Cisco Next Generation Firewall Protects Students and Staff at Cyprus University of Technology

Customer Summary

Organization
Cyprus University of Technology

Primary Location
Limassol, Cyprus

Users
4,000 students, 625 staff

Industry
Higher Education
The Challenge

Protect students and staff across large university campus

Cyprus University of Technology was established in 2004 and welcomed its first students in September 2007. The mission of the university is to provide high-quality education, research, and training in the fields of Science and Technology. The University is located in the second largest city of Cyprus, Limassol, and is distributed across more than 40 buildings in an open campus. The university is staffed by about 225 Administrative personnel and 400 Academic personnel, and serves 4000 students studying at the University’s undergraduate, postgraduate and PhD programs.

Protecting that many people across so many different locations was difficult. That’s 4,625 people moving throughout 40 different buildings that house labs, classrooms, and libraries. 4,625 people, all with different devices and different access levels, constantly moving throughout the campus. The IT team at Cyprus University of Technology was challenged with distinguishing between the location, the person, and the device, and then granting the right access to the authorized user and device.

The team also needed a centralized management console to have a clear view of their network and device activity. From a single screen, they needed to see what is connected, who is connected, and what permissions do users have. This is important because visibility consolidated in one place increases the speed of security decision-making. If the team could see the information all in one place, not only could they spot malicious behavior faster, but they could respond more rapidly and take immediate action.

Objective

Protect 4,625 students and staff across a campus of 40 buildings in Limassol, Cyprus. The IT team lacked the network visibility to efficiently protect that many people and devices on campus. They sought an updated firewall system that could provide insight into those users and devices. They also sought out a centralized management console for their firewall to help streamline management and accelerate security investigations.

Solution

Firepower Management Center

Cisco Firewalls:

• Cisco Firepower 5555-X (2) running Firepower Threat Defense (FTD)
• Cisco Firepower 5525 (2)

Cisco ISE and pxGrid

Impact

With Cisco NGFWs running Firepower Threat Defense, Firepower Management Center, and ISE with pxGrid, Cyprus University of Technology achieved the following benefits:

• Consolidated the number of security products they use, saving time and resources
• Centralized firewall management, making firewall administration and operations easier
• Full visibility into network activity
• Faster response times
• Improved ease of segmentation and policy management

“The visibility we get from the Cisco NGFW makes us more secure.”

Kika Christou
Network Engineer
Cyprus University of Technology

© 2019 Cisco and/or its affiliates. All rights reserved.
The Solution

A firewall solution that increases network visibility and ease of management, while improving security.

In the face of multiple challenges, the Cyprus University of Technology IT Team was searching for a solution that delivered a few key outcomes:

- First, it needed to increase visibility into network traffic and network events. Simply put, the team wanted to see more.
- Second, it needed to make firewall management easier. The team wanted a single console to view threat information, policies, and users.
- Third, it needed to integrate seamlessly with the rest of their deployed security tools.
- Fourth, the solution would need to scale and grow as the network needs of the university increased over time.

The Cyprus University of Technology IT Team were previously using Cisco ASA stateful firewalls with Firepower Services. They decided to upgrade to Cisco’s newest next-generation firewalls running the Firepower Threat Defense platform. This is managed by the centralized management console, Firepower Management Center. They paired their new firewalls with identity services from Cisco ISE and pxGrid.

“Firepower Management Center makes our job so much easier because we don’t have to pivot between multiple interfaces in order to get the information we need.”

Andreas Mouskos
Network Security Engineer
Cyprus University of Technology
The Results

Cisco firewalls transform cybersecurity

Cyprus University of Technology deployed Cisco Next-Generation Firewalls that provided many new features, including:

- built-in intrusion prevention services
- advanced malware protection
- continuous monitoring of malicious network behavior
- web and application filtering

These features provided a few key benefits:

First, the move to Cisco NGFW consolidated the number of security products used by the team, which saved time and resources. “Because these new features were built into the firewall, it allowed us to consolidate the number of products we use,” says Andreas Mouskos, Network Security Engineer for Cyprus University of Technology. “We used to use multiple products to achieve this, but now we have one firewall that does it all for us. This saves us time and money, without compromising security.”

Second, centralized management provided by Firepower Management Center made firewall administration and operations much easier. “I don’t have to pivot between multiple interfaces to get information or to figure something out,” says Andreas Mouskos. “It’s all there in the firewall management console for you to see, and that is so much easier.”

Third, the IT team achieved better visibility across their entire network. “With the next gen firewall from Cisco, we see more,” says Kika Christou, IT Network Administrator for Cyprus University of Technology. “I have full visibility into what is coming into or going out of our network and DMZ Zones. NGFW services like IPS and AMP are able to see and detect threats, and are automatically blocking large amounts of bad traffic and threats for us. I can quickly identify infected or compromised machines and servers, and fix them immediately.”

Finally, segmentation and policy management became easier. “We can manage access and security policies delegated to the user or machine level and we can apply stronger security policies easier and faster,” says Kika Christou. “Segmentation and management is easier because the firewall shows us connection events and security intelligence. This helps us understand details about our very large and complex network.”