

How Cisco IT Deployed Firewall Protection for a Small Business Acquisition

FWSM is flexible enough to secure small businesses as well as large enterprises

Cisco IT Case Study / Security and VPN / Small Business Firewall Protection: Linksys, a division of Cisco®, needed to replace a PC-based firewall with a solution that would provide greater security and reliability. In a project to improve overall network availability, Cisco IT helped the Linksys network staff implement a pair of redundant Cisco Catalyst® 6500 Series switches with Cisco Firewall Services Modules and Cisco Content Switching Modules. This solution delivers greater network security, failover capabilities, and tools for central management. Cisco small and midsize business customers can draw on Cisco IT's real-world experience in this area to help support similar enterprise needs.

“The Cisco Catalyst 6500 Series switches with the Cisco Firewall Services Modules and Cisco Content Switching Modules give Linksys a cost-effective solution for improving network security while achieving 99.99 percent availability.”

– Steve Acheson, Senior Information Security Architect, Cisco Information Security Group

CHALLENGE

Linksys was a global company with a few hundred employees when it was acquired by Cisco in 2003. Operating as a separate division within Cisco, Linksys manages its own network and Websites, including security elements such as firewalls.

Like many small and midsize businesses, Linksys previously used a Linux-based PC as the firewall for its external Website. This internally developed firewall was satisfactory at that time because the availability of the Linksys Website was not considered business critical. However, as the Linksys business

continued to grow and the complexity of its Website increased, availability and support requirements of the PC-based firewall were no longer satisfactory.

Linksys IT wanted to deliver 99.99 percent (four 9s) availability for Linksys.com. After initial investigation, Cisco and Linksys engineers determined that this level of availability was not possible given the limitations of the PC-based firewall, such as:

- The low reliability of the PC limited its fault tolerance and ability to be used for disaster recovery.
- Performing any maintenance or repair activity on the PC meant that the Linksys Website was not accessible.
- Denial-of-service attacks were a concern because vulnerabilities in the firewall's operating system or filtering software could cause the firewall to fail or go offline.
- The network supporting the firewall was based on a single switch, and if the switch failed, it was perceived as a firewall failure.
- The PC's limited processing power meant that network-level protocol statistics could not be easily collected and processed, which was a new business requirement.

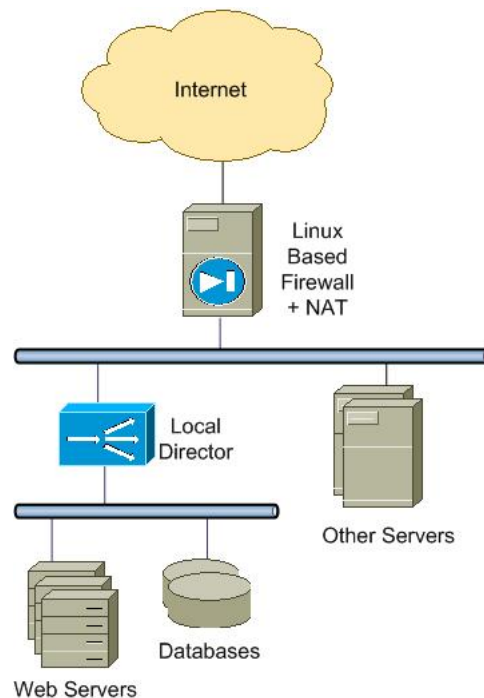
“The existing firewall was not keeping up with the needs of the Linksys Website in many different ways. Even minor problems were causing the firewall to fail, which created more frequent downtime for the Website,” says Ed Scarberry, a Linksys IT support manager. “We also wanted to allow external access to more of our networked

applications, but the existing firewall could not support them.”

Steve Acheson, senior information security architect in the Cisco Information Security Group, says, “Perhaps the most troublesome IT issue was that no backup firewall was available, which meant that the PC was a single point of failure in the network.”

Other limitations existed in the Linksys network. Network switches were installed in a standalone design, so that each switch was a potential single point of failure. Additionally, load balancing for the Website was accomplished through a single Cisco Local Director 430, a product that had reached “end of life” by the time of the Linksys project. (Figure 1)

Figure 1. The Linksys network design formerly was based on standalone servers and other elements, which hindered security and availability.



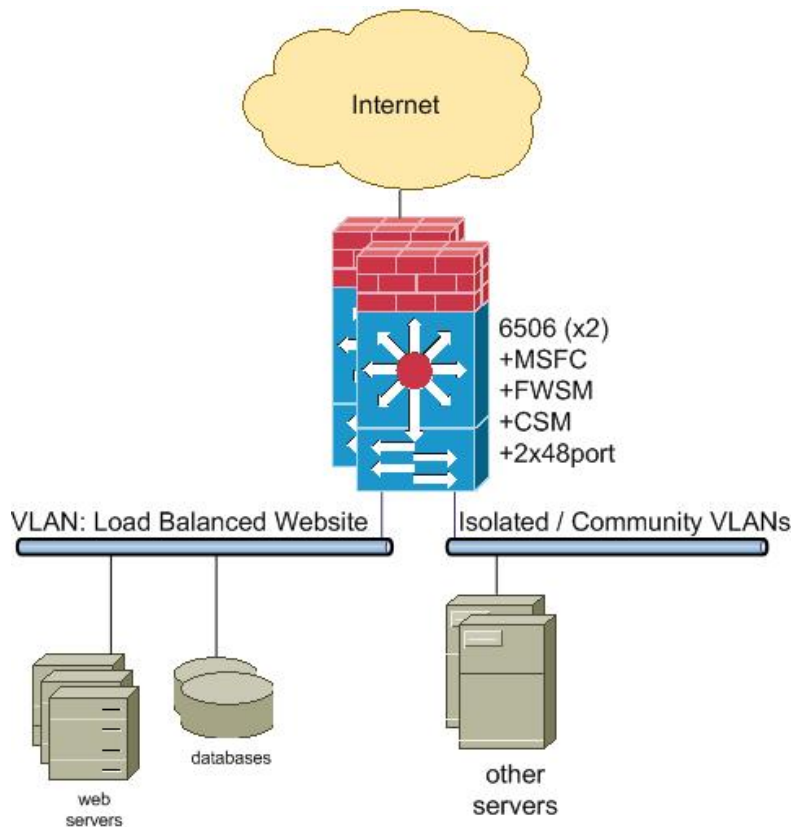
Along with improving the firewall, the project team wanted to upgrade the Linksys network to support higher availability through failover capabilities, greater capacity for increasing traffic, and central management of network elements.

SOLUTION

Cisco helped Linksys IT evaluate the changing business requirements of the division’s external network and Website to identify the best replacement solution. Despite the differences in size, cost considerations, and needs for network availability and security, a large enterprise like Cisco and a smaller company like Linksys both found that their best security solutions were very similar. Both companies used the Cisco Catalyst® 6500 Series switches and Cisco Firewall Services Module (FWSM); the only difference is in the architecture.

To improve overall network security and performance, the project team determined that a pair of redundant Cisco Catalyst 6500 Series switches with Cisco FWSMs and Cisco Content Switching Modules (CSMs) would meet the business needs with a powerful, yet cost-effective solution. Deployed in parallel in the Linksys data center, the switches provide redundancy and failover capabilities, as well as capacity for future growth in Linksys network traffic (Figure 2).

Figure 2. Two Cisco Catalyst 6500 switches with Cisco FWSMs and Cisco CSMs improve security and availability in the Linksys network.



The Cisco FWSM provides a high-performance, stateful inspection firewall with engines for examining traffic at the application and protocol levels. The Cisco CSM provides high-performance load balancing for traffic directed to firewalls, servers, and other devices.

“Linksys.com is an example of a Website where the company has determined that 99.99 percent availability is an appropriate objective because the site doesn’t currently support any e-commerce or other essential business functions,” says Acheson. “The Cisco Catalyst 6500 Series switches, Cisco Firewall Services Modules, and Cisco Content Switching Modules offer a powerful, cost-effective solution for improving network availability and security in this midsized business environment.”

A Simple Migration with No Downtime

“The deployment process for the new switches and modules was fairly simple,” Acheson says. “The original firewall used Network Address Translation [NAT], which meant that we could use bidirectional NAT to install the new firewall in parallel with the original firewall and migrate the applications one at a time.” For the migration, the team simply created a new, public-facing IP address and configured the new firewall to translate that address into the same private address used by the original firewall.

The team also translated the incoming Internet addresses into the internal private address of the FWSM, which prevented return traffic from routing out through the old firewall (over the existing default route) and breaking the NAT translations and stateful inspections. This translation appeared to internal applications as if all connections were originating from the FWSM. Without this extra translation, routing and NAT issues would have prohibited correct operation of the Website.

According to Acheson, “We followed a similar process for migrating from Cisco Local Directors to the Cisco CSMS by creating new, load-balanced IP addresses on the Cisco CSMS. We also found that sharing the back-end server VLANs between the new and old load balancers would allow for migration without downtime.”

After installing the Cisco Catalyst switches and configuring them for failover, Acheson adds, the project team duplicated the load-balancing configuration from the Cisco Local Director to the Cisco CSMS and the firewall policy from the PC to the Cisco FWSMs. Because the Linksys.com site was not very complex, the project team decided to manually recreate the original load balancing, firewall configurations, and NAT rules on the appropriate modules.

The only external dependency on the migration was to coordinate with Linksys business partners for business-to-business transactions that used the original external IP addresses. Working with the partners to test and change their configurations went smoothly and also resulted in no downtime to the Linksys Website.

At the point when the new load-balancing and firewall solutions were active and functional in parallel with the original solutions, the production Domain Name System (DNS) entries still referred to the original firewall. After the project team tested and validated that applications were working as expected through the new firewall configurations, the next step was to change the DNS addresses for the Linksys.com applications and Website to point to the Cisco FWSMs instead of the original firewall. No other major changes were necessary in the Linksys network infrastructure to place the Cisco FWSMs into full operation.

After all DNS entries for applications had been migrated to the new firewalls, the project team found a few legacy applications that had hard-coded the public IP addresses. The team determined that migrating those public IP addresses to the new firewall was the easiest way to support them until those applications were modified to accept the Cisco FWSM address.

The final step was to remove the NAT translations to the incoming Internet addresses so that the Web and FTP servers would again see the true client addresses and make it easier to inspect the Web logs.

RESULTS

Linksys realized the following benefits by implementing the Cisco Catalyst switches with Cisco FWSMs and CSMS:

- Increased network security, stability, and availability because of the redundancy and failover capabilities throughout the network, firewalls, and load balancers
- Greater security capabilities and firewall availability so that the Linksys.com Website can achieve 99.99 percent availability while also supporting scalability to meet traffic growth or new availability requirements
- Improved capabilities for firewall management and reporting, including the ability to centrally monitor and manage the Cisco FWSMs
- Ability to monitor network activity and detect denial-of-service attacks by analyzing Cisco Catalyst 6500 port activity and NetFlow statistics. This solution also offers improved diagnostics and incident response capabilities for a network attack.
- No downtime for the Linksys.com Website or impact on applications or users during migration from the PC-based firewall, or during firewall maintenance activities. Future downtime will also be minimal, because one switch can remain active while the other switch is taken offline for maintenance or upgrades.
- Easier integration of other Cisco network products because the Cisco FWSM is already configured to support them, unlike the PC-based firewall

“Over the long term, this solution also gives us more flexibility for growing and expanding the network and services offered by the Linksys.com Website as well as supporting external access to other applications,” says Scarberry.

LESSONS LEARNED

Focusing the initial firewall implementation to support only the Linksys Website simplified the migration process. Acheson also identified several lessons gained from this project:

- Using NAT as the migration tool proved successful, because the original Website used NAT and Linksys required minimal downtime both for the internal network access and for Website users.
- Using bidirectional NAT resulted in an interim loss of directly accessible Web logs for client IP addresses, because NAT of the incoming IP addresses made all transactions appear to be coming from internal, private IP addresses. For the duration of the migration, NetFlow information supplemented the Web logs to provide traffic data.
- Running both the new and original firewalls in parallel allowed the team to detect and correct hard-coded IP addresses in legacy applications, with no significant downtime or modifications to those applications.
- Using DNS to migrate the production public reference to the Linksys.com Website meant that users were not affected and were migrated to the new site when new connections detected the changed IP address. Existing connections were not affected, and applications could be migrated one at a time rather than forcing the change from one firewall to the other as a complete cutover. This process also allowed the team to resolve and re-test any issues discovered in testing before an application was migrated.

NEXT STEPS

Linksys IT is evaluating internal applications for allowing firewall-protected, external access by users. New types of traffic are also anticipated for Linksys.com—such as alternative ways for handling downloads and firmware, as well as an online chat feature for technical support—that will require accommodation by the firewall.

Additional capabilities are planned for improving the security and availability of the Linksys network, including:

- Implementing a server-level failover capability by using the dual Ethernet ports on servers to connect separately to the two Cisco Catalyst switches. The previous single-switch design of the Linksys network could not support failover at the server level.
- Investigating the addition of Cisco Catalyst 6500 Series Intrusion Detection System Modules and the Cisco Guard distributed denial of service (DDoS) mitigation appliance for greater protection against denial-of-service attacks.
- Examining NetFlow statistics to improve methods for detecting anomalies in network traffic that might indicate a security threat, and considering use of the Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) for detecting subtle or complex security issues.
- Evaluating an engagement of the Cisco Remote Operations Service (Cisco ROS) to provide operational and security support for the Linksys network.

For more information about the products in this solution, visit:

- Cisco Catalyst 6500 Series switches: www.cisco.com/go/catalyst6500.
- Cisco Firewall Services Module: www.cisco.com/en/US/products/hw/modules/ps2706/ps4452/index.html
- Cisco Content Switching Modules: www.cisco.com/en/US/products/hw/modules/ps2706/ps780/index.html

In addition, a detailed case study about Cisco IT's deployment of the FWSM within the Cisco global network is available at http://www.cisco.com/web/about/ciscoatatwork/security/enterprise_firewall_protection.html.

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.

©2007 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, CCSF, 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, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, ScriptShare, 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. (0705R)