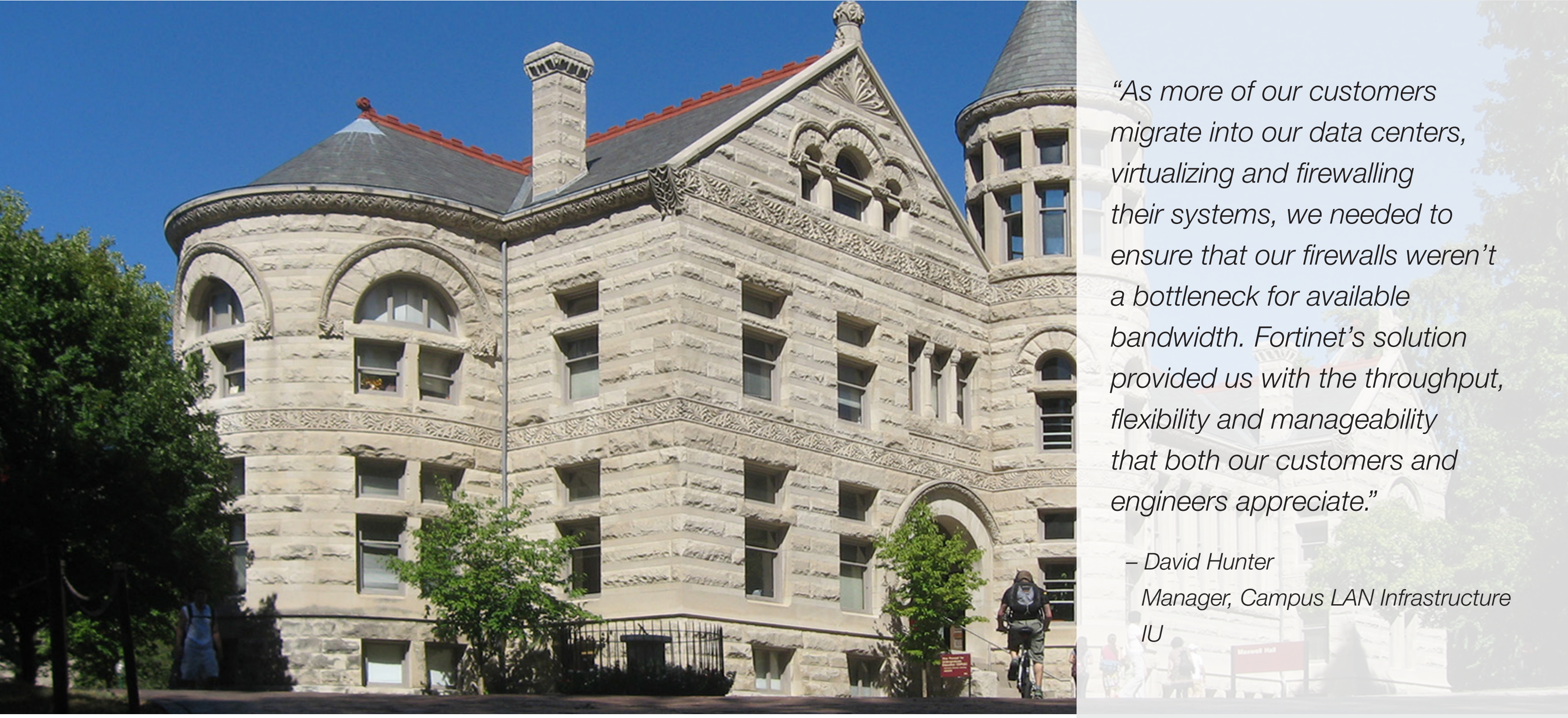
CASE STUDY



> *"As more of our customers migrate into our data centers, virtualizing and firewalling their systems, we needed to ensure that our firewalls weren't a bottleneck for available bandwidth. Fortinet's solution provided us with the throughput, flexibility and manageability that both our customers and engineers appreciate."*
>
> *– David Hunter*
> *Manager, Campus LAN Infrastructure*
> *IU*

INDIANA UNIVERSITY

Fortinet Consolidates and Improves Security at Indiana University

Universities, community colleges, and other institutions of higher education are known for their adoption of technology and openness to allow students and faculty to explore a wide variety of topics facilitating learning and research. Massive Open Online Courses (MOOCs), extended campuses, the proliferation of video and Government requirements are stressing existing network infrastructures. Many Higher education institutions struggle to build adaptive and cost-effective network infrastructures to support today's sophisticated styles of teaching and learning while enduring state and federal cuts facing many of these institutions. Even though IT has moved from a back office operation to foundation of education in America, the change has not always been well funded. While openness is a primary concern for higher education environments, security has often suffered as a result.

Many universities today resemble large enterprises, supporting hundreds of applications and tens of thousands of users. These institutions also have to contend with privacy concerns as well as other regulatory compliance mandates such as the Payment Card Industry Data Security Standard (PCI DSS) and the Health Insurance Portability and Accountability Act (HIPAA). As a result, higher education institutions are moving their infrastructures to data centers in order to centralize support and

Details

Customer Name: Indiana Univerisity
Industry: Education
Location: Bloomington and Indianapolis, Indiana (core campuses)

Challenges

- Security was a bottleneck
- Management was too complex

Objectives

- Increase available bandwidth
- Improve manageability of the network

Deployment

- FortiGate
- FortiManager

improve efficiencies within the IT organization. While these moves are required, a whole new class of equipment is required to operate and defend these environments.

This case study will examine Indiana University's decision to adopt Fortinet equipment in the data center core. In 2012, Indiana University found that it needed an improved security infrastructure as part of its distributed data center environment. Indiana University was looking for a solution that could support a wide variety of new technologies without any degradation in performance. As the result of an RFP process Fortinet was selected for their performance, manageability, and competitive price.

About Indiana University

Indiana University is a multi-campus public university system in the state of Indiana. Indiana University has a combined student body of more than 110,000 students, spread across eight campuses including core campuses in Bloomington and Indianapolis, and regional campuses in Fort Wayne, Gary, Kokomo, New Albany, Richmond, and South Bend. The university also has more than 17,000 faculty and staff and more than 200 research centers and institutes.

Indiana University's mission is to provide broad access to undergraduate, graduate, and continuing education for students throughout Indiana, the United States, and the world, as well as outstanding academic and cultural programs and student services. Indiana University seeks to create dynamic partnerships with the state and local communities in economic, social, and cultural development and to offer leadership in creative solutions for 21st century problems. Indiana University strives to achieve full diversity, and to maintain friendly, collegial, and humane environments, with a strong commitment to academic freedom.

The Requirements

Supporting all the requirements of a multi-campus environment requires a dedicated staff and data centers. Securing the wide variety of applications, databases, and information flow is just as critical as having the infrastructure in place. Indiana University had very specific security requirements as part of their data center security upgrade. Many of the requirements are described below.

High Performance to Increase Available Bandwidth

Network bandwidth is generally thought of in terms of the overall speed of the network. Most IT organizations place the importance of bandwidth on the routing and switching infrastructure of the network. Unfortunately, security appliances can also be a cause of lowered bandwidth, causing lowered performance across the network. Although it is essential for any network security solution to have as little effect on network performance as possible, metrics like latency have not been a focus for most network security vendors.

Indiana University was looking for a solution that would increase the overall firewalled throughput, in and out of their data centers. Indiana University needed a solution that could provide multi-gigabyte firewall performance while still delivering high levels of sessions. Due to the bandwidth sensitive nature of many of the applications running over the Indiana University network (several voice, video and data applications), being served by a large virtualized environment, increased bandwidth and latency were key factors.

Improved Management Functionality

Another important consideration for Indiana University in choosing a new security infrastructure provider was the ability to easily change rules and manage the large number of devices – both physical and virtual – on the network. With fifty to sixty rules changes required per week, Indiana University needed a management platform that could effect those changes quickly and efficiently, without a steep learning curve.

High Performance Support for IPv6

Indiana University is one of over 200 hundred universities participating in internet2. Internet2 is a member-owned advanced technology community founded by the nation's leading higher education institutions in 1996. Internet2 provides a collaborative environment for U.S. research and education organizations to solve common technology challenges, and to develop innovative solutions in support of their educational, research, and community service missions. Internet2 consists of more than 220 U.S. universities, 60 leading corporations, 70 government agencies, 38 regional and state education s and more than 100 national research and education networking partners representing more than 50 countries.

In addition to being part of the consortium, Indiana University also hosts the Global Network Operations Center (NOC) for internet2. One of the core requirements for internet2 is support for IPv6. Indiana needed a solution that could secure both IPv4 and IPv6 traffic without a significant drop in performance.

Security for Virtualized Environment

Data entering and leaving the cloud should be treated like any other data entering or leaving the network. Traditional security precautions such as firewall, intrusion prevention, and content filtering all need to be applied. The additional challenge associated with securing data in the cloud is that the security architecture must also secure the multi-tenant nature of the traffic. This translates into the security architecture having the ability to provide entirely separate policies on traffic, depending on origin. The security appliances in place must also have the ability to keep traffic entirely separate in order to avoid any risk of exposure.

High Availability and Disaster Recovery (DR) Capabilities

Being a highly distributed campus environment, Indiana University needed to configure and maintain high availability and disaster recovery capability between its data centers. These capabilities must be extremely responsive, having the ability to move traffic to a different site at the smallest sign of a disruption. Indiana University relies on a Multiprotocol Switching Label (MPLS) network and any infrastructure security device would need to support that configuration.

Fortinet Delivers the Answer

Fortinet was one of the vendors who made a bid to win Indiana's University's business. After reviewing proposals, IU chose to conduct a formal Proof of Concept with Fortinet, and Fortinet was chosen as the new security infrastructure vendor. There were a number of factors that allowed Fortinet to shine, but the three key areas that drove the decision were Fortinet's performance, management, and ultimately lowered TCO. These are described below.

Performance

Indiana University found that Fortinet performed well in throughput testing. Because of Fortinet's investment in creating custom ASIC processors that provide switch-like latency for any size data packet, data center customers can experience ultra-low latency while deploying multiple security technologies, such as firewall, intrusion prevention, and application control.

Increased Bandwidth

Bandwidth constraints were one of the key challenges facing Indiana University. The bandwidth available to applications was limited by their security equipment. Fortinet has undergone extensive third party validation around its capabilities to provide very low latency and a high number of sessions. The combination of these performance factors allowed Indiana to see a noticeable difference in performance the moment the appliances were installed.

Fortinet Delivers Top Notch IPv6 Performance

Indiana University also required superior IPv6 performance. Their positioning as a top tier research school and their positioning within internet2 required a solution that could deliver as close to equal performance between IPv4 and IPv6 traffic. Fortinet has worked diligently to ensure that its performance on IPv6 networks is as close to IPv4 as possible. Fortinet's custom hardware design allows for customized processing of traffic.

Management

Fortinet's management capabilities were another key factor in Indiana University's choice of Fortinet. By default, Fortinet provides the ability for customers to segment their security by Virtual Domains (VDOMs). VDOMs provide separate security domains that allow separate zones, user authentication, firewall policies, routing, and VPN configurations. VDOMs separate security domains and simplify administration of complex configurations—security administrators do not have to manage as many settings at one time. This is critical for complex networks that might have different administrators for different functional domains or for different groups of devices.

VDOMs also provide an additional level of security because regular administrator accounts are specific to one VDOM — an administrator restricted to one VDOM cannot change information on other VDOMs. Any configuration changes and potential errors will apply only to that VDOM and limit any potential down time. Using this concept, you can further split settings so that the management domain is only accessible by a single admin and does not share any settings with the other VDOMs.

Customized, Separate Security

VDOMs also provide a continuous path of security. When a packet enters a VDOM, it is confined to that specific VDOM and is subject to any firewall policies for connections between that VDOM and any other interface. When hosting separate clients or entities on a single cloud architecture (very common with public and community clouds), the ability to guarantee that no data can pass from one connection to another is a critical requirement.

Single Pane of Glass Management

Fortinet's management platform is focused on delivering users a 'single pane of glass'. What that helps do is help mitigate risk through the ability to consolidate security platforms and simplify the overall network management capabilities. It offers the ability to see layers one through seven and all of the information that passes through the networks, all the devices and users that connect to the network. We are there to view it, log it, audit it and report on it to provide an overall security posture to the covered entities and users. Fortinet offers users the ability to propagate changes, view logs and events, and manage the entire network – physical and virtual – from a single centralized location in the network.

Overall Lower Costs

The ability to lower overall costs the final key factor in the decision to choose Fortinet. By consolidating a wide variety of functions on high performing hardware, Fortinet is capable of providing a single security platform to organizations, allowing them to invest in one platform.

Lower Maintenance Costs

Fortinet consolidates all the security and management functions under a single platform. This allows organizations to pay for support and maintenance just one time. When a mix of solutions is deployed, organizations pay maintenance and support fees to each vendor increasing the overall costs of security.

Lower Training and Support Costs

Fortinet provides an intuitive, consistent user interface that allows end users to perform complex tasks quickly. Indiana University was able to deploy new appliances, build policies, monitor performance, and build out administrative domains with a minimum of training. These lowered support costs allow for less ramp time for new employees and allows existing employees to move seamlessly into different roles in the organization.

Conclusion

Higher education environments are becoming some of the most technologically advanced networks in use. The large user base and push for high bandwidth applications are driving universities to deploy complex networks with demanding performance and feature requirements. The Indiana University network environment is indicative of this trend. Indiana University required an advanced security infrastructure to support its multi-campus environment that would enable the speed of operations.

After an extensive review process, Indiana University selected Fortinet as its firewall vendor for their data center. IU also chose Fortinet to protect their specialized networks created for PCI DSS and Health Sciences. Fortinet provides the performance, support for new features, management capabilities, and lowered total cost of ownership required by Indiana University. In just a short time, Indiana University has seen a significant increase in bandwidth and network performance. Management and support time has already decreased and the entire network is running more smoothly than it ever has.

FORTINET®

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA SALES OFFICE
Paseo de la Reforma 412 piso 16
Col. Juarez
C.P. 06600
México D.F.
Tel: 011-52-(55) 5524-8428