

UAE UNIVERSITY, AL AIN

Fortinet secures network and infrastructure

Case Study

Situation

Back in 1976, the United Arab Emirates University (UAEU) was established based on a clear, far-reaching vision of H. H. Sheikh Khalifa Bin Zayed Al Nahyan, the president of the United Arab Emirates, of placing itself at the forefront of scientific and technical learning places and being compared to other internationally renowned universities.

Today, UAEU is still fully committed to the achievement of its goals and contributes towards the advancement of science and technology as well as the development of knowledge in the country. It strives to provide a strong and purposeful educational environment in order to prepare students to confront the competitive world. It also addresses the issue of self-learning and independence of thinking through the use of the latest educational philosophies and technological environments.

Since Information Technology (IT) infrastructure has become a necessity for every modern progressive society, UAEU has wasted no time in adopting the latest technology to build a fully integrated IT infrastructure which supports all its academic services. Faculty, staff and students can use electronic services through the Internet, Intranet, messaging services, specialized IT labs, online training, course information on the Web, etc.

UAEU has nine separate campuses mostly based in Al Ain with one in Abu Dhabi. Each college campus has its dedicated on-site IT support that can escalate a problem to the central helpdesk, which, in turn, refers it to either the Applications Division or to the central Infrastructure and Core Technologies Division. The Applications Division handles all software related issues whereas the Infrastructure and Core Technologies Division deals with all other issues related to the IT infrastructure in the UAEU.

"IT works in layers, and we are focused on providing good quality IT services and infrastructure to our end users, meaning the students and staff of the University," said Manmohan Singh, director of Infrastructure & Core Technologies at UAE University.

On the security front, the Infrastructure and Core Technologies Division at UAEU realized that its existing security set up had some limitations in terms of hardware and support. The previous firewall and Content Services Switch (CSS) had reached end of life and end of support since 2003. Support in terms of spares, telephone support, new patches and software updates were unavailable and the University had no form of monitoring/reporting/alert or centralized management. This put the University at very high risk and UAEU therefore decided to replace its existing firewall and security setup with a complete security solution, which would provide multiple layers of protection aka Unified Threat Management (UTM).

Hani Sultan, security project manager at UAEU said, "The previous Cisco Intrusion Detection System (IDS) was out of date and not functioning. The university constantly experienced worm and virus infections that were attacking servers, consuming network bandwidth and causing considerable network downtime. That's why we wanted to replace the outdated broken intrusion monitoring system with new multipliable- layered UTM technology, which would provide complete online protection to the university users."

UAEU also had no SMTP gateway. Internet users were directly connected to the University's internal email server, which made it vulnerable to attacks, spoofing and mailbox hijacking.

So, as part of its continued overhaul of its IT infrastructure, the university decided to upgrade and update its security implementations, including setting up proper security standards, in order to be able to provide free access to learning tools through the Internet to its staff and students without jeopardising the integrity of its network and other services.



Deployment:
2 x FortiMail-2000A
2 x FortiGate-3600A
2 x FortiGate-1000A
1 x FortiAnalyzer

Industry:
Education

Solution

In order to provide true protection against the Internet threats and other malware, UAEU was looking for a solution that would allow the migration of its 20,000+ email users to a proactive anti-virus, anti-spam service for both its outgoing and incoming email application, with a managed service that would be easy to configure and would provide a friendly user interface. At the network level, the university wanted a high-performance firewall solution with multiple DMZ's.

Both Manmohan Singh and Hani Sultan, Security Project Managers at UAEU, evaluated several security products and solutions in the market and found that Fortinet's range of security appliances provided all the features they were looking for without affecting the overall network performance. So, the university opted for two FortiGate™-3600A multi-threat security systems for its firewall needs and two FortiGate-1000A appliances to provide all the built-in network-level and content-level threat protection. Combined with multi-gigabit performance, all the FortiGate appliances ensure security and throughput.

In order to effectively combat spam within the academy and secure its internal email server, UAEU deployed two FortiMail™-2000A multi-layered, email security platforms. This deployment provided Secure Messaging Platform (SMTP Gateway) to provide optimum configuration flexibility with enterprise-class anti-spam and antivirus functions to secure mission-critical email applications. This gives its 20,000+ users authenticated access to their mails and prevents spam and spoofing.

On top of the deployment of those security appliances, UAEU wanted to be able to get a comprehensive view of its network usage and security information. The university therefore deployed Fortinet's FortiAnalyzer™, which securely aggregates and analyzes log data from the FortiGate security appliances deployed throughout its network. FortiAnalyzer provides UAEU with real-time network log records, as well as a comprehensive report and analysis of network usage and security information, supporting its need for discovering and addressing vulnerabilities across dispersed FortiGate systems. FortiAnalyzer also provides advanced security management functions such as quarantine archiving, event correlation, vulnerability assessments, traffic analysis, and content archiving.

Success

Today, FortiGate security appliances provide integrated security for both UAEU internal (at the datacenter level to protect servers and resources) and external communications, with multiple DMZs deployed for SSL VPN, VOIP, etc. FortiAnalyzer is an essential tool for reports and troubleshooting.

In terms of email protection, despite a total of over 20,000 users, many of whom are using the email services simultaneously, UAEU managed to migrate its system from a Cisco configuration to Fortinet's FortiMail within 36 hours with a record down time of less than one minute.

"We found the Fortinet solutions easy and flexible to deploy," continued Singh. "We were able to activate as many or as few applications as we needed. Besides, unlike Symantec, FortiMail has provided us with excellent results by reducing spam and viruses. We feel we have more control and, using Fortinet, we have succeeded in protecting the entire network from all types of Internet threats."

About Fortinet

Fortinet is the pioneer and leading provider of ASIC-accelerated unified threat management, or UTM, security systems, which are used by enterprises and service providers to increase their security while reducing total operating costs. Fortinet solutions were built from the ground up to integrate multiple levels of security protection--including firewall, antivirus, intrusion prevention, VPN, spyware prevention and anti-spam -- designed to help customers protect against network and content level threats. Leveraging a custom ASIC and unified interface, Fortinet solutions offer advanced security functionality that scales from remote office to chassis-based solutions with integrated management and reporting. Fortinet solutions have won multiple awards around the world and are the only security products that are certified in seven programs by ICSA Labs (Firewall, Antivirus, IPSec, SSL, Network IPS, Anti-Spyware, and Anti-Spam). Fortinet is privately held and based in Sunnyvale, California.

CAS181-0508