How Cisco IT Deployed Cisco Firewall Services Modules at Scientific Atlanta

Deployment increases network security, reliability, and availability.

Cisco IT Case Study / Security / Firewall Services Module: This case study describes Cisco IT's internal deployment of the Cisco® Firewall Services Module (FWSM) within the network of the former Scientific Atlanta company, which was acquired by Cisco in February 2006. Cisco customers can draw on Cisco IT's real-world experience in this area to help support similar enterprise needs.

"The failover capability of the Cisco FWSM is seamless and nearly instantaneous. We could lose several ports in the primary module and never notice it because the transition to backup occurs so quickly."

– Kelly Alexander, Network Architect, Cisco Information Security Group

BACKGROUND

On November 18, 2005, Cisco announced its acquisition of Scientific-Atlanta of Lawrenceville, Georgia. Scientific Atlanta is a leading global provider of set-top boxes, end-to-end video distribution networks, and video systems integration. The acquisition allows Cisco to offer a world-class, end-to-end data, voice, video, and mobility solution for carrier networks and the digital home. With the addition of Scientific-Atlanta technologies, the Cisco IP Next Generation Network architecture offers providers an open platform for service differentiation, allowing them to move beyond digital video/IPTV to develop and deliver a variety of integrated media services in the connected home.

CHALLENGE

As with every Cisco acquisition, the network of the organization being acquired must conform with and become integrated into the larger Cisco worldwide network. In the case of Scientific-Atlanta, this meant integrating a network that supported 7500 employees worldwide. The company's headquarters location consisted of a five-building campus with approximately 2000 employees. Another 15 sites were scattered around the globe, including a manufacturing facility in Mexico.

Scientific-Atlanta's network infrastructure, including firewalls, was built on equipment from non-Cisco vendors. In an effort to conform fully to Cisco IT standard architecture and design principals, plans were drawn to replace and upgrade non-Cisco equipment. Among the highest priorities for replacement were the firewalls, which would no longer be supported by the supplier in less than six months. Before being acquired, Scientific-Atlanta had planned to upgrade the firewalls with the latest product version from the same equipment vendor. Once part of Cisco, Scientific Atlanta committed to replace the firewall devices with a Cisco solution.

EXECUTIVE SUMMARY

BACKGROUND

- Cisco announced its acquisition of Scientific-Atlanta of Lawrenceville, Georgia.

CHALLENGE

- Scientific-Atlanta's network infrastructure, including firewalls, was built on equipment from non-Cisco vendors.
- Scientific-Atlanta's firewalls would not be supported by the supplier in less than six months..

SOLUTION

- Cisco standardized the deployment of firewall solutions across its worldwide network, using the Cisco Firewall Services Module (FWSM) for its largest sites.

RESULTS

- The deployment of Cisco FWSMs within the Scientific-Atlanta network has provided conformity to Cisco IT standards.
- From an operational standpoint, the reliability and availability of the FWSMs is far superior to the previous firewall solution.

LESSSON LEARNED

- Due to the architectural differences between the old firewalls and the Cisco firewalls, it was necessary to convert the existing rule sets for the new firewalls.

NEXT STEPS

- Once the Multiple-context Transparent mode standard is approved, the data center firewalls at Scientific Atlanta will be converted from Single-context Routed mode to Multi-context Transparent mode.

SOLUTION

In 2005, Cisco standardized the deployment of firewall solutions across its worldwide network, using the Cisco Firewall Services Module (FWSM) for its largest sites. "We chose the Cisco FWSM for our larger sites, which provide both Internet and VPN connectivity," says Julie Nordquist, program manager for Next-Generation Corporate Firewall project. Smaller Internet connectivity sites continue to use Cisco PIX® security appliances. (Refer to http://www.cisco.com/web/about/ciscoitatwork/security/enterprise_firewall_protection.html for a case study on the evaluation and selection of Cisco FWSM for large Cisco sites.) "Considering the size of the Scientific-Atlanta network and anticipated growth, we decided that Cisco FWSM was the best solution," says JJ Kim, the lead network engineer for the architecture and design of the DMZ network integration at Scientific-Atlanta.

Key advantages of the Cisco FWSM include:

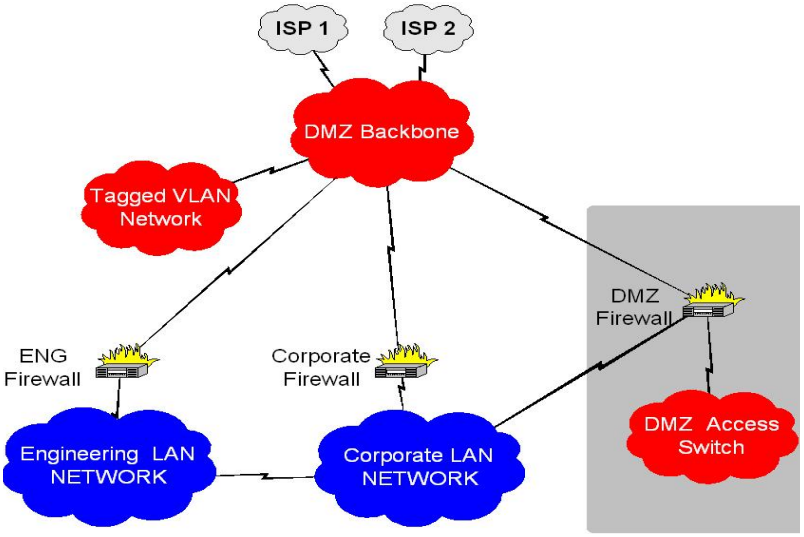
- Outstanding performance with aggregate throughput of 5 Gbps and the ability to combine up to four FWSM blades into a single Cisco Catalyst® switch to support throughput of 20 Gbps, making it the fastest and highest-performing firewall available
- Deep-packet inspection without significant performance degradation
- Transparent-mode support for enhanced system integration and security
- Multiple-Context mode support to create multiple logical firewalls, resulting in a high return on investment
- Seamless integration with the rest of the network and conformity to Cisco IT standard architecture and design principles
- Savings in total cost of ownership

PLANNING AND IMPLEMENTATION

It took many weeks of planning and design to formulate a deployment plan for the new firewalls at the headquarters campus. Cisco spent several weeks testing traffic flow, throughput, and response times. To test rule sets, the implementation team created a test subnet. Using a traffic generator, the team sent traffic based on those rules. The process was carried out for both internal and external DMZ traffic. The failover capability was also tested.

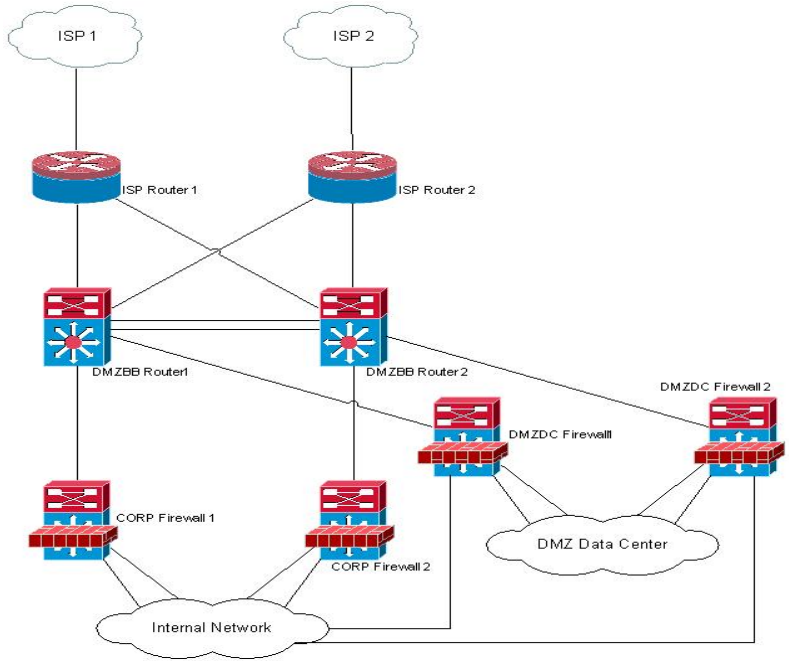
At the time of the acquisition, the headquarters campus had two DMZ backbone gateways, two ISP gateways managed by separate ISPs for diverse routing, and three pairs of firewalls (active and standby) securing the Engineering Lab LAN (referred to as ENG in Figure 1 below), the corporate LAN (CORP), and the data center (DMZDC) that supports Scientific-Atlanta's e-commerce applications. Internet connectivity was provided through two redundant ISPs, an arrangement that was retained.

Figure 1. Legacy Firewalls at Scientific-Atlanta



In the new Cisco-based DMZ infrastructure (see Figure 2), the two backbone gateways (DMZBB) were replaced with two Cisco Catalyst 6509 Layer-3 switches. Scientific-Atlanta took over the two ISP gateways and replaced their routers with high-performance Cisco routers. Finally, the CORP and DMZDC firewalls were replaced with Cisco FWSM modules—after moving the Engineering LAN inside the corporate LAN to do away with the need for a third pair of firewalls.

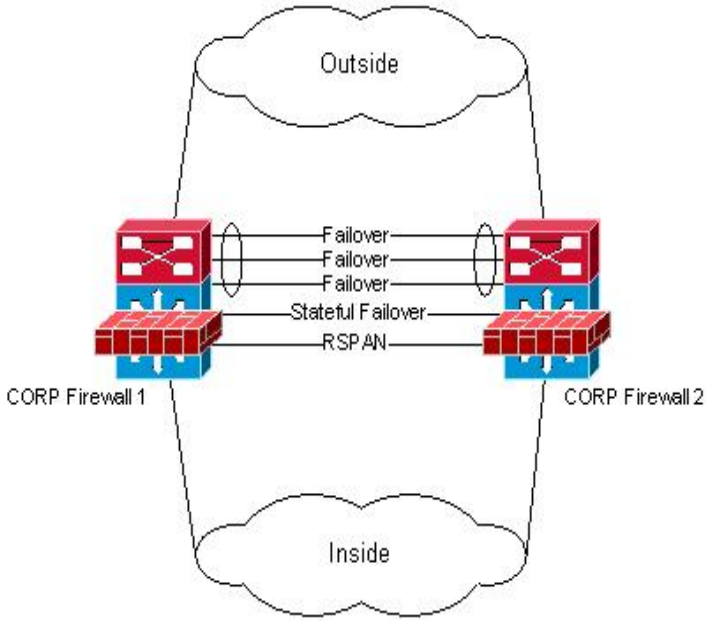
Figure 2. Cisco FWSM Deployment at Scientific-Atlanta



The two corporate firewalls are planned to be deployed as a high-availability pair and configured in Transparent mode, the Cisco IT corporate firewall standard, with an inside and an outside interface (see Figure 3). This design allows separation of security and routing. Routing will be handled by neighboring router devices, not by the Cisco

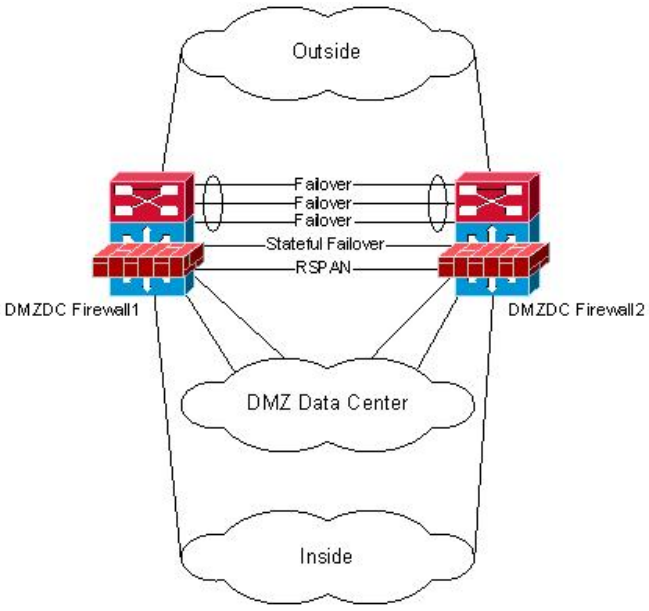
FWSM units themselves. The firewalls will be dedicated for packet inspection with an IP address assigned for management purposes only. The firewall interfaces will be Layer-2 interfaces in Transparent mode, so the firewall will be hidden in the data path from a Layer-3 perspective.

Figure 3. Corporate Firewall at Scientific-Atlanta



For the DMZDC firewall configuration (see Figure 4), the design team chose to deploy the high-availability pair of firewalls in Routed mode because, unlike the corporate firewall, it must support more than two interfaces. For the present, the firewall has three types of interfaces: inside, outside, and DMZ. However, Multiple-context transparent mode is being considered as a firewall standard for the data center. This mode provides the ability to partition firewalls into as many as 256 virtual firewalls, creating a very secure data path and separation of data packets.

Figure 4. DMZDC Firewall at Scientific-Atlanta



RESULTS

The deployment of Cisco FWSMs within the Scientific-Atlanta network has provided conformity to Cisco IT standards and seamless integration with the rest of the Cisco global network. FWSMs also offer superior performance and capacity for future growth. In addition, it has reduced the total cost of ownership for Cisco IT by increasing manageability of the firewalls at the Scientific-Atlanta campus. Because the firewalls are housed in Cisco Catalyst 6500 Series switches, additional network services can be easily deployed using the switch's service modules. This results in a higher return on investment for Cisco IT.

From an operational standpoint, the reliability and availability of the FWSMs is far superior to the previous firewall solution. "The failover capability of the Cisco FWSM is seamless and nearly instantaneous," says Kelly Alexander, network architect with Cisco in Atlanta. "We could lose several ports in the primary module and never notice it because the transition to backup occurs so quickly. It all takes place at Layer 2 between the switches. We've never seen a failover occur in the eight months since the FWSMs were installed."

LESSONS LEARNED

Cisco IT learned some important lessons that can facilitate the migration from non-Cisco firewall products to Cisco FWSMs. Due to the architectural differences between the old firewalls and the Cisco firewalls, it was necessary to convert the existing rule sets for the new firewalls. The tool used to perform this conversion was not as helpful as had been expected due to the complexity of the existing rules. As a result, all rule sets had to be manually inspected and converted to the appropriate format for the Cisco FWSMs. This process was time consuming, but it presented an opportunity to review the security policy, allowing rules to be removed that were no longer relevant and keep the rule sets current.

NEXT STEPS

The firewalls for Scientific-Atlanta's data center are currently deployed in Routed mode. This is a short-term solution as Multiple-context Transparent mode is currently under evaluation and is expected to become a Cisco IT global standard in the near future. Once the new standard is approved, the data center firewalls at Scientific Atlanta will be converted from Single-context Routed mode to Multi-context Transparent mode.

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.**