Growing University in Namibia Moves to Next-Generation Security

Customer Case Study

EXECUTIVE SUMMARY

Company: The Polytechnic of Namibia
Industry: University
Location: Windhoek, Namibia
Students/Employees: 13,000 students, 1000–1500 faculty/staff

Challenge

- Prepare network for anticipated doubling of student body size
- Strengthen network security against increasing infections and attacks
- Simplify security implementations and management for limited staff

Solution

- Cisco ASA 5585-X Series Next-Generation Firewalls
- Cisco Identity Services Engine
- Cisco AnyConnect

Results

- Simplified integration of Cisco solutions with planned roadmap
- Virtualized firewalls to ease and simplify deployments
- Gained scalability to meet future needs

Polytechnic of Namibia secures campuses and offices across country with Cisco ASA 5585-X Series.

Challenge

Unlike traditional hacking targets such as financial institutions, universities are open and inviting. Their faculty, staff, students, and visitors expect fast, easy access to on-campus resources, as well as the ability to quickly connect their own devices to the network. Faculty, in particular, has special needs, such as accessing other universities' systems. Unfortunately, that openness and accessibility often create vulnerabilities in network security. These vulnerabilities could place university assets – as well as those of students, faculty, staff, and guests themselves – at risk.

At The Polytechnic of Namibia, a 13,000-student university with 11 offices across the country, Marco Maartens, network manager, says major network outages due to virus infections and worms increased from one to several per year. More troubling, however, was the trend he saw - prevalent in universities worldwide - toward hackers using the university as a conduit to launch external attacks – the well-known botnets.

"Universities in general are not known for securing themselves well, and we have a lot of equipment available to serve very diverse needs. We've seen a rise in instances where hackers invade our infrastructure, not to steal anything here, but to use it to go after more valuable targets," Maartens says.

The Polytechnic of Namibia has an IT staff of 60, with just five people, including Maartens, focused on network security. In addition to addressing the growing threat from outside hackers, Maartens' team had to develop a roadmap to manage the dramatic growth that the university predicts for the next several years.

The university will change its name in 2015 to Namibia University of Science & Technology, and by 2017 expects to serve 20,000 students - almost twice as many as are now enrolled. At least one more campus will be added, and the number of faculty and staff will increase as well. For Maartens and his team, that means thousands more users - and devices - to secure, while still maintaining the ease of access that those users expect.

"We don't have to change our security policy to match the Cisco hardware we buy. The hardware does what our security policies demand, which is very important to us."

Marco Maartens
Network Manager
The Polytechnic of Namibia

"Students are here to learn, and academics are here to give classes and to do research. They're not here to fiddle with patching machines and updating them before they can connect," says Maartens. "That's why we need security measures in place on the back end, so users don't have to worry about it."

Solution

The Polytechnic of Namibia began moving to end-to-end Cisco solutions about 10 years ago when the previous vendor stopped providing support. When Maartens came on board about three years ago, he recognized the growing security threats and the need for increased scalability. He began moving the university toward a virtualized solution with two Cisco® ASA 5585-X Series Next-Generation Firewalls supporting about 26 virtual firewalls.

The Cisco ASA 5585-X firewalls were the only such devices that Maartens could find that had 10 GB/s throughput as well as a powerful and fully enabled intrusion prevention system (IPS). The ASA appliances are partitioned into multiple virtual devices, or security contexts. That effectively segments the network, so each faculty member, as well as departments such as finance, has its own virtual firewall through which all traffic passes.

The university is also in the midst of implementing Cisco Identity Services Engine (ISE) to perform profiling and posture assessments before allowing access to the network. "Right now, we fight fires one at a time, so for example, if someone adds an infected machine to the network, we have to track where it is and disconnect it. With ISE, it won't get connected to begin with," says Maartens, "in line with the goal of providing seamless yet secure connectivity."

ISE will be a key part of the university's bring-your-own-device policy, which provides unique levels of access for staff, students, and computer labs. His team will be looking at how Cisco TrustSec® can provide role-based access for every user and every device, from smartphones to printers and laptops, both wireless and wired.

Results

Given his small staff, Maartens indicated that a key part of his decision to go with Cisco solutions was the ease of implementation and support. "I only have nine staff for network and telephony," he says, "so I didn't want to waste time trying to get multiple vendors to integrate with each other. If I have a problem, I can just get on a call with Cisco and get it resolved quickly."

The need to save time also factored into Maartens' decision to virtualize dozens of firewalls from just two Cisco ASA 5585-X appliances. In fact, he says his entire network design was based on that feature. "With the ASA, we don't have to cable up 20 boxes; we only have to cable up two. It's obviously easier to manage that way, and it takes a lot less time to test and monitor the cabling," he says.

The ability to scale rapidly is also extremely important as the university continues to grow. That point became clear recently when the university outsourced its printing operations, which in the past would have been delayed six to eight weeks while a new firewall appliance was procured and implemented. Instead, Maartens and his team simply added another virtual firewall, which was ready in less than two days.

Additionally, Maartens' team can segment access to social media, such as Facebook, according to user protocols, to further protect the network.

Implementing Cisco ISE will further strengthen the university's network visibility and control, with 802.1x port authentication capability for wired access, and wireless access for mobile devices. In the future, Maartens says he will add Cisco AnyConnect®, Cisco ASA Botnet Traffic Filter, and more advanced security solutions, as well as rapidly expanding the number of wireless access points.

Maartens indicated that it makes his job easier to have one company with integrated solutions that he can rely on. "We don't have to change our security policy to match the Cisco hardware we buy," he says. "The hardware does what our security policies demand, which is very important to us."

For More Information

To find out more about the Cisco ASA-5585-X Next-Generation Firewall and other Cisco Security products, go to:
http://www.cisco.com/go/asa

http://www.cisco.com/go/ise

http://www.cisco.com/go/anyconnect

http://www.cisco.com/go/ips

http://www.cisco.com/go/trustsec

PRODUCT LIST

Security
- Cisco ASA 5585-X Next-Generation Firewall
- Cisco Identity Services Engine
- Cisco AnyConnect
- Cisco Intrusion Prevention System (IPS)
- Cisco TrustSec

Data Center
- Cisco Nexus 5585UP
- Cisco UCS B-Series Blade Servers

Routers and Switches
- Cisco Nexus® 5585P
- Cisco ASR 1002 Routers

Wireless
- Cisco Flex® 7500 Series Wireless Controllers
- Cisco 3600, 3500, 1300 Series Access Points

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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**.

C36-732194-00 07/14