Deploying Firewalls Throughout Your Organization

Avoiding break-ins requires firewall filtering at multiple external and internal network perimeters.

Firewalls have long provided the first line of defense in network security infrastructures. They accomplish this by comparing corporate policies about users' network access rights to the connection information surrounding each access attempt. User policies and connection information must match up, or the firewall does not grant access to network resources; this helps avert break-ins.

In recent years, a growing best practice has been to deploy firewalls not only at the traditional network perimeter—where the private corporate network meets the public Internet—but also throughout the enterprise network in key internal locations, as well as at the WAN edge of branch office networks. This distributed-firewall strategy helps protect against internal threats, which have historically accounted for a large percentage of cyber losses, according to annual studies conducted by the Computer Security Institute (CSI).

The rise of internal threats has come about by the emergence of new network perimeters that have formed inside the corporate LAN. Examples of these perimeters, or trust boundaries, are between switches and back-end servers, between different departments, and where a wireless LAN meets the wired network. The firewall prevents access breaches at these key network junctures, ensuring, for example, that sales representatives are unable to gain access to the commission tracking finance system.

Placing firewalls in multiple network segments also helps organizations comply with the latest corporate and industry governance mandates. Sarbanes-Oxley, Gramm-Leach-Bliley (GLB), Health Insurance Portability and Accountability Act (HIPAA), and Payment Card Industry Data Security Standard, for example, contain requirements about information security auditing and tracking.

Protecting All Points of Access

The private-public network edge is still considered particularly vulnerable to intrusions, because the Internet is a publicly accessible network and falls under the management purview of multiple network operators. For these reasons, the Internet is considered an untrusted network. So are wireless LANs, which—without the proper security measures in place—can be hijacked from outside the corporation when radio signals penetrate interior walls and spill outdoors.

It is still critical to protect the LAN-WAN edge. However, network firewalls now must also keep communications between internal network segments in check so that internal employees cannot access network and data resources that corporate policy dictates are off-limits to them. By partitioning the corporate intranet with firewalls, departments within an organization are offered additional defenses against threats originating from other departments.

All contents are Copyright © 1992–2006 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

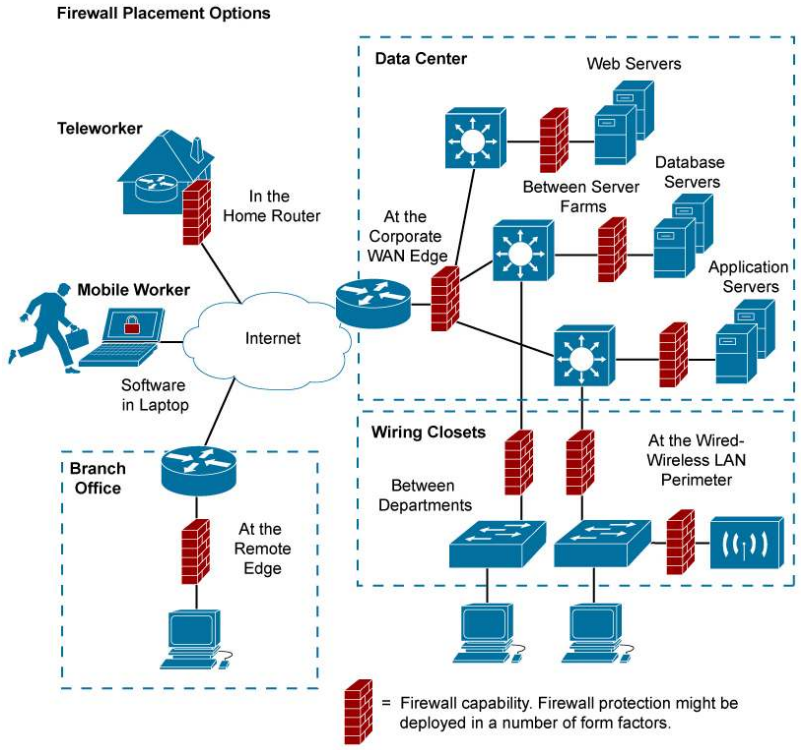
In addition, network usage continues to rise, as employees become geographically more dispersed across branch offices and increasingly use mobile and remote networks. Now, nearly 90 percent of employees work in branch offices, away from the headquarters facility, according to Nemertes Research, a firm specializing in quantifying the business impact of technology. As a result, a network perimeter now exists also at the edge of each branch office network, where a WAN access router meets the public Internet or other wide-area network. This edge must also be protected.

In its role as the first line of security defense, then, the firewall has a place in the following network segments:

- At the traditional corporate network perimeter (where the data center meets the WAN and Internet)
- Between departments, to segregate access according to policy among user groups
- Between corporate LAN switch ports and Web, application, and database server farms in the data center
- Where the wired LAN meets the wireless LAN (between Ethernet LAN switches and wireless LAN controllers)
- At the WAN edge of the branch office
- In laptops, smartphones, and other intelligent mobile devices that store corporate data (in the form of personal firewall software) in the case of telecommuters and mobile workers

Figure 1 shows a sample configuration of firewalls deployed throughout an enterprise.

Figure 1. Sample Enterprise Firewall Configuration



Basic firewall filtering is recommended at every trust boundary, externally and internally, throughout the enterprise network.

All contents are Copyright © 1992–2006 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Internal Versus External Attacks

Many organizations continue to attribute a significant percentage of their corporate "cyber losses" to inside attacks, indicating the need for more robust firewall filtering throughout the enterprise network segments. Well over a third (39 percent) of the corporate respondents to the 2006 Computer Crime and Security Survey, for example, attributed 20 percent or more of these losses in 2005 to internal attacks. This annual survey is conducted by the CSI with the participation of the San Francisco FBI Computer Intrusion Squad. Of the 616 respondents to the 2006 CSI report, 313 were able or willing to estimate their losses associated with Internet crime in 2005.

A more dramatic finding was that 7 percent of the 313 CSI survey respondents quantifying cyber losses attributed more than 80 percent of these losses to insiders. The CSI survey respondents were primarily from large companies and government entities spanning all vertical industries; more than a third (34 percent) had annual revenues of US$1 billion or more and 57 percent had $100 million or more in revenues.

"Unauthorized access to information" accounted for $10.6 million of the nearly $52.5 million in cyber losses that the 313 survey respondents reported in 2005. It was the second-largest contributor, next to viruses ($15.7 million). The "theft of proprietary information" accounted for $6 million of the cyber losses, ranking as the fourth largest contributor following "laptop or mobile hardware theft" ($6.6 million).

Since unauthorized access and theft are still substantial, the strategic placement, configuration, and management of firewalls throughout the enterprise clearly remain critical, and further enterprise investments need to be made. Internal firewall deployment is at the heart of preventing these losses, working with other security architecture components to combat the full suite of security threats.

Role in the Overall Security Architecture

When investigating network protection mechanisms, it is important to recognize the existence of multiple threat vectors to a given enterprise: attacks, intrusions, and Internet threats. In the case of attacks and intrusions, hackers attempt to improperly access information resources from inside or outside the organization. Internet threats take the form of viruses, spyware, and other types of malware. These are introduced from the Internet to an unsuspecting user during everyday communications activities, such opening an e-mail attachment or downloading a file.

Because there are myriad threat vectors, firewalls are usually paired with intrusion prevention systems (IPSs), as well as with endpoint security systems (also called anti-X and gateway anti-malware systems). IPSs provide another layer of internal security by detecting and blocking known malicious traffic and anomalous traffic patterns. Endpoint security systems check remote client devices for viruses and ensure that client software is in compliance with the organization's current software versions and standards. They also support URL, or content filtering. In addition, most firewalls today inherently support virtual private network (VPN) technology, which encrypts data to avoid its theft in transit.

The various security components can reside in converged devices or can be deployed separately, depending on an organization's preferences and requirements for performance, consolidating functions, and capital budget. Table 1 shows form factor options available from Cisco® and a sampling of implementation considerations.

All contents are Copyright © 1992–2006 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Table 1. Cisco Firewall Options and Deployment Considerations

Network Location	Cisco Platform(s)	Decision Criteria
WAN edge: Corporate headquarters or branch office	Cisco ASA 5500 Series or Cisco PIX Security Appliance	Require plug-and-play capabilities (no changes needed to existing network) and very high performance. Wish to combine with IPS, SSL VPN, and anti-X security functions for stronger security, CapEx, and operational benefits using Cisco ASA 5500 Series
	Cisco IOS Firewall running on Cisco integrated services routers	Want to take advantage of firewall filtering in router software capabilities for CapEx consolidation benefits; require good performance
Between enterprise LAN switch and back-end servers	Cisco Catalyst 6500 Series Firewall Services Module (blade)	Have open slot on Cisco Catalyst switch; wish to conserve capital real estate; require very high performance
	Cisco ASA 5500 Series or Cisco PIX Security Appliance	Require high performance; no switch slot available; might wish to add integrated IPS module (on Cisco ASA 5500 Series) for stronger security and higher performance than is available when separate
Between internal departments	Cisco Catalyst 6500 Series Firewall Services Module (blade)	Have open slot on Cisco Catalyst switch; wish to conserve capital real estate; require very high performance
	Cisco ASA 5500 Series Adaptive Security Appliance	Require high performance, high degree of accuracy, and might wish to add integrated IPS module
Laptops and other mobile equipment	Cisco Security Agent / personal firewall software	Recommended in all instances where corporate data is stored on device

How Firewalls Are Evolving

In addition to being deployed in more enterprise locations, firewalls have grown more sophisticated since their mainstream introduction about a decade ago. They have gained additional preventive capabilities, such as application and protocol inspection, which help avoid exploits of operating system and application vulnerabilities.

Firewalls have been enhanced with extra preventive features such as application inspection capabilities—the ability to examine, identify, and verify application types and treat traffic according to detailed policies based on variables beyond just connection information. This helps identify, and thus block, traffic and users that unlawfully try to gain admittance to the network using an open port.

For example, the Hyper-Text Transfer Protocol (HTTP) is extensively used to transport Web data and services. It comprises about 75 percent of network bandwidth usage today and natively uses application port 80. In most firewalls, port 80 is left open at all times, so any traffic destined for port 80 is admitted. Hackers, worms, and viruses might use this pinhole, however, to attack a Web application and to possibly gain access to sensitive data.

To protect against this, application filtering involves deep packet inspection to determine exactly what HTTP application traffic is attempting to enter the network. There are many HTTP applications that organizations will wish to let onto their networks; however, there might be some that they prefer to block. The application firewall will also use deep packet inspection to determine whether the application protocol (in this case, HTTP) is behaving in an irregular manner.

Policies can be set, for example, to identify and block overly long HTTP headers or those containing binary data, which suggest a possible attack. Administrators can also set a policy to limit server requests to a certain number per minute to avoid denial of service (DoS) attacks.

All contents are Copyright © 1992–2006 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

In addition to application filtering, virtual firewall capabilities are now available that are useful particularly to organizations that have consolidated servers and data centers. Using this firewall feature, a single physical firewall can operate as several logical firewalls, allowing a single firewall in a given form factor to do the job of multiple devices and thereby helping reduce capital expenditures (CapEx).

Conclusion

Internet crime persists as a business concern. In addition, corporations now operate under the rules of corporate governance and industry mandates that carry strict requirements about controlling information security.

To best protect against improper system access, it behooves businesses to install firewalls at every major interconnectivity point in the network, both internally and externally. Some enterprises estimate that more than 80 percent of their cyber losses are from internal attacks; distributing firewall filtering throughout the organization helps alleviate unauthorized internal access by providing multiple check points.

In addition to granting or denying access to network resources based on user profiles, firewalls now also filter network traffic based on application-layer information. This filtering, which uses deep packet inspection to look deep within each network packet, allows IT departments to filter out traffic based on additional criteria. For example, noncompliant traffic using an open port to break into the network can be detected and blocked. Undesired Web application traffic, such as certain peer-to-peer traffic, can be filtered. Application filtering also helps identify suspicious traffic—and then block it—based on the way the application protocol is behaving.

The primary locations in which to implement firewall filtering are between the WAN access router and backbone switch in the corporate data center, where the private LAN meets the public Internet; between enterprise LAN switches and back-end servers; between wired and wireless LANs; at the branch-office network edge; and, in the case of mobile users, on laptops and other portable devices. In the latter instance, the form factor would be a personal firewall, a piece of client software that filters outside attempts to access the data stored on the device, not the network.

Firewalls represent the first level of access checking. They work with other security technologies, including intrusion prevention, encryption, and endpoint security, to provide a well-rounded defense-in-depth enterprise security system.

All contents are Copyright © 1992–2006 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

©2006 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0609R)

Printed in USA

C11-377025-00 11/06

All contents are Copyright © 1992–2006 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.