Avaya™ SG203 and SG208 Security Gateway Hardware Installation Guide

670-100-101
Issue 1
June 2003

Copyright 2003, Avaya Inc.
All Rights Reserved

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.

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 Lists*, which includes escalation phone numbers within the USA.
- Outside the United States, click *Escalation Lists* then click *Global Escalation List*, which includes phone numbers for the regional 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.

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

Table of Content

Preface 7

Contacting Technical Support . . . 7
Documentation . . . 7

Chapter 1 *Introduction* 9

Functional overview . . . 10
Additional features . . . 11
VPNmanager . . . 11
Security . . . 11
Performance . . . 12
Plug-and-Play installation . . . 12
Hardware components . . . 13
Ethernet ports . . . 14

Chapter 2 *Installing SG203 and SG208 Security Gateway* 15

Site requirements . . . 15
Environmental requirements . . . 15
Site power considerations . . . 15
Equipment requirements . . . 16
Physical installation . . . 16
Required tools . . . 17
Safety recommendations . . . 17
Desktop . . . 17
Rackmount . . . 18
Overview of front panel . . . 19
Console port . . . 19
Multi-interface ports . . . 20
Connecting the SG203/SG208 security gateway to the network . . . 20

Chapter 3 *Setting up the security gateway for configuration* 23

Connecting to the private port . . . 23
Performing the quick setup . . . 24

Index 29

Preface

The Avaya™ SG203 and SG208 Security Gateways are dedicated hardware-based network security devices designed to provide overlay security on an IP data network.

This guide describes the Avaya SG203 and SG208 Security Gateway and how to install and preconfigure these devices. It is recommended that you read the entire installation guide before installing the security gateway.

Contacting Technical Support

Technical support is available to registered users of the Avaya security gateway products.

Domestic support

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

International support

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

Documentation

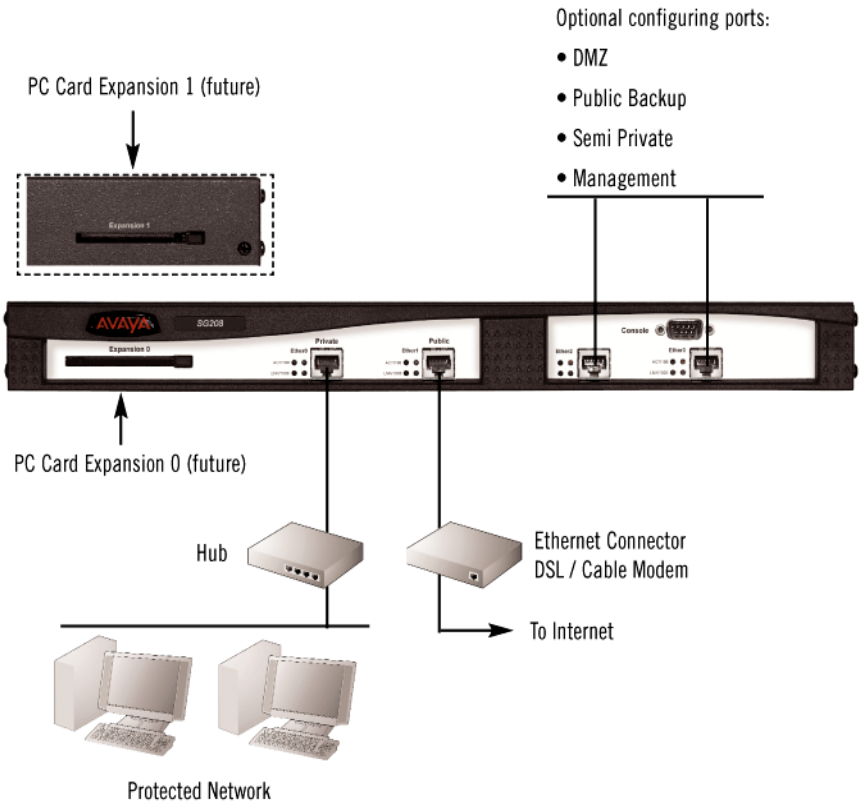
The security gateway documentation includes both the Hardware Installation Guide and the Security Gateway Configuration Guide for VPNos 4.3. You can down load these guides from http://www.support.avaya.com. Navigate to Product Documentation, VPN and Security.

Chapter 1 Introduction

The Avaya ™ SG203 and SG208 Security Gateways are high-performance integrated firewall, security zone, and IPSec VPN gateway devices. They are designed to provide the high capacity, scalability and reliability required by your networks for IPSec/firewall services in one unit or multiple units for enterprise headquarter locations requiring a rack mountable device.

The security gateway is easy to configure and can either be managed locally from the Web interface or remotely using Avaya™ VPNmanager.

Figure 1 Typical SG203/SG208 security gateway installation



Functional overview

The SG203 and SG208 security gateways are dedicated hardware-based network security devices designed to provide overlay security services on an IP data network. The security gateway sits behind an edge router and has auto-detecting ethernet interfaces on the public and private ports.

The security gateway's primary function is to perform IPSec and firewall security services to protect enterprise networks and to secure data being sent over shared IP networks. The security gateway establishes an Internet Key Exchange (IKE) protocol session with its IPSec peer to perform an authentication and to negotiate the security associations (SAs) that are used to secure the session. Once the successful

negotiation is completed data can then be encapsulated in IPSec tunneling packets that can only be decrypted by the peer on the other end of the IPSec tunnel.

Additional features

Table 1 Additional features

Parameter	Specification
Encryption	DES, Triple DES, and AES hardware encryption. DES uses a 56-bit key. Triple DES uses three 56-bit independent keys for an effective key length of 168 bits. AES is a symmetric 127 bit block data encryption technique. AES can be used in place of DES. All weak and semi-weak keys are automatically discarded.
Authentication	Keyed MD5™ Message Digest (RFC 1321) HMAC-MD5 and HMAC SHA-1 (RFC 2104)
Key Management	ISAKMP (Internet Security Association Key Management Protocol). Supports network address translation for firewall support.
User Authentication	CHAP, PAP

VPNmanager

Avaya VPNmanager is an optional Avaya application that lets network managers define, configure and manage VPNs from any location. Large networks would want to use VPNmanager to do distributed managed firewall rules as well as VPN management across the network.

Security

The SG203 and SG208 security gateway employes cryptographic algorithms and keys powerful enough for the most sensitive business communications to provide data stream privacy. It supports DES and Triple DES, and AES encryption, as well as the ISAKMP key management standard.

Data authenticity is assured by using HMAC-MD5™ or HMAC-SHA-1 packet signatures to reject altered or forged packets. All security mechanisms employed by the security gateway conform to IPSec standards, in order to provide interoperability and broaden the use of VPN technology.

Performance

For maximum network flexibility, the SG203 security gateway supports four 10/100BASE-T Ethernet interfaces, and the SG208 supports four 10/100/1000BASE-T Ethernet interfaces.

When packets are encrypted and authenticated according to IPSec protocol guidelines, additional bytes, in the form of IPSec headers, must be added to packets. In many cases, the additional packet overhead imposes a performance penalty in return for security. The extra bytes tend to lengthen packets and reduce the throughput (measured in packets per second). The overhead depends on the IPSec policy and could be up to 63 bytes.

Table 2 SG203/208 performance specifications

	SG203	SG208
IKE Sessions	3000	8000
IPSec Sessions	12,000	16,000
Subnets supported	2	1
Firewall TCP/UDP Sessions	200,000	300,000
VPNremote users (Default/Max)	100/3000	100/8000
Site to Site (Default/Max)	50/300	100/1000
Protected FW/VPN Devices	3000	8000

Plug-and-Play installation

The auto sensing interfaces of the security gateway enables installation into any Ethernet network. By default, the security gateway functions as a DHCP client on the public interface and as a DHCP server on the private interface. Immediately after receiving IP connectivity, the network administrator can locate the security gateway via https://192.168.1.1 on

the private interface. The administrator enters the name as *root* and the password as *password* for the user's credentials. The quick set up guides the network administrator through the minimal network configuration.

Hardware components

Each of the major components are shown in Figure 2 and Figure 3 .

Figure 2 Front panel

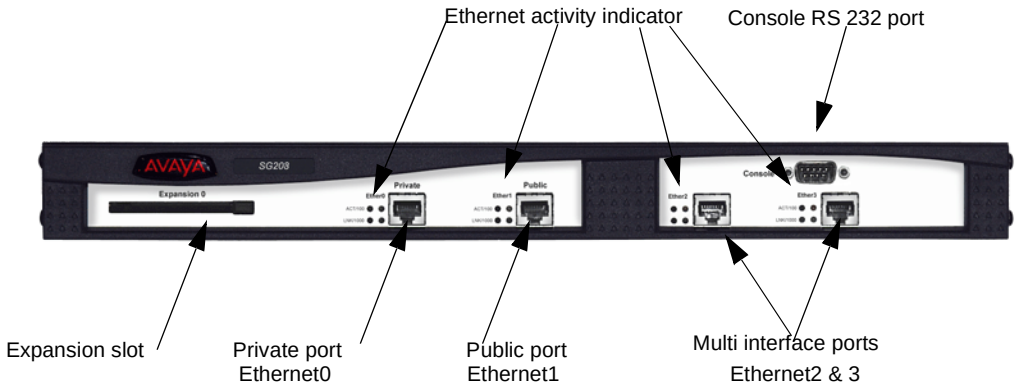


Figure 3 Back panel

Table 3 Physical specifications

Parameter	SG203	SG208
Dimensions	17”W x 18.5”D x 1.75”H (46.9cm x 43.1cm x 4.4cm)	17”W x 18.5”D x 1.75”H (46.9cm x 43.1cm x 4.4cm)
Weight	17 pounds (7.7 Kilograms)	17 pounds (7.7 Kilograms)
LAN Interface	Four 10/100/Base-T Ethernet	Four 10/100/1000Base-T Ethernet
Management Interface	RS-232	RS-232

Ethernet ports

Etnernet0 is reserved for the Private port and Ethernet1 is reserved for the Public port. Ethernet2 and Ethernet3 are software configurable and can be used for fail-over, DMZ, or other functions.

Each Ethernet port has status indication LEDs that show whether the link is active.

Chapter 2 Installing SG203 and SG208 Security Gateway

This chapter provides instructions for the physical installation of the SG203 and SG208 security gateways, including rack mounting, placement, and connection to the network.

Site requirements

This section describes the requirements your site must meet for safe installation and operation of the security gateway. Ensure that your site is properly prepared before beginning installation.

Environmental requirements

The security gateway devices are intended for use in a normal office environment. For more extreme conditions, verify that temperature, humidity, and power conditions meet the following specifications:

- Temperature range - 32° to 104° F (0° to 40°C)
- Relative humidity - 5-95%, non-condensing

Site power considerations

Check the power at your site to ensure that you are receiving “clean” power (free of spikes and noise). Install a power conditioner, if necessary.

Table 4 Electrical specifications

Voltage	100-240 VAC
Input frequency	47-63 Hz
AC input current	3.5 Amps

Equipment requirements

The security gateway devices shipping carton should contain:

- 1 ea. Security Gateway
- 2 ea. Cat5e cable
- 1 ea. Power supply
- 1 ea. Null modem cable for console connection
- 1 set Rack mount kit including two mounting brackets and screws for attaching the brackets to the security gateway.

  Hardware required to mount the unit to the rack must be provided by the customer.
- 1 ea. Quick Start Guide

To install and use the security gateway in a typical network, the customer must supply the following:

- Router, DSL, cable or ISDN modem, providing connectivity to a WAN such as the Internet
- A workstation on the LAN to communicate with the security gateway, installed with a Java-enabled (JDK1.1.8 or later), 128-bit encryption-capable browser, either Internet Explorer 5.5 or later or Netscape 6.2 or later.

Physical installation

The security gateway can be placed on a desktop or mounted in a rack. It is easy to install and requires a screwdriver for rack mounted devices.

Required tools

The security gateway chassis can be mounted in a standard 19-inch equipment rack. Rack mounting requires a Phillips-head screwdriver, the device rack mount bracket kit, and four screws to match the rack. (Screws for attaching the mounting brackets to the chassis are not provided.) Instructions for rack mounting are provided in the section "Rackmount" on page 18.

Safety recommendations

When using the SG203/SG208 security gateway devices, follow these safety guidelines:

- Keep the chassis area clear and dust-free during and after installation
- Keep the ventilation gratings clear of any blockages
- Do not rest equipment in excess of 10 pounds on top of the chassis
- Disconnect all power before mounting or unmounting a unit from an equipment rack
- Never assume power is disconnected from a circuit, always check

Circuit Breaker (15A) Warning

WARNING: *This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that a fuse or circuit breaker no larger than 120 VAC, 15A U.S. (240 VAC, 10A international) is used on the phase conductor (all current-carrying conductors).*

SELV Circuit Warning

WARNING: *The Ethernet 10/100/1000BASE-T, serial console, and auxiliary ports contain safety extra-low voltage (SELV) circuits. Do not connect to a telephone line.*

Desktop

To install on a desktop, allow sufficient depth in the rear for cabling and on the sides for ventilation flow.

Rackmount

The SG203 and SG208 security gateways can be mounted in a standard 19-inch equipment rack. The location of the chassis and the layout of your equipment rack or wiring room are extremely important for proper system operation. Equipment placed too close together, inadequate ventilation, and inaccessible panels can cause system malfunctions and shutdowns and can make system maintenance difficult.

The following information can help you plan an acceptable equipment rack configuration.

- Enclosed racks must have adequate ventilation. Ensure that the rack is not overly congested because each unit generates heat. An enclosed rack should have louvered sides and a fan to provide cooling air.
- When mounting a chassis in an open rack, ensure that the rack frame does not block the ventilation grates. If the chassis is installed on slides, check the position of the chassis when it is seated all the way into the rack.

To attach the device to a standard 19-inch equipment rack:

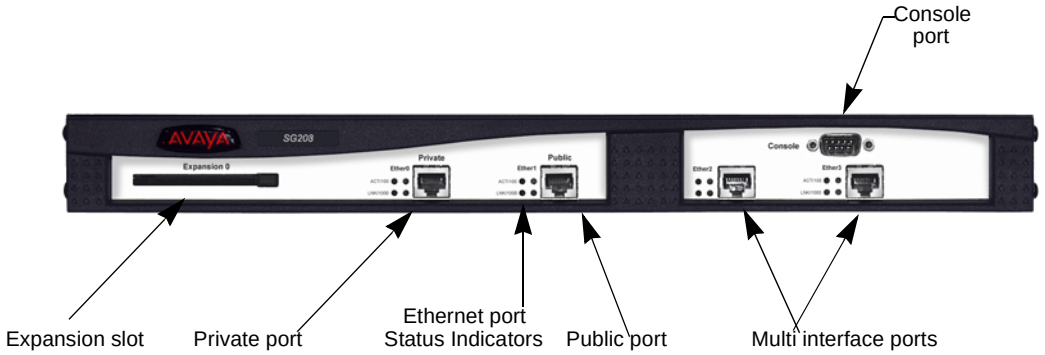
1. From one side of the device, remove the four front side screws.
2. Using the screws provided with the bracket, attach the bracket to the device.

Figure 4 Attaching the Rack Mount Brackets

3. Repeat bracket installation on the other side.
4. Install the device into a standard 19-inch rack, using screws that fit the rack (not provided).

Overview of front panel

Figure 5 Front panel of the security gateway



Console port

The console port accepts an RS-232 DB-9 connection from an asynchronous ASCII terminal or a PC running terminal emulation software. The connection requires a null modem cable which is supplied.

The communication settings for a device interfacing with the console port are provided in Table 5.

Table 5 Terminal settings

Parameter	Setting
Baud	9600
Data Bits	8
Parity	None
Stop bits	1
Flow control	None

Multi-interface ports

Four ports are available on the security gateway, public, private and two other interface ports that are not designated.

The public port provides an interface to the public Internet network, while the private port provides an interface to the private local network. The other two could be used for public-backup, semi-private, DMZ, or management interface zones.

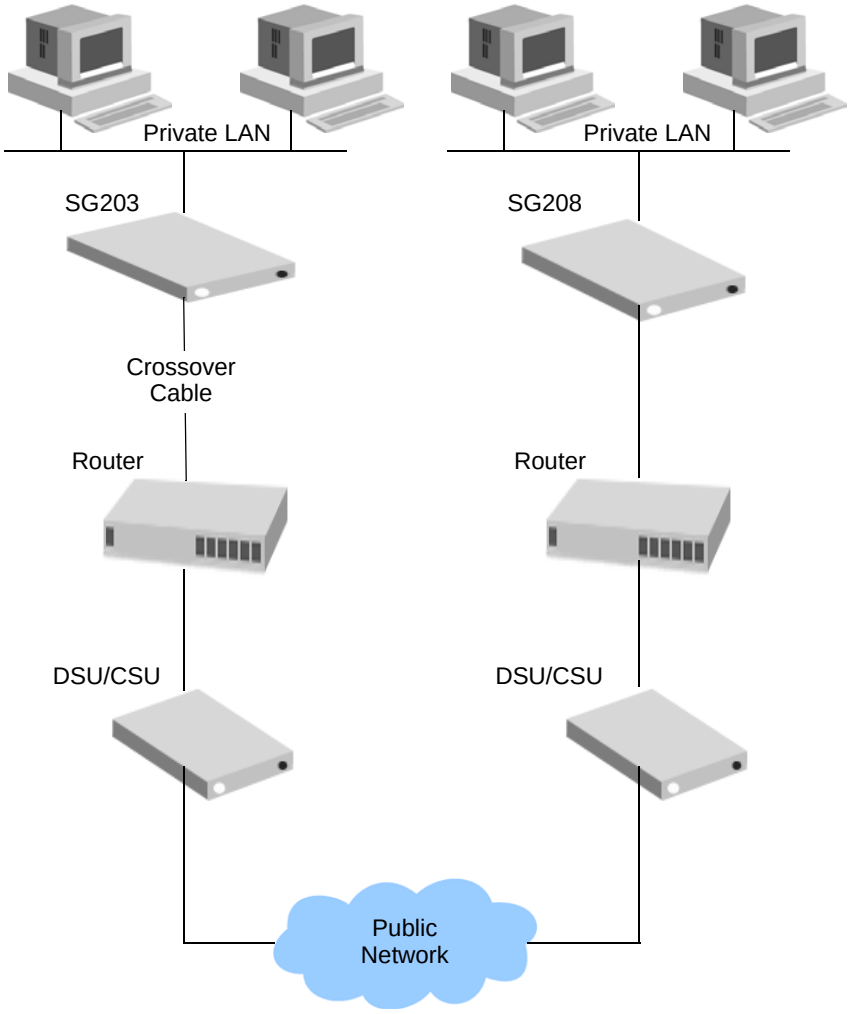
The SG203 requires a crossover cable when connecting to a router and uses a straight-through cable when connecting to a hub or switch. The SG208 can use any type of cable (crossover or straight-through) when connecting to a hub, switch, or router.

NOTE: *To realize maximum performance when operating at the 1000 Base-T rate, it is necessary to use CAT5e cables, shipped with the device. Standard CAT5 cables are not rated for full Gigabit data rates (generally, this is problematic when cable run lengths greater than 100 meters are involved).*

Connecting the SG203/SG208 security gateway to the network

The supplied Cat5e cables are used to connect the security gateway to the public network and the private LAN. Figure 6 shows a typical network using the SG203 and SG208 security gateway.

Figure 6 Example of two security gateway's hardware installations



1. Connect one end of the Cat5e cable to the public port (Ethernet1) on the security gateway. Connect the other end to the router's Ethernet port, ethernet connector on the DSL, or the cable modem. For the SG203, use the crossover cable. (Figure 6).

   See "Multi-interface ports" on page 20 about using Cat5e cables.

***Note**: If DHCP related functionality (DHCP server on the private interface and DHCP client on the public network) disrupts your network, change the default settings via the console port, prior to plugging in the ethernet cables.*

2. Connect one end of the Cat5e straight-through cable to the private port (Ethernet0) on the security gateway. Connect the other end to the LAN hub or switch.

   Note: A crossover cable is required if the SG203 security gateway is connected directly to a workstation.

3. Connect the power cable to the security gateway and then plug it in to an AC outlet.

4. Power on the security gateway and proceed to Chapter 3, Setting up the security gateway for configuration.

The following are the default values for the security gateway.

- DHCP Client public interface is enabled
- DHCP Server private interface is enabled
- Private Interface IP address is 192.168.1.1
- Administrative user name is *root*
- Password is *password*

Chapter 3 Setting up the security gateway for configuration

This chapter describes how to set up the security gateway addressing and remote connectivity capabilities. This preliminary configuration is performed using a browser on your workstation connected to the security gateway's private port. When the security gateway is initially installed and connected to the local LAN, it is provisioned with a default IP address for the DHCP server (serving the private port), allowing access to the device through a Web browser on a workstation.

The following procedure assumes that the security gateway has been physically installed on the network, according to the instructions provided in Chapter 2, Installing SG203 and SG208 Security Gateway.

The security gateway quick setup consists of two basic steps:

1. Establishing connectivity between a workstation or IP device on your local network with the security gateway's private port
2. Setting up the security gateway's public port to reach the Internet

Through the Web interface, you can assign a static IP address for the public port, a password, server addresses, DHCP settings, and a default gateway. Once this has been done, the security gateway can be completely configured and incorporated into your Virtual private Network either by using the Web interface locally, or using Avaya VPNmanager from a central location.

Connecting to the private port

From the workstation's control panel, select your TCP/IP network component for your Ethernet controller. In the IP Address window select "enable the setting" to "Obtain an IP address automatically" .

Restart your workstation, if the operating system asks you to do so. As your workstation restarts, it automatically obtains its required IP address/ mask and default router IP address from the security gateway.

NOTE: *Unless you have other DNS servers at your local site, it is recommended that the Windows DNS and WINS server lists be empty. The DNS server built into the security gateway should normally be the sole DNS server that users see.*

Performing the quick setup

Quick Setup collects and preconfigures the essential information required to remotely configure and manage the security gateway.

Note: *If the security gateway is to be configured and managed locally, see the Security Gateway Configuration Guide for the VPNos, to perform a comprehensive device configuration.*

The Quick Setup wizard collects the necessary information to communicate with the remote VPNmanager application through the security gateway's public port. The following information is required to complete the quick setup:

- The type of addressing to be used on the security gateway's public port, either Static IP Addressing, Dynamic Addressing (DHCP), or PPPoE. Typically, DSL connections use PPPoE and cable modems use DHCP. The default is DHCP
- A network mask for the above
- A default route. This is the service provider's router used only if Static IP Address is selected
- The user name and password, if your connection to your ISP is PPPoE

To connect to the security gateway

1. From a workstation on the private side of the security gateway, open your browser and type into the location field one of the following:
   - https://sg.private
   - https://192.168.1.1 (security gateway default address)
2. Click **Yes,** to accept the security alert message. The security gateway login window appears.

Figure 7 Security Gateway Login Window

3. Enter the User Name, **root** and the Password, **password**.

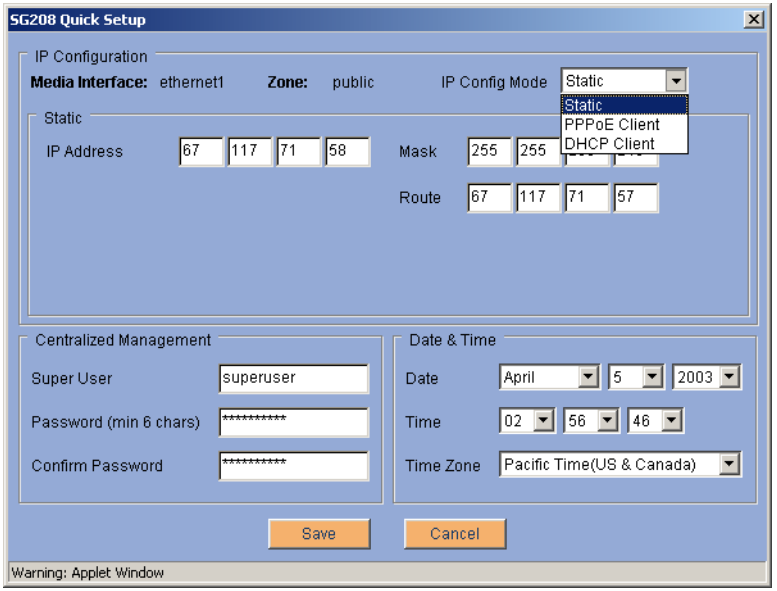
   Click **Log In**, when it is highlighted.

4. The first time you connect to the security gateway, two sequential pop-up messages appear over the main screen. The first is a password change alert that advises you to change the factory default password. Change the default password to a secure password.

5. The next alert message indicates that the security gateway has not yet been configured.

   Click **OK**, to launch the Quick Setup wizard.

Figure 8 Quick Setup Dialog



6. The Quick Setup wizard dialog appears. In the IP Configuration area, select one of the following IP Config Modes.
   - **Static Addressing**. If you are going to use static addressing on the public port, click the **Static Addressing** radio button and enter your IP address, network mask, and default route information.
   - **DHCP**. If you plan to use DHCP, the public port automatically obtains its address from a DHCP server. This method is typical for cable modem connections.
   - **PPPoE**. This method is typically used with DSL connections. Click the **PPPoE** radio button and enter your PPPoE user name and password.
7. Depending on the IP config mode selected, complete the fields that populate the dialog.
   - For Static, enter the IP address, mask and route
   - For PPPoE, enter the user name and password

8. In the **Centralized Management** area, if VPNmanager is used, enter the superuser name and password.

9. In the **Date & Time** area, enter the date, time, and time zone.

   A 24-hour clock is used. For example, 13:00:00 is equivalent to 1:00 PM.

10. Click **Save** and then click **Log Out** from the main page to log of the Web interface.

NOTE: *When you use Log out, you are prompted to save any unsaved changes before exiting. If you close your browser, unsaved changes are lost.*

You now have entered enough information to allow the security gateway to be accessed over the Internet. The remaining configuration process can be completed remotely, using VPNmanager, or if the security gateway is managed locally, you can continue the configuration. Refer to the Security Gateway Configuration Guide for VPNos.

Index

A
admin name 25
AES 11
AES encryption 11
authentication specification 11

B
back panel 20

C
cat5e cables 20
CE marks 4
compliance 2
configuring
  static addressing,DHCP,PPPoE 26
connecting the SG203/SG208 to network 20
connecting to private port 23
connections
  router 21
console port 19
contacting
  technical support 7

D
default settings 22
DES 11
documentation 7

E
electrical specifications 16
electromagnetic compatibility standards 3
email support 7
encryption specification 11
environmental requirements 15
equipment
  provided by Avaya 16
  provided by customer 16

H
hardware components 13
humidity specification 15

I
installation
  desktop 16
  rackmount 16
IPSec standards 11

L
log out 27

P
password 25
performance 12
performance specification 12
phone support 7
plug-and-play installation 12
power 15

Q
quick setup 24

R
rackmount installation procedure 18
recommendations
  safety 17
required tools 17
requirements
  environmental 15
router connections 21
RS-232 19

S
safety recommendations 17
security 11
SHA1 11
specifications
  authentication 11
  encryption 11
  key management 11
standards
  electromagnetic compatibility 3

T
technical support 7
temperature range 15
tools
  rackmount 17
triple DES 11

U
user authentication 11

W
warranty 2
world wide web support 7