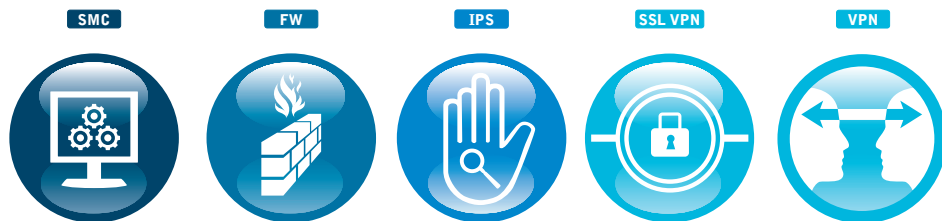


STONESOFT



Installation Guide

StoneGate SOHO Firewalls

Updated for StoneGate Management Center 4.3.3

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

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, 1313290, 1326393, 1379046, 1330095, 131711, 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 and 7,406,534; 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 © 2008 Stonesoft Corporation. All rights reserved. All specifications are subject to change.

Table of Contents

INTRODUCTION

CHAPTER 1 Using StoneGate Documentation 7

- How to Use This Guide 8
 - Typographical Conventions 8
- Documentation Available 9
 - Product Documentation 9
 - Support Documentation 10
 - System Requirements 10
- Contact Information 10
 - Licensing Issues 10
 - Technical Support 10
 - Your Comments 10
 - Other Queries 10

CONFIGURATION AND INSTALLATION

CHAPTER 2 Preparing for Installation 13

- Introduction to StoneGate SOHO Firewalls 14
- Overview to the Installation Procedure 14
- Important to Know Before Installation 15
 - System Communications and NAT 15
 - Internal Clients and NAT 15
 - Licensing 15
 - Pre-Installed Firmware 15
 - RADIUS Server for Wireless User Authentication 15
- Selecting a Wireless Access Mode 16

CHAPTER 3 Configuring NAT Addresses 17

- Configuration Overview 18
- Defining Locations 19
- Adding SMC Server Contact Addresses 20
- Adding the Central Firewall Contact Address 22

CHAPTER 4 Creating SOHO Firewall Elements 25

- Configuration Overview 26
- Creating New SOHO Firewall Elements 26
- Defining Basic Properties 28
- Selecting Interface Types 29
- Configuring External Interfaces 30
 - Configuring an External Interface for ADSL or PPPoE 30
 - Configuring an External Interface for Standard Ethernet 33
- Configuring Corporate and Guest Interfaces 34
 - Defining Security Settings for Wireless Access 36
 - Defining a RADIUS Server for WPA Enterprise 37
 - Defining General Wireless Settings 38
- Finishing the SOHO Firewall Configuration 39

CHAPTER 5 Configuring a VPN 41

- Overview 42
- Creating an Internal Gateway Element 43
- Creating a SOHO Gateway Group 44
- Creating a VPN Element 45
- Creating a VPN Access Rules for the Central Firewall 47

CHAPTER 6 Initializing SOHO Firewall Appliances 49

Allowing SOHO Communications Through a Central Firewall 50

Saving the Initial Configuration 50

MAINTENANCE

CHAPTER 7 Upgrading 55

Getting Started with Upgrading 56

Configuration Overview 56

Upgrading the SOHO Firewall Engines 57

Checking File Integrity 57

Manually Importing an Upgrade File 58

Upgrading a SOHO Firewall Appliance 58

Legal Information 61

Index 77

Introduction

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](#), on page 8
- ▶ [Documentation Available](#), on page 9
- ▶ [Contact Information](#), on page 10

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: *Product 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 guides. PDF versions of these 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 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	Detailed instructions for configuration and use. 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 Monitoring Client. 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 Monitoring Client.
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/Certified_Servers/.

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.

Configuration and Installation

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](#), on page 14
- ▶ [Overview to the Installation Procedure](#), on page 14
- ▶ [Important to Know Before Installation](#), on page 15
- ▶ [Selecting a Wireless Access Mode](#), on page 16

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.
- Backup Internet connection: models that have an ISDN port support the use of ISDN as a backup in case the ADSL line becomes temporarily unavailable.

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 *Reference Guide* for StoneGate Firewall/VPN.

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](#), on page 17.
2. Define the SOHO Firewall element(s) in the Management Client. This is explained in [Creating SOHO Firewall Elements](#), on page 25.
3. Configure a VPN to encrypt traffic between the SOHO firewalls' protected network and other internal networks. This is explained in [Configuring a VPN](#), on page 41.
4. Generate the initial configuration file for the SOHO firewall appliance(s). This is explained in [Saving the Initial Configuration](#), on page 50.
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.

Important to Know Before Installation

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.

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.

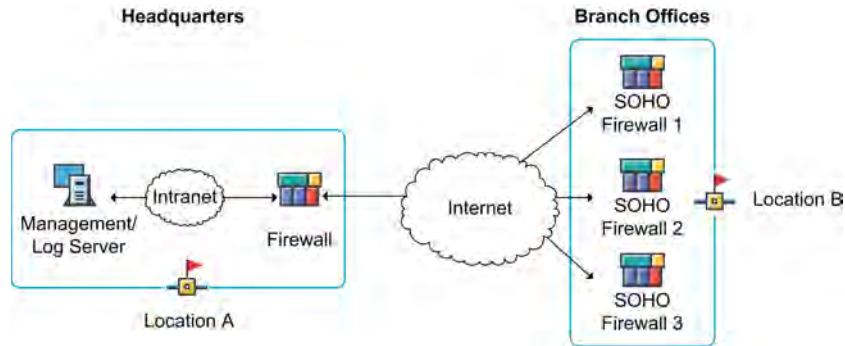
The following sections are included:

- ▶ [Configuration Overview](#), on page 18
- ▶ [Defining Locations](#), on page 19
- ▶ [Adding SMC Server Contact Addresses](#), on page 20
- ▶ [Adding the Central Firewall Contact Address](#), on page 22

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.

Illustration 3.1 A Scenario for Using Locations



In the illustration, 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](#), on page 19.
2. Define contact addresses for the Management Server(s) and Log Server(s). See [Adding SMC Server Contact Addresses](#), on page 20.
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](#), on page 22.
4. Select the correct Location for SOHO firewalls when you create the SOHO Firewall elements. See [Creating SOHO Firewall Elements](#), on page 25.

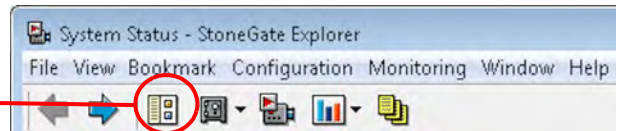
Defining Locations

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.

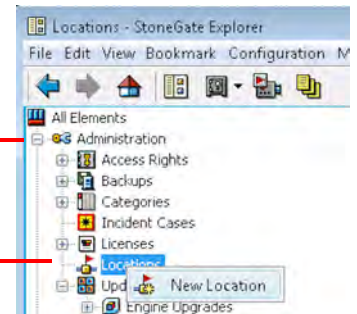
The steps below instruct you to create a new Location element that can be used for all SOHO firewalls. The Management Center components can stay in their current Location (Default or something else you have defined). If there are previously configured Locations in the system, you may be able to reuse 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. The Configuration view opens.

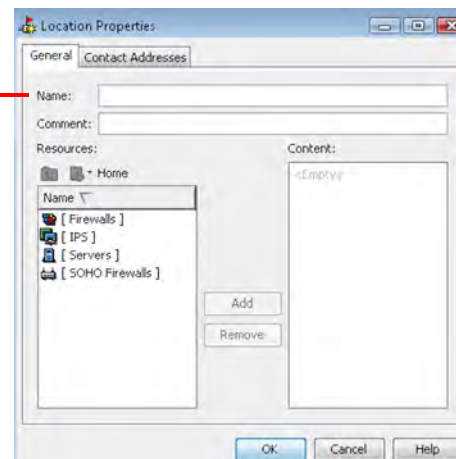


2. Expand **Administration** in the tree view.



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

4. Type in a **Name**.



5. Click **OK**.

Continue by [Adding SMC Server Contact Addresses](#), on page 20.

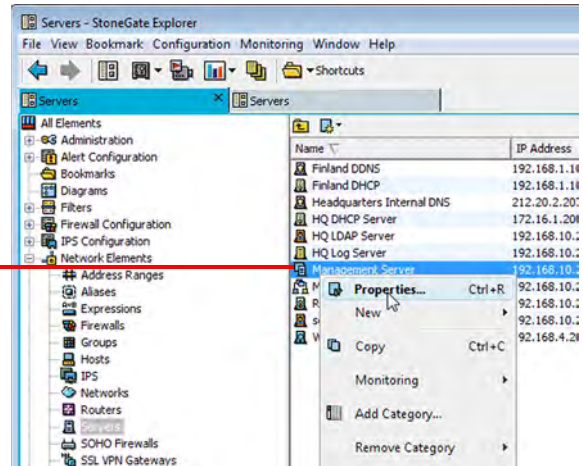
Adding SMC Server Contact Addresses



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.

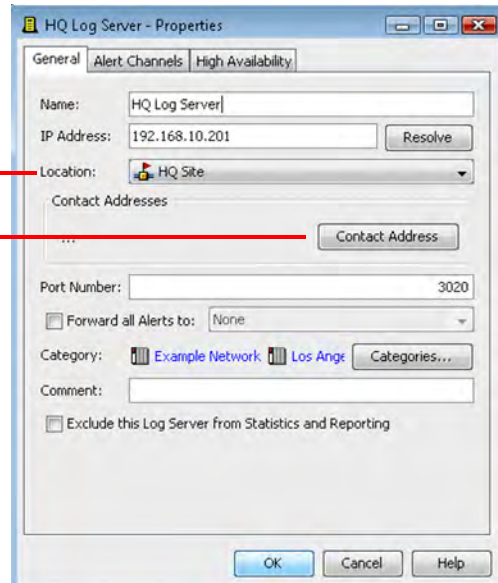
▼ To define the SMC Server contact addresses

1. Right-click 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. Click the **Contact Address** button. The Contact Addresses dialog opens.

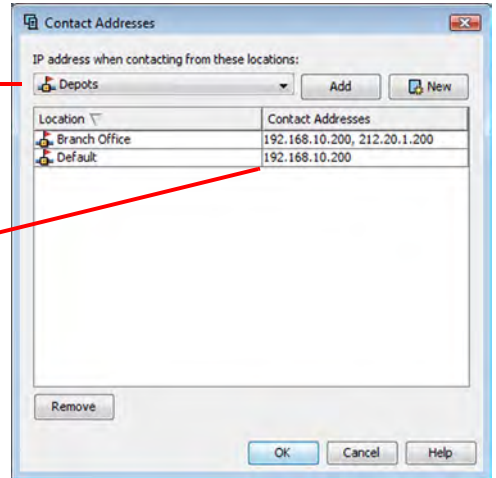


4. Select the SOHO firewalls' **Location** and click **Add** to create an entry in the table below.

5. Click the **Contact Addresses** cell of the SOHO firewalls' Location and enter the server's translated (external) IP address that the SOHO firewalls must use to make contact.

6. Click **OK**.

7. 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.

Proceed as follows:

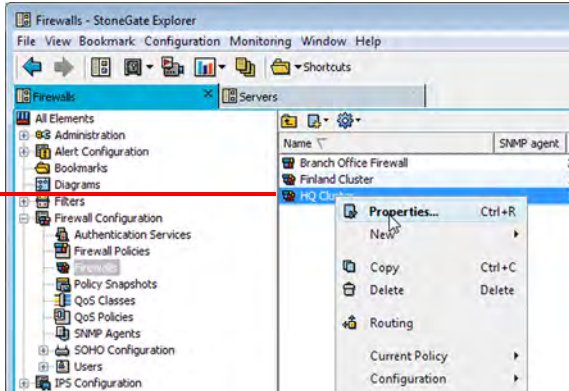
- If the central firewall's VPN endpoint address is translated by external equipment, continue by [Adding the Central Firewall Contact Address](#), on page 22.
- Otherwise, continue by [Creating SOHO Firewall Elements](#), on page 25.

Adding the Central Firewall Contact Address

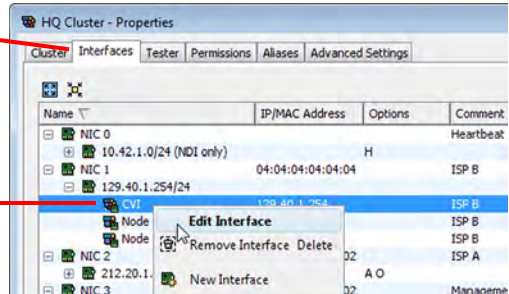
The SOHO firewall is designed to establish a VPN to a central StoneGate firewall to provide access to internal resources. If the central firewall/VPN gateway has a private IP address (translated by external equipment), you must define the public IP address as a contact address to support the VPN. If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

▼ To define the central firewall's contact address

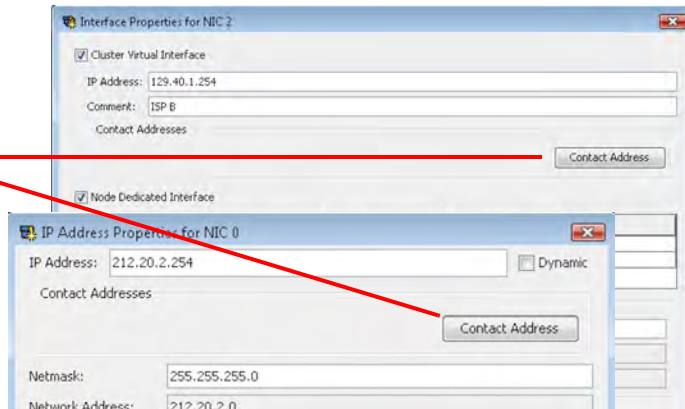
1. Right-click a Firewall or Firewall Cluster element and select **Properties**. The properties dialog for the firewall opens.



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**.

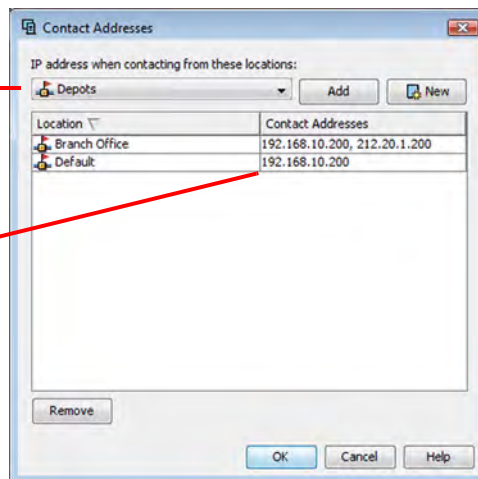


4. In the interface properties dialog, click the **Contact Address** button (for CVI on clusters). The Contact Addresses dialog opens.



5. Select the **Location** of the SOHO firewalls and click **Add** to create an entry in the table below.

6. Click the **Contact Addresses** cell and enter the central firewall's translated (external) IP address that the SOHO firewalls must use to make contact.



7. Click **OK**.



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](#), on page 25.

Creating SOHO Firewall Elements

SOHO firewalls are configured and managed centrally through the StoneGate Management Center. The configuration is then 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](#), on page 26
- ▶ [Creating New SOHO Firewall Elements](#), on page 26
- ▶ [Selecting Interface Types](#), on page 29
- ▶ [Configuring External Interfaces](#), on page 30
- ▶ [Configuring Corporate and Guest Interfaces](#), on page 34
- ▶ [Finishing the SOHO Firewall Configuration](#), on 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](#), on page 26.
2. Select the role of each network port, see [Selecting Interface Types](#), on page 29.
3. Define settings for the External (Internet) interface, see [Configuring External Interfaces](#), on page 30.
4. Define settings for the Corporate (internal network) and Guest (visitor network) interfaces, see [Configuring Corporate and Guest Interfaces](#), on page 34.
5. If you created multiple elements using the wizard, fill in details that must be entered individually for each generated SOHO firewall, see [Finishing the SOHO Firewall Configuration](#), on page 39.

Start by [Creating New SOHO Firewall Elements](#).

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.

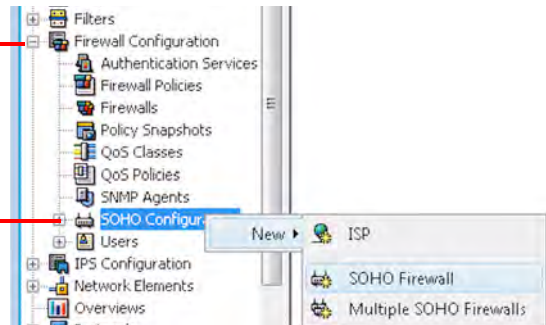
You can either add the elements one by one or use a wizard to generate several elements if you want them to have the same general configuration.

▼ To create SOHO Firewall elements

1. Click the **Configuration** icon.
The Configuration view opens.



2. Expand **Firewall Configuration**.
3. Right-click **SOHO Configuration** 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](#), on page 28. 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).

Create Multiple SOHO Firewalls

Name Prefix: SOHO FW

Global Corporate IP Range: 10.10.10.0 - 10.10.10.255

No. of SOHO Firewalls: 10

DHCP Server

No. of Static IP Addresses (Not Included in DHCP Range):

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

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

Create Multiple SOHO Firewalls

Name Prefix: SOHO FW

Global Corporate IP Range: 10.10.10.0 - 10.10.10.255

No. of SOHO Firewalls: 10

DHCP Server

No. of Static IP Addresses (Not Included in DHCP Range): 2

Generate

Name	Corporate Local IP Address	Corporate Local Network	Corporate DHCP Address R...
SOHO FW - 000	10.10.10.1	10.10.10.0/28	10.10.10.2 - 10.10.10.14
SOHO FW - 001	10.10.10.17	10.10.10.16/28	10.10.10.18 - 10.10.10.30
SOHO FW - 002	10.10.10.33	10.10.10.32/28	10.10.10.34 - 10.10.10.46
SOHO FW - 003	10.10.10.49	10.10.10.48/28	10.10.10.50 - 10.10.10.62
SOHO FW - 004	10.10.10.65	10.10.10.64/28	10.10.10.66 - 10.10.10.78
SOHO FW - 005	10.10.10.81	10.10.10.80/28	10.10.10.82 - 10.10.10.94
SOHO FW - 006	10.10.10.97	10.10.10.96/28	10.10.10.98 - 10.10.10.110
SOHO FW - 007	10.10.10.113	10.10.10.112/28	10.10.10.114 - 10.10.10.126
SOHO FW - 008	10.10.10.129	10.10.10.128/28	10.10.10.130 - 10.10.10.142
SOHO FW - 009	10.10.10.145	10.10.10.144/28	10.10.10.146 - 10.10.10.158

< Previous Next > Cancel Help



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.

Continue by [Defining Basic Properties](#), on page 28.

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**.

2. Select a **Log Server** for storing the produced log data.

3. If required due to NAT, select the **Location** (see [Configuring NAT Addresses](#), on page 17).

4. (Optional) Enter the IP address or hostname of your NTP Server in at least the **Primary Time Server** field.

5. (Optional) Select **DNS** and define DNS server(s) in the fields below. If you leave the option inactive, the local (ISP) DNS servers are used.

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



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).

Continue by [Selecting Interface Types](#), on page 29.

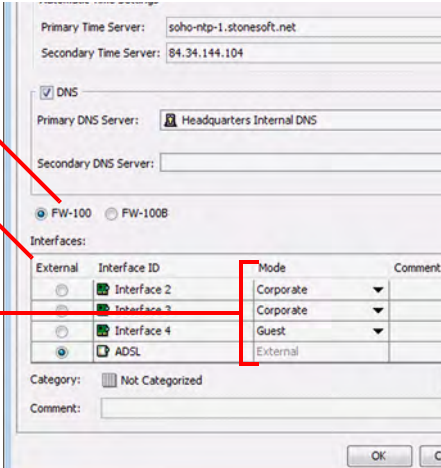
Selecting Interface Types

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.
- *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. Each SOHO firewall must always have at least one Corporate interface. Wireless Corporate access can also be activated as needed.
- *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, but if you want to offer wireless Guest access, there must be at least one physical Guest port.

▼ To select the interface types

1. Select **FW-100** or **FW-100B** according to the model of the appliance. This affects the number of available interfaces.
2. Select the External interface (for Internet access): either **ADSL** or one of the Ethernet interfaces 1-4.
3. Select the interface modes:
 - You must have at least one **Corporate** interface.
 - **Guest** interfaces are optional.
 - Select **Disabled** for the interfaces that you do not want to use.
 - (*FW-100B only, if ADSL is active*) Select **Backup** as the mode for **ISDN** to activate the ISDN line if the ADSL line goes down.



The screenshot shows a configuration window with the following sections:

- Time Servers: Primary Time Server: soho-ntp-1.stonesoft.net, Secondary Time Server: 84.34.144.104
- DNS: DNS, Primary DNS Server: Headquarters Internal DNS, Secondary DNS Server: (empty)
- FW-100 (selected) / FW-100B
- Interfaces table:

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

Category: Not Categorized
Comment: (empty)

Buttons: OK, Cancel



Note – A local browser-based administration tool is available through interface 1. For this reason, we recommend you designate interface 1 as a Corporate interface.

Continue by [Configuring External Interfaces](#), on page 30.

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](#), on page 30.
- If the External interface is a regular Ethernet interface (connected to an external router), proceed to [Configuring an External Interface for Standard Ethernet](#), on page 33.

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

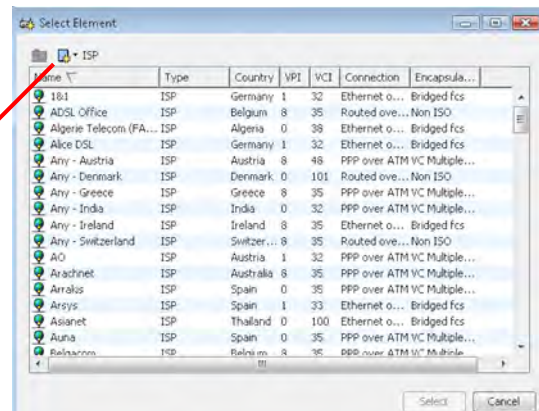
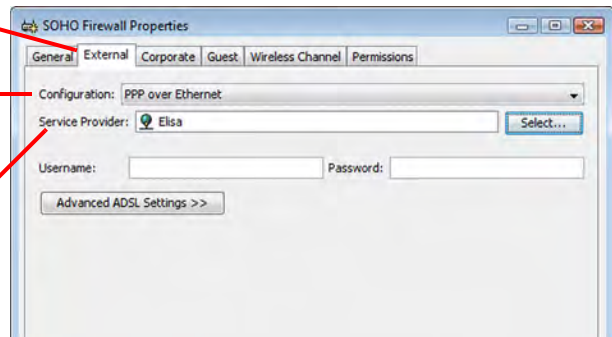
1. Switch to the **External** tab.

2. (Ethernet ports only) Select **PPP over Ethernet** as the **Configuration**.

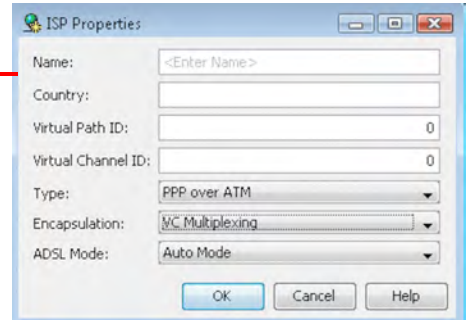
3. Click **Select** for **Service Provider**. The Select Element dialog opens.

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 button (see the next illustration).



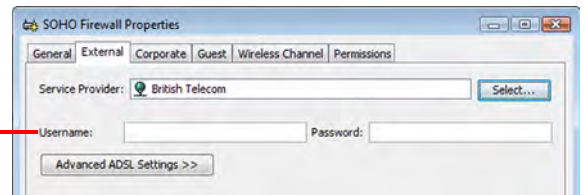
- The **Name** and **Country** are only for your reference.
- Fill in the other settings according to information supplied by your service provider.



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.

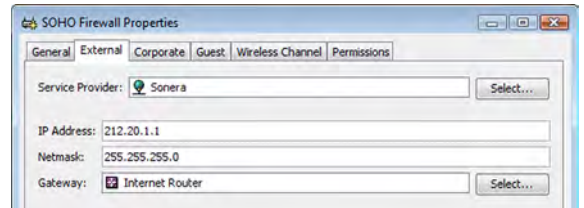
▼ **To select additional settings (PPP over ATM or Ethernet over ATM)**

(Not available in wizard) Enter the ADSL **Username** and **Password**.

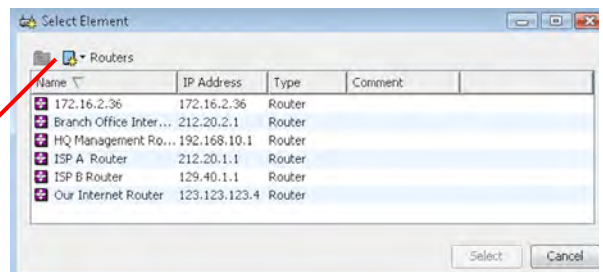


▼ **To select additional settings (Routed over ATM)**

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.



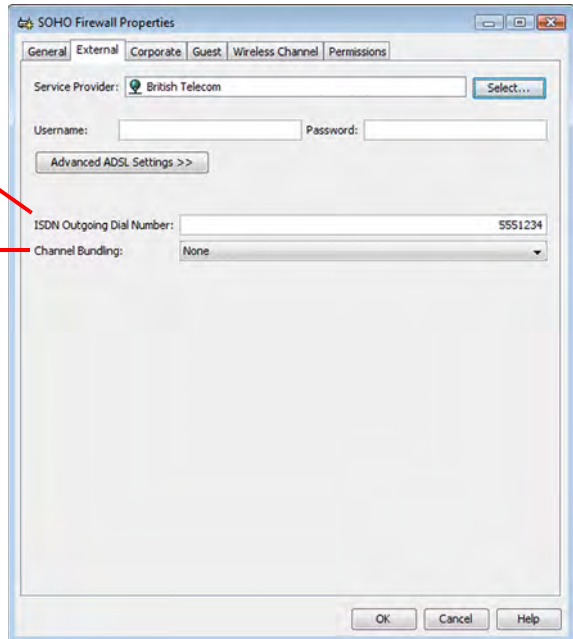
(FW-100B only) If you activated the ISDN backup line on the General tab, configure the related settings as explained below.

▼ **To select ISDN settings (FW-100B)**

1. Enter the number to dial in **ISDN Outgoing Dial Number**.

2. Select **Channel Bundling** (bonding) options:

- **None**: only one channel is opened (max. 64k throughput)
- **Static**: both channels are opened (max. 128k throughput)
- **Dynamic**: the second channel is opened and closed based on need. This setting may cause unnecessary costs if your ISDN provider charges a fixed fee for each channel opening.



Continue by [Configuring Corporate and Guest Interfaces](#), on page 34.

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**.

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.

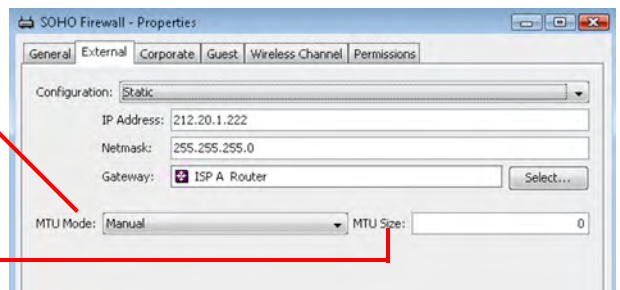
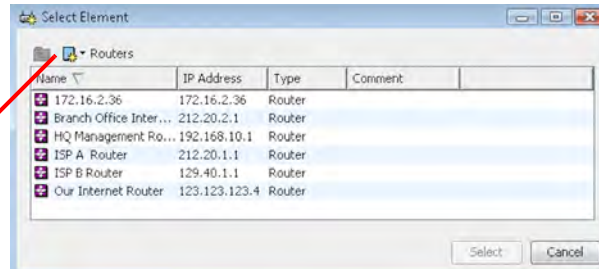
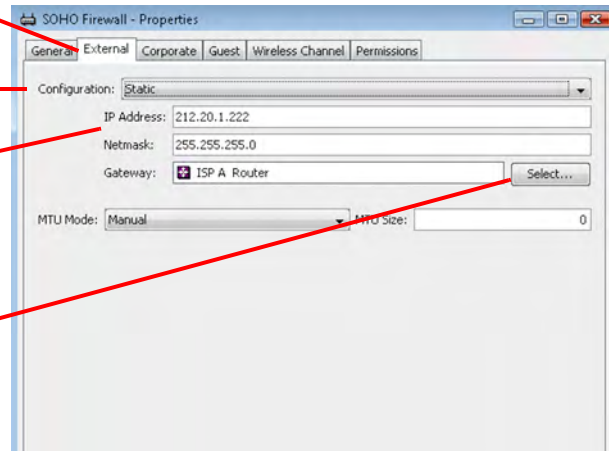
5. (Static only, not available in wizard) Select a Router element from the list and click **Select**. You can add a new Router to the list through the New icon. Only a name and IP address are needed for the new element.

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.

Continue by [Configuring Corporate and Guest Interfaces](#).



Configuring Corporate and Guest Interfaces

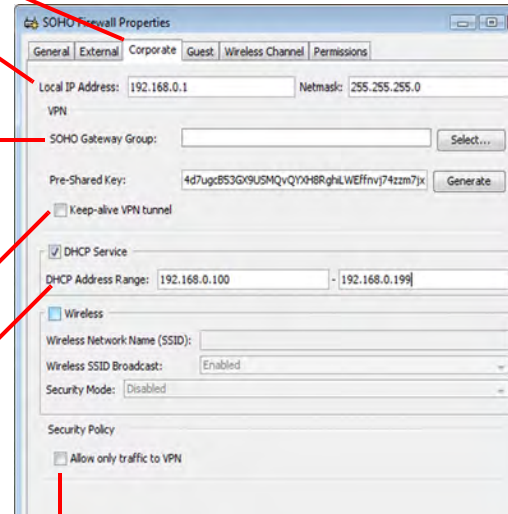
Each SOHO firewall has just one IP address for each interface type (default gateway for the clients). Corporate and Guest addresses are used on all relevant ports depending on interface type selection, as well as with the wireless Corporate/Guest connection. If you are creating multiple elements using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

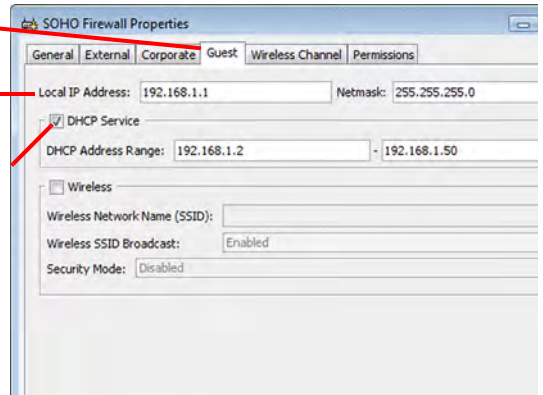
▼ To define the Corporate interface settings

1. Switch to the **Corporate** tab.
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.
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 and they are explained together in the next section.



▼ 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.

Proceed to one of the following:

- If you want to define wireless access, continue by [Defining Security Settings for Wireless Access](#), on page 36.
- Otherwise, the interface definition of your SOHO Firewall is now ready. Click **OK** to close the dialog and continue by [Finishing the SOHO Firewall Configuration](#), on 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.

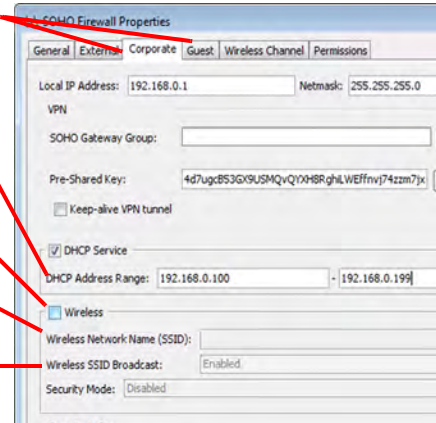
2. Select **Wireless**. The options for wireless connections are enabled.

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](#), on page 16.

TABLE 4.1 Settings per Security Mode

Mode(s)	Setting(s)	Description
WEP 40 WEP 104	Default Key	Selects the key that clients must provide to gain access.
	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.
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.

After selecting the correct security settings, proceed to one of the following:

- If you selected WPA Enterprise, continue by [Defining a RADIUS Server for WPA Enterprise](#), on page 37.
- Otherwise, continue by [Defining General Wireless Settings](#), on 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

The screenshot shows the 'SOHO Firewall - Properties' dialog box with the 'Wireless Channel' tab selected. The 'Wireless' checkbox is checked. The 'RADIUS Server' field is empty and has a 'Select...' button next to it. A red line points to this field.

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

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.

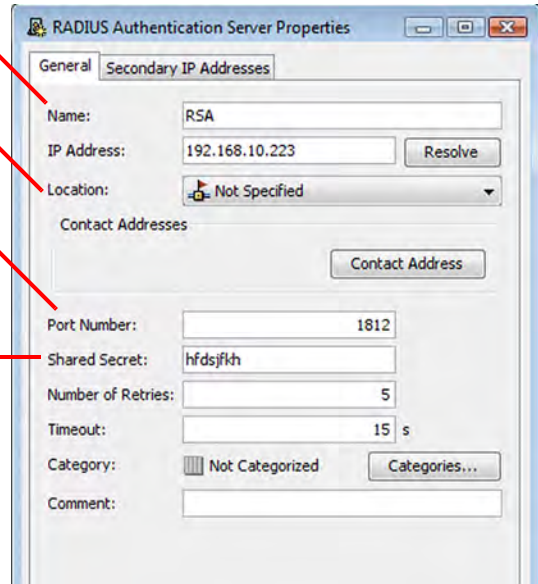
Name	IP Address	Type	Comment
RSA	192.168.10.223	RADIUS Au...	

▼ To create a RADIUS server element

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

The screenshot shows the 'Select Element' dialog box with a table that is currently empty. A red line points to the 'New' icon (a small square with a plus sign) in the top-left corner of the dialog.

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 **Contact Address** for the SOHO firewalls' Location.
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.
6. Click **OK** to return to the previous dialog.
7. Select the new element and click **Select**.



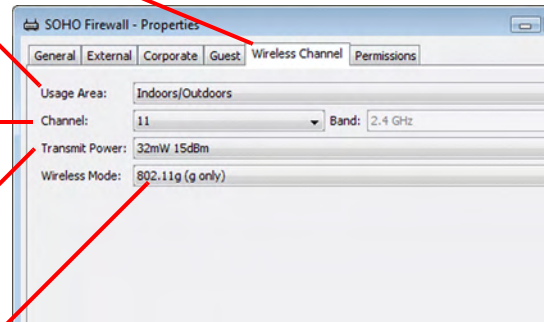
Continue by [Defining General Wireless Settings](#), on page 38.

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.

The interface configuration is now ready. Click **OK** and continue by [Finishing the SOHO Firewall Configuration](#), on page 39.

Finishing the SOHO Firewall Configuration

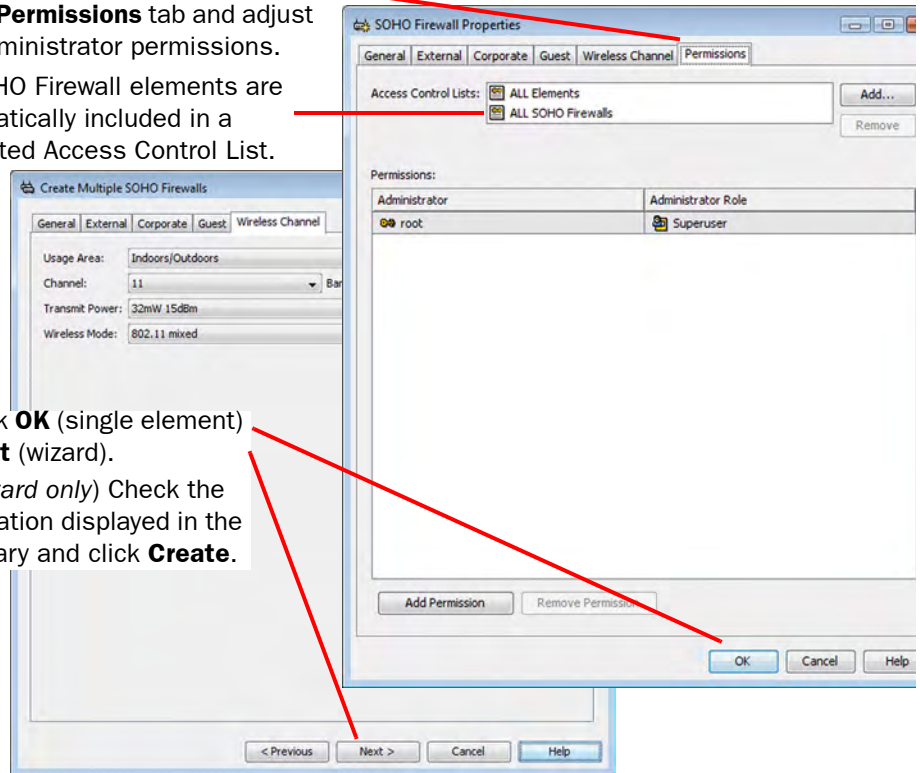
▼ To finish the configuration

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.

To continue the configuration:

- 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](#), on 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](#), on page 49. It is possible to configure a VPN later and then transfer the configuration to the SOHO firewalls remotely.

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 *Reference Guide* for StoneGate Firewall/VPN.

The following sections are included:

- ▶ [Overview](#), on page 42
- ▶ [Creating an Internal Gateway Element](#), on page 43
- ▶ [Creating a SOHO Gateway Group](#), on page 44
- ▶ [Creating a VPN Element](#), on page 45
- ▶ [Creating a VPN Access Rules for the Central Firewall](#), on page 47

Overview

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* 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](#), on 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](#), on page 44.
3. Create the VPN, see [Creating a VPN Element](#), on page 45.
4. Allow VPN access to the protected clients in the policy of the central firewall, see [Creating a VPN Access Rules for the Central Firewall](#), on page 47.

Creating an Internal Gateway Element

▼ To create an internal Gateway element

1. Make sure you are in the Configuration view.

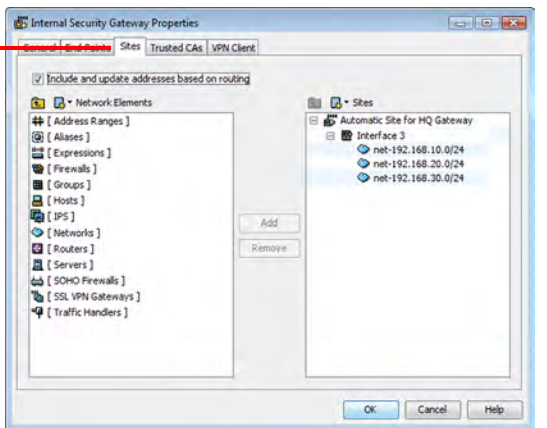
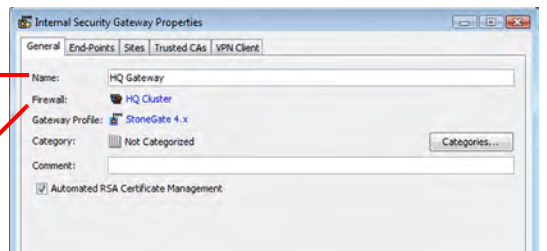
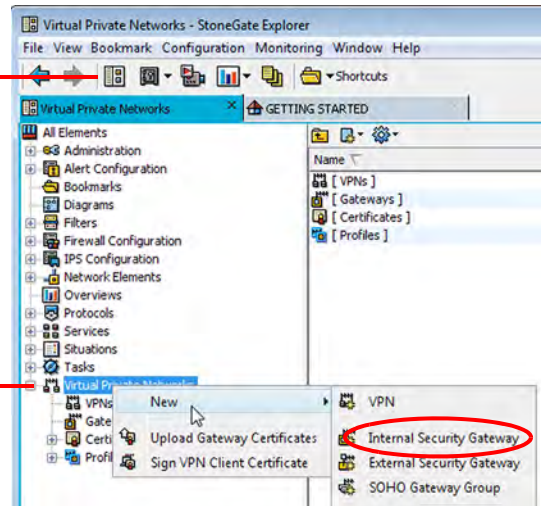
2. Right-click **Virtual Private Networks** and select **New**→**Internal Security Gateway**.

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

4. Select the **Firewall** that the Gateway element represents.

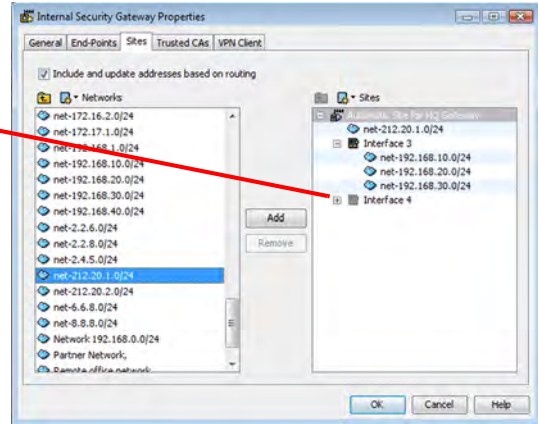
5. Switch to the **Sites** tab.

- Sites define the addresses that are routable through the VPN.
- Leave the **Include and Update Addresses Based on Routing** option selected. See the next steps for adjustments.



6. (Optional) Right-click interfaces that you want to exclude and select **Disable**. Disabled interfaces are greyed-out.

- To include some network from a disabled interface, drag-and-drop the network manually onto the top-level Site element.
- Note that manually dragged-and-dropped definitions are not updated automatically based on routing changes.



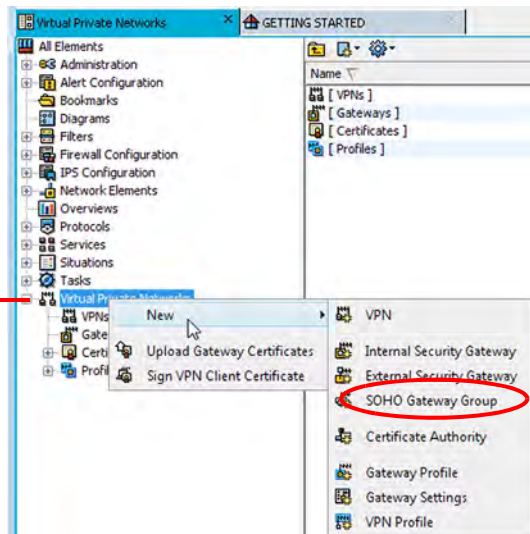
Note – If you plan to use NAT to translate the IP addresses of the internal hosts that make connections through this VPN, drag-and-drop the network(s) for the NAT address space on top of the (top-level) automatic Site element on the right and disable the corresponding interfaces that contain the untranslated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

Click **OK** and continue by [Creating a SOHO Gateway Group](#), on page 44.

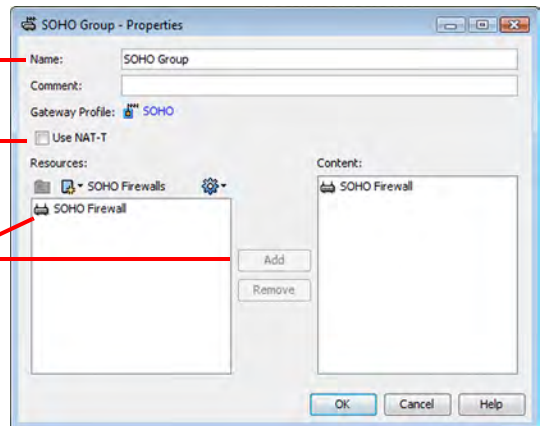
Creating a SOHO Gateway Group

▼ To create a SOHO Gateway Group element

1. Right-click **Virtual Private Networks** 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**.

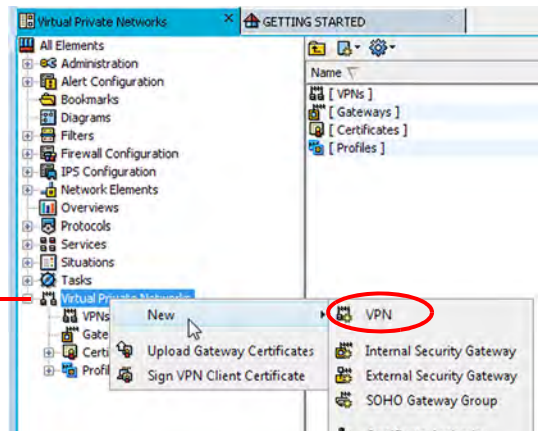


Continue by [Creating a VPN Element](#), on page 45.

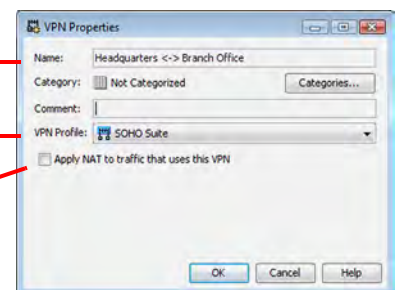
Creating a VPN Element

- ▼ To create a VPN element

1. Right-click **Virtual Private Networks** and select **New**→**VPN**.



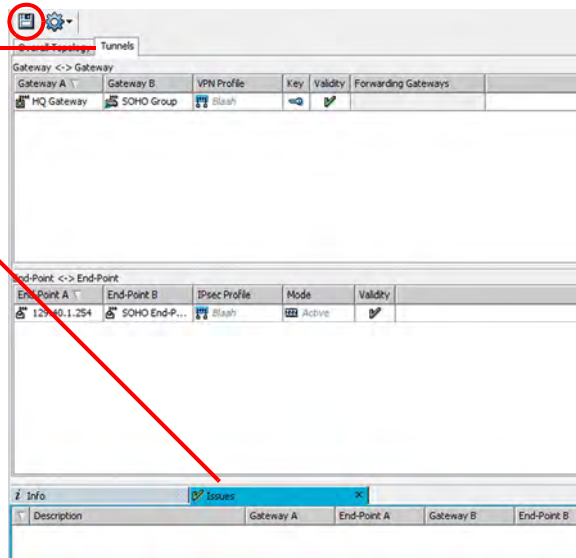
2. Give the new element a unique **Name**.
3. Select **SOHO Suite** from the **VPN Profile** list. The VPN Profile defines IPsec settings.
4. If you want to NAT traffic that goes through the VPN, select the **Apply NAT Rules to Traffic That Uses This VPN** option.
5. Click **OK**. The VPN opens for editing.



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 (circled).



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 (Corporate tab).

Creating a VPN Access Rules for the Central Firewall

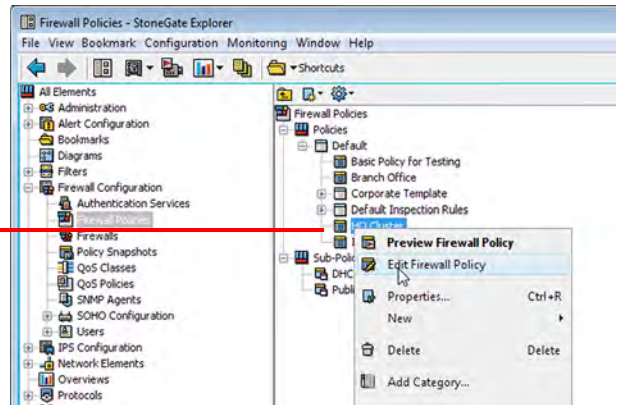
On the central firewall, the Access rules define which connections are forwarded to the VPN and which connections are allowed out of the VPN. The two rules in this example always allow new connections in both directions when the VPN tunnel is already open. However, if a SOHO firewall has a dynamic external 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 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.

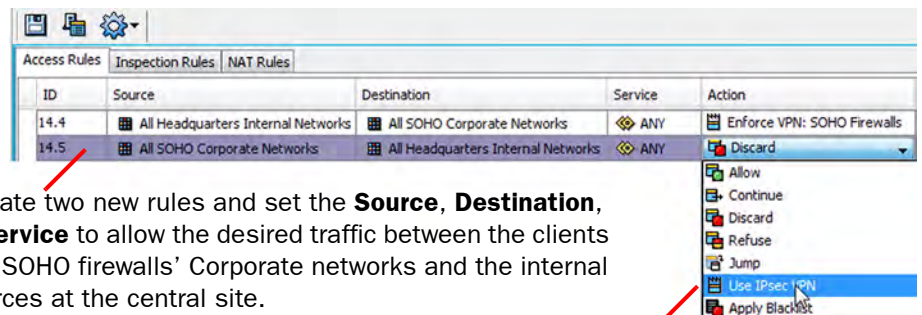
▼ To create VPN Access rules

1. Open the central firewall's policy for editing.

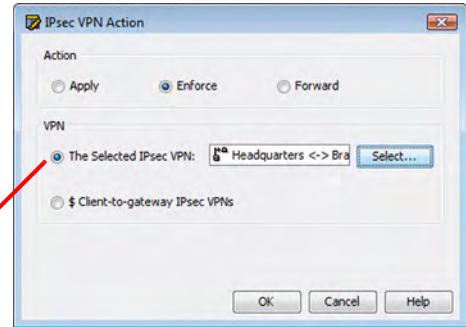


2. Create two new rules and set the **Source**, **Destination**, and **Service** to allow the desired traffic between the clients in the SOHO firewalls' Corporate networks and the internal resources at the central site.

3. Click the **Action** cell and select **Use IPsec VPN**. The IPsec VPN Action dialog opens.



4. Select one of the following actions:
 - **Apply**: if establishing the VPN tunnel fails, connections that would have been sent through the VPN are matched to the next rule in the policy.
 - **Enforce**: if establishing a VPN tunnel fails, all matching connections are discarded.
5. 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.

Continue by [Initializing SOHO Firewall Appliances](#), on page 49.

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](#), on page 50
- ▶ [Saving the Initial Configuration](#), on page 50

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

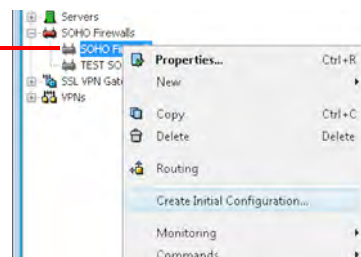
Source	Destination	Port	Service Element Name
SOHO firewall	Management Server	TCP 8924	SG SOHO Initial Contact
SOHO firewall	Management Server	TCP 8922	SG SOHO Control
SOHO firewall	Log Server	TCP 8923	SG SOHO Log

Saving the Initial Configuration

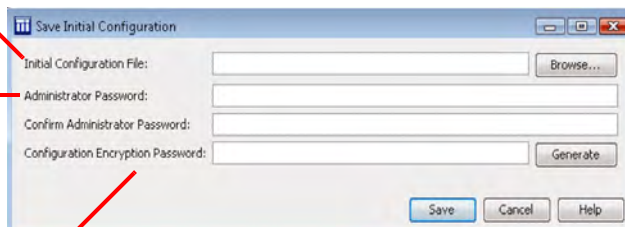
The SOHO firewall engines are initialized by importing an initial configuration file through the SOHO Firewall's web interface.

▼ 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.

Maintenance

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](#), on page 56
- ▶ [Upgrading the SOHO Firewall Engines](#), on page 57

Getting Started with Upgrading

You can upgrade without uninstalling the previous version. Only remote upgrades are supported for SOHO Firewall appliances. Local upgrades are not supported.

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 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.

Proceed to the [Configuration Overview](#) to begin with the configuration.

Configuration Overview

To upgrade a StoneGate SSL VPN 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*, on page 57) and import the upgrade file (see *Manually Importing an Upgrade File*, on page 58).
3. Upgrade the appliances, see *Upgrading the SOHO Firewall Engines*, on page 57.

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.

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 **Administration**→**Updates and Upgrades** in the Configuration view), proceed to [Upgrading a SOHO Firewall Appliance](#), on page 58.
- Before manually importing the file, check the installation package integrity using the MD5 or SHA-1 file checksums as explained in [Checking File Integrity](#), on page 57.

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](#), on page 58.

Manually Importing an Upgrade File

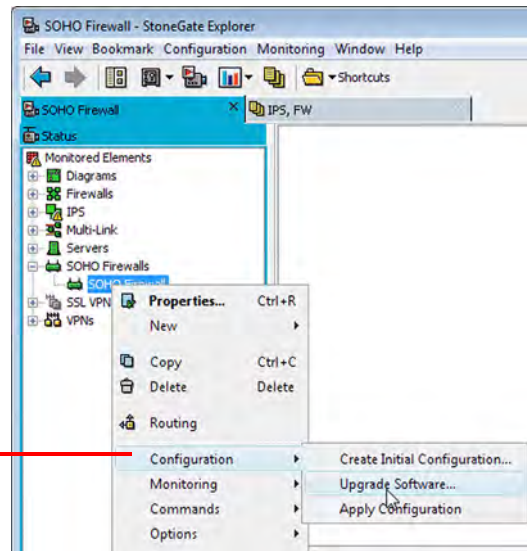
▼ To manually import the upgrade file

1. Select **File**→**Import**→**Import Engine Upgrades**. The StoneGate Engine Upgrades File Browser 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 **Administration**→**Updates and Upgrades** in the 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

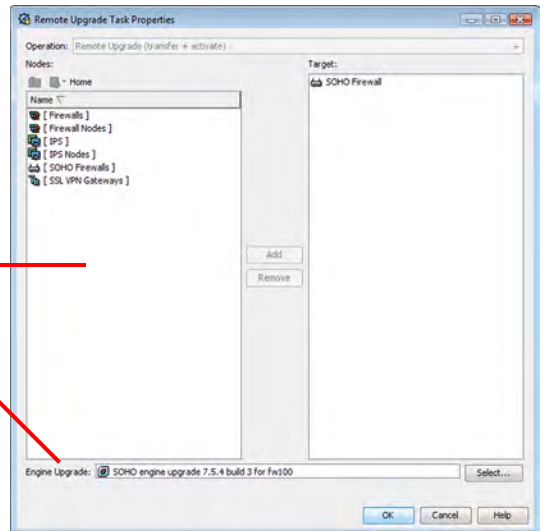
1. Right-click the SOHO Firewall element and select **Configuration**→**Upgrade Software** from the menu that opens.



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.



Legal Information

Licenses

Stonesoft products are sold pursuant to their relevant End-User License Agreements. By installing or otherwise using Stonesoft products in any way, end-users agree to be bound by such agreement(s). See Stonesoft's website, www.stonesoft.com for further details.

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.

Patent Notice

Multi-Link, Multi-Link VPN, and the StoneGate clustering technology—as well as other technologies included in StoneGate—are protected by pending patent applications in the U.S. and other countries.

End-User Licence Agreement

The use of the Stonegate products 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.

Software Licensing Information

The StoneGate software includes several open source or third-party software packages to support certain features. This section provides the appropriate software licensing information for those products.

GNU General Public License

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software—to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

1. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.
You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.
2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:
 - a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
 - b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
 - c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:
 - a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
 - b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
 - c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your

rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.
6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.
7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.
9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.
Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.
10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.
12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>

Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.

This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items-whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program

'Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software—to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages—typically libraries—of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law; that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

- c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.
- d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work

under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

- a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified

Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

- b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.
- c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.
- d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.
- e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

- a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.
- b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version

or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>

Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail. You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990

Ty Coon, President of Vice

That's all there is to it!

OpenSSL Toolkit

This software includes the OpenSSL toolkit.

LICENSE ISSUES

=====

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

Copyright (c) 1998-2000 The OpenSSL Project. All rights reserved.

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

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"

The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

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

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscape's SSL. This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com). Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

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

Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related:-).

If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

OpenLDAP

This software includes the OpenLDAP client developed by The OpenLDAPFoundation. Original version of the OpenLDAP client can be downloaded from <http://www.openldap.org>

This software includes the OpenLDAP server.

The OpenLDAP Public License

Version 2.7, 7 September 2001

Redistribution and use of this software and associated documentation ("Software"), with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain copyright statements and notices,

2. Redistributions in binary form must reproduce applicable copyright statements and notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution, and
3. Redistributions must contain a verbatim copy of this document.

The OpenLDAP Foundation may revise this license from time to time. Each revision is distinguished by a version number. You may use the Software under terms of this license revision or under the terms of any subsequent revision of the license.

THIS SOFTWARE IS PROVIDED BY THE OPENLDAP FOUNDATION AND CONTRIBUTORS "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OPENLDAP FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

OpenLDAP is a trademark of the OpenLDAP Foundation.

Copyright 1999-2001 The OpenLDAP Foundation, Redwood City, California, USA. All Rights Reserved. Permission to copy and distributed verbatim copies of this document is granted.

libradius1

This software includes the `libradius1` package.

Copyright (C) 1995,1996,1997,1998 Lars Fenneberg <lf@elemental.net>

Permission to use, copy, modify, and distribute this software for any purpose and without fee is hereby granted, provided that this copy ight and permission notice appear on all copies and supporting documentation, the name of Lars Fenneberg not be used in advertising or publicity pertaining to distribution of the program without specific prior permission, and notice be given in supporting documentation that copying and distribution is by permission of Lars Fenneberg.

Lars Fenneberg makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

Copyright 1992 Livingston Enterprises, Inc.

Livingston Enterprises, Inc. 6920 Koll Center Parkway Pleasanton, CA 94566

Permission to use, copy, modify, and distribute this software for any purpose and without fee is hereby granted, provided that this copyright and permission notice appear on all copies and supporting documentation, the name of Livingston Enterprises, Inc. not be used in advertising or publicity pertaining to distribution of the program without specific prior permission, and notice be given in supporting documentation that copying and distribution is by permission of Livingston Enterprises, Inc.

Livingston Enterprises, Inc. makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

[C] The Regents of the University of Michigan and Merit Network, Inc. 1992, 1993, 1994, 1995 All Rights Reserved.

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies of the software and derivative works or modified versions thereof, and that both the copyright notice and this permission and disclaimer notice appear in supporting documentation.

THIS SOFTWARE IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE REGENTS OF THE UNIVERSITY OF MICHIGAN AND MERIT NETWORK, INC. DO NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET LICENSEE'S REQUIREMENTS OR THAT OPERATION WILL BE UNINTERRUPTED OR ERROR FREE. The Regents of the University of Michigan and Merit Network, Inc. shall not be liable for any special, indirect, incidental or consequential damages with respect to any claim by Licensee or any third party arising from use of the software.

Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work. RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

TACACS+ Client

This software contains TACACS+ client.

Copyright (c) 1995-1998 by Cisco systems, Inc.

Permission to use, copy, modify, and distribute this software for any purpose and without fee is hereby granted, provided that this copyright and permission notice appear on all copies of the software and supporting documentation, the name of Cisco Systems, Inc. not be used in advertising or publicity pertaining to distribution of the program without specific prior permission, and notice be given in supporting documentation that modification, copying and distribution is by permission of Cisco Systems, Inc.

Cisco Systems, Inc. makes no representations about the suitability of this software for any purpose. THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

MD5C.C - RSA Data Security, Inc., MD5 message-digest algorithm

Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

libwww

This software contains libwww software.

Copyright © 1995-1998 World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University). All Rights Reserved.

This program is distributed under the W3C's Intellectual Property License. This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See W3C License <http://www.w3.org/Consortium/Legal/> for more details.

Copyright © 1995 CERN. "This product includes computer software created and made available by CERN. This acknowledgment shall be mentioned in full in any product which includes the CERN computer software included herein or parts thereof."

W3C® SOFTWARE NOTICE AND LICENSE

<http://www.w3.org/Consortium/Legal/2002/copyright-software-20021231>

This work (and included software, documentation such as READMEs, or other related items) is being provided by the copyright holders under the following license. By obtaining, using and/or copying this work, you (the licensee) agree that you have read, understood, and will comply with the following terms and conditions.

Permission to copy, modify, and distribute this software and its documentation, with or without modification, for any purpose and without fee or royalty is hereby granted, provided that you include the following on ALL copies of the software and documentation or portions thereof, including modifications:

1. The full text of this NOTICE in a location viewable to users of the redistributed or derivative work.
2. Any pre-existing intellectual property disclaimers, notices, or terms and conditions. If none exist, the W3C Software Short Notice should be included (hypertext is preferred, text is permitted) within the body of any redistributed or derivative code.
3. Notice of any changes or modifications to the files, including the date changes were made. (We recommend you provide URIs to the location from which the code is derived.)

THIS SOFTWARE AND DOCUMENTATION IS PROVIDED "AS IS," AND COPYRIGHT HOLDERS MAKE NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF THE SOFTWARE OR DOCUMENTATION WILL NOT INFRINGE ANY THIRD PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS.

COPYRIGHT HOLDERS WILL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF ANY USE OF THE SOFTWARE OR DOCUMENTATION.

The name and trademarks of copyright holders may NOT be used in advertising or publicity pertaining to the software without specific, written prior permission. Title to copyright in this software and any associated documentation will at all times remain with copyright holders.

This formulation of W3C's notice and license became active on December 31 2002. This version removes the copyright ownership notice such that this license can be used with materials other than those owned by the W3C, reflects that ERCIM is now a host of the W3C, includes references to this specific dated version of the license, and removes the ambiguous

grant of "use". Otherwise, this version is the same as the previous version and is written so as to preserve the Free Software Foundation's assessment of GPL compatibility and OSI's certification under the Open Source Definition. Please see our Copyright FAQ for common questions about using materials from our site, including specific terms and conditions for packages like libwww, Amaya, and Jigsaw.

Other questions about this notice can be directed to site-policy@w3.org.

Joseph Reagle <site-policy@w3.org>

Last revised by Reagle \$Date: 2003/01/16 15:01:10 \$

Last revised by Reagle \$Date: 2003/01/16 15:01:10 \$

XML-RPC C Library License

This software contains software covered by the XML-RPC C Library License.

Copyright (C) 2001 by First Peer, Inc. All rights reserved.

Copyright (C) 2001 by Eric Kidd. All rights reserved.

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

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Expat License

This software contains software covered by the Expat License.

Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

ABYSS Web Server License

This software contains software covered by the ABYSS Web Server License

Copyright (C) 2000 by Moez Mahfoudh <mmoez@bigfoot.com>. All rights reserved.

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

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING

NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Python 1.5.2 License

This software contains software covered by the Python 1.5.2 License.

Copyright 1991, 1992, 1993, 1994 by Stichting Mathematisch Centrum, Amsterdam, The Netherlands.

All Rights Reserved

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the names of Stichting Mathematisch Centrum or CWI or Corporation for National Research Initiatives or CNRI not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

While CWI is the initial source for this software, a modified version is made available by the Corporation for National Research Initiatives (CNRI) at the Internet address <ftp://ftp.python.org>.

STICHTING MATHEMATISCH CENTRUM AND CNRI DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL STICHTING MATHEMATISCH CENTRUM OR CNRI BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

The Apache Software License, Version 1.1

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>).

Copyright (C) 1999 The Apache Software Foundation. All rights reserved.

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

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The end-user documentation included with the redistribution, if any, must include the following acknowledgment: "This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>).". Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.
4. The names "log4j" and "Apache Software Foundation" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact apache@apache.org.
5. Products derived from this software may not be called "Apache", nor may "Apache" appear in their name, without prior written permission of the Apache Software Foundation.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the Apache Software Foundation. For more information on the Apache Software Foundation, please see <http://www.apache.org/>.

Bouncy Castle notice and license.

Copyright (c) 2000 The Legion Of The Bouncy Castle (<http://www.bouncycastle.org>)

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Package: discover-data

Debian package author: Branden Robinson

The contents of this package that are not in the debian/ subdirectory are simple compilations of data and are therefore not copyrightable in the United States (c.f. *_Feist Publications, Inc., v. Rural Telephone Service Company, Inc.*, 499 U.S. 340 (1991)).

Feist holds that: Article I, s 8, cl. 8, of the Constitution mandates originality as a prerequisite for copyright protection. The constitutional requirement necessitates independent creation plus a modicum of creativity. Since facts do not owe their origin to an act of authorship, they are not original and, thus, are not copyrightable. Although a compilation of facts may possess the requisite originality because the author typically chooses which facts to include, in what order to place them, and how to arrange the data so that readers may use them effectively, copyright protection extends only to those components of the work that are original to the author, not to the facts themselves. This fact/expression dichotomy severely limits the scope of protection in fact-based works. Therefore, the hardware information lists that comprise the "meat" of this package enjoy no copyright protection and are thus in the public domain. Note, however, that a number of trademarks may be referenced in the hardware lists (names of vendors and products). Their usage does not imply a challenge to any such status, and all trademarks, service marks, etc. are the property of their respective owners.

The remainder of this package is copyrighted and licensed as follows:

Package infrastructure: Copyright 2001,2002 Progeny Linux Systems, Inc. Copyright 2002 Hewlett-Packard Company
Written by Branden Robinson for Progeny Linux Systems, Inc.

Ist2xml conversion script: Copyright 2002 Progeny Linux Systems, Inc. Copyright 2002 Hewlett-Packard Company
Written by Eric Gillespie, John R. Daily, and Josh Bressers for Progeny Linux Systems, Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDER(S) BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Copyright (c) 1999, 2004 Tanuki Software

Permission is hereby granted, free of charge, to any person obtaining a copy of the Java Service Wrapper and associated documentation files (the "Software"), to deal in the Software

without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sub-license, and/or sell copies of the Software, and to permit persons to

whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Portions of the Software have been derived from source code developed by Silver Egg Technology under the following license:

Copyright (c) 2001 Silver Egg Technology

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sub-license, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.



Index

A

access rules, 47, 50
administrator password, 50
administrator permissions, 39
ADSL, 30
AES, 16, 36
authentication server, 37

B

background, 14
browser-based interface password, 50

C

comments, 10
communication ports, 50
configuration encryption, 50
contact addresses, 18
 central firewall, 22
 management and log server, 20
contact information, 10
corporate interfaces, 29, 34
customer support, 10

D

date and time settings, 15

defining elements

 internal security gateways, 43
 ISPs, 30
 RADIUS servers, 37
 routers, 31
 sites, 43
 SOHO firewalls, 26
 SOHO gateway groups, 44
DHCP, 34
DNS (domain name service), 28
documentation available, 9
dynamic IP addresses, 34

E

EAP, 15, 37
encrypting initial configuration, 50
end-user license agreement, 61
external authentication server, 37
external interfaces, 29

F

file integrity check, 57
firewall (central) contact address, 22
firmware upgrade, 55
FW-100/FW-100B, 29

G

general wireless settings, 38
guest interfaces, 29, 34

H

hardware requirements, 10

I

importing initial configuration to appliance, 51
importing upgrade manually, 58
include and update addresses based on routing, 43
initial configuration file, 50
installation overview, 14
interfaces
 ADSL, 30
 corporate, 34
 ethernet external, 33
 guest, 34
 ISDN, 32
 PPPoE, 30
 type selection, 29
internal security gateway, 43
introduction to SOHO firewalls, 14
ISDN, 29, 32
issues view, 46

K

keep-alive VPN tunnel, 34

L

legal information, 61
licenses, 15
locations, 18
 creating, 19
 setting for SOHO firewalls, 28

log server contact address, 20
logging VPN connections, 48

M

management server contact address, 20
MD5, 57
MTU, 33

N

NAT (network address translation), 15, 44
 applying to tunneled traffic, 45
 contact addresses, 18
 traversal (NAT-T), 45
network interfaces, 29
NTP (network time protocol), 15, 28

O

overall topology, 46
overall topology tab, 46
overview to the installation, 14

P

pairing SOHO firewalls with SMC, 50
password, 50
PEAP, 15, 37
permissions, 39
ports, 50
PPPoE, 30
preparations, 13
pre-shared keys, 46
primary time server, 28
proof of purchase, 15

Q

queries, 10

R

- RADIUS, 15, 36, 37
- release notes, 56
- remote authentication, 15
- remote upgrade, 55
- requirements for hardware, 10

S

- saving an initial configuration file, 50
- security mode, 36
- SHA-1, 57
- shared secret, 38
- sites, 43
- software upgrade, 55
- SOHO gateway groups, 34, 44
- SOHO Suite, 42
- SSID, 36
- support services, 10
- system communications, 50
- system overview, 14
- system requirements, 10

T

- technical support, 10
- TKIP, 16, 36
- tunnels, 46
- types of network interfaces, 29
- typographical conventions, 8

U

- upgrading, 55

V

- validity, 46
- VPNs, 46
 - access rules, 47
 - central gateway, 43
 - example configuration, 42
 - logging, 48
 - NAT, 44
 - pre-shared keys, 46
 - sites, 43
 - SOHO gateway groups, 44
 - tunnel keep-alive, 34
 - tunnels tab, 46

W

- web interface password, 50
- WEP, 16, 36
- wireless
 - authentication, 15
 - general settings, 38
 - security modes, 16
 - security settings, 36
- WPA, 16, 36
- WPA enterprise, 15, 37

Available StoneGate Guides:

Product Documentation

- Administrator's Guide
- Installation Guides
- Reference Guides
- VPN Client Administrator's Guide

End User Documentation

- Monitoring Client User's Guide
- VPN Client User's Guide

For PDF versions of the above guides and the StoneGate technical knowledge base, visit www.stonesoft.com/support

Stonesoft Corporation

Itälahdenkatu 22 A
00210 Helsinki
Finland
tel. +358 9 476 711
fax. +358 9 4767 1234

Stonesoft Inc.

1050 Crown Pointe Parkway
Suite 900
Atlanta, GA 30338, USA
tel. +1 770 668 1125
fax. +1 770 668 1131