SOLUTION BRIEF

Securing Higher Education

Striking the Right Balance between an Open and Secure Academic Environment

Executive Summary

Higher Education institutions are environments that are by nature open, collaborative, rich, and multifaceted. They contend with a large, diverse, and dispersed population and manage multiple networks through which copious amounts of data are accessed.

Their communities contain a treasure chest of information which can include intellectual property, financial records, and health records. Unfortunately, the many users and high value data that they need to protect creates a perfect storm for hacking. It should come as no surprise then that Higher Education was ranked, according to Symantec's 2015 Internet Security Threat Report, the third most-attacked and breached sector. This vulnerability drives IT administrators to find the right security posture that meets the challenges and satisfies the requirements of an institution's network environment.

Joint Solution Benefits

- High Performance and Scalable Network Solution
- Fine Tune Security Services
- Maintain Data Integrity
- Protect Intellectual Data
- Robust Visibility and Protection
- Service Availability

Higher Education Security Challenges

Keeping an Open and Secure Environment

Higher Education draws its success from a communal experience between faculties, students, and partner institutions both locally and worldwide. It is this collaborative approach of sharing best practices and knowledge which enables the institution's growth. Nevertheless, this open environment leaves Higher Education networks exposed to attacks, necessitating a regular and close examination of their network behavior. The challenge for IT administrators is to provide a robust security solution that protects the resources that make this collaborative learning environment possible without hindering it.

Segmenting Network Environment

Higher Education networks are usually organized into the following branches; academic, administrative, and research. This decentralized system with different faculties, branches, and research groups, each managing their own data and resources, makes it difficult for an institution to protect sensitive data and monitor the network. Furthermore, WiFi access adds an additional layer of vulnerability by providing guests and students access to the network from anywhere in the campus. To overcome this obstacle, institutions need to segment their campus networks accordingly (by branch, guest, student, etc.) in order to secure administrative information while permitting open parts of the network to support academic and research programs. Furthermore, a particular focus on securing research traffic is paramount since there is a great deal of valuable intellectual property that must be protected.

Scalability and High Performance

The Higher Education community has been involved with building out high-speed research and scientific networks like the U.S. based Internet2 consortium's 100Gbps wide area network, which is also internationally peered with dozens of like efforts in other countries (JANET in the UK). With typical research networks scaling out into 100 GB environments, Higher Education needs robust solutions that can accommodate these high performance networks. Also, with such a large heterogeneous population to serve, IT administrators need to anticipate network usage and scale accordingly.

Managing Bandwith and Service Availability

With the competitive landscape in Higher Education so intense, service availability can be a significant determinant in a student's selection process. Institutions need to guarantee connections and ensure a seamless academic experience while roaming the campus. Furthermore, with limited bandwidth to go around, IT administrators need to give priority applications and academic sites a guaranteed service level at the expense of less important traffic. Since application priority is relative, administrators are looking to apply unique policies for certain user groups, devices or applications.

Limited Resources

Higher Education is understaffed with a limited budget. They are unable to compete with industry salaries for qualified IT security. According to a survey done by the SANS Institute in 2014:

- 73% of Institutions surveyed indicate lack of budget as an obstacle in maintaining or increasing IT security staff.
- 43% of Institutions reported being unable to compete with higher paying organizations for skilled IT security staff.

The Cost of Breach

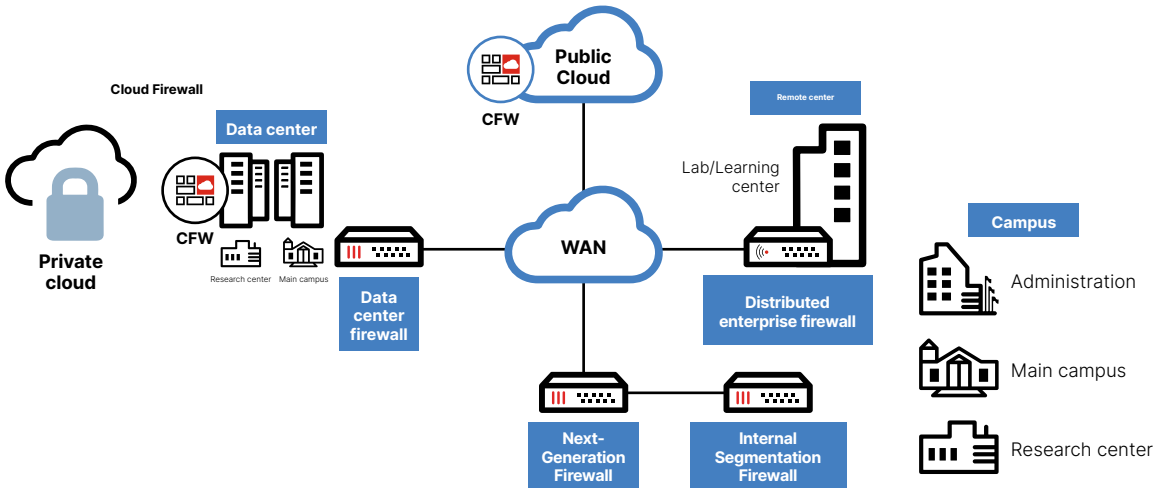
Due to its open culture, Higher Education is particularly exposed to cyber-attacks and at 300$ per lost record, it has the second highest data breach cost across all industries. Besides financial loss, a data breach can be indicative of larger issues in an institution's administration and management, placing its reputation at risk. Furthermore, these security breaches can compromise data integrity holding an institution accountable not only to its students and faculty but to its board of trustees and the academic community as well.

Fortinet Secures Higher Education

Enterprise Firewall Solution

Higher Education requires a network security strategy that addresses the unique requirements of its distributed environment- disparate sites each with their own distinct networking and security requirements.

The traditional approach to this scenario was to mix and match firewalls from different vendors depending upon their perceived position in the market; Vendor A for the data center, Vendor B for the enterprise edge and Vendor C for the remote sites. While it was possible to make this work, the responsibility of creating network wide security policies and managing multiple vendors fell on the IT staff. The drawbacks were the level of complexity introduced into the network, increasing the possibility of human error which could lead to gaps that could be exploited by the hacker or cyber criminal. A second issue was the lack of a single source of threat intelligence. Different vendor's products would have different sources of threat intelligence with no guarantee in the quality or reliability of the individual sources and certainly nothing to synchronize the threat intelligence across multiple vendors. This again would lead to gaps in the level of protection across the network as a whole.



Fortinet's response is its Enterprise Firewall Solution. Due to the breadth and depth of the FortiGate product family, the right product at the right price with the right level of protection and performance can be deployed at any site in the network—remote site, campus edge and data center and in any form factor; physical, virtual or cloud. With a common security operating system, FortiOS, and a single source of threat intelligence, FortiGuard, the Enterprise Firewall Solution meets both the functionality requirements of the institution and eliminates both the complexity and the protection shortcomings of mixing different vendors in the same network.

Having a single security solution ensures that the entire Higher Education ecosystem behaves as a single entity from a policy and logging perspective reducing the risk from advanced threats. Furthermore, security services can be fine-tuned in accordance to an institution's security posture (open or locked down as taken by certain colleges).

Fortinet's Enterprise Firewall Solution can be complemented with wireless technology for a seamless roaming experience as well as with sandboxing technology for Advanced Threat Protection (ATP) across the entire network. Finally, no solution is complete without management and analytic tools to vigilantly monitor student and network activity and generate reports.

Solution Heights

The Enterprise Firewall Solution is unique as it provides Higher Education with the flexibility to choose from five different deployment modes that which best aligns to its security posture and network infrastructure.

Three parameters dictate which deployment mode best corresponds to an institution's security posture:

- Location in the network
- Required functionality (security, performance, access, etc.)
- Security services required

Distributed Enterprise Firewall (DEFW)	Next-Generation Firewall (NGFW)	Cloud Firewall (CFW)
The DEFW is suited to those Institutions with remote sites (labs, learning centers, etc.) looking to deploy networking, security, and access functionality at those remote branches. With networking, security, and access consolidated onto one platform, the solution is cost effective and all aspects of it are managed through a single interface.	The NGFW can be easily deployed at the edge of a Higher Education network looking to secure its access network. It delivers unparalleled protection, ease of use, and ultrafast performance without adding latency and complexity. Security services can be tweaked to accommodate the level of openness required.	The CFW benefits those Institutions managing limited resources and moving their network services to the cloud. Cloud computing is all about elasticity, scalability and automation. The solution provides agile end-to-end security with a broad choice of physical and virtual appliances, helping protect critical data from an Institution to the cloud and back.

Internal segmentation firewall (ISFW)

The ISFW can be used for zoning. It is ideal for Institutions providing guest and student network access and with various faculties, departments, and research networks (Internet2 or JANET) that need to protect critical data such as Intellectual property. ISFW offers an additional security layer to complement existing boundary protections and provides an increased awareness of what's going through the network at all times. It delivers intelligent, adaptive threat protection from the inside out, shortening the window of exposure and limiting damages. ISFW mitigates threats and protects critical assets and data by using network quarantining, actionable security, and complete logging and auditing.

Data center firewall (DCFW)

The DCFW is ideal for those Institutions encountering issues with their existing firewall solutions when employing high-speed networks (Internet2, JANET) and looking to scale to 100GbE security appliances that maximize the utility of these research networks. Furthermore, those Institutions facing congestion with student and other campus user traffic could benefit from a DCFW deployment. All DCFW models are high-performance firewalls and consolidate security services including IPS, antimalware, and application control.

Network management and analytics

Fortinet provides a family of management and analytic tools to vigilantly monitor student and network activity as well as generate reports to meet the security standards of Higher Education as well as external compliance requirements and standards (Prevent Directive in the UK).

Authentication	Analysis	Management
Supports single login, social login, and captive portal authentication options.	Network security logging, analysis and reporting to analyze, interpret, and visualize network threats, inefficiencies and bandwidth usage.	Centralized policy management, analytics and reporting reducing management costs, deployment time, and simplifying configuration.

The Enterprise Firewall Solution is an integral part of a family of solution sets offered by Fortinet. These solutions are a realization of our technology vision, the Fortinet Security Fabric, which is designed to address the security issues and challenges of the enterprise network, like Higher Education. The Fortinet Security Fabric includes the key capabilities for a complete cybersecurity solution by providing broad, powerful, and automated security throughout a university network.

Summary

The Enterprise Firewall solution enables Higher Education to deploy a comprehensive security solution across all parts of its infrastructure while maintaining the same level of services and protection throughout. With the flexibility to choose amongst five deployment modes, the solution can be adapted to an Institution's security posture so that the balance between security and openness is maintained.

September 14, 2021 4:59 AM
485435-B-0-EN