

Symantec™ Clientless VPN Gateway 4400 Series

Comprehensive, secure remote access to corporate networks via Web browsers

Increasingly, businesses must support a growing number of remote employees, customers, and partners who need secure remote access to network resources such as email, file shares, Web and traditional client-server applications. In addition, users may experience difficulty using IPSec VPN systems, resulting in excessive downtime, lost productivity, and increased overall IT support costs.



> Next-generation, secure remote access appliance

Symantec Clientless VPN Gateway is a stand-alone security appliance that runs behind a company's firewall and provides a simple, secure, and cost-effective way to connect large numbers of remote users to corporate networks. The plug-and-play design of the appliance enables companies to extend selected corporate applications to remote employees, customers, and business partners through a standard Web browser. Also known as SSL VPN, the Symantec Clientless VPN leverages the power of the Secure Sockets Layer (SSL) protocol and the Internet to deliver the same features and enterprise-level secure remote access as traditional IPSec VPNs, without the need for client software implementation and reconfiguration.

> Multiple-access methods

With the Symantec Clientless VPN Gateway, remote users using any dial-up, broadband, wireless access point, or cellular phone with Internet access can gain access to specific applications through a Web interface. Using Symantec's proven proxy technology, the appliance ensures access to Web data and applications, even complex Web sites that use HTML, DHTML, JavaScript™, VBScript, Flash, Java™, and XML. Users also have access to any email server via an embedded secure Web front end; direct access to TCP/UDP applications and email servers via encrypted IMAP, POP, and SMTP; as well as access to Windows® and Novell® file servers; FTP; Telnet, SSH, and terminal applications; and traditional client-server applications like Microsoft Outlook® and Lotus Notes®. To protect customer's existing VPN investments, the Symantec Clientless VPN Gateway is fully compatible with traditional VPN technology, including Citrix, Microsoft® Terminal Services, pcAnywhere™, and integrates with leading authentication servers and network management systems products.

> Enterprise-level security

The Symantec Clientless VPN Gateway protects all network communications with the strongest banking-grade encryption, thereby securing all network communications. The embedded Web portal can prohibit access to all command lines, control panels, and desktops, eliminating the most common network and operating system vulnerabilities such as worms, viruses, and Trojan horses. It also includes an application-level reverse proxy built using Symantec's field-tested security technology. This proxy uses industry-standard SSL encryption, PKI certificates, authentication protocols, and TCP/IP filtering, which together enable companies to securely extend network resources to remote users anywhere.

KEY POINTS

- > Stand-alone, secure remote access appliance (Clientless VPN) that enables remote users to access corporate resources without requiring the installation and maintenance of any client software
- > Delivers robust data protection (SSL encryption)
- > Extends secure remote access to wireless handheld devices such as Windows Mobile 2003 and Palm™ 5.x based PDA devices
- > Provides portal-based access for web-enabled and non-web based applications via Web VPN
- > Enables administrators to configure granular, policy-based user and group extranet access

> **Administration, management, and ease-of-use**

The Symantec Clientless VPN Gateway includes an intuitive, secure, Web-based administrator interface that enables centralized management of all functions. The appliance helps administrators implement strong and consistent security policies, role-based access, and global security monitoring and reporting. It also authenticates users with single- and multi-factor authentication via standard protocols, including RADIUS, LDAP, Active Directory, and RSA SecurID®. In addition to the Web interface, administrators can perform simple set up using the LCD display or complex management using the menu-driven command-line interface (CLI) locally or remotely over a secure SSH connection.

The appliance also includes powerful configuration and management capabilities such as Role-Based User/Group Policy Management and Access Control capabilities. For example, with complementary Granular File Access Controls, administrators can control user access down to the individual file and/or application level and configure granular, policy-based user and group extranet access.

By utilizing the SSL encryption engine already available on most PCs, laptops, and handhelds, users do not need to download and configure client software or learn new procedures. By simply pointing their browsers to the Symantec Clientless VPN Gateway appliance and logging in, remote users can securely access their corporate network from virtually any location, even via wireless handheld devices such as market leading PDAs.

> **Scalable and flexible**

The Symantec Clientless VPN Gateway is designed to scale up to 5,000 concurrent connections in load-balanced clusters (equivalent to approximately 50,000 users), or up to 1,000 concurrent connections or 10,000 users with a single appliance. With support for high-availability configurations and peering, a disk for logging, and built-in upgrade capabilities that make it easy to add future security functions to existing appliances, the Symantec Clientless VPN Gateway provides unmatched flexibility to meet changing business needs.

Symantec Clientless VPN Gateway uses hardware that is compatible with Symantec™ Gateway Security appliances. Symantec Clientless VPN Gateway functions will be integrated into a future version of Symantec™ Gateway Security software so that customers with Symantec Clientless VPN Gateway appliances will be able to upgrade to Symantec Gateway Security.

COMPARISON MODEL OF THE APPLIANCES

MODEL	4420	4460
FEATURES		
Web page translation	HTML, DHTML, Javascript, ActiveX, Java, ASP, CSS	HTML, DHTML, Javascript, ActiveX, Java, ASP, CSS
Terminal emulation applications	Citrix, Citrix Nfuse, pcAnywhere, Microsoft Terminal Services, telnet, SSH, VNC	Citrix, Citrix Nfuse, pcAnywhere, Microsoft Terminal Services, telnet, SSH, VNC
User authentication protocols	Microsoft Active Directory, Two-factor (RSA SecurID), LDAP/LDAPS, RADIUS, Windows NT Domain	Microsoft Active Directory, Two-factor (RSA SecurID), LDAP/LDAPS, RADIUS, Windows NT Domain
Email protocols	SMTP, IMAP, POP, MAPI	SMTP, IMAP, POP, MAPI
Web-based mail applications	Microsoft Outlook Web Access (OWA), IBM Lotus iNotes	Microsoft Outlook Web Access (OWA), IBM Lotus iNotes
Client/server messaging applications	Microsoft Outlook, Microsoft Exchange, IBM Lotus Notes	Microsoft Outlook, Microsoft Exchange, IBM Lotus Notes
Client/server applications	TCP, UDP	TCP, UDP
Granular authorization	File, server and URL level support	File, server and URL level support
SSL encryption level	Up to 256-bit	Up to 256-bit
Share file protocols	Microsoft File Sharing, Novell File System (NFS)	Microsoft File Sharing, Novell File System (NFS)
Supported OS	Microsoft Windows XP/2000 (legacy Windows), Apple Mac OS X, Microsoft Mobile 2003 for Pocket PC, Palm OS 5.x, Linux	Microsoft Windows XP/2000 (legacy Windows), Apple Mac OS X, Microsoft Mobile 2003 for Pocket PC, Palm OS 5.x, Linux
Layer 3 VPN	Microsoft Windows XP/2000	Microsoft Windows XP/2000
Maximum recommended concurrent sessions	350	1000
Standard NICs	2 x 10/100	2 x 10/100/1000
NICs for use at a later time	4 x 10/100	6 x 10/100/1000
Clients (Internet browsers)		
Windows	Microsoft Internet Explorer (5.5+) Netscape 7.x	Microsoft Internet Explorer (5.5+) Netscape 7.x
Linux	Mozilla 1.5 Netscape 7.0	Mozilla 1.5 Netscape 7.0
Mac	Safari and Mozilla 1.3	Safari and Mozilla 1.3
Windows CE/Mobile 2003	Microsoft Internet Explorer	Microsoft Internet Explorer
Palm	5.x with WebPro 3.0	5.x with WebPro 3.0
PHYSICAL AND OPERATIONAL SPECIFICATIONS		
Rack space	1U	2U
AC power	90-264 V AC (47-63 Hz); Nominal: 175W, Peak: 300W	90-264 V AC (47-63 Hz); Nominal: 400 W, Peak 575W
Operating	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
Non-operating	-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
Operating altitude	Up to 3,000 m (10,000 ft)	Up to 3,000 m (10,000 ft)
Safety	EN 60950-2 (2002)	EN 60950-2 (2002)
Emissions	EN 55022 Class A, EN61000	EN 55022 Class A, EN61000
Immunity	EN 55025	EN 55025
Height	4.45 cm (1.75 in)	8.90 cm (3.5 in)
Width	44.45 cm (17.5 in)	44.45 cm (17.5 in)
Depth	43.8 cm (17.25 in)	61 cm (24.0 in)
Weight	6.12 kg (13.6 lb)	10.22 kg (22.7 lb)
Enclosure	Fits 19-inch rack	Fits 19-inch rack



SYMANTEC ENTERPRISE 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.

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 36 countries.
For specific country
offices and contact numbers
please visit our Web site.**

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org>)