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.

BUSINESS BENEFITS

- Greater security achieved by mitigation of DoS attacks and fewer holes in firewall
- High availability
- Easy integration as a result of Layer 2 transparency
- Sophisticated traffic analysis
- High performance

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

– Steven Song, Cisco Information Security Network Engineer

The rising volume of denial of service (DoS) attacks and other Internet threats has spurred many organizations to investigate advanced firewall technology. Like other companies, Cisco Systems® needs to connect its intranets to the public Internet to remain competitive and successful. But while connecting to the Internet is critical to Cisco's survival, it also exposes the network to potential attacks from anywhere in the world. Cisco® IT and Cisco Information Security (InfoSec) collaborated to design, deploy, and manage an advanced firewall solution as a critical first line of defense.

There are two general types of packet filtering performed by network firewalls : nonstateful inspection performed by access control lists (ACLs), and stateful inspection performed by equipment such as Cisco PIX® security appliances and the Cisco Firewall Services Module (FWSM). Firewalls without stateful inspection have significant weaknesses. To accommodate traffic from numerous business applications, they must always keep many ports open, increasing their vulnerability to attacks.

A stateful inspection firewall was the needed solution. That technology would tell when packet addresses were being spoofed, and thereby mitigate malicious traffic and DoS attacks. The Cisco FWSM maintains a state application table for every TCP session that flows across the firewall, making sure that only legitimate traffic is allowed through.

Previously, to support dynamic services and applications, Cisco needed to open holes in the firewall. Now, by configuring the Cisco 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, Session Initiation Protocol (SIP), H.323-based videoconferencing, and other dynamic services and protocols.

The Cisco FWSM features protocol analysis and traffic characterization capabilities. Deploying the FWSM and the Network Analysis Module (NAM-2) in the same Cisco Catalyst® 6500 or Cisco 7600 switch enables sophisticated traffic analysis, troubleshooting, and policy verification.

With aggregate throughput of 5 Gbps, and the ability to combine four FWSM blades into a single Cisco Catalyst switch to support throughput of 20 Gbps, the Cisco FWSM is the fastest and highest-performing firewall available today.

The Cisco FWSM supports multicast and emerging dynamic applications.

Case Study: http://wwwin.cisco.com/it/technology/at_work/sec-fwsm.shtml

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.**