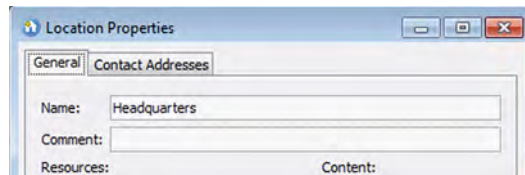
1. Click the Configuration icon in the toolbar and select **Administration**. The Administration Configuration view opens.



2. Expand **Other Elements** in the tree view.



3. Right-click **Locations** and select **New Location** from the menu. The Location properties dialog opens.



4. Type in a **Name**.

5. Click **OK**.

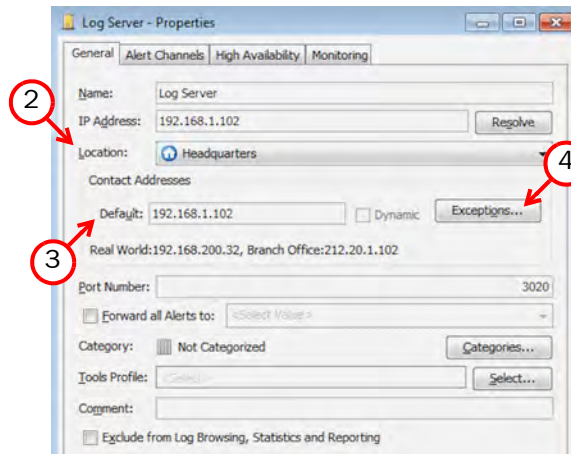
Adding SMC Server Contact Addresses



Note – SOHO firewalls can only utilize one IP address per component for the management connections. Multi-Link or automatic switch-over to a backup Management Server are not supported.

▼ To define the SMC Server contact addresses

1. Right-click the Management Server or Log Server and select **Properties**. The Properties dialog for that server opens.



2. Make sure the **Location** is different from the Location of the SOHO firewalls.
3. Enter the **Default** contact address (the server's translated external IP address). It is used by default whenever a component that belongs to another Location connects to the server.
4. If the SOHO firewalls cannot use the Default contact address to contact the server, click **Exceptions** to define a contact address for the SOHO firewalls' Location.
5. Click **OK** to close the Server element's properties and define the contact addresses for other servers in the same way.



Note – Elements that are grouped in the same Location element never use the contact address when communicating with each other.

What's Next?

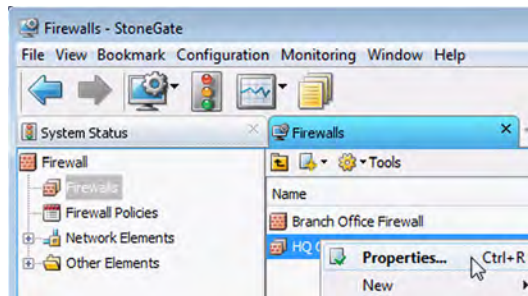
- ▶ If the central firewall's VPN endpoint address is translated by external equipment, continue by [Adding the Central Firewall Contact Address](#) (page 18).
- ▶ Otherwise, continue by [Creating SOHO Firewall Elements](#) (page 21).

Adding the Central Firewall Contact Address

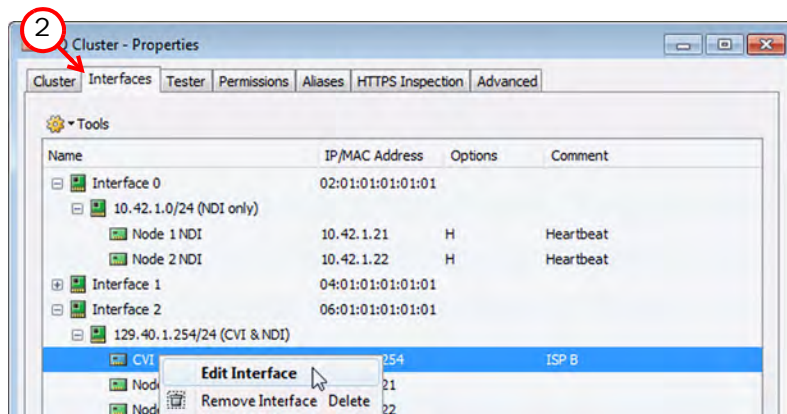
The SOHO firewall is designed to establish a VPN to a central StoneGate firewall to provide access to internal resources. If the central firewall/VPN gateway has a private IP address (translated by external equipment), you must define the public IP address as a contact address to support the VPN. If the central firewall is clustered, you must also define a contact address for the CVI address (as opposed to the NDI address).

▼ To define the central firewall's contact address

1. In the Firewall Configuration view, right-click a Firewall or Firewall Cluster element and select **Properties**. The properties dialog for the firewall opens.

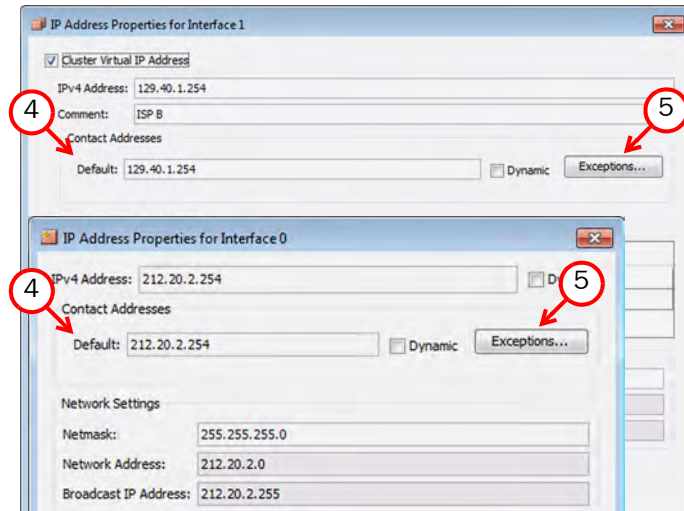


2. Switch to the **Interfaces** tab.



3. Open the properties for an Internet-facing interface:
 - On single firewalls, right-click an IP address and select **Edit IP Address**.
 - On firewall clusters, right-click a CVI address and select **Edit Interface**.

4. Enter a **Default** contact address for the interface or select **Dynamic** if the default contact address is dynamic. The Default contact address is used by default whenever a component that belongs to another Location connects to this interface.



5. If the SOHO firewalls cannot use the Default contact address to connect to the interface, click **Exceptions** to define a contact address for the SOHO firewalls' Location.



Note - SOHO firewalls do not support Multi-Link, so the SOHO firewalls can use only one endpoint even if the central site has several Internet links.

After all necessary contact addresses are defined, you can proceed to configuring the SOHO firewall settings. Continue by [Creating SOHO Firewall Elements](#) (page 21).

CHAPTER 4

CREATING SOHO FIREWALL ELEMENTS

SOHO firewalls are configured and managed centrally through the StoneGate Management Center. The configuration is transferred to the appliance from the Management Server. For this reason, the SOHO firewall settings must be configured in the Management Center before installation. This chapter explains how you can create new SOHO Firewall elements one by one or through a wizard that creates multiple SOHO Firewall elements simultaneously.

The following sections are included:

- ▶ [Configuration Overview](#) (page 22)
- ▶ [Creating New SOHO Firewall Elements](#) (page 22)
- ▶ [Selecting Interface Types](#) (page 26)
- ▶ [Configuring External Interfaces](#) (page 27)
- ▶ [Configuring Corporate and Guest Interfaces](#) (page 31)
- ▶ [Finishing the SOHO Firewall Configuration](#) (page 39)

Configuration Overview

You must have the StoneGate Management Center (SMC) installed and running to be able to configure the SOHO firewalls. The configuration is done using the StoneGate Management Client.

The tasks you must complete are as follows:

1. Create SOHO Firewall elements. See [Creating New SOHO Firewall Elements](#) (page 22).
2. Select the role of each network port. See [Selecting Interface Types](#) (page 26).
3. Define settings for the External (Internet) interface. See [Configuring External Interfaces](#) (page 27).
4. Define settings for the Corporate (internal network) and Guest (visitor network) interfaces. See [Configuring Corporate and Guest Interfaces](#) (page 31).
5. If you created multiple elements using the wizard, fill in the details that must be entered individually for each generated SOHO firewall. See [Finishing the SOHO Firewall Configuration](#) (page 39).

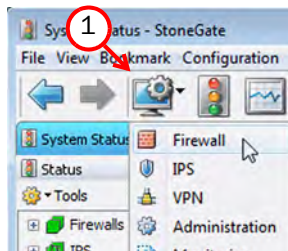
Creating New SOHO Firewall Elements

To introduce SOHO firewall engines to the Management Center, you must create SOHO Firewall elements that define and store the configuration information.

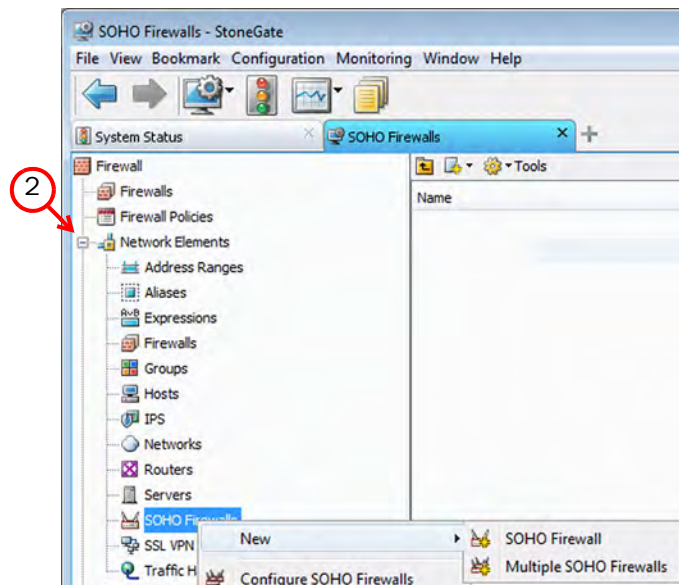
You can either create the elements one by one or use a wizard to generate several elements if you want them to have the same general configuration.

▼ To create SOHO Firewall elements

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



2. Browse to **Network Elements**→**SOHO Firewalls**.



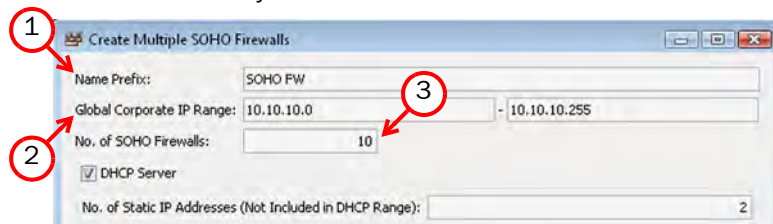
3. Right-click **SOHO Firewalls** and:

- select **New**→**SOHO Firewall** to create one new element.
- select **New**→**Multiple SOHO Firewalls** to launch the wizard for creating several elements.

If you are creating a single element, you can proceed directly to [Defining Basic Properties](#) (page 25). If you are creating multiple elements using the wizard, you will first need to supply information necessary for generating the elements.

▼ **To supply information for generating multiple SOHO Firewall elements**

1. Enter the **Name Prefix**. The system adds a number to this to name each element.



2. Enter the **Global Corporate IP Range** you want to use for the internal networks.

3. Enter the number of SOHO Firewall elements you want to create.

4. (Optional) If you want to use only static IP addresses in the internal network, deactivate **DHCP Server**.

5. If you left the DHCP server active, give a number for static addresses that are reserved from the beginning of the internal IP address range of each firewall. The minimum amount is one static IP address (for the SOHO firewall itself).

- Click **Generate** to create the name and IP address information for the SOHO Firewall elements.

Name	Corporate Local IP Addr...	Corporate Local Network	Corporate DHCP Addr...
SOHO FW - 000	10.10.10.1	10.10.10.0/28	10.10.10.4 - 10.10.10.14
SOHO FW - 001	10.10.10.17	10.10.10.16/28	10.10.10.20 - 10.10.10.30
SOHO FW - 002	10.10.10.33	10.10.10.32/28	10.10.10.36 - 10.10.10.46
SOHO FW - 003	10.10.10.49	10.10.10.48/28	10.10.10.52 - 10.10.10.62
SOHO FW - 004	10.10.10.65	10.10.10.64/28	10.10.10.68 - 10.10.10.78
SOHO FW - 005	10.10.10.81	10.10.10.80/28	10.10.10.84 - 10.10.10.94
SOHO FW - 006	10.10.10.97	10.10.10.96/28	10.10.10.100 - 10.10.10.110
SOHO FW - 007	10.10.10.113	10.10.10.112/28	10.10.10.116 - 10.10.10.126
SOHO FW - 008	10.10.10.129	10.10.10.128/28	10.10.10.132 - 10.10.10.142
SOHO FW - 009	10.10.10.145	10.10.10.144/28	10.10.10.148 - 10.10.10.158



Note – If you want to modify any of the information in the table, change the values and click **Generate** again. More detailed modifications are possible only after the wizard is complete and the elements have been generated.

- Click **Next**. The General tab opens.

Defining Basic Properties

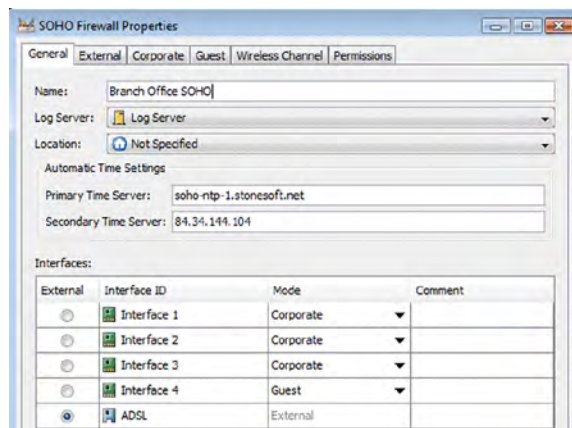
If you are configuring multiple elements using the wizard, some of the settings are not available because they are generated based on the information on the first page of the wizard or because they must be defined individually for each generated element.

The time settings of SOHO firewall appliances are automatically synchronized with an NTP server. Stonesoft maintains NTP servers that are freely available for all SOHO Firewall users at the following addresses:

- soho-ntp-1.stonesoft.net: 192.89.38.174 (default Primary Time Server)
- soho-ntp-2.stonesoft.net: 84.34.144.104 (default Secondary Time Server)

▼ To define the basic properties

1. (Not available in wizard) Type in a **Name**.



External	Interface ID	Mode	Comment
<input type="radio"/>	Interface 1	Corporate	
<input type="radio"/>	Interface 2	Corporate	
<input type="radio"/>	Interface 3	Corporate	
<input type="radio"/>	Interface 4	Guest	
<input checked="" type="radio"/>	ADSL	External	

2. Select a **Log Server** for storing the produced log data.
3. If required due to NAT, select the **Location** (see [Configuring NAT Addresses](#) (page 13)).
4. (Optional) Enter the IP address or hostname of your NTP Server in at least the **Primary Time Server** field.



Caution – The SOHO firewall must be able to contact the NTP server over the Internet at the time of installation. Otherwise the installation fails. If you use an NTP server maintained by your organization, make sure it can be reached through the Internet (the VPN is not used for the time queries).

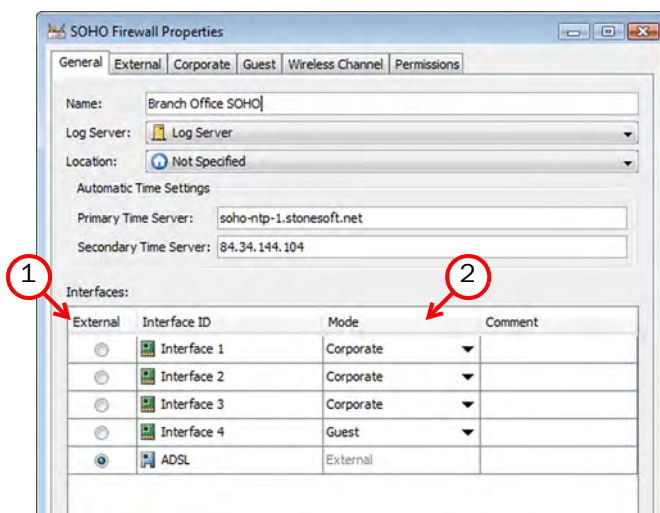
Selecting Interface Types

The types assigned to the SOHO firewalls' network ports affects routing and the rules for filtering traffic as follows:

- The *External* interface routes traffic to and from the Internet. The external IP address is used for dynamic source address translation if the protected clients are allowed direct Internet connections. The configuration must contain an External port.
- *Corporate* interfaces are for internal hosts. They allow both inbound and outbound connections through the VPN and the other Corporate ports. Corporate interfaces can also allow direct outbound connections to the Internet depending on your selection. Wireless Corporate access can also be activated as needed. Each SOHO firewall usually has at least one physical Corporate interface. However, you can also provide only wireless access through the Corporate interface without allocating a physical port for the Corporate interface.
- *Guest* interfaces are for visitor access. They allow only outgoing connections to the Internet. There is no connectivity between different Guest ports. Wireless Guest access can also be activated as needed. The configuration does not have to contain any Guest ports. You can provide wireless access through the Guest interface also without allocating a physical port for the Guest interface.

▼ To select the interface types

1. Select the External interface (for Internet access): either **ADSL** or one of the Ethernet interfaces 1-4.



2. Select the interface modes:

- Select the **Corporate** interface(s) and optionally the **Guest** interface(s) if you want to allocate physical ports for them.
- Select **Disabled** for the interfaces that you do not want to use.



Note – A local browser-based administration tool is available through interface 1. If you allocate one or more physical ports for Corporate interfaces, we recommend that you designate interface 1 as a Corporate interface.

Configuring External Interfaces

To configure the External interface, continue as follows:

- If the External interface is an ADSL line or uses PPPoE, proceed to [Configuring an External Interface for ADSL or PPPoE](#) (page 27).
- If the External interface is a regular Ethernet interface (connected to an external router), proceed to [Configuring an External Interface for Standard Ethernet](#) (page 29).

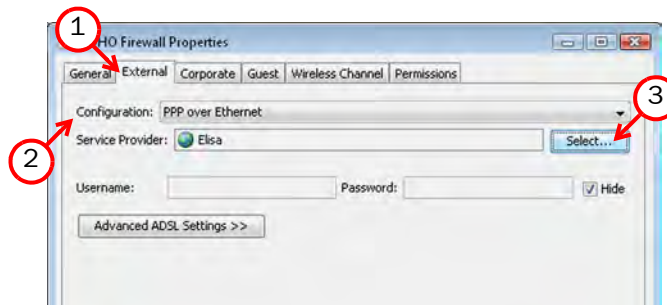
Configuring an External Interface for ADSL or PPPoE



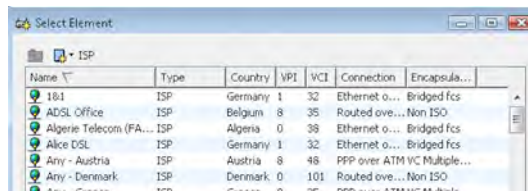
Note – A username and password are required for ADSL access. These details must be entered in the properties of each individual element. They are not available in the wizard.

▼ To select ISP settings for ADSL or PPPoE

1. Switch to the **External** tab.

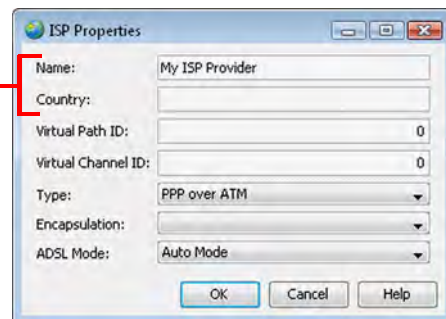


2. (Ethernet ports only) Select **PPP over Ethernet** as the **Configuration**.
3. Click **Select** for **Service Provider**. The Select Element dialog opens.



4. Select your service provider from the list and click **Select**.
 - If your service provider is not listed, create a new ISP element using the New icon (see the next illustration).

- The **Name** and **Country** are only for your reference.
- Fill in the other settings according to information supplied by your service provider.



The rest of the settings on the External tab depend on the type of Internet connection you have. See the two illustrations below for the two different versions of the tab.

If you are creating multiple SOHO Firewalls using the wizard, you cannot enter the settings shown in the illustrations on this page. The settings must be added to the properties of each SOHO Firewall element after the wizard is complete.

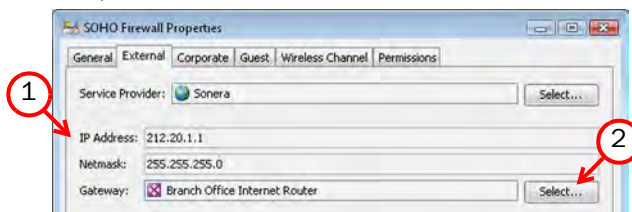
▼ To select additional settings (PPP over ATM or Ethernet over ATM)

- ➔ (Not available in wizard) Enter the ADSL **Username** and **Password**, and deselect **Hide** if you want to view the Password in cleartext in the SOHO firewall properties.

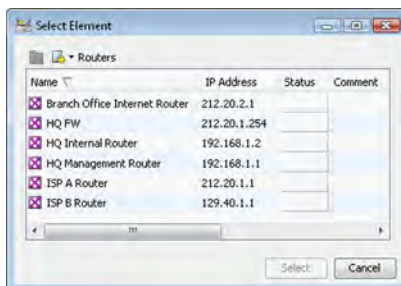


▼ To select additional settings (Routed over ATM)

1. (Not available in wizard) Enter the ADSL **IP Address** and **Netmask**.



2. (Not available in wizard) Click **Select** for **Gateway**.



3. (Not available in wizard) Select a Router element from the list and click **Select**.
 - You can add a new Router to the list through the New icon. Only a name and IP address are needed for the new element.

What's Next?

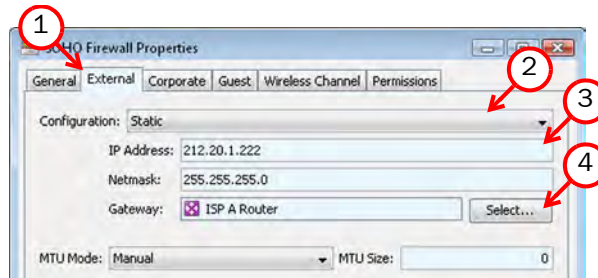
- ▶ If you want to define static DNS servers for the External and Guest Interfaces, proceed to [Defining DNS Servers for the External and Guest Interfaces](#) (page 30).
- ▶ Otherwise, continue by [Configuring Corporate and Guest Interfaces](#) (page 31).

Configuring an External Interface for Standard Ethernet

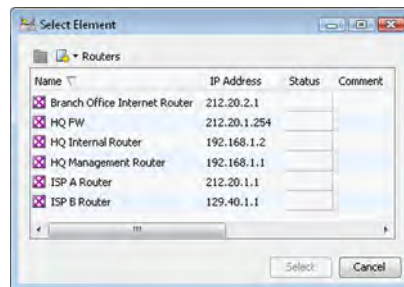
If you are configuring multiple SOHO firewalls using the wizard, any static IP addresses must be entered individually after the elements have been created.

▼ To configure the External Interface for a standard Ethernet connection

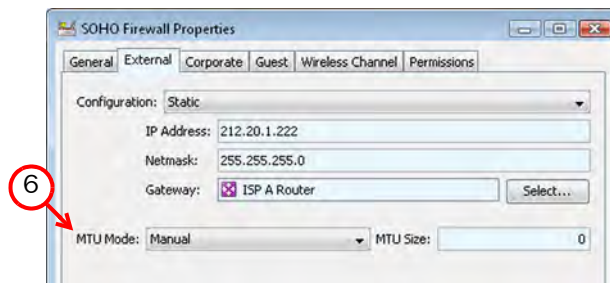
1. Switch to the **External** tab.



2. Select the IP address allocation method from **Configuration**:
 - **DHCP** for normal dynamic IP address. Proceed to [Step 6](#).
 - **Static** for a static IP address.
3. (Static only, not available in wizard) Enter the **IP Address** and **Netmask** for the external interface of the SOHO firewall.
4. (Static only, not available in wizard) Click **Select** for **Gateway**. The Select Element dialog opens.



5. (Static only, not available in wizard) Select a Router element from the list and click **Select**.
 - You can add a new Router to the list through the New icon. Only a name and IP address are needed for the new element.



6. Select the **MTU Mode**:
 - **Automatic** determines MTU based on ICMP messages.
 - **Manual** lets you set the MTU yourself.

7. For the manual mode, type in the MTU. The largest possible value is 1500.

What's Next?

- ▶ If you want to define DNS servers for the External and Guest interfaces, proceed to [Defining DNS Servers for the External and Guest Interfaces](#) (page 30).
- ▶ Otherwise, continue by [Configuring Corporate and Guest Interfaces](#) (page 31).

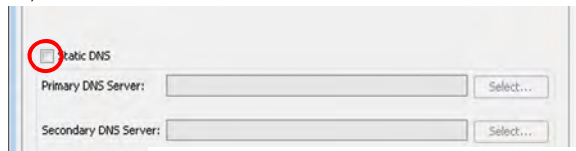
Defining DNS Servers for the External and Guest Interfaces

By default, the SOHO firewall uses the DNS settings it has received from the local (ISP) DNS servers on all its interfaces. However, you can also define which DNS server(s) are used for distributing IP addresses and for resolving the primary and secondary NTP servers' IP addresses.

You can define DNS server settings on the External or Corporate tabs. By default, the static DNS server settings that you define on the External tab are used for all the interfaces (External, Corporate, and Guest interfaces). However, you can also define DNS server settings separately for the Corporate interface on the Corporate tab (see [Defining DNS Servers for the Corporate Interface](#) (page 32)).

▼ To define static DNS server(s) for the External and Guest interfaces

- ➔ On the **External** tab, select **Static DNS** and define the DNS server(s) in the fields below.



The screenshot shows a configuration window titled "Static DNS". It contains two rows of input fields. The first row is labeled "Primary DNS Server:" and has a text input field followed by a "Select..." button. The second row is labeled "Secondary DNS Server:" and has a text input field followed by a "Select..." button. A red circle highlights the "Static DNS" title in the top left corner of the window.

Configuring Corporate and Guest Interfaces

Each SOHO firewall has just one IP address for each interface type (default gateway for the clients). Corporate and Guest addresses are used on all relevant ports depending on interface type selection, as well as with the wireless Corporate/Guest connection.

If you are creating multiple elements using the wizard, you cannot enter any IP addresses on the Corporate tab, including the DHCP options. These settings were generated on the wizard's first screen.



Note – For VPN traffic routing, each SOHO firewall must have a unique Corporate address space. The SOHO firewall does not NAT the addresses in the VPN.

▼ To define the Corporate interface settings

1. Switch to the **Corporate** tab.

The screenshot shows the 'SOHO Firewall Properties' dialog box with the 'Corporate' tab selected. The 'Local IP Address' is set to 192.168.0.1 and the 'Netmask' is 255.255.255.0. The 'VPN' section has an empty 'SOHO Gateway Group' field and a 'Pre-Shared Key' field with a 'Generate' button. The 'DHCP Service' is checked, with a 'DHCP Address Range' of 192.168.0.100 to 192.168.0.199. There are 'Select...' buttons for 'Corporate Primary DNS Server' and 'Corporate Secondary DNS Server'. The 'Wireless' section has 'Wireless Network Name (SSID)' and 'Wireless SSID Broadcast' (Enabled) fields. The 'Security Policy' section has a 'Security Policy' dropdown set to 'Disabled' and a checkbox for 'Allow only traffic to VPN'.

2. (Not in wizard) Enter the **Local IP Address** and **Netmask** of the SOHO Firewall in the internal network.
3. If there is a previously defined VPN, click **Select** to choose the correct existing **SOHO Gateway Group**. If you do not have a VPN configured, leave the setting empty for now.
4. (Optional) Select **Keep-alive VPN tunnel** to prevent idle VPN tunnels from closing.
5. (Not in wizard) If you want the SOHO Firewall to act as a DHCP server for the Corporate network, select **DHCP Service** and define a unique internal address range for distributing addresses. You can optionally also define DNS server(s) for distributing the addresses in the fields below (see [Defining DNS Servers for the Corporate Interface](#) (page 32)).
6. (Optional) To prevent direct connections to the Internet, select **Allow only traffic to VPN** (Internet traffic may then be relayed through the VPN).
7. If Guest access is allowed, define the settings for Guest now. The wireless settings you see on this tab are identical on both the Corporate and Guest tabs. They are explained together in the section [To define the Guest interface settings](#) (page 33).

Defining DNS Servers for the Corporate Interface

By default, the SOHO firewall uses the DNS settings it has received from the local (ISP) DNS servers on all its interfaces. You can alternatively specify the DNS servers on the External or on the Corporate tab. The static DNS server settings that you define on the External tab (see [Defining DNS Servers for the External and Guest Interfaces](#) (page 30)) are applied by default to all the SOHO interfaces (External, Corporate, and Guest interfaces). However, you can alternatively define DNS server settings specifically for the Corporate interface on the Corporate tab.

▼ To define DNS server(s) for the Corporate Interface

- ➔ (Not in wizard; optional) Define the **Corporate Primary DNS Server** and optionally the **Corporate Secondary DNS Server**:
 - If you want to use the DNS settings from the local (ISP) DNS servers as the first choice, leave the **Corporate Primary DNS Server** field to its default value.
 - Click **Select** to select a static (internal) DNS server as the **Corporate Primary DNS Server** or **Corporate Secondary DNS Server**.

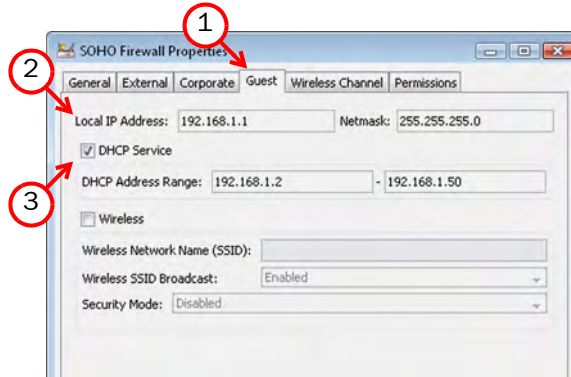
The screenshot shows a configuration window for the Corporate interface. The 'DHCP Service' checkbox is checked. The 'DHCP Address Range' is set to 192.168.0.100 - 192.168.0.199. The 'Corporate Primary DNS Server' field is set to 'Use the External DNS Server' with a red arrow pointing to it. The 'Corporate Secondary DNS Server' field is also set to 'Use the External DNS Server'. Below these are fields for 'Wireless Network Name (SSID)', 'Wireless SSID Broadcast' (set to 'Enabled'), and 'Security Mode' (set to 'Disabled'). At the bottom, there is a 'Security Policy' section with a checkbox for 'Allow only traffic to VPN' which is unchecked. The dialog has 'OK', 'Cancel', and 'Help' buttons at the bottom right.

What's Next?

- ▶ If you want to define wireless access, continue by [Defining Security Settings for Wireless Access](#) (page 34).
- ▶ If you want to define the settings for the Guest interface(s), proceed to the section [To define the Guest interface settings](#) (page 33).
- ▶ Otherwise, the interface definition of your SOHO Firewall is now ready. Continue by [Finishing the SOHO Firewall Configuration](#) (page 39).

▼ To **define the Guest interface settings**

1. Switch to the **Guest** tab.



2. Enter the **Local IP Address** and **Netmask** of the SOHO Firewall in the visitor network.
3. If you want the SOHO Firewall to act as a DHCP server for the Guest network, select **DHCP Service** and define the internal address range for distributing addresses.

The IP address information on the Guest tab is used only locally, so overlap between different SOHO firewalls is allowed.

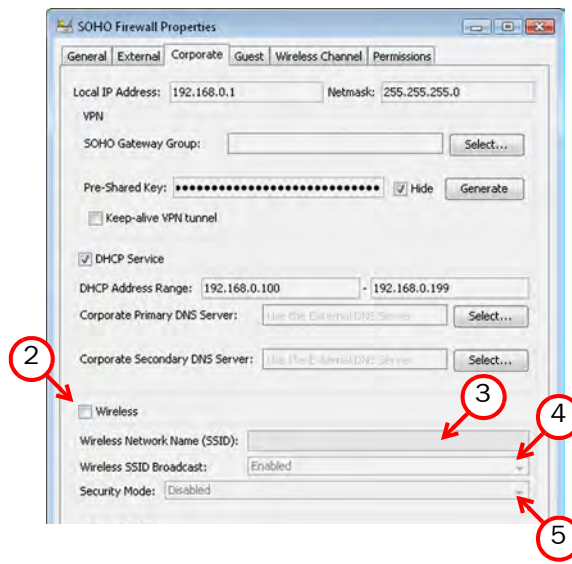
What's Next?

- ▶ If you want to define wireless access, continue by [Defining Security Settings for Wireless Access](#) (page 34).
- ▶ Otherwise, the interface definition of your SOHO Firewall is now ready. Continue by [Finishing the SOHO Firewall Configuration](#) (page 39).

Defining Security Settings for Wireless Access

▼ To define security settings for Corporate and/or Guest wireless access

1. Select the correct tab for the type of access.



2. Select **Wireless**. The options for wireless connections are enabled.
3. Enter the **Wireless Network Name**.
4. 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).
5. Select the **Security Mode** according to the security policy of your organization. The options for that mode are enabled. See [Table 4.1](#).
6. Repeat for the other tab as necessary (different settings can be selected freely).

WPA is more secure than WEP. Additional background information on the different security modes is provided in [Selecting a Wireless Access Mode](#) (page 12).

Table 4.1 Settings per Security Mode

Mode(s)	Setting(s)	Description
WEP 40	Default Key	Selects the key that clients must provide to gain access.
WEP 104	WEP Key 1...4	Pre-shared keys for authentication and encryption of communications. Fill in at least one key. For WEP 40, the keys must be 5 characters long. For WEP 104, the keys must be 13 characters long.

Table 4.1 Settings per Security Mode (Continued)

Mode(s)	Setting(s)	Description
WPA-PSK	WPA Mode	Either WPA, WPA2, or both. WPA uses TKIP encryption; WPA2 uses more secure AES encryption. WPA and WPA2 mode uses either TKIP or AES depending on client support.
WPA Enterprise	Pre-shared key	(WPA-PSK) Pre-shared key for authentication and encryption of communications. The key must be 8 - 63 characters long.
	RADIUS server	(WPA Enterprise) The RADIUS Server element that defines the external authentication server for authenticating users.

What's Next?

- ▶ If you selected WPA Enterprise, continue by [Defining a RADIUS Server for WPA Enterprise](#) (page 36).
- ▶ Otherwise, continue by [Defining General Wireless Settings](#) (page 38).

Defining a RADIUS Server for WPA Enterprise

See the documentation of your RADIUS server for information on how to allow the authentication requests from external components. The external server must be configured to accept standard RADIUS wireless (WiFi) authentication requests from the SOHO firewall using the protected EAP (PEAP) mode. Take care to ensure that the shared secret is defined identically in both StoneGate and on the external server.



Note – We recommend that you set up the RADIUS server at the central site and make it accessible only through the VPN. To route the traffic through the VPN, the RADIUS server's internal IP address must be included in the VPN definition and the external IP address must not be added as a Contact Address.

▼ To select a RADIUS Server element for authenticating wireless users

1. Click **Select** for **RADIUS Server**. The Select Element dialog opens.

SOHO Firewall Properties

General External Corporate Guest Wireless Channel Permissions

Local IP Address: 192.168.0.1 Netmask: 255.255.255.0

VPN

SOHO Gateway Group: [] Select...

Pre-Shared Key: [] Hide Generate

Keep-alive VPN tunnel

DHCP Service

DHCP Address Range: 192.168.0.100 - 192.168.0.199

Corporate Primary DNS Server: [] Select...

Corporate Secondary DNS Server: [] Select...

Wireless

Wireless Network Name (SSID): MoD8VTPd7rnkvk

Wireless SSID Broadcast: Disabled

Security Mode: WPA Enterprise (802.11i/TKIP) 1

WPA Mode: WPA2 (with AES Encryption)

Radius Server: [] Select...

2. If there is an existing element, select it and click **Select**.
 - If there is no suitable element yet, you can create a new one as explained in the next illustrations.

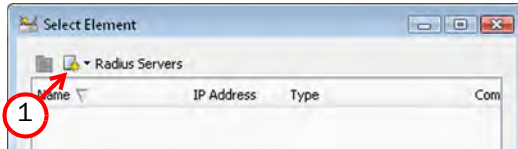
Select Element

Radius Servers

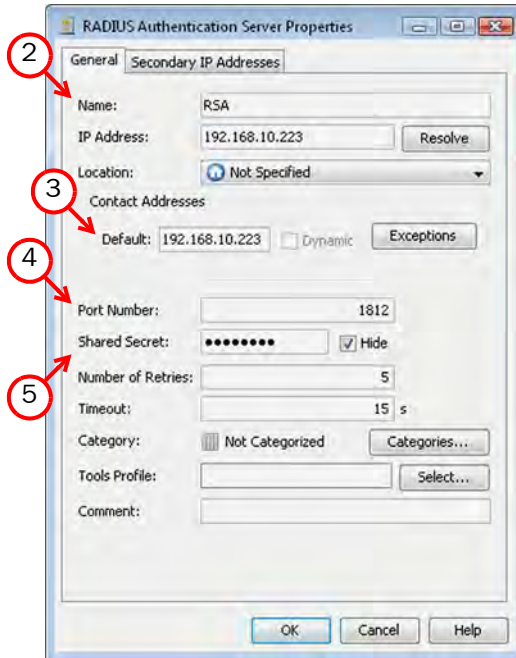
Name	IP Address	Type	Com
RSA	192.168.10.223	RADIUS Authentication Server	

▼ To create a RADIUS server element

1. Click the New icon and select **RADIUS Authentication Server**. The RADIUS Authentication Server Properties dialog opens.



2. Fill in the **Name** and **IP address**.



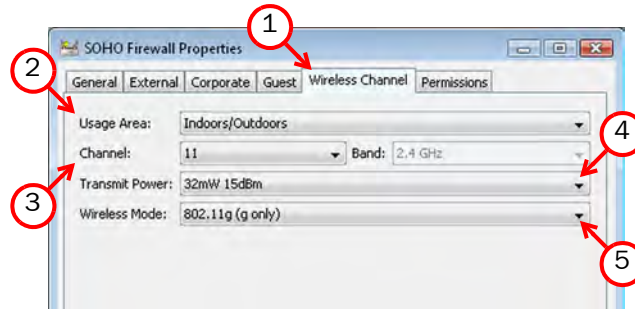
3. (Optional, not recommended) To route RADIUS traffic out of the VPN, add the external address as a **Default** contact address or click **Exceptions** to define a contact address for the SOHO firewalls' Location. See [Adding SMC Server Contact Addresses](#) (page 17).
4. Change the **Port Number** if your RADIUS server uses a non-standard port.
5. Enter the **Shared Secret** for authenticating the SOHO Firewall to the RADIUS server. Deselect **Hide** if you want to view the shared secret in cleartext in the RADIUS Server properties.
6. Click **OK** to return to the previous dialog.
7. Select the new element and click **Select**.

Defining General Wireless Settings

General wireless settings are common for both Corporate and Guest interfaces.

▼ To define general wireless settings

1. Switch to the **Wireless Channel** tab.

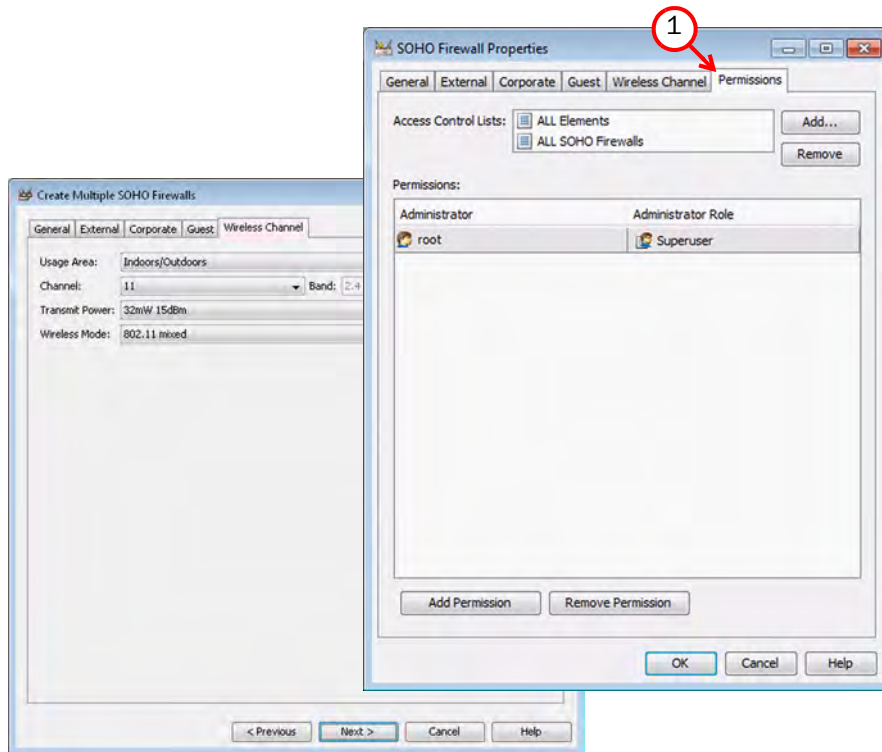


2. Select the **Usage Area**. This affects how the signal is transmitted.
3. Select the **Channel**. If there are other wireless access points nearby, use channels that are as far apart as possible to avoid interference.
4. Select the **Transmit Power** of the signal. Lower power reduces the area covered.
5. Select the **Wireless Mode** according to the capabilities of the connecting clients. Mixed modes work with both wireless-b and wireless-g clients, but carry a small performance penalty for faster wireless-g clients.

Finishing the SOHO Firewall Configuration

▼ To finish the configuration

1. (Not in wizard, optional) Switch to the **Permissions** tab and adjust the Administrator permissions.
 - All SOHO Firewall elements are automatically included in a dedicated Access Control List.



2. Click **OK** (single element) or **Next** (wizard).
3. (Wizard only) Check the information displayed in the summary and click **Create**.

If you configured multiple SOHO Firewall elements using the wizard, you may need to open the properties of the created elements (through the right-click menu) and fill in the following details:

- If the external interface of the SOHO Firewalls has a static IP address, fill in the IP Address, Netmask, and Gateway fields on the External tab of each created element.
- Enter the username and password on the External tab to include the information in the initialization file.

What's Next?

- ▶ If you want to create the VPN configuration so that the VPN can be used as soon as the appliance(s) are initialized, proceed to [Configuring a VPN](#) (page 41).
- ▶ If you want to initialize the appliance without configuring a VPN between the SOHO firewall(s) and the central corporate site at this time, you can proceed directly to [Initializing SOHO Firewall Appliances](#) (page 51). It is possible to configure a VPN later and then transfer the configuration to the SOHO firewalls remotely.

CHAPTER 5

CONFIGURING A VPN

The SOHO firewall can establish a VPN to a central StoneGate firewall. The VPN provides clients in the SOHO firewalls' Corporate network access to internal resources at the central site. This chapter describes the basic configuration steps for creating a VPN. For more detailed instructions, see the *Administrator's Guide* or the *Online Help* of the Management Client. For background information on IPsec VPNs, see the *Firewall/VPN Reference Guide*.

The following sections are included:

- ▶ [Overview to Configuring a VPN](#) (page 42)
- ▶ [Creating an Internal Gateway Element](#) (page 43)
- ▶ [Creating a SOHO Gateway Group](#) (page 45)
- ▶ [Creating a VPN Element](#) (page 46)
- ▶ [Creating VPN Access Rules for the Central Firewall](#) (page 48)

Overview to Configuring a VPN

This basic configuration scenario walks you through creating a secure VPN connection through the Internet between a central StoneGate firewall/VPN engine and a group of SOHO firewalls, all managed through the same Management Center. The Internet link on the central firewall/VPN engine must have a fixed IP address (not DHCP- or PPPoE-assigned). The address spaces protected by the different devices must not overlap (the Corporate networks of each SOHO firewall and the internal networks at the central site).

This scenario uses the **SOHO Suite** VPN Profile that contains the default VPN settings for SOHO firewalls. The profile uses pre-shared keys for authentication.

This scenario does not explain how to set up the VPN for forwarding connections from the SOHO firewalls' Corporate network through the central firewall/VPN engine to the Internet in cases where direct Internet connections through the SOHO firewalls are disabled. After configuring this basic scenario, see information about the additional configuration required in the *Administrator's Guide* PDF or the *Online Help* of the Management Client.

This basic configuration scenario does not explain all settings related to VPNs. For more information, consult the *Online Help* of the Management Client.

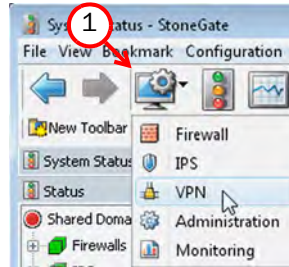
The configuration proceeds as follows:

1. Define VPN-related settings for the central firewall. See [Creating an Internal Gateway Element](#) (page 43). If you have already configured a Gateway element for the central firewall, reuse the same element for this VPN. There is no need to change any of the settings.
2. Create a SOHO Gateway Group element to represent the SOHO firewalls in the VPN. See [Creating a SOHO Gateway Group](#) (page 45).
3. Create the VPN element. See [Creating a VPN Element](#) (page 46).
4. Allow VPN access to the protected clients in the policy of the central firewall. See [Creating VPN Access Rules for the Central Firewall](#) (page 48).

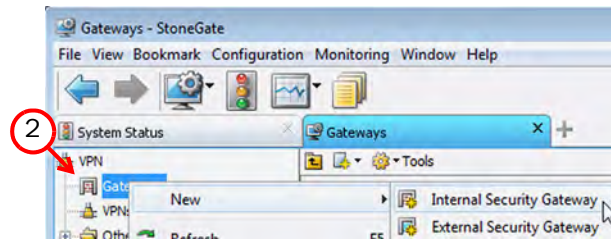
Creating an Internal Gateway Element

▼ To create an internal Gateway element

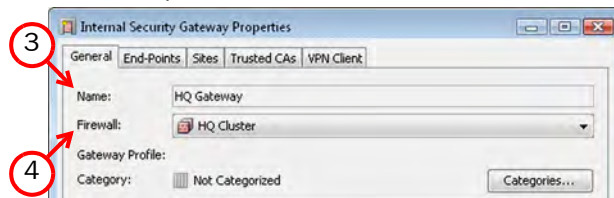
1. Click the Configuration icon in the toolbar and select **VPN**. The VPN Configuration view opens.



2. Right-click **Gateways** and select **New**→**Internal Security Gateway**.

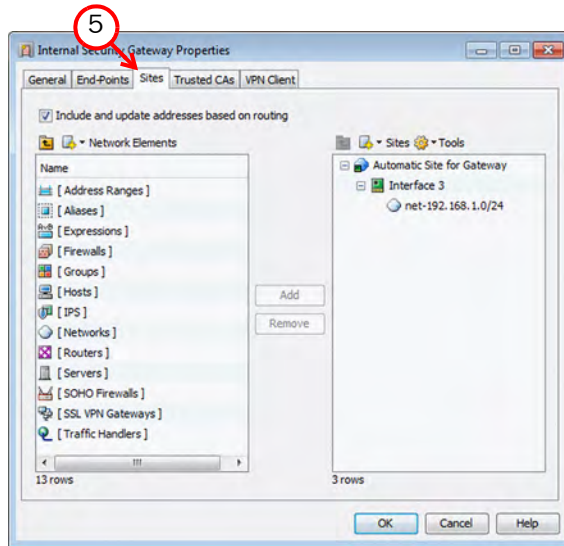


3. Give the new element a unique **Name**.



4. Select the **Firewall** that the Gateway element represents.
5. Switch to the **Sites** tab.
 - Sites define the addresses that are routable through the VPN.
 - Leave the **Include and Update Addresses Based on Routing** option selected if you want the Sites information to be automatically updated based on routing changes. If you want

to want define the Sites manually, deselect the option. See the *Online Help* for more information.



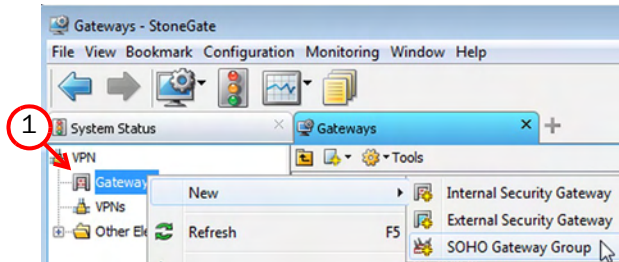
Note – If you plan to use NAT to translate the IP addresses of the internal hosts that make connections through this VPN, drag and drop the network(s) for the NAT address space on top of the (top-level) automatic Site element on the right and disable the corresponding interfaces that contain the untranslated IP addresses.

6. Click **OK**.

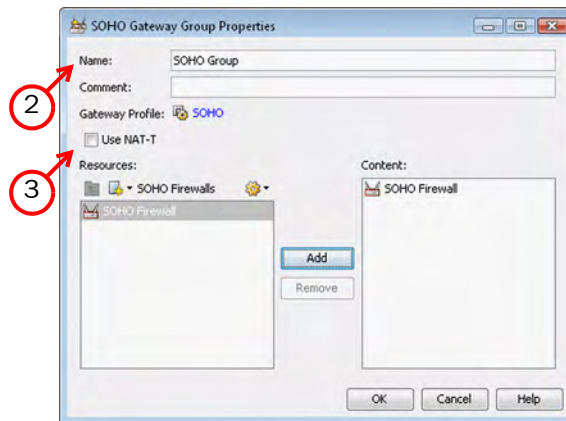
Creating a SOHO Gateway Group

▼ To create a SOHO Gateway Group element

1. Right-click **Gateways** and select **New**→**SOHO Gateway Group**.



2. Give the new element a unique **Name**.

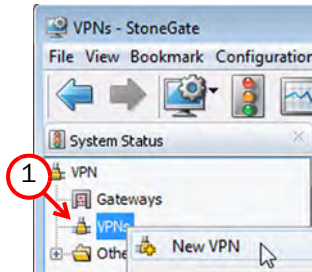


3. If the SOHO firewalls are behind a NAT device, select the **Use NAT-T** option.
4. Select the SOHO Firewall element(s) you want to include in the VPN and click **Add**. Each SOHO firewall can belong to only one SOHO Gateway Group.
5. Click **OK**.

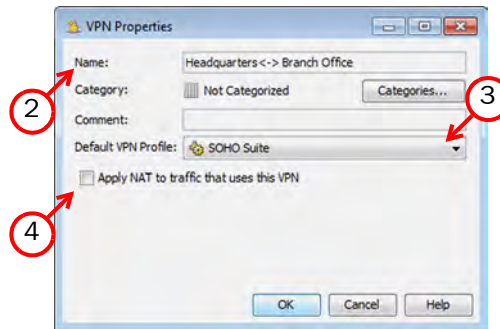
Creating a VPN Element

▼ To create a VPN element

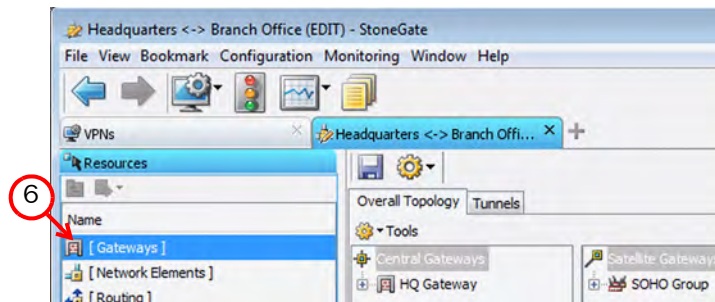
1. Right-click **VPNs** and select **New VPN**.



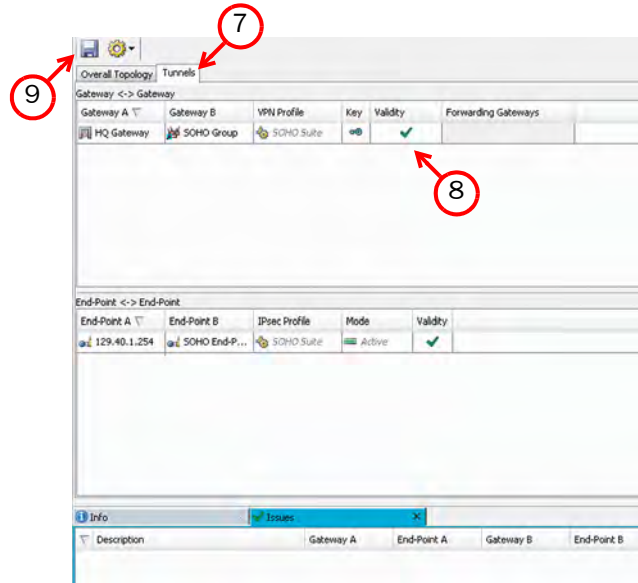
2. Give the new element a unique **Name**.



3. Select **SOHO Suite** from the **Default VPN Profile** list. The VPN Profile defines IPsec settings.
4. If you want to NAT traffic that goes through the VPN, select the **Apply NAT to Traffic That Uses This VPN** option.
5. Click **OK**. The VPN opens for editing.
6. Expand **Gateways** and drag and drop the element for the central gateway to Central Gateways and the SOHO Gateway Group to Satellite Gateways.



7. Switch to the **Tunnels** tab.



8. Check that the **Validity** columns have a green check mark.

- If the **Validity** column of a tunnel has a warning icon, see the **Issues** panel (if the panel is not displayed, open it through the **View** menu).

9. Click the Save icon in the view-specific toolbar.



Caution – Change the pre-shared encryption keys periodically (for example, monthly) to ensure continued confidentiality of the data. These encryption keys are set in the properties of the SOHO Firewall elements (on the Corporate tab).

Creating VPN Access Rules for the Central Firewall

On the central firewall, the Access rules define which connections are forwarded to the VPN and which connections are allowed out of the VPN. The two rules in this example always allow new connections in both directions when the VPN tunnel is already open. However, if a SOHO firewall has a dynamic external IP address, the VPN can only be opened by a connection originating from the SOHO firewall's protected networks.

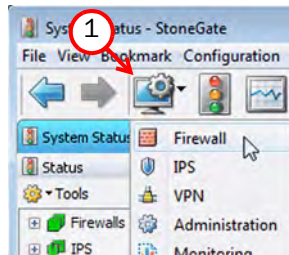
If you are unfamiliar with creating Access rules, see the *Online Help* of the Management Client for more detailed information.



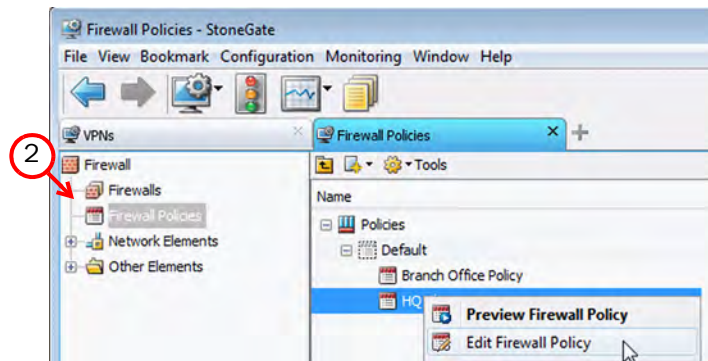
Note – Make sure that the rule order and the scope of the rules are correct. Traffic that is not routable through the selected VPN is dropped if it matches these rules.

▼ To create VPN Access rules

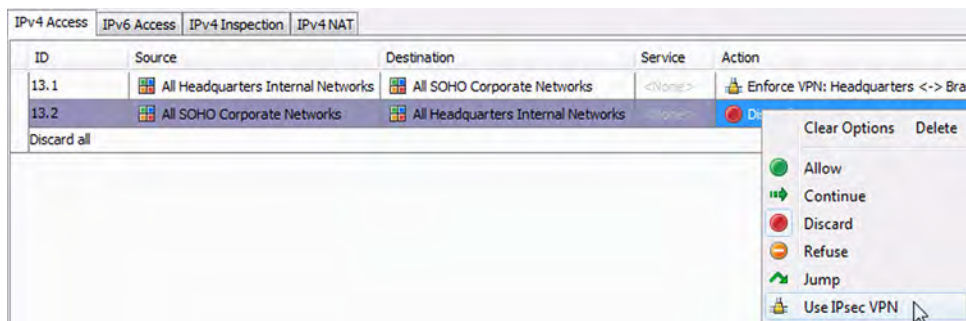
1. Click the Configuration icon in the toolbar and select **Firewall**. The Firewall Configuration view opens.



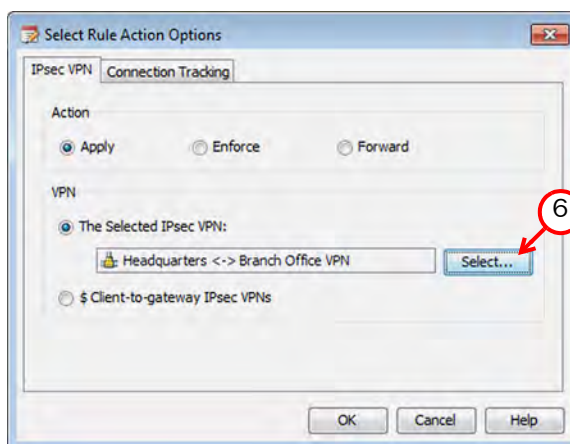
2. Select **Firewall Policies** in the Firewall tree.



- Right-click the central firewall's policy and select **Edit Firewall Policy**. The policy opens for editing.



- Create two new rules and set the **Source**, **Destination**, and **Service** to allow the desired traffic between the clients in the SOHO firewalls' Corporate networks and the internal resources at the central site.
- Right-click the **Action** cell and select **Use IPsec VPN**. The Select Rule Action Options dialog opens.



- Select the correct VPN element and click **OK**.

If you want to ensure that the connections through the VPN are logged, set the logging options for this rule to **Stored**. Activate the connection closing and accounting logging as well if you want to create reports based on traffic volumes. Remember to refresh the policy of the central firewall to activate the new configuration in anticipation of the SOHO firewalls coming online. The VPN is established when there is traffic that needs to use the VPN.

What's Next?

- ▶ Continue by [Initializing SOHO Firewall Appliances](#) (page 51).

CHAPTER 6

INITIALIZING SOHO FIREWALL APPLIANCES

To initialize the SOHO firewall and pair it with the Management Server, you will export a configuration file and import it to the corresponding SOHO firewall appliance. After this initial configuration import is done, the appliance can be fully managed, monitored, and upgraded remotely.

The following sections are included:

- ▶ [Allowing SOHO Communications Through a Central Firewall](#) (page 52)
- ▶ [Saving the Initial Configuration](#) (page 52)

Allowing SOHO Communications Through a Central Firewall

For monitoring, log transmissions, and remote management, any intermediary firewall (including any StoneGate firewall) must be set to allow the following communications:

Table 6.1 SOHO Firewall Management Communications

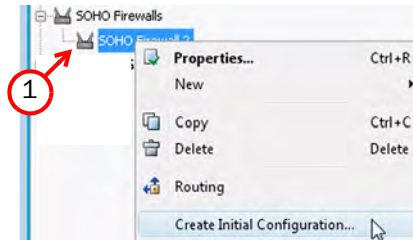
Source	Destination	Port	Service Element Name
SOHO firewall	Management Server	TCP 8924	SG SOHO Initial Contact
SOHO firewall	Management Server	TCP 8922	SG SOHO Control
SOHO firewall	Log Server	TCP 8923	SG SOHO Log

Saving the Initial Configuration

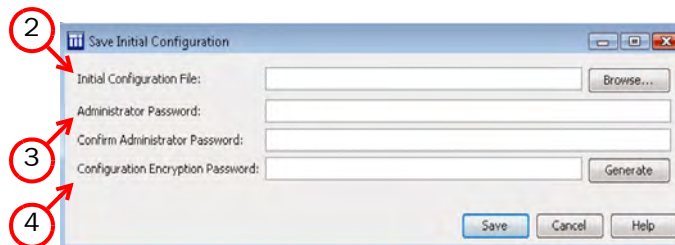
The SOHO firewall engines are initialized by importing an initial configuration file through the SOHO firewall's web interface.

▼ To export the initial configuration file

1. Right-click a SOHO Firewall element and select **Create Initial Configuration** or **Configuration**→**Create Initial Configuration** from the menu. The Save Initial Configuration dialog opens.



2. Select where the initial configuration will be saved and enter a file name.



3. Enter the **Administrator Password** and confirm it in the second field. This password is for access to the SOHO firewall's web interface.
4. (Recommended) Enter a **Configuration Encryption Password** or click **Generate** to create one automatically. The password controls access to the file; make sure to take note of it.
5. Click **Save**.

After the initial configuration is saved, you are ready to install the appliances. If someone else takes care of the appliance installation, send the password(s) securely and separately from the configuration file.

To safely set up the appliance and to import the configuration file, refer to the model-specific *Appliance Installation Guide* booklet delivered with each appliance. After the initialization, you can change the settings through the corresponding element in the Management Client and push the changes to the appliance remotely through the SOHO Firewall element's right-click menu.

Tip – When the elements are created, you can select several SOHO Firewall elements and open common properties for them through the right-click menu. The common properties dialog that opens has similar restrictions on configuration changes as the configuration wizard.



Note – The Web interface is meant only for importing the configuration file. Other configuration options that you may encounter are not meant for centrally managed operation. Other changes may cause configuration conflicts and prevent any of the appliance's features from working correctly and consistently.

CHAPTER 7

UPGRADING

When there is a new version of the SOHO firewall firmware, you should upgrade as soon as possible.

The following sections are included:

- ▶ [Getting Started with Upgrading](#) (page 56)
- ▶ [Upgrading the SOHO Firewall Engines](#) (page 56)

Getting Started with Upgrading

You can upgrade without uninstalling the previous version. Only remote upgrades are supported for SOHO firewall appliances.

You can configure the Management Server to automatically check for new upgrades and download them so that they are ready in the system whenever you want to upgrade. See the Online Help of the Management Client or the Administrator's Guide PDF for more information.

In many cases, you must upgrade the Management Center components before you can upgrade the appliances, because the old Management Center version may not be able to recognize appliances that have a new version and generate a valid configuration for them. Most older appliance firmware versions can be controlled by newer Management Center versions. See the *Release Notes* for version-specific restrictions.

Configuration Overview

To upgrade a SOHO firewall appliance:

1. Read the Release Notes for the new version you are about to install. They can be found at the Stonesoft website at http://www.stonesoft.com/en/support/technical_support_and_documents/. Note the supported Management Center version and upgrade the Management Center first if necessary.
2. If your Management Server is not set up to download upgrades automatically, obtain the files at <https://my.stonesoft.com/download/>, check the file integrity (see [Checking File Integrity](#) (page 56)) and import the upgrade file (see [Manually Importing an Upgrade File](#) (page 57)).
3. Upgrade the appliances. See [Upgrading the SOHO Firewall Engines](#) (page 56).

Upgrading the SOHO Firewall Engines

SOHO firewall appliances are upgraded remotely from the Management Server. On SOHO firewalls, both transfer and activation of the changed configuration must always be done in the same task (activation cannot be postponed). You can alternatively create a scheduled Task for the remote upgrade as instructed in the *Online Help* of the Management Client.

If you have not configured the upgrade files to be downloaded automatically, you must first import the upgrade file in the system.

- If the file is already in the system (stored under **Other Elements**→**Engine Upgrades**→**SOHO Firewall** in the Administration Configuration view), proceed to [Upgrading a SOHO Firewall Appliance](#) (page 57).
- Before manually importing the file, check the installation package integrity using the MD5 or SHA-1 file checksums as explained in [Checking File Integrity](#) (page 56).

Checking File Integrity

You can check the installation file integrity using the MD5 or SHA-1 file checksums. The checksums are at the product-specific download pages at the Stonesoft website at <http://www.stonesoft.com/download/>. For more information on MD5 and SHA-1, see *RFC1321* and *RFC3174*, respectively.

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

▼ To check MD5 or SHA-1 file checksum

1. Obtain the checksum files from the Stonesoft website at <http://www.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.

Illustration 7.1 Checking the File Checksums

```
2a4a4359a0190635390db0d57fc22ee4  
soho_engine_7.5.4.3._fw100.rey
```

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



Caution – Do not use files that have invalid checksums.

If the checksum is correct, proceed to [Manually Importing an Upgrade File](#) (page 57).

Manually Importing an Upgrade File

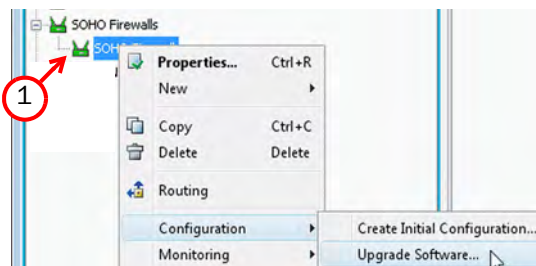
▼ To manually import the upgrade file

1. Select **File**→**Import**→**Import Engine Upgrades**. The Import Engine Upgrade dialog opens.
2. Select the engine upgrade file (`soho_engine_version_platform.rey`) and click **Import**. The upgrade is imported to your Management Server.
 - See the status bar at the bottom of the window for messages regarding the status of the import, as this will take some time.
 - The file is stored under **Other Elements**→**Engine Upgrades**→**SOHO Firewall** in the Administration Configuration view. You can manage the upgrade files here. For example, you can delete old upgrade files that you no longer need.

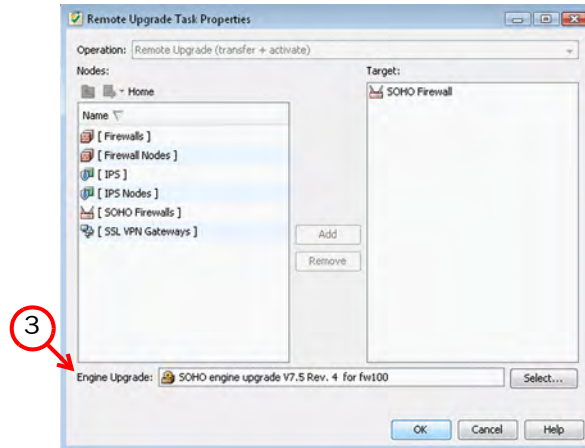
Upgrading a SOHO Firewall Appliance

▼ To upgrade a SOHO firewall appliance

1. Right-click the SOHO Firewall element and select **Configuration**→**Upgrade Software** from the menu.



2. (Optional) Add additional SOHO firewalls to the operation.



3. Check the **Engine Version** for the upgrade and change it if necessary.

4. Click **OK**.

A new tab opens to show the progress of the upgrade. The time it takes to upgrade varies depending on the equipment, load, and the network environment. Once the appliance is successfully upgraded, it is automatically rebooted.

APPENDIX A

DEFAULT COMMUNICATION PORTS

This chapter lists the default ports used in connections between StoneGate components and the default ports StoneGate uses with external components.

The following sections are included:

- ▶ [Management Center Ports](#) (page 60)
- ▶ [Firewall/VPN Engine Ports](#) (page 62)

Management Center Ports

The illustrations below present an overview to the most important default ports used in communications between the Management Center (SMC) components and from the SMC to external services. See [Table A.1](#) for a complete list of default ports.

Illustration A.1 Destination Ports for Basic Communications Within SMC
Management Client

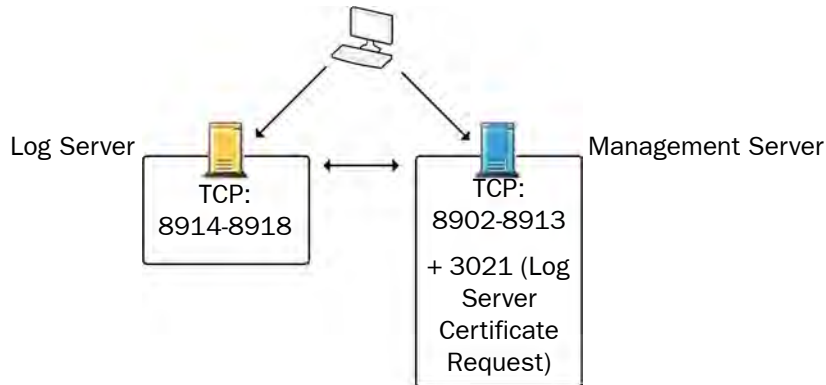
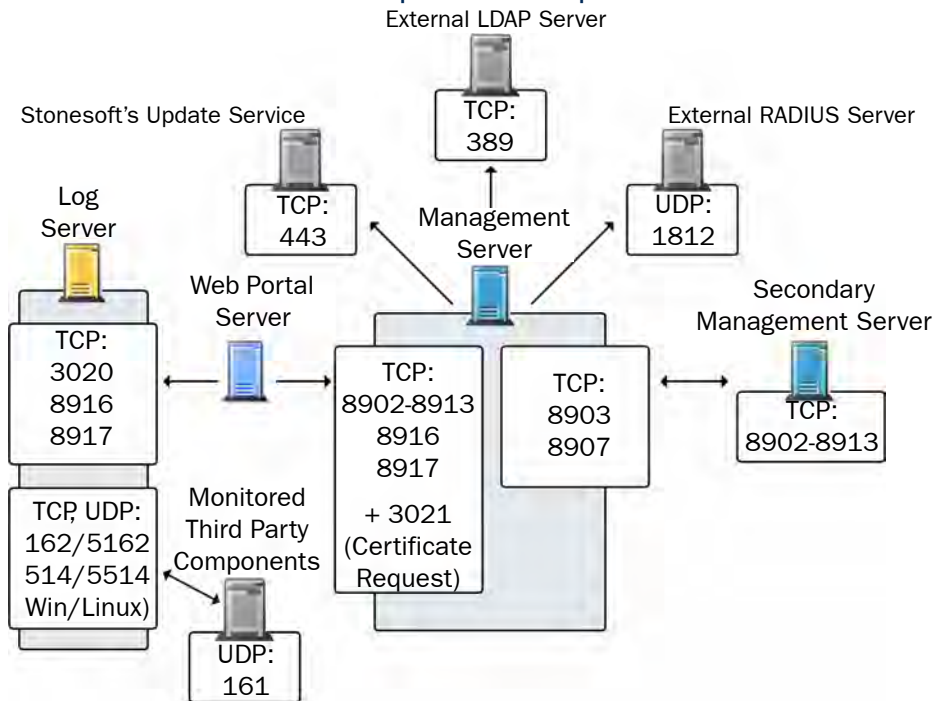


Illustration A.2 Default Destination Ports for Optional SMC Components and Features



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 A.1 Management Center Default Ports

Listening Host	Port/ Protocol	Contacting Hosts	Service Description	Service Element Name
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	3020/TCP	Log Server, Web Portal Server	Alert sending.	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)
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
Monitored Third Party Components	161/UDP	Log Server	SNMP status probing to external IP addresses.	SNMP (UDP)
Primary Management Server	8903, 8907/TCP	Secondary Management Servers	Database replication (pull) to the secondary Management Server.	SG Control

Table A.1 Management Center Default Ports (Continued)

Listening Host	Port/ Protocol	Contacting Hosts	Service Description	Service Element Name
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)
Secondary Management Servers	8902-8913/TCP	Primary Management Server	Database replication (push) to the secondary Management Server.	SG Control
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 export to syslog servers. The default ports can be modified in the LogServerConfiguration.txt file.	Syslog (UDP) [Partial match]

Firewall/VPN Engine Ports

The illustrations below present an overview to the most important default ports used in communications between firewall/VPN engines and the SMC and between clustered firewall engines. See [Table A.2](#) for a complete list of default ports for the fully-featured firewall/VPN engines and [Table A.3](#) for a list of default ports for SOHO Firewalls.

Illustration A.3 Destination Ports for Basic Firewall/VPN Engine Communications

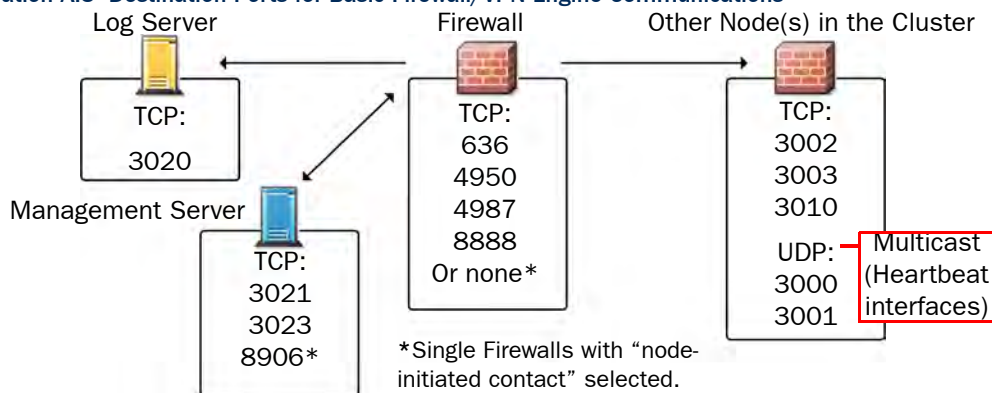


Illustration A.4 Destination Ports for Basic SOHO Firewall Engine Communications

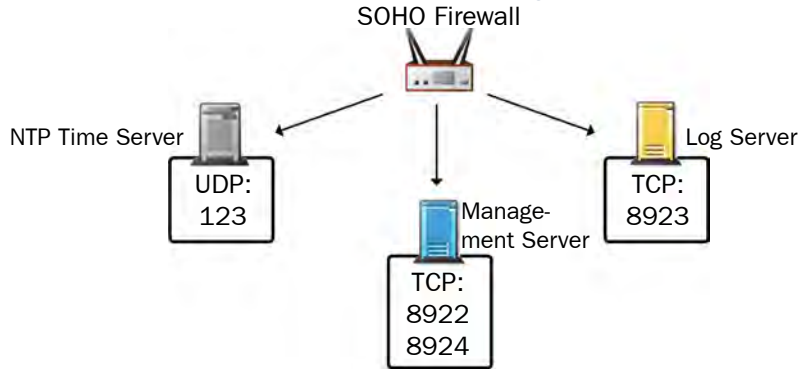
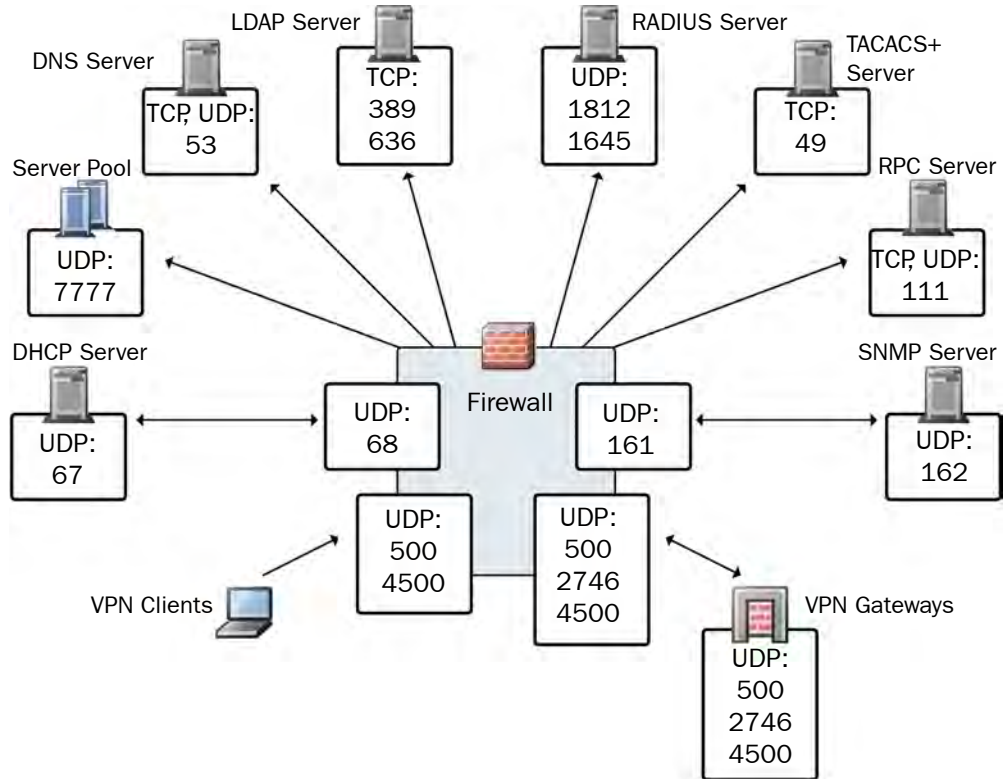


Illustration A.5 Default Destination Ports for Firewall/VPN Engine Service Communications



The table below lists all default ports StoneGate Firewall/VPN 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.

Table A.2 Firewall/VPN 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
BrightCloud Server	2316/TCP	Firewall	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	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	161/UDP	SNMP server	SNMP monitoring.	SNMP (UDP)
Firewall	500/UDP	VPN clients, VPN gateways	VPN negotiations, VPN traffic.	ISAKMP (UDP)
Firewall	636/TCP	Management Server	Internal user database replication.	LDAPS (TCP)
Firewall	2543/TCP	Any	User authentication (Telnet) for Access rules.	SG User Authentication
Firewall	2746/UDP	StoneGate VPN gateways	UDP encapsulated VPN traffic.	SG UDP Encapsulation
Firewall	3000-3001/ UDP 3002-3003, 3010/TCP	FW/VPN engine	Heartbeat and state synchronization between clustered firewalls.	SG State Sync (Multicast), SG State Sync (Unicast), SG Data Sync
Firewall	4500/UDP	VPN client, VPN gateways	VPN traffic using NAT-traversal.	NAT-T
Firewall	4950/TCP	Management Server	Remote upgrade.	SG Remote Upgrade
Firewall	4987/TCP	Management Server	Management Server commands and policy upload.	SG Commands

Table A.2 Firewall/VPN Default Ports (Continued)

Listening Host	Port/Protocol	Contacting Hosts	Service Description	Service Element Name
Firewall	8888/TCP	Management Server	Connectivity monitoring; monitoring of blacklists, connections, and status for old engine versions.	SG Monitoring
Firewall	15000/TCP	Management Server, analyzer	Blacklist entries.	SG Blacklisting
LDAP server	389/TCP	Firewall	External LDAP queries, including StartTLS connections.	LDAP (TCP)
Log Server	3020/TCP	Firewall	Log and alert messages; monitoring of blacklists, connections, status, and statistics.	SG Log
Management Server	3021/TCP	Firewall	System communications certificate request/renewal (initial contact).	SG Initial Contact
Management Server	3023/TCP	Firewall	Monitoring (status) connection.	SG Reverse Monitoring
Management Server	8906/TCP	Firewall	Management connection for Single Firewalls with “node-initiated contact” selected.	SG Dynamic Control
RADIUS server	1812, 1645/UDP	Firewall	RADIUS authentication requests.	RADIUS (Authentication), RADIUS (Old)
RPC server	111/UDP, 111/TCP	Firewall	RPC number resolve.	SUNRPC (UDP), Sun RPC (TCP)
Server Pool Monitoring Agents	7777/UDP	Firewall	Polls to the servers’ Server Pool Monitoring Agents for availability and load information.	SG Server Pool Monitoring
SNMP server	162/UDP	Firewall	SNMP traps from the engine.	SNMP Trap (UDP)
TACACS+ server	49/TCP	Firewall	TACACS+ authentication requests.	TACACS (TCP)
VPN gateways	500/UDP, 2746/UDP (StoneGate gateways only), or 4500 UDP	Firewall	VPN traffic. Ports 2746 and 4500 may be used depending on encapsulation options.	ISAKMP (UDP)

Table A.3 SOHO Firewall Default Ports

Listening Host	Port/Protocol	Contacting Hosts	Service Description	Service Element Name
SOHO Firewall engine	500/UDP	VPN gateway	Internet Key Exchange (IKE) for IPsec.	ISAKMP (UDP)
Management Server	8922/TCP	SOHO Firewall	Configuration and status communication to the Management Server.	SG SOHO Control Server
Management Server	8924/TCP	SOHO Firewall	System communications certificate request/renewal (initial contact).	SG SOHO Initial Contact
NTP server	123/UDP	SOHO Firewall	Time synchronization.	NTP (UDP)
RADIUS server	1812/UDP	SOHO Firewall	RADIUS authentication requests.	RADIUS (Authentication)

INDEX

A

- access rules, 48, 52
- administrator password, 52
- administrator permissions, 39
- ADSL, 27
- AES, 12, 35
- authentication server, 36

B

- background, 10
- browser-based interface password, 52

C

- comments, 8
- communication ports, 52
- contact addresses, 13–19
 - central firewall, 18–19
 - exceptions, 17, 19
 - management and log server, 17
- contact information, 8
- corporate interfaces, 26, 31
 - DNS, 32
- customer support, 8

D

- date and time settings, 11
- defining elements
 - internal security gateways, 43
 - ISPs, 27
 - RADIUS servers, 36
 - routers, 28
 - sites, 43
 - SOHO firewalls, 22
 - SOHO gateway groups, 45
 - VPNs, 46
- DHCP, 31
- DNS (domain name service), 30, 32
- DNS servers
 - for all interfaces, 30
 - for corporate interfaces, 32
- documentation available, 7
- dynamic IP addresses, 31

E

- EAP, 11, 36
- exceptions to contact addresses, 17, 19
- external authentication server, 36
- external interfaces, 26

F

- file integrity check, 56
- firewall (central) contact address, 18–19
- firmware upgrade, 55–58

G

- general wireless settings, 38
- guest interfaces, 26, 31

H

- hardware requirements, 8

I

- importing initial configuration to appliance, 53
- importing upgrade manually, 57
- include and update addresses based on routing, 43
- initial configuration file, 52
- installation overview, 10
- interfaces
 - ADSL, 27
 - corporate, 31
 - DNS, 30
 - ethernet external, 29
 - guest, 31
 - PPPoE, 27
 - type selection, 26
- internal security gateways, 43
- introduction to SOHO firewalls, 10
- issues view, 47

K

- keep-alive VPN tunnel, 31

L

- licenses, 11
- locations, 13–19
 - creating, 15–17
 - setting for SOHO firewalls, 25
- log server contact address, 17
- logging VPN connections, 49

M

- management server contact address, 17
- MD5, 56
- MTU, 29

N

- NAT (network address translation), 11
 - contact addresses, 13–19
- network interfaces, 26

NTP (network time protocol), 11, 25

O

overview to the installation, 10

P

pairing SOHO firewalls with SMC, 52

password, 52

PEAP, 11, 36

permissions, 39

ports, 52

PPPoE, 27

preparations, 9

pre-shared keys, 47

primary time server, 25

proof of purchase, 11

Q

queries, 8

R

RADIUS, 11, 35, 36

release notes, 56

remote authentication, 11

remote upgrade, 55–58

requirements for hardware, 8

S

saving an initial configuration file, 52

security mode, 34

SHA-1, 56

shared secret, 37

sites, 43

software upgrade, 55–58

SOHO gateway groups, 31, 45

SOHO Suite, 42

SSID, 34

support services, 8

system communications, 52

system overview, 10

system requirements, 8

T

technical support, 8

TKIP, 12, 35

types of network interfaces, 26

typographical conventions, 6

U

upgrading, 55–58

V

validity, 47

VPNs

access rules, 48

central gateway, 43

defining, 46

example configuration, 42

logging, 49

pre-shared keys, 47

sites, 43

SOHO gateway groups, 45

tunnel keep-alive, 31

W

web interface password, 52

WEP, 12, 34

wireless

authentication, 11

general settings, 38

security modes, 12

security settings, 34

WPA, 12, 35

WPA enterprise, 11, 36

StoneGate 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

Secure Information Flow

Stonesoft Inc.

1050 Crown Pointe Parkway
Suite 900
Atlanta, GA 30338
USA

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