Customer Case Study

Cisco Integrated Firewall Services Modules Safeguard Diverse Academic Resources

Switch-Based Firewall Modules Enforce Wide-Ranging Security Policies at Three Leading U.S. Universities.

EXECUTIVE SUMMARY

Harvard University Information Systems (UIS), and prominent northern California- and Georgia-based universities (names withheld per the universities' requests)

- Education and research

BUSINESS CHALLENGE

- Protect the university community against network-borne threats without obstructing open communications and research
- Adapt security policies to the needs of individual groups
- Maintain network performance, avoid management complexity, and contain costs

NETWORK SOLUTION

- Firewall modules deployed in existing Cisco switches
- Each group given its own security context
- Transparent firewall enables quick deployment

BUSINESS RESULTS

- Provides strong, comprehensive security
- Maintains high network performance levels
- Simplifies security implementations and management
- Helps reduce manpower requirements and expenses

BUSINESS CHALLENGE

Each of the many academic departments, schools, research institutes, laboratories, business offices, classrooms, dormitories, and other campus facilities that make up a world-class university has its own unique computing and networking requirements. And a university's need to protect information resources from externally and internally generated threats has never been greater. But network expertise can vary greatly among the individual groups, and users' exposure to security risks also varies depending on the sort of work that they do and the type and amount of information that they exchange. Adding to the challenge are the university's independent-minded faculty, staff, and students, who often voice concerns that a stronger security profile could limit their research or discourage collaboration.

"In a corporate environment, the IT group might install central firewalls that strictly control the network border, but this university campus wanted a border that is more open to encourage information interchange," says David Paul Zimmerman, senior network architect for Information Services and Technology (IST) at a prominent northern California university. "Initially network-level firewalls were installed by individual departments, with IST providing architectural guidance and network services. We needed to help ensure that departments continued to have the functionality that they wanted, but we also wanted to make sure that central network management would not be impeded."

Many academic groups within a university are capable of running their own firewalls, and indeed may have been doing so for years. But there are dangers to this independent approach. "At our university there were a lot of security 'entrepreneurs' doing their own thing, some better than others," says the director of academic research and research technologies at a prestigious Georgia-based university. "What really worried us was when systems got infected or compromised and caused problems for other groups. That required a huge expenditure of resources. In addition, we needed to design a security infrastructure that would preserve the high performance and bandwidth that users had come to expect from the network."

Besides their diversity, the sheer magnitude of some academic networks presents daunting challenges. "Some access control lists (ACLs) were exceeding 3000 lines and we were running into resource walls," says Jay Tumas, Harvard UIS's network operations manager. "Even though there was plenty of processing power, the size and complexity of what people wanted to do with ACLs was not working for us. We needed a way to let the individual departments manage the lists locally."

NETWORK SOLUTION

To help implement stringent yet flexible network security, all three universities chose to install Cisco® Firewall Services Modules (FWSMs) on their existing **Cisco Catalyst® 6500 Series switches**.

By deploying **transparent** (Layer 2) **firewalls** with the FWSMs in the Cisco Catalyst 6500 switches, the California university's IST division was able to service widely dispersed functional areas from the core switch platforms, eliminating the need for firewall appliances in each individual department. One FWSM provides firewalls for all the subnets serving the groups in a particular network zone, with each subnet/group getting its own security "context," or firewall rules. This institution has also deployed modules in an **active/standby** configuration in the data center to help ensure **high availability**.

"Very often a department is capable of running its own firewall, so we came up with a network model to facilitate that approach," says Zimmerman. "But if a department wants IST to provide firewall services, the FWSMs give us the flexibility to do that as well. We use a 'hidden' virtual LAN (VLAN) model with a public and a private side. From the viewpoint of the FWSM, it is all transparent. Layer 2 transparency lets us leverage the VLANs and other configurations that were in place previously. I have not found any other product that fits our environment as well from a core services perspective. And the graphical user interface makes it very simple for departments with any level of technical expertise to control their own security situation."

"The FWSMs give us both **scalability** and **flexibility**," says Michael Sinatra, IST principal network architect at the university. "Before we installed them, IST could not really add value by offering firewall services. Now we can build on economies of scale by centrally managing the physical firewall hardware, and we can delegate the management of firewall rules to the departments to preserve their autonomy and flexibility."

At the university in Georgia, the firewall initiative was one of the largest and most extensive projects that the Academic and Research Technologies staff has undertaken. The security team worked closely with approximately 130 individual user groups to provide them with **security contexts** that match the way that they do business and provide access to the services that they need. The contexts essentially act as virtual firewalls; up to 250 contexts are available per module with the latest FWSM software release. Firewall modules have also been deployed at the network border to counter external threats, while others have been implemented in a few locations where specialized policies had to be implemented.

"Many of the objections that users raised about the firewall initiative disappeared after the implementation," says the networking integrity team leader at the Georgia-based school. "Users were satisfied after they saw the benefits obtained by peers who were protected by the FWSMs. The success of others is how we got more people to join the process. Credit goes to our technicians who collaborated with the various units to accomplish the overall goal."

The Harvard University Information Systems network supports more than 125,000 users and runs 250–300 terabytes of data a day. With a staff of 20, the network group has the in-house resources to develop many of their own solutions, including management, accounting, and intrusion detection technology. They deployed 11 FWSMs across the network after determining that the modules would fit their customized environment and could handle the high data rates.

"We spread the FWSMs across the core to achieve an efficient security posture that allows us to apply rules quickly if we want to shut down certain traffic to, for instance, stop the spread of a worm or Trojan," says Network Operation Manager Tumas. "The network's 'customer' groups enter ACLs through a portal at the network operations center, and we have built tools to let them manage their own firewall rule beds."

"A major reason that we selected the FWSMs is because we already had the Cisco chassis," Tumas says. "The combination gave us the best architecture available for our environment. With the close compatibility between switches and firewalls, we do not have to worry about creating vulnerabilities by keeping a lot of ports open. The protocol inspection engines integrated into the FWSMs maintain open ports only for current legitimate sessions." The integration of services modules within existing chassis, allows organizations to simplify their infrastructures, enhance perimeter security, and reduce costs.

BUSINESS RESULTS

Senior Information Security Officer at the university in Georgia has found that the FWSMs have had a dramatic impact on a network that used to experience hundreds of incidents a week. “We have seen a **91 percent reduction in reported incidents** after implementation,” he says. “Plus, we have been able to cut way down on the manpower that was previously needed to review the compromised systems, clean them up, or rebuild them.”

“We have avoided management problems because there is a high degree of department ownership,” says Zimmerman. “The FWSMs make it easy for us to run the firewalls according to the department manager’s rules. We have been able to take the services that we provide to a higher level.”

The Georgia school’s networking integrity team leader concurs. “From a management standpoint, it is simple to add contexts,” he says. We deployed around 50 contexts in each FWSMs and found the transparent firewall easy to deploy. “If we need to turn on a basic firewall, we can get it going in about **15 minutes**, and there is no need to provision power, rearrange network architecture, or change VLAN and router interfaces.”

The FWSMs have also **reduced manpower requirements** and associated costs. “Since each security context represents an area where a separate firewall would have had to be installed, we have saved the labor associated with registration, wiring, and hardware installation,” says Zimmerman. “I estimate that the FWSMs were **10 times easier for us to implement than appliances** would have been.”

“All in all, we have been able to reallocate resources to better purposes,” says the director of Academic Research and Research Technologies at the Georgia university. “The investment has certainly paid off for the network team. In fact, we have even seen a reduction in workloads at the system administrator level.”

Patrick McEvilly, network engineering manager at Harvard UIS, brought up another important business benefit that might tend to be overlooked in an academic setting. “Transactions for the student store, arts box office, and other campus businesses must be in **compliance with Payment Card Industries (PCI) regulations**,” he says. “That requires a number of security technologies, and the FWSMs provide the necessary firewall component.”

NEXT STEPS

All three universities expect to expand FWSM security coverage to more groups and users in the future.

“We will be rolling out firewall services to the zones of the campus network that do not already have them, as well as to off-campus locations,” says Zimmerman. “We are looking forward to upgrading our FWSMs to expand capabilities, such as running multiple subnets off one context. In addition, the firewalls will eventually need to protect a future voice-over-IP system that will involve a relatively complex protocol suite.”

PRODUCT LIST

- Cisco 6500 Series switches or Cisco 7600 Series routers
- Cisco Firewall Services Module (FWSM)Broadband Cable

The large Georgia university is gearing up for the last phase of its three-year firewall initiative. “When we are done, every functional unit on the network will have a security policy implemented through an FWSM,” says the team leader. “The campus backbone will be running at 10 Gigabit Ethernet rates, and our firewalls will need to keep pace.”

The Harvard UIS team looks forward to the day when a team member will be able to key in one command and disseminate emergency rules across the entire network, alleviating a security problem without having to resort to local troubleshooting. Says Tumas, “Integrated firewalls give us the capability to **react quickly and deploy security policies everywhere in the network, even as attacks adapt and evolve.**”

FOR MORE INFORMATION

To find out more about Cisco Firewall Services Modules, visit: http://www.cisco.com/go/security.

CISCO SYSTEMS

Corporate 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: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
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

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco.com Website at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Printed in the USA

C36-362402-00 08/06