



## Avaya SG203 and SG208 Security Gateways

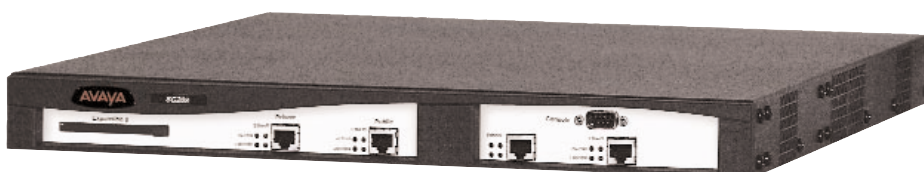
The Avaya SG203 and SG208 Security Gateways deliver security as an integrated component of Avaya enterprise IP telephony solutions. Incorporating advanced stateful firewall, VPN, bandwidth management, and IP telephony management capabilities, the SG203/208 allow large enterprises, contact centers, and hosted IP telephony networks to securely extend a full range of IP telephony and communications solutions to mobile workers, remote call agents, telecommuters, branch offices, and call center partners.

### Firewall Security for Converged IP Telephony and Data Networks

The Avaya SG203 and SG208 Security Gateways integrate VoIP firewall, multi-interface security zone, IPSec VPN gateway, and IP Telephony configuration and support services into a compact 1U chassis featuring four Fast Ethernet interfaces (SG203) or four Gigabit Ethernet interfaces (SG208). Both gateways also feature two industry-standard CardBus/PCMCIA slots that will accept a variety of future interface-expansion cards, providing a low-cost solution for expanding the system with additional interfaces or adding wireless gateway capability.

Two interface ports are reserved as private (network to be secured/protected from outside intrusion and attack) and public interfaces (outside network that is considered inherently insecure). The others can be configured for the following types of logical interfaces:

- **DMZ (Demilitarized Zone):** Part of corporate network accessible from the public network, but is not considered part of the internal private network.
- **Semi-Private Network:** Used for media such as wireless LAN, where the network is considered part of the protected network, but the media may be vulnerable to attack. The semi-private interface can be configured to provide IPSec VPN encryption and user authentication security.
- **Back-Up Public:** Back-up interface to the primary public interface for use in fail-over scenarios.
- **Management Interface:** Used to set-up a secure, isolated management network.





- Firewall Security for Converged IP Telephony and Data Networks
- Scalable and Flexible VPN for Remote Access, Site-to-Site, and Wireless LANs
- IP Telephony Support
- Centralized Firewall and VPN Management

An advanced Stateful Multi-Layer Inspection (SMLI) Firewall features predefined templates that make it easy to set-up and customize firewall policies. Separate firewall policies can be applied for each interface, allowing the enterprise to deploy firewall security zones within the corporate network for enhanced security. A set of common network services is provided, and custom network services/objects can be easily defined for use in both firewall and QoS policies. Firewall rules can be individually enabled to track state information on TCP/UDP/ICMP packet flows and can be user-configured with advanced state timers. In addition, DoS attack protection can be enabled to mitigate common DoS service attack signatures such as Ping of death, IP Spoofing, Smurf, Tear Drop, WinNuke, and Buffer Overflow.

For enterprises deploying remote telecommuters with IP phone access, or remote contact center agents, the security gateways provide enhanced firewall security protection using an H.323 application proxy to connect IP telephony connections across the secured firewall. Acting as an intermediary, the proxy intelligently validates and filters H.323 RAS (Registration, Admission, and Status) and signaling exchanges, identifies negotiated ports, and dynamically opens and closes these ports in the firewall only as required to support VoIP connections.

The application proxy also supports H.323 IP trunk connections, enabling enterprises to deploy secure perimeter VoIP firewall protection for multi-site IP telephony networks, distributed contact centers, or to secure hosted IP telephony services. For added flexibility, the application proxy provides H.323 Network Address Translation (NAT/pNAT) services that will operate on both the Layer 3 address and the embedded H.323 address, greatly simplifying the deployment of distributed IP telephony solutions by providing enterprises with

the flexibility of using NAT to help manage multi-site addressing across a public network.

The SG203/SG208 Security Gateways can be easily integrated as an adjunct to an existing firewall or VPN gateway to provide support for dynamic IP telephony firewall traversal. This allows enterprises to deploy IP telephony applications while minimizing impact on existing network security infrastructure and policies.

### **Scalable and Flexible VPN for Remote Access, Site-to-Site, and Wireless LANs**

The SG203/SG208 are full-featured VPN gateways supporting site-to-site and remote access applications. For networks deploying wireless LANs, available interfaces on the SG203/SG208 can be configured to initiate/terminate VPN tunnels, allowing the gateway to be used simultaneously to secure WAN and internal wireless LAN networks.

To help ensure low latency for real-time applications such as IP Telephony, the SG203 and SG208 feature hardware IPsec acceleration using DES, 3DES, or AES encryption. IPsec NAT traversal is also supported, allowing VPN connections to be established between security gateways across a network even if NAT is performed by an intervening device.

The base SG203 gateway is licensed to support 100 remote access VPN users and 50 site-to-site VPN connections, and can be easily scaled via licensing to a maximum of 3000 remote access users or 300 site-to-site VPN connections. The base SG208 gateway is licensed to support 100 remote access VPN users and 100 site-to-site VPN connections, and is scalable to a maximum of 8000 remote access users or 1000 site-to-site VPN connections.

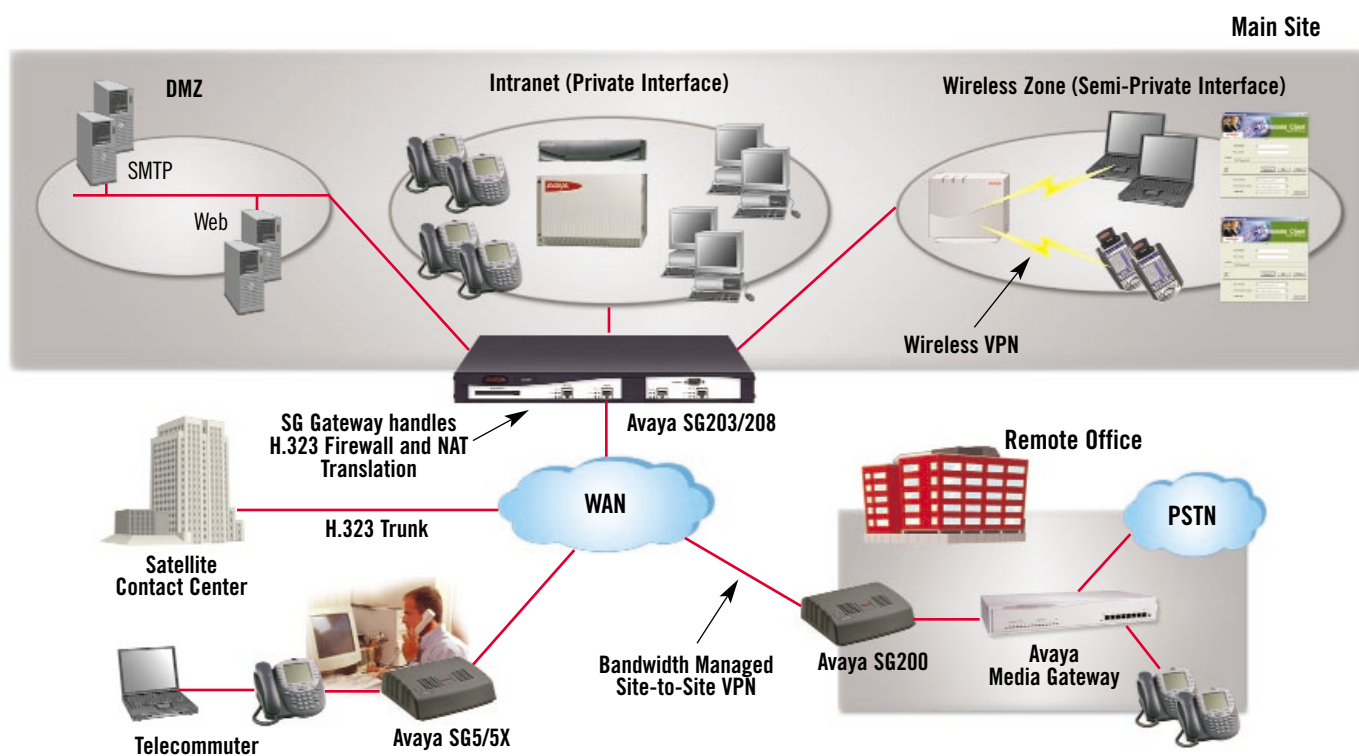
## IP Telephony Support

An integrated CBQ (Class-Based Queuing) bandwidth manager provides granular control over the allocation of available bandwidth to different types of applications. The bandwidth manager supports up to four separate classes of traffic, which can be specified based on a combination of DiffServ Code Point (DSCP) values, TCP/IP services, and networks. Each class can be configured with an allocation of bandwidth, and optionally with the ability to borrow available bandwidth from a common pool.

To simplify IP telephony deployments, the bandwidth manager automatically identifies Avaya IP telephony

streams, and places these streams into the highest-priority class. The gateways can also take advantage of IP-based quality of service support over the WAN by marking IPSec packets with DSCP values, allowing differential QoS support in an MPLS or diffserv-supported environment.

The SG203/SG208 can also be configured as DHCP servers with IP telephony extensions to provide IP addresses to trusted network devices and IP telephones. In this mode, the SG pushes IP address, TFTP Server and Gatekeeper configuration parameters down to Avaya IP Telephones, eliminating the need for a separate server.





## Centralized Firewall and VPN Management

Avaya VPNmanager® Software lets network managers define and manage VPN and firewall policies, configure QoS and VoIP settings, upgrade firmware, and manage remote user access policies from a centralized location.

Built on a client/server architecture that combines a Java console and an LDAP directory server, VPNmanager decouples the management console from the underlying directory server, which provides several benefits:

- **Scalability:** Management console and directory server can reside on separate, dedicated servers within the network to provide better performance for updating and configuring large numbers of security gateways.
- **Role-Based Management:** Security management can be distributed to multiple administrators across multiple console platforms. VPNmanager allows the enterprise to define policy-based roles and privileges for each administrator, and provides security for all management traffic via SSL.

Instead of a device-centric model, VPNmanager Software is built on a policy-based architecture. By focusing on security policy rather than individual device management, administration of large-scale networks is simplified. If the administrator makes a change to a VPN policy, VPNmanager Software automatically identifies the affected security gateways. The administrator can then have the configuration updates delivered by simply pushing the update button.

This distributed approach also applies to firewall management. VPNmanager firewall policy management includes domain firewall rules, device firewall rules, and firewall templates. The software provides multiple firewall templates that can be used as a general rule set or as a starting point for creating a customized firewall template.

Administrators can then apply these templates at the domain level for all security gateways, for a specific gateway, or for a defined gateway group. Device-level firewall rules can be separately defined to create custom policies for an individual gateway.

For local device management, all security gateways feature a Web graphical interface accessible from a Web browser and secured via SSL. This simple to use interface offers configuration tools for firewall, VPN, QoS, and H.323 application proxy configuration, and options for monitoring and logging firewall, VPN, and device events.

The SG203/SG208 also offer a full-featured command line interface (CLI), accessible via the console port, which supports all device commands.

## The Avaya Enterprise Security Practice

Avaya has created the Enterprise Security Practice to help safeguard the privacy of network users, ensure confidentiality of information, and control access to mission-critical infrastructure resources in voice, data and converged networks. With the Avaya Enterprise Security Practice, you are investing in the future of your enterprise by providing a secure network environment for business success. This comprehensive portfolio of protection services complements Avaya security product solutions by helping you to assess and audit existing network security practices, facilitating development of a security policy, and creating the security architecture and design that provides you with a security solution that fits your needs.

## Key Features

Performance	SG203	SG208
Firewall Concurrent Sessions	200,000	300,000
Firewall Performance	90 Mbps	600 Mbps
3DES (168-bit) Encryption	90 Mbps	400 Mbps
AES (128-bit) Encryption	90 Mbps	500 Mbps
Remote Access VPN Support (Base System)	100 users	100 users
Remote Access VPN Support (Maximum)	3000 users	8000 users
Site-to-Site VPN Support (Base System)	50 tunnels	100 tunnels
Site-to-Site VPN Support (Maximum)	300 tunnels	1000 tunnels

Interfaces	SG203	SG208
Integrated Network Ports	Four 10/100 Fast Ethernet (RJ-45)	Four 10/100/1000 Gigabit Ethernet (RJ-45)
Expansion	Two CardBus/PCMCIA slots	Two CardBus/PCMCIA slots
Console Port	One RS-232 (RJ-45) 9600 baud	One RS-232 (RJ-45) 9600 baud

### Firewall

- Stateful Multilayer Inspection (SMLI) architecture
- TCP/UDP/ICMP state tracking
- DoS attack protection
- H.323 Application Proxy (H.225, H.245, Fast Connect)
- Distributed firewall policy management (with VPNmanager)

### VPN

- IKE key management (RFC 2409)
- MD5 and SHA-1 data authentication
- DES (56-bit), 3DES (168-bit), and AES (128-bit)
- Perfect Forward Secrecy
- IPSec Compliance: RFC 2401/2402/2403/2405/2406/2407/2408/2409/2410/2412/2451

### Traffic Management

- Class-Based Queuing architecture
- Four user-definable classes of traffic
- Configurable bandwidth allocation with support for bandwidth borrowing

### IP Addressing

- **Trusted interface:** DHCP relay and DHCP server with extensions to support IP phone configuration

### Management

- Web Interface (HTTPS)
- Command Line Interface (SSH)
- VPNmanager (SSL)
  - Distributed VPN policy management
  - Distributed firewall policy management
  - Distributed remote access user management
- SNMP v1/v3 monitoring

## Specifications

### Physical

- Dimensions (H x W x D): 1.75" x 17" x 18" (45mm x 432mm x 457mm)
- Weight: 18.5 lbs (8.5 kg)
- Power: 100 to 240 VAC, 110W

### Environmental

- Operating Temperature: 32 – 104∞ F (0 - 40∞ C)
- Humidity: 5 – 90% (non-condensing)

### Certifications

- Safety: CE, CSA/C/US, Check Mark
- EMI/RFI: FCC Class A, VCCI, BSMI

## Ordering Information

Gateway	Description	Material Code
Avaya <b>SG203</b> Security Gateway	Base SG203 with license for 100 remote access users and 50 site-to-site VPN tunnels	700257991
Avaya <b>SG208</b> Security Gateway	Base SG208 with license for 100 remote access users and 100 site-to-site VPN tunnels	700262124


## Ordering Information (continued)

Remote User		
Product	Description	Material Code
VPNremote 5 User Bundle	License for additional 5 VPN remote access users	700258049
VPNremote 10 User Bundle	License for additional 10 VPN remote access users	700256118
VPNremote 25 User Bundle	License for additional 25 VPN remote access users	700256412
VPNremote 50 User Bundle	License for additional 50 VPN remote access users	700256159
VPNremote 75 User Bundle	License for additional 75 VPN remote access users	700256167
VPNremote 100 User Bundle	License for additional 100 VPN remote access users	700256175
VPNremote 200 User Bundle	License for additional 200 VPN remote access users	700256183
VPNremote 500 User Bundle	License for additional 500 VPN remote access users	700256431
VPNremote 700 User Bundle	License for additional 700 VPN remote access users	700262132
VPNremote 1000 User Bundle	License for additional 1000 VPN remote access users	700256449
VPNremote 2000 User Bundle	License for additional 2000 VPN remote access users	700256456
SG203 VPNremote Site License	Remote Access Site License for SG203	700256464
VPNremote 5000 User Bundle	License for additional 5000 VPN remote access users	700262140
SG208 VPNremote Site License	Remote Access Site License for SG208	700262165
Site-to-Site		
Product	Description	Material Code
VPN 1 Site-to-Site Bundle	License for additional 1 VPN site-to-site connection	700256399
VPN 5 Site-to-Site Bundle	License for additional 5 VPN site-to-site connections	700256407
VPN 10 Site-to-Site Bundle	License for additional 10 VPN site-to-site connections	700256415
VPN 50 Site-to-Site Bundle	License for additional 50 VPN site-to-site connections	700256423
VPN 125 Site-to-Site Bundle	License for additional 125 VPN site-to-site connections	700258056
VPN 250 Site-to-Site Bundle	License for additional 250 VPN site-to-site connections	700258064
VPN 500 Site-to-Site Bundle	License for additional 500 VPN site-to-site connections	700262157

## Learn More

For additional information on our VPN and Security Gateway solutions, please contact your Avaya Client Executive, Authorized BusinessPartner, or visit us at

[avaya.com/learnmore/ip](http://avaya.com/learnmore/ip). For more information about Avaya and our other award-winning solutions, visit [avaya.com](http://avaya.com).

<p><b>About Avaya</b></p> <p>Avaya enables businesses to achieve superior results by designing, building and managing their communications networks. Over one million businesses worldwide, including more than 90 percent of the FORTUNE 500®, rely on Avaya solutions and services to enhance value, improve productivity and gain competitive advantage.</p>	<p>Focused on enterprises large to small, Avaya is a world leader in secure and reliable IP telephony systems, communications software applications and full life-cycle services. Driving the convergence of voice and data communications with business applications – and distinguished by comprehensive worldwide services – Avaya helps customers leverage existing and new networks to unlock value and enhance business performance.</p>		
IP Telephony	Contact Centers	Unified Communication	Services

© 2003 Avaya Inc.

All Rights Reserved. Avaya and the Avaya Logo are trademarks of Avaya Inc. and may be registered in certain jurisdictions. All trademarks identified by the ®, SM or TM are registered trademarks, service marks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners.

Printed in the U.S.A.

07/03 • EF-LB2153