Avaya Security Gateway Configuration Guide

for VPNos® Release 4.6

670-100-602
Issue 4
May 2005

Notice

Every effort was made to ensure that the information in this document was complete and accurate at the time of release. However, information is subject to change.

Warranty

Avaya Inc. provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language as well as information regarding support for this product, while under warranty, is available through the following website:

http://www.avaya.com/support

Preventing Toll Fraud

"Toll fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there may be a risk of toll fraud associated with your system and that, if toll fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Fraud Intervention

If you suspect that you are being victimized by toll fraud and you need technical assistance or support, in the United States and Canada, call the Technical Service Center's Toll Fraud Intervention Hotline at 1-800-643-2353.

Disclaimer

Avaya is not responsible for any modifications, additions or deletions to the original published version of this documentation unless such modifications, additions or deletions were performed by Avaya. Customer and/or End User agree to indemnify and hold harmless Avaya. Avaya's agents, servants and employees against all claims, lawsuits, demands and judgements arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation to the extent made by the Customer or End User.

How to Get Help

For additional support telephone numbers, go to the Avaya Web site: http://www.avaya.com/support/. If you are:

- Within the United States, click *Escalation Management* link. Then click the appropriate link for the type of support you need.
- Outside the United States, click *Escalation Management* link. Then click *International Services* link that includes telephone numbers for the International Centers of Excellence.

Providing Telecommunications Security

Telecommunications security (of voice, data, and/or video communications) is the prevention of any type of intrusion to (that is, either unauthorized or malicious access to or use of) your company's telecommunications equipment by some party.

Your company's "telecommunications equipment" includes both this Avaya product and any other voice/data/video equipment that could be accessed via this Avaya product (that is, "networked equipment").

An "outside party" is anyone who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf. Whereas, a "malicious party" is anyone (including someone who may be otherwise authorized) who accesses your telecommunications equipment with either malicious or mischievous intent.

Such intrusions may be either to/through synchronous (time-multiplexed and/or circuit-based) or asynchronous (character-, message-, or packet-based) equipment or interfaces for reasons of:

- Utilization (of capabilities special to the accessed equipment)
- Theft (such as, of intellectual property, financial assets, or toll-facility access)
- Eavesdropping (privacy invasions to humans)
- Mischief (troubling, but apparently innocuous, tampering)
- Harm (such as harmful tampering, data loss or alteration, regardless of motive or intent)

Be aware that there may be a risk of unauthorized intrusions associated with your system and/or its networked equipment. Also realize that, if such an intrusion should occur, it could result in a variety of losses to your company (including but not limited to, human/data privacy, intellectual property, material assets, financial resources, labor costs, and/or legal costs).

Responsibility for Your Company's Telecommunications Security

The final responsibility for securing both this system and its networked equipment rests with you - Avaya's customer system administrator, your telecommunications peers, and your managers. Base the fulfillment of your responsibility on acquired knowledge and resources from a variety of sources including but not limited to:

- Installation documents
- System administration documents
- Security documents
- Hardware-/software-based security tools
- Shared information between you and your peers
- Telecommunications security experts

To prevent intrusions to your telecommunications equipment, you and your peers should carefully program and configure:

- Your Avaya-provided telecommunications systems and their interfaces
- Your Avaya-provided software applications, as well as their underlying hardware/software platforms and interfaces
- Any other equipment networked to your Avaya products.

TCP/IP Facilities

Customers may experience differences in product performance, reliability and security depending upon network configurations/design and topologies, even when the product performs as warranted.

Standards Compliance

Avaya Inc. is not responsible for any radio or television interference caused by unauthorized modifications of this equipment or the substitution or attachment of connecting cables and equipment other than those specified by Avaya Inc. The correction of interference caused by such unauthorized modifications, substitution or attachment will be the responsibility of the user. Pursuant to Part 15 of the Federal Communications Commission (FCC) Rules, the user is cautioned that changes or modifications not expressly approved by Avaya Inc. could void the user's authority to operate this equipment.

Product Safety Standards

This product complies with and conforms to the following international Product Safety standards as applicable:

- Safety of Information Technology Equipment, IEC 60950, 3rd Edition including all relevant national deviations as listed in Compliance with IEC for Electrical Equipment (IECEE) CB-96A.
- Safety of Information Technology Equipment, CAN/ CSA-C22.2 No. 60950-00 / UL 60950, 3rd Edition
- Safety Requirements for Customer Equipment, ACA Technical Standard (TS) 001 - 1997
- One or more of the following Mexican national standards, as applicable: NOM 001 SCFI 1993, NOM SCFI 016 1993, NOM 019 SCFI 1998

Electromagnetic Compatibility (EMC) Standards

This product complies with and conforms to the following international EMC standards and all relevant national deviations:

Limits and Methods of Measurement of Radio Interference of Information Technology Equipment, CISPR 22:1997 and EN55022:1998.

Information Technology Equipment – Immunity Characteristics – Limits and Methods of Measurement, CISPR 24:1997 and EN55024:1998, including:

- Electrostatic Discharge (ESD) IEC 61000-4-2
- Radiated Immunity IEC 61000-4-3
- Electrical Fast Transient IEC 61000-4-4
- Lightning Effects IEC 61000-4-5
- Conducted Immunity IEC 61000-4-6
- Mains Frequency Magnetic Field IEC 61000-4-8

- Voltage Dips and Variations IEC 61000-4-11
- Powerline Harmonics IEC 61000-3-2
- Voltage Fluctuations and Flicker IEC 61000-3-3

Federal Communications Commission Statement

Part 15:

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Canadian Department of Communications (DOC) Interference Information

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

This equipment meets the applicable Industry Canada Terminal Equipment Technical Specifications. This is confirmed by the registration number. The abbreviation, IC, before the registration number signifies that registration was performed based on a Declaration of Conformity indicating that Industry Canada technical specifications were met. It does not imply that Industry Canada approved the equipment.

DECLARATIONS OF CONFORMITY

United States FCC Part 68 Supplier's Declaration of Conformity (SDoC)

Avaya Inc. in the United States of America hereby certifies that the equipment described in this document and bearing a TIA TSB-168 label identification number complies with the FCC's Rules and Regulations 47 CFR Part 68, and the Administrative Council on Terminal Attachments (ACTA) adopted technical criteria.

Avaya further asserts that Avaya handset-equipped terminal equipment described in this document complies with Paragraph 68.316 of the FCC Rules and Regulations defining Hearing Aid Compatibility and is deemed compatible with hearing aids.

Copies of SDoCs signed by the Responsible Party in the U. S. can be obtained by contacting your local sales representative and are available on the following Web site:

http://www.avaya.com/support

All Avaya media servers and media gateways are compliant with FCC Part 68, but many have been registered with the FCC before the SDoC process was available. A list of all Avaya registered products may be found at:

http://www.part68.org/

by conducting a search using "Avaya" as manufacturer.

European Union Declarations of Conformity

CE

Avaya Inc. declares that the equipment specified in this document bearing the "CE" (*Conformité Europeénne*) mark conforms to the European Union Radio and Telecommunications Terminal Equipment Directive (1999/5/EC), including the Electromagnetic Compatibility Directive (89/336/EEC) and Low Voltage Directive (73/23/EEC). This equipment has been certified to meet CTR3 Basic Rate Interface (BRI) and CTR4 Primary Rate Interface (PRI) and subsets thereof in CTR12 and CTR13, as applicable.

Copies of these Declarations of Conformity (DoCs) can be obtained by contacting your local sales representative and are available on the following Web site:

http://www.avaya.com/support

Japan

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may occur, in which case, the user may be required to take corrective actions.

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

China

BMSI (Chinese Warning Label)

警告使用者：
這是甲類的資訊產品，在居住的環境中使用時，
可能會造成射頻干擾，在這種情況下，使用者會
被要求採取某些適當的對策。

Hardware, including technical data, is subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Customer agrees to comply strictly with all such regulations and acknowledges that it has the responsibility to obtain licenses to export, re-export, or import hardware.

Environmental Health and Safety:

⚠ WARNING:

Risk of explosion if battery is replaced by an incorrect type. Dispose of used batteries according to Avaya Environmental Health and Safety guidelines.

Documentation:

For the most current versions of documentation, go to the Avaya support Web site: http://www.avaya.com/support/

Contents

About this guide

This guide provides configuration and administration information for the Avaya SG5, SG5x, SG200, SG203, and SG208 Security Gateway that are upgrade to VPNos® 4.6 and Avaya VSU® devices that are upgraded to VPNos 3.x.

The term security gateway is used generically throughout this guide to refer to the Avaya security gateway platform supported by the VPNos 4.6 software version.

The screen captures throughout this manual indicate a model SG208 security gateway, however, the actual security gateway model number is displayed dynamically. This is true of messages produced by the security gateway as well.

What's new in VPNos 4.6

The following new features are available in the current release of the VPNos software:

- CLAN support

  This feature enhancement increases the number of CLANs that are configurable in the CLAN list for IP Telephony settings. This enhancement increases the number of configurable CLANs from 5 to 20 IP addresses or symbolic host names. For more information regarding CLAN, refer to Chapter 2: Configuring interfaces, NAT and static routes.

- Support for TFTP servers and CLANs as DNS names

  This feature enhancement allows the configured TFTP servers and CLANs to be configured as traditional IP addresses or as symbolic host names. This enhancement also allows a maximum of five TFTP servers with IP addresses or symbolic host names. For more information regarding host names, refer to Chapter 2: Configuring interfaces, NAT and static routes.

What's new in VPNos 4.5

The following features were available in the previous release of the VPNos software:

- Firewall rules

  This feature enhancement increases the number of predefined firewall templates from three to five. The new firewall templates are none and VPN-only. The five levels of predefined firewall rules templates available are none, low, medium, high, and VPN-only. For more information regarding firewall rules, refer to Chapter 5: Establishing security.

- Dynamically addressed device management

  This new feature extends the administrator's power when monitoring remote devices, and delivering new and updated configuration to devices in a domain in a single step. For more information regarding dynamically addressed device management, refer to Chapter 5: Establishing security.

- Failover enhancement

  This feature enhancement allows greater network failure tracability when traceroute is configured. By using traceroute, the administrator is better able to trace where the network failure occurred. For more information regarding failover and traceroute, refer to Chapter 7: Using advanced features.

- Keep alive

  This new feature gives administrators the ability to set up connectivity checks to devices inside and outside of the VPN tunnel and to initiate traceroute when specified criteria are met. For more information regarding keep alive and traceroute, refer to Chapter 7: Using advanced features.

- Converged network analyzer (CNA)

  This new feature provides a distributed system tool for real-time network monitoring and detects and diagnoses converged-network-related issues. For more information regarding converged network analyzer, refer to Chapter 7: Using advanced features.

- Path maximum transmission unit (MTU)

  This new feature allows packets to travel through routers that are inside the protected network and outside the protected network with greater ease. For more information regarding converged network analyzer, refer to Chapter 7: Using advanced features.

- Routing

  This feature enhancement includes VPN traffic auto forwarding. VPN traffic auto forwarding allows the remote sites or users to communicate with each other without the data traffic going through the private head-end device. For more information regarding VPN traffic auto forwarding, refer to Chapter 2: Configuring interfaces, NAT and static routes.

How this guide is organized

Chapter 1: Introduction: Managing a security gateway locally, explains how to use the VPNos Web interface. In addition the chapter describes how to create and change administrative passwords.

Chapter 2: Configuring interfaces, NAT and static routes explains how to use the Network tab to change the default configuration, how to configure multiple interfaces, NAT and static route.

Chapter 3: Configuring and managing users explains how to use the Users tab to configure and mange security gateway users and remote users.

Chapter 4: Using the device tab explains how to configure the day and time, reboot the security gateway and, for SG5 and SG5X security gateways, how to do a hardware reset.

Chapter 5: Establishing security explains how to configure the security functions, including VPN setup, Services, Network Objects, Firewall Rules, Denial of Service, Dynamic Policy, and Voice of IP.

Chapter 6: Monitoring the security gateway explains how to view the Inspect and Monitor functions as well as use the Text Interface function for high-level debugging and the text interface tab to inport or export security gateway configurations.

Chapter 7: Using advanced features explains the advanced feature options of the security gateway including DNS relay, Failover, adding new licenses, SNMP, and QoS.

Chapter 8: Upgrading the VPNos software explains how to upgrade the security gateway to a new VPNos release.

Appendix A: Preconfigured firewall rules, explains the preconfigured firewall rules that can be applied to the secuirty gateway.

Appendix B: Error messages, explains common configuration error messages and the appropriate correction actions.

Appendix C: Command line interface, explains the CLI architecture and conventions. This appendix also provides instructions for accessing the security gateways for limited configuration and monitoring purposes.

Contacting technical support

Technical support is available to support contract holders of security gateway products.

Domestic support

- Toll free telephone support: (866) 462-8292 (24x7)
- Email: vpnsupport@avaya.com
- Web: http://support.avaya.com

International support

- For regional support telephone numbers, go to: http://www.avayanetwork.com/site/GSO/default.htm/

Related documentation

VPN administrators can also see the VPNmanager Configuration Guide, 670-100-600, for more configuration information, when central management is used.

The following hardware installation guides are available

- For the SG203 and SG208; documentation number 670-100-101
- For the SG5, SG5X and SG200; documentation number 670-100-102

Chapter 1: Introduction: Managing a security gateway locally

This chapter explains how to use the Web interface to configure the Avaya security gateways. You use the security gateway's Web interface for local and remote configuration and management.

This chapter also describes how to:

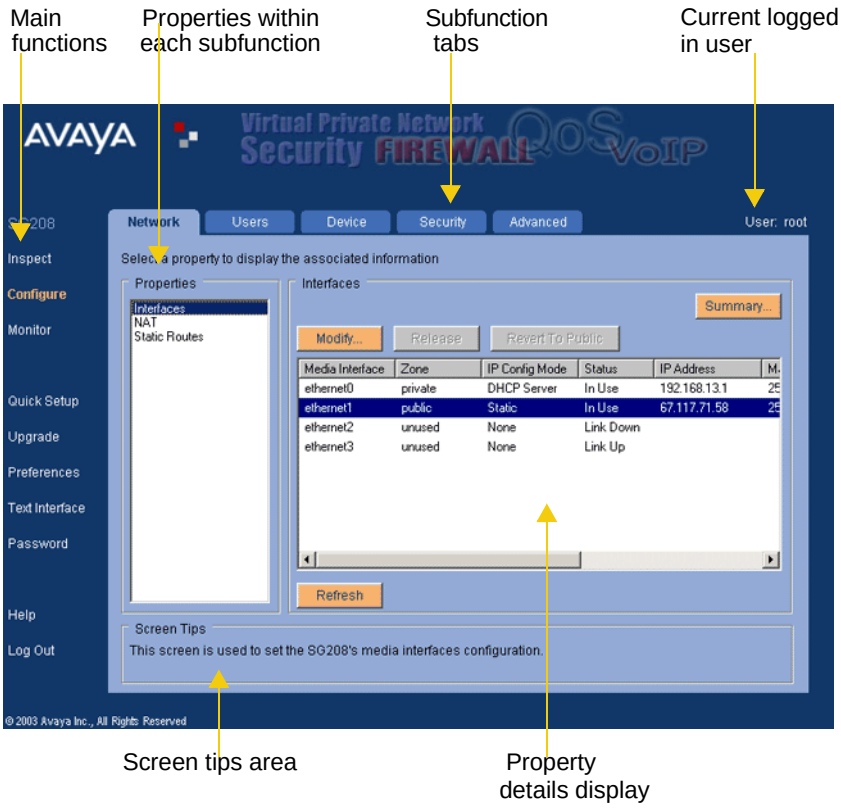
- Create and change administrative password
- Access the Web interface
- Use the Web interface functions

Using the Web interface

The Web interface of the security gateway consists of the following five major elements. These elements are available from the main Web page. Figure 1 shows these functional elements on the main Web page.

- A vertical column of *main functions*
- A set of horizontal tabs that displays the *subfunctions* within a main function
- A list of *properties* for each subfunction
- A display area for *detailed information* about the selected property
- A *screen tips* area at the bottom of the window for context-sensitive Help about the currently selected item

Figure 1: VPNos Web interface main page



Local or central administration

By default, you can configure and manage the security gateway remotely from a central location with the Avaya VPNmanager® application. If you are going to use VPNmanager to configure the security gateway, see the VPNmanager Configuration Guide.

If only the Web interface should be used to access the security gateway, centralized management can be disabled from the *Configure>Security> Management* screen, Figure 2.

When the security gateway is managed through the Web interface, the configuration exists independently of the VPNmanager and its security gateway database, therefore you can have limited access to some remote VPNs and services.

Avaya recommends that you record your security gateway configuration parameters for backup protection as permitted by your company's security policy. You can use the Text Interface>Export function to save your configuration.

When management is performed through both the VPNmanager application and the Web interface, the active security gateway configuration is the most recently changed set of properties, regardless of whether it was changed through the Web interface or through VPNmanager.

Administrative users

Within a security gateway, the following users can configure and monitor the security gateway:

- The *root user* has read and write privileges. This is the default administrator and is configured at the factory with a default password. When the administrator logs in to the security gateway for the first time, the administrator is prompted to change the default password. The root user name cannot be modified or deleted.

  The root user has full privileges on the security gateway to configure and maintain the security gateway network and user configuration, device security, and VoIP gatekeeper configuration.

- The *monitor user* has read-only permissions. The monitor user name cannot be modified or deleted. Only the password can be changed. When the monitor user logs in to the security gateway for the first time, the monitor user is prompted to change the default password.

  The monitor user can view the following properties: Inspect, Web Interface Access, and Monitor.

  The Inspect property includes interfaces, software, and general security gateway information.

  The Web Interface Access property is located under the *Configure>Security>Management* property and includes web management and centralized management.

  The Monitor property includes VPN, network, and log information.

- The *superuser* is enabled for centralized management from the Web interface *Configure>Security>Management* property. The user ID and password is entered from the VPNmanager console for authentication before VPNmanager is used to make configuration changes on the security gateway. VPNmanager has full read and write privileges to the security gateway, once it is authenticated by the security gateway.

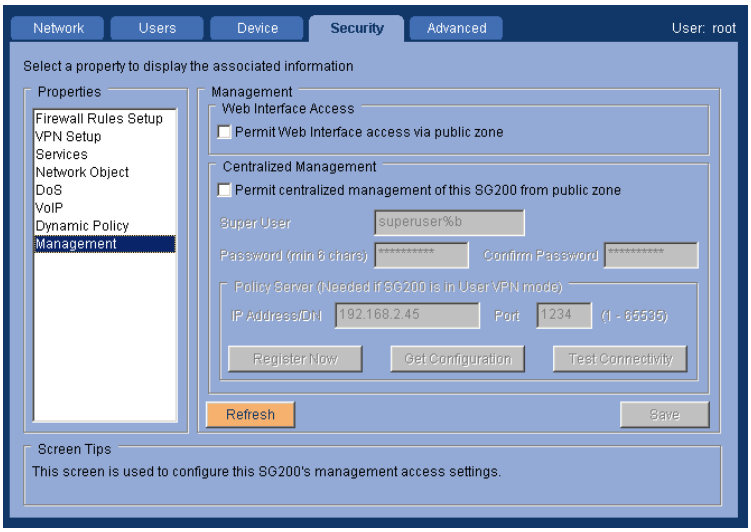
The root user or monitor user can access the Web interface remotely when the *Permit Web Interface access via public zone* box is selected. When this box is selected, you can access the Web interface through the public port. When this box is not selected, you can access the Web interface of the security gateway only from the private side.

When the *Permit Web Interface access via public zone* box is enabled, the remote administrator directs his or her browser to the IP address of the public port. When a connection with the security gateway is established, the login screen is displayed.

In addition to remote administrator access, this can be used for technical support.

The root user and the monitor user can use the *Password* function on the Web interface main page to change their passwords. The password can be from 6 to 31 alphanumeric characters.

Figure 2: Configure security management screen



Web interface access

All users log in using the Web interface. To log into the Web interface:

1. From a workstation, open the browser and type one of the following addresses in the address field.

- If DHCP domain is not the default, enter https://sg.<domainname>
- If private port address is the default, enter https://192.168.1.1
- If private port address is not the default, enter https://<dhcpserveraddress>

2. The system displays the security gateway Login screen (Figure 3).

Figure 3: Security gateway login screen

3. Type your user name and your password, and click **Log In**.

   Note:

   New users whose authentication credentials reside only on a remote security gateway or authentication server on the VPN, log in through the default VPN user account. If the user authentication credentials reside on a central security gateway (or associated authentication server) on the VPN, **Logon user default VPN** is selected.

4. The system displays the main security gateway Web interface *Inspect* function screen.

   Note:

   Once the user logs into the security gateway, an inactivity timer begins. As a security measure, if no Web interface operations are performed for 15 minutes, the session is automatically ended. The user logs in again to resume the session. This timer resets whenever the Web interface is used to send a request to the security gateway.

Logout

Use Log Out to close the security gateway Web interface. Before you log out, you must save any changes that you made during the session.

Working with the main functions

The main Web interface includes eight functions for configuration, access and monitoring the security gateway. Following is a brief description of each.

To select a main function, click the function name, it is highlighted. When a main function is selected, the appropriate subfunction tabs are displayed. To select a subfunction, click on the tab and select an individual property of that subfunction. The property details area populates with data about that particular property.

Within the property details display area, various action buttons appear, such as Refresh, Save and Cancel.

On some of the screens a Summary button is displayed. When you click this button, a text file shows the current details about the data listed in the table. You can select and copy this information to any text editor.

To save any changes click **Save**.

Use *Log Out* to quit the Web interface. Clicking the close button in the upper right-hand corner of the Web page is the same as clicking Cancel. The Web interface closes and changes that were not saved are lost.

Inspect function -

Use the *Inspect* function to view current security gateway interfaces, software version, and general system information such as the date and time, system uptime, memory used, and CPU use.

Configure function

Use the *Configure* function to configure the security gateway through the Web interface, when the *Permit Web Interface access via public port* facility is enabled. You can select from the following tabs to configure different functions of the security gateway.

- Select the *Network* tab to configure the security gateway within your network environment. You can set interface operating parameters, Network Address Translation (NAT), and Routing.
- Select the *Users* tab to configure and manage the security gateway users, including remote users and authentication source.
- Select the *Device* tab to set the date and time, perform a soft reboot, to set which configuration parameters are deleted following a hardware reset, and to configure SSH/ Telnet setting and Syslog server information.

- Select the *Security* tab to configure extended functionality of the security gateway, including Firewall rules, VPN setup, Services, Network object, Voice of IP, Denial of Service (DoS), Dynamic policy, and Management.
- Select the *Advanced* tab to configure extended functionally of the security gateway, including DNS relay configuration, failover, license, SNMP, QoS policies, and QoS mapping, NAT, Keep alive, CNA test plug, High availability, and Path MTU.

Monitor function

Use the *Monitor* function for routine observation of your connection activity and network traffic. You also can determine if any security attacks or compromises have occurred. You can select any one of the following tabs:

- Select the *VPNs* tab to monitor the connections and traffic on the VPNs. The three VPN properties monitored are IPSec security associations, IKE security associations, and VPN statistics.
- Select the *Network* tab to monitor the connections and the traffic on the network. The five properties monitored are traffic statistics, proxy ping, trace route, ARP table, and VPN packets.
- Select the *Logs* tab to view the event log, IKE log, Web interface log and firewall log. Note that these logs are maintained in circular buffers of fixed size. When a buffer is filled, wraparound occurs.

Quick Setup function

Use the *Quick Setup* function to initially establish the public zone IP address, the date, the time, and the superuser password for centralized management with Avaya VPNmanager. Select VPN mode to configure the policy server for MDAD devices.

Upgrade function

Use the *Upgrade* function to perform an upgrade of the current system image that is executing in the security gateway.

Preferences function

Use the *Preferences* function to set the refresh mode or interval for the data on an active screen and to set warning options that appear before you save or delete.

Text Interface function

Use the *Text Interface* function for low level debugging of the security gateway from the Debug tab. You can also perform configuration export and import operations from the Text Interface tab, Export and import can be used for archiving and applying configuration for selected operations.

Password function

Users logged into the Web interface can change their password.

Help

Use Help to get quick information about what a specific function or properties is used for.

Chapter 2: Configuring interfaces, NAT and static routes

When the security gateway is installed, interfaces and Network Address Translation (NAT) are preconfigured with default settings. This chapter describes how to use the Network tab to change this default configuration for your specific network environment. This chapter includes the following sections:

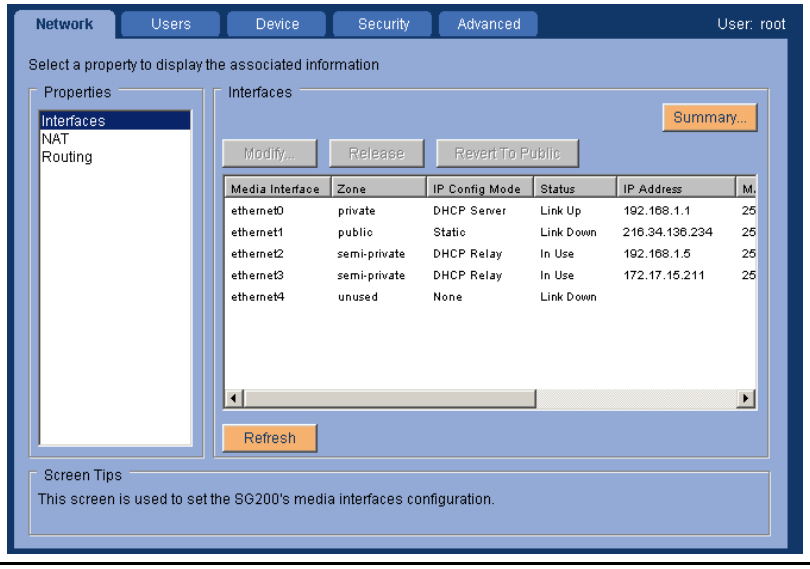
- Configuring multiple interfaces
- Configuring NAT
- Configuring static route

Configuring network interfaces

Depending on the model, a security gateway has up to six interfaces. These interfaces support Ethernet, and optionally, other media types. The Ethernet media is based on IEEE 802.3 and uses twisted-pair cabling at the physical layer.

When you select *Configure>Network>Interfaces*, the Network property display screen (Figure 4) displays the available media interfaces, with a summary of their configuration and current status.

Figure 4: Network interface property display screen



The Network Interfaces property display screen shows the following information. Scroll to see all the information.

- The name of the media interface
- The zone that is assigned to the media interface
- The IP configuration mode
- The status. Status identifies if the physical link is up or down, and if the interface is being used by network applications
- The IP address
- The mask
- The default route, if relevant
- The MAC address

Configuring network zones

Interfaces can be assigned to one of six different network uses, called *zones*. The number of zones that can be configured depends on the security gateway model (Table 1). Ethernet0 and Ethernet1 are present in all models and are assigned to the public and the private zones. The media interfaces that remain are unused and can be configured as required.

Table 1: Network zones

Media interface	SG5 and SG5X	SG200	SG203	SG208
Ethernet0	Public	Public	Private	Private
Ethernet1	Private	Private	Public	Public

1 of 2

Table 1: Network zones (continued)

Media interface	SG5 and SG5X	SG200	SG203	SG208
Ethernet2	NA	• Unused • Public backup • Semiprivate • DMZ • Management	• Unused • Public backup • Private • Semiprivate • DMZ • Management	• Unused • Public backup • Private • Semiprivate • DMZ • Management
Ethernet3 to Ethernet5	NA	NA	• Unused • Public backup • Private • Semiprivate • DMZ • Management	• Unused • Public backup • Private • Semiprivate • DMZ • Management

2 of 2

Types of network zones

The following section describes the six network zones.

Public. - The public network interface provides connection to the Internet, usually by way of a wide area network (WAN). By default, DHCP Client is used to configure the public IP address. Only one public zone can be configured on the security gateway.

Public-backup. - The public-backup network interface is used in conjunction with the Advanced>Failover function on some security gateway models, see Failover to configure failover. If a public-backup network interface is configured, and the public primary network interface cannot reach the Internet, the failover module deactivates the public primary interface, activates the public-backup interface, and then redirects all encrypted traffic to this link. When the public primary interface is again available, you can click **Revert to Public** on the *Configure>Network>Interfaces* screen to revert back to the public primary interface.

Note:

If the public zone and the public-backup zone are both configured, only one zone can operate at a given time.

To have the interface automatically revert to public, you can configure the **Timer Settings**. When you enable the idle timer, if no VPN or other traffic flows through the public-backup in the configured amount of time, the public primary interface is automatically reestablished. If the idle timer is enabled, select **Ignore Non-VPN Traffic** if you do not want non-VPN traffic to reset the idle timer. Only one public-backup zone can be configured on the security gateway.

To set the amount of time delay to switch from a secondary interface to the primary interface once the primary link has been detected, configure the **Hold Down Timer**. This delay provides the necessary time for the primary interface to stabilize. The Hold Down Timer applies to failover conditions occurring due to a link-level failure on the public primary interface only.

The Hold Down Time value is expressed in seconds. The value range is 0 to 3600 seconds. The default value is 60 seconds.

Note:

There is a scenario in which the switchover from the public backup interface to the public interface will occur before the hold down timer has expired. If the idle timer is set to a value less than that of the hold down timer, and the public primary interface link becomes available while at roughly the same time traffic ceases to flow through the public backup interface, the switchover will occur when the idle time expires rather than when the hold down timer expires.

Private. - The private network interface usually provides connection to your private local area network (LAN) or your corporate LAN. By default, the private network interface is configured with DHCP Server.

Semi-private. - The semi-private network interface provides connection to a network whose equipment can be made physically secure, but whose medium is vulnerable to attack, such as a wireless network used within a corporation's private network infrastructure). Traffic on the semi-private interface is usually encrypted. Only one semi-private zone can be configured on the security gateway.

DMZ. - The demilitarized zone (DMZ) network interface is usually used to provide Internet users with access to some corporate services without compromising the private network where sensitive information is stored. A DMZ network contains resources such as Web servers, FTP servers, and SMTP (e-mail) servers. Because DMZ networks are vulnerable to attack (that is denial of service), corporations usually add additional security devices such as intrusion detection systems, virus scanners, and so on. Only one DMZ zone can be configured on the device.

Management. - The management interface connection can be configured to simplify network deployments, to eliminate enterprise network dependencies on switches or routers. The management network interface is usually used as an access point for a dedicated VPNmanager management station or as a dedicated interface for dumping log messages to a syslog server.

Options for IP addressing for interface zones

You can configure each zone with different addressing options and the private port can be configured as a DHCP server or DHCP relay used to obtain IP addresses from the DHCP server. (Table 2). This section explains the options in detail.

Table 2: Type of IP addressing available by zone

	Public	Private	Public-backup	Semi-private	DMZ	Manage-ment
Address assigned						
H.323	X	X		X	X	
Static	X	X	X	X	X	X
DHCP Client	X	X*	X			
PPPoE	X		X			
Server modes						
None	X	X	X	X	X	X
DHCP Server		X		X	X	
DHCP Relay		X		X	X	
H.323	X	X		X	X	

* The DHCP Client for the Private zone is for SG5/5X/200 and VSU 5/5X/500 bootcode only.

Static addressing

Use static addressing if a dedicated IP address should be assigned to the public interface of the security gateway. To configure static addressing, complete the following information:

Field	Description
IP Address	The public IP address that is assigned to the security gateway
Network Mask	The subnet mask
Route	The IP address of the gateway router to the Internet

DHCP addressing

Use DHCP addressing if the gateway obtains its IP address dynamically from the internet service provider (ISP). DHCP is the default configuration.

When DHCP Client is configured, the Release/Renew button on the *Network>Interfaces* property screen is active. This button can help you to resolve some problems with the network connection without the need to reboot the security gateway. Click **Release** to end an established DHCP Client session. Click **Renew** to create a new DHCP Client session.

Point-to-Point Protocol Over Ethernet (PPPoE) Client

Use PPPoE Client addressing as a convenient way to connect the public interface of the security gateway to the Internet, if your ISP supports PPPoE addressing. PPoE Client addressing requires user authentication. To configure PPPoE addressing, complete the following information

Field	Description
PPPoE User ID	Account user name which your ISP assigns
Password	Account password

When PPPoE is configured, the **Connect** button on the *Network> Interfaces* property screen is active. This button can help you to resolve some problems with the network connection without the need to reboot the security gateway. Click to terminate an already established PPPoE session and **Renew** to create a new session.

Note:

Avoid resetting the security gateway by power cycling the unit when PPPoE is configured, as this method requires a proper shutdown in order to avoid a lockout condition during reconnection. This lockout period can last for a few minutes (time varies from ISP to ISP).

Local DHCP Server

The local DHCP server private port configuration is the default configuration to support the IP devices that are connected to your LAN. In the local DHCP server mode, the protected devices are automatically provided with an IP address, a default route, a domain name (the security gateway), and primary and secondary WINS.

To configure the local DHCP server, complete the following information:

Field	Description
IP Address	The IP address assigned. The default IP address is 192.168.1.1 for the private interface. If multiple interfaces on a security gateway have DHCP server configured, their IP addresses must be unique.
IP Range From/To	The range of IP addresses that the DHCP server that runs on the interface assigns to DHCP clients. The default DHCP address range for the private interface is 192.168.1.32 to 192.168.1.127. Each security gateway on the VPN requires a unique DHCP range. In addition, if multiple interfaces on a security gateway have DHCP server configured, the DHCP range on each also must be unique.
Domain Name	The domain assigned to the interface. This is only applicable to the private interface. The default for domain name is “private.”

Field	Description
Primary WINS	This is optional. Configure primary WINS when delivering network configuration information to DHCP clients. The security gateway will deliver the primary WINS server information before the secondary WINS server information. This order of delivery will ensure that DHCP clients will use the WINS servers in the specified configuration order.
Secondary WINS	This is optional. Configure secondary WINS when delivering network configuration information to DHCP clients. The security gateway will deliver the secondary WINS server information after the primary WINS server information. This order of delivery will ensure that DHCP clients will use the WINS servers in the specified configuration order.
IP Device Configuration	This is configured to add support for additional IP devices to the virtual DHCP Server.
IP Telephony Settings	This is optional. Configure IP Telephony when IP telephones are connected to the security gateway. See IP Telephony Configuration below.

When DHCP server is configured, you can configure the IP Device and the IP Telephony settings. Click **IP Devices** to display a list of all IP devices that the DHCP server currently supports. The MAC address and IP address are listed, along with information that relates to IP telephony devices

Note:

When changing the DHCP IP address range, execute an ipconfig release and renew command, then either reopen your browser and/or enter into the location field the domain name or address that was specified or changed. For example https://sg.domainname or https://newipaddress.

Changing the DHCP Server IP address can result in losing current connectivity with the security gateway. Also all active DHCP clients can require “renewal” through an OS utility (e.g., using winipcfg or ipconfig in Windows), or rebooting.

IP telephone configuration - If you are using the security gateway with the Avaya Definity® series of IP Telephones, you must configure the TFTP server IP, the TFTP file path, the Definity Clan IP and the Definity Clan port (See the Definity documentation for further information). Non-Avaya IP telephones require at a minimum, the TFTP server IP address.

The following IP telephone DHCP options are supported:

- Option 150. Proprietary to Avaya IP telephones. This option is for the TFTP server IP address.
- Option 176. Proprietary to Avaya IP telephones. Definity Clan IP address and port along with optional TFTP server IP address (all four fields in the IP Telephony Configuration section must contain entries).
- Option 66. The standard DHCP option for TFTP server.

Note:

When you add an IP device, you must also modify the Device Account User. For more information on the Device Account User, see To modify a user profile.

DHCP Relay

When you select DHCP relay, the DHCP relay agent binds to the private interface and forwards only DHCP requests from the network behind the device to a DHCP server on the public side of the network. This server is usually a corporate DHCP server. The corporate DHCP server is usually within the private network of the corporation, so the DHCP requests and responses are tunneled (i.e. IPSec) between the security gateway and the corporate network.

Note:

DHCP relay and DHCP server services are mutually exclusive. When the security gateway acts as a DHCP relay, the security gateway cannot also be a DHCP server at the same time.

When the DHCP relay agent receives DHCP client requests from the private port, the DHCP server(s) creates new DHCP messages and forwards the messages to the DHCP server(s) on the public network. THE DHCP servers on the public network send DHCP offer messages that contain the IP addresses to the DCHP relay agent. The agent broadcasts the DHCP offer messages to the DHCP clients.

For the DHCP relay process to begin, the IP address of the remote DHCP server(s) and the private port of the security gateway must be part of the VPN.

None

When you select **None**, the security gateway is configured with a static IP address and Mask. IP devices on the network that are connected by this interface must assign their IP address, Mask, Default route, DNS servers, WINS servers, and domain name manually or use an external DHCP server.

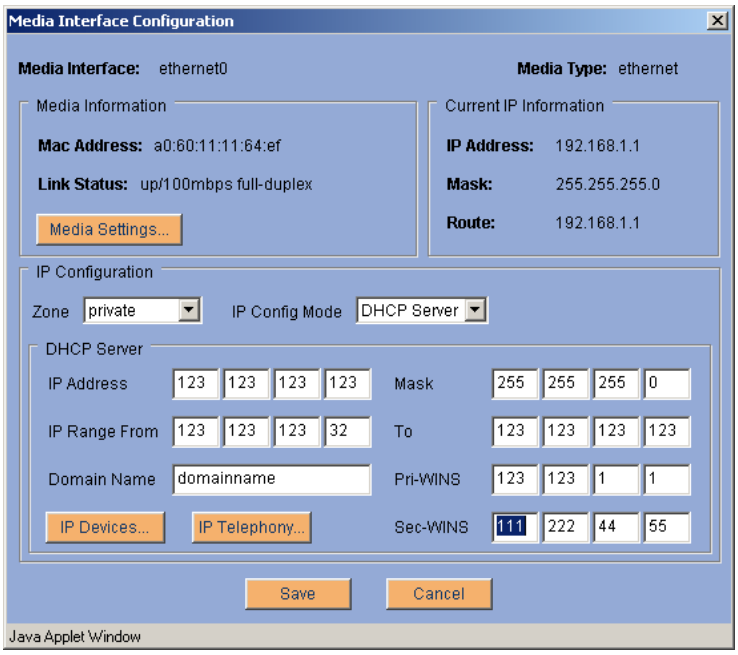
Changing network interfaces

From the Network Interfaces property display screen, you can modify the media settings, change the IP information, add an IP device, and configure IP telephony settings.

To change the media interface configuration:

1. Click the **Configure>Network>Interfaces** property. Select the media interface that you want to modify. Click **Modify**. The Media Interface Configuration dialog is displayed.(Figure 5)

Figure 5: Media interface configuration dialog



Note:

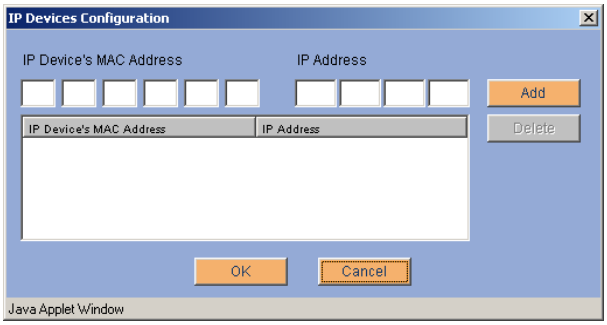
The fields displayed in the screen are based on the type of zone selected.

2. In the **IP Configuration** area, make the required changes.
   - From the **Zone** list, select the zone. Only the zones that apply to that media interface are displayed.
   - From the **IP Config Mode** list, select the IP addressing mode. Depending on your selection, complete the required information.
   - If public-backup is selected, complete the **Hold Down Timer** and **Idle Timer Settings** configuration if failover is enabled.
3. Click **Save** when you finish.

To add an IP device to the security gateway:

1. Click the **Configure>Network>Interfaces** property, select the media interface that is configured with private, DHCP Server. Click **Modify**. The Media Interface Configuration dialog is displayed.
2. Click **IP Devices**. The IP Device Configuration dialog is displayed.

Figure 6: IP devices configuration screen

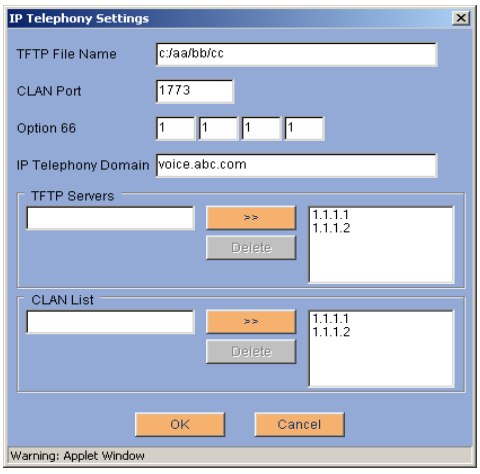


3. Enter the following information
   - The MAC address of the IP device. If the device is an Avaya IP telephone, the MAC address is on the back of the telephone.
   - The IP address. This IP address must be within the same subnet as the DHCP server. Avaya recommends that you use an IP address for the device that falls into the DHCP subnet but not in the DHCP range.
4. Click **Add**, and then click **OK**.

To add an IP telephony device to the security gateway:

1. Click **IP Telephony**. The IP Telephony Settings dialog is displayed.

Figure 7: IP telephony configuration screen



2. Enter the following information

- TFTP File Path. The TFTP file path is used when the file path is other than the default path.
- Definity CLAN Port. The port number for the Definity server. The default port is 1719. The port range is 0 to 65535.
- Option 66. The standard DHCP option for TFTP server.
- IP Telephony Domain. This is the domain name that the IP telephone device is assigned.

Important:

When symbolic host names are included in the TFTP server or CLAN lists, the IP telephone will append the IP Telephony Domain name (if entered) to the list entry in order to create a fully qualified domain name (FQDN). You can, however, enter the host names using FQDN form of <myhost>@<mydomain>.<topleveldomain>, in which case you should leave the IP Telephone Domain name field empty.

Also, be aware that the current version of IP telephone firmware will truncate the TFTP and CLAN lists to a maximum of 255 characters each. Thus, when using the FQDN form of host name entries, it would be possible to exceed that limitation very quickly.

- TFTP Server IP address. This is the server on which the latest version of the IP telephone firmware is maintained for upgrade purposes. A maximum of five TFTP servers with IP addresses or symbolic host names can be configured on security gateways running VPNos 4.6 and higher.
- CLAN IP List. The IP address of the Definity CLAN server. A maximum of 20 CLAN IP addresses or symbolic host names can be configured on security gateways running VPNos 4.6 and higher.

3. Click **OK**, and then click **Save**.

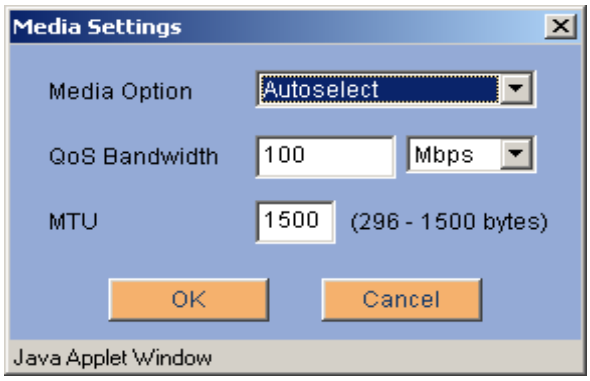
Note:

When you configure an IP telephone, secure tunnels are created for TFTP and Definity CLAN. However, if only VPN users are connected, the secure tunnels are created on demand. That is, the secure tunnels are created only when traffic exists on the associated tunnel.

To change media settings:

1. Click the **Configure>Network>Interfaces** property. Select the media interface that you want to modify. Click **Modify**. The Media Interface Configuration dialog is displayed.

Figure 8: Media settings screen



2. To change the media settings, click **Media Settings**. The Media Settings dialog is displayed. The media option choices depend on the media type selected and the capabilities of the underlying device hardware and driver.
3. Enter the **QoS bandwidth** value.
4. The Qos bandwidth value is used by the QoS module to restrict the bandwidth of the interface to the upstream limit of the network. For example, to allow QoS to regulate maximum bandwidth of a 100 mbps to 25 mbps, enter 25 mbps.
5. Enter the **MTU** value.
6. The MTU value ranges from 296 MTU to 1500 MTU. For maximum MTU performance, set the MTU minimum value to 512 and the maximum value to 1492.

Note:

If the system is configured as PPPoE, the maximum recommended MTU value is 1492.

7. Click **OK**, and then click **Save**.

Note:

Under most circumstances Reboot is not necessary. Reboot the security gateway if the Web interface recommends that you reboot or if the device does not work properly after you reconfigure the media settings.

Setting NAT

Network Address Translation (NAT) is an Internet standard that allows private (nonroutable) networks to connect to public (routable) networks. To connect private networks and public networks, address mapping is performed on a security gateway that is located between the private network and the public network.

You can set up three types of NAT mapping on the security gateway:

- Static NAT. With static NAT, addresses from one network are permanently mapped to addresses on another network. One private IP address can be translated to one public IP address. Static NAT is bidirectional, that is, for outgoing packets, static NAT translates the source IP address of the packets. For incoming packets, static NAT translates the destination address of the packets. You must specify both the original address and the translated address to configure static NAT.
- Port NAT. With port NAT, addresses from internal, nonroutable networks are translated to one routable address in port NAT. Port numbers, in the case of TCP/UDP packets and sequence numbers and IDs in the case of ICMP packets, are used to create unique channels. Port NAT is unidirectional. That is, port NAT translates only outgoing packets and not incoming, but it does translate the replies. On the way out, the source address of the packet is translated. For the replies, the destination address is translated back. You can choose from predefined network objects or user-defined network objects, or you can specify the IP address and the Mask for the original address. You must specify the IP address and the port ranges for the translated address. The port ranges must be in a range from 5000 to 65535.
- Port Redirection. With port redirection, addresses from a specific address and a specific port are redirected to another address and port. Port redirection translates the destination address of an incoming packet and the source address of the reply. You must specify the from address, the to address, and the port number.

By default, NAT is enabled, and the *Share public address to reach the internet* feature is selected. NAT affects only clear traffic. If your network contains any nonroutable addresses, Avaya recommends that you enable the share public address to reach the internet feature.

Note:

Any firewall rules that are in use can block translated traffic.

Priority of NAT types

NAT is a rule-based policy, where the priority is based on the NAT type and than the order in which the NAT types appear in the NAT list. NAT types have the following priority:

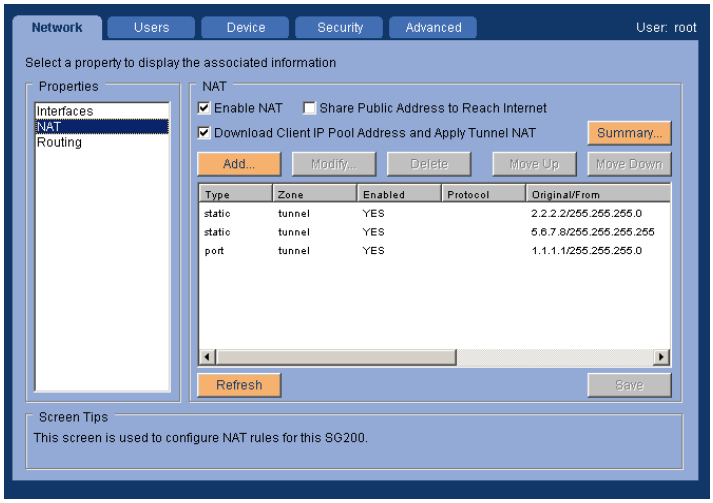
1. Redirection
2. Static NAT
3. Port NAT

Configuring NAT

You should have a good understanding about how NAT works before trying to configure NAT for VPNos. This guide does not explain how NAT works.

When you select the NAT property, the Configure>NAT property display screen (Figure 9) displays the NAT rules that are configured.

Figure 9: NAT property detail screen



The NAT property detail screen displays the following information for each rule. Scroll to see all the information.

- The type of rule. The types are static, port, or redirection.
- The zone to which the NAT rule applies.
- The status of the rule. Status is enabled or not enabled.
- The protocol. Protocols are TCP, UDP, TCP/UDP, or ANY.
- The Original/From IP address/mask.
- The Translation/To IP address.

- The Start/From port.
- The End/To port.

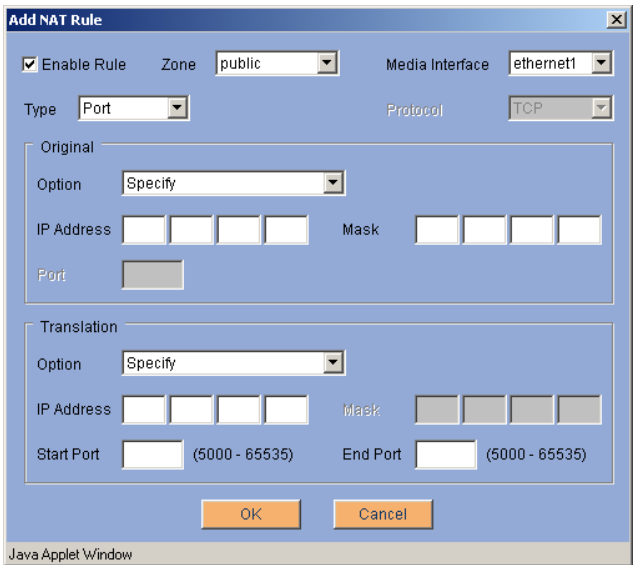
You can add, modify, and delete NAT rules. You can construct a series of rules, and enable or disable each rule as necessary.

A rule can be moved up or down to change the priority. See Priority of NAT types on page 36.

To add a pubic or private NAT rule:

1. Select the **Configure>Network>NAT** property. Click **Add**. The Add NAT Rule dialog is displayed (Figure 10).

Figure 10: Add public or private NAT rule dialog



2. Select the zone for the NAT rule. The Media Interface field displays the media that corresponds to the zone that you select.
3. From the **Type** list, select either static, port, or redirection. See Setting NAT on page 35.

   Note:

   The screen displays only the fields that must be configured according to the zone and the translation type that you select.

4. In the **Original** area, complete the available or active areas:
   - Option. Select from the list of predefined network objects and user defined network objects or select *Specified*.
   - IP Address. Type the original/from address
   - Mask. Type the mask
   - Port. Type the from TCP/UDP port number. This port number can be from 1 to 65535.

5. In the **Translation** area, complete the areas that are not grayed out
   - Option. Select from the list.
   - IP Address, Type the translated/to address
   - Start Port. Type in the Start port. This port number can be from 5000 to 65535
   - End Port. Type in the End port. This port number can be from 5000 to 65535
   - Port. Type in the To port. This port number can be from 1 to 65535
6. To enable this NAT rule, select **Enable Rule**.
7. Click **OK**, and then click **Save**.

Tunnel NAT rules

Tunnel NAT rules are applied to VPN traffic before encapsulation and encryption.

During VPN setup, tunnel NAT rules are applied. Select the **Download Client IP Pool Address and Apply Tunnel NAT** check box when the security gateway is configured in the user VPN mode.

Note:

When the Download Client IP Pool Address and Apply Tunnel NAT check box is selected, all other NAT rules will be ignored.

Selecting this check box enables the head-end security gateway to download the client IP address pool to the remote device, and apply a port NAT rule on the tunnel zone. The original IP address translates to the private zone subnet and the tunnel NAT address translates to the client IP address.

The Download Client IP Pool Address and Apply Tunnel NAT check box is not applicable is the security gateway is configured in VPN gateway mode.

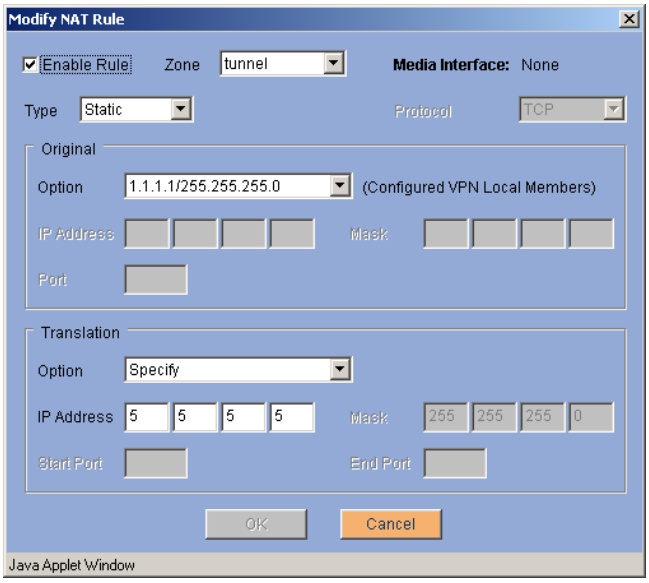
Note:

The client IP pool address is only downloaded during the first VPN user or VPN default user login. The client IP pool address is not downloaded again for another VPN user or VPN default user login. the client IP pool address is released when all VPN users or VPN default users have logged out and the device user account is disabled.

To add a tunnel NAT rule:

1. Select the **Configure>Network>NAT** property. Click **Add**. The Add NAT Rule dialog is displayed (Figure 11).

Figure 11: Add tunnel NAT rule dialog



2. Select the **tunnel** zone for the NAT rule. The Media Interface field displays the media that corresponds to the zone that you select.
3. From the **Type** list, select either static or port. See Setting NAT on page 35.

   Note:

   Redirection NAT rule cannot be applied to the tunnel zone.

4. In the **Original** area, complete the available or active areas:

   - Option. From the list, select a pair of configured VPN local members IP address and subnet mask.

   Note:

   If the security gateway is configured in VPN gateway mode, it must have VPNs configured in order to populate the list of configured VPN local members ip addresses and subnet masks. If the security gateway is configured in user VPN mode, only the private zone subnet is displayed in the available list.

5. In the **Translation** area, complete the areas that are not grayed out:
   - Option. Select from the list.
   - IP Address, Type the translated/to address

   Note:

   If Static NAT is selected, the subnet mask is automatically populated and is the same as the original subnet mask.
6. Click **OK**, and then click **Save**.

To modify a NAT rule

1. Select the **Configure>Network>NAT** property. Select the rule that you want to modify. Click **Modify**. The Modify NAT Rule dialog displays.
2. Change the information as required.
3. Click **OK**, and then click **Save**.

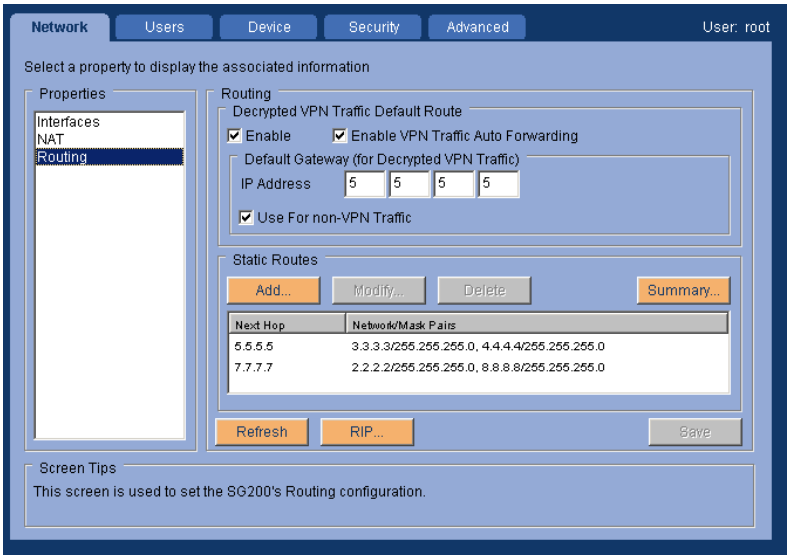
To delete a NAT rule

1. Select the **Configure>Network>NAT** property. Select the rule that you want to delete. Click **Delete**. An information box appears to verify the deletion.
2. Click **OK**, and then click **Save**.

Setting routing

The Routing property detail screen shows the VPN traffic default routes, including the IP address of the default gateway. The Routing property detail screen also shows static routes, including the IP address of the hop, and the IP address and network mask pairs for this hop. You can add, modify and delete static routes.

Figure 12: Static route property detail screen



To build a decrypted VPN default routes table:

1. Select the **Configure>Network>Routing** property.
2. Select the **Enable** box to enable default route.
3. Select the **Enable VPN Traffic Auto Forwarding** box to disable traffic auto forwarding.

   Beginning with VPNos 4.5, the SG is able to enable and disable automatic re-encapsulation and encryption forwarding.

   If an SG receives a VPN packet that is not destined for the protected network, the SG will automatically forward this packet to the configured remote TEP. By default, the **Enable VPN Traffic Auto Forwarding** box is selected, or checked.

   To disable the automatic forwarding of packets, the **Enable VPN Traffic Auto Forwarding** box should be un-checked.

   When the VPN traffic auto forwarding is disabled, the SG will divert the packets to the private interface. By redirecting the packets to the private interface the packets can be monitored by Intrusion Detection Systems software before sending the packets to the remote TEP on the private network.

   Before disabling VPN traffic auto forwarding, confirm that a VTDR or static route is configured on the private interface. If a VTDR is not configured on the private interface, the redirected packet will not be sent back to the SG to be forwarded to the remote TEP.
4. Enter the **IP address** for the default gateway.
5. Select the **Use for non-VPN traffic** box to use default gateway for non-VPN traffic.
6. Click **Save**.

Static Routes

Static routes are specified when more than one router exists on a network that the security gateway must forward either VPN traffic or non-VPN traffic. You can build a static route table with up to 32 network address/mask pairs.

To build a static routes table:

1. Select the **Configure>Network>Routing** property. Click **Add**. The Add Static Route dialog displays.
2. Enter the next hop address, the IP address, and the network mask. Click **Add**.
3. Add additional IP addresses and network masks, as required. Click **Add** after each IP address and mask that you add.
4. Click **OK**, when you finish. The property detail screen is displayed.
5. Click **Save**, to save the changes that you made to static routes.

To modify a static route to delete an IP addresses/mask pair

1. Select the **Configure>Network>Static Route** property. Selected the hop route that you want to change. Click **Modify**
2. Select the specific address to delete. Click **Delete**.
3. Click **OK**.The property detail screen is displayed.
4. Click **Save**, to delete the configuration and update the static routes.

To delete a specific static route from the property detail screen

1. Select the **Configure>Network>Static Route** property. Selected the route you want to delete. Click **Delete**. The route is removed from the list.
2. Click **Save**, to delete the route and update the static routes.

Routing information protocol (RIP)

If the security gateway is in a protected network with many routers or gateways to other TCP/IP networks, there can be more than one possible path to a specific router. In this case, routers are building routing tables from the information exchanged by a routing protocol. Security gateways can use such protocols to dynamically build a routing table.

To build a RIP table:

1. Select the **Configure>Network>Routing** property.
2. Click the **RIP** button to configure RIP parameters.
3. Select the boxes for **Listen/Learn** and **Advertise** that apply to your configuration.
4. Click the **Advanced** button to configure the network metric values.
5. In the **Route Idle Timer** text box, enter the time, in seconds, that the route will transition from active to idle. The timeout period between active and idle is configurable from 1 to 3600 seconds.
6. In the **Active Metric** text box, enter the metric value for active route traffic flow.

   As traffic flows through the route, the route transitions from initial to active.
7. In the **Initial Metric** text box, enter the metric value for initial route traffic flow.

   When the VPN route is added to the route table and before traffic begins to flow, the initial value is applied to the route. Set the initial value higher than the idle metric value, yet lower than the active metric value.
8. In the **Inactive Metric** text box, enter the metric value for inactive route traffic flow.
9. Click **OK** to exit the RIP Advanced Settings window.
10. Click **OK** to exit the RIP Configuration window.
11. Click **Save**.

Chapter 3: Configuring and managing users

This chapter explains how to configure and manage the following users:

- Security gateway users
- Remote users

Note:

The VPNos Web interface can be used to quickly create a small number of users, or to change individual user configurations on a security gateway. To easily configure and maintain a large number of users in a VPN, use VPNmanager.

Configuring and managing security gateway users

Three default users are configured on the security gateway.

- **Monitor (Monitor User)**. The monitor user is an admin type of user who is configured with permissions to use the Web interface to monitor the security gateway. You cannot modify or delete the monitor user profile. Only the password can be changed. See the Administrative users.
- **Device Account User**. You can configure the Device Account user to act as a proxy VPN user for all configured IP devices. You cannot delete the device account user.
- **Default VPN User**. The Default VPN user is the default SG5X CCD user when the security gateway is in User VPN mode or Dynamic VPN mode. If a default user is configured, the SG5X users can login to the VPN using the profile of the Default VPN user.

  The authentication credentials of the users reside only on a remote security gateway or an authentication server in the VPN, log in through the default VPN user account. Thus administrative efforts to manage users is reduced.

  Default VPN user is not a login name. Users must enter a login name and a password. Default VPN users must also select the **Log in using default VPN** when the users log in.

  Note:

  VPN users must exist on the central authenticating security gateway in order for logins to succeed.

Configuring new users

You can add individual users, modify user profiles, and delete individual users of the VPN. You can also configure individual users authentication profiles for users that do not need to use the default VPN when they log in.

Note:

Once users are created, a Web interface session must be activated to allow VPN traffic to occur. This is also true following a reboot of the security gateway.

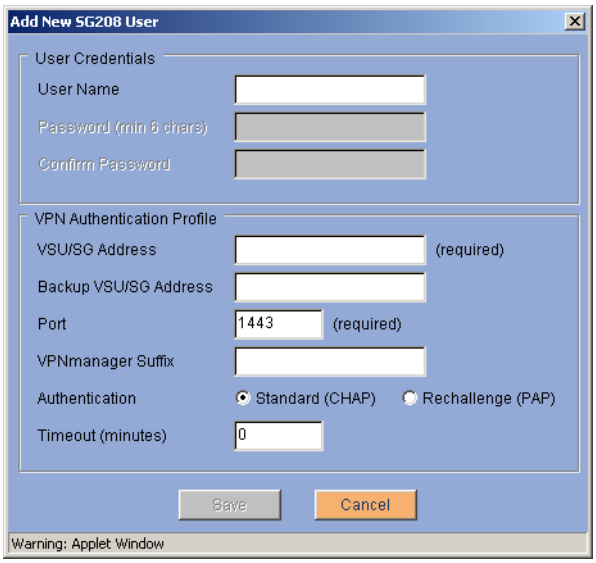
Before you can add a new user, you must determine

- The user name
- A default password for the first time that a new user logs in
- A VPN authentication profile that includes
- Address of the security gateway or domain name
- Backup security gateway address or domain name
- Type of authenticating to use

  Standard (CHAP). When you select Standard (CHAP) as the authentication mechanism, users are not presented with a rechallenge screen before logging in.

  Rechallenge (PAP). When you select rechallenge (PAP) as the authentication mechanism, the user is presented with a challenge screen to return the required login information to the SecurID server. The first time that the user tries to log in, a setup screen appears to establish the user PIN. From that point on, the users use a passcode to log in, which consists of both the PIN and the current number on the token.

Figure 13: Add new security gateway user screen



To add a new user

1. Select the **Configure>User>SGxxx** property. Click **Add**. The Add New User dialog is displayed (Figure 13).
2. Enter the user name.
3. Complete the **VPN Authentication Profile** area.
   - **VSU/SG Address**. Enter the device address.
   - (Optional) **Backup VSU/SG Address**. Enter a backup device address to be used.
   - **Port**. Enter the number of the port to use. The default is 1443.
   - (Optional) **VPNmanager Suffix**. Enter the VPNmanager suffix for the security gateway that authenticates this user (optional). This suffix is used when two users on a VPN have the same user name (in different trees) and the authentication source is an LDAP server.
   - **Authentication**. Select the authentication type to use, either Standard (CHAP) or Rechallenge (PAP).
   - **Timeout (minutes)**. Enter the number of minutes that this user can remain active before the VPN session is stopped. The default is 0, that is, the session does not time out.
4. Click **Save**, to complete the configuration.

To modify a user profile

The following table shows the type of information that you can modify for the various types of users.

User type	Name	Password	VPN Authentication
Monitor		X	
Default VPN			X
Device Account User	X	X	X
VPN User			X

To modify a user profile:

1. Select the **Configure>User>SGxxx** property. Select the user profile that you want to modify.
2. Click **Modify**, to display the Modify User dialog.
3. Enter the required user credentials and VPN authentication information.
4. Click **Save**.

To delete a VPN User

You can delete only individual VPN users.

1. Select the **Configure>User>Security Gateway Users** property. Select one or more users to delete.
2. Click **Delete**. A message is displayed that warns that you are deleting users.
3. Click **OK**, to delete the users credentials and authentication profiles from the security gateway.

Configuring and managing VPNremote Client users

VPNremote Client users who log in to the VPN through the security gateway must have their user authentication configured on that security gateway.

As a minimum, you must configure the user name and the password for each remote user. User names can be up to 128 characters long and can contain any character except a comma (,). Note that once you add a user name, you cannot change the name.

You can configure a remote user as a default user. When a remote user is configured as default user, the user password is not required to log in.

You can also change the default Internet Key Exchange (IKE) identity, the split tunneling option and the security option. Table 3 describes these settings.

Table 3: VPNRemote Client user advanced configuration

Setting	Description
IKE Identity	Internet Key Exchange (IKE) is a protocol by which a secure tunnel is established between the security gateway and the remote user. You can define the type of IKE identifier that is associated with the user. Four types of identifiers can exist in the certificate generated for the remote users: IP address, DNS name, directory name, email ID.
Split Tunneling	By default, split tunneling is allowed. You can disable split tunneling to prevent remote users from browsing the Internet while the users are connected to the VPN.
Security	Security is the option to storing the VPN configuration in the VPN remote workstation. The default is to always authenticate. When the default is in effect, the authentication policy is downloaded to the user automatically. When the remote user disconnects, the policy is removed from the client. You can change the security option to either "Authenticate only to receive latest configuration," when this option is in effect, and a remote user connects. or "Secure Dyna-Policy with a user-defined key (password)," When this option is in effect, and a remote user connects, the user's dyna-policy is downloaded to the user automatically. The policy is permanently stored in the VPNremote Client, and the user is automatically prompted to create a password to protect the dyna-policy.

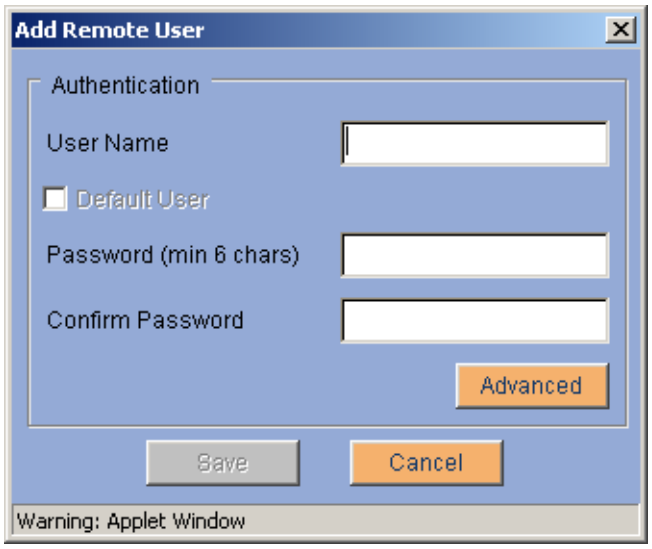
Configuring remote users

From the security gateway, you can add, modify and delete remote users. From Advanced settings, you can make changes to the default IKE identity, the split tunneling option, and the security option.

To add a remote user

1. Select the **Configure>Users>Remote Users** property. Click **Add**. The Add Remote User screen is displayed, Figure 14.

Figure 14: Add remote user screen

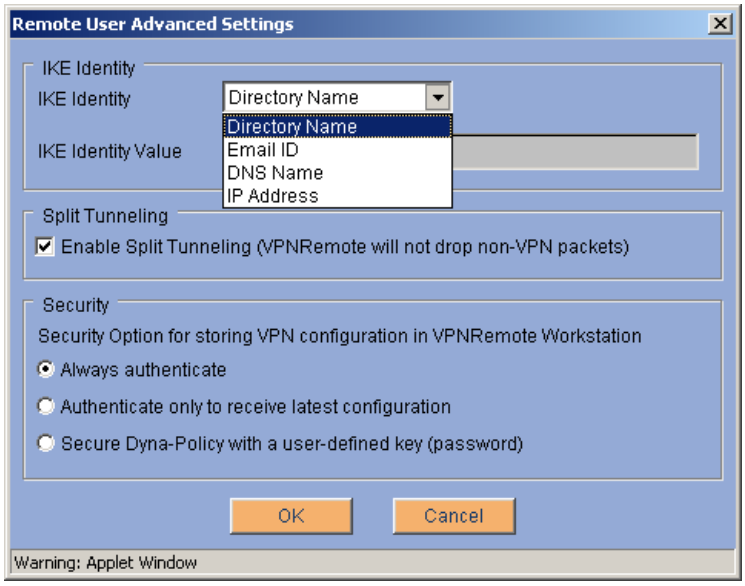


2. Enter the user name and password.

   The user name can be up to 255 characters long and can contain any character except a comma (,).

3. (Optional) To change the default settings for IKE, split tunneling, or security, click **Advanced**. The Remote User Advanced Settings dialog is displayed, Figure 15.

Figure 15: Remote user advanced settings



4. Change the advanced settings as required, including:
   - From the list select either IP address, DNS name, directory name, or e-mail ID.
   - Note that Enable Split Tunneling is checked.
   - Select a security option.
5. Click **OK** to close the Advanced Settings screen and return to Add Remote User.
6. Click **Save** to add the remote user.

To modify a remote user

The type of information that you can change for a remote user depends on the original configuration of the user. You cannot change any fields that are unavailable.

1. Select the **Configure>Users>Remote Users** property. Select the name that you want to modify. Click **Modify**. The Modify Remote User screen is displayed.
2. Make the required changes, including any advanced setting changes.
3. Click **Save**, to modify the user configuration.

To delete a remote user

1. Select the **Configure>Users>Remote Users** property. select one or more user profiles to delete.
2. Click **Delete**. A message box is displayed, warning that you are deleting users.
3. Click **OK** to delete the remote user from the security gateway.

Configuring and managing authentication source

Prior to VPNos 4.3, the only source of authentication for remote users in the VPN was local authentication on the security gateway. The user credentials are stored in the security gateway local database.

RADIUS Authentication

In VPNos 4.3, RADIUS authentication, an external authentication source, has been incorporated. RADIUS authentication involves using an external RADIUS server for remote user authentication. The user credentials are stored in the RADIUS server's database.

A RADIUS client has been implemented in the security gateway that sends authentication requests to the external RADIUS server(s) on behalf of the remote users. Upon authentication success, the client notifies the security gateway's client configuration download (CCD) server to provide the VPN policy and user configuration to the remote user.

The only source of VPN policy configuration for remote users is the security gateway local database. The VPN policy and user configuration is stored in the security gateway.

When the RADIUS Authentication property is selected, the two options for remote client configuration (CCD) are:

- by the security gateway, select **Local Authentication**

  The security gateway authenticates remote users in the VPN from the local configuration database.The security gateway authentication supports local authentication with local configuration.

- by the RADIUS server, select **RADIUS Authentication**

  The RADIUS server authenticates remote users whose credentials are stored in its local database. The RADIUS server authentication supports RADIUS authentication with local configuration.

RADIUS server IP address assignment

The RADIUS server supports configuration and storage of a user IP address. This IP address is stored with the user credentials in the server's database. Upon successful user authentication, the server sends the IP address to the security gateway's RADIUS client that provides the IP address to the CCD server. This IP address is assigned to the user during CCD.

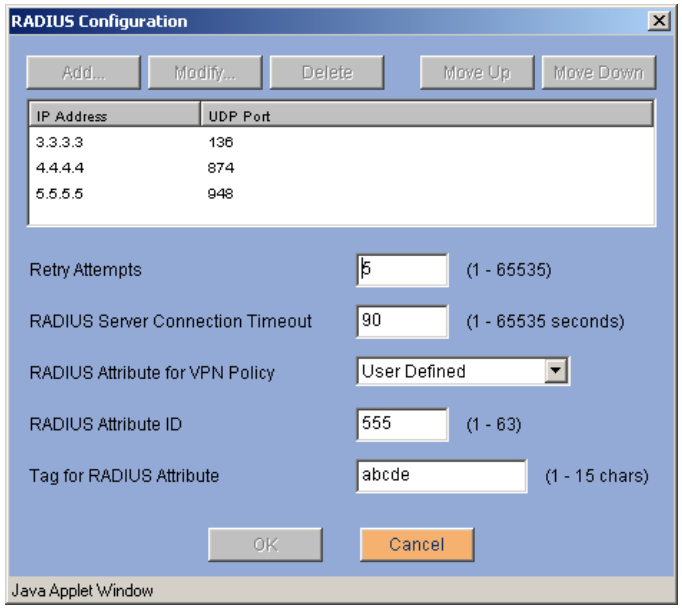
Configuring RADIUS authentication source

From the security gateway, you can add, modify and delete RADIUS authentication source. From RADIUS Configuration, you can make changes to the RADIUS options.

To configure RADIUS configuration:

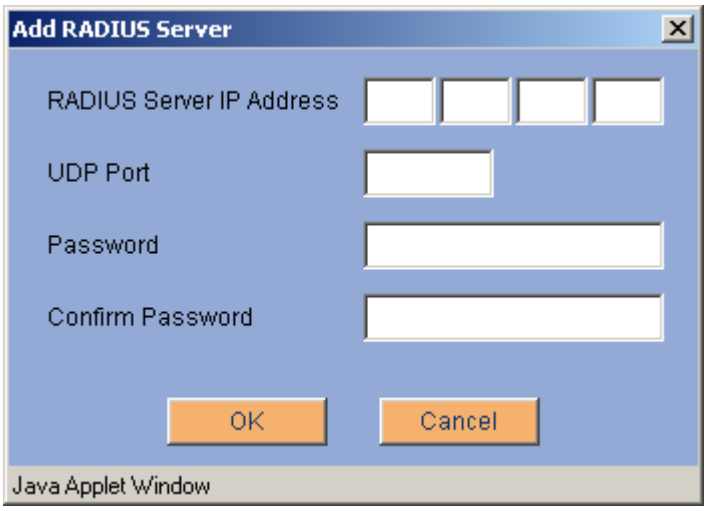
1. Select the **Configure>Users>Authentication Source** property. Click **RADIUS Configuration**. The RADIUS Configuration screen is displayed.

Figure 16: RADIUS Configuration Settings



2. Click **Add** to add a RADIUS server.

Figure 17: Add RADIUS Server Settings



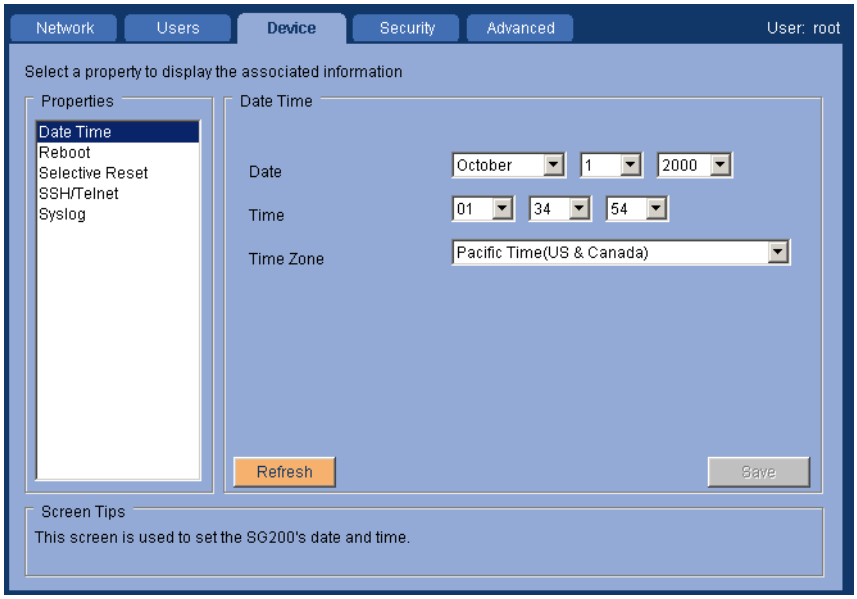
3. Enter the following settings:
   - RADIUS server IP address
   - UDP Port
   - Password
   - Confirm Password
4. Click **OK** and confirm default RADIUS configuration settings.
5. Click OK to close the RADIUS configuration settings screen and return to Authentication Source.

Chapter 4: Using the device tab

This chapter explains the *Configure* > *Device* subfunction. From the Device tab, Figure 18, you can:

- Configure day and time for the security gateway
- Perform a software reboot of the security gateway
- Set which configuration parameters are deleted after a hardware reset for the SG5 and SG5X.
- Configure SSH/Telnet parameters
- Configure Syslog settings

Figure 18: Configure device date and time details



Date and time

Use the Date Time property to set the internal clock and calendar of the security gateway.

The date and time settings are primarily used to ensure accurate timestamps when events are logged. A 24-hour clock is used to set the time. For example, 13:00:00 is equivalent to 1:00 p.m.

Reboot

Use the Reboot property to do a soft reset of the security gateway. The system displays a Reboot button when you select the Reboot property.

When you click **Reboot**, the system displays a warning message before the security gateway is reset. The applet is then closed, and a new login screen appears. Any unsaved changes are lost when you click **Reboot**.

Note:

All active VPN user sessions are ended when you click **Reboot**.

Selective reset

Use the **Configure >Device >Selective Reset** property to select options to be reset and deleted when you must use a hard reset to shut down the security gateway.

Note:

Only the SG5 and SG5X security gateways can be reset at this time.

The actions that can occur following a hardware reset are to

- Reset the root user password
- Delete all certificates, except manufacturing certificates
- Delete all users, except the preconfigured users
- Delete all VPNs.

Figure 19 shows the Selective Reset dialog box. The Selective Reset dialog is available only to the root administrator.

Two different types of reset are available: selective reset and connectivity reset.

To reset the SG5 and the SG5X, push the Reset button through the pinhole on the security gateway.

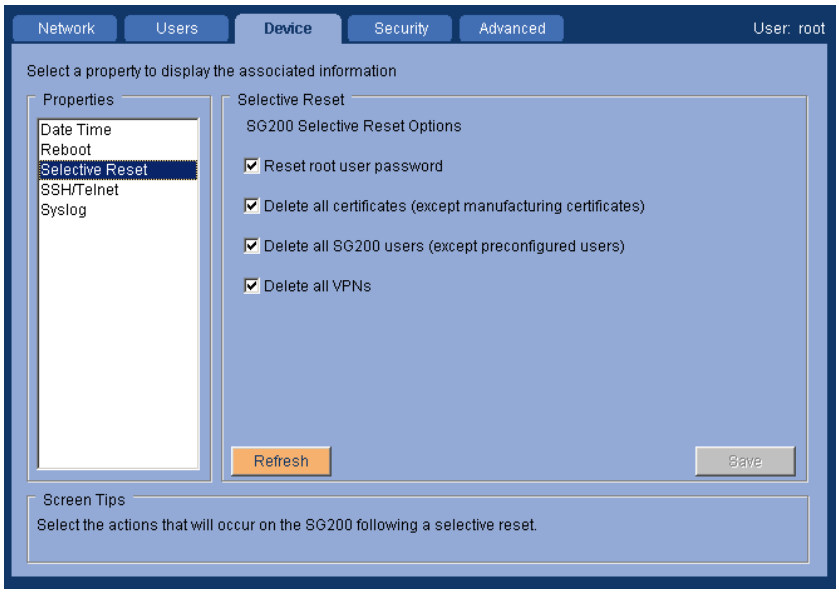
Selective reset

When the Reset button is pressed briefly (less than five seconds) and released, the action enabled as determined by the Hard Reset property window occur.

Note:

After this type of hard reset, you must reconfigure any item that is selected on this page.

Figure 19: Configure device selective reset



Connectivity reset

The second type of reset, a “connectivity reset” occurs when the Reset button is pressed and held in for more then five seconds. This type of reset is useful when a configuration error results in the loss of connection to the security gateway. Actions that occur include:

- Public IP address, the private DHCP address are removed
- All firewall rules are removed
- All VPN definitions are removed
- Root user password is reset to its default value.

Important:

When either type of reset is performed, you must reboot the security gateway. Go to Configure>Device>Reboot.

Note:

To recover from an accidental reset, immediately power the security gateway off, then back on to prevent the reset actions from being saved to flash.

SSH/Telnet

SSH (Secure Shell) and Telnet can be used to access the security gateway's CLI. If you use SSH to transfer data, the entire log in session, including transmission of the password, is encrypted. If you use Telnet to communicate with the security gateway, data transfer is not encrypted.

You can turn on both SSH and Telnet, and specify the port to use and the allowed IP addresses that can access the security gateway. The default is the following:

- SSH is enabled for Any host on the private zone, all other zones are disabled.

  Only the root and the monitor users can use SSH/Telnet to access the security gateway.

- Telnet is disabled on all zones.

  Hosts in a designated zone must access the security gateway through the designated zone's IP address.

Be advised that Telnet transfers data in the clear. Telnet data is not encrypted.

Use the **Configure>Device>SSH/Telnet** property to change the defaults and to configure or change the security gateway SSH/Telnet feature.

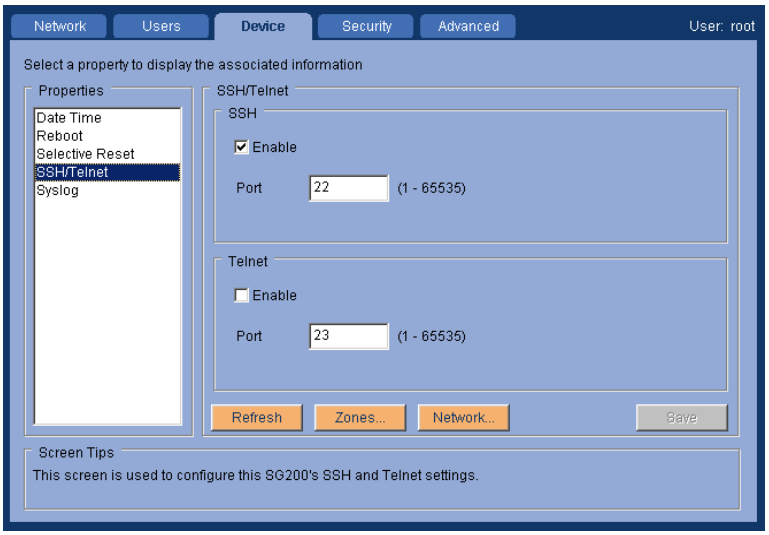
When you log in to the security gateway using either SSH or Telnet, the security gateway's CLI interface is displayed. You can then use the CLI commands to troubleshoot the security gateway.

To use SSH/Telnet in the VPN zone, the following must be configured:

1. Enable the zone to access the security gateway.
2. Configure the security gateway IP address as part of the VPN.

To set up SSH or Telnet

1. From the **Configure>Devices>SSH/Telnet** property, select Enable for SSH or Telnet.



2. Specify the port number.
3. Click **Zones** to configure the Blocked and Allowed network zones.
4. Click **Network** to configure the Network Objects and the IP Address and Mask.
5. Click **Add** to include the IP Address and Mask in the designated list. Click **OK**.
6. Click **Save** to save the configuration.

Syslog

Security gateways have a syslog messaging facility for logging system error messages. The messages can be automatically sent to a destination running a Syslog server.

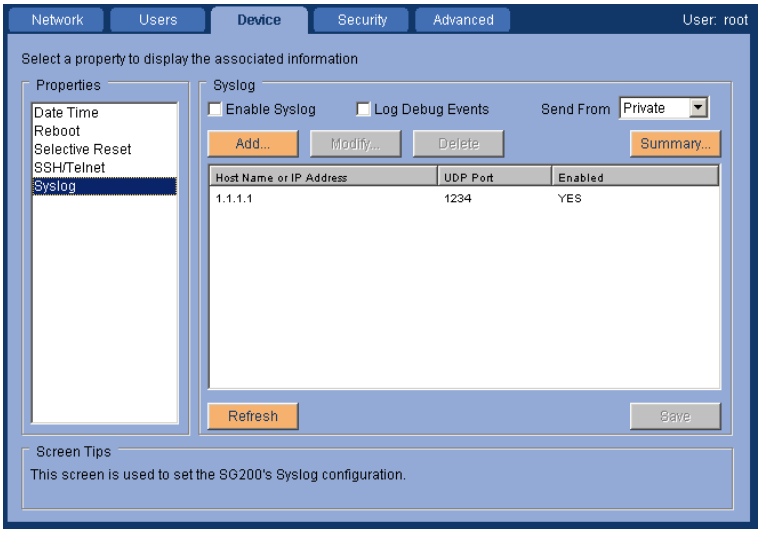
When the Enable Syslog box is checked, syslog reporting to the target hosts in the list occurs.

Host Name/IP Address — The domain name or IP address of the target logging archive machine.

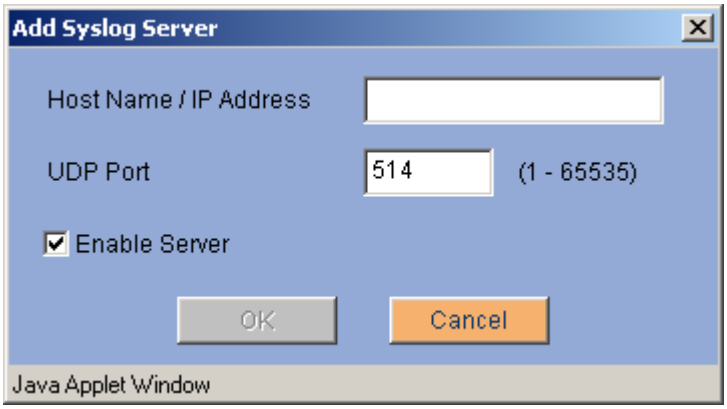
UDP Port — The port number of the Syslog host.

To enable the Syslog server:

1. From the **Configure>Devices>Syslog** property, select Enable Syslog.



2. Click **Add**. The Add Syslog dialog appears.



3. In the Host Name/IP Address field, enter the host name or the **host IP address** of the Syslog server.
4. In the UDP Port field, confirm the port number. The default is 514.
5. Select the **Enable Server** checkbox to enable Syslog message logging to the specified server.
6. Click **OK**.
7. Click **Save**.

Chapter 5: Establishing security

This chapter explains the functions used to establish a secure gateway.The *Configure Security* subfunction is used to configure extended functionality of the security gateway, including Firewall rules, VPN setup, Services, Network Objects, Denial of Service, Dynamic Policy, Voice over IP, and Management.

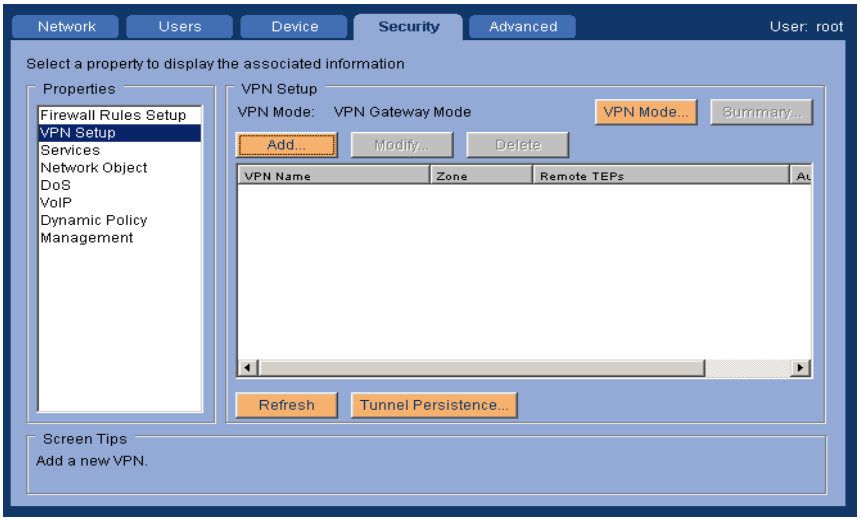
VPN setup

The *VPN Setup* property provides additional information about the security gateway. You can also use this property to add VPNs or extranet in which participation is desired.

To construct a VPN for the security gateway, you must configure the following:

- A unique name that identifies the VPN. One VPN can be configured as the default VPN.
- An authentication method. This is the means by which a remote user is authenticated.
- Local IP groups. Used for a site-to-site and/or user VPN setup.
- Remote tunnel endpoints. Used for a site-to-site and/or user VPN setup.
- IP groups
- Remote users
- Security, IKE security, and IPSecurity Protocol (IPSec) security. When you set up an IKE-based VPN object, you use IPSec to encrypt and decrypt VPN traffic. IKE VPNs always operate in tunnel mode. In tunnel mode, the entire original packet is encrypted and inserted in the payload of the IPSec packet before the IPSec packet goes out to the public networks.

Figure 20: Configure security VPN property



VPN mode

When you setup the VPN, you can configure the VPN mode. The VPN mode specifies what type of VPN policies the security gateway applies. The two types of VPN modes are *static* and *dynamic*.

Three types of VPN policies are supported for the security gateway:

- Static VPN policy is for site-to-site VPNs. This VPN policy can be applied in Static VPN mode only.
- Remote Users VPN policy is for remote VPN users. This VPN policy can be applied in both VPN modes.
- Dynamic VPN policy is dynamically downloaded by the security gateway for the VPN user, the default VPN user, and the Device Account user. This VPN policy is applied in Dynamic VPN mode only.

For the SG5, SG5X and the SG200 security gateways, the default is Dynamic. You can switch the VPN mode to Static.

For the SG203 and SG208 security gateways, the default is Static.You cannot switch the VPN mode to Dynamic.

Static VPN mode is also called VPN gateway mode. The following VPN policies are applied in this VPN mode: remote users VPN policy and Static VPN policy. VPN users are not allowed to log in from the private zone.

Dynamic VPN mode is also called User VPN mode. The following VPN policies are applied in this VPN mode: Remote Users VPN policy and Dynamic VPN policy. Site-to-site VPNs are not applied in this VPN mode.

Note:

When Failover with the public-backup zone is configured and the security gateway is using the public-backup zone, the VPN mode is automatically changed to dynamic.

VPN wizard

Use the VPN wizard to help you set up the VPN. The wizard helps you to enter the necessary configuration parameters to define a new VPN or extranet.

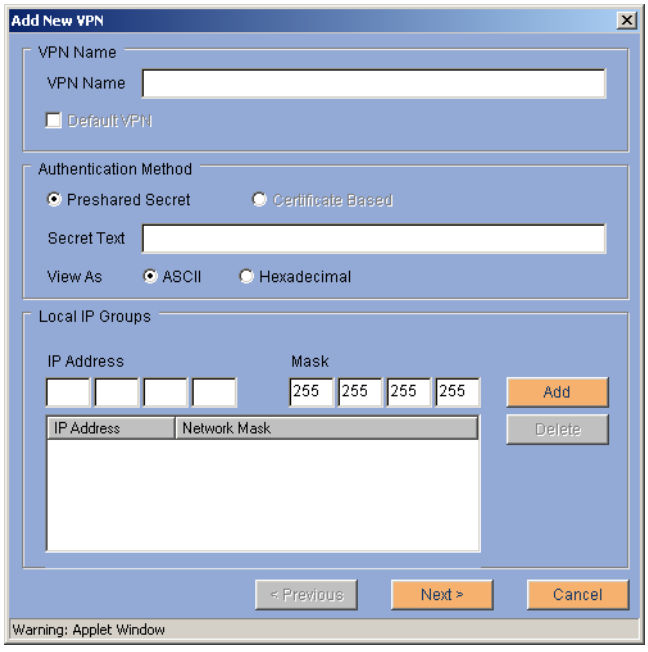
Note:

Some VPNs are created dynamically by remote users who have logged in and you cannot modify or delete these VPNs.

To add a VPN

1. Select the **Configure>Security>VPN Setup** property. Click **Add**. The VPN Wizard is launched.

Figure 21: VPN wizard screen 1



2. In the **VPN Name** area,
   - Enter a unique name that identifies the VPN. This name can be up to 31 characters long.
   - If you want this VPN to be the default, select the Default VPN checkbox.
     When selecting the Default VPN checkbox, the remote user should be a member of this VPN. Remote user who are not configured on the security gateway can login to the VPN using the default remote user profile.
3. In the **Authentication Method** area, the Preshared Secret is enabled.

   Only this choice is available for this release. Both the local and the remote security gateway must have the identical preshared secret text, or a secure tunnel cannot be established between them.
   - In the **Secret Text** field, enter the secret text, up to 64 characters.
   - In the **View As** field, select ASCII or Hexadecimal.
4. In the **Local IP Groups** area, enter the IP Address. Click **Add** to move the information into the Member IP group(s) window.

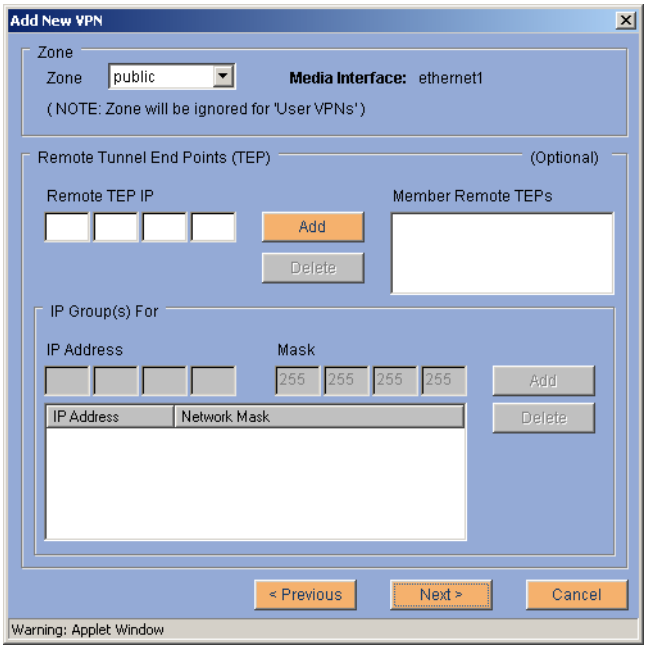
   This window lists the IP addresses of the IP groups on the private side of the security gateway that belong to this VPN.

   Note:

   Be sure that the local IP Groups cover the private address of the security gateway. Member Groups are the Local IP Groups on the remote security gateway.

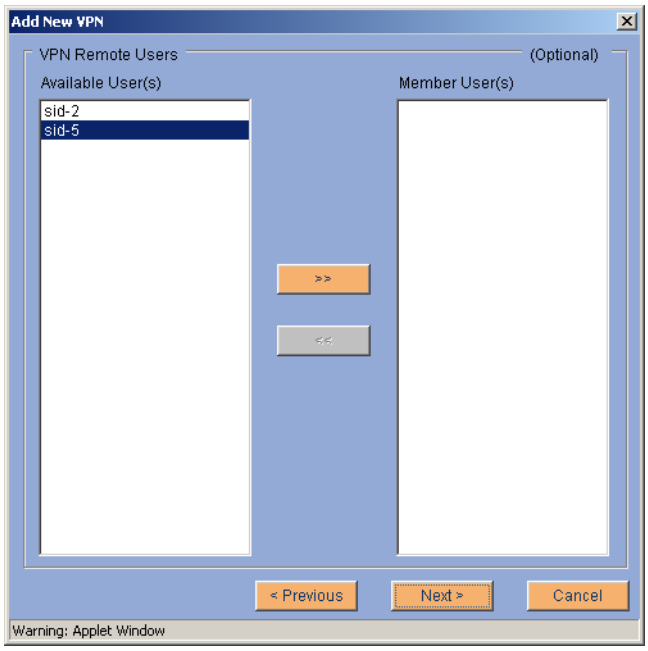
   To designate remote user access to a specific VPN, create the VPN with specific IP address for remote users only. The remote users must be included in the local IP group configured for the specific VPN.
5. Click **Next**, when you finish. The second VPN Wizard dialog is displayed.

Figure 22: VPN wizard screen 2



6. In this dialog, configure the following:
   - Remote Tunnel Endpoints area. In the **Remote VSU IP** field, enter the IP address of the remote security gateway that belongs to the new VPN. Click **Add**.
   - IP Groups For: area. In the **IP Address** field, enter the IP group address (behind the remote security gateway) that belongs to this VPN. Click **Add**.
7. Click **Next**, when you finish building the remote security gateway and IP group membership. The last VPN wizard dialog is displayed.

Figure 23: VPN wizard screen 3



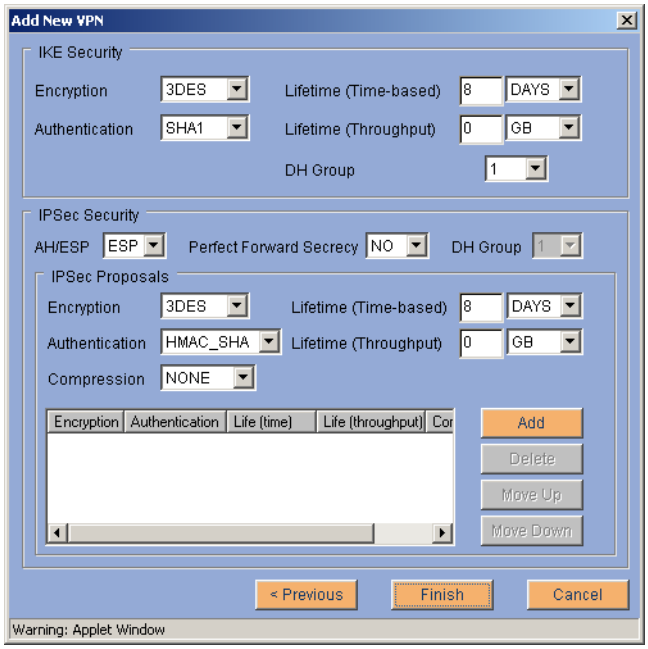
8. From the **Available Users** list, select the remote users that belong to the new VPN. Click the right arrows to move the user names to the **Member Users** list. Click **Next**.

   Note:

   You can add only one default remote user to the member user list.

   The dialog that is displayed is used to configure IKE and IPSec security.

Figure 24: VPN wizard screen 4



9. In the IKE Security area set up the key-exchange parameters that you want used for the VPN. Complete the following fields:

Field	Description
Encryption	Select one of the following types: • DES. A common encryption algorithm that is not subject to export regulations. • 3DES. A robust encryption algorithm. 3DES is subject to government regulation. Contact Avaya for a current list of controlled and uncontrolled application and territories. • Any. Accepts any encryption proposal that is made by the device on the other side. IKE VPNs use ESP to encrypt IP packets as defined in RFC2406. You can choose either DES-CBC or 3DES-CBC (Domestic U.S./Canada only) encryption.

Field	Description
Authentication	Select one of the following types: • MD5 (RFC1321) • SHA1 • Any. Accepts any authentication proposal that is made by the device on the other side. IKE VPNs use either an ESP trailer as defined in RFC2406, or AH as defined in RFC2402 to authenticate IP packets.
Lifetime	Payload key lifetime defines the extent to which a single set of cryptographic keys is used when applying VPN services to IP packets. Lifetimes are either time based or based on throughput. **Time-based** lifetimes are based on the amount of time that the keys are used without a key change. **Throughput-based** lifetimes are defined by the amount of data that is acted on by a set of keys. The more often a key is changed, the “more secure” the system. However, frequent key changes can affect system performance. Enter a numerical value and select a unit of measure for both time-based and throughput lifetimes. Whichever occurs first triggers the new key. **Note:** For time-based lifetime, the following are the minimum values in each category: Day = 1, Minutes = 1, and Seconds = 60.

Field	Description
DH Group (Diffie-Hellman Group)	Diffie-Hellman groups define the cryptographic key strengths used during IKE negotiations. The level of security increases as the DH group number increases. Using a higher level DH group results in longer key exchange times. • Group 1 Key strength: 768 bit Platform support: SG5, SG5x, SG200, SG203, and SG208 • Group 2 Key strength: 1024 bit Platform support: SG5, SG5X, SG200, SG203, and SG208 • Group 5 Key strength: 1536 bit Platform support: SG5, SG5X, SG200, SG203, and SG208 • Group 14 Key strength: 2048 bit Platform support: SG203 and SG208 See RFC2409 for more information on Diffie-Hellman Groups.

10. In the IPSec Security area (parameters relating to the payload) set up the IPSec protocol information that you want the VPN to use. Complete the following fields:

Field	Description
AH/ESP	Select either AH (Authentication Header) or ESP (Encapsulation Security Payload) to use either an ESP trailer as defined in RFC2406, or AH as defined in RFC2402 to authenticate IP packets.

Field	Description
Perfect Forward Secrecy	Select Yes or No This field defines a parameter in which disclosure of long-term secret keying material does not compromise the secrecy of the exchanged keys from previous communications. Enabling Perfect Forward Secrecy is “more secure” but involves more overhead. Avaya recommends that you use this option if your VPN encryption algorithm is DES. See RFC2409 for more information on Perfect Forward Secrecy. When you select (Yes) to enable Perfect Forward Secrecy, you must also select, a Diffie-Hellman Group number.
DH Group (Diffie Hellman Group)	Diffie-Hellman groups define the cryptographic key strengths used during IPSEC negotiations. The level of security increases as the DH group number increases. Using a higher level DH group results in longer key exchange times. • Group 1 Key strength: 768 bit Platform support: SG5, SG5x, SG200, SG203, and SG208 • Group 2 Key strength: 1024 bit Platform support: SG5, SG5X, SG200, SG203, and SG208 • Group 5 Key strength: 1536 bit Platform support: SG5, SG5X, SG200, SG203, and SG208 • Group 14 Key strength: 2048 bit Platform support: SG203 and SG208 See RFC2409 for more information on Diffie-Hellman Groups.

11. The **IPSec Proposals** area displays a list of all currently defined proposals ranked by priority of negotiation. You can use up to four proposals.

    For an example, you might have several proposals for an extranet. When you use several choices, you increase the possibility that both sides can find a mutually common proposal. Also, when international security gateways (DES only) and domestic security gateways (DES or 3DES) are part of the VPN, having a DES proposal establishes a common ground for two security gateways to communicate.

12. Complete the following fields:

Field	Description
Encryption	Select one of the following types: • DES. A common encryption algorithm not subject to export regulation. • 3DES. A robust encryption algorithm. • AES-128. The advanced encryption standard that uses a 128 bit block to help resist large attacks. • Any. Accepts any encryption proposal made by the device on the other side.
Authentication	Select one of the following types: • Any. Accepts any authentication proposal that is made by the device on the other side. • None • HMAC-MD5 • HMAC-SHA
Compression	Select one of the following types: • None • LZS The security gateway supports IP payload compression using IPCOMP. Use of the LZS parameter improves usage of bandwidth and throughput. This is the default configuration. This parameter applies to VPN traffic only.

Field	Description
Lifetime	Payload key lifetime defines the extent to which a single set of cryptographic keys is used when applying VPN services to IP packets. Lifetimes are either time based or based on throughput. **Time-based** lifetimes are based on the amount of time that the keys are used without a key change. **Throughput-based** lifetimes are defined by the amount of data that is acted on by a set of keys. Enter a numerical value and select a unit of measure for both time-based and throughput lifetimes. Whichever occurs first triggers the new key. **Note:** For time-based lifetime, the following are the minimum values in each category: Day = 1, Minutes = 1, and Seconds = 60.

13. Click **Add** to complete security configuration.

    The IPSec proposals are ranked by order of negotiation with the device on the other side. The first proposal in the list is attempted first, and so on. To change the order of negotiation, use Move Up and Move Down.

14. Click **Finish**. The VPN set up is complete.

Tunnel persistence

Two types of tunnel persistence are supported for the security gateway:

- Maintain VPN tunnels on device update
- Rebuild all VPN tunnels on device update

In a multiple VPN structure with tunnel persistence set to *Maintain VPN tunnels on device update*, traffic is interrupted within the modified VPN only. In a multiple VPN structure with tunnel persistence set to *Rebuild All VPN tunnels on device update*, all VPNs related to the security gateway being updated are interrupted until the configuration update is complete.

Figure 25, illustrates tunnel persistence between SGs. If *Maintain VPN tunnel* is enabled, the addition of SG_D to VPN_2 interrupts and re-establishes tunnel persistence in VPN_2 only. Because modifications were not made in VPN_1 (SG_A and SG_B), or VPN_3 (SG_B and SG_D) tunnels remain persistent.

Figure 25: Security Gateway Tunnel Persistence

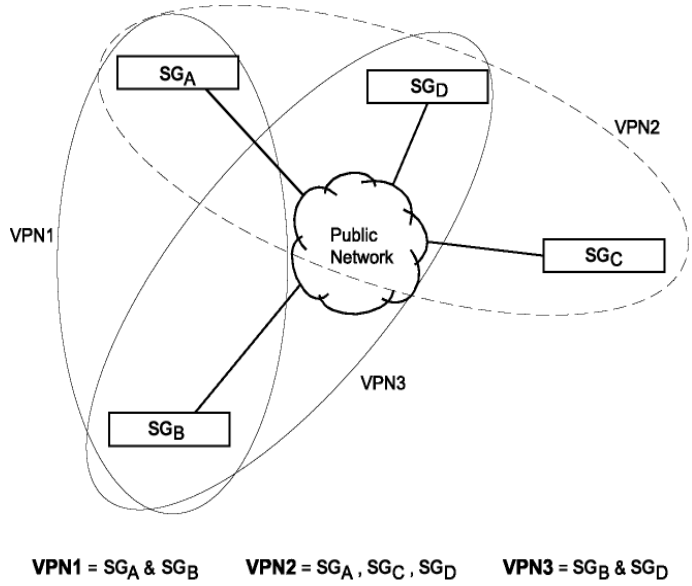
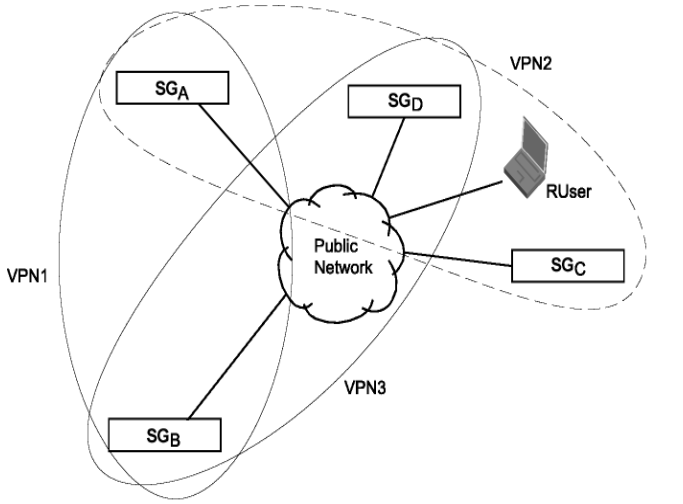


Figure 26 illustrates tunnel persistence between SGs and remote users (RUser). The addition of SG_D to VPN_2 (SG_A, SG_C, SG_D, and Remote User) interrupts tunnel persistence in VPN_2, thus breaking the remote connection. Once the configuration update is complete, the remote connection will be restored. Because modifications were not made in VPN_1 (SG_A and SG_B) and VPN_3 (SG_B and SG_D), tunnels remain persistent.

If a change in configuration is made to the IKE policy, the remote connection is broken. Once the configuration update is complete, the remote connection will not be restored. To restore the remote connection, the remote user must log out of the security gateway and login to the security gateway again.

Figure 26: Remote User Tunnel Persistence

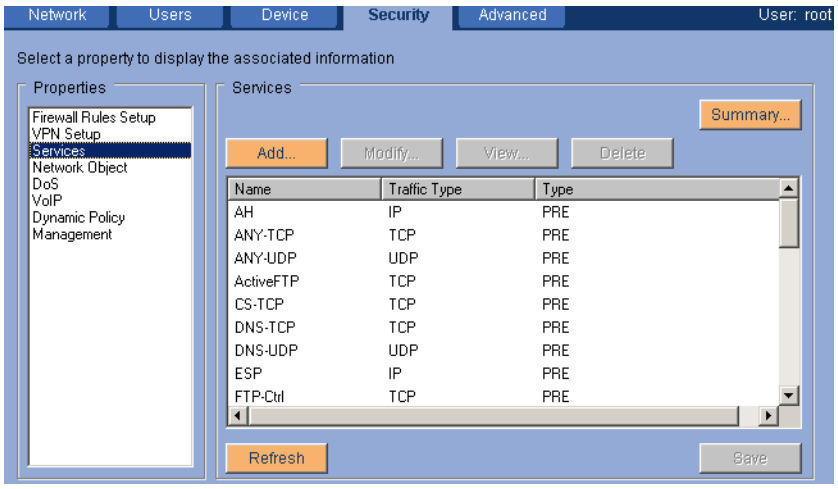


VPN1 = SG_A & SG_B **VPN2** = SG_A , SG_C , SG_D , RUser **VPN3** = SG_B & SG_D

Services

The Services property provides a list of predefined traffic types and user-defined traffic types that enhance the firewall and Quality of Service (QoS) rules. For instance, you can add a user-defined service for use in firewall rules that allows or blocks a specific type of traffic.

Figure 27: Configure security services property

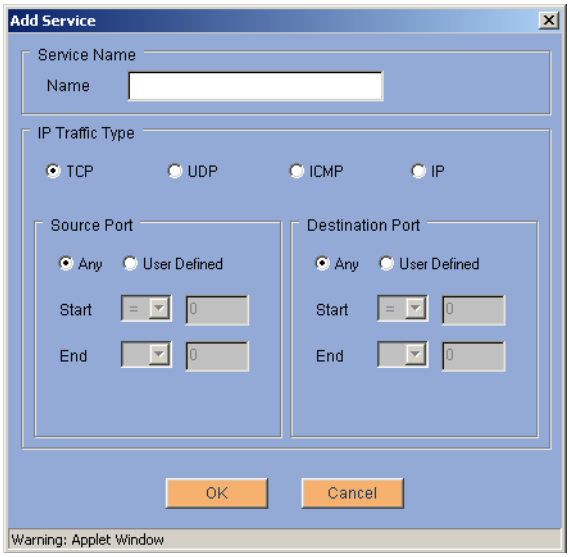


- Predefined services are read only. You can view the set up, but you cannot modify or delete any of the predefined services.
- You can add, modify, or delete user defined services.

To add a new service

1. Select the **Configure>Security>Service** property. Click **Add**, the Add Service dialog is displayed.

Figure 28: Add services screen

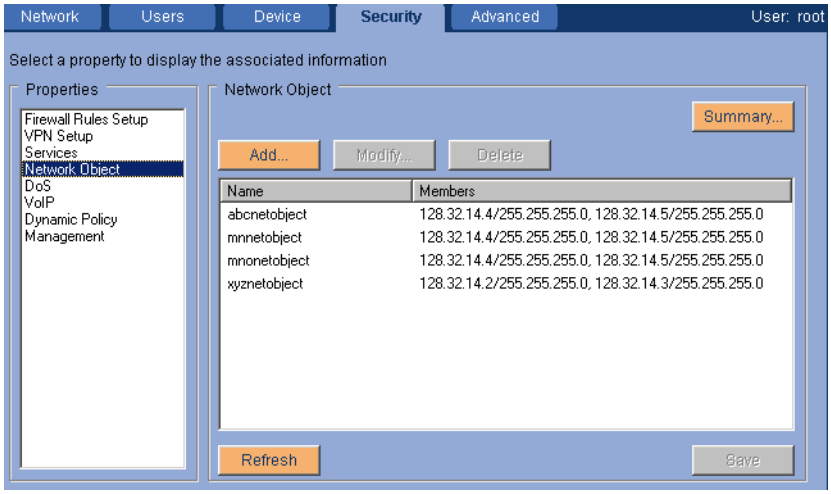


2. Enter a descriptive name for the service.
3. In the IP Traffic Types area, select the IP protocol.
   - TCP defines TCP traffic for specified source and destination ports.
   - UDP defines UDP traffic for specified source and destination ports.
   - ICMP defines types and codes for ICMP messages.
   - IP defines IP traffic for a specified Protocol ID.
4. Depending on the IP traffic type, continue to complete the fields in the dialog.
5. Click **OK**, and then click **Save**.

Network Objects

Use the Network Objects to configure the network objects of the security gateway. Double click a network object entry to view the details about the object.

Figure 29: Configure security network objects screen



To add network objects

1. Select the **Configure>Security>Network Object** property. Click **Add**, the Add Service dialog is displayed.
2. Enter the network object name, the IP address, and the network mask.
3. Click **Add**.
4. Add additional network objects, IP addresses and network masks, as required. Click **Add** after each IP address and mask that you add.
5. Click **OK**, when you finish. The property detail screen is displayed.
6. Click **Save**, to save the network objects.

To modify a network object IP addresses/mask pair

1. Select the **Configure>Security>Network Object** property. Selected the network object that you want to change. Click **Modify**.
2. Change the information for the IP address. You can add new addresses or delete addressees for the network object.
3. Click **Add** (or **Delete**) and then **OK**. The property detail screen is displayed.
4. Click **Save**.

To delete a network object from the property detail screen

1. Select the **Configure>Security>Network Object** property. Selected the network object you want to delete. Click **Delete**. The network object is removed from the list.
2. Click **Save**, to delete the route and update the static routes.

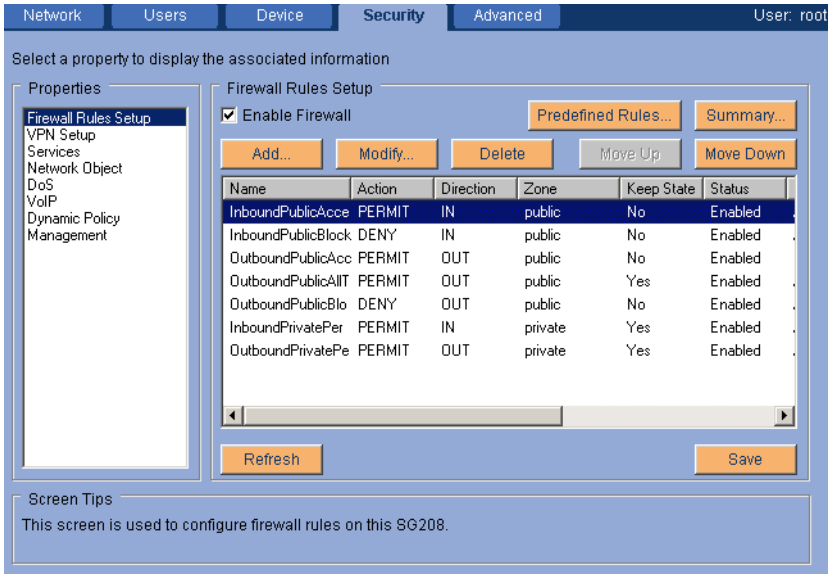
Firewall rules setup

Use the Firewall Rules Setup property to manage the firewall rules that the security gateway uses. The security gateway operating system contains a powerful stateful multi-layer inspection engine to provide extensive inspection capabilities, essential when you have a full-time connection to the Internet.

The security gateway uses a rules-based method of packet inspection, where the priority of each rule is determined by its position in the list (highest is top priority). The first match determines the fate of the packet: permit or deny. If no matching rule is found, the default action is to permit the packet.

For convenience, you can select from three predefined sets of general firewall rules or templates. Which set of rules you select depends on the interface zones that are configured and your general network requirements. If you select Add or Modify, the Firewall Wizard is launched to assist in setting up more specific rules.

Figure 30: Configure advanced firewall rules setup screen



Note:

When you finish the firewall rules setup, Avaya recommends that your corporate network administrator review the rules for compliance with the corporate security policy. The Enable Firewall check box is selected by default. If you clear Enable Firewall, the firewall rules and DoS rules are automatically disabled.

Predefined Rules

For each of the multi-interface zones, except public-backup which is configured with the same rules as public, five levels of firewall rules templates are available: none, low, medium, high, and vpn-only. When you select one of the levels, the security gateway immediately populates the Firewall Rules table with a suite of firewall rules that are based on the selection. You can then change these rules as needed to meet your specific security needs.

Note:

You can set predefined rules for zones that are not yet configured. After a zone is configured, the predefined rules take effect immediately.

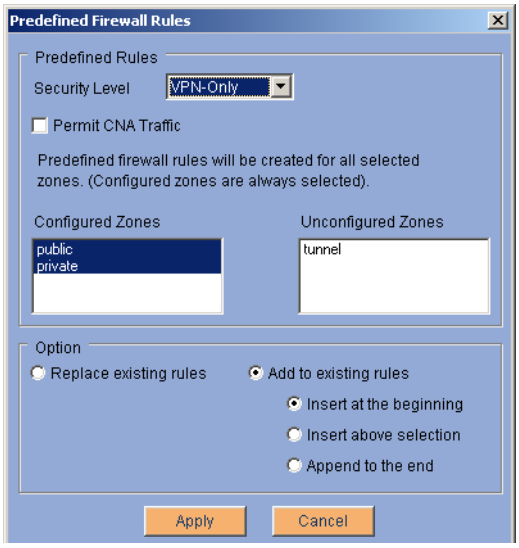
The most recently configured firewall rules replace any existing rules, regardless of whether the existing rules were configured locally or remotely. In other words, the most recent rules established are the current rules.

See Appendix A: Preconfigured firewall rules for tables that define the rules within each level, and describe the functions of the rules on each interface.

Setting predefined rules

You can set predefined rules for configured zones or for all zones at once.

Figure 31: Firewall rules option screen



1. To set predefined rules, select the **Configure>Security>Firewall Rules Setup** property. Click **Predefined Rules**.
2. The Predefined Firewall Rules dialog displays the existing firewall security level for the zones that are selected. Predefined rules are always created for all the configured zones.
3. From the **Security Level** list, select the level of firewall security.
   - Select **Low** or **Medium** when the interface zone of the security gateway is connected to a router.
   - Select **High** when the interface zone of the security gateway is connected directly to a cable modem or DSL, and is not protected by a router.
   - Select **VPN-only** when the security gateway is configured as a VPN tunnel endpoint for the public zone or semi-private zone. Only VPN traffic will be allowed trough the endpoint. All non-VPN traffic will be blocked.
4. Select the **Permit CNA Traffic** checkbox to allow CNA traffic to through the selected firewall template.
5. In the **Add options** area, select **Replace existing rules** or **Add to existing rules**, depending on whether you want to replace the existing rules or add to the existing rules. If you select Add to existing rules, you must also select where you want to place the rules in the existing rules file.
6. Click **Apply**, and then click **Save**.

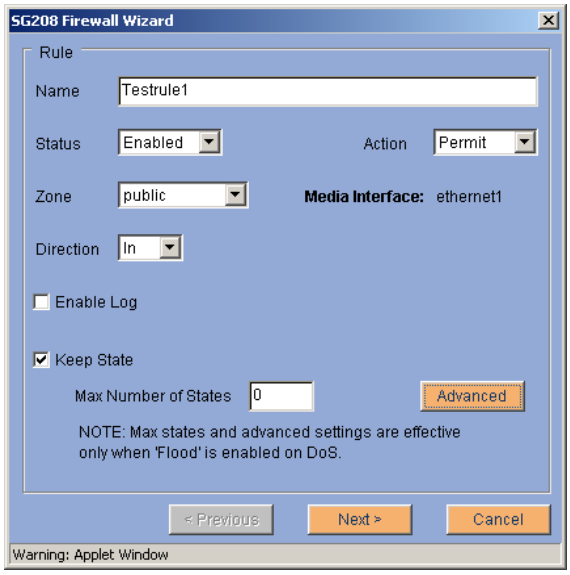
To make changes to individual rules or their order, use the Add, Modify, Delete, Move Up, or Move Down buttons as needed.

To add a new rule

Use the Firewall wizard to set up new firewall rules.

1. Select the **Configure>Security>Firewall Rule Setup** property. Click **Add**. The Firewall Wizard is launched.

Figure 32: Firewall wizard screen 1



2. In the **Name** box, enter a unique name that identifies the rule.
3. By default, the **Status** is *Enabled* and the **Action** is *Permit*. Change these if this is not the correct settings.
4. From the **Zone** list, select the zone to which you want to apply this rule. For maximum flexibility and capability, the firewall rules for the security gateway can be specified on each zone. The packets are checked against the firewall rules at the interface where they are defined.
5. in the **Direction** list, select **In** or **Out**. The direction is in respect to the security gateway.
6. If you want this rule to be logged. Select **Enable Log**. If you do not select Enable Log, this rule does not appear in the Monitor>Firewall Log display.
7. If the filter rule set for the intended traffic is also to be applied to the reply packets, select **Keep State**. This function can be applied to TCP, UDP, and ICMP packets.

   Keep State sets up a state table, with each entry set up by the sending side. Reply packets pass through a matching filter that is based on the respective state table entry. A state entry is not created for packets that are denied.

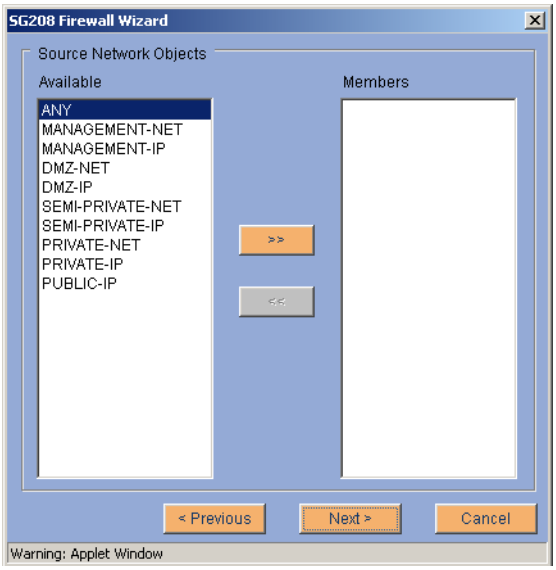
8. If you want to change the default timeout settings for the TCP state, UDP state, or ICMP state, click **Advanced**.

   Note:

   Although UDP is connectionless, if a packet is first sent out from a given port, a reply is expected in the reverse direction on the same port. **Keep State** "remembers" the port and ensures that the replying packet enters in the same port.

9. Click **Next**, to display the Source Network Objects dialog. Select the source network objects for this rule.

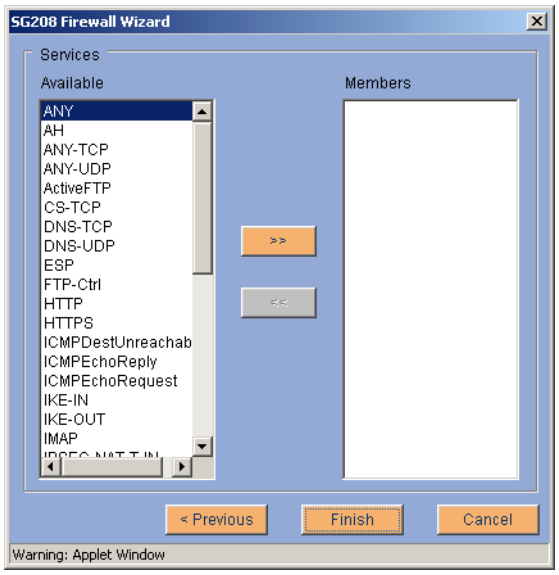
Figure 33: Firewall wizard source network objects screen



10. Click **Next** to display the Destination Network Objects dialog. Select the destination network objects for this rule.

11. Click **Next** to display the Services dialog. Select the services for this rule.

Figure 34: Firewall wizard services screen



12. Click **Finish**, to complete the set up of the firewall rules set. Click **Save**.

Setting up Firewall Rules when NAT is set up

When packets pass through zones that have both Firewall rules and NAT rules set up, NAT rules are applied before the firewall rules are applied. Depending on the type of NAT rule: static, port NAT, or redirection, either the source IP address or the destination IP address of packets are changed. When you set up your firewall rules, you need to consider the type of NAT configured, as you must create the firewall rule to filter on the translated IP address and ports not on the original address and ports.

Setting up firewall rules for FTP

All FTP protocols cannot be set up in one firewall rule. FTP protocol creates two channels, FTP control and FTP data. In addition, FTP data includes passive mode and active mode data connection. Do not add active FTP service rules that filter to the FTP control and/or passive FTP rules.

To add a new firewall rule for FTP-control or passive FTP

1. Complete Steps 1 through 7, for adding a new rule. Enter the required firewall information in the wizard.

   Note:

   Be sure to define the firewall rule at the interfaces and directions that the FTP server opens a data connection to the client. For example, if the FTP client is on the private side of the security gateway and the FTP server is on the public side of the security gateway, define the interface and direction as **Public/In** or **Private/Out**.

2. Click **Next**, to display the Source Network Objects dialog. Select FTP Client.
3. Click **Next** to display the Destination Network Objects dialog. Select the FTP Server.
4. Click **Next** to display the Services dialog. Select FTP Control and select Passive FTP.
5. Click **Finish**, to complete the set up of the firewall rules. Click **Save**.

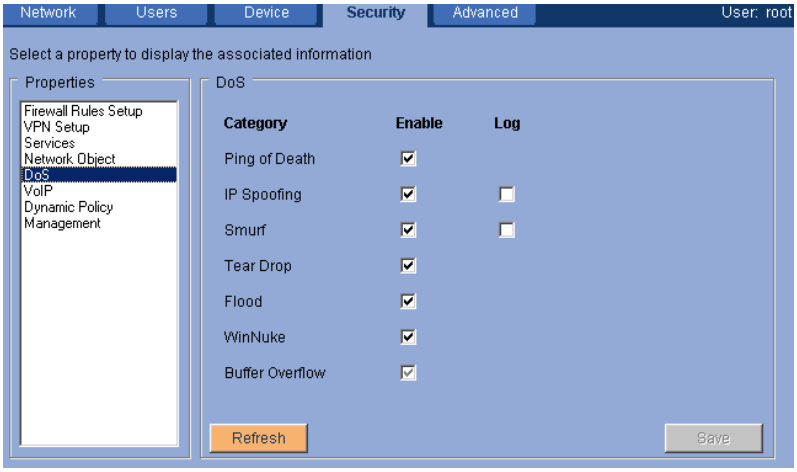
To add a new firewall rule for active FTP

1. Complete Steps 1 through 7, for adding a new rule. Enter the required firewall information in the wizard.
2. Click **Next**, to display the Source Network Objects dialog. Select FTP Server.
3. Click **Next** to display the Destination Network Objects dialog. Select the FTP Client.
4. Click **Next** to display the Services dialog. Select Active FTP.
5. Click **Finish**, to complete the set up of the firewall rules. Click **Save**.

Denial of Service (DOS)

Use the Denial of Service property to protect the security gateway from attacks by hackers.

Figure 35: Security denial of service screen



You can enable protection for the following seven areas of attack:

Ping of Death. - The ping of death sends packets with invalid lengths. When the receiving system attempts to rebuild the packets, the system crashes because the packet length exhausts the memory.

IP Spoofing. - This attack sends an IP packet with an invalid IP address. If the system accepts this IP address, the attacker appears to reside on the private side of the security gateway. The attacker is actually on the public side, and bypasses the firewall rules of the private side.

Smurf Attack. - This attack floods the system with broadcast IP packet pings. If the flood is large enough and long enough, the attacked host is unable to receive or distinguish between real traffic.

Tear Drop. - This attack sends IP fragments to the system that the receiving system cannot reassemble and the system can crash.

Flood Attack. - This attack floods the system with TCP connection requests, which exhausts the memory and the processing resources of the firewall. Flood attacks also attack the UDP ports. This attack attempts to flood the network by exhausting the available network bandwidth.

Note:

When you enable Flood Attack, you must also enable the Keep State feature in the Firewall Rules Setup in the Security tab.

WinNuke Attack. - This attack attempts to completely disable networking on computers that are running Windows 95 or Windows NT. This attack can be swift and crippling because it uses common Microsoft NetBIOS services. WinNuke attacks ports 135 to port 139 on platforms that are based on Windows 95 and Windows NT.

Buffer Overflow. - This attack overflows the internal buffers of the application by sending more traffic than the buffers can process. This attack can contain a program at the end of a packet which can run and attack the system.

To select or deselect DOS categories

1. To set DOS rules, select the **Configure>Security>DOS** property. Select the rules that should be enabled and select to log details about attack attempts, if the log function is available.
2. Click **Save**.

Voice over IP

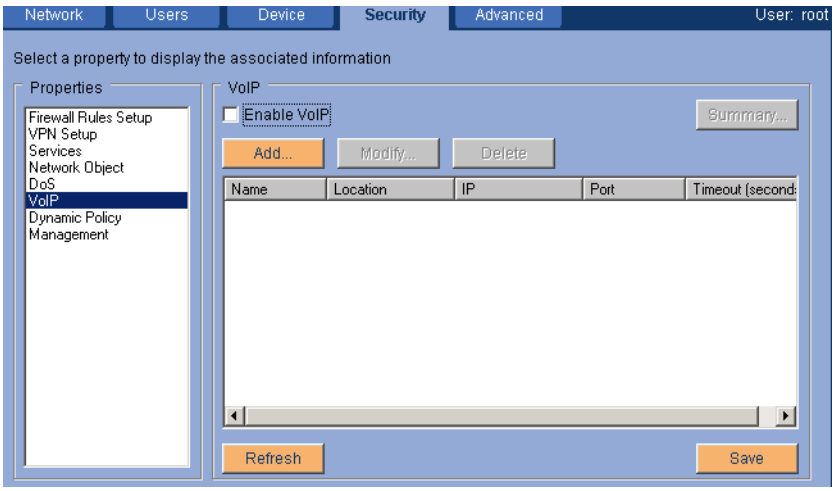
Configure>Security>VoIP property allows you to enable or disable the Voice over IP (VoIP) function. Configuration parameters include the gatekeeper IP address, location of the gatekeeper with respect to the firewall, registration, authentication and status protocol port and time-out setting.

VoIP feature description

This feature enhances the Security Gateway (SG) with the capability to NAT and/or filter the H.323 VoIP packets transparently. The security gateway accepts H.323 packets, translates the IP addresses of H.323 VoIP packets and/or allows the appropriate H.323 VoIP packets through the firewall, opens the appropriate ports, forwards the packet to the correct destination, and closes those ports upon completion of the VoIP call.

When an H.323 packet is received by the SG, the SG opens only those ports necessary to allow subsequent packets of the communication to pass through the firewall (a.k.a. pinholes), and be forwarded to the correct destination such as the gatekeeper or an IP trunk endpoint.

Figure 36: Configure security VoIP property screen



Using the Gatekeeper Routed Call Model

The Gatekeeper Routed call model should be used when there is an SG in the network path between IP endpoints (e.g. IP hard phones and IP soft phones) and the Gatekeeper with which those IP endpoints register and 1) either the IP endpoints or the Gatekeeper is being NATed by the SG or 2) the SG's Firewall function is enabled.

When using the Gatekeeper Routed Call Model rule, configure the following:

- Service Port. The port to which the IP endpoints will send Registration/Access/Status (RAS) messages.
- Source Endpoints Zone. The zone where the IP endpoints are located with respect to the SG (e.g. "private" when the IP endpoints are on private side of the SG).
- Source Endpoints Network Objects. The IP networks that define the IP address space of the IP endpoints
- Gatekeeper Zone. The zone where the gatekeeper is located with respect to the SG (e.g. "public" when the Gatekeeper is on the public side of the SG).
- Gatekeeper IP address. The Gatekeeper's configured IP address.

The Proxy IP and Proxy Port in the "Add Gatekeeper" dialog are used typically when the Gatekeeper is on the private side of the SG and is getting NATed by the SG. In that case, the Proxy IP and Proxy Port would be configured to be the IP address and port by which the Gatekeeper is known to IP endpoints wanting to register with that Gatekeeper. If the Gatekeeper IP address is not being NATed by the SG, the Proxy IP and Proxy Port do not need to be configured.

Using the IP Trunking Call Model

The IP Trunking call model should be used when there is an IP Trunk configured between Gatekeepers at separate locations and the call signaling messages (i.e. H.225 and Q.931 packets) between those Gatekeepers is NATed by the SG.

When using the IP Trunking Call Model rule, configure the following:

- Service Port. The port to which the Gatekeeper sends call-signaling messages.
- Source Trunk Zone. The zone where the Gatekeeper is located with respect to the SG (e.g. “private” when the Gatekeeper is on private side of the SG).
- Source Trunk Network Objects. The IP networks that define the IP address space of the Gatekeeper.
- Destination Trunk Zone. The zone where the Gatekeeper receiving call-signaling messages is located with respect to the SG (e.g. “public” when the receiving Gatekeeper is on the public side of the SG).
- Trunk IP. The receiving Gatekeeper’s configured IP address.

The Proxy IP and Proxy Port in the “Add Destination Trunk” dialog are used typically when the Gatekeeper receiving call-signaling messages is on the private side of the SG and is getting NATed by the SG. In that case, the Proxy IP and Proxy Port would be configured to be the IP address and port by which the receiving Gatekeeper is known to the Gatekeeper wanting to send call-signaling messages. If the receiving Gatekeeper is not being NATed by the SG, the Proxy IP and Proxy Port should not be configured.

Using the LRQ Required checkbox of the IP Trunking Call Model

When a Gatekeeper of an IP Trunk is not pre-configured with translations to map phone extensions to Gatekeepers, but rather uses Location Request (LRQ) and Location Confirm (LCF) messages to determine the Gatekeeper to which call-signaling messages will be sent, check the LRQ Required checkbox. This will direct the SG to translate the IP addresses and ports embedded within LRQ messages sent by the Gatekeeper so that the receiver of those LRQ messages will respond to the NATed address.

The LRQ functionality is available on Security Gateways running VPNos 4.6 and higher.

Note:

Firewall openings for any other vender-specific packets will not be affected. For example, trunk endpoints running Avaya MV1.2 that send pings to the endpoint at the other end of trunk to determine the status of the CLAN. If the ping response do not come back, the sig group and trunk group are taken out of service. In this case, confirm that appropriate rules are setup so vendor-specific packets are not blocked by the firewall. Such rules can be configured easily on the security gateway using the firewall wizard on web interface or VPNmanager.

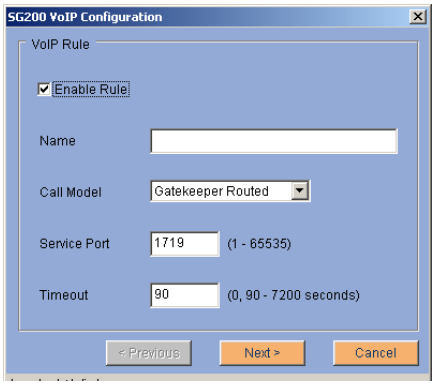
Note:

Global VoIP capability can be enabled or disabled by selecting the Enable VoIP checkbox.

To enable VoIP and add gatekeeper settings

1. From the Configure>Security>VoIP property, select **Enable VoIP**.
2. Click **Add**. The Add Gatekeeper Settings dialog is displayed.

Figure 37: Add gatekeeper setting for VoIP



3. In the Name field, enter a descriptive, unique name to identify the gatekeeper. Once the name is saved, the name cannot be changed.
4. In the Call Model field, select **gatekeeper routed** from the drop-down menu.
5. In the Service Port field, enter the specific H.323 protocol port. The default is 1719.
6. In the Timeout field, specify the idle timeout for the connection. Timeout is the number of seconds that the security gateway allows for inactivity on the connection. If the inactivity continues beyond the specified timeout, the connection is closed. The default is 90 seconds. Click **Next**.
7. In the Zone field, specify the location of the zone. Select public if the gatekeeper is outside the firewall. Select private if the gatekeeper is behind the firewall.
8. In the Media Interface field, specify the interface port.
9. In the Network Objects field, specify the Member Network Object. Click **Next**.
10. In the Gatekeeper dialog, click **Add**.
11. In the IP field, specify the Gatekeeper IP address.
12. In the Proxy IP field, specify the public IP address that is being shared.
13. In the Proxy Port field, specify the H.225/RAS protocol port. The default is 1719.
14. Click **OK**.
15. Click **Finish**.

H.323 Voice over IP Trunking

The security gateway does not open a range of ports when a H.323 VoIP packet is received. When the security gateway receives an H.323 VoIP packet, the security gateway opens only the necessary port to allow the packet to pass through the firewall and routed to the destination security gateway. In order for the H.323 VoIP packet to be routed and received successfully, the security gateways at each end must have the Enable VoIP property selected and the Call Model configured as IP Trunking.

Note:

Firewall openings for any other vender-specific packets will not be affected. For example, trunk endpoints running Avaya MV1.2 that send pings to the endpoint at the other end of trunk to determine the status of the CLAN. If the ping response do not come back, the sig group and trunk group are taken out of service. In this case, confirm that appropriate rules are setup so vendor-specific packets are not blocked by the firewall. Such rules can be configured easily on the security gateway using the firewall wizard on web interface or VPNmanager.

Beginning with VPNos Feature Pack 4.3, use the VoIP property to configure the IP trunking properties. You can add, modify, or delete IP trunking configuration.

When adding IP trunking, include the IP Trunk name, call model selection, service port, timeout connection in seconds, source zone, and destination zone.

Note:

Global VoIP capability can be enabled or disabled by selecting the Enable VoIP checkbox.

To enable VoIP and add IP Trunking:

1. From the Configure>Security>VoIP property, select **Enable VoIP**.
2. In the Name field, enter a descriptive, unique name to identify the IP trunk.
3. In the Call Model field, select IP Trunking from the drop-down menu.
4. In the Service Port field, enter the specific H.323 protocol port. The default is 1720.
5. In the Timeout field, specify the idle timeout for the connection. Timeout is the number of seconds that the security gateway allows for inactivity on the connection. If the inactivity continues beyond the specified timeout, the connection is closed. The default is 90 seconds. Click **Next**.
6. In the Zone field, specify the location of the zone. Select public if the trunk is outside the firewall. Select private if the trunk is behind the firewall.
7. In the Media Interface field, specify the interface port.
8. In the Network Objects field, specify the Source Trunk Network Object.
9. Click **Next**. The Destination Trunk dialog appears.

10. In the Zone field, specify the location of the zone. Select public if the trunk is outside the firewall. Select private if the trunk is behind the firewall.
11. In the Media Interface field, specify the interface port.
12. Click **Add**. The Add Destination Trunk dialog appears.
13. In the Trunk IP field, specify the IP address.
14. In the Proxy IP field, specify the public IP address that is being shared.
15. In the Proxy Port field, specify the public port of the IP address that is being shared.
16. Click **OK**.
17. Click **Finish**.

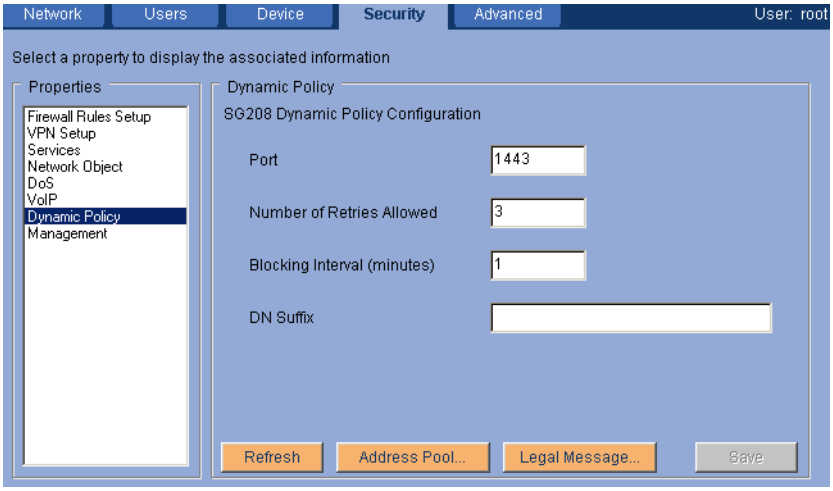
Dynamic policy

Use the Dynamic Policy property to configure the security gateway's dynamic policy for VPNremote Client users. The dynamic policy establishes the following:

- The port number. The default is 1443.
- The number of times a user can enter an incorrect password before log on fails. The default is 3.
- The number of minutes that a user is locked out after the password fails. The default is 1 minute.
- The domain name suffix, including the organizational unit and the organization.

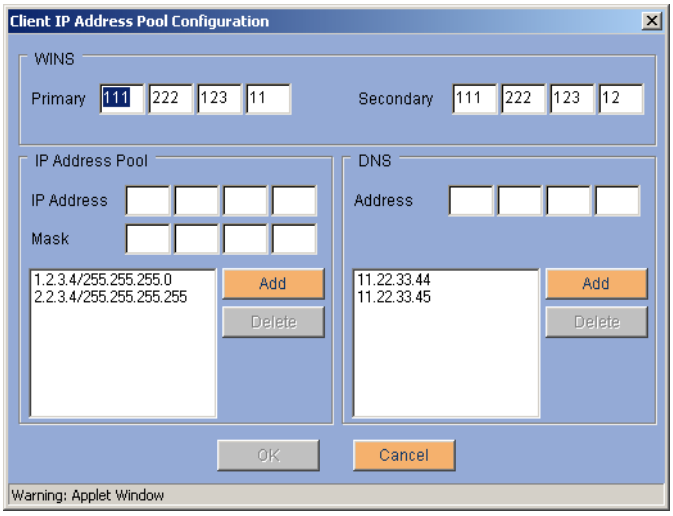
In addition, dynamic policy is used to configure the address pool for the security gateway and the legal message displayed.

Figure 38: Security dynamic policy property screen



Client IP Address Pool Configuration - The security gateway can be configured with multiple pools. When selecting a list of source addresses to pool, choose ranges that are not used by the destination network. The IP addresses or IP address range used for the IP address pool must be unique with regard to the destination network. If not, the destination network cannot route responses back to the security gateway.

Figure 39: Dynamic policy client IP address pool configuration



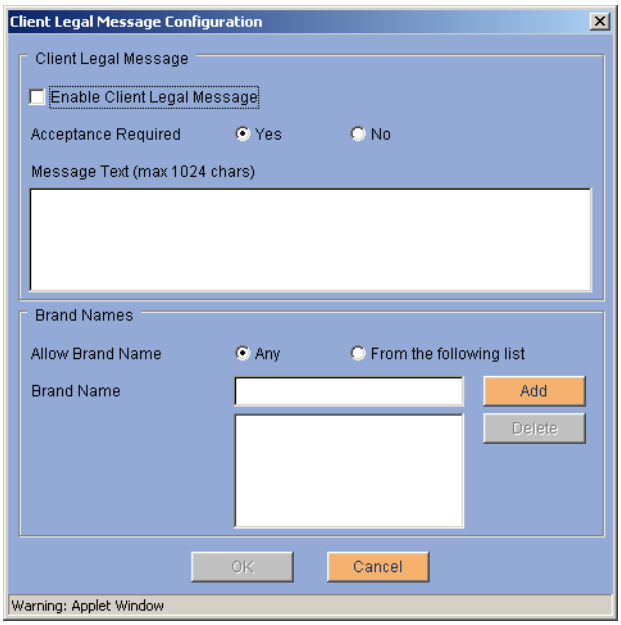
WINS. - When remote users log on, the WINS address is downloaded for host name resolution.

IP Address Pool. - You can configure a range of source IP addresses in the security gateway. For VPNos 3.X, when an inbound packet from a VPNremote Client is received, the security gateway swaps the source address with one from the pool. For VPNos 4.X, when a remote user connects to the security gateway an IP address is downloaded from the IP address pool. The security gateway uses the downloaded IP address for the virtual interface. All secure traffic from the remote user will use the downloaded IP address as the source. A security gateway using tunnel NAT with the Downloaded IP Address from Pool and Apply Tunnel NAT option selected also obtains IP addresses from the IP address pool.

When the security gateway recognizes an outbound packet as a pooled address, the security gateway changes the destination address to the remote client's address.

DNS. - The DNS address entered here is downloaded by remote users for their DNS IP address.

Client Legal Message Configuration. - You can configure a message that remote users see every time they log in. This message can be a legal message about company policy for using the network or any other type of message to communicate information when remote users log in. This message can be configured so that remote users are required to accept the message before the log in is complete.

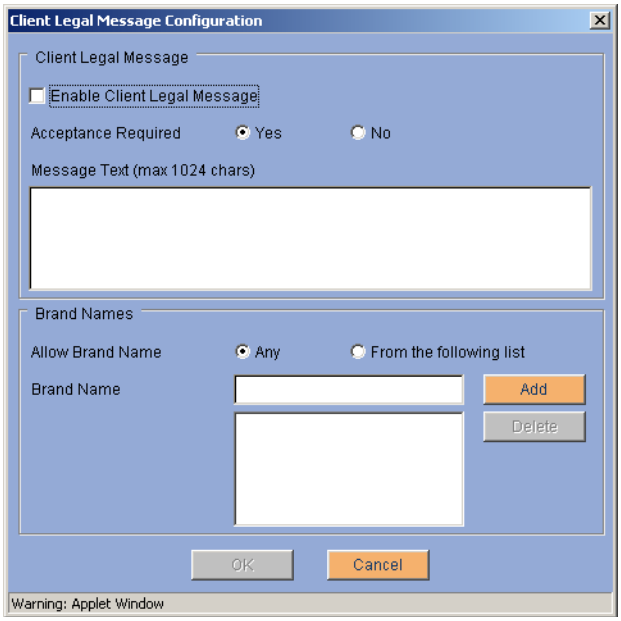


Brand Names. - You can specifying the brand name used for VPNremote Client. The brand name is the name that the VPNremote Client is licensed under. For example, a service provide can specify that their name be displayed instead of Avaya when a user uses the VPNremote Client application. The administrator can allow any brand name or restrict access by specifying a brand name. Note that this brand name must be specified in the VPNmanager and in the Avaya VPNremote Client for this feature to work properly. The default is allow any brand name.

To configure Dynamic Policy

1. Select the **Configure>Security>Dynamic Policy** property. The dynamic policy displayed is the security gateway default configuration for port, number of retires allowed, blocking interval in minutes and the domain suffix. Make any changes as required for your company dynamic policy
2. Click **Address Pool**. The Client IP Address Pool Configuration dialog is displayed. Configure the following
   a. In the **IP Address Pool** area enter the range of IP addresses on the security gateway that can be substituted for addresses received from a VPNremote Client.
   b. In the **DNS** area enter the IP addresses of the DNS servers for your network.
3. Click **OK**. The Dynamic Policy screen is displayed. If you are configuring a legal message, click **Legal Message**, otherwise, click **Save**.
4. (Optional) If you configure a legal message, select **Enable Client Legal Message** on the **Client Legal Message** dialog.

Figure 40: Client legal message dialog



5. For **Acceptance Required**, select **Yes** to require the remote user to accept the message before log on is authenticated. Select **No**, if the message is displayed, but the remote user is not required to accept the message to authenticate to the security gateway. The default is No.
6. In the message box, type the message that should be displayed. The message can be up to 1024 characters long.

7. In the **Brand Names** area, if specific brand names should be allowed, select **From the following list**. Enter the brand name and click **Add**.
8. Click **OK** and then **Save**.

Management

Within a security gateway, the following users can configure and monitor the security gateway:

- The *root user* has read and write privileges. This is the default administrator and is configured at the factory with a default password. When the administrator logs in to the security gateway for the first time, the administrator is prompted to change the default password. The root user name cannot be modified or deleted.

  The root user has full privileges on the security gateway to configure and maintain the security gateway network and user configuration, device security, and VoIP gatekeeper configuration.

- The *monitor user* has read-only permissions. The monitor user name cannot be modified or deleted. Only the password can be changed. When the monitor user logs in to the security gateway for the first time, the monitor user is prompted to change the default password.

  The monitor user can view the following properties: Inspect, Web Interface Access, and Monitor.

  The Inspect property includes interfaces, software, and general security gateway information.

  The Web Interface Access property is located under the *Configure>Security>Management* property and includes web management and centralized management.

  The Monitor property includes VPN, network, and log information.

- The *superuser* is enabled for centralized management from the Web interface *Configure>Security>Management* property. The user ID and password is entered from the VPNmanager console for authentication before VPNmanager is used to make configuration changes on the security gateway. VPNmanager has full read and write privileges to the security gateway, once it is authenticated by the security gateway.

Web interface management

The root user or monitor user can access the Web interface remotely when the *Permit Web Interface access via public zone* box is selected. When this box is selected, you can access the Web interface through the public port. When this box is not selected, you can access the Web interface of the security gateway only from the private side.

When the *Permit Web Interface access via public zone* box is enabled, the remote administrator directs his or her browser to the IP address of the public port. When a connection with the security gateway is established, the login screen is displayed.

In addition to remote administrator access, this can be used for technical support.

The root user and the monitor user can use the *Password* function on the Web interface main page to change their passwords. The password can be from 6 to 31 alphanumeric characters.

Centralized management

By default, you can configure and manage the security gateways remotely from a central location with the Avaya VPNmanager® application. For more information regarding the VPNmanager to configure the security gateways, see the VPNmanager Configuration Guide.

The centralized management feature significantly enhances the administrators ability to manage remote security gateways. To utilize the centralized management functionality with dynamically assigned IP addresses, the security gateways must be configured with the IP address, DNS name, and the port number of the VPNmanager policy server that the security gateway will register.

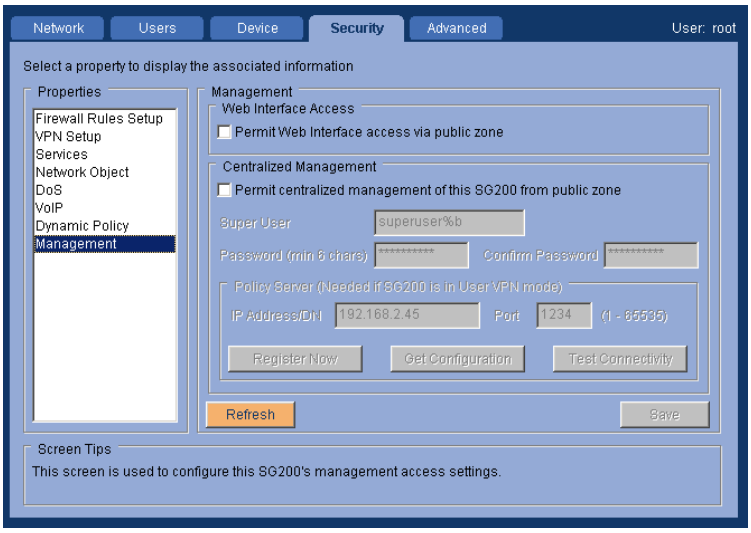
Once the SGs are configured for centralized management with dynamically assigned public IP addresses (DHCP or PPPoE), the SGs will register their IP addresses with their configured VPNmanager policy server. In turn, the VPNmanager policy server publishes the IP addresses and the VPNmanager assigned device name to the DNS server.

To configure centralized management with dynamically addressed devices:

1. Select the **Configure>Security>Management** property. The Web interface and centralized management screen is displayed.
2. In the **Centralized Management** area, select the **Permit centralized management** checkbox.
3. Enter the super user name, password, and password confirmation.
4. The *super user* is enabled for centralized management from the Web interface. The super user ID and password are entered from the VPNmanager console for authentication before VPNmanager is used to make configuration changes on the security gateway. VPNmanager has full read and write privileges to the security gateway, once it is authenticated by the security gateway.

5. In the **Policy Server** area, enter the SGs assigned IP addresses or the DNS name, and the port number of the VPNmanager policy server that the security gateway will register.
6. Click the **Register Now** button to register the SG with the configured VPNmanager policy server.
7. Click the **Get Configuration** button to retrieve the policy server configuration to update the current SG configuration.
8. Click the **Test Connectivity** button to test the connectivity between the SG and the VPNmanager policy server.
9. Click **Save**.

Figure 41: Configure security management screen



Chapter 6: Monitoring the security gateway

This chapter explains how to view the security gateway configuration information with the following Web interface functions:

- Inspect
- Monitor
- Text Interface

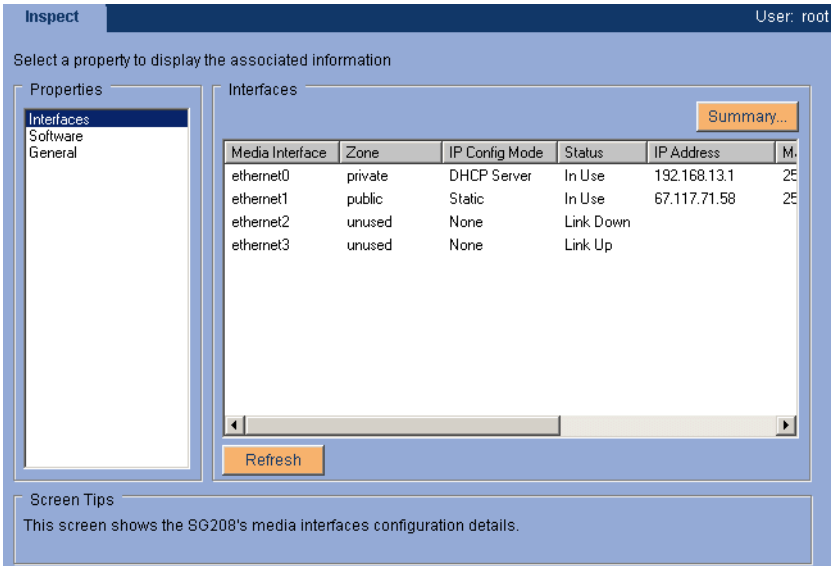
Inspecting the security gateway

Use the Inspect function to view the current settings of the security gateway. Inspect is a read-only function. To change any of the settings use the Configure function.

The following properties can be viewed from Inspect, Figure 42:

- **Interfaces**. Select *Interfaces* to view the media interface configuration for the security gateway, including the zones that are configured, the IP configuration mode, and addressing.
- **Software**. Select *Software* to view the security gateway model, the serial number, and the VPNos software and boot code versions on the security gateway.
- **General**. Select *General* to view the configured date, time, and time zone. This screen also shows the number of days, hours, and minutes that the security gateway has been running, the memory that the security gateway used, and the CPU use.

Figure 42: Inspect interfaces property



Monitoring the security gateway

Use the Monitor function for routine observation of your connection activity and network traffic. Monitoring and logging functions can be configured to help ensure the integrity of your network security. With the Monitor function, you can determine when security attacks or compromises occur.

The following subfunctions can be monitored:

- VPNs
- Network
- Logs

Monitoring VPNs

Use the Monitor>VPNs subfunction to view the connections and traffic on your VPNs. Three VPN properties are monitored: IPSec Security Associations, IKE Security Associations, and VPN Statistics.

IPSec SA

The *Monitor>VPNs>IPsecSA* property displays IPSec Security Association (SA) information. Each security association provides live information for a secure connection. When VPN Setup was used to set up the VPN, IPSec was configured. See VPN setup in Chapter 5: Establishing security.

IKE SA

The *Monitor>VPNs>IKE SA* property displays a list of IKE Security Associations information. Each security association provides live information for a secure connection. When VPN Setup was used to set up the VPN, IKE was configured.

VPN Statistics

The *Monitor>VPNs>VPN Statistics* property displays a list of the VPN packets sent and received by this security gateway.

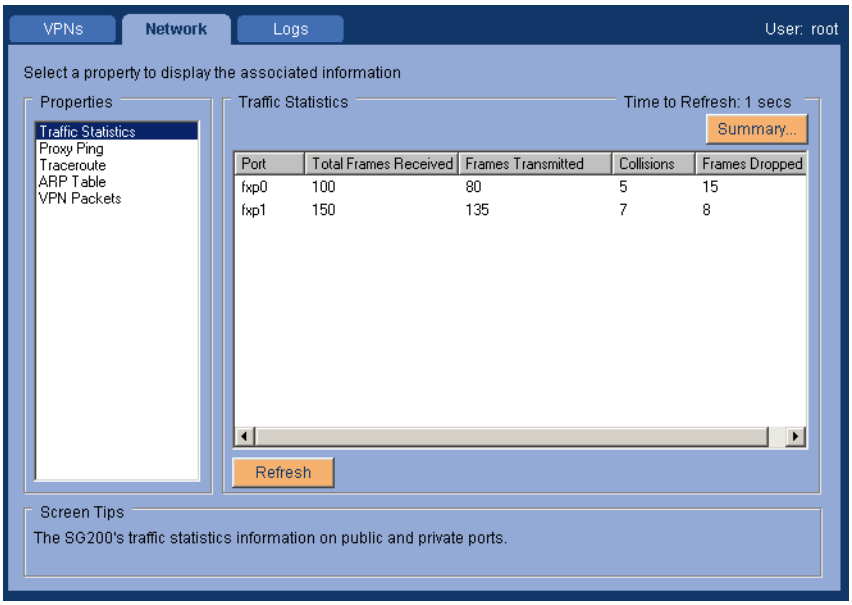
Monitoring the Network

Use the Monitor>Network subfunction to monitor the connections and the traffic on your network. Five properties are monitored: Traffic Statistics, Proxy Ping, Traceroute, ARP Table, and VPN Packets. Proxy Ping is provided as a convenience to verify that the security gateway is connected to target IP addresses.

Traffic Statistics

The *Monitor>Network>Traffic Statistics,* Figure 43*,* displays a list of traffic statistics on the security gateway's public and private ports of the security gateway. These statistics are collected in real time.

Figure 43: Monitor network traffic statistics screen

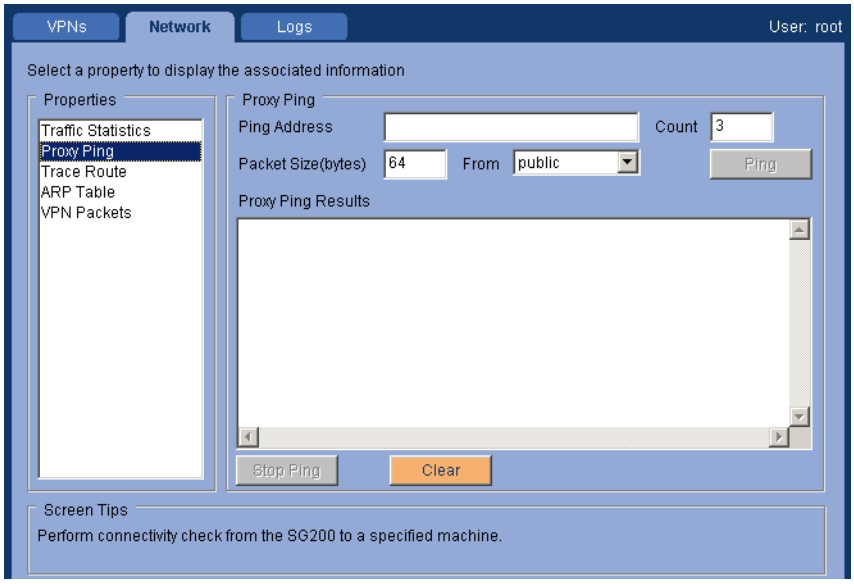


Proxy Ping

The *Monitor>Network>Proxy Ping* property, Figure 44, allows you to perform a connectivity check from the security gateway to a specified address.

Packet size and count can be specified for the ping. Results are displayed in the Proxy Ping Results window.

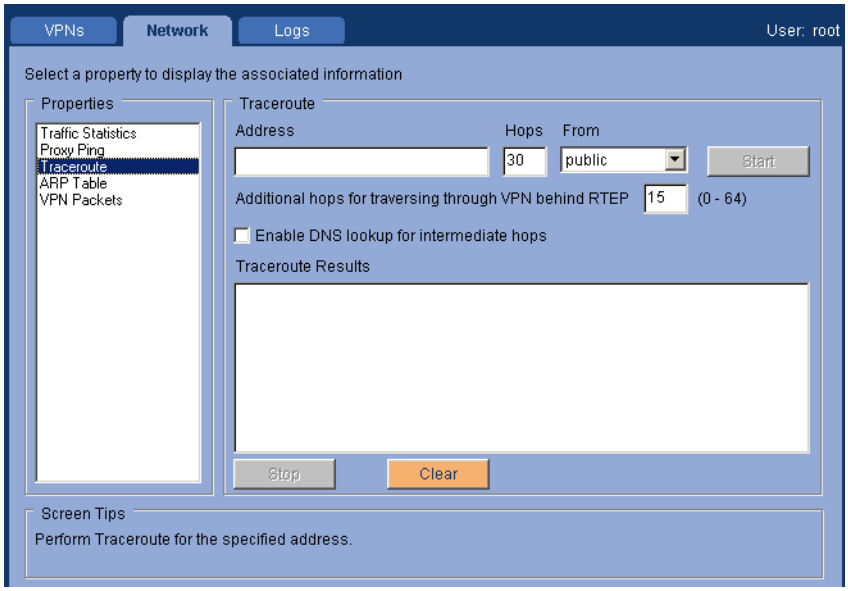
Figure 44: Monitor network proxy ping screen



Traceroute

The *Monitor>Network>Traceroute* property, Figure 45, is used to capture and display information about the route through which UDP probe packets pass from source to destination. Enter the destination IP address in the Address field to start the trace. Use the Hops field to set the upper limit on the maximum time-to-live of the probe packets from source to destination.

Figure 45: Monitor network traceroute screen

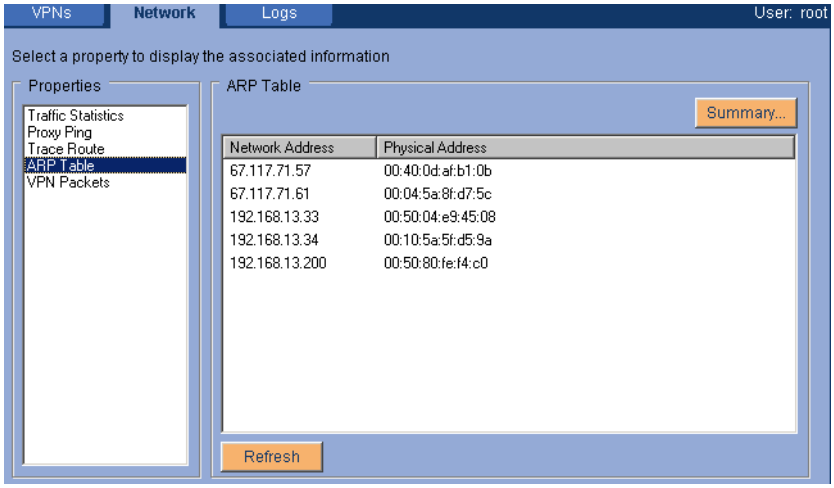


Use the trace route property when you need more information than the Ping function provides. The Trace Route Results list displays the hop count, IP address, and the time that is required for the packet to reach the address.

ARP Table

The *Monitor>Network>ARP Table* property displays data from ARP table of the security gateway. This data includes port, network address, and physical address.

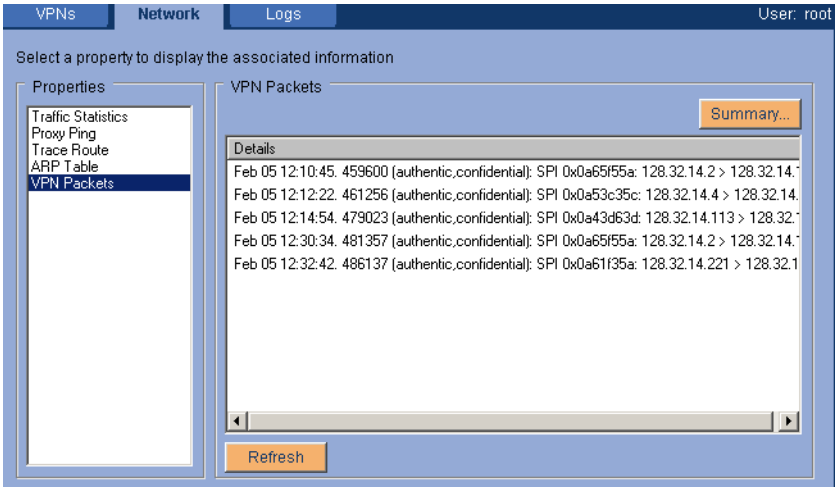
Figure 46: Monitor network ARP table screen



VPN Packets

The *Monitor>Network>VPN Packets* property displays the VPN packet header information for tunnel traffic before encryption and after decryption.

Figure 47: Monitor network VPN packets screen



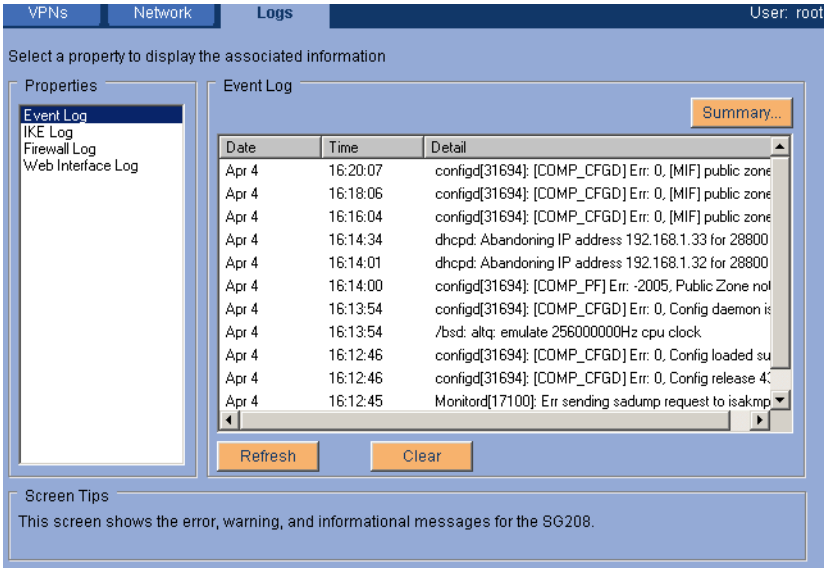
Logs

Use the Monitor>Logs subfunction to display the four categories of logs that are maintained in the security gateway: Event, IKE, Firewall, and Web interface. These logs are maintained in circular buffers of a fixed size. When a buffer is filled, wraparound occurs.

Event log

The *Monitor>Logs>Event Log* property displays a list of security gateway events from the security gateway Event Log. The log displays the date, the time, and details of the event. The Event Log buffer holds about 150 messages.

Figure 48: Monitor event log screen



IKE log

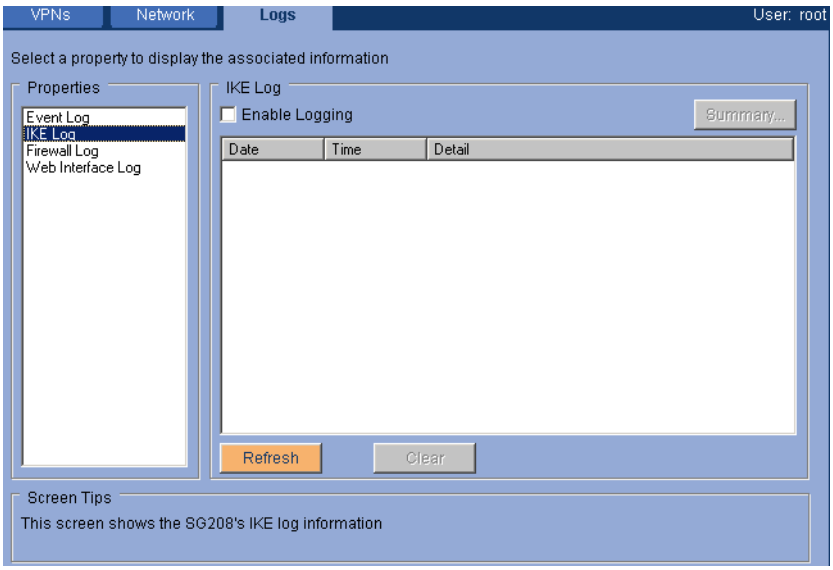
The *Monitor>Logs>IKE Log* property displays the IKE data from the security gateway IKE Log. The log displays the date, the time, and the details of the event. The IKE Log buffer holds 150 messages before wraparound occurs.

Note that you must select *Enable Logging* for IKE logging to occur.

Important:

Activation of this logging facility can reduce the performance of the security gateway. Avaya recommends that you activate IKE logging only when needed.

Figure 49: Monitor IKE log screen



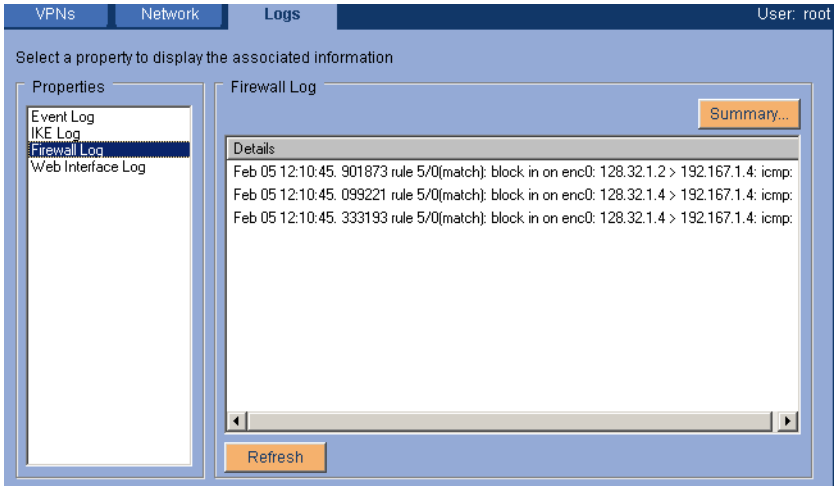
Firewall Log

The *Monitor>Logs>Firewall Log* property displays a list of any attempt to break into your protected devices from the public side of the security gateway. This screen displays a list of all firewall rule hits that have the logging option enabled.

Important:

You must enable the logging option for each firewall rule that you want to monitor. Logging is enabled through the Configure/Security/Firewall rules setup wizard.

Figure 50: Monitor firewall log screen



Web interface log

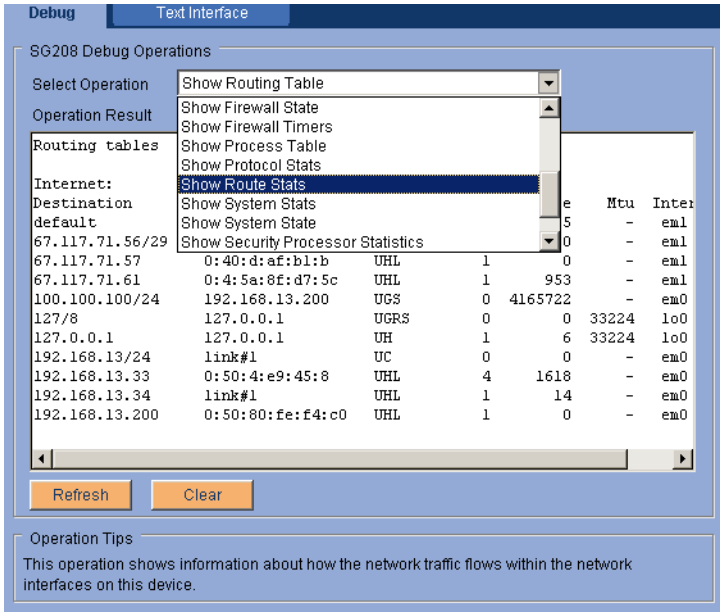
The *Monitor>Logs>Web Interface Log* property displays a list of current events from the security gateway Web interface Log. The log displays the date, the time, the operation performed, and the result of that operation. The Web interface Log buffer holds approximately 500 messages.

Note that you must select *Enable Logging* for Web interface logging to occur. The default is for logging to be off.

Debug

Debug is a subfunction of Text Interface. The Text Interface>Debug subfunction provides convenient access to several facilities that you can use to troubleshoot common configuration problems. This subfunction is available to the root user only.

Figure 51: Debug screen



The following operations show internal network-related information for the security gateway. These operations are provided to help you diagnose configuration problems and network problems.

Generate Diagnostic Report - shows system diagnostic report.

Routing Table - shows information about how the network traffic flows within the network interfaces in the security gateway.

Flow Table - shows secure traffic packet flow information for the VPN.

SA Table - shows secure traffic security association information for the VPN.

Interface Table - shows MAC address information for all network interfaces in the security gateway.

Socket Table - shows the active connection (UDP and TCP) state table of the security gateway. Each entry contains IP address and port information for the connection.

Network Memory - shows network memory usage information, and any errors that occur in network memory allocation.

System Memory - shows the memory table for the kernel processes that are running in the security gateway.

Interrupt Stats - shows the interrupt counters that the security gateway handles.

Firewall State - shows information about each firewall rule configured in the security gateway.

Firewall Timers - shows firewall timer information for the various IP protocols.

Process Table - shows information about all user processes that are currently running in the security gateway.

Protocol Stats - shows information about the network traffic that the security gateway handles. Information is presented according to the type of protocol.

Route Stats - shows network routing table statistics.

System Stats - shows statistics about system resources.

System State - shows a snapshot of all system resources.

Security Processor Statistics - shows the statistics for the Hifn chip. These statistics are only applicable for SG200, SG203, and SG208.

Flush Configuration - deletes existing Firewall, VPN, QoS, Failover, SNMP, DNS Relay, NAT, VoIP, Remote Access, and Static Routes configurations on the security gateway. The settings are returned to the factory default. Caution! Use this operation only as a last resort to recover lost administrator connectivity with the security gateway.

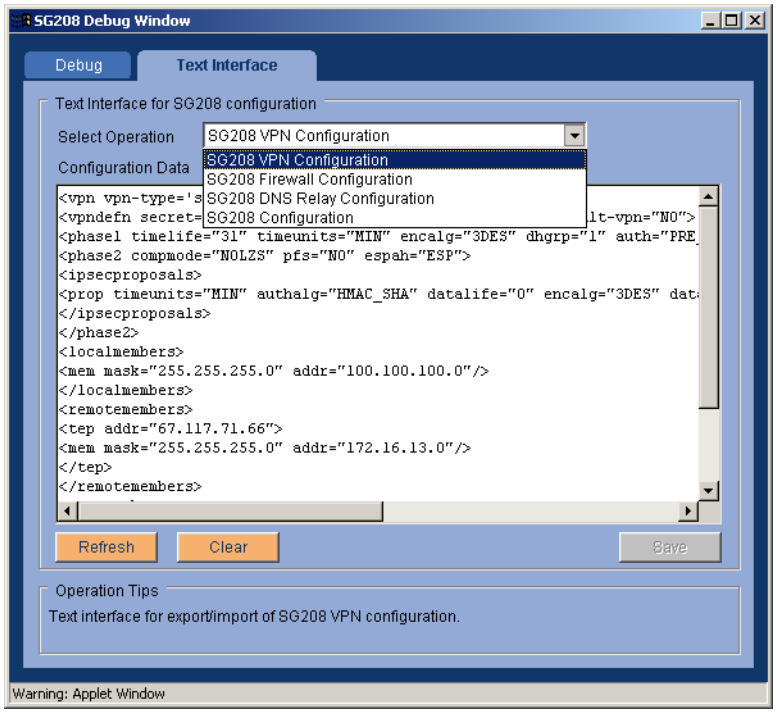
Reset Configuration to Factory Defaults - deletes all existing configurations except the license. All configuration parameters are returned to the factory default configuration except for the license parameter. Unless the security gateway device is in an inconsistent state (that is, if the configd process is not running) the license parameter is also returned to the factory default setting. *Caution*! Use this operation only as a last resort to recover lost administrator connectivity with the security gateway.

Text interface

The Text Interface function uses a text file as a convenient way to export and import the configuration of a security gateway. Use the Text Interface to copy the configuration of one security gateway and duplicate the configuration on another security gateway of the same model.

You can use Text Interface to import and export the following operations: VPN configuration, firewall configuration, DNS relay configuration, and security gateway configuration.

Figure 52: Text interface screen



To export configuration data:

1. From the Text Inteface>Text Interface tab, select the operation that you want to export.
2. From the Configuration Data area, select all of the text for the configuration by pressing Ctl+Alt.
3. Press **Control+C**, to copy the text.
4. Open a text editor program.
5. Press **Control+V**, to paste the copied configuration into a text editor file.
6. Save the text editor file that contains the copied configuration on a diskette, or other form of storage media.

To Import configuration data

1. From the **Text Inteface>Text Interface** tab, select the operation for which you want to import a new configuration.
2. Click **Clear**, to delete the configuration in the Configuration Data area.
3. Open the text file that contains the configuration that you want to import and select the content. Press **Control+C**, to copy the text.

4. Go back to the **Text Interface** tab screen, press **Control+V**, to paste the copied configuration into the Configuration Data area.
5. Click **Save** and then **OK**.

Chapter 7: Using advanced features

This chapter explains the advanced function for the security gateway. The following can be configured for the security gateway.

- **DNS relay configuration**. Displays the configured definitions of the domain name service (DNS) resolution questions and the location where the resolution requests are forwarded. Use this property to add, modify, or delete DNS relay configuration and static DNS servers.
- **Failover**. Displays the configured failover settings. Use this property to add or delete IP addresses for tunnel endpoints (TEP) and to configure failover reconnect. This property is also used to configure Traceroute Criteria settings.
- **Keep Alive**. Displays the configured keep alive settings. Use this property to add or delete configured hosts and keep alive intervals. This property is also used to configure traceroute criteria.
- **License**. Displays general license information. Use the License Management feature to add new licenses.
- **SNMP**. Displays the Simple Network Management Protocol (SNMP) target settings. Use the SNMP property to modify the SNMP settings.
- **QoS Policies**. Displays the configured classes of quality of service (QoS) policies. Use this property to add, modify, and delete QoS policies.
- **QoS Mapping**. Displays the configure zones for the quality of service policies. Use this property to add, modify, and delete QoS mapping zones.
- **NAT Traversal**. Displays the enabled NAT traversal property and the configured keep alive timer interval. Use this property to enable the security gateway or remote security gateway behind NAT device to successfully pass VPN traffic.
- **Converged Network Analyzer (CNA) Test Plug**. Displays the CNA test plug settings. Use this property to enable CNA test plug, and to configure real-time monitoring of the protected network.
- **High Availability**. Displays the configured high availability (HA) settings. Use this property to enable HA, and to modify the HA virtual IP address configuration.
- **Path MTU**. Displays the path MTU settings. Use this property to enable path MTU discovery, set path MTU timeout, and to set the fragmentation control for encapsulated VPN traffic.

DNS relay configuration

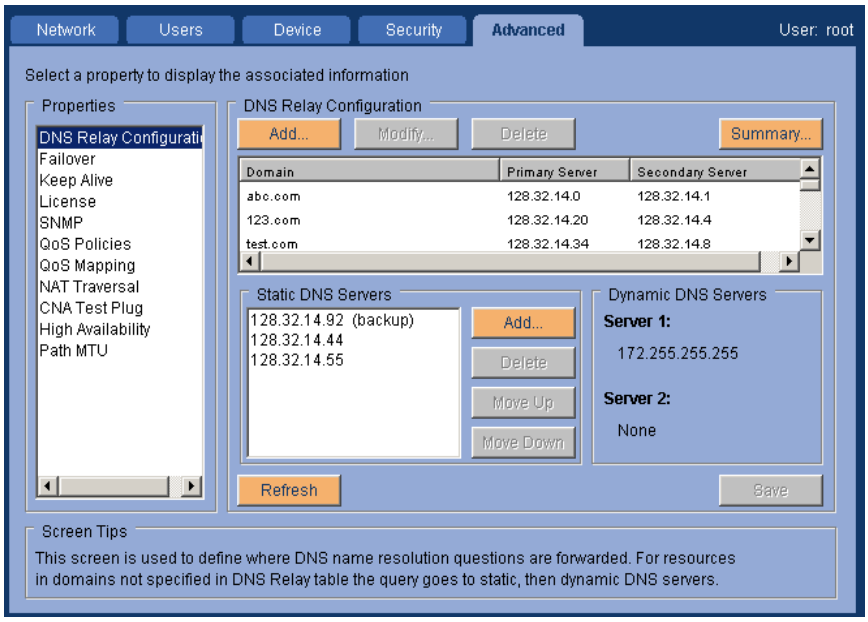
Use the DNS Relay Configuration property to define where DNS name resolution requests from the IP devices on the private side of the security gateway are forwarded.

The security gateway includes a DNS name server, and accepts DNS queries from devices on the private side. DHCP devices on the private side receive access to the DNS service automatically. Non-DHCP devices must be manually configured to identify the security gateway as their DNS server. The security gateway server maintains a DNS database on all DHCP clients on the private interface. Non-DHCP clients have no DNS identity.

Note:

The security gateway performs DNS relay functionality only for the private zone.

Figure 53: Advanced DNS relay property screen



To resolve DNS queries, the security gateway first consults its own database. If this is unsuccessful, the query is forwarded through the public interface. If DNS Relay Configuration domain entries exist, the security gateway tries to find the match of the DNS request domain with the entries' domains. If a match is found, the security gateway only forwards the query to name servers associated with that domain. If no match occurs, the security gateway sequentially forwards the query to the specified static DNS servers. If no static DNS servers exist, queries go to Internet name servers. Note that once static DNS servers are added, Internet root name servers are no longer referenced.

When a DNS server is selected to send the DNS query, and no response is received within a short time, another DNS server is selected by continuing the process as described in the previous paragraph. But if the previous server replies to the DNS query, another DNS server is not selected, regardless of whether response is positive or negative.

By default, when a DHCP client in the private zone sends requests for an IP address and the private zone DHCP server is being used, the DHCP server on the private zone sends it's interface IP address as the DNS server in the DHCP response. In this way, all of the DNS queries are automatically forwarded to the security gateway.

Configuring DNS

Use the DNS Relay Configuration property to set up DNS Relay Configuration and the static DNS servers. The maximum number of DNS relay rules is 100. You cannot configure Dynamic DNS Servers.

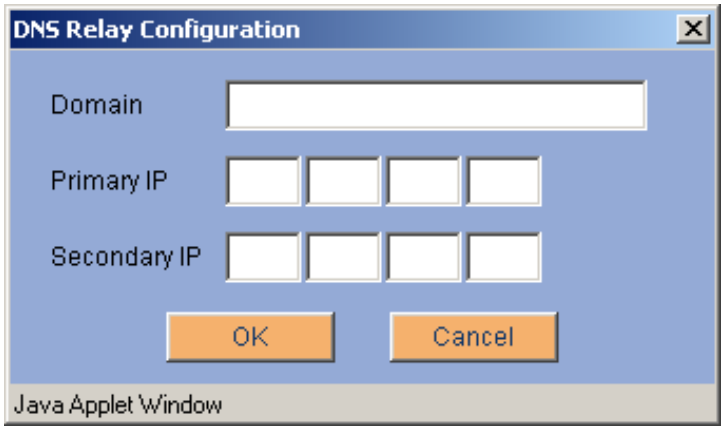
Note:

The **Delete**, **Move Up** and **Move Down** buttons in the DNS Relay Configuration area apply to the IP Address that is currently highlighted.

To add a DNS Relay

1. Select the **Configure>Advanced>DNS Relay Configuration** property. Click **Add**. The DNS Relay Configuration dialog is displayed.
2. Enter the **Domain** name and the **Primary IP** address of the DNS server. The secondary IP address is optional.

Figure 54: Add DNS relay configuration



3. Click **OK**.

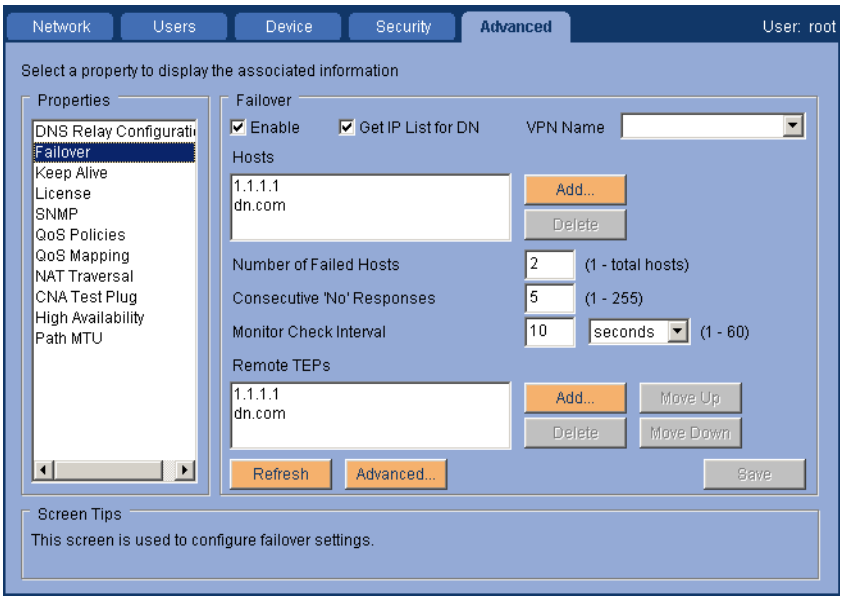
To set up a static DNS server

1. Select the **Configure>Advanced>DNS Relay Configuration** property. In the **Static DNS Servers** area, click **Add**. Enter the IP address of the DNS server and enable the back-up link, if required.
2. The backup link is the DNS server that is used when backup ethernet is in use. Only one of the interfaces, either public or public-backup can be in use at the same time.
3. Click **OK**.
4. The maximum number of Static DNS servers is four.

Failover

Use the Failover property to configure up to five IP addresses for tunnel endpoints (TEP) and to configure failover reconnection. These IP addresses are used for failover locations in the case of VPN or clear traffic failure.

Figure 55: Advanced failover property screen



When Failover is configured, a security gateway periodically checks connectivity to designated devices to evaluate the availability of the network path to the central-site resources. These devices can be within the VPN, such as the corporate e-mail server at the central site. These devices can also be outside the VPN, such as a public DNS server.

When a network path fails, the remote security gateway tries to establish a network path through an alternate central-site. If the remote security gateway cannot use that second central-site TEP to establish a network path, the remote security gateway continues through the list of configured TEPs, and tries to establish a usable network path to the central-site resources. If none of the configured tunnels can establish a network path, and the remote security gateway is configured with a public-backup interface, the remote device tries to establish a path through this alternate link.

When the public-backup interface is in use, the security gateway does not perform failover connectivity checks to the designated hosts. When the idle timer is enabled, and as long as there is traffic, this alternate network link is used. If the configured idle time elapses, the public-backup interface is taken down. The security gateway then tries to reestablish the network connectivity through the primary network path.

If the security gateway is using the public-backup interface, it can be returned to the public interface from the *Configure>Network>Interfaces* property. Click the **Revert to Public** button.

Note:

If the public-backup interface idle timer is disabled, the security gateway continues to use the alternate network interface.

Network path failure is defined as the configured number of consecutive connectivity checks without a response from the number of hosts that need to fail. The following is an example of a network path failure criteria.

The configuration is as follows:

- The number of consecutive “no” responses is five.
- The idle time between each connectivity check is 10 seconds.
- The number of hosts to monitor is three.
- The number of hosts that must fail to respond, out of the hosts configured is two.

Table 4 shows which hosts respond (Y) and which hosts do not respond (N) during the 10-second interval connectivity check.

Table 4: Failover connectivity checks in 10-second intervals

	10	20	30	40	50	60	70	80	90	100	110	120	130
Host													
1	Y	Y	Y	N	N	N	Y	Y	Y	Y	Y	Y	Y
2	Y	Y	Y	Y	N	N	N	N	**N**	**N**	**N**	**N**	**N**
3	N	N	N	N	N	Y	Y	Y	**N**	**N**	**N**	**N**	**N**

The network path failure criteria are met only when *both* hosts 2 and 3 *concurrently* fail to respond five times (at the 130 second mark to the connectivity checks. Host 3 failed to respond five consecutive times (between the 10-second interval and the 50-second interval). Host 2 failed to respond five consecutive times (between the 50-second interval and the 90 second interval). But only host 2 and host 3 both fail to respond to the same five consecutive security checks are the failure criteria met.

To configure failover:

1. Select the **Configure>Advanced>Failover** property, and complete the following:
   a. Select **Enable** to provide an alternate network path to re-establish access to the central-site resources.
   b. Select **Get IP List for DN** so when a DNS query is made, the security gateway keeps all the IP addresses that are returned in the cache. The security gateway attempts to respond to the queries in the same order that the queries were received.

      If this parameter is not selected and a DNS query is made, the security gateway uses the first IP address of the DNS response that is returned.
   c. In the **VPN Name** field, enter the name of the VPN that you want to monitor. This field is optional, if Set VPN Mode is set to dynamic.
   d. In the **Hosts** field, enter the network host or hosts you want to monitor connectivity. You can define up to five DNS names or IP addresses. These hosts can be either within the VPN or outside the VPN. If the host is within the VPN, the host information is encapsulated in the associated VPN policy. If the host is outside the VPN, the host information is sent in the clear.
   e. In the **Number of Failed Hosts** field, enter the number of configured hosts that can fail before network path f criteria is reached. If multiple hosts are configured and all hosts are critical, enter 1. If any one of the configured hosts failed to respond, network path failover occurs.
   f. In the **Consecutive “No”Responses** field, enter the number of consecutive connectivity checks without a response that you want to allow. The default is 10.
   g. In the **Monitor Check Interval** field, Enter the number of seconds that you want to allow between connectivity checks to the configured host or hosts. The interval is also used to define the response time of the host. Monitor checks are made at the same time to each host. The default is 10 seconds.
   h. In the **Remote TEP field**, enter the tunnel endpoints (TEP) for the central site that the remote VPN device establishes a network connection. If the network path failure criteria is met while the remote security gateway is trying to establish a network connection, the remote VPN tries to alternate TEPs until a network connection is made.
2. Click **Save**.

Failover reconnect

When failover is configured on the security gateway, the security gateway is enabled to detect connectivity failures to the configured TEPs. If failover is detected, the security gateway will attempt to connect to an alternate TEP.

In some network configurations, alternate TEPs are considered temporary, and the expected behavior is that a system reboot would revert to the original TEP. However, the security gateway remains connected to the alternate TEP until the administrator switches the connection back to the original TEP.

Beginning in release VPNos 4.4, failover reconnect option can be set using the failover advanced settings. The failover advanced settings include preserve current remote tunnel end point (RTEP) and restore primary remote tunnel end point (RTEP).

If a system reboot occurs, the security gateway inspects the failover reconnect value. If the value is set to preserve current RTEP, the failover proxy remains at the current value allowing the security gateway to remain connected to the RTEP in use prior to the system reboot. If the value is set to restore primary RTEP, the failover proxy retrieves the information for the original RTEP and restores the RTEP to the original values.

To set up failover reconnect:

1. Select the **Configure>Advanced>Failover** property. Click **Advanced**.
2. Select the appropriate failover reconnect option.
   - Preserve current RTEP
     In the event of tunnel failover, leave the current remote tunnel endpoint in effect following a system reboot.

     In previous releases of VPNos 4.x, a system reboot would not restore the original RTEP.
   - Restore primary RTEP
     In the event of tunnel failover, restore the original, primary remote tunnel endpoint in effect following a system reboot.

     Beginning with VPNos 4.4, restore primary RTEP is the default setting.

If restore primary RTEP is configured and the system reboots, failover reconnect will attempt to connect to the first entry of the failover RTEP list.

Traceroute

When traceroute is configured on the security gateway, the network administrator is better able to trace where the network failure occurred.

Beginning in release VPNos 4.5, the traceroute feature has been enhanced to allow network administrators to trace network path failures with the VPN tunnel, and to bind the user data protocol (UDP) to the SG private interface. This enhancement allows the traceroute feature to send traffic in the VPN tunnel. However, these enhancements only occur if configured. If these enhancements are not configured using the VPNos 4.5 release, the traceroute feature remains the same as previous release.

To set up traceroute during failover:

1. Select the **Configure>Advanced>Failover** property. Click **Advanced**. Select **Enable**, and complete the following:
2. Configure the traceroute settings.
   - Enable traceroute during failover

     In the event of tunnel failover, leave the current remote tunnel endpoint in effect following a system reboot.

     In previous releases of VPNos 4.x, a system reboot would not restore the original RTEP.
   - Set **consecutive no responses**.

     The number of consecutive connectivity initiation checks without a response from the number of failed hosts specified in the failover configuration to initial traceroute.
   - Select the **target host**. Click **OK**.

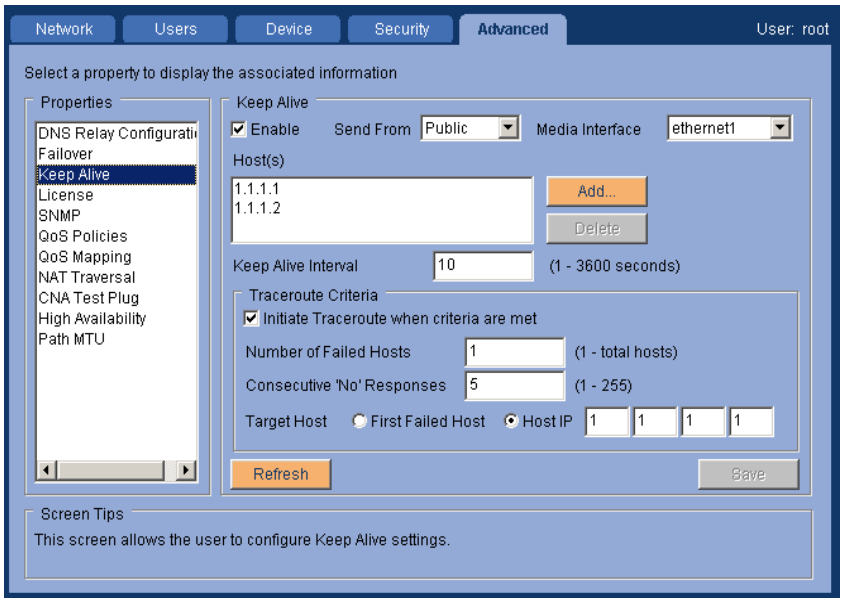
     The target host is the host where traceroute will be initiated.
   - **First Failed Host**. The network host IP address specified in the failover host list. Traceroute will be initiated to the first failed host from the configured list of failover hosts.
   - **Host IP**. The network host IP address to monitor connectivity.Traceroute will be initiated on the specified host IP address.

Keep Alive

The Keep Alive property allows the security gateway to send keep alive packets (ICMP) to the configured host at every configured interval in the network. Keep alive hosts can be configured anywhere in the network. The keep alive property also allows configuring traceroute capability when the traceroute criteria are met allowing network administrators to trace network path failures.

Keep alive packets can be sent to configured hosts that are in a protected networks and unprotected networks; therefore, these packets can be encrypted or clear traffic based on the VPN policy on the device.

Figure 56: Advanced keep alive property screen



To configure keep alive:

1. Select the **Configure>Advanced>Keep Alive** property, select **Enable**, and complete the following:
   a. From the **Send From** drop-down menu, select a network zone.
      - **Public**. The public network interface provides connection to the Internet, usually by way of a wide area network (WAN). By default, DHCP Client is used to configure the public IP address.
      - **Private**. The private network interface usually provides connection to your private local area network (LAN) or your corporate LAN.

   b. Confirm that the **Media Interface** field is displaying the correct interface.

   c. In the **Hosts** field, enter the network host or hosts you want to monitor connectivity. You can define up to five DNS names or IP addresses. These hosts can be either within the VPN or outside the VPN. If the host is within the VPN, the host information is encapsulated in the associated VPN policy. If the host is outside the VPN, the host information is sent in the clear

   d. In the **Keep Alive Interval** field, enter the interval in seconds that packets will be sent to configured hosts. The default is 10 seconds.

2. Select **Initiate Traceroute when criteria are met**, and complete the following:
   a. In the **Number of Failed Hosts** field, enter the number of hosts from the configured keep alive hosts that can fail to receive keep alive responses. If multiple hosts are configured and all hosts are critical, enter 1. If any one of the configured hosts failed to respond, network path failover occurs.
   b. In the **Consecutive "No"Responses** field, enter the number of consecutive connectivity checks without a keep alive response before traceroute is initiated. The default is 10.
   c. From the **Target Host** area, select the host type.
      - **First Failed Host**. The network host IP address specified in the keep alive host list. Traceroute will be initiated to the first failed host from the configured keep alive host list that meets the traceroute criteria.
      - **Host IP**. The network host IP address to monitor connectivity.Traceroute will be initiated on the specified host IP address.
   d. Click **Save**.

License

The security gateway license controls the number of site to site connections and remote user.

Go to the *Configure>Advanced>License* property to view general information about the license (Figure 57), including the serial number, security gateway platform, software release it is associated with and the number of licenses for site to site and remote users.

Figure 57: Advanced license property screen

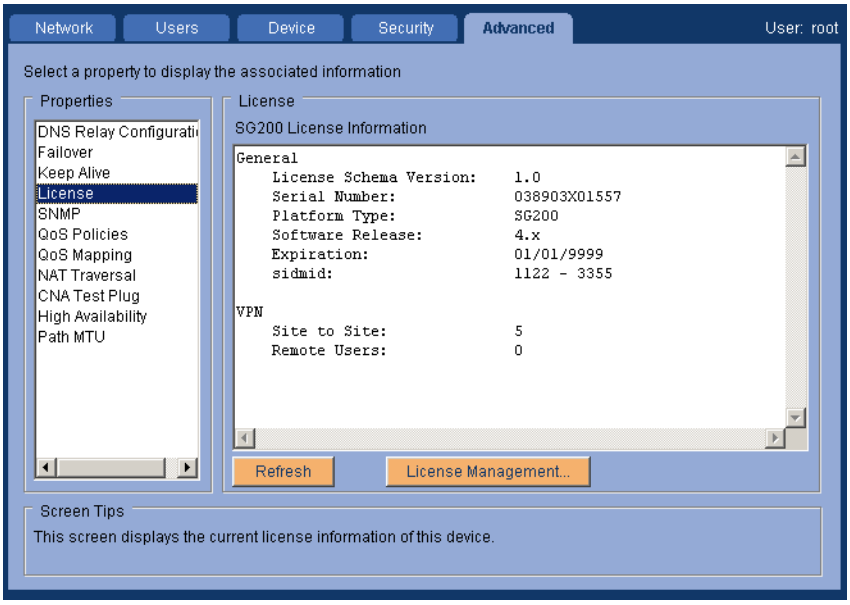


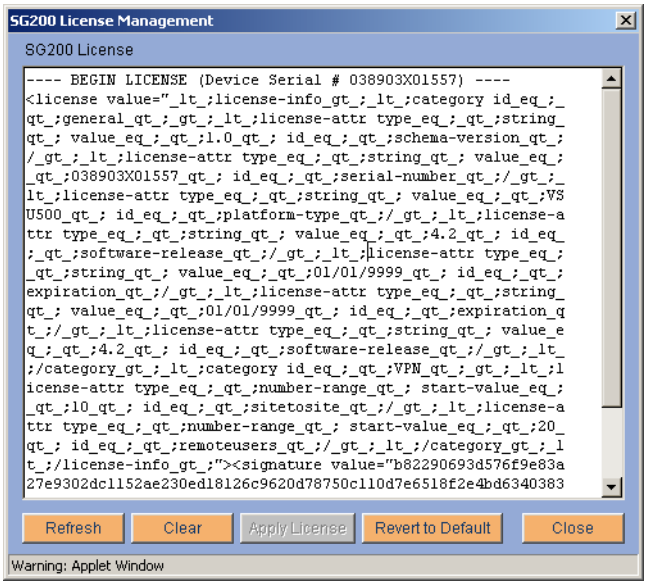
Table 5 shows the default number and the maximum number of licenses for each security gateway. When usage increases, you can purchase additional licenses. The License property display includes a license management feature so that you can uploaded new licenses to the security gateway.

Table 5: Number of security gateway licenses allowed

Model	Number of Site-to-Site Licenses	Number of Remote User Licenses
SG5	Default = 5, Maximum = 5	Default = 0, Maximum = 5
SG5X	Default = 5, Maximum = 5	Default = 0, Maximum = 5
SG200	Default = 25, Maximum = 150	Default = 50, Maximum = 500
SG203	Default = 50, Maximum = 300	Default = 100, Maximum = 3000
SG208	Default = 100, Maximum = 1000	Default = 100, Maximum = 8000

When you click License Management, the License Management screen shows the encrypted license information for the security gateway.

Figure 58: License management screen



Adding licenses

When you purchase additional licenses, you receive a file with the encrypted information. This file is created based on the serial number of the security gateway and the number of licenses that are available on that security gateway. This file cannot be applied to another security gateway.

To install the additional licenses:

1. Save the license file to a directory on the computer. Open the file and copy the contents.
2. Select the **Configure>Advanced>License** property. Click **License Management**, the existing license is displayed.
3. Click **Clear**, to clear the screen of the existing license.
4. Paste the contents of the security gateway license file into the text area. Click **Apply License** to apply the new license. The new license is immediately available.

   Note:

   Revert to Default allows you to reapply the original license settings at any time.

SNMP

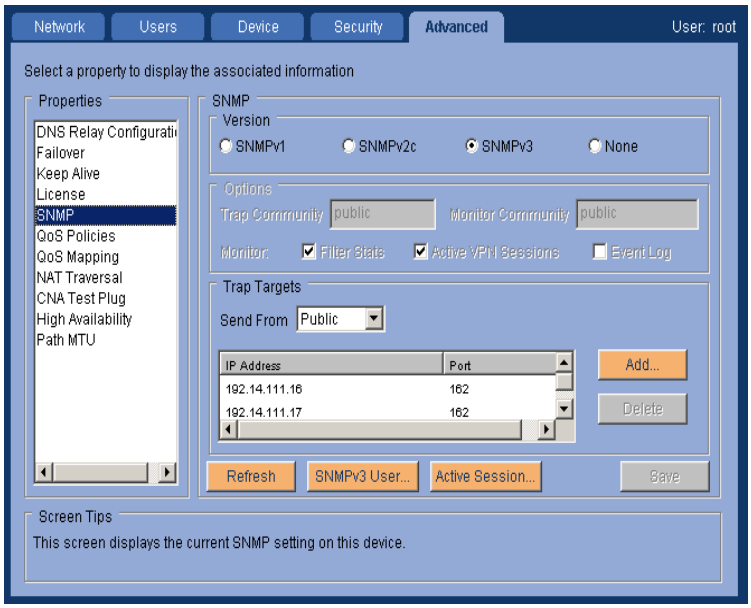
Use the SNMP property to configure the SNMP target devices or SNMP destination devices to which all security gateways report their status and alarm information. In larger enterprises, the security gateways might also report to a network monitoring application, such as HP Openview.

The security gateway includes an SNMP agent that supports MIB-II and a proprietary MIB. The MIB is read-only and cannot be used to configure the security gateway. The agent can also send traps to a list of trap targets.

SNMPv1, SNMPv2c, or SNMPv3 can be configured. You configure the trap and monitor communities and trap targets for SNMPv1 and SNMPv2c. You configure the trap targets and the SNMP user for SNMPv3.

If you select None, SNMP is disabled on the security gateway.

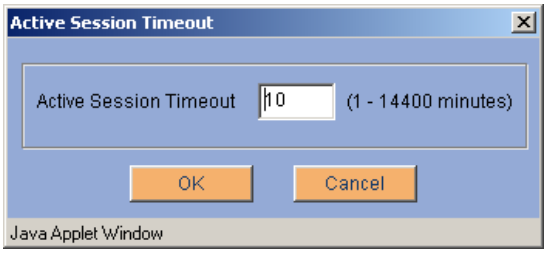
Figure 59: Advanced SNMP property screen



To configure SNMP:

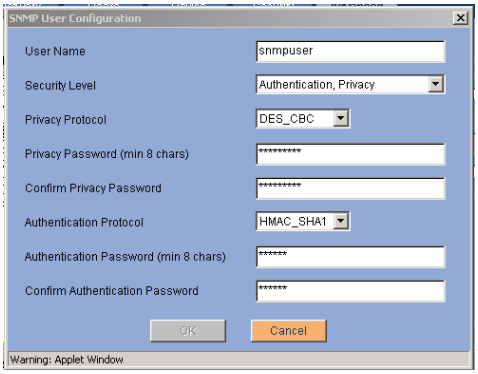
1. Select the Configure>Advanced>SNMP property. In the **Version** area, select the type of SNMP to use.
   - The SNMP version must match the version number that the monitoring tool is using.
   - Select **None** to disable the SNMP agent on the security gateway.

2. If SNMPv1 or SNMPv2c are selected, in the **Options** area, configure the **Trap Community** and **Monitor Community**. Select whether Filter Statistics, Active VPN Session, and Event Log should be enabled.
   - **Filter Statistics -** Filter statistics and firewall statistics are reported via SNMP.
   - **Active VPN Session -** Ability to monitor the active VPN sessions on the security gateway. Active VPN sessions are monitored using SNMP protocol. The monitored information is logged in the VPNET MIB and displays the following information: user name or RTEP, original IP address, VPN IP address, length of time connected, and packets sent and received.
   - **Event Log -** The security gateway sends syslog messages to the event log. The syslog messages can include critical or major events in the system. Most error conditions within the system are captured in the event log.
3. In the **Trap Target** area, select a network zone from the **Send From** drop-down menu. Select **Public**, **Private**, or **Any**.
   - **Public.** The source of the SNMP trap is the public interface.In order for the trap information to be encrypted, the trap destination must match the VPN policy, including the public IP address as the local IP group in the VPN from the public interface. Trap information is sent in the clear when the VPN policy is undefined, and the SG or destination IP address is dynamic or part of a public internet.
   - **Private.** The source of the SNMP trap is the private interface. In order for the trap information to be encrypted, the trap destination must match the VPN policy from the private interface. Trap information is sent in the clear when the VPN policy is not matched.
   - **Any.** The source of the SNMP trap is the any interface. Trap information is sent as designated in the routing table. If the trap destination is sent in the private subnet, the packet will send from the private interface. If the trap destination is in the Internet or the packet has an unmatched route, the packet will send from the public interface.
4. Enter the IP address and port.
5. If SNMPv1 or SNMPv2c are selected, configure the Active VPN Sessions Time Out information. Click **Active Session** below the Trap Targets area. The Active Session dialog is displayed.



6. Enter the **Active Session Timeout** duration in minutes. The default timeout is 10 minutes. Click **OK**.

7. If SNMPv3 is selected, configure the SNMPv3 User information. Click **SNMPv3 User** below the Trap Targets area. The SNMP User Configuration dialog is displayed.



The default user name is snmpuser. You can modify the user name. To complete the configuration, enter the following:

- **Security Level**. Choose either Authentication, Privacy or Authentication, No Privacy. Based on the selection, the privacy settings are enabled or disabled.
- **Privacy Protocol**. Only DES_CBC is available.
- **Privacy Password**. Enter the privacy password of the SNMPuser.
- **Authentication Protocol**. Choose either HMAC-SHA1 or HMAC-MD5.
- **Authentication Password**. Enter authentication password.

8. Click **OK**, and then click **Save**.

QoS policy and QoS mapping

The Quality of Service (QoS) function allows the administrator to classify and prioritize traffic based on DSCP values and/or TCP/IP services and networks. The bandwidth available to a class of traffic can be restricted or rate-limited to a specific percentage of the total upstream bandwidth. This restriction or rate-limiting of bandwidth is only applicable to upstream or outgoing traffic on the interface.

A QoS policy can be created with up to four classes, highest, high, medium, and low. Attributes that can be assigned to these classes are percentage of bandwidth allocation, type of services, network objects, DSCP, and burst.

QoS policies can be mapped to public, public-backup, and semi-private zones. By default, QoS is enabled and VoIP is given the highest priority and there is no restriction of bandwidth or rate-limiting. In the default configuration, VoIP is identified solely by IP precedence values of three and five. This corresponds to the following DSCP values: 24-31 and 40-47.

If QoS is disabled, all traffic receives the same priority. VoIP is treated the same as data traffic.

QoS Policy

This property allows you to add, modify and delete QoS policies. Each policy can include up to four configurable classes, highest, high, medium and low.

You can configure each class according to how network traffic should be prioritized. Each class can contain data, voice or both. Within each class the following is configured:

- **Bandwidth allocation**. Percentage of bandwidth to be allocated to the class. The sum of all allocations for a QoS policy should be 1 to 98%.The remaining 2% is internally allocated by default to ICMP, IGMP, and RSVP. The excess bandwidth not specified in the sum of allocations of the policy is reserved for all other traffic not defined in the classes. Therefore, it is not necessary to create a class for all other traffic. If 0% is allocated, the class is removed from the existing configuration.

  Note:

  When the media interface is configured, the total upstream bandwidth can be specified in Media Settings and this setting is partitioned to the specified classes.

- **Whether Burst is enabled**. For each class, the burst capability value can be set to Yes or No. The default is No. If bursting is configured for a class, when this class becomes over-limit, it tries to borrow from the unused bandwidth of other classes. If no unused bandwidth is available, the packets are dropped when the class becomes over-limit.

  CAUTION:

  Allowing bursting in classes that do not contain voice traffic can affect the availability of bandwidth to voice traffic.

- **DSCP values are assigned**. The valid range of values is 0-63. The default value is 0. This indicates that DSCP is not used for classification. Non-zero DSCP values must be unique among all the classes for one zone because the DSCP value is the only distinguishing factor once a packet is encrypted and sent of the VPN. For example, if DSCP value 10 is assigned to the High class for media interface Ethernet0, DSCP value 10 cannot be assigned to Highest, Medium or Low for Ethernet1. It can be assigned to the High class for Ethernet 1.

1. When DSCP value of 0 is specified during configuration, the security gateway generates an internal non-zero DSCP value within the range of 1-63. The non-zero DSCP value generated by the security gateway cannot be used in other classes.

   - **Source Network Objects**. Traffic originating from specific networks/hosts can be selected from existing Network Objects. See Network Objects in Chapter 5: Establishing security. The source network object specifies the source IP address of the IP packets in this class.

   - **Destination Network Objects**. Traffic destined to specific networks/hosts can be selected from existing network objects. The destination network object specifies the destination IP address of the IP packets in this class.

- **Service**. Traffic can be specified by predefined or user-configured services. A service specifies the IP protocol, TCP/UDP source and destination ports to describe the traffic in this class. See Services in Chapter 5: Establishing security.

Note:

ESP or IKE cannot be assigned with a class as these encrypted packets are assigned to all the classes based on the DSCP value of the packet.

Note:

It is **not** recommended that a user creates a class with DSCP=, Services=ANY, and Networks=ANY because it is an ambiguous configuration. All traffic not assigned to classes is treated as default traffic. Hence it is not necessary to create such a class.

Note:

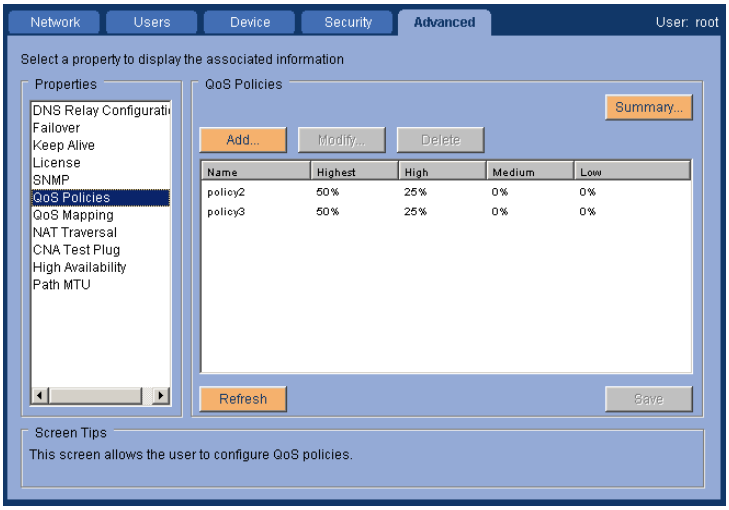
It is **not** recommended to assign similar traffic in different classes. Example: One class containing any FTP and another class containing “ANY TCP”. This would be ambiguous because “ANT+YTCP” would include FTP also. Similar cases might cause ambiguity in classification.

Note:

It is **not** recommended to use Services containing ICMP or port-ranges. QoS does not support port-ranges.

When the *Configure>Advanced>QoS Policies* property is selected, the screen displays the QoS policies that have been created and their configuration.

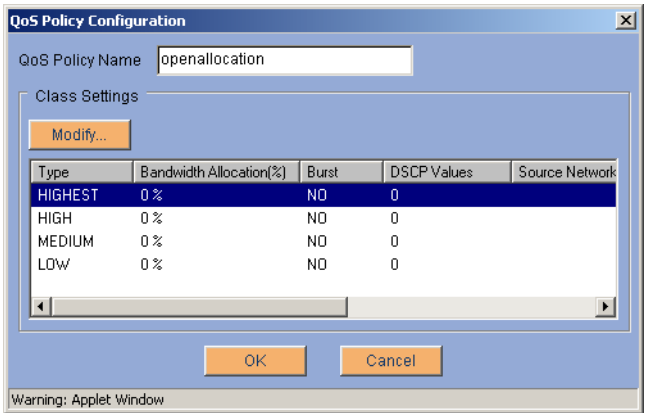
Figure 60: Advanced QoS policy property screen



To add a QOS policy:

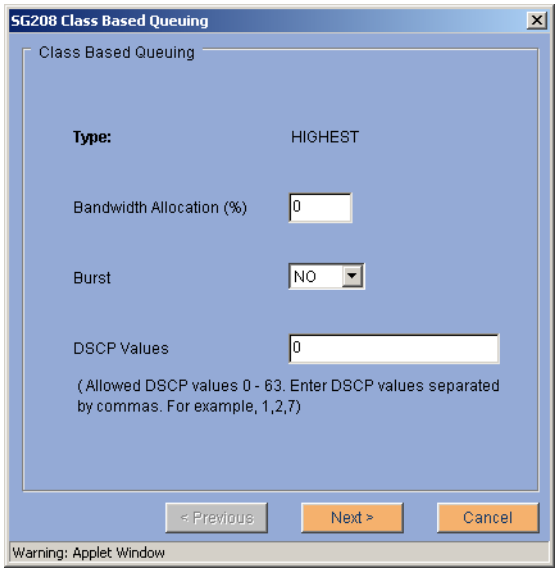
1. Select the **Configure>Advanced>QoS** policy. Click **Add**. The QoS Policy Configuration dialog is displayed.

Figure 61: QoS policy configuration screen



2. In the **QoS Policy Name** text box, enter a unique QoS policy name.
3. Next configure each class setting with associated values. Click the row for the type to be configured. The Class Based Queuing dialog appears.

Figure 62: Modify QoS bandwidth, burst, and DSCP value screen



4. Configure bandwidth, burst and DSCP values.
   - Enter the percentage of bandwidth to be allocated for this type.

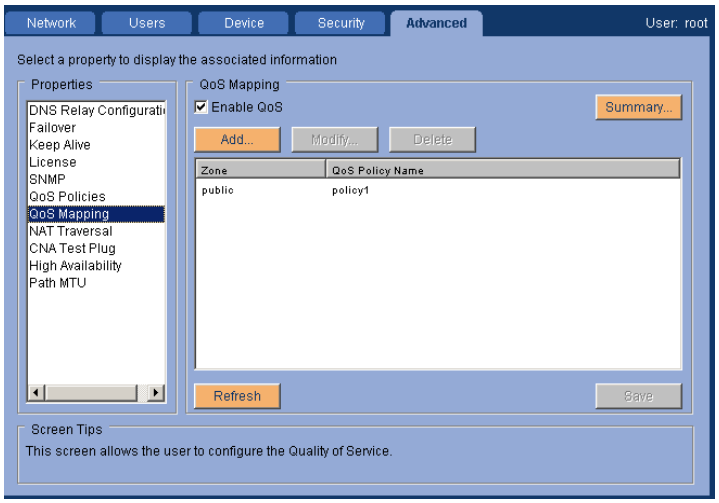
     When classes are configured, it is recommended that the sum total allocation of all the classes be less than 98% and allow bursting to take advantage of the unused bandwidth. 2% is always internally allocated to control traffic.
   - Burst is set to **No**. Change to Yes if bursting should be allowed.

     If bursting is configured, when this class becomes over-limit, it tries to borrow from the unused bandwidth. If there is no unused bandwidth, then the packets are dropped when the class becomes over-limit.
   - The same DSCP value cannot be assigned in multiple classes for one interface. Do not specify the same DSCP-Services-Network combination in multiple classes.
5. If DSCP will not be specified as a criteria in a class, leave the DSCP default value of 0. In this case, it is recommended to assign unique services/networks to this class. Do not assign *ANY* service and *ANY* network objects.
6. Click **Next**. The Source Network Objects dialog appears. Select the network object from the **Available** source and move it to the **Members** column.
7. Click **Next**. The Destination Networks Objects dialog appears. Select the network object from the **Available** destinations and move it to the **Members** column.
8. Click **Next**. The Services dialog is displayed listing the predefined and user defined traffic types. Select the services from the **Available** column and move to the **Members** column.
9. Do not assign ESP or IKE as a service within a class as these encrypted packets are assigned to all the classes based on the DSCP field on the packet.
10. Click **Finish**.
11. Complete the configuration of each of the classes from step 3.
12. When the classes have been configured, click **OK** and then click **Save**.

QoS mapping

QoS Mapping is the mapping of a QoS policy to a zone. A zone can map to only one QoS policy, but a QoS policy can be applied to multiple zones.

Figure 63: Advanced QoS mapping property screen



When you map QoS policies consider the following:

- If QoS is configured over multiple interfaces, the DSCP values belonging to a class for a particular zones should not belong to a different class for other zones.
- When QoS is applied over multiple zones, the QoS policies should be identical in definition of classes, DSCP, and service-networks attributes. The only difference in these QoS policies should be in the bandwidth allocation percentage.

Mapping QoS policies

After the QoS policies are created, they can be mapped to either public, public-backup or a semi-private zone.

1. Select the **Configure>Advanced>QoS Mapping** property. Click **Add**. The QoS Configuration dialog is displayed.
2. From this dialog select the **Zone** to be configured and the **Media Interface** used for that zone.
3. Select the policy from the **Available** column and move it to the **Member Policy** column.
4. Click **OK** and then click **Save**.

NAT traversal

NAT Traversal

Network address translation (NAT) traversal is available for VPNos 4.3 feature pack and later releases. When a NAT device exists in a network path between security gateways that are part of a VPN, NAT traversal allows the VPN traffic to successfully pass from one device to another. The default is NAT traversal enabled.

From the device Configure>Advanced>NAT Traversal property, you can do the following:

Disable NAT traversal

Avaya suggests that you do not disable this feature even when a NAT device does not exist in the network path between the VPN peers devices.

Set the value for KeepAlive

The time configured is used when the security gateway is in the private network of a NAT device. The security gateway behind the NAT device sends a keep alive packet to reserve the dynamic source port in the NAT device when VPN traffic is not flowing. The default is 20 seconds.

Because NAT devices can clear port assignments after a period of inactivity, a still open VPN session may be broken. When a new packet arrives after a certain period of inactivity, a NAT device can assign a new dynamic source port for the packet that causes the VPN connection to fail. To avoid this problem, keep alive packets are sent from the peer which is behind the NAT device.

VPNos Feature Pack 4.3, and later releases, use the UDP source port 2070 during IKE negotiation when configured as User VPN mode or dynamic VPN mode. The following information states the functionality and the expected VPNos 4.3 and later releases behavior.

Table 6: Encapsulation Behaviors

Functionality	VPNos Behavior
UDP listening ports for IKE	Ports 500, 2070, 4500
Ports used for UDP encapsulation	Ports 500, 2070, 4500

1 of 2

Table 6: Encapsulation Behaviors (continued)

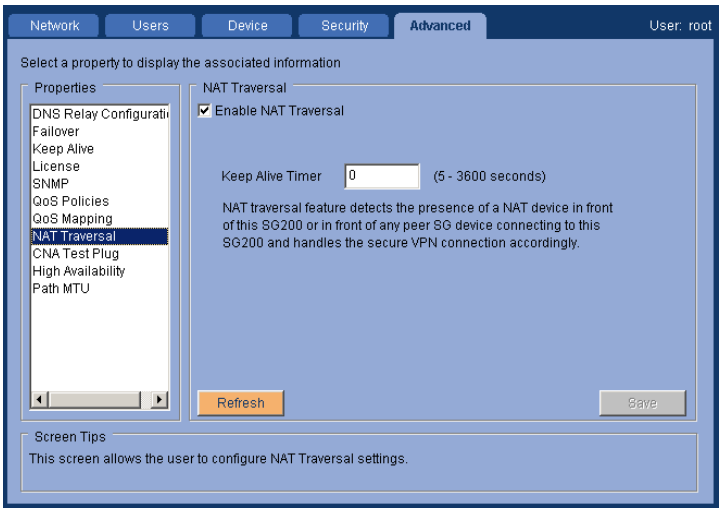
Functionality	VPNos Behavior
UDP source port used when acting as IKE initiator and UDP encapsulation	• Port 2070 when VPNos 4.x is configured as User VPN mode or dynamic VPN mode. This is done to avoid issues with NAT devices with IPsec pass through in the case where a remote VPN peer device dose not support port floating. • Port 500 when VPNos 4.x is configured as VPN Gateway Mode, static VPN mode, or NAT traversal is disabled. This option is not configurable.
Port floating	Float the port from 500 or 2070 to 4500 if new IKE draft is supported.

2 of 2

UDP source port is kept as 500 in VPNos 4.3 and later releases in VPN gateway mode or static VPN mode as VPNos 3.2 does not support UDP source port other than 500 during IKE negotiation for site-to-site VPNs. When creating a site-to-site VPN with VPNos 3.2 VSUs with a remote security gateway or VSU behind the NAT device, apply static NAT mapping in the NAT device to avoid changing the UDP source port, port 500, during IKE negotiation. Also make sure that NAT device should not perform IPsec pass through.

In the case of a remote VPN peer running VPNos 3.2, only one VPNos 4.3 or later release security gateway configured in VPN gateway mode can be placed behind a NAT device.

Figure 64: Advanced NAT Traversal



Converged Network Analyzer Test Plug

The converged network analyzer (CNA) test plug feature provides a distributed system tool for real-time network monitoring that detects and diagnoses converged-network-related issues. When enable, this monitoring tool is proactive and can identify network conditions or impairment that can degrade the overall network performance and diagnose if the security gateway is experiencing difficulty. Within the CNA, the test plugs are independent software modules that are injected into the fault-tolerant network to collect and analyze the network test data. If potential network problems are detected, they are escalated using standards-based alarms and notification.

This feature includes enabling CNA, setting the test plug services, configuring the RTP test port and CNA unit port, and adding CNA units for registration.

Multiple CNA units can be configured in the network to monitor network topology and run various tests. A GUI application called ChaPl is used for configuring network tests, scheduling network tests, and viewing the results of each test.

The following network tests are available using the CNA test plug. To configure the following tests, use the ChaPI GUI application.

- Ping test

  The ping test includes unary and binary test. The ping test sends an ICMP echo message to a target IP address, and reports whether or not a response was returned. This report includes the return travel time (RTT).

  The binary test plug requires a pair of test plugs.

- RTP test

  The real-time transport protocol (RTP) test measures one-way delay, packet loss, and jitter to another test plug by sending a simulated RTP data stream that is echoed back. The test provides data regarding the VoIP performance over the network. If the RTP test source and destination IP addresses are outside the VPN, the RTP delay calculation excludes the host effect. For example, the RTP delay excludes any overhead by the security gateway. If the RTP test source and destination IP addresses are inside the VPN, the RTP delay calculation includes the host effect including the QoS overhead.

- Traceroute test

  The traceroute test discovers the route hops from a source test plug to destination IP or test plug. It measures return time travel (RTT) for each intermediate router hop.

- TCP Connect test

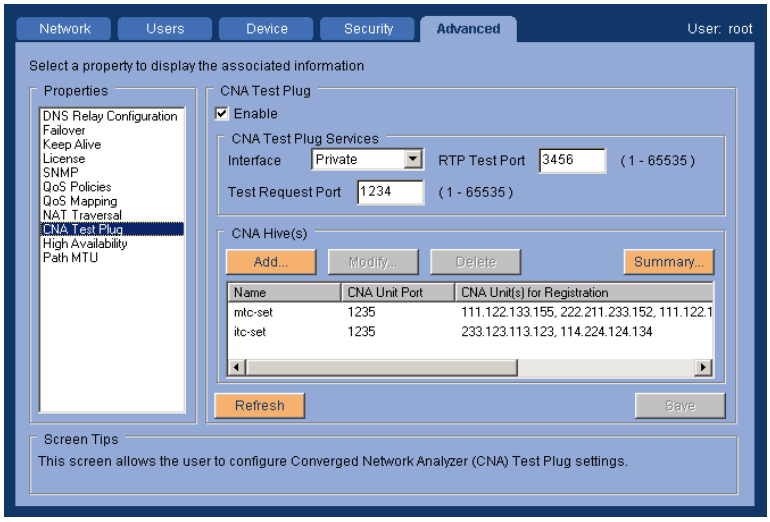
  The TCP connect test runs a TCP test from a source test plug to a destination IP address or test plug on a configurable TCP port. This test calculates the time delay to establish the TCP connection and provides error information.

- Merge Test

  The merge test in not configurable using ChaPI. This test automatically runs to discover if more than one IP address in the topology belongs to the same router hop. If the test discovers more than one IP address, the addresses will be merged into a single node in the ChaPI.

To enable CNA test plug using the Web interface:

1. From the **Configure>Advanced>CNA Test Plug** property, select **Enable**.



2. In the CNA Test Plug Services area, enter the following information:

   - **CNA Test Plug Services** interface.

     The security gateway runs CNA test plug on the selected interface only. Select public or private. For example, the security gateway registers only the selected interface IP address with the CNA unit. In addition, the CNA test plug tests are run using the selected interface IP address only. The private interface is the default setting for CNA.

   - **Test request port** value.

     The test request port value is the port that the test plug receives a test request. The test request includes authentication, and a validly formatted request from the CNA test plug scheduler. The value for the test report port ranges from 1 to 65535. The default test request port value is 50000. It is not recommended to change the default test port value.

   - **RTP test port** value.

     The RTP test port value is the value of the real-time transport protocol. The value for the RTP test port ranges from 1 to 65535. The default RTP test port value is 50001. It is not recommended to change the default RTP test port value.

3. In the CNA Hive(s) area, click **Add** and enter the CNA hive configuration information:
   - **CNA unit name**
   - **CNA unit port**

     The CNA unit port for registration is the value of the CNA registration port. The value for the CNA registration port ranges from 1 to 65535. The default CNA unit port value is 50002.
4. In the CNA Units for Registration area, click **Add** to enter the IP address of the CNA unit to register. Click **OK**.
5. Use the Move Up and Move Down buttons to adjust the unit priority.
6. Click **Save**.

The security gateway will begin the registration process by selecting the first configured CNA unit in the list. The security gateway will continue to attempt the registration process with the remaining CNA units in the list until a registration is successful. The security gateway will stop the registration process at the end of the CNA unit list. The CNA unit registration process will be reinitiated if the CNA test plug is enabled and any changes are made in the CNA test plug configuration or the IP address of the CNA test plug interface is changed.

Important:
Converged network analyzer is not NAT aware. For example, if the interface IP address used by the CNA test plug is NATed in the network path, or tunnel NAT is applied to communicate with the CNA unit or peer CNA test plugs, CNA test plug will not behave correctly.

High Availability

The high availability feature provides a fault tolerant infrastructure that minimizes the downtime of the protected network. Fault tolerant infrastructure is achieved by pairing two like security gateways together to form a high availability (HA) group. The HA group is comprised of a primary or active security gateway and secondary or passive security gateway.

This feature includes enabling high availability, setting the revision value, confirming the HA status, setting the CARP (Common Address Redundancy Protocol) advertisement interval, setting the group ID value, setting the missed advertisements value, setting and confirming the pass phrase, and modifying the public and private virtual addresses.

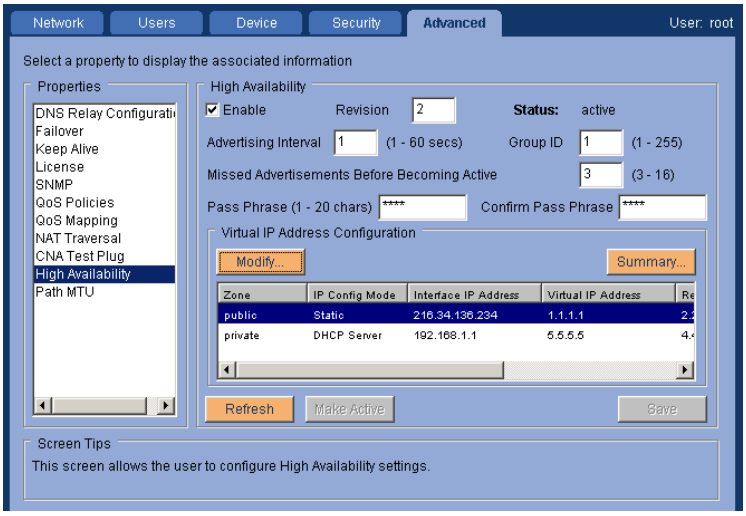
To configure high availability using the web interface, you must ensure that the security gateways in the HA group are configured identically with the exception of the SG's physical interface IP address. Configuration of each security gateway in the HA group must be done through the web interface for each security gateway. This feature is support on SG203 and SG208 only.

Important:

The high availability feature and the failover feature cannot be configured concurrently. If these features are concurrently configured, their configuration is invalid and is not supported by the software.

To enable high availability:

1. From the **Configure>Advanced>QoS Availability** property, select **Enable**.



2. Enter the **Revision** value.

   The revision value is the number that forces one of the HA units to become the primary HA unit. The HA member with the higher revision number is the HA member that will become the HA primary unit. The revision numbers on both of the SGs in the HA group are typically configured with the same values. However, to force one member of the HA group to be the active unit, configure that unit with a higher revision number.

3. Enter the **Advertising Interval** value.

   The advertising interval is the time interval in seconds that the active member advertises to the passive member. The advertising interval ranges from 1 to 60 seconds.

4. Enter the **Group ID** value.

   The group ID allows configuration of a unique identifier for the HA group. By using the group ID, the HA group avoids conflicts with other CARP or VRRP implementations on the network. The value for the group ID ranges from 1 to 255.

5. Enter the **Missed Advertisements Before Becoming Active** value.

   The missed advertisements before becoming active value determines the number of advertisement intervals. At least one advertisement must be received by the passive member from the active member. If the passive member does not receive the advertisement, the passive member assumes that the active member is down and will force the election to become the active member. The value for missed advertisement ranges from 3 to 16.

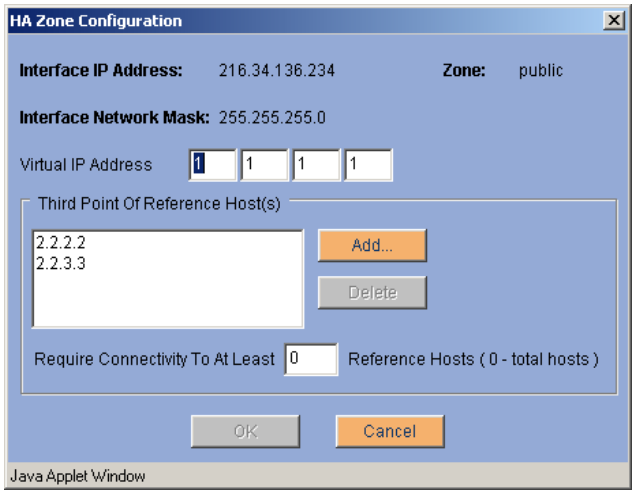
6. Enter the **Pass Phrase** value.

   The pass phrase value is a character text string used as the authentication key to generate the SHA1 message that is used to verify the CARP advertisements.The maximum length of the pass phrase character string is 20 characters.

7. Confirm the **Pass Phrase**.

To configure high availability:

1. In the Virtual IP Address Configuration area, select the **public** or **private** network zone to create the HA group. Click **Modify**.



2. Enter the **Virtual IP Address** that corresponds with the network zone.

   Public virtual IP address. This IP address is shared by all units in the HA group on the public side. The public virtual IP address is the tunnel end point, is the address seen by other network devices on the public side, and is distinct from the interface network zone IP address.

   When HA is enabled and configured on a device, the public interface must have been configured statically. DHCP client and PPPoE IP configuration modes (dynamic IP config modes) are not supported on public interface in a HA enabled device.

   - **Private virtual IP address**. This IP address is shared by all units in the HA group on the private side.The private virtual IP address is the address seen by other network devices on the private side, and is distinct from the interface network zone IP address.

     If the private interface has DHCP server configuration, the private virtual IP address cannot be in the assignable range of the DHCP server.

3. In the **Third Point of Reference Host(s)** area, click **Add** to enter the IP address of the points of reference.

4. Reference host IP addresses are addresses of reference hosts that serve as third points of reference that an inactive device checks for connectivity before trying to become the active device. Up to eight reference hosts can be configured for each network zone.

5. If the network requirements do not permit having the private interface or the public interface plugged into the same network device, configure a reference host(s).
6. Enter the minimum number of **Reference Hosts Needed for Connectivity**.
7. The minimum number of reference hosts needed for connectivity on each network zone that must respond before an inactive device attempts to become active.
8. Click **OK**.

Path MTU

When a device communicates with another network device, it attempts to discover the largest packet it can transmit to the other network device without fragmentation. The largest packet the network can transmit is called maximum transmission unit (MTU).

As a packet is routed through different networks, it may be necessary for a router to divide the packet into smaller pieces because it might be too large to transmit as a single packet on a different network. This may occur at the interfaces of physically different networks.

The MTU of a security gateway passing secure traffic is configured from the **Configure>Network>Interfaces** property. The MTU value ranges from 296 bytes to 1500 bytes. For optimal MTU performance, the recommended MTU minimum value is 512.

Note:

If the system is configured as PPPoE, the maximum recommended MTU value is 1492.

Following are reasons why you may not want a security gateway to participate in Path MTU:

- A firewall sits between the security gateway and the source of packets needing VPN services. This would prevent the source from receiving security gateway ICMP messages indicating that fragmentation is needed.
- The source of packets needing VPN services does not fragment packets, even when notified by a security gateway ICMP message.
- A router in the network is outdated and will not send an ICMP need fragmantation message, or will not send a message at all.

The symptom of either of these situations would be that a network sniff indicates the security gateway is sending a fragmentation-needed ICMP message, but the traffic initiator is retransmitting the original packet.

To configure the Path MTU:

1. From the **Configure>Advanced>Path MTU**, to display the Path MTU values.
2. Select the **On** radio button to enable Path MTU Discovery, or select the **Off** radio button to disable Path MTU Discovery.

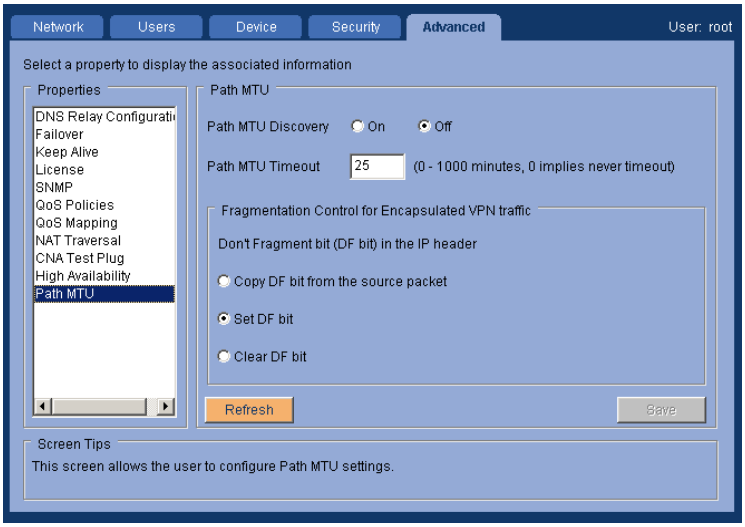
3. Enter the **Path MTU Timeout** value.

   The path MTU timeout value is the number of minutes the SG will remember the new MTU learned for a path. When the timeout expires, the SG will attempt to send the maximum configured packet size. The default value is 0. The timeout value 0 means that the path MTU will never timeout.

4. In the **Fragmentation Control for Encapsulated VPN Traffic** area, select the appropriate Do Not Fragment (DF) bit property.

- **Copy DF bit from the source packet.** If this DF property is selected, the DF bit from the source IP header is copied to the VPN traffic. When Path MTU is enabled (On), the copy DF bit from the source packet property is the default behavior. When Path MTU is disabled (Off), the copy DF bit from the source packet property is a configurable behavior.
- **Set DF bit.** If this DF property is selected, the DF bit for VPN traffic is always on. When Path MTU disabled (Off), the set DF bit property is a configurable behavior.
- **Clear DF bit.** If this DF property is selected, the DF bit for the VPN traffic is always off. When Path MTU disabled (Off), the clear DF bit property is a configurable behavior.

5. When you want to send the configuration to one or more SGs, click **Save**.



Chapter 8: Upgrading the VPNos software

Use the Upgrade function to perform an upgrade of the current system image executing in the security gateway. Upgrade is a stand-alone utility that uses a CGI process to download a new firmware image from a host computer into the FLASH memory of the security gateway.

Preparing to upgrade

To perform the upgrade, you must first obtain a copy of the latest security gateway firmware image from the Avaya download site http://.support.avaya.com. This software requires you to have an active service agreement, and is password protected. You must send an e-mail to VPNsupport@avaya.com to request a password before you begin the download. Include your company name and telephone number, the serial number of the security gateway, and the name and product number of the release that you want to download.

You can download the file to any computer that can connect to the target security gateway through either the public port or private port on the security gateway.

Only administrators with root privileges can upgrade the security gateway's firmware.

Upgrading the security gateway

When you have your password, go to the Avaya Support Technical Database Web page at http://support.avaya.com to get the upgrade.

1. From the Avaya support site, click **VPN and Security** and select the appropriate security gateway type to download.
2. Click **Software Downloads** and follow the links. To begin the download, click the link that matches the type of security gateway you want to upgrade.
3. Select **Save** to save this file on the computer.
4. Browse to find the directory you want to save the VPNos download. Click **Save**.
5. Double-click the downloaded zip file to begin extracting the VPNos upgrade files. The password screen appears.

6. Enter the password that you received from Avaya technical support. The firmware will be downloaded to the designated directory.

   Note:

   If “Authentication to the device fails,” the password was not recognized. Reenter the password. If any other error appears, contact your customer support center for help.

7. From the web interface, click **Upgrade**. The Security Gateway Upgrade Utility screen appears.
8. Enter your **User ID** (administrative ID) and **password**. Click **Login**.
9. Navigate to the directory where you saved the extracted VPNos upgrade files and select the subdirectory where the security gateway firmware is stored. Select the firmware file. Click **Open**.
10. Click **Upgrade Now**. The security gateway factory default access to the public port is enabled.
11. When the new image is downloaded and saved to FLASH memory, a message is displayed indicating the upgrade was successful.
12. Click **Reboot**.
13. Close the Upgrade window.

Appendix A: Preconfigured firewall rules

General

The security gateway contains a powerful multi-layer inspection engine to provide extensive filtering capabilities, essential for a full-time connection to the Internet. You can configure your own rules, but, as a convenience in setting up the Firewall on the security gateway, predefined general firewall rules (templates) can be selected to protect the public, private, semi-private, DMZ, and maintenance zones.

These predefined firewall rules are grouped into security levels of high, medium, and low. One firewall security level is applied to the security gateway, and the rules for each zone are enforced according to the type of zone being protected. How the template rules are applied to a zone are described in this appendix.

The Firewall engine uses a rule-based method of packet filtering, where the priority of the rule is determined by its position in the list (highest is first priority).

Note: The *common services* referred to in this appendix include all of the following:

- Ping
- FTP control, Passive Data FTP
- SSH, TELNET
- HTTP, HTTPS
- POPS, IMAP, SMTP, and NNTP

High Security. - Selecting high security enforces a set of rules that try to protect the security gateway itself and the internal network zones. For high security the following policy is defined:

- Private networks and management networks are considered internal networks, and can initiate connections to access common services on the Internet.
- Except for access to the DMZ zone, traffic initiated from the Internet is denied.
- VPN outgoing and incoming traffic is allowed.
- DMZ common services can be accessed from all interfaces. The DMZ network cannot initiate any traffic.
- The semi-private zone is not considered completely trusted. Access from semi-private to private zones is allowed only if it is VPN traffic. All other incoming traffic is blocked.

Medium Security. - Selecting medium security enforces the same security policy as high security for all zones except the semi-private zone. The semi-private zone with medium security is trusted the same as the private zone. That is, the same security policy that is enforced on the private zone is enforced on the semi-private zone. In medium security, semi-private zone can also access all the resources in the private zone.

Low Security. - Selecting low security enforces the same security policy as specified for medium and the access from the internal network to the Internet is not limited to only the common services. Access to all TCP and UDP services are allowed.

VPN only. - Selecting VPN-only security enforces the security policies as specified at the domain and device levels. The security policies are enforced at the tunnel end point. VPN traffic is given a higher inbound and outbound priority than IKE traffic.

None. - Selecting None as the firewall template allows all traffic through the gateway. Security gateway policies are not enforced.

The details about rules and what types of traffic are allowed and denied for each level and zone are in the following tables.

Public zone firewall templates

The public network interface provides connection to the Internet and the security gateway functions as the firewall/VPN gateway.

Usually the public interface has the strongest firewall policy. Few incoming packets are allowed and outgoing packets are allowed only for commonly used services.

The public high security rules are enforced for both incoming and outgoing packets as follows.

Incoming traffic to the public zone allowed include:

- VPN packets from private, DMZ, Management or Semi-private zones
- ICMP unreachable packets
- Publicly accessible DMZ services allowed include ping, FTP, SSH, Telnet, HTTP, HTTPS, POP3, IMAP, SMTP, NNTP and DNS.

All other incoming traffic is blocked.

Outgoing traffic from the public zone allowed include:

- Outgoing VPN traffic
- ICMP unreachable
- Ping from any IP to any
- DNS from any IP to any
- Common services originating from all internal networks, private, DMZ, management and semi-private.

All other outgoing traffic is blocked.

The medium security policy for the public zone is the same as that of the high security policy.

The low security policy allows all the traffic allowed for medium security. In addition, all TCP, UDP packets from all networks are allowed to go out.

Table 7: Public high and medium security firewall rules

Rule Name	Action	Source	Destination	Service	Direction	Zone	Keep State	Description
InBoundPublicAccess	Permit	Any	PublicIP	IKE_IN IPSEC_NAT_T_IN AH/ESP ICMPDestUnreach	In	Public	no	Permit incoming VPN traffic and ICMP unreachable packet
InBoundPublictoDMZAccess	Permit	Any	DMZNet	ICMPEchoReq(PING) FTP-Ctrl/PassiveFTP SSH/TELNET HTTP/HTTPS DNS-TCP/DNS-UDP POP3/IMAP/SMTP NNTP	In	Public	Yes	Permit incoming traffic to DMZ network
InBoundPublicBlockAll	Deny	Any	Any	Any	In	Public	No	Deny the rest of traffic
OutBoundPublicAccess	Permit	PublicIP	Any	IKE_OUT IPSEC_NAT_T_OUT AH/ESP ICMPDestUnreach	Out	Public	no	Permit outgoing VPN traffic
OutBoundPublicGeneralAccess	Permit	Any	Any	ICMPEchoReq(PING) FTP-Ctrl/PassiveFTP SSH/TELNET HTTP/HTTPS DNS-TCP/DNS-UDP POP3/IMAP/SMTP NNTP	Out	Public	Yes	Permit traffic with the services to go out. The traffic can come from any network.
OutBoundPublicBlockAll	Deny	Any	Any	Any	Out	Public	No	Deny the rest of traffic

Table 8: Public low security firewall rules

Rule Name	Action	Source	Destination	Service	Direc-tion	Interface	Keep State
InBoundPublicAccess	Permit	Any	PublicIP	IKE_IN IPSEC_NAT_T_IN AH/ESP ICMPDestUnreach	In	Public	no
InBoundPublictoDMZAccess	Permit	Any	DMZNet	ICMPEchoReq(PING) FTP-Ctrl/PassiveFTP SSH/TELNET HTTP/HTTPS DNS-TCP/DNS-UDP POP3/IMAP/SMTP NNTP	In	Public	Yes
InBoundPublicBlockAll	Deny	Any	Any	Any	In	Public	No
OutBoundPublicAccess	Permit	PublicIP	Any	IKE_OUT IPSEC_NAT_T_OUT AH/ESP ICMPDestUnreach	Out	Public	no
OutBoundPublicGeneralAccess	Permit	Any	Any	ICMPEchoRequest(PING) ALL TCP ALL UDP	Out	Public	Yes
OutBoundPublicBlockAll	Deny	Any	Any	Any	Out	Public	No

Table 9: Public VPN-only firewall rules

Rule Name	Action	Source	Destination	Service	Direc-tion	Interface	Keep State
InBoundPublicAccessVPNData	Permit	Any	Public-IP	ESP IPSEC_NAT_T_IN	In	Public-IP	Yes
OutBoundPublicAccessVPNData	Permit	Public-IP	Any	ESP IPSEC_NAT_T_IN	Out	Public-IP	Yes
InBoundPublicAccessVPNKeyMgmt	Permit	Any	Public-IP	IKE-IN IKE-AVAYA-IN	In	Public-IP	Yes
OutBoundPublicAccessVPNKeyMgmt	Permit	Public-IP	Any	IKE-IN IKE-AVAYA-IN	Out	Public-IP	Yes
InBoundPublicICMP	Permit	Any	Public-IP	ICMPDESTUNREACHABLE ICMPTIMEEXCEEDED	In	Public-IP	No
OutBoundPublicICMP	Permit	Public-IP	Any	ICMPDESTUNREACHABLE	Out	Public-IP	No
InBoundPublicBlockAll	Block	Any	Any	Any	In	Public	No
OutBoundPublicBlockAll	Block	Any	Any	Any	Out	Public	No

Private zone firewall templates

The private network interface provides connection to the private/corporate LAN. Private zones are considered trusted networks and because of this most traffic is allowed.

The private high security rules are enforced for both incoming and outgoing packets as follows.

Any incoming traffic from the private zone is allowed except traffic that is destined to the management zone.

For outgoing traffic to the private zone, traffic initiated from DMZ is strictly denied. All other traffic is allowed.

The private medium security rules and the low security rules are the same as the private high security rules.

Table 10: Private high security firewall rules

Rule Name	Action	Source	Destina-tion	Service	Direc-tion	Zone	Keep State	Description
InBoundPrivateToMgmtDenyAccess	Deny	Any	ManagementNet	Any	In	Private	No	Traffic to ManagementNet is denied.
InBoundPrivatePermitAll	Permit	Any	Any	Any	In	Private	Yes	Permit VI/VMGR and VP, clear traffic to PUBLIC
OutBoundPrivateDMZSemiPriDenyAccess	Deny	DMZNet	Any	Any	Out	Private	No	Deny traffic from DMZNet and SemiPrivateNet
OutBoundPrivatePermitAll	Permit	Any	Any	Any	Out	Private	Yes	Permit incoming VPN

Table 11: Private medium security firewall

Rule Name	Action	Source	Destination	Service	Direction	Zone	Keep State	Description
InBoundPrivateDenyAccess	Deny	Any	ManagementNet	Any	In	Private	No	Traffic to ManagementNet is denied.
InBoundPrivatePermitAll	Permit	Any	Any	Any	In	Private	Yes	Permit WI/VMGR and VPN, clear traffic to PUBLIC
OutBoundPrivateDenyAccess	Deny	DMZNet	Any	Any	Out	Private	No	Deny traffic from and SemiPrivateNet
OutBoundPrivatePermitAll	Permit	Any	Any	Any	Out	Private	Yes	Permit incoming VPN

Table 12: Private low security firewall rules

Rule Name	Action	Source	Destination	Service	Direction	Zone	Keep State	Description
InBoundPrivateDenyAccess	Deny	Any	ManagementNet	Any	In	Private	No	Traffic to ManagementNet is denied.
InBoundPrivatePermitAll	Permit	Any	Any	Any	In	Private	Yes	Permit WI/VMGR and VPN, clear traffic to PUBLIC
OutBoundPrivateDenyAccess	Deny	DMZNet	Any	Any	Out	Private	No	Deny traffic from and SemiPrivateNet
OutBoundPrivateDenyAll	Permit	Any	Any	Any	Out	Private	Yes	Permit incoming VPN

Semi-private zone firewall templates

A semi-private network interface provides connection to a network whose equipment can be made physically secure, but whose medium is vulnerable to attack (such as a Wireless network used within a corporation's Private network infrastructure).

Because wireless connections cannot be easily controlled, strict firewall policy should be enforced on the semi-private interface to limit the access from the semi-private zone to VPN traffic. Clear traffic to Private and Management zones is not allowed. Common services to DMZ are allowed and clear traffic to Public is allowed.

The semi-private high security rules are enforced for both incoming and outgoing packets as follows.

Incoming traffic to the semi-private zone allowed includes:

- VPN traffic. The VPN tunnel endpoints could be semi-private IP or Public IP.
- Ping, DNS
- ICMP unreachable packets

The following clear traffic is allowed

- The source is semi-private and the destination is DMZ servers, with the following common services: PING, FTP control, Passive Data FTP, SSH, Telnet, HTTP, HTTPs, POP3, IMAP, SMTP, and NNTP.
- The destination is Public and the services are FTP, SSH, Telnet, HTTP, HTTPS, POP3, IMAP, or ICMPechorequest.

All other incoming traffic is blocked.

Outgoing traffic to the semi-private zone that is allowed includes

- Any allowed traffic from other zones
- VPN traffic

Table 13: Semi-private high security firewall rules

Rule Name	Action	Source	Destination	Service	Direction	Zone	Keep State	Keep State
InBoundSemiPrivateVPNAccess	Permit	Any	SemiPrivateIP PublicIP	IKE_IN IPSEC_NAT_T_IN AH/ESP ICMPDestUnreach	In	SemiPrivate	No	Permit incoming VPN and ICMP unreachable
InBoundSemiPrivatePingAccess	Permit	Any	SemiPrivateIP PublicIP	ICMPEchoReq(PING)	In	SemiPrivate	Yes	Permit incoming PING
InBoundSemiPrivatetoDMZAccess	Permit	Any	DMZNet	ICMPEchoReq(PING) FTP-Ctrl/PassiveFTP SSH/TELNET HTTP/HTTPS DNS-TCP/DNS-UDP POP3/IMAP/SMTP NNTP	In	SemiPrivate	Yes	Permit incoming services to DMZNet
InBoundSemiPrivateDenyAccess	Deny	Any	DMZNet PrivateNet ManagementNet SemiPrivateIP	Any	In	SemiPrivate	No	Deny traffic to PrivateNet, ManagementNet and DMZNet
InBoundSemiPrivatetoPublicAccess	Permit	Any	Any	ICMPEchoReq(PING) FTP-Ctrl/PassiveFTP SSH/TELNET HTTP/HTTPS DNS-TCP/DNS-UDP POP3/IMAP/SMTP NNTP	In	SemiPrivate	Yes	Permit clear traffic to Public network/VPN traffic with Public IP as tunnel endpoint
InBoundSemiPrivateBlockAll	Deny	Any	Any	Any	In	SemiPrivate	No	Deny the rest of traffic
OutBoundSemiPrivateVPNAccess	Permit	SemiPrivateIP PublicIP	Any	IKE_OUT IPSEC_NAT_T_OUT AH ESP ICMPDestUnreach	Out	SemiPrivate	No	Permit outgoing VPN traffic.
OutBoundSemiPrivatePermitAll	Permit	Any	Any	Any	Out	SemiPrivate	Yes	Permit everything with Keep state. (For any traffic initiated from Private/ ManagementNET)

Table 14: Semi-private medium security firewall rules

Rule Name	Action	Source	Destination	Service	Direction	Zone	Keep State	Description
InBoundSemiPrivateDenyAccess	Deny	Any	ManagementNet	Any	In	SemiPrivate	No	Traffic to ManagementNet is denied.
InBoundSemiPrivateVPNAccess	Permit	Any	SemiPrivateIP PublicIP	IKE_IN IPSEC_NAT_T_IN AH/ESP ICMPDestUnreach	In	SemiPrivate	no	Permit incoming VPN traffic and ICMP unreachable packet
InBoundSemiPrivatePermitAll	Permit	Any	Any	Any	In	SemiPrivate	Yes	Permit WI/ VMGR and VPN, clear traffic to PUBLIC
OutBoundSemiPrivateDenyAccess	Deny	DMZNet	Any	Any	Out	SemiPrivate	No	Deny traffic from DMZNet
OutBoundSemiPrivateVPNAccess	Permit	SemiPrivateIP PublicIP	Any	IKE_OUT IPSEC_NAT_T_OUT AH/ESP ICMPDestUnreach	Out	SemiPrivate	no	Permit outgoing VPN traffic
OutBoundSemiPrivateDenyAll	Permit	Any	Any	Any	Out	SemiPrivate	Yes	Permit incoming VPN

Table 15: Semi-private low security firewall rules

Rule Name	Action	Source	Destination	Service	Direction	Zone	Keep State	Description
InBoundSemiPrivateDenyAccess	Deny	Any	ManagementNet	Any	In	SemiPrivate	No	Traffic to ManagementNet is denied.
InBoundSemiPrivateVPNAccess	Permit	Any	SemiPrivateIP PublicIP	IKE_IN IPSEC_NAT_T_IN AH/ESP ICMPDestUnreach	In	SemiPrivate	no	Permit incoming VPN traffic and ICMP unreachable packet
InBoundSemiPrivatePermitAll	Permit	Any	Any	Any	In	SemiPrivate	Yes	Permit WI/ VMGR and VPN, clear traffic to PUBLIC

Table 15: Semi-private low security firewall rules (continued)

Rule Name	Action	Source	Destination	Service	Direction	Zone	Keep State	Description
OutBoundSemiPrivateDenyAccess	Deny	DMZNet	Any	Any	Out	Semi Private	No	Deny traffic from DMZNet
OutBoundSemiPrivateVPNAccess	Permit	SemiPrivateIP PublicIP	Any	IKE_OUT IPSEC_NAT_T_OUT AH/ESP ICMPDestUnreach	Out	Semi Private	no	Permit outgoing VPN traffic
OutBoundSemiPrivateDenyAll	Permit	Any	Any	Any	Out	Semi Private	Yes	Permit incoming VPN

2 of 2

DMZ zone firewall templates

The Demilitarized Zone (DMZ) network interface is typically used to allow Internet users access to some corporate services without compromising the private network where sensitive information is stored. For all the services setup in the DMZ, access is allowed from any network, including Public, Private, Management and Semi-private. Because the DMZ is not a trusted network, all outgoing traffic is blocked.

The same security rules are enforced for high security, medium security, and low security. The DMZ high security rules are enforced for both incoming and outgoing packets as follows.

Incoming traffic from the DMZ zone are denied.

Outgoing traffic to the DMZ zone allowed includes

- Packets from the following networks: private, management, semi-private, and the destination is the servers with the common services.

Table 16: DMZ high, medium, and low security firewall rules

Rule Name	Action	Source	Destination	Service	Direction	Zone	Keep State	Description
InBoundDMZBlockAll	Deny	Any	Any	Any	In	DMZ	No	Deny the rest of traffic

1 of 2

Table 16: DMZ high, medium, and low security firewall rules (continued)

Rule Name	Action	Source	Destination	Service	Direction	Zone	Keep State	Description
OutBoundDMZAccess	Permit	Any	DMZNet	ICMPEchoReq(PING) FTP-Ctrl/PassiveFTP SSH/TELNET HTTP/HTTPS DNS-TCP/DNS-UDP POP3/IMAP/SMTP NNTP	Out	DMZ	Yes	Permit outgoing traffic with the services
OutBoundDMZBlockAll	Deny	Any	Any	Any	Out	DMZ	No	Deny the rest of the traffic

2 of 2

Management zone security

Management interface connection can be configured to simplify network deployments to eliminate enterprise network dependencies on switches or routers.

The Management zone is a trusted network similar to the Private zone. Outgoing traffic is allowed, but incoming traffic is restricted. Only traffic initiated by the security gateway is allowed.

High, medium and low security rules are the same.

Incoming

All traffic is allowed to come in from the management network.

Outgoing

Only packets from the Management IP to the Management zone are allowed.

Table 17: Management high, medium, and low security firewall rules

Rule Name	Action	Source	Destination	Service	Direction	Zone	Keep State
InBoundManagementInterfacePermitAccess	Permit	Any	ManagementIP	Any	In	Management	No
InBoundManagementPermitAll	Permit	Any	Any	Any	In	Management	Yes
OutBoundManagementInterfaceAccess	Permit	ManagementIP	Any	Any	Out	Management	No
OutBoundManagementBlockAll	Deny	Any	Any	Any	Out	Management	No

Converged Network Analyzer template

The converged network analyzer (CNA) template is a selection of firewall rules that can be configured to permit non-VPN CNA traffic to travel through the network when the security gateway is setup as a firewall device. Typically, the security gateway will not allow CNA traffic to travel through the device, however; when the CNA template is configured and added to existing firewall rules CNA traffic is allowed.

The CNA template can be combined with any public zone firewall template security level - high, medium, low, or none.

Table 18: Converged network analyzer firewall rules CNA high, medium, and low firewall rules

Rule Name	**Action**	**Source**	**Destination**	**Service**	**Direc-tion**	**Zone**	**Keep State**
InBoundCNAPing	Permit	Any	Public-IP	ICMP-EchoRequest	In	Public	Yes
InBoundCNARTP	Permit	Any	Public-IP	CNA-RTP	In	Public	No
InBoundCNATestPlug	Permit	Any	Public-IP	CNA-TestPlug	In	Public	No
OutBoundCNAPing	Permit	Public-IP	Any	ICMP-EchoRequest	Out	Public	Yes
OutBoundCNAALLTCP	Permit	Public-IP	Any	Any-TCP	Out	Public	Yes
OutBoundCNAALLUDP	Permit	Public-IP	Any	Any-UDP	Out	Public	Yes
InBoundCNABlockUDPICMPUnreachable	Deny	Any	Public-IP	Any-UDP	In	Public	No

Appendix B: Error messages

Table 19 describes the most common error messages.

Table 19: Error messages

Message	Meaning	Action
Authentication Failed: no such user	A username is not configured	Verify the username and retry to log in again.
Authentication Failed: incorrect password	The password is invalid for the username.	Verify the username and retry to log in again.
Required information missing. Configure this user.”	A user tried to log in as default VPN user, and a default user is not configured.	Configure the user as part of the default VPN.
Invalid VSU IP Address/DNS Name”	During a secure VPN configuration download process, the IP address or the DNS name of the remote security gateway was invalid.	Confirm your configuration for the correct address or the DNS name.
Unable to connect to VSU	During a secure VPN configuration download process, the connection to the remote security gateway failed.	Check configuration and network connectivity.
VSU connection has been timed out	During the creation of a secure VPN connection, the connection timed out.	Restart the connection and log in again.
validateVPN: VPN: {VPN name} Option RC5 not supported for Phase2 Encryption	RC5 encryption is not supported for IPSec.	Review the type of encryption that is configured in the IPSec proposal for the VPN.
validateVPN: VPN: {VPN name} Option NULL not supported for Phase2 Encryption	NULL encryption is not supported for IPSec.	Review the type of encryption that is configured in the IPSec proposal for the VPN.

Appendix C: Command line interface

This appendix describes the Avaya security gateway command line interface (CLI) architecture and conventions, and describes how to access the security gateway to perform limited configuration and monitoring procedures. The configuration procedure involves establishing a serial connection to access the CLI of the security gateway.

Security levels

The Avaya security gateway CLI has two security access levels, administrator (Root) and monitor.

- Use the admin (Root) level to configure and monitor the operation of the security gateway.
- Use the monitor level to view the configuration and monitor the operation of the security gateway.

Conventions used

The following conventions are used in this chapter to convey instructions and information:

- Mandatory keywords are in **bold type**.
- Variables that you supply are in angle brackets <>.
- Optional keywords are in square brackets [ ].
- Alternative but mandatory keywords are in braces { } and separated by a vertical bar |.
- If you enter an alphanumeric string of two words or more, enclose the string in inverted commas, ‘ ,.
- Information displayed on screen is displayed in `text` font.

Keyboard shortcuts and environment

The CLI contains a simple text editor. Table 20 lists the functions of the editor, and the keyboard commands to perform the functions.

Table 20: Keyboard shortcuts

Keyboard	Functions
Ctrl-L	Clear the screen leaving the current line at the top
Ctrl-A	Move the cursor to the start of the current line
Ctrl-E	Move the cursor to the end of the current line
Ctrl-B or the Left Arrow key	Move the cursor one character to the left
Ctrl-F or the Right Arrow key	Move the cursor one character to the right
Esc-F	Move the cursor forward to the end of the next word
Esc-B	Move the cursor back to the start for the current or previous word
Ctrl-P or the Up Arrow key	Fetch the previous command from the history list
Ctrl-N or the Down Arrow key	Fetch the next command from the history list
Ctrl-H or the Backspace key	Delete the character to the left of the cursor
Ctrl-D	Delete the character at the cursor
Ctrl-X	Delete all characters on the current line
Ctrl-K	Delete all text from the cursor to the end of the line
Ctrl-U	Delete all text from the cursor to the start of the line

Table 21: Environment

Environment	Description
color	Enable or disable the colored display. Default setting is ON. Not all terminals support this feature.
context-prompt	Enable or disable context prompt
context-switch	Enable or disable automatic context switching
show	Disable the current settings of CLI environment
timeout <3..3600>	Sets CLI inactivity timeout to a specified value in seconds. A zero value disables the timeout. The default value is 3600.

Command syntax

Commands are case sensitive. You must enter uppercase characters and lowercase characters exactly as they appear.

The general format of a command is: **<command-name><parameters>**

Where **<command-name>** is a keyword or a sequence of keywords separated by spaces, and **<parameters>** is a parameter or a sequence of parameters.

Each parameter is defined in either of the following forms: **<name>**, **<value>**, or **<name><value>** where <name> is a keyboard preceded by a hyphen (-) symbol (without intervening spaces).

Each parameter **<name>** in the command syntax must be unique.

The value specifies the parameter to modify or view in the CLI.

Command line prompt

When a CLI client logs in to the security gateway, the CLI application displays the following screen:

```
                    Welcome to SG208
Login: yyy
Password: xxxxx
Password accepted.
SG (super)[1]#>
```

Five factors determine the appearance of the command line prompt:

- **Host name of the CLI entity**. The host name is used as the prefix of the command prompt.
- **Login user name**. The login user name is either the root user or monitor user.
- **Context level**. A context level is shown in a parentheses (), and only on a local context level.
- **Command number**. Each time a command is entered, an entry is created in the history buffer. The command number is the index into the history buffer for the current command. The command number is shown in square brackets [].
- **The prompt sign #**.

CLI commands

General

The following commands are associated with CLI operations rather than system configurations.

Command	Description
!<num>	Execute the specified ‘number’ of the command in the history buffer.
!!	Execute the previous command in the history buffer.
exit	Exit from CLI.

Command	Description
quit	Quit from CLI.
history	Display the command history.
?	Display commands and command trees.
top	Go to the top level of CLI.
up	Go up one level from current level.
version	Display the version and time of the system build.
help	Same as ?.
help -all	Display all commands the current CLI supports.
help <keyword>	Display the usage and description of a given command.
help -editing	Display the command line editing keys.
quicksetup <staticip|ipdhcp|ippppoe|show> [**-ip**<ip address>] [**-mask**<netmask>] [-gateway <gateway>] [**-user**<user-name>] [**-password**<password>] [**-superuser**<superuser-name>] [**-superpasswd**<superuser-password>] [**-date** ”<newdate>”]	Perform Quick Install from the security gateway. The superuser account is used for VPNmanager’s centralized management. The new date string must be in one of the forms: “mm/dd/yyyy hh:mm:ss”, “mm/dd/yyyy.”, or “hh:mm:ss” for the 24-hour clock. For option staticip, IP-address, mask, and gateway mandatory parameters. For option dhcp, there are no mandatory parameters. For option PPPoE, the user and password are mandatory parameters.
ping [**-c**<count>] [**-s**<packet-size>] [**-ip**<ipaddress>]	Ping a host or gateway.

System commands

Command	Description
system date [**-s** ”<newdate>”] | **[-u**]	Shows or sets the system date and time. Option: -s set the date and or time of this system to <newdate> string. The newdate string must be in one of the forms: ”mm/dd/yyyy hh:mm:ss”, ”mm/dd/yyy”, or ”hh:mm:ss” for the 24 hour clock. -u show the time and date in Coordinated Universal Time (also known as Greenwich Mean Time) instead of in the local time.
system show -info	Displays general system information. Without options, it will show the basic system and network configuration. -info shows basic system information.
system reboot	Reboots the system.
system shutdown	Shuts down the system.

Configure commands

Command	Description
configure arp show	Display the system ARP table.
configure show event log	Display the current event log messages.
configure firewall show <log | rules | statistics>	Display firewall log messages, rules, or statistics.

Command	Description
configure interface set <**public** | **private**> [**-mode** <ipstatic | ipdhcp | ippppoe>] ipdhcp-relay [**-ip**<IPaddress>] [**-mask** <netmask>] [**-gateway <gateway**>] [**-user** <username>] [**-password** <password>] [**-serverip** <DHCP relay serverIP>] [**-mtu** <MTU (296 - 1500)>]	Set interface parameters for public or private port. Options: public — Set the interface parameters for public port. Mandatory parameters for this option are: mode<ipstatic |ipdhcp| ipppoe>. <ipstatic> -ip <ipaddress> -mask <netmask> - gateway <gateway> <ipdhcp> <ipppoe> -user <username> - password <password> private —- Set the interface parameters for the private port. Mandatory parameters for this option are: -mode <ipdhcp-relay | ipnone> -ip <ipaddress> - mask <netmask> -serverip <dhcp relay server IP> **Note:** *setting up the private port will cause the local DHCP server to be turned off*.
configure interface media set <public | private> <autoselect | 10 | 100 | 1000> **-duplex** <full>	Set interface media parameters.
configure path mtu set <path - mtu **on** | **off** > <path - mtu - timeout (0 - 1000), 0 = NEVER> df - bit set | copy | clear	Set interface media parameters.
configure show path mtu	Display the current path mtu settings.
configure interface show **<traffic | all public | public-backup | private | semi-private | dmz | management.>**	Displays interface statistics. Shows the basic interface statistics without any options. Options: -traffic Show the interface traffic statistics -public Show the public port statistics -public-backup Show the public-backup port statistics -private Show the private port statistics -semi-private Show the semi-private port statistics -dmz Show the dmz port statistics -management Show the management port statistics.

Command	Description
configure route add <IPaddress><netmask><gateway IP>	Add a route entry.
configure route delete <IPaddress><netmask>	Delete a route entry.
configure vpn show **<ipsecsa | ikesa | packets | statistics |** <vpnname>**>**	Display one of the VPN options.
configure **remoteaccess addrpool** <release_all | report>	Release all chached CCD client IP addresses.
configure authsource set <local | radius>	

Diagnostic commands

Command	Description
diagnostics **show all**	Display all system diagnostics in one report.
diagnostics show <**date_time**>	Display the current date and time.
diagnostics show <**uptime**>	Display the duration of VSU uptime.
diagnostics show <**vsuinfo**>	Display the VSU information.
diagnostics show <**kern_diag**>	Display the kernel diagnostic information.
diagnostics show <**route_table**>	Display the routing table information.
diagnostics show <**flow_table**>	Display the traffic flow routing table information.
diagnostics show <**sa_table**>	Display the VPN security association table information.
diagnostics show <**if_table**>	Display the interfaces table information
diagnostics show <**if_config**>	Display the interface configuration.
diagnostics show <**sock_table**>	Display the socket table information.
diagnostics show <**net_mem**>	Display the network memory information.
diagnostics show <**sys_mem**>	Display the system memory information.
diagnostics show <**intr_state**>	Display the interrupt state information.
diagnostics show <**fw_state**>	Display the firewall state information.

Command	Description
diagnostics show <**proc_table**>	Display the process table information.
diagnostics show <**pronto_stats**>	Display the protocol statistics information.
diagnostics show <**route_stats**>	Display the route statistics information.
diagnostics show <**sys_stats**>	Display the system statistics information.
diagnostics show <**sys_state**>	Display the system state information.
diagnostics show <**addr_map**>	Display the address map report information.
diagnostics show <**sec_proc_stats**>	Display the security processor statistics information.
diagnostics show <**ike_sa**>	Display the IKE security associations information.
diagnostics show <**arp_table**>	Display the ARP table information.
diagnostics show <**vpn_stats**>	Display the VPN statistics information.
diagnostics show <**ha_stats**>	Display the high availability statistics information.
diagnostics show <**rip_stats**>	Display the RIP statistics information.
diagnostics show <**vtdr_stats**>	Display the VTDR statistics information.
diagnostics show <**h323_stats**>	Display the H323 statistics information.
diagnostics show <**event_log**>	Display the event log information.
diagnostics show <**xml_cfg**>	Display the SGXML configuration information.
diagnostics show <**kern_state**>	Display the kernel state information.
diagnostics show <**proto_stats**>	Display the protocol statistics information.
diagnostics show <**split_tunnels**>	Display the split tunnel information.

Glossary

A

Aggressive mode An IKE mechanism used in the first phase of establishing a security association. Aggressive mode accomplishes the same authentication negotiating goal between clients as Main mode but faster (three packets versus six).

AH/ESP In an IPSec packet, the Authentication Header (AH) and Encapsulation Security Payload (ESP) header. IKE VPNs authenticate IP packets using either an ESP header as defined in draft-ietf-ipsec-esp-v2-03.txt, or AH as defined in IETF draft-ietf-ipsec-auth-header-04.txt.

Alarms When a security gateway in the VPN reports an alarm condition, details about the alarm including type, timestamp, and the originating security gateway can be found in the VPNmanager main screen Alarm pane.

Authentication Generic

The process of ensuring that the data received is the same data that was sent from the source.

Local

Local Authentication is used in non-dynamic VPNs (VPNs not using RADIUS or a directory server (LDAP) as the authentication database). Here, the user is authenticated from the database stored in the security gateway's flash memory.

RADIUS

RADIUS Authentication uses an external RADIUS server and database for user authentication.

LDAP

LDAP Authentication uses the designated directory server database for user authentication.

B

Brute Force Attack A hack attack that attempts to recover a cryptographic key by trying all reasonable possibilities.

C

CCD Client Configuration Download. The protocol used to download the VPN session parameter configuration file from the security gateway to the remote client as part of a successful authentication when the security gateway is configured for Local Authentication.

CARP Common Address Redundancy Protocol. This protocol is similar to Virtual Router Redundancy Protocol (VRRP).

Certificate Authority A trusted company or organization that serves as a repository of digital certificates. Once a CA accepts your public key (with some other proof of identity), others can then request verification of your public key.

Certificates Issuer

Issuer Certificates also reside in the security gateway and are used to authenticate the other side. For example, if the VPNmanager server presents a certificate for an SSL session, the security gateway must have an Issuer Certificate that can verify the VPNmanager's certificate is valid. Devices wishing to use IKE must be validated with an Issuer Certificate. All Issuer certificates are public.

My Certificates

My Certificates is a list of nine (0 through 8) certificates that exist inside the security gateway and are used to identify the security gateway to an opposite endpoint. Requires generation of a public/private key pair where the private key never leaves the security gateway.

Signing

Similar to the security gateways Issuer Certificates necessary to verify the VPNmanager Certificate, the Signing Certificates are for the VPNmanager Console to verify the security gateway Certificate.

Certificate Revocation List (CRL), checking Certificate Revocation List checking looks to a directory server (maintained by CAs) to validate a new certificate by searching a list of no longer valid digital certificates.

D

DCI Direct Configuration Interface is a VPNet Technologies, Inc. proprietary protocol developed to facilitate passing setup and configuration data between the VPNmanager console and the security gateway. DCI traffic can pass in the clear if the LAN on which they both reside is behind a firewall, or over SSL if not.

DES Data Encryption Standard (DES) is a block-cipher algorithm created by IBM used to rapidly encrypt large amounts of data at one time. The technique uses a 56-bit key and operates on blocks of 64 bits. See Triple DES.

Diffie-Hellman A popular mechanism used to define the mathematical parameters used during IKE negotiations. Group 1 specifies use of a 768 bit modulus, Group 2 a 1024 bit modulus (Group 2 is "more secure").

Digital Certificate An electronic document used to establish a company's identity by verifying its public key. Digital Certificates are issued by a certificate authority.

Domain Name Service (DNS) The network service that converts text-based names into numeric IP addresses and vice-versa.

Domains, VPN A VPN Domain is a collection of Virtual Private Network devices that compose a Virtual Private Network.

Dynamic VPNs Dynamic VPNs are VPNs that can be readily scaled as dictated by business demands. As the remote client user population grows, the authentication and session configuration information for each new user must necessarily also grow. By maintaining this information not in the security gateway's flash memory but on a dedicated network host device, the number of users becomes unlimited. Two techniques of achieving this functionality normally used are LDAP or RADIUS.

Dyna Policy An Avaya VPN term relating to a dynamic configuration download of VPN session security parameters to the remote client computer upon connection to a security gateway. This technique assures maximum security in a VPN session.

E

Encapsulation The process of placing the contents of one packet into that of payload of another packet.

Extranet security gateway It is possible to create a Group associated with a VSU that is not managed by your company's VPNmanager. This happens when creating "extranets," or VPNs between partner corporations. In an extranet, each corporate network uses VPN components that are managed separately by each company's system administrator.

F

Firewall A network device acting as a filter to restrict access to private network resources from the public. Filtering typically is based on the types of packets exchanged between two devices on the network.

H

Heartbeat A special VPN packet broadcast by a primary security gateway used to facilitate the resilient tunnel function.

I

IKE (Internet Key Exchange) A key-management protocol, IKE defines procedures and packet formats to establish, negotiate, modify and delete Security Associations (SAs) and defines payloads for exchanging key generation and authentication data. These formats provide a consistent framework for transferring key and authentication data which is independent of the key generation technique, encryption algorithm and authentication mechanism. Now combined with Oakley to form IKE.

IP Groups IP Groups are a convenient means of managing your VPN resources. IP Groups are collections of IP network mask pairs associated with security gateways, hosts, and workstations located behind the security gateway.

IPSec The network cryptographic protocols for protecting IP packets.

ISAKMP The key-management protocol used in conjunction with IPSec.

Issuer Certificates See Certificates, Issuer

L

LAN Local Area Network

LDAP Lightweight Directory Access Protocol is a simplified version of the standard X.500 distributed directory model standard. LDAP specifies how a client accesses a directory server. LDAP has emerged as a favored protocol since it also handles key management with key and certificate storage.

Lifetime, Key Payload key lifetime defines the extent to which a single set of cryptographic keys is used when applying VPN services to IP packets. Key lifetimes can be defined by either the amount of data acted on by this single set of cryptographic keys or the amount of time these keys are used before a key change. The more often a key is changed, the “more secure” the system, although performance may be affected by frequent key changes.

LZS Lempel-Ziv-Stac, a compression algorithm.

M

Mask Pairs A network address and network mask. Two 4-byte pairs. For example, 1.1.1.0 and 255.255.255.0.

MIB - Enterprise The enterprise-specific Management Information Base in the VPNet Technologies, Inc. security gateways. The Enterprise MIB information allows the administrator to obtain basic monitoring information such as the network table, packet counter, and general information regarding the security gateway using third party software.

MIB-II (Non-Enterprise) The non-enterprise specific Management Information Base in the VPNet Technologies, Inc. security gateways. The MIB-II allows the administrator to obtain basic monitoring information such as device ethernet information, routing and ARP tables, SNMP traps, packet statistics, and other general information regarding the security gateway using third party software.

Migration A utility by which an existing VPNmanager database is converted into an LDAP database for compatibility with VPNmanager 3.0 or later.

My Certificates See Certificates, My Certificates

N

NAT Network Address Translation (NAT) is a mechanism that allows private (non-routable) networks to connect to public (routable) networks.

Not My security gateway If you are creating an extranet, choose “Not My VSU” as the Group’s associated VSU. Doing this enables the “IP Address of Extranet VSU” entry field. Enter the IP address of the your partner company’s VSU. This is required if any VPNs serviced by a VSU-1100, VSU-1010 or VSU-10 are in tunnel mode.

O

Oakley A key exchange protocol used in IPSec as part of the Internet Key Exchange protocol.

P

Packet Filter Hardware or software mechanism used in firewalls to discards packets based on the contents of the packet headers.

Perfect Forward Secrecy Perfect Forward Secrecy defines a parameter of ISAKMP in which disclosure of long-term secret keying material does not compromise the secrecy of the exchanged keys from previous communications. Enabling Perfect Forward Secrecy is “more secure”. See the IETF draft-ietf-ipsec-oakley-02.txt for more information on Perfect Forward Secrecy.

PKI Public Key Infrastructure is the organization of certificate issuers and certificate management processes.

Preshared Secret Preshared Secret is the simplest key management method used to construct a VPN. Authentication key exchanges between security gateways in the VPN are based on a single pre-shared secret known to all security gateways.

Public Key Certificate A special block of data used to identify the owner of a particular public key. It describes the value of a public key, the key’s owner, and the digital signature of the issuing authority.

R

RADIUS Remote Authentication Dial In User Service is a client/server remote user authentication protocol in widespread use.

Resilient Tunnel A mechanism of providing automatic backup of a secure tunnel between two endpoints. In practical application, a primary security gateway sends a “heartbeat” packets to a secondary security gateway every few seconds (configurable). Should the primary security gateway fail, the secondary security gateway will stop receiving the heartbeat packets. When this happens, the secondary security gateway switches over and takes on the role of primary security gateway.

S

SA Security Association is an IPSec agreement between to communicating devices on which authentication and encryption algorithms (including key lifetimes) are used.

Session Key A cryptographic key that has a finite life expectancy, typically for a single session.

Signing Certificates See Certificates, Signing

SKIP — **Simple Key-Management for Internet Protocol** – SKIP differs from ISAKMP in the area of negotiation. In SKIP, all of the security parameters are identified within each SKIP secured packet in the form of a SKIP header. The cryptographic algorithms defining the VPN services in a SKIP VPN are predefined, instead of negotiated dynamically as in ISAKMP.

Smart Card — A special type of credit-card like authentication device (assigned to an individual user) that offers a greater degree of private network access security.

Split Tunneling — Split tunneling allows the remote client to simultaneously maintain both a VPN (secure) connection and a clear connection. This function is active by default, however, disabling Split Tunneling turns it off allowing only secure VPN traffic from the remote client's computer. Control of Split Tunneling is normally set when the Dyna-Policy configuration download to the remote client's computer occurs.

SSL — Secure Sockets Layer is a protocol that provides authentication for servers and browsers as well as secure communications between a web server and browser. Used by the VPNmanager Console to communication with the security gateways and the VPNmanager Server.

Syslog — Syslog enables each security gateway in the VPN to provide logging data to a specified destination for historical purposes.

T

Triple DES — A cryptographic algorithm based on DES that encrypts a block of data three times with different keys.

U

User Groups — User Groups are logical groups in which individual VPN user members reside. User Groups have a single-level hierarchy. Users can belong to more than one User Group.

V

VPN — Virtual Private Network. A VPN allows the sending of sensitive, secured data through an unsecure network like the Internet by using dynamically created connections between member of the VPN.

Index

Numerical

A

B

C

D

E

F

G

H

I

K

L

M

N

P

Q

R

S

T

U

V

W

Z