Symantec™ Web Security 2.5

High-performance content filtering and virus protection for the HTTP/FTP gateway

Organizations ranging from corporations to educational institutions are using the Internet to support collaboration, facilitate information exchange, foster effective learning, and provide online business services. Yet, the Internet also provides a conduit for virus attacks and introduces the possibility of threats to network bandwidth, employee productivity, student learning, corporate liability, and network security. Blended threats—such as the recent Nimda worm, which used Web pages as transmission routes—are posing new hazards to enterprises and educational institutions alike.

Symantec Web Security protects an organization's HTTP/FTP gateway against viruses and other threats to promote secure and productive Internet access. Using scalable, integrated antivirus and content filtering technologies that Symantec develops and supports, Symantec Web Security simultaneously scans for both viruses and Web content. This efficient, multi-protocol solution facilitates employee productivity, maximizes learning, and reduces liability exposure by analyzing and managing Internet usage; preserves valuable network bandwidth by managing file downloads and reducing non-productive Web surfing; and improves network security by screening out blended threats.

Single-scan efficiency and integrated technology effectiveness

Symantec Web Security employs a low-latency, one-time scanning process that efficiently protects against malicious code attacks and effectively scans Web content without draining network resources. It is the only single-scan solution that integrates heuristic, context-sensitive analysis tools with list-based techniques.

INDUSTRY-LEADING ANTIVIRUS TECHNOLOGIES

Symantec Web Security is comprised of the following proprietary technologies:

- Norton AntiVirus Extensible Engine Technology (NAVEX™) A modular virus-scanning engine that reprograms the Norton AntiVirus™ engine to detect new classes of viruses—without having to uninstall existing software or deploy new software
- Symantec Digital Immune System™ Closed-loop technology that automatically manages the detection-analysis-cure process by sending quarantined files over secure lines to Symantec Security Response.
- Symantec Striker™ A detection system that applies profiles to identify and quickly root out entire classes of malicious code (including mobile).
- Symantec Bloodhound™ Technology that is capable of detecting up to 80% of new and unknown executable file viruses including malicious mobile code.

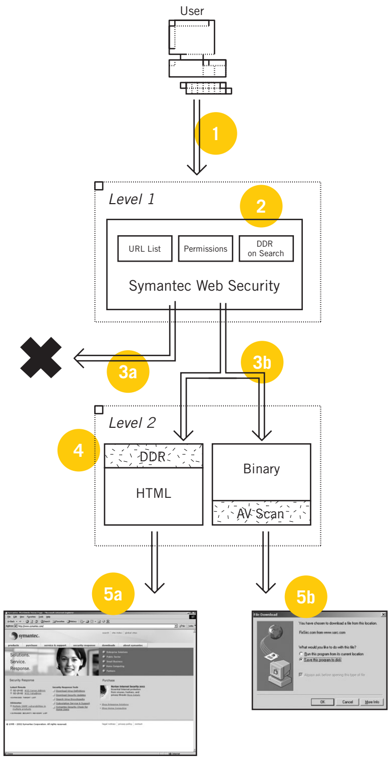
KEY POINTS

- NEW: Supports LDAP, Active Directory, and Windows NT® user/group external directory services and databases via Secure Socket Layer (SSL) technology
- Enables highly granular, policy-based centralized management across Windows NT, Windows® 2000, and Solaris® platforms
- Protects Web traffic with scalable, high-performance, one-time integrated virus scanning and content filtering at the HTTP/FTP gateway
- Ensures maximum protection by combining list-based prevention with heuristic content analysis of both viruses and inappropriate content
- Improves network performance and user productivity while ensuring conformance to acceptable use policies
- Reduces the amount of Web-based traffic, enhancing firewall and network reliability

Comprehensive content filtering technologies

Symantec's patented, multi-lingual Dynamic Document Review™ (DDR) technology works in conjunction with supplied, categorized URL lists to provide comprehensive content filtering. DDR exceeds simple keyword searches to analyze context-sensitive word relationships. It works in real time as it accurately determines whether to block inappropriate Web content, even if that content is not yet categorized in a content category (filter) list. DDR can effectively detect and block newly accessible sites, previously accepted sites whose content has changed, and once-blocked sites with new domain names.

In addition to DDR, Symantec™ Web Security provides customizable URL filter lists that are developed and supported by Symantec. This gives IT administrators the ability to screen out Web sites worldwide, according to organizational policies using 31 pre-defined categories—such as sex, gambling, and intolerance—on an entire system, in groups, or on an individual basis. Symantec automatically updates this software's filter lists daily.



1 User surfs, sends request
2 Is request allowed?
3 a If no, reject immediately
b If yes, retrieve and proceed
4 Is request truly clean?
5 If ok, display 5a, or
download 5b on client

Symantec Web Security provides the first line of defense against Web-based viruses, as well as a tool for reporting and managing employee Internet usage. IT administrators are able to define policies for single users, individual computers, groups, and the entire organization while leveraging standard databases and directory services such as LDAP, Active Directory, and Windows NT® users/groups.

Centralized, policy-based management

For simple, enterprise-wide configuration, and management from any Web browser, Symantec™ Web Security provides an intuitive HTML-based interface and SSL support for LDAP, Active Directory, and Windows NT® user/group external directories and databases. IT administrators are able to create and schedule customized browsing profiles for single users, individual PCs, and groups, restricting access to administrator- or pre-defined content categories according to criteria such as title, location, and time-of-day. Administrators can also monitor and log all Web activity on both filtered and non-filtered sites, as well as use auditing and reporting tools to assess adherence to acceptable use policies. Symantec Web Security automatically alerts administrators via email when policies are breached and the AutoLock feature can deny Internet access to non-compliant accounts that make repeated attempts to view blocked content. It issues integrated antivirus and Web usage reports, which can be exported to a comma-separated file for use in spreadsheet programs and other applications. Finally, Symantec LiveUpdate™ provides continuous, up-to-date protection—even at remote locations —by retrieving virus definitions from the Symantec Web site on-demand or as scheduled.

Improved network performance

To promote network performance, Symantec Web Security scans only suspicious Web traffic, caches duplicate Web content requests locally, and has the capability to manage large file downloads. IT administrators can control Internet access by time-of-day and day-of-week, providing high-bandwidth usage during peak periods to those who need the Internet most.

Backed by Symantec Security Response

Symantec Security Response, the industry's largest team of dedicated virus experts, works continuously to identify and neutralize viruses before they can endanger systems and files. Symantec Security Response is committed to providing proactive research on future threats, ongoing security education, and swift, global response to virus outbreaks.

Learn more

For more information about Symantec Web Security, visit http://enterprisesecurity.symantec.com

VIRUS PROTECTION AND CONTENT FILTERING ARE KEY COMPONENTS 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.

SYSTEM REQUIREMENTS

SYMANTEC™ WEB SECURITY VERSION 2.5

SYMANTEC WEB SECURITY FOR WINDOWS NT®

- PC-based on an Intel Pentium II or compatible processor, or better
- Microsoft® Windows NT Server 4 with SP6a
- Minimum 256 MB of RAM
- Minimum 500 MB of available disk space for the program files, online documentation, configuration files, and so on
- Additional disk space as required for storage of activity logs and caching. A minimum of 400 MB is suggested, with 1 GB or more preferred.
- CD-ROM drive
- Internet access
- World Wide Web (WWW) browser
- Correctly configured DNS server which contains both A and PTR records

SYMANTEC WEB SECURITY FOR WINDOWS® 2000

- PC-based on an Intel Pentium II or compatible processor, or better
- Microsoft Windows 2000 Server 4 with SP2
- Minimum 256 MB of RAM
- Minimum 500 MB of available disk space for the program files, online documentation, configuration files, and so on
- Additional disk space as required for storage of activity logs and caching. A minimum of 400 MB is suggested, with 1 GB or more preferred.
- CD-ROM drive
- Internet access
- World Wide Web (WWW) browser
- Correctly configured DNS server which contains both A and PTR records

SYMANTEC WEB SECURITY FOR SOLARIS®

- Sun® SPARC-based system
- Solaris® 2.6, 7, or 8 operating system
- Minimum 256 MB of RAM
- Minimum 500 MB of available disk space for the program files, online documentation, configuration files, and so on
- Additional disk space as required for storage of user bookmarks and history, activity logging, and caching. A minimum of 400 MB is suggested, with 1 GB or more preferred.
- CD-ROM drive
- Internet access
- World Wide Web (WWW) browser
- Correctly configured DNS server which contains both A and PTR records

SYMANTEC WEB SECURITY FOR CHECKPOINT FIREWALL-1 ON NT

- PC-based on an Intel Pentium II or compatible processor, or better
- Microsoft® Windows NT Server 4 with SP6a
- Minimum 256 MB of RAM
- Minimum 500 MB of available disk space for the program files, online documentation, configuration files, and so on
- Additional disk space as required for storage of activity logs. A minimum of 100 MB is suggested, with 500 MB or more preferred.
- CD-ROM drive
- Internet access
- World Wide Web (WWW) browser
- Correctly configured DNS server which contains both A and PTR records

SYMANTEC WEB SECURITY FOR CHECKPOINT FIREWALL-1 ON SOLARIS

- Sun SPARC-based system
- Solaris 7 or later operating system
- CheckPoint Firewall-1 version 4, patch level 4031 or later
- Minimum 256 MB of RAM
- Minimum 500 MB of available disk space for the program files, online documentation, configuration files, and so on
- Additional disk space as required for storage of activity logs. A minimum of 100 MB is suggested, with 500 MB or more preferred.
- CD-ROM drive
- Internet access
- World Wide Web (WWW) browser
- Correctly configured DNS server which contains both A and PTR records

WWW BROWSER REQUIREMENTS

Any CERN HTTP Proxy protocol compliant browser, such as:

- Microsoft Internet Explorer (IE) version 5.0 or later
- Netscape® Navigator version 4.7 or later

WORLD HEADQUARTERS

20330 Stevens Creek Blvd.
Cupertino, CA 95014 U.S.A.
1.408.253.9600
1.800.441.7234

www.symantec.com

For Product Information
In the U.S., call toll-free
800.745.6054.

Symantec has worldwide operations in 38 countries. For specific country offices and contact numbers please visit our Web site.