Symantec Firewalls & VPNs

WHITE PAPER

symantec™

Understanding firewalls: secure gatekeepers for your business

INSIDE

Contents

Executive Summary

In today's networked business environment the need for security can only grow. Businesses are attacked everyday through their networks and, based on the nature of the attack, businesses can lose data, productivity, and money.

Firewalls are an important component in any business network security plan. This paper will discuss firewalls, their components and functions, and how they help businesses protect their assets.

In the past few years, firewalls and firewall technology has leapt ahead. Today's firewalls come in both software and appliance product lines. There are firewalls appropriate for the perimeters of a business, for desktops, and for functions, including virtual private networking, that actually extend the secure perimeter of the business when needed.

This paper will also show that today's firewalls aren't just for large enterprises—there are firewall products available for businesses of all sizes. Some firewalls protect small businesses in the same manner as big businesses and others make the enterprise as nimble as any small business. This paper will help businesses understand the kind of firewall appropriate for their needs, and what to expect from a specific type of firewall.

Today's Firewalls

Network connectivity and the blending of private networks with the computing infrastructures that sit on top of those networks has changed the way business works. As information becomes more valuable, and at the same time more transportable, it is more important than ever to protect data and network assets while facilitating information transfer between protected and unprotected segments of the network.

If you own a business or manage your company's information technology and networking infrastructure, taking care of what's there can prompt questions:

- Is your business network connected to the Internet
- Is there confidential information accessible through your network
- Are your employees and information assets protected
- Do you have remote or mobile workers; how are their systems protected
- Do you have remote offices; do they have information assets that need protection
- Have you suffered financial losses because of attacks
- Are you happy with the level of protection you currently have in place; do you have protection in place

Firewalls are one of the primary tools since they stand at the gateways of businesses, protecting assets and examining all communications that enter. Today's firewalls are the best way to safeguard information assets on servers, at desktops, and on the road.

Firewalls 101

What is a firewall? What do firewalls do? In the past few years, they've come a long way in technology and their ability to protect networks.

A firewall is a system, hardware- or software-based, mounted strategically at the edge of, or inside of, private or closed networks. It prevents unauthorized access into those networks or segments of those networks. This is why they are called perimeter defense mechanisms or security gateways. There are also desktop firewalls that function to protect an individual computer from malicious attacks.

Depending on the needs of the business, firewalls can be software, hardware, or both. A good firewall will examine all traffic coming into the protected network or segment from the Internet or external network. It provides protection by analyzing network traffic and permitting entrance based on pre-established rules. It blocks any traffic that doesn't meet specified, rules-based security criteria.

FIREWALL TYPES AND FUNCTIONS

Most commercial firewalls mix characteristics from several firewall technologies, creating hybrid firewalls, but the five basic types are

- packet filtering
- stateful inspection
- circuit-level gateway
- application gateway
- hybrid firewall

Packet filtering is often employed on simple routers. A packet-filtering firewall examines incoming and outgoing IP packets and decides to accept or deny access based on one or both of the following:

- the source or destination of the IP address
- the source or destination of the TCP/UDP port numbers

Remember that packet filtering only looks at the IP packet header, not the data contained within the packet—this limits the types of security decisions that can be made.

Stateful inspection provides a higher level of security and complexity than does the simple packet filter. A firewall implementing stateful inspection examines IP headers, as well as the flags and header IP options within the packet, to verify that the packet is part of an authorized connection. These kinds of firewalls can also provide network address translation (NAT) services.

A circuit-level gateway looks at the TCP handshaking process. It allows the creation of authorized connections but it doesn't monitor data traffic over those connections. It also keeps records of active, authorized connections, and allows network traffic only over those connections.

An application gateway screens packets by looking at all of the information contained within the packet, including both the IP header and data portion. This ensures that not only is the connection permitted by security rules, but that it follows the proper commands and specifications of the application protocol. The application gateway also acts as an application proxy, meaning that it allows no direct connection between the host and remote computers. This kind of firewall is considered by many to offer the most security.

Hybrid firewalls combine various functions from other firewalls, most often packet inspection and proxy capabilities.

OTHER CRITICAL CAPABILITIES

Today's firewalls have capabilities far beyond the filtering, inspection, gateway, and proxy functions that enterprises expect, including authentication, management, virtual private networking, encryption, high availability and load balancing, network address translation, logging and reporting, and backup.

Authentication

Authentication identifies individuals with user names and passwords. These sign-on capabilities strengthen a company's security posture to ensure that sensitive information gets to the right people. Many of today's firewalls support authentication—either in-band or as authentication proxies—acting as intermediary systems between the firewall and authentication servers.

Management

Management capabilities are critical to any significant network security component because of the many different security elements that need to work together in order to deliver the best protection. Security administrators need to be able to monitor and control all activity, including security elements. Good firewalls supply a variety of tools and utilities to manage, monitor, and work with the firewall systems and security management frameworks. These tools could include the graphical management console, event notification, log file tools, configuration reports, and/or packet-sniffing utilities. Some even offer remote access to the system's operating environment for troubleshooting.

Virtual Private Networks

Virtual Private Networks, or VPNs, are becoming practical ways to extend business—both large and small—beyond the confines of a specific place. VPNs become important as businesses pursue business alliances or need connectivity between main and satellite offices. They also provide protected access to organizational resources for telecommuters or mobile workers.

Encryption

Encryption, a method of scrambling or coding information that passes across public networks, is the most effective way to ensure the security of data. Firewalls can encrypt data from an authorized user and let that information pass through the firewall onto a public network. The firewall protecting the receiving network can then inspect the message, decrypt it, and deliver it to the correct authenticated user. By using encryption, most firewalls can now act as VPN gateways, sometimes doubling as VPN servers by protecting information passed from site-to-site over the Internet. VPN client support for individual remote PCs used by telecommuters or traveling workers is also an option, depending on the type of firewall.

High availability and load balancing

It is important to eliminate single points of failure in the network environment. Traditionally, firewalls have been a bottleneck and a single point of failure because all Internet traffic addressed to the business needed to pass through the firewall. The traditional approach was to use a stand-by firewall however, this could be quite expensive when used only for disasters or failures. The best approach to eliminate this problem and protect today's environments is to use a high-availability, load-balanced (HA/LB) solution.

High-availability, load-balanced solutions designed into firewalls allow administrators to configure specific systems, all of which are already processing traffic, as part of the larger cluster. If one firewall host in the cluster fails, the high availability mechanism simply redirects traffic to the functioning firewall, with virtually no network interruption. Load balancing will ensure all systems are facilitating network traffic to make the most of your investment.

Network address translation

Hiding the actual network topology of protected networks is important for comprehensive network security. Enterprise firewalls can hide IP addresses on the networks they protect. Security administrators should have the freedom to customize how the firewall enables address translation—especially when it is necessary to hide the identity of certain inside hosts—while leaving other hosts accessible by their true IP address. Firewalls can also apply address translation to clients as they pass through the firewall to gain access to data at another location.

Logging and reporting

Successful security management includes monitoring. Today's firewalls often provide utilities to view log files directly by applying filters for customized searches through the logs and securely transferring them from the firewall system to a remote processing location. Firewalls can also be configured to notify security administrators of events logged at any message level. Look for reporting tools that detail the access controls configured, code versions, and licensed features.

Backup

Because they are more functional than ever, this new generation of firewalls becomes almost self-managing—by taking backups, offering a restore option, and managing the underlying system routes directly—often through a browser.

Software or appliance

Firewalls deliver a wide variety of capabilities in both software and appliance forms. Appliances feature hardware integrated with software and firmware, plus their own hardened operating system kernel. Software firewalls can be hosted on workstations or servers already in your business's network, or that are purchased for this purpose.

Firewall appliances are convenient and easy to install. Usually, they are designed to *plug and protect,* making them operational in minutes. They ensure security more effectively, because of their design, and are often the best choice for businesses without setup security-specific IT resources—because they lower the complexity of firewall security setup as well as total cost of ownership.

Software firewalls can be installed on multi-processor systems that offer better scalability than single-processor appliances. Large enterprises must examine their traffic requirements to determine whether a software or appliance firewall will meet their needs based on the amount of traffic they have to manage. Software firewalls often provide many more sophisticated functions. They can also be cost-effective, because they can be installed on existing hardware.

Firewalls and business

Today, nearly every operating system, communications protocol, or application running in any business, anywhere, has inherent security vulnerabilities. The consequence of these vulnerabilities is that most enterprises are left open to many types of attacks, from hostile outsiders to accident-prone insiders. Hackers and attackers alike take aim at a company's ability to do business by attacking its networks, computing infrastructures, and information assets. It is the prevention of penetration attacks, malicious code, and employee abuse that stops the disclosure of confidential customer or company data, the interruption of services, and the corruption or loss of important data.

THREATS COME IN ALL SHAPES AND SIZES

The annual 2001 FBI/Computer Security Institute survey is a snap shot of just how vulnerable business is to security breaches and attacks: 85% of the businesses responding said that break-ins had occurred during the previous 12 months, 64% of which suffered financial losses from those attacks. The Internet gateway in 70% of these businesses was the point of most frequent attack.

There are hundreds of attack profiles that businesses must protect against—these are just a few:

- application-level attacks, which target common server or client applications
- routing-based attacks
- IP-fragmentation attacks
- IP source routing attacks
- Trojan horse viruses
- cache-poisoning attacks
- remote client attacks
- application protocol-level attacks
- blended threats

Each of the attack types listed above creates problems for businesses by corrupting data, shutting down systems, or enabling the disclosure of important information. Blended threats—like CodeRed and Nimda—may be the most difficult and most damaging of all.

The Nimda worm has four alternate methods of propagation—network scanning, email propagation, visitor infection, and system hard disk attack when file sharing has been enabled over the network. Appearing first in North America and then migrating to Asia and Europe, Nimda not only took down systems, it also brought network traffic to a virtual halt through denial of service (DoS)—by allowing infected systems to continually scan the network and send infected email. It was because of this that Nimda was able to spread so quickly across the world.

CodeRed, another blended threat, launched DoS conditions at designated IP addresses, defaced Web servers, and then, with the permutation of CodeRed II, left Trojan viruses behind for later execution.

Businesses of all sizes are vulnerable, not just to attackers who are focused on them specifically, but also to general network attacks like blended threats, that threaten all businesses. Firewalls are the cornerstones of protection against these kinds of threats.

CHOOSING THE RIGHT FIREWALL TO PROTECT YOUR BUSINESS

Different businesses need different solutions, but they all need protection for the expanding and changing edges of their networks. When used alone, firewalls can protect businesses against many of these threats. But, when used in concert with other security products, firewalls offer protection against most of these threats. Depending upon the size of a business and its needs, the marketplace can offer a broad variety of excellent firewall solutions.

YOUR BUSINESS DETERMINES YOUR FIREWALL SOLUTION

Whether a company is large or small, the network that connects it internally has a perimeter. This perimeter is defined by each computing entity, host or desktop, which directly sends or receives messages from public networks. It is only the businesses that have firewalls already in place, whether on hosts or at desktops or at their network edge, that are protected.

The edge of a business's network can also extend and migrate depending on the locations of branch offices, individuals working from home, and mobile workers. Virtual private networks extend and migrate the network edge flexibly and safely when they are a characteristic of the protective firewall infrastructure.

Business size and type are important when choosing a firewall. Small, medium, and large businesses all have the same concerns but often need to protect differently.

1) Small businesses have fewer than 50 employees and are housed in a single building. Their external network connections are most often FracT1, DSL, Basic Rate ISDN, or cable modem. Usually, these businesses are knowledge worker-based and could be accounting or law firms, medical practices, or consulting firms. These businesses often have confidential materials on hand but no staff of IT or security experts. Small businesses need basic network services, including email, the Web and FTP, and sometimes end-user remote access.

Small businesses need to look for simple, easy-to-install, low-cost security and networking devices that can be managed long-term by their system administrator. It's a good idea to look for firewall products that are self-installing or, if there is no in-house expertise at all, choose to outsource for installation and security audit services .

2) Medium businesses range from 500 to 5,000 employees and often have more than one building along with small sales offices. Their Internet bandwidth needs are T1 or Primary Rate ISDN, xDSL, or cable modem. These businesses often have one or more individuals with some knowledge of security to handle network issues including running wire and configuring hubs and routers.

IT resources in medium companies are limited so it is important to find ways to leverage the best firewalls possible. The firewalls that work best in this environment are those that meet buying criteria that include certifications, excellent reviews, and awards. Security is important, but easy deployment is critical. If there are smaller branch offices associated with the business, easy setup and remote management are also important factors to consider.

It is likely that many of these businesses are still growing and the best firewall may be more powerful and full-featured that they initially need. However, most services within the firewall can be turned off, but would still be available for future use. Another important capability that firewalls bring to medium businesses is a VPN alternative to modem banks for secure, easily-managed remote access.

3) In today's business environment large companies of 5000 or more employees tend to be geographically disbursed into a variety of campuses, branch sites, and both large and small branch offices. Their bandwidth requirements are usually met with multi-T1 or T3, xDSL, or cable modem solutions.

These businesses need an assortment of firewalls that will work together throughout their geographically expanded sites. Branch sites tend to have the same needs as small and medium businesses, but the complex network environments of a company's central facilities require much higher performance in top security capabilities, and for comprehensive remote management and monitoring. VPN capabilities, enabling the mobile part of large business workforces, are extremely important.

4) Service providers, including Internet service providers, managed security providers, and storage and application providers can all offer firewalls as a value-added service to their enterprise and consumer customers. Any firewall deployed by a service provider will benefit all of their customers by reducing the costs associated with battling hackers who may well use the service provider's under-protected customers as relay points for attacks.

Firewalls in the marketplace

You know what kind of business you have, its size, and its focus. So what kinds of firewalls are available to meet your needs? The marketplace offers enterprise-class firewalls, desktop firewalls, remote firewalls, and even firewalls with VPN capabilities—firewalls that can protect and extend your business at the same time.

ENTERPRISE FIREWALLS

Enterprise-class firewalls enable multi-tier protection. They support large-scale local and remote management that extends to other firewalls in the enterprise, desktop, mobile, or branch-office classes. They frequently support VPN capabilities to extend secure networking infrastructures and integrate with large-scale networks.

These firewalls offer the strongest and most flexible authentication capabilities, allowing the businesses that deploy them to leverage their existing security databases. These are also the most feature-rich firewalls, offering automatic system hardening by disabling unneeded operating system features while supporting high availability and load balancing for fail-over security and efficient traffic throughput.

This class is built on comprehensive architectures for security policy and rules-based management. They have extensive logging and reporting capabilities enabling detailed statistical and session-trend reports or custom analysis. They provide enterprise-class gateway security with full inspection application proxy technology and automatic system hardening and monitoring.

SMALL/MEDIUM BUSINESS AND BRANCH OFFICE FIREWALLS

These mid-sized firewalls deliver security and networking capabilities for small offices and remote locations. They are usually affordably priced and easy to install and manage. Their most important functions are providing secure Internet connectivity, network protection, and integrated firewall functionality.

This class often ensures secure cost-effective access to networks for remote offices and business partners through integrated VPN capabilities. They provide high-speed access, reliable connectivity, ample bandwidth, and easy remote management and monitoring.

DESKTOP AND REMOTE FIREWALLS

These firewalls are small scale, flexible, and rapid to deploy while providing safe connection to private business networks. They not only protect desktops but provide protection for corporate networks from backdoor attacks over remote connections. The best of these firewalls reduces administration and support costs with remote installation and fast, automatic configuration. They work with enterprise and branch office firewalls to complete VPN connections by supporting an array of encryption protocols, providing added protection over the public Internet.

As part of a managed security strategy look for desktop firewalls that install on desktop and laptop PCs quickly, easily accepting automatic policy updates from security administrators.

Firewall solutions from Symantec

With its family of firewall and VPN products, Symantec™, a world leader in Internet security technology, and the leading provider of firewall and virtual private network products for businesses of all sizes, can meet your business's firewall needs—no matter what they are.

ENTERPRISE SOLUTIONS

Symantec enterprise solutions include Symantec Enterprise Firewall, Symantec Enterprise VPN, Symantec VelociRaptor™, and Symantec Firewall/VPN appliances.

Symantec Enterprise Firewall provides complete protection by integrating application level proxies, stateful inspection, and packet filtering into its unique hybrid architecture. In addition to protecting the enterprise at all levels of the network stack, Symantec Enterprise Firewall features an intuitive cross-platform manager, multi-processor/multi-threading performance, flexible authentication methods, built-in protection against Denial of Service attacks, and initial and ongoing network and operating system hardening.

To securely extend corporate perimeters to telecommuters and business partners, Symantec Enterprise Firewall seamlessly integrates with Symantec Enterprise VPN, allowing organizations to securely extend network perimeters beyond the enterprise firewall. It allows organizations to establish safe, fast, and inexpensive connections, enabling new forms of business and secure access to information for authorized partners, customers, telecommuters, and remote offices.

Symantec VelociRaptor™ is an integrated hardware and software firewall/VPN appliance that uses full-inspection technology to provide fast and secure connections to the Internet, delivering enterprise-class network security. This plug-and-protect appliance ensures complete control of information entering and leaving the network with data inspection technology that filters traffic and integrates application level proxies, network circuit analysis, and packet filtering into the gateway security architecture. To bar access to private networks and confidential information, Symantec VelociRaptor applies full-inspection scanning techniques, ensuring that data is validated at all levels of the protocol stack, including application proxies.

SMALL/MEDIUM BUSINESS AND BRANCH OFFICE SOLUTIONS

Symantec™ Firewall/VPN appliance models 100, 200, 200R meet small/medium business and branch office needs. These appliances are integrated security and networking devices that provide easy, secure, and cost-effective Internet connectivity between locations. With this all-in-one functionality, small businesses and branch offices can create a high-speed local network that enables secure access and interaction across the Internet with remote locations, business partners, and corporate networks.

These appliances can be installed quickly, offering offices with up to 30 employees a turnkey solution to secure out- and inbound Web, email, FTP, and application traffic. For larger, dispersed organizations, the Symantec Firewall/VPN appliances offer an affordable and easy-to-manage solution for extending firewall protection: IPSec gateway-to-gateway VPN access to satellite offices and branch locations, and a remote client-to-gateway IPSec VPN for traveling users.

THE DESKTOP SOLUTION

Today's enterprises demand solutions that protect the rapidly growing population of remote and mobile users from hacker attacks and prevent those systems from being used by hackers to gain backdoor access to corporate networks. As the industry's easiest-to-use and least-intrusive solution, the Symantec Desktop Firewall enables administrators to quickly rollout a highly-effective solution that works intelligently in the background, monitoring both in- and outbound communications. Symantec Desktop Firewall is optimized for always-on broadband connections such as DSL and cable modems, favored by mobile users, making it an important solution for desktops within the enterprise, offsite, and on the move.

REMOTE AND MOBILE VPN

Today's mobile workforce needs secure connections back to the heart of the business from an array of remote workplaces: the home, airports, satellite offices, or hotel rooms around the world. While the Internet is a reliable and cost-effective solution for enterprise network access it leaves systems and information exposed to attack or misuse. Symantec Enterprise VPN Client safely connects field personnel, telecommuters, and trusted partners to critical business systems and data—without leaving them vulnerable. It includes personal firewall features that can be combined with the Symantec Desktop Firewall for a comprehensive solution.

Conclusion

Protect your business, protect your livelihood, protect your future.

Large or small, at one site, at many sites, or on the road, firewalls protect a business's valuable information. They are a powerful first line of defense against threats and attacks of all kinds and are the cornerstone of any strategy to protect business networks. In concert with VPNs, they can securely protect and extend the business network, no matter where you need to do business.

Symantec™ is the industry leader in firewall and VPN technologies. If you'd like to know more about what Symantec has to offer your business, visit Symantec on the Web at www.symantec.com.

SYMANTEC, A WORLD LEADER IN INTERNET SECURITY TECHNOLOGY, PROVIDES A BROAD RANGE OF CONTENT AND NETWORK SECURITY SOLUTIONS TO INDIVIDUALS AND ENTERPRISES. THE COMPANY IS A LEADING PROVIDER OF VIRUS PROTECTION, FIREWALL AND VIRTUAL PRIVATE NETWORK, VULNERABILITY MANAGEMENT, INTRUSION DETECTION, INTERNET CONTENT AND EMAIL FILTERING, REMOTE MANAGEMENT TECHNOLOGIES, AND SECURITY SERVICES TO ENTERPRISES AROUND THE WORLD. SYMANTEC'S NORTON BRAND OF CONSUMER SECURITY PRODUCTS LEADS THE MARKET IN WORLDWIDE RETAIL SALES AND INDUSTRY AWARDS. HEADQUARTERED IN CUPERTINO, CALIF., SYMANTEC HAS WORLDWIDE OPERATIONS IN 37 COUNTRIES.

FOR MORE INFORMATION, PLEASE VISIT WWW.SYMANTEC.COM

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

The information in this document is subject to change without notice and must not be construed as a commitment on the part of Symantec Corporation. Symantec assumes no responsibility for any errors that may appear in this document. Symantec and the Symantec logo are U.S. registered trademarks of Symantec Corporation. Other brands and products are trademarks of their respective holders. All product information is subject to change.