

Symantec™ Gateway Security 400 Series

Multi-function firewall appliance provides manageable security for remote and small branch offices

> The need to securely manage remote locations

Many medium and large enterprises maintain hundreds or thousands of central hub sites and remote/branch offices (ROBOs) that require real-time connectivity to the corporate network via the Internet to access business applications and data. While the Internet enables significant savings as a transport mechanism, it also introduces potential security threats. Today's enterprises are challenged to comprehensively protect data at remote locations, while managing and pushing critical security policies to those same locations.

Symantec™ Gateway Security 400 Series appliances provide integrated firewall and five additional security technologies with centralized, flexible, policy-based management for remote/small branch office sites. The series offers four models supporting a range of users, firewall throughput, and VPN encryption performance.

By integrating multiple security functions, networking capabilities, wireless LAN (WLAN) access/security, and global security management, the appliance allows enterprises to simplify management and reduce overhead by centrally pushing policies and monitoring thousands of remote sites.



> Entry-level firewall with integrated security functions

Symantec™ Gateway Security 400 Series is a multi-functional firewall appliance providing the following six integrated security technologies for maximum effectiveness, while reducing the complexity of security management:

- **FIREWALL:** Stateful packet inspection engine with unique enhancements, including five definable access groups, support for IPsec pass-through and more.
- **ANTIVIRUS POLICY ENFORCEMENT:** Monitors clients using the gateway to ensure they have up-to-date Symantec antivirus protection before accessing the internal or external network.
- **VPN:** IPsec-compliant VPN with hardware-assisted encryption for gateway-to-gateway, client-to-gateway, and WAN/LAN/WLAN client-to-gateway tunnels.
- **INTRUSION DETECTION:** Offers comprehensive attack detection, logging, and reporting that is more comprehensive than most entry-level security appliances.
- **INTRUSION PREVENTION:** Protects against identified threats by blocking packets identified as malicious or abnormal.
- **CONTENT FILTERING:** Provides on-box URL filtering per operator controlled static Deny and Allow tables.

KEY POINTS

- > Integrates stateful inspection firewall with antivirus policy enforcement, IPsec VPN, intrusion detection, intrusion prevention, and content filtering technologies
- > Offers integrated networking functions including a multi-port LAN switch, a router, and Internet link protection with automatic detection and failover capabilities
- > Provides protection for wireless LAN networks with an Access Point option that extends security protection to clients while allowing seamless roaming within a facility
- > Simple installation eases deployment across thousands of remote sites
- > Simplifies the task of managing global network security through centralized logging, alerting, reporting, and policy configuration management via a single, Java-based management console
- > Four models meet the needs of any size organization, with a range of supported users, firewall throughput, VPN encryption performance, and load aggregation capabilities
- > Minimizes license administration – the base appliance includes: licenses for all security functions with unrestricted users and licenses for the Event and Advanced Manager plug-in that enable scalable centralized management
- > Delivers automatic security and firmware updates via LiveUpdate™ technology from Symantec™ Security Response, the world's leading Internet security research and support organization

> Scalable, centralized management

The Symantec Gateway Security 400 Series integrates seamlessly with the Symantec Security Management System (SSMS), enabling a range of advanced management and reporting capabilities. Each appliance comes fully licensed for the Event and Advanced Manager plug-in.

- **EVENT MANAGER:** Enables centralized logging, alerting, and reporting, providing IT administrators a real-time view of traffic and security trends – even in distributed enterprises.
- **ADVANCED MANAGER:** Allows administrators to define rule sets and manage security policies for hundreds or even thousands of sites through a centralized console.
- **POLICY-BASED MANAGEMENT:** Via the SSMS console, administrators can define multiple groups of 400 Series appliances and, for each group, set a different security policy and configuration that can be automatically applied to all the members of the group.
- **SCALABLE MANAGEMENT FOR WLAN ACCESS POINTS:** For 400 Series appliances with a WLAN Access point add-on installed, centralized wireless security policy and event logging and alerting may be managed across the organization.
- **LIVEUPDATE™:** Automatic delivery of firmware updates via LiveUpdate technology from Symantec Security Response.

> Integrated networking functions

The appliance integrates the following networking capabilities, alleviating the time and costs needed to procure and manage multiple networking devices:

- **WAN CONNECTIVITY FOR INTERNET SHARING:** Allows quick access to the most popular Internet services when connected to the external service point for cable, DSL, ISDN, Analog dial-up, or T1 services. Also connects directly to internal LANs, as well as many other services via a number of configurable network protocols.
- **ROUTING AND PROTOCOLS:** Natively supports popular WAN protocols such as PPPoE (Point-to-Point Protocol over Ethernet) and PPTP (Point-to-Point Tunneling Protocol), and allows configuration of routing table entries using the RIPv2 routing protocol or static routes.
- **DYNAMIC DNS:** Allows use of expensive domain names without static IP addresses by automatically updating the DNS for your domain name with every IP address change.
- **10/100 LAN SWITCH:** Provides local Ethernet LAN switching for file and print devices or for numerous devices that need to share the gateway connection to the external network.
- **DHCP SERVER/CLIENT WITH NAT/PAT:** Allows all LAN-connected devices to share the gateway's external IP address(es) instead of requiring an additional static address for each LAN device.
- **LINK FAILURE PROTECTION:** Provides additional ports for back-up WAN connection that automatically sense failures and transfer WAN data to the back-up connection. The Symantec Gateway Security 420 and 440 models offer a serial port to which an external dial-up modem can be attached. The 460 and 460R models provide a second, full-speed WAN port, in addition to the serial port.
- **BANDWIDTH AGGREGATION:** The Symantec Gateway Security 460 and 460R models offer dual WAN ports that allow ingress/egress of data through both ports simultaneously when load balancing is used, effectively doubling the throughput to the external network.
- **GLOBAL TUNNELS:** Smaller sites needing deep packet inspection or dynamic content filtering can use the appliance configured with Global Tunnels, which securely transfer traffic via VPN encryption to a larger site with Symantec Gateway Security 5400 Series appliances installed.

> **Integrated WLAN security**

An optional upgrade allows all models to function as a standards-based wireless access point, featuring highly secure IPsec VPN tunnels that protect open transmissions from wireless LAN clients to the gateway. All Symantec Gateway Security 400 Series models can use the same robust IPsec VPN encryption and user client currently used by most organizations for remote or traveling users.

- **CARDBUS-BASED WLAN OPTION SLOT:** Accepts the Symantec Gateway Security Series 802.11b/g WLAN Access Point Add-on option. The WLAN access point add-on is comprised of special wireless Access Point firmware functions for the appliance and a CardBus-sized integrated 802.11b/g radio and antenna.
- **OPTIONAL SECURITY MODES:** The WLAN port may be configured as VPN-Secure™ or be protected using current WLAN standards such as WEP (Wired Equivalent Privacy).

> **Scalable performance**

To meet the needs of a wide range of remote and small branch office sites, the 400 series offers four models. With up to 200 recommended users, firewall throughput up to 90 Mbps, and AES (Advanced Encryption Standard) VPN throughput up to 35 Mbps, the appliance provides robust performance for many enterprise sites.

> **Reliable security from the security experts**

Symantec Gateway Security is backed by Symantec™ Security Response—the world's largest team of dedicated experts working to identify and neutralize network attacks. Backed by two decades of experience, Symantec Security Response provides swift, global responses to virus outbreaks and blended threats, proactive research on future threats, and ongoing education. By leveraging Symantec's breadth of security expertise and leading technology across all categories of security, as well as support through intelligence and security response teams, organizations can rest assured of reliable protection from even the most threatening Internet security attacks.

For more information about the Symantec Gateway Security 400 Series, visit
<http://enterprisesecurity.symantec.com>

FIREWALL/VPN TECHNOLOGY IS A KEY COMPONENT OF SYMANTEC ENTERPRISE SECURITY. SYMANTEC ENTERPRISE SECURITY COMBINES WORLD-CLASS TECHNOLOGIES, COMPREHENSIVE SERVICES, AND GLOBAL EMERGENCY RESPONSE TEAMS TO HELP BUSINESSES RUN SECURELY AND WITH CONFIDENCE.

COMPARISON OF SYMANTEC GATEWAY SECURITY 400 SERIES MODELS

MODEL	420	440	460/460R
FEATURES			
Maximum Rec nodes	75	150	200
Size of organization supported	Small/Medium ROBO	Small/Medium ROBO	Small/Medium/Large ROBO
Stateful Inspection	60 Mbps	75 Mbps	90 Mbps
High Availability type	Dial-Up (Active/Passive)	Dial-Up (Active/Passive)	High Speed (Active/Active) + Dial-up
VPN 3DES Encryption	20Mbps	30Mbps	35Mbps
VPN AES Encryption	20Mbps	30Mbps	35Mbps
Memory	64MB	64MB	64MB
10/100 Ethernet Ports	1 WAN / 4 LAN	1 WAN / 4 LAN	2 WAN / 8 LAN
Wireless LAN option	802.11 g/b	802.11 g/b	802.11 g/b
Concurrent Connections	10,000	10,000	10,000
VPN Clients	SCVPN Add-on Available	SCVPN Add-on Available	460: SCVPN Add-on Available 460R: SCVPN + 50 session lic & media included
Recommended Tunnels	25*	30*	50*
PHYSICAL AND OPERATIONAL SPECIFICATIONS			
Operational Environment	0° C to 40° C (32° F to 104° F), 10% to 80% relative humidity, non-condensing	0° C to 40° C (32° F to 104° F), 10% to 80% relative humidity, non-condensing	0° C to 40° C (32° F to 104° F), 10% to 80% relative humidity, non-condensing
Non-Operating Environment	-40° C to 65° C (-40° F to 149° F), 95% relative humidity, non-condensing	-40° C to 65° C (-40° F to 149° F), 95% relative humidity, non-condensing	-40° C to 65° C (-40° F to 149° F), 95% relative humidity, non-condensing
Height	3.3 cm (1.31 in)	3.3 cm (1.31 in)	3.3 cm (1.31 in)
Width	30.4 cm (12 in)	30.4 cm (12 in)	30.4 cm (12 in)
Depth	15 cm (5.9 in)	15 cm (5.9 in)	15 cm (5.9 in)
SUPPORT			
Silver	- Included with Purchase - Unlimited calls for first 90 days	- Included with Purchase - Unlimited calls for first 90 days	- Included with Purchase - Unlimited calls for first 90 days
Gold	Support after the first 90 days may be extended with Gold Maintenance providing business hour telephone support plus a 1 year extension of warranty and advanced warranty replacement. Available in one or two year terms	Support after the first 90 days may be extended with Gold Maintenance providing business hour telephone support plus a 1 year extension of warranty and advanced warranty replacement. Available in one or two year terms	Support after the first 90 days may be extended with Gold Maintenance providing business hour telephone support plus a 1 year extension of warranty and advanced warranty replacement. Available in one or two year terms
Platinum	Adds 24 x 7 telephone support and Level 2 escalation entitlement.	Adds 24 x 7 telephone support and Level 2 escalation entitlement.	Adds 24 x 7 telephone support and Level 2 escalation entitlement.
Warranty	1 Year return-to-factory included with purchase	1 Year return-to-factory included with purchase	1 Year return-to-factory included with purchase

* Maximum number of tunnels may vary due to traffic and network characteristics.

SYSTEM REQUIREMENTS

The Symantec Gateway Security 400 Series devices are self-contained appliances with all hardware and software required for normal operation pre-installed in the device.

The Symantec Event Manager and Advanced Manager for Security Gateways (Group 2) requires the following SESA 2.0. components (See the SESA 2.0 System Requirements for full details.)

SESA 2.0 Directory computer

- Windows: 2000 Server SP3 or SP4, 2000 Advanced Server SP3 or SP4 is required
- Required and included components:
 - IBM Directory Server 4.1.1, FixPack 1; - IBM Apache HTTP 1.3.19.5;
 - IBM DB2 Personal Edition 7.2, FixPack 5 (For demonstration purposes only)
- Supported, but not included, components:
 - existing installations of IBM DB2 Workgroup/Enterprise/Enterprise Extended Edition 7.2, FixPack 11

SESA 2.0 Manager computer

- Windows: 2000 Server SP3 or SP4, 2000 Advanced Server SP3 or SP4 is required
- Required and included components:
 - SUN Java Development Kit (JDK) / SUN Java Runtime Environment (JRE) 1.3.1_09;
 - IBM Apache HTTP 1.3.19.5; - Tomcat 4.03
- Supported, but not included, components:
 - SUN Java Development Kit (JDK) / SUN Java Runtime Environment (JRE) 1.3.1_02;
 - IBM DB2 Runtime client 7.2, FixPack 11
(To support remote connections with an IBM DB2 DataStore)

SESA 2.0 DataStore computer

- Windows: 2000 Server SP3 or SP4, 2000 Advanced Server SP3 or SP4 is required
- Included and optional-install components:
 - IBM DB2 Personal Edition 7.2, FixPack 5 (For demonstration purposes only);
- (Note: When IBM DB2 Personal Edition 7.2, FixPack 5 is used for the SESA DataStore, it must be installed on the same machine as the SESA Manager.); (Note: SESA's use of the IBM DB2 Personal Edition component has a single Intel processor & 2GB storage limit)
- Supported, but not included, components: existing installations of IBM DB2 Workgroup/Enterprise/Enterprise Extended Edition 7.2, FixPack 11

Symantec management console

- Windows: 98 or later required components:
 - SUN Java Runtime Environment (JRE) 1.3.1_02 or 1.3.1_09 (recommended & included)
- SUN Solaris: Version 7 or later required components:
 - SUN Java Runtime Environment (JRE) 1.4.2
- RedHat Linux: Versions 6.2, 7.0, 7.1, 7.2 or later required components:
 - SUN Java Runtime Environment (JRE) 1.3.1_02 or 1.3.1_09 (recommended & included)

WORLD HEADQUARTERS

20330 Stevens Creek Blvd.
Cupertino, CA 95014 U.S.A.
408 517 8000
800 721 3934

www.symantec.com

For Product Information
In the U.S., call toll-free
800 745 6054

Symantec has worldwide
operations in 35 countries.
For specific country
offices and contact numbers
please visit our Web site.