Securing Foreign Service Studies at Georgetown University Qatar

The customer summary

Customer name
Georgetown University

Industry
International branch campus of Georgetown University

Location
Qatar
Case study
Cisco Public

Challenge
• Protect student, faculty personal information
• Keep malware command and control out of their network
• Increase visibility and keep up to date on latest threats

Solution
• Two Cisco Firepower 4140 NGFWs with Firepower Threat Defense
• Firepower Management Center
• Advanced Malware Protection subscription
• Next-generation intrusion prevention subscription
• URL filtering subscription
• AMP for Endpoints

Results
• Gained substantial visibility into threats and malware attacking the network
• Talos automatic daily threat feeds saves administrator’s time in protecting against latest threats

Georgetown University Qatar School of Foreign Service (GU-Q) is an international branch of Washington, D.C.–based Georgetown University. Offering a four-year undergraduate program in international affairs leading to the Bachelor of Science in Foreign Service (BSFS) degree, GU-Q prepares students for a variety of careers in international service by providing a four-year liberal arts education focused upon the multidisciplinary study of international affairs.

The resources of Georgetown University coupled with those of the Qatar Foundation allow students and faculty to study, conduct research, and be a part of an educational enterprise that is uniquely positioned to shape international affairs in the century ahead. To that end, Nadim El-Khoury, Associate Director of Information Technology has built out the university’s data center and network with Cisco equipment.

Mr. El-Khoury has supported the IT requirements of 180 employees and 270 students at GU-Q for 13 years. In 2013, he and his team evaluated several competitive security products for installation in their network. This was shortly after the acquisition of Sourcefire so, they included the FirePOWER 8130 in that evaluation. During that proof of concept exercise, Nadim found the ability to drill down on incidents to identify the source of infection to be far superior to what other solutions provided. As a result, the team decided to outfit their network with 2 FirePOWER 8130 appliances deployed in passive mode along with two ASA 5585-X firewalls in the data center, and two ASA 5525-X appliances to handle student and faculty VPN traffic. With FirePOWER, Nadim could see threats and set policy on the ASA 5585-X to block them, great improvement over other solutions. El-Khoury was a pioneer, this would be the first FirePOWER installation in Doha’s Education City.

“The correlation of security events between the FirePOWER 8130 and our new Firepower Threat Defense 4130 appliances was phenomenal. We have complete confidence that we made the right choice to upgrade”

Nadim El-Khoury
Associate Director of Information Technology, Georgetown University Qatar
Fast forward five years to fall of 2017. Both FirePOWER 8130 and ASA 5585-X appliances have reached end-of-sale status. The team was also faced with throughput limitations of the ASA 5525-X that forced the team to set limits on the amount of remote traffic coming through the VPN. Students and faculty would instead work off-line and without security protection compromises occurred. Connecting back with the GU-Q network frequently introduced malware command and control agents into the GU-Q network. Nadim’s team needed find a compromise so fewer infections entered through student and faculty endpoints.

Without hesitation, Nadim called upon his Cisco Sales Engineer Ro’ya Hatamie for guidance. He has had good support over the years with Cisco. At times when he has endeavored to introduce equipment from multiple vendors, deployment was a nightmare with each vendor blaming the other for problems. His path was clear to stick with Cisco for his network upgrade project.

Since 2017, significant advancements have been made at Cisco to integrate the Sourcefire NGIPS, AMP and threat visibility technology with the Cisco Firewall hardware that was currently installed at GU-Q. Now the Cisco and Sourcefire technologies are combined into single device with a single management console for all NGFWs in the network.

To improve throughput for the busy GU-Q campus, Ro’ya recommended that Nadim replace the FirePOWER 8130s with two Firepower 4140 NGFW appliances, with Integrated NGIPS, Advanced Malware Protection, and URL filtering. She also recommended installation of the Firepower Management Center (FMC) appliance to centrally manage all current and any future devices that would be added. And to combat infections coming from off-network devices, Ro’ya advised that AMP for endpoints be added to protect devices when they are not on the campus VPN.

Again, the innovator, Nadim with the assistance of Cisco Gold Partner Mannai NTD, was the first in Education City to install a new Firepower 4140 solution. With NGIPS, URL, and AMP on the NGFW, they are now able to both monitor and block threats without manual intervention. With FMC, the team can see everything happening in the network and save even more time setting policies centrally and analyzing any threats attacking the network from a single console.

Since deploying the Firepower 4140’s, Nadim’s team has kept the old FirePOWER devices running passively in the network. They were amazed to see the 100% correlation of threat events detected on each generation of Cisco security devices. That correlation gave the team confidence that no protection would be lost by decommissioning the old equipment.

Now that AMP for Endpoints is deployed on mobile devices, Nadim’s team no longer is troubled with C&C intrusions on the network. Students and faculty can now have the peace of mind to work off-line and be assured that when they connect back to the campus network there will not be any issues.