How Cisco IT Migrated to Stronger Firewall Protection for Large Sites

Power, speed, and new capabilities make the Cisco FWSM the firewall of choice for large sites.

Cisco IT Case Study / Security and VPN / Small Business Firewall Protection: This case study describes Cisco IT's internal use of the Cisco Firewall Services Module (FWSM) within the company's global network, a leading-edge enterprise environment that is one of the largest and most complex in the world. Cisco customers can draw on Cisco IT's real-world experience in this area to help support similar enterprise needs.

"During the migration process from the stateless ACLs to the new FWSMs, a large number of firewall holes were closed. The elimination of those holes alone was a huge win for Cisco's network security."

– Steven Song, Cisco Information Security Network Engineer

CHALLENGE

The rising volume of denial of service (DoS) attacks and other Internet threats has spurred many organizations to investigate advanced firewall technology. Within Cisco Systems®, this investigation—and the current design, deployment, and management of an advanced firewall solution—was a collaborative effort between Cisco Information Security (InfoSec) and Cisco IT. Like most corporations, Cisco needs to connect its internal networks (intranets) to the public Internet to remain competitive and successful. More than 90 percent of Cisco's revenue comes from e-commerce, and Cisco uses the Internet to provide technical support, maintain close ties to partner networks, and support VPN connectivity for the company's several thousand employees who work remotely. But while connecting to the Internet is critical to Cisco's survival, it also exposes the company's network to potential attacks from anywhere in the world. The most basic network defense is a perimeter defense, and the best form of perimeter defense is a firewall.

A firewall can be hardware- or software-based. Firewalls examine all network packets and then use access control lists (ACLs) and rules to decide whether to forward them to their destinations. While there are application-layer firewalls that examine the entire packet, most firewalls are network firewalls that restrict themselves to the network and transport layers. Network firewalls look at where a packet is coming from and going to, which port and protocol it is using, and possibly which session it is a part of, to determine if the packet is legitimate. The network firewall allows or blocks traffic in or out of the corporate network based on rules that can be any combination of this information.

The firewall attempts to allow all legitimate traffic through and to deny everything else. For example, it may only allow traffic coming from one location (perhaps a partner site) to be sent to a separate Cisco subnetwork, or it may deny all traffic using a certain port known to be used by a virus or worm.

People who design attacks on network firewalls attempt to find out which type of traffic is allowed and then mask their malicious traffic as legitimate traffic. Cisco InfoSec and Cisco IT work together to design network firewall rules that minimize the possibility that malicious traffic will be allowed through the firewall; the teams also design further layers of security in the network to block and investigate malicious traffic that may succeed in getting through the firewall. Network engineers must design and support multiple layers of defense to protect the network, and a strong firewall is an essential and critical first line of defense.

There are two general types of packet filtering performed by network firewalls: non-stateful inspection performed by

packet-filtering ACLs (used by router-based firewalls, for example), and stateful inspection performed by equipment like Cisco PIX® security appliances and the Firewall Services Module (FWSM).

Non-stateful-inspection firewall routers with ACLs have a significant weakness—they are unable to recognize the session that each packet belongs to. As a result, the firewalls have to use static rules based only on packet address and port. Firewalls using these static rules are enough to stop most malicious traffic from entering the Cisco intranet, but they have weaknesses. For example, they must always keep many ports open. Many legitimate business applications use protocols (like Trivial File Transfer Protocol [TFTP] and Simple Network Management Protocol [SNMP]) that select a port to use from a large pool of possible ports available to that application. In this case, the static firewall must allow all of those ports to remain open for that application—even though the firewall can check both the source and termination address to make sure it is coming from and going to only legitimate servers. Keeping open a large number of ports increases a firewall's vulnerability to attacks that are clever enough to exploit those permanently open ports. Another weakness is that these non-stateful-inspection firewalls can be spoofed, or fooled, by clever attackers who rewrite their packets to make them appear to be coming from a legitimate location.

Firewalls with stateful inspection can tell when packet addresses are being spoofed. They can keep out more malicious traffic—they can record the state of a traffic flow passing through in one direction so that when the flow returns in the other direction, the firewall recognizes it and passes it through to its destination. The firewall maintains a state application table that tracks each session and makes sure that only traffic that is part of a legitimate session is allowed through.

"A Cisco Technical Assistance Center engineer may connect from Cisco to a customer site over a secure VPN link to help solve a problem. This is obviously legitimate traffic," explains Michael Trahtenherts, Cisco network engineer. "But the return traffic will come from an outside address, over any one of a number of ports. Without stateful inspection, we would have to allow all traffic from all reasonable outside addresses to come through all of those possible ports. The non-stateful-inspection firewall cannot accurately determine whether traffic is part of the original, legitimate session and should be permitted. In contrast, a stateful inspection firewall creates state information for every TCP session that flows across the firewall. When the return packet comes in, the firewall just checks the state table to determine if it is part of a legitimate session, and will allow only legitimate packets into the network."

In addition to supporting stateful inspection, the FWSM allows the firewall to avoid keeping large numbers of ports open, even for applications (like those using H.323, Session Initiation Protocol (SIP), and Active FTP that need a large range of ports available to them. The FWSM uses "fix-ups" to keep track of each application session, and dynamically adjusts the ports to be kept open based on the ports that are currently in use by legitimate application sessions. The FWSM uses a state application table to accomplish this – a list of all the legitimate application session and the ports they are currently using at any given time..

This additional capability prompted Cisco IT to begin a migration to stateful inspection firewalls. "We wanted to migrate to stateful inspection firewalls at all sites because of their better security, manageability, and performance," says Amy Bock, IT engineer with Cisco InfoSec. "Not having a stateful inspection firewall is risky—you have to open large holes in the firewall to make applications work, and that's never desirable."

In evaluating stateful inspection firewalls, Cisco wanted a solution that could be easily integrated into the existing production network without requiring complex design and operations changes. "We were looking for a solution with Layer 2 transparency, that we could just pop into any router," says Trahtenherts.

SOLUTION

Cisco IT evaluated different stateful inspection firewall solutions, looking for one that would support multicast and emerging dynamic applications. "We chose the Cisco FWSM for our large sites, which provide both Internet and VPN connectivity," says Julie Nordquist, program manager for Next-Generation Corporate Firewall project. Large sites include San Jose, California; Research Triangle Park, North Carolina; Amsterdam, Netherlands; and Sydney,

Australia. Smaller Internet connectivity sites would continue to use Cisco PIX security appliances.

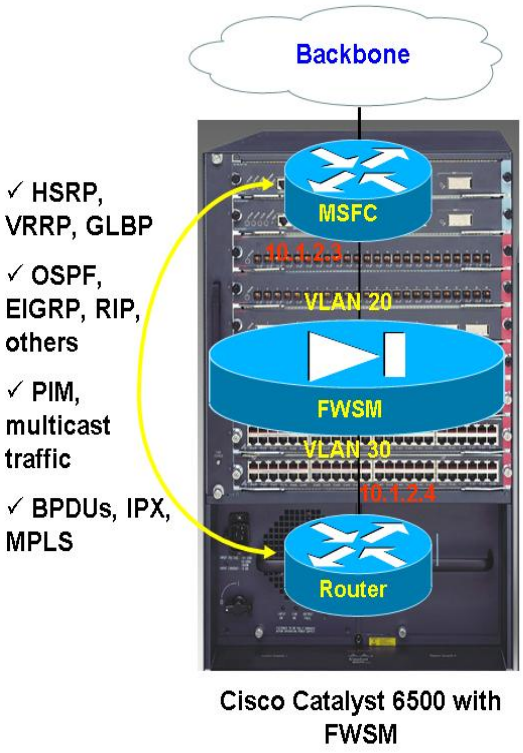
Advantages of the FWSM for Cisco include:

- Ability to pass multicast traffic through the firewall (Figure 1).
- Ability to pass Enhanced Interior Gateway Routing Protocol (EIGRP) through the firewall. The Cisco network uses EIGRP for communication among network devices.
- Performance—With aggregate throughput of 5 Gbps, and the ability to combine four FWSM blades into a single Catalyst switch to support throughput of 20 Gbps, the FWSM is the fastest and highest-performing firewall available today.
- Improved security with dynamic port applications—Applications such H.323, Session Initiation Protocol (SIP), and Active FTP require the negotiation of dynamic TCP ports when a session is initiated; the FWSM reduces the number of ports open at any time, improving security..

“Companies cannot support these applications with a stateless firewall unless they open huge holes, which is an action that has serious security implications,” says Jawahar Sivasankaran, network engineer at Cisco. “A stateful firewall would help Cisco IT support these types of applications in the future.”

Cisco deployed two redundant FWSMs at each of four sites, to provide protection for larger Internet access points on the Cisco network.

Figure 1. FWSM Transparently Passing Layer 3 Traffic



Preparation

Leading this transition were the Cisco IT Global Internetworking Solutions (GIS) team, Cisco InfoSec, and the Cisco on Cisco team, which contributed technical resources for development of the design and testing. “We used our normal global deployment processes and in-theater deployment resources,” says Nordquist.

To prepare for migration, Cisco InfoSec first converted the ACLs from the Cisco IOS® Software format to the format used by both FWSMs and Cisco PIX firewalls. “During migration, to keep it simple, we decided to keep the same firewall policy for traffic to allow and deny,” says Bock. “The change we made was to apply rules for traffic denial in the outbound direction instead of the inbound direction—a traffic session that is allowed in the outbound direction creates a state allowing return traffic that matches the session.”

The ACL conversion process took one person approximately eight hours per site, and three reviewers looked over each ACL. “During the conversion process, we closed a significant number of firewall holes,” says Steven Song, Cisco InfoSec network engineer. “With the stateless ACLs, those holes were needed for some basic business applications to work. With the FWSM’s ability to perform stateful inspection, those holes were no longer needed. The elimination of those firewall holes alone was a huge win for Cisco’s network security,”

Next, because the FWSM uses subnet masks and the Cisco IOS routers use wildcard masks, the InfoSec team wrote a script to convert the wildcard masks into appropriate subnet masks. Finally, InfoSec performed a device configuration review and security audit for the FWSM units, which is standard policy when a new host or network device is added to the DMZ. “We have guidelines and standard configurations that must be followed,” says Bock.

Testing

Testing in the Cisco Proof of Concept lab began in November 2003, using early field trial versions of the FWSM. Cisco created an exact replica of its production network, including all of the routers and switches surrounding the FWSM. The comprehensive testing included management, security, DoS attacks, and failover. The main testing focus was on Layer 2 transparency. “Layer 2 transparency is the answer for multicast and EIGRP, which other firewalls don’t support,” says Bock. The team used a traffic generator to generate high traffic volumes to validate the performance of the FWSM. Testing was conducted for several weeks, up until two weeks before the deployment.

During testing, the team assigned critical importance to testing the interoperability of the FWSM with EIGRP and other technologies. “Because the Layer 2 transparency feature creates a bridged domain, we performed extensive testing to make sure there were no Layer 2 loops, and to make sure that the Spanning Tree configuration worked in the Layer 2 domain,” says Sivasankaran.

Problem Solving

During the testing and early deployments, some bugs were discovered in early versions of the FWSM software. The solutions to these bugs have significantly improved the FWSM’s quality and scalability, providing a better product for Cisco’s general customers.

Deployment

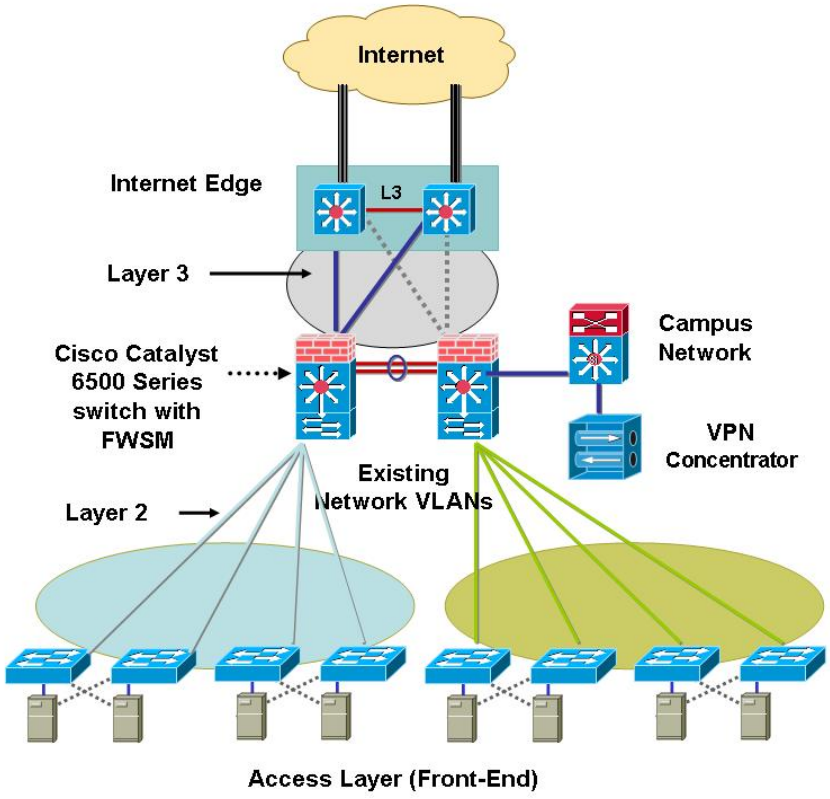
Cisco followed a three-stage process to deploy the FWSMs at each of the four sites:

- **Prepare the network by converting point-to-point links to a bridged network.** “The end goal was for the FWSM to work in Layer 2 transparent mode, which requires a bridged network,” says Sivasankaran. “We needed to convert existing point-to-point /30 links to a larger Layer 2 domain, so that all Layer 3 traffic could be passed across the firewall.” Figure 2 illustrates the deployment. After this step, the team waited 72 hours in the first site and 48 hours in the remaining sites to ensure the network continued to operate normally, which it did.
- **Install and configure the FWSMs.** The Cisco IT team configured the FWSM with virtual LANs (VLANs) and

other Layer 2 requirements, and then introduced the FWSM in the data path. The Cisco 7500 Series routers continued to provide firewall functions; the FWSMs simply passed traffic so the team could ensure that they did not introduce any problems. This stage lasted four days.

- **Begin using the FWSM security features.** The team turned off the Cisco IOS Software security features and turned on the FWSM security features. The previous routers are still in use, primarily for the Cisco NetFlow feature of the Cisco IOS Software.

Figure 2. Cisco FWSM Connecting the Internet Edge to the Existing Topology



The deployment proceeded smoothly; all deployments were completed within the change management window. “With the three-stage process, we didn’t introduce too many changes at any one time, and we completed each stage before moving to the next,” says Sivasankaran. “If we’d had an issue, we could have easily isolated it and reverted to the previous configuration without difficulty.”

RESULTS

Greater Security

The FWSM has increased the security of the Cisco network by mitigating DoS attacks, enabling applications to be deployed in a more secure manner, and reducing network visibility from the outside.

Mitigation of DoS attacks

A stateful inspection firewall improves Cisco’s ability to mitigate primary DoS attacks, which occur when a hacker tries to initiate a session with a server using a spoofed IP address and the server tries to respond. “A stateless firewall can’t identify this traffic as undesirable, and the result is that this firewall is vulnerable to a Syn flood attack,” says

Bock. “The FWSM does not allow this traffic, which better protects Cisco’s network resources.”

Fewer holes in firewall

Previously, to support dynamic services and applications, Cisco needed to open holes in the firewall, which made the network more vulnerable to hackers. Now, by configuring the FWSM in transparent mode, the network passes dynamic routing protocols and multicast traffic across Layer 3 policy boundaries. As a result, Cisco can securely enable services such as active FTP, SIP, H.323-based videoconferencing, and other dynamic services and protocols. “With a transparent firewall, we have a lot of flexibility—we don’t have to re-engineer the way traffic is routed through the network,” says Noel Shen, IT Network Engineer for Cisco GIS.

Reducing network visibility from the outside

“When configured in transparent mode, the FWSM is not detectable via normal means such as tracerouting or ping sweeps,” says Song. “Due to its transparency and lack of a publicly accessible IP address, the FWSM cannot be probed or attacked directly from outside networks.”

High Availability

“The FWSM is highly available because Cisco has implemented it in redundant fashion, with stateful failover,” says Shen. “If the active firewall becomes inactive, the failover partner assumes the active role, maintaining the state of existing connections across the firewall for an uninterrupted user experience.”

Architectural Congruence

Layer 2 transparency enables the FWSM to fit into the network without changes. “Because it offers Layer 2 transparency, the FWSM is easy to integrate into our existing architecture,” says Sivasankaran. “This allows us to maintain existing routing protocol relationships and to silently pass allowed multicast traffic through.”

Ability to Perform Sophisticated Traffic Analyses

The FWSM works with Cisco Catalyst 6500 Series and Cisco 7600 Series switches. These switches can also accommodate other service blades, such as the Network Analysis Module-2 (NAM-2), which provides protocol analysis and traffic characterization capabilities. “By combining the FWSM and the NAM-2 in the same switch, we can conduct traffic analyses both before and after firewall rules have been applied to inbound and outbound traffic,” says Roland Dobbins, Cisco IT network engineer. “This gives us sophisticated capabilities for forensic purposes, troubleshooting, and policy and conformance verification.”

High Performance

“By configuring the FWSM in transparent mode, we gained a high-performance, stateful inspection firewall that allows us to increase our security posture without changing our existing network infrastructure or topology,” says Shen. “The high performance of the FWSM enables us to take advantage of firewall features such as access list logging, which is useful for creating audit trails but increases the load on routers.”

LESSONS LEARNED

The success of the deployment arose from careful planning and a thorough understanding of the network environment. “The phased implementation was also key to success,” says Nordquist. “When you introduce change into a network, breaking the deployment into phases helps ensure service availability before, during, and after the change.

“Everything worked as it should from a project management and deployment perspective,” adds Nordquist. “Lessons learned from each global deployment were communicated to each subsequent deployment team to reduce our deployment risk exposure. When Cisco manages any global projects, the key is for project management resources to collaborate closely with the implementation team.”

"Another lesson was to really understand our own infrastructure," says Trahtenherts. "We had deployed the FWSM in many major sites, and we expected that deploying it in San Jose would be similar. But San Jose was different from all other Cisco sites. Because San Jose maintains the Cisco e-commerce Website, the amount of traffic was significantly higher. Cisco.com resides outside the firewall, which created additional issues."

The Cisco San Jose site was different in another respect, as well: it supported a lot of tools that use UDP traceroutes. This was not known to the Cisco IT team installing the FWSM. "One odd problem resulted from our closing UDP ports and denying UDP outbound traffic," says Shen. "We broke some tools that used traceroutes, since one of the operating systems uses UDP to perform traceroutes. We had to tune the FWSM to support this traffic from these tools."

"Communication with the application owners before and during the FWSM cutover was critical," says Nordquist. "We had to identify all of the application owners who could be affected by the FWSM cutover, and in San Jose, the new firewall affected a lot of applications. The owners needed to be aware that despite our planning and testing, something might happen to their applications when we cut over to the new firewall. We had to be prepared to listen to their responses and to cut back to the previous firewall if the results required us to—and they did the first time we cut over. It was also critical to listen for unusual application problems that occurred to determine if the new firewall cutover was related to the problems, and to learn how to support these applications in a safe and secure way. Keeping syslog messages from the firewalls allowed us to troubleshoot application problems more easily."

"We were a little reluctant to turn on syslog on the FWSM, since our experience with Cisco IOS Software-based firewalls was that turning on syslog can force the router's CPU utilization to be too high," says Bock. "But it turned out that with the FWSM, the CPU utilization was hardly affected by turning on syslog. So we turned on all logs—and the log information was very valuable for troubleshooting and for investigating security issues."

NEXT STEPS

Cisco has installed a stateful inspection firewall at all of the company's sites, deploying Cisco PIX security appliances at smaller sites and FWSMs at larger sites (see the Cisco PIX Firewall case study at http://www.cisco.com/web/about/ciscoitatwork/security/pix_firewall_in_enterprise_network.html). The GIS and InfoSec teams are currently evaluating policy changes to improve productivity, such as allowing outside voice and video conferencing through the firewall. An implementation guide is being developed for use in future FWSM deployments.

Another plan is object grouping—grouping devices by protocol, server name, or address. This decreases the sizes of ACLs, thereby improving manageability.

Finally, Cisco wants to use the FWSM's multiple-context feature in its data center environment to provide transparent, stateful inspection firewall capabilities for both inter- and intra-data center traffic. "The virtualization feature will allow one physical firewall to act like multiple virtual firewalls," says Sivasankaran. "We'll be able to manage one device instead of ten."

"Part of InfoSec's mission is to improve network security without affecting business productivity," says Bock. "With its Layer 2 transparency feature and stateful inspection capability, the FWSM supports that goal."

FOR MORE INFORMATION

To read the entire case study or for additional Cisco IT case studies on a variety of business solutions, visit Cisco on Cisco: Inside Cisco IT www.cisco.com/go/ciscoit

NOTE

This publication describes how Cisco has benefited from the deployment of its own products. Many factors may have contributed to the results and benefits described; Cisco does not guarantee comparable results elsewhere.

CISCO PROVIDES THIS PUBLICATION AS IS WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some jurisdictions do not allow disclaimer of express or implied warranties, therefore this disclaimer may not apply to you.

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.**