✸ symantec™

Symantec™ Gateway Security 5400 Series

Full-inspection firewall appliance with integrated security technologies

Symantec™ Gateway Security 5400 Series provides maximum protection against even the most malicious Internet security threats while reducing the complexity of security management. As the industry's most comprehensive enterprise firewall appliance, it seamlessly integrates a full inspection firewall, protocol anomaly and signature-based intrusion prevention and intrusion detection engines, award-winning virus protection, URL-based content filtering, anti-spam and IPsec-compliant virtual private networking technology with hardware-assisted high-speed encryption.

⟩ Next-generation, integrated firewall appliance

Symantec Gateway Security 5400 Series is a next-generation firewall appliance that integrates full packet inspection firewall technology with intrusion prevention intelligence at the gateway between the Internet and corporate network or between network segments. The solution leverages tightly integrated, industry-leading technologies to control and validate data packets as they pass through the gateway.

First, the full inspection firewall, which allows administrators to set granular policies for complete control of information entering and leaving the network, performs deep packet inspection that drops and logs bad packets. If a VPN session is active, the proxy-secured, virtual private networking technology decrypts the packet and drops it into the data stream. Next, the firewall performs session checks at the circuit layer and once again, drops and logs bad packets. The integrated intrusion prevention and intrusion detection technologies block packets that contain threats, and automatically notify the the firewall of malicious sessions from specific IP addresses, which will enable the firewall to block specific sessions that contain threats or block specific IP addresses that continue to pose a threat.

The firewall then opens and examines application layer protocol packets. These packets are checked to ensure conformity with the applicable RFCs and valid commands. Once again, bad packets are dropped and logged. If the packets are HTTP based, content filtering technology compares the source IP against a list of prohibited Web sites. Prohibited content is dropped and logged. If the packets are HTTP, FTP, or SMTP protocol based, files and attachments are sent to the award-winning virus scanner, which also actively blocks email messages by subject line text, file name attachment type, and message size. If a virus is found, the file is either repaired or dropped. All viruses are logged and a message is added to mail messages indicating that a virus was found and the attachment was deleted. If all of these checks are passed, the appliance allows the packet to enter or leave the network. This unique combination of security technologies helps stop viruses, malicious attacks, and blended threats at the network perimeter.

Timely updates of new virus definitions, attack signatures, and URL filtering lists are delivered automatically via Symantec's LiveUpdate for rapid and easy deployment across the enterprise (or manually if the administrator prefers).

KEY POINTS

⟩ Seven essential enterprise security functions, which combine firewall protection with protocol anomaly and   signature-based intrusion prevention and intrusion detection, award-winning virus protection, URL-based content filtering, anti-spam, and IPsec-compliant VPN technologies

⟩ Comprehensive network protection to secure networks at the connection to the Internet or subnets of WANs and LANs

⟩ Centralized management simplifies managing network security through centralized logging, alerting, reporting, and policy configuration

⟩ Meets the performance requirements of any size organization with integrated high availability and load balancing option

⟩ Three high-performance models deliver throughput scaling from 200 Mbps to more than 3.5 Gbps in a clustered configurations

⟩ Delivers automatic security updates via LiveUpdate™ technology from Symantec™ Security Response, the world's leading Internet security research and support organization

⟩ Advanced management capabilities

The 5400 Series has standalone policy configuration management capabilities via a secure web-based interface (SSL). Additionally, it integrates seamlessly with the Symantec Management Console enabling a range of advanced management and reporting capabilities. The optional Event Manager plug-in provides centralized logging, alerting, and reporting. It provides IT administrators a real-time view of traffic and security trends – even in distributed enterprises.

The Advanced Manager plug-in, which includes Event Manager, enables administrators to define rule sets and manage security policies for hundreds or even thousands of appliances through a centralized console.

⟩ Flexible configuration and licensing

While the standard pre-loaded Symantec Gateway Security contains all of the security functions, several of the security functions are licensed separately, providing the customer with flexibility to meet unique enterprise security requirements. The base license enables a 50-node firewall, unlimited gateway-to-gateway VPNs, one client-to-gateway VPN session. Functional add-ons are available for antivirus, content filtering, and additional client-to-gateway VPN sessions. Optional high availability and load balancing can be added at any time, without the need to install software. And, additive licenses for any function can be purchased in increments to accommodate growth in the number of nodes requiring protection or concurrent VPN sessions. The software license includes one year of Gold Maintenance, providing a number of services – including telephone support, content updates, upgrade insurance and advanced replacement – designed to keep enterprises up and running.

⟩ Scalable performance

To meet the bandwidth and scalability requirements of any enterprise, the Symantec Gateway Security 5400 Series offers three high-performance models, all with an integrated high availability and load balancing option for maximum uptime. With its clustering and centralized management capabilities, Symantec Gateway Security provides robust and easily managed security for environments ranging from small offices to distributed networks with tens of thousands of nodes. And regardless of the network environment, the appliance delivers throughput that scales from 200 Mbps to more than 3.5 Gbps in clustered configurations.

⟩ New features in this release

The latest version of Symantec Gateway Security includes the following enhancements:

A WEB-BASED GUI for standalone management.

EVENT MANAGER* Plug-in for Symantec Management Console, enables centralized, scalable logging, alerting, and reporting, including the generation of both standardized and customized reports. Both Symantec and select third-party security products are supported.

ADVANCED MANAGER* Web-based plug-in to the Symantec Management Console, that provides a centralized, scalable management GUI, allowing administrators to push configuration information and policies out to multiple appliances simultaneously. Advanced Manager includes Event Manager capabilities.

HYBRID ANOMALY INTRUSION PREVENTION AND DETECTION ENGINES* Provides real-time monitoring, intrusion prevention and intrusion detection of new and unknown attacks using protocol anomaly detection and attack signatures.

ENHANCED ANTIVIRUS ENGINE* Provides improved detection of malformed MIME-based threats.

STATE-SHARING INTEGRATED HIGH AVAILABILITY/LOAD BALANCING* Extends the appliance's scalability and eliminates network downtime. Firewall and VPN sessions will failover automatically to another machine, preserving state.

ENHANCED PERFORMANCE Faster processors, Gigabit Ethernet ports, up to 610 Mbps 3DES encryption acceleration with VPN tunnels, and up to eight Ethernet ports per appliance ensure rapid response to threats without interfering with overall network performance.

IMPROVED VPN Support for UDP-IPSec encapsulation, retry on alternate gateway when primary gateway is unavailable, and LiveUpdate support to increase ease of use.

FLEXIBLE LICENSING Choice of security functions, number of nodes, and number of concurrent VPN sessions.

⟩ 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.

Optional add-on functions.

For more information about the Symantec Gateway Security 5400 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 MODEL OF THE APPLIANCES

MODEL	5420	5440/5441	5460/5461
FEATURES			
Maximum Recommended Nodes	500	2500	4500
Stateful Thruput	200 Mbps	1.4 Gbps	1.8 Gbps
High-Availability Type	A/A, A/P, LB (A/A - Active/Active; A/P - Active/Passive; LB - Load Balancing)	A/A, A/P, LB (A/A - Active/Active; A/P - Active/Passive; LB - Load Balancing)	A/A, A/P, LB (A/A - Active/Active; A/P - Active/Passive; LB - Load Balancing)
Maximum Cluster Size	8	8	8
Full Inspection	95 Mbps	680 Mbps	730 Mbps
VPN 3DES Encryption	90 Mbps	400 Mbps	600 Mbps
VPN AES Encryption	30 Mbps	80 Mbps	90 Mbps
Memory	512 MB	1 GB	2 GB
Disk	40 GB	80 GB	80 GB
Rack space	1U	2U	2U
Fast Ethernet NIC	6	0	0
Gigabit NIC	0	6 (Model 5441- has 2 copper and 4 SX Multi-Mode fiber ports)	8 (Model 5461 has 2 copper and 6 SX Multi-Mode fiber ports)
Connections per second	5000	11300	15300
Concurrent Connections	64,000	190,000	200,000
PHYSICAL AND OPERATIONAL SPECIFICATIONS			
Operating Environment	5° C to 35° C (41° F to 95° 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	-40° C to 65° C (-40° F to 149° F),	-40° C to 65° C (-40° F to 149° F),	-40° C to 65° C (-40° F to 149° F),
Environment	95% relative humidity, non-condensing	95% relative humidity, non-condensing	95% relative humidity, non-condensing
Operating Altitude	Up to 3000M (10,000 Ft)	Up to 3000M (10,000 Ft)	Up to 3000M (10,000 Ft)
Safety	UL 1950, EN 60950	UL 1950, EN 60950	UL 1950, EN 60950
Emissions	EN 55022 Class A, FCC Class A	EN 55022 Class A, FCC Class A	EN 55022 Class A, FCC Class A
Immunity	EN 55025	EN 55025	EN 55025
Height	4.45 cm (1.75 in)	8.9 cm (3.5 in)	8.9 cm (3.5 in)
Width	43.8 cm (17.25 in)	43.8 cm (17.25 in)	43.8 cm (17.25 in)
Depth	43.8 cm (17.25 in)	61 cm (24.0 in)	61 cm (24.0 in)
Weight	6.12 kg (13.6 lb)	9.59 kg (21.3 lb)	10.22 kg (22.7 lb)
Enclosure	Fits 19-inch Rack	Fits 19-inch Rack	Fits 19-inch Rack
MAINTENANCE			
	One year of Gold Maintenance with the base license and all function add-ons and additive licenses. Gold Maintenance renewal contracts are available in one or two year terms. Platinum Support Uplifts are available for all Gold Maintenance terms.	One year of Gold Maintenance with the base license and all function add-ons and additive licenses. Gold Maintenance renewal contracts are available in one or two year terms. Platinum Support Uplifts are available for all Gold Maintenance terms.	One year of Gold Maintenance with the base license and all function add-ons and additive licenses. Gold Maintenance renewal contracts are available in one or two year terms. Platinum Support Uplifts are available for all Gold Maintenance terms.
MANAGEMENT/REPORTING			
	Optional centralized logging, alerting and reporting	Optional centralized logging, alerting and reporting	Optional centralized logging, alerting and reporting
	Optional centralized policy management	Optional centralized policy management	Optional centralized policy management

Symantec Gateway Security 5400 Series is available in models capable of managing from 50 to 4500 nodes. For larger networks, multiple 4500-node appliances can be clustered together.

SYSTEM REQUIREMENTS

Any system that runs Microsoft Internet Explorer V6 or higher or Netscape Navigator V7 or higher can be used to manage the Symantec Gateway Security 5400 Series.