Web Security: Protecting Networks from Inappropriate Web Content and Malicious Code

INSIDE

INSIDE

- Requirements for a Web content security solution
- Symantec™ Web Security: Integrated virus protection and content filtering

Contents

Executive summary 3

Need for Web content security 4

Network security: The virus threat 4

Need for content filtering 6

Requirements for a Web content security solution 7

Proactive antivirus scanning 7

Intelligent content filtering 7

Centralized administration and reporting tools 8

Automatic updating 8

Symantec™ Web Security: Integrated virus protection and content filtering 9

List-based and heuristic filtering 9

Up-to-date protection through Symantec technologies 9

Centralized administration and auditing tools 10

Summary 11

References 11

Executive summary

Threats to corporate infrastructures like the recent Nimda worm signal the dawn of a new era of destructive virus and malicious code attacks on enterprises and academic institutions. The multi-pronged attack of this worm—which used email messages and Web pages as transmission routes—caused organizations to redefine the concept of network security.

The widespread infection inflicted by Nimda "in the wild," with destruction often spread by the simple act of visiting a Web site, means that organizations now need a multi-protocol defense to maintain network security. In addition to protection at the SMTP gateway, administrators must implement virus protection and content filtering at the HTTP/FTP gateway to protect networks from becoming unwitting carriers of this new class of attack.

Integrated virus protection and content filtering strengthen network security, while avoiding inappropriate URL access by employees with an inherent loss of productivity, corporate liability, and bandwidth consumption; and inappropriate access by students and researchers with resulting ineffective learning and potential loss of funding. The Symantec Web Security solution is the answer to a multi-protocol defense: it offers tight integration, and provides a low-latency, high-performance solution that meets the needs of both administrators and users.

Need for Web content security

The Internet provides quick, easy access to research for corporate employees and executives, as well as academic researchers and students. It supports collaboration across geographic areas and facilitates information delivery to a wide audience. Web content has evolved from static online brochures with simple text and photographs to dynamic, interactive, multimedia files with animated graphics. Along with meteoric growth in terms of number of Web sites and number of users, organizations use the Web in a growing number of business and educational applications.

Yet, the benefit of easy information access is accompanied by the rapid growth of a range of threats to network security, employee productivity, effective learning, corporate liability, and bandwidth consumption.

NETWORK SECURITY: THE VIRUS THREAT

The continued rise in viruses

The ICSA Labs 6th Annual Computer Virus Prevalence Survey (conducted in 2000) reports that organizations can expect between 14 and 91 virus encounters per month per 1000 PCs[1]. The same survey showed that 76 percent of organizations perceived that the virus problem was somewhat worse or much worse in the year 2000.

Compounding the threat that email-borne viruses (e.g., macro viruses) pose, is the potential for infection with malicious code that can spread quickly throughout an organization's network before detection. Malicious code can accompany mobile code on Web pages, Web-based mail, and HTTP and FTP file downloads. Malicious code threats include attachments to Web-based email programs; mobile code such as Java, JavaScript, and ActiveX used to execute simple graphics or animation programs on Web pages; and documents or software downloaded via FTP or HTTP. For example, Internet users could download what appears to be a perfectly legitimate program when in actuality it is one that carries hidden intent (i.e., a Trojan Horse program); this would expose the network to hackers. In another example, programming code authorizing remote access to a network can reside unnoticed in browser cookies or Web applets.

Nimda, the blended threat attack

A recent example of a new type of blended threat was a worm that used multiple methods of mass-mailing to spread. Deriving its name from the reverse spelling of "admin", the Nimda worm would send itself out via email, infecting machines over a network as it pinpointed unpatched or already vulnerable Microsoft® IIS Web servers. It also created such side effects as increased network traffic which caused bandwidth problems, and created security holes by forging guest accounts with administrator privileges which in turn generated open shares on infected systems.

This is how Nimda worked: a message would arrive at an inbox with an attachment that was not always visible and which contained a randomly generated subject line and no body message. By searching the user's incoming and outgoing email boxes, the worm would use its own SMTP engine to email itself to all of the addresses stored on the recipient machine. Just opening the email was enough to infect users' PCs.

A second Nimda transmission method involved shared drives. The worm would search for open shares over a network and attempt to copy its executable self onto those systems.

Nimda also used the Web to propagate. When users visited a compromised Web site (which also included legitimate sites), the server would run a script in an attempt to download a Microsoft Outlook file that contained the Nimda worm. The worm would then create an open network share on the infected machine, thus allowing access to the system. Nimda specifically targeted Microsoft IIS servers by taking advantage of the known Universal Web Traversal exploit, which was similar to the exploit used in the CodeRed attack.

Nimda, the multi-pronged attack which affected tens of thousands of companies worldwide in September 2001, illustrates the rise in Web-based virus attacks. While email-based attacks remain the leading source of infections, Nimda demonstrated that merely an innocent visit to an infected Web site could lead to an epidemic. Even further, it showed that taking the drastic step of temporarily shutting down corporate email servers does not always protect an enterprise from the spread of viruses like itself, since they are able to spread in a variety of ways. What this means is that the Web itself is an entry point for malicious content, and the scope of network security must now expand to address this threat. Network security, in effect, now encompasses Web security. In addition to addressing potential threats from the SMTP protocol, administrators must focus on the HTTP and FTP protocols as potential virus transmission routes.

NEED FOR CONTENT FILTERING

In parallel with this expanded viral threat to network security, the need for filtering of Web URLs, also known as content filtering, remains acute. Inappropriate or unauthorized access to various Web sites can negatively affect organizations and academic institutions in terms of lost productivity, corporate liability, and bandwidth consumption.

Loss of productivity and ineffective learning

According to a survey conducted by U.S. based National Family Opinion (NFO), 50 percent of corporate employees regularly use the Internet for personal activities.[2] An employee with an annual salary of $65,000 who spends one hour per day surfing the Web on company time could cost a company over $8,125 per year. Multiply this number by one thousand or several thousand employees and the productivity costs to an organization from inappropriate Internet use quickly rise. In an educational setting, an hour spent chatting or playing games results in a less effective learning experience.

Corporate liability and education legislation

Internet access to inappropriate material—including pornographic or hate-related materials—can expose an organization to charges of creating a hostile work environment. Organizations and executives may be held liable for failing to enforce federal, state, and local laws regarding sexual harassment, discrimination, and child pornography if employees or students download, display, or forward inappropriate materials received over the Internet. Even cached HTML pages and images viewed in privacy may be used as evidence of criminal activity. In one example of the potential impact of inappropriate Internet material, employees at U.S. based CitiGroup and Morgan Stanley Dean Witter sued employers for distress caused by racist jokes received over company email systems.[2]

In the educational arena, the Children's Internet Protection Act (CIPA), which became law in the United States on April 20, 2001, could decrease funding at schools and libraries that fail to prevent exposure of minors to inappropriate Web content and fail to institute content filtering. CIPA imposes restrictions on the universal service assistance available through the Library Services and Technology Act, Title III of the Elementary and Secondary Education Act, and the Universal Service discount program known as "E-rate."

Bandwidth consumption

Unauthorized bandwidth usage—bandwidth that carries traffic without benefit to the organization—can result in bottlenecks that slow legitimate network traffic and activities. Applications that require sustained Internet access (e.g., streaming media such as Internet Radio, Pointcast/EntryPoint, and stock ticker agents) can negatively affect network performance. Upgrading to a faster line in an attempt to improve performance only increases ongoing costs.

Requirements for a Web content security solution

A Web content security solution with both proactive antivirus scanning and intelligent content filtering at the HTTP/FTP gateway provides two-tier protection against the "Web vector"access point being increasingly exploited. Since viruses typically exploit the weak link in a system, including only one type of protection exposes the network to potential infection.

Of equal importance, the Web content security solution must not interfere with the normal flow of business or impair the learning process in educational institutions. Slow-to-respond client machines lead to helpdesk complaints, frustrated students and teachers, and administrative headaches. Antivirus scanning and intelligent content filtering must be performed without introducing latency; a high-performance, high-throughput solution is needed. Integration between the two scanning functions, plus centralized administration, ensures a high-performance low-latency solution.

The primary requirements for a Web content security solution include the following:

- Proactive antivirus scanning
- Intelligent content filtering
- Centralized administration and reporting tools
- Automated updating

PROACTIVE ANTIVIRUS SCANNING

Viruses and malicious code have evolved from transmission primarily via removable media to transmission via email, and now to propagation via the Web. In each step of this evolution, virus writers have exploited the least protected media or transmission route.

In this ongoing joust with writers of viruses and malicious code, proactive antivirus scanning at the HTTP/FTP gateway minimizes exposure to potentially lethal executables and provides the same level of protection for Web-based email, HTTP/FTP downloads, and Web page browsing that is provided for SMTP email. As with context filtering, a product that provides antivirus scanning at the HTTP/FTP gateway, which is list-based and heuristic, protects the organization from both known and unknown malicious code.

INTELLIGENT CONTENT FILTERING

In the past, content filtering techniques used lists of known Web site URLs with inappropriate content. Although this solution provided a relatively effective way of blocking access to known problem Web sites, the software vendors' ability to find and update the list of URLs limited this technique. This method of filtering is losing its effectiveness due to changes in the way that Web content is delivered. Today, URLs are rapidly redirected or use multiple host IPs. And cached pages can give users access to restricted content even if a specific site address is blocked.

Intelligent content filtering combines list-based URL blocking with heuristic analysis—a technique similar to methods used in some advanced virus protection products. Heuristic analysis checks for keywords within the HTML page and compares word relationships to understand the context of the keywords.

Keyword filtering, without checking for context, might unnecessarily block sites that are part of a legitimate search request. For example, a student may initiate a search on breast cancer. Access to sites that include the word "breast" when found in association with the word "cancer" would be permitted. But without the ability to filter content intelligently, a medical site that contained the word "breast" might be blocked as a potential pornographic site. The Gamble House, an example of Greene and Greene architecture in Pasadena, California, provides another example. Without contextual filtering capabilities, a search for Gamble House might be perceived as an illegal gaming activity.

In addition to traditional URL filtering, content filtering has assumed new meaning in the wake of threats such as Nimda. In a Web site-based viral attack, content filtering also enables administrators to deny access to legitimate sites with known infections.

Besides providing protection from inappropriate material and potentially infected sites, content filtering improves network performance by reducing the amount of Web-based traffic that passes through the firewall and across the network. Reducing traffic flow enhances the overall reliability and security of these critical services.

Further, content filtering can enable administrators to block access to Web sites that offer potentially harmful hacker programs and other malicious programs. Although most malicious code reaches corporate networks inadvertently, without content filtering disgruntled employees could access the large number of hacker-oriented sites and download tools.

CENTRALIZED ADMINISTRATION AND REPORTING TOOLS

IT organizations also need flexible, centralized administration and reporting tools. Sufficient granularity, particularly in the area of access permissions, is required to address an organization's needs and respond to change. Examples of granularity include time-of-day, type-of-user, geographic location, and need-to-know categories.

A product that includes automated alerts to notify IT administrators when it detects multiple attempts to access restricted sites is required. For example, if an employee seeks access to hacker sites in search of destructive tools, the administrator is notified automatically.

AUTOMATIC UPDATING

A content security program is only as effective as its last update. With the rapid pace of change in the Internet environment, automatic updates are a requirement for any network security system. Updates include the identification of new malicious code and URL addresses for Web sites with inappropriate content. Security products that allow system administrators to update and add new scan engines without redeploying the software provide effective protection.

Symantec Web Security: Integrated virus protection and content filtering

Symantec™ Web Security provides both content filtering and antivirus protection for enhanced content security at the Web gateway. By including both filtering and antivirus capabilities in a single integrated product, Symantec provides a high-performance low-latency solution. Symantec Web Security includes the following features:

- List-based and heuristic filtering
- Up-to-date protection through Symantec technologies
- Centralized administration and auditing tools

LIST-BASED AND HEURISTIC FILTERING

Symantec Web Security features a two-level "safety-net" with list-based and heuristic filtering that blocks inappropriate Web content and malicious code (see Figure 1). The first level determines whether the URL is allowed (based on a URL list and established permissions). The second level determines if the incoming content is truly "clean"—free of malicious or inappropriate content. Both (virus and content) scans on inbound content are achieved in a single pass, resulting in a high-performance product for protecting the Web gateway.

The patented content analysis technology, Dynamic Document Review™ (DDR), analyzes word relationships in 14 languages, preventing a user in the United States from circumventing the organization's AUP (Acceptable Use Policy) by using a language other than English.

UP-TO-DATE PROTECTION THROUGH SYMANTEC TECHNOLOGIES

Symantec owns both the content filtering and antivirus technologies used in Symantec Web Security. Because the research, development, and support of all antivirus technologies, international URL filter lists, and patented multi-lingual DDR content-analysis technology is conducted in-house, users are assured of the most effective, up-to-date protection. Regular, automated updates are included with the product.

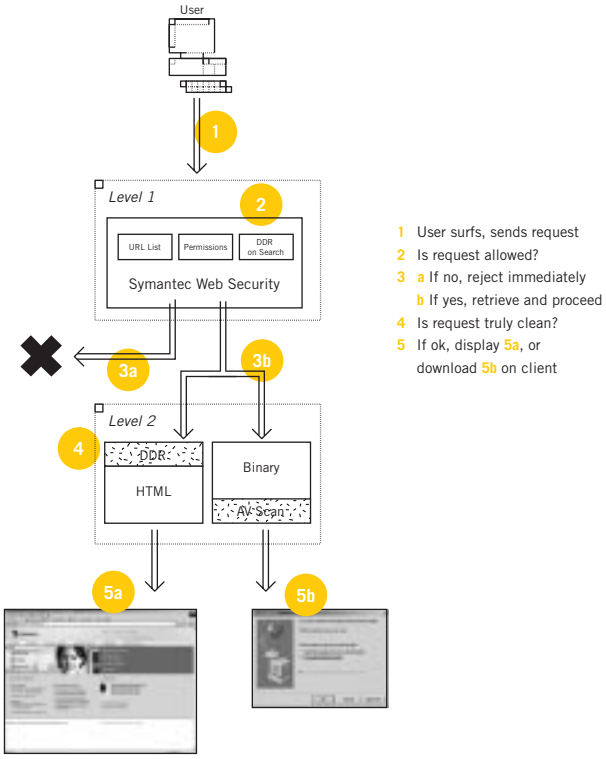

Figure 1. Symantec Web Security supports two levels of integrated scanning.

In addition, Symantec™ Web Security leverages the following Symantec response technologies for automatic virus detection and protection:

- Norton AntiVirus Extensible Engine Technology (NAVEX™) is a modular virus-scanning engine that reprograms the Norton AntiVirus™ engine to detect new classes of viruses—without having to uninstall existing software or redeploy new software. All Symantec antivirus products can be upgraded regardless of server platform and without the need to shut down the scanner or reboot the system. NAVEX and the Symantec Digital Immune System™ ensure the highest level of automatic virus detection and protection.
- The Symantec Striker™ detection system patrols the enterprise for worms, malicious code, and mobile code. Striker offers multi-level detection and high-speed resolution by applying profiles that can identify entire classes of viruses.
- Symantec Bloodhound™ technology is capable of detecting 80% of new and unknown executable file viruses including malicious mobile code.
- LiveUpdate™ provides scheduled or on-demand updates to assure protection without interruption of daily activities.

CENTRALIZED ADMINISTRATION AND AUDITING TOOLS

Symantec Web Security centralized server-based management allows IT administrators to create customized browsing profiles based on individuals, PCs, and groups. A high level of granularity is provided, allowing access according to time-of-day, title, geographic location, or need-to-know. Predefined content categories including pornography, sports, gambling, and news are provided for easy filtering. Other categories can be easily established to match the needs of the organization.

Web activity is monitored, logged, and analyzed so that even when sites are not blocked the organization can monitor Web content being accessed. Auditing tools help assess adherence to the organization's Internet policies and automated alerting tools help guard against illegal activity, such as access to hacker sites.

Summary

Evolving Web-based threats necessitate an integrated, multi-faceted network security solution. Proactive virus protection at the HTTP/FTP gateway, which complements email-based protection, coupled with content filtering has become a requirement to ensure secure networks in enterprise and academic environments.

Symantec™ Web Security secures an organization's Web traffic with high-performance, low-latency scanning for viruses and inappropriate content at the gateway. By combining list-based prevention with heuristic content analysis for both virus protection and content filtering, Symantec Web Security improves network performance and user productivity while eliminating malicious code and inappropriate content.

References

1. ICSA Labs 6th Annual Computer Virus Prevalence Survey 2000.
2. Berg, Al. "Pulling the Plug on Surfing and Spam," Information Security, April 2000.

SYMANTEC, THE WORLD LEADER IN INTERNET SECURITY TECHNOLOGY, PROVIDES A BROAD RANGE OF CONTENT AND NETWORK SECURITY SOFTWARE AND APPLIANCE SOLUTIONS TO INDIVIDUALS, ENTERPRISES, AND SERVICE PROVIDERS. THE COMPANY IS A LEADING PROVIDER OF VIRUS PROTECTION, FIREWALL AND VIRTUAL PRIVATE NETWORK, VULNERABILITY ASSESSMENT, INTRUSION PREVENTION, INTERNET CONTENT AND EMAIL FILTERING, AND REMOTE MANAGEMENT TECHNOLOGIES AND SECURITY SERVICES TO ENTERPRISES AND SERVICE PROVIDERS AROUND THE WORLD. SYMANTEC'S NORTON BRAND OF CONSUMER SECURITY PRODUCTS IS A LEADER IN WORLDWIDE RETAIL SALES AND INDUSTRY AWARDS. HEADQUARTERED IN CUPERTINO, CALIF., SYMANTEC HAS WORLDWIDE OPERATIONS IN 38 COUNTRIES.

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.