# Education Provider Assures Protected Campus Learning

Customer Case Study

## Fontys University of Applied Science responds to 50 percent annual rise in BYOD with strategy for zero-threat security

### EXECUTIVE SUMMARY

**Customer Name:** Fontys University of Applied Science

**Industry:** Education

**Location:** Netherlands

**Number of Employees:** 4100

**Challenge**

- Cope with growth in bring-your-own-device numbers
- Support mobile endpoints while maintaining IT security

**Solution**

- Intrusion prevention system with next-generation firewall services based on advanced Cisco ASA platform

**Results**

- Provided stable network security environment
- Maintained full protection since implementation

### Challenge

Security's an important issue in any learning environment. But at Fontys University of Applied Science in the Netherlands, IT security is particularly challenging because of the high caliber of students involved. Some of the brightest and most technologically-savvy minds in the country apply to Fontys to take advantage of its reputation for educational excellence.

Paradoxically, this level of excellence multiplies the chances of members of the 40,000-strong student body encountering, or even releasing, potential online threats. This hazard has increased in recent years as students have taken to bringing their personal devices on campus. The bring-your-own-device (BYOD) trend saw the proportion of campus-based personal devices growing by 50 percent in 2013, with a further 30 percent growth expected for 2014.

Many students now carry multiple devices, from laptops to smartphones, each representing a potential malware entry point. For the university any IT security breach from whatever source could have serious consequences. "We need to protect internal administration systems and prevent unauthorized access," says Eduard Croese, network operations support for Fontys University of Applied Science. "Student data confidentiality is another prime concern."

### Solution

Fontys is a longstanding user of Cisco® technology and services, having deployed its Transformative Networking methodology to update its educational infrastructure in 2013. Fourteen years previously, the university deployed Cisco firewalls using Cisco Private Internet eXchange (PIX) 510 and 520 firewalls after centralizing IT security, which had been the responsibility of individual departments. The PIX Firewalls were subsequently replaced by powerful Firewall Security Modules (FWSM), which were installed in the university's Cisco Catalyst® 6500 switches.

When the FWSM devices became due for replacement, Fontys was keen to stick with Cisco as a security vendor but wanted to upgrade to a platform that could handle next-generation threats associated with trends such as BYOD and mobility. The university compiled a new high-level design for the security infrastructure and, following a European tender, chose two Cisco ASA 5585-X Series Adaptive Security Appliances with CX40 Security Services Processors.

"We know we can carry on using this firewall for the next few years, and there won't be any bottlenecks. It allows for growth."

Eduard Croese
Network Operations Support
Fontys University of Applied Science

The physical devices, which were installed in a single day by the Dutch service provider KPN, are divided logically into 19 separate firewalls that check VPN and other traffic crossing the border of the university's enterprise network.

## Results

The Cisco ASA platform is allowing the university to maintain a zero-threat environment, despite facing increasing network growth. The campus network currently carries about 1.4Gbps of Internet traffic and supports approximately 19,000 connections, most of which originate and terminate on BYOD endpoints.

"We know we can carry on using this firewall for the next few years, and we don't expect any bottlenecks," says Croese. "It allows for growth." And the performance of the ASA has so far been exemplary. "We don't have nor receive complaints, we don't have to worry about it, and it doesn't cause trouble tickets," Croese adds.

If a final accolade were needed, the university's IT team has not so far explored more advanced features of the technology. Croese concludes: "We recognize that the maintenance demands of the ASA, already low, can be reduced still further with some of the sophisticated tools it provides, but we don't see that as an immediate priority."

## For More Information

To learn more about the Cisco architectures and solutions featured in this case study go to: www.cisco.com/go/security

## Product List

### Security

- Cisco ASA 5585-X Series Adaptive Security Appliance featuring the Cisco CX SSP-40 (Security Services Processor-40)

**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.**