

Top Netherlands University Achieves a Higher Degree of Network Security

HAN University improves network protection while streamlining management using Cisco integrated security solutions.

EXECUTIVE SUMMARY
<p>EMERGING MARKETS TECHNOLOGY GROUP, CISCO SYSTEMS</p> <ul style="list-style-type: none"> • Customer Name: HAN University • Industry: Education • Location: Arnhem and Nijmegen, the Netherlands • Number of Users: 26,000 students and 2500 staff
<p>BUSINESS CHALLENGE</p> <ul style="list-style-type: none"> • Boom in student population required higher performance and more frequent changes in security policies • Complex, device-level firewall configuration slowed response to access needs and security threats and also introduced the chance for errors when making changes
<p>NETWORK SOLUTION</p> <ul style="list-style-type: none"> • Cisco Security Manager centralizes and streamlines firewall configuration changes based on global policies • Cisco high-performance switching chassis with integrated firewall services modules add capacity and redundancy
<p>BUSINESS RESULTS</p> <ul style="list-style-type: none"> • High performance security solution allows growing student population to access online university resources, while protecting the network from attacks or inappropriate usage • The ability to change firewall configurations rapidly provides greater protection in response to security breaches • Time saved in manual firewall configurations frees up IT staff to work on new security projects

Business Challenge

In 1996, three of the Netherlands' higher education institutions in Arnhem and Nijmegen merged to become the Hogeschool van Arnhem en Nijmegen, or HAN University. Today, HAN University ranks among the top 10 professional universities in the Netherlands. The school's enormously popular curricula, including the Arnhem Business School's well-respected international business and management program, attract students from around the world.

During the last five years alone, HAN's student population has more than doubled to over 26,000 students. As programs and enrollment have grown, demands on the network have also increased. In the university's data center, server farms are constantly expanding to support online courses, e-mail, the university's Website, and other needs. The rapid growth of network-based resources has heightened the concern regarding exposure to security threats.

Jeroen Langestraat and his staff have responsibility for the university's data network infrastructure, and his team's highest priorities have included helping ensure top network performance and securing the university's information assets. "As a university, we

want to be as open as possible and allow students and the public to connect with the online resources that we offer," says Langestraat. "At the same time, we need to protect against hackers, unauthorized access to resources, and other security-related issues."

One of Langestraat's critical issues was streamlining network and security management. The network team had kept up with security demands by deploying six firewalls across the two campuses. However, the firewalls were configured on a device-by-device basis, and configuration required translating policies into technical rules. "It had become a very labor-intensive process to keep up with the almost daily changes in access requirements, and the chance for error was growing," says Langestraat. "We were also concerned that it might take too long to close all the possible gaps in response to a security threat, or just an unauthorized or inappropriate use of

network resources.”

“We strengthened our security with adaptability, throughput, scalability, and redundancy. At the same time we greatly simplified administration of our security devices, freeing up valuable technical resources for new security initiatives.”

—Jeroen Langestraat, Network Manager, HAN University

In addition, the school still maintains campuses in Arnhem and Nijmegen, about 25 km apart, and with a relatively small network staff supporting two geographically distributed campuses, Langestraat needed to centralize and simplify the management of network resources as much as possible.

Network Solution

In 2006, Langestraat’s team migrated all of the fiber interfaces on the backbone to the Cisco® Catalyst® 6500 Series Switches. “Deploying the high-performance, chassis-based switch gives us a lot of advantages, one of which was the opportunity to integrate Cisco Firewall Services Modules into the switching chassis,” says Langestraat.

The Cisco Firewall Services Module (FWSM) is a high-speed, integrated firewall module that provides firewall data rates of 5-Gbps throughput, 100,000 CPS, and 1M concurrent connections. “By implementing the firewall modules, we eliminated the need for separate firewall appliances around the campus, added greater redundancy, and increased performance so that the access and authorization process was not an obstacle. We are only using about five percent of the capacity of the FWSM, compared to over 95 percent or greater utilization previously,” says Langestraat. “The integration of services modules within the existing chassis also met the larger goal for simplifying our infrastructure whenever possible.”

During the same period of time, the network team began evaluating products for centralized management of security device configuration and policies. “We had a lot of experience with Cisco products and we trust our experience with them. We decided that the Cisco Security Manager would give us the optimum capabilities for managing our Cisco network,” says Langestraat. Cisco Security Manager, part of the Cisco Security Management Suite, centrally provisions all aspects of device configuration and security policies for Cisco firewalls, virtual private networks (VPNs), and intrusion prevention systems (IPS). As networks expand, Cisco Security Manager scales easily through intelligent policy-based management techniques that can simplify administration.

To prepare for the migration, the network team froze the network on November 1, 2006, so that there would be no new firewall configuration changes. Over a three-week period, four members of the network team took the existing access controller information for the firewall appliances and created high-level security policies. “We needed to go up a level from the device configuration rules, and abstract 18-pages of technical data to global security policies,” says Langestraat. The policies were implemented in the Cisco Security Manager, which would then automatically configure the FWSMs and the supervisor modules on the Cisco 6500 Switches.

“We decided that there was really no way to do a phased rollout of a campuswide security system.

We tested the concept within our own group and made the decision to go live with the whole network in one night," says Langestraat.

The existing firewall devices remained in place for the month of November. On December 1, 2006, the team switched the entire network over from the firewall appliances to the integrated FWSMs.

Langestraat asked his entire team to remain on standby for the week following the cutover to help ensure that everyone was available to answer ringing phones and urgent e-mails from students and faculty. "Because of the enormous complexity of these configurations and policies, we had to assume that there would be calls coming in from across the university because of denial or access problems," says Langestraat.

But nothing happened. "We did not get a single complaint—no problems, no calls," says Langestraat with satisfaction. "Our team translated the technical configurations to global policies flawlessly, and the Cisco Security Manager turned global policies into device-level configurations without a single error. It was an amazingly successful migration."

Business Results

With the new Cisco Security Manager and the integrated security products, it is now much more efficient for the network staff to administer security policies. "The Cisco Security Manager has eliminated all of the overhead associated with having technical staff spend time on device-level configurations," says Langestraat. "We can implement security changes much more quickly, which allows us keep up with policy changes and act faster in the event of security threats."

The time savings have also freed up staff to focus on new security initiatives. "We have many security programs that we would like to implement, but we had to put them on hold," says Langestraat. "Now managing security is an administrative task, not a technical one, so we can use our technical resources to focus on more strategic projects."

Not only can the network staff more efficiently administer security policies, but they can also communicate those policies more effectively. "We are probably two years ahead of the university's expectations in terms of centralized security management. As security becomes more visible and vital, we will be able to provide a very good, high-level overview of security policies to management and administration any time they want an update," says Langestraat.

The team also found an unanticipated benefit of the Cisco Security Manager that they use almost daily. "We can specify which policies are shared and automatically inherited by new devices to help ensure corporate policies are implemented consistently." Langestraat says that they still have the flexibility to customize policies at the local device level, but "we try to avoid that practice."

In addition, the network team uses Cisco Security Manager to manage the university's new Cisco ASA 5500 Series Adaptive Security Appliance. The ASA handles HAN's VPNs, which are used extensively by Langestraat's team for remote management of the network. Previously, the VPNs were terminated through the firewall appliances and were configured at the device level. Now all VPN traffic is supported with a single Cisco ASA 5500. "VPN remote access is not a large application for us, but now we can centrally manage configuration of the VPNs as well, which is important to our simplified management model," says Langestraat.

Langestraat feels that the migration met or exceeded the team's expectations. "We strengthened our security with adaptability, throughput, scalability, and redundancy. At the same time we greatly simplified administration of our security devices, freeing up valuable technical resources for new

security initiatives.”

Next Steps

With the Cisco Catalyst 6500 Series Switches, FWSMs, and Cisco Security Manager in place, the network team is now taking advantage of the ability to create virtual firewalls. “We can use this feature to create multiple virtual firewalls with a single FWSM,” says Langestraat. “We are in the process of setting up virtual firewalls throughout the network to further reduce the complexity of managing the network infrastructure.” After this phase is completed, Langestraat plans to set up a test configuration of the Cisco Security Monitoring, Analysis, & Response System (MARS), which may further simplify security management by aggregating and synthesizing network and security data to help Langestraat’s team effectively identify and respond to threats.

Sometime in the future, Langestraat anticipates that the university will be upgrading its wireless network security as students and faculty increase their use of wireless devices on campus. “We already upgraded the wireless network by implementing Cisco’s Wireless Infrastructure Service Modules (WISM) and LWAP [Lightweight Access Point] technology,” he says. “The next step will be to use the same security system, which will handle any increased traffic and manage all of the new access policies without a problem.”

For More Information

To find out more about Cisco Security solutions and the Cisco vision of the Self-Defending Network, go to: <http://www.cisco.com/go/security>.

Product List

Routing and Switching

- Cisco Catalyst 6500 Series Switch

Security and VPN

- Cisco Security Manager
- Cisco ASA 5500 Series Adaptive Security Appliance
- Cisco Catalyst 6500 Series Firewall Services Module

**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, CCSP, 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, RateMUX, ScriptShare, SlideCast, 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. (0704R)