SECURE ACCESS SOLUTION

With Fortinet, universities and colleges get everything they need to effortlessly onboard thousands of devices, manage and prioritize application usage, scale capacity with ease, and enjoy world-class protection from current and evolving threats.

Secure Access for Higher Education

Superior Wi-Fi Experience and Threat Protection

Every semester thousands of new mobile devices join the wireless network for the first time, bandwidth demands sky-rocket, new applications ascend and new cyberthreats manifest.

Shifting usage from the “trusty laptop” to a smartphone one minute, a tablet the next, an eBook reader next, often using multiple devices together, has made students completely dependent on Wi-Fi and the cloud. They expect reliable connections and need better security and smarter application prioritization.

Fortinet’s Secure Access Architecture for higher education complements breakthrough WLAN quality of experience, streamlined onboarding and the industry’s easiest deployment, with world-class cybersecurity, to provide an outstanding Wi-Fi experience with complete protection from current and evolving cyberthreats.

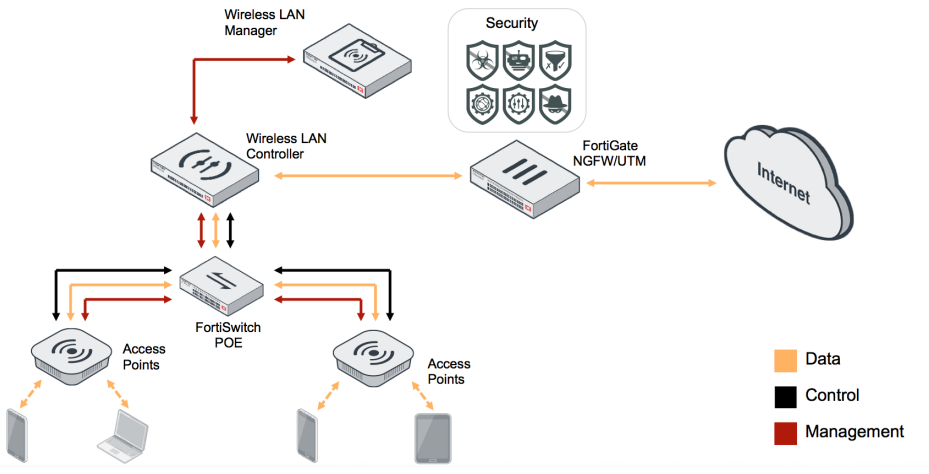

Figure 1: Fortinet Infrastructure secure access solution

- Easiest deployment and capacity scaling in the industry
- Better Quality of Experience with faster, more reliable roaming
- Bonjour multicast suppression to prevent bandwidth waste
- Superior 802.11ac performance with site-wide channel-bonding
- Comprehensive threat protection consolidated on one appliance
- Exceptional visibility and control of applications and utilization
- Security kept up to date through regular signature updates from FortiGuard Labs

Higher Education Access Challenges

Reliance on the Network

The days of working offline are over. Nowadays, students and faculty are connected 24/7, and highly dependent on cloud resources. Over 50% of U.S. students use learning apps on their mobile devices, while 50 million students worldwide rely on Google Apps for Education and Office 365 for Email, Calendaring, PowerPoint, etc., and hundreds of millions more cannot function without access to their music and files on cloud storage (iCloud, Dropbox, Google Drive, etc.).

Paralyzed without it, students need reliable Internet access day and night. It goes beyond uptime. It's about roaming without dropping connections, connecting from anywhere without failure, having the resources to do anything on all of their myriad devices – downloading lecture notes on the run between classes; Skyping from the café; watching a movie in the dorm while catching up on Facebook – and having it all work, every time, without interruption.

Surging Application Usage

When students are not learning, they are playing, gaming and socializing online in their dorm rooms, the cafeteria, outside their next class, everywhere. From multimedia courseware to Netflix, streaming video is growing 40-60% annually and "Trailing Millennials" (ages 14-25) are its top consumers.

There is no escaping the spiraling bandwidth demands, and on the horizon wearables (watches, trackers, augmented reality, etc.) and Wi-Fi Calling threaten to strain the network further. With only budget enough to replace 20-25% of older access points each year, universities have no choice but to manage bandwidth better – selectively throttling the bursty (Bonjour) and hungry (rich media) applications while prioritizing the important ones, to prevent non-academic abuse from disrupting education delivery.

Onboarding Users and Devices

Securely onboarding new users and devices on the scale facing academic institutions is no trivial matter. Every new device poses a threat to the network, through the malicious activity of a student or simply as a vehicle for malware.

However, without sophisticated self-service onboarding mechanisms tied into your AAA security framework, getting the vast array of student devices onboarded quickly can bring your support team to its knees.

But device onboarding is not the endgame. It is just one facet of a much bigger access security picture. Educational institutions should be equally concerned about securing the real-time data traversing your network, blocking known malicious sites, and internal segmentation to break or delay the infection chain should a hacker or virus penetrate your defenses.

New Threat Vectors

Cyberattacks are more frequent and more sophisticated. Standard wireless security features such as WPA2, 802.1X, the various EAP types, Rogue AP Detection and Wireless Intrusion Prevention are all valuable. But, complete protection normally requires a variety of security appliances for Firewall, IPS, Anti-malware, Web Filtering and Application Control, which can add considerable deployment complexity.

Mobile operating systems, gaming devices, wearables and other headless devices are some of the most attractive entry point for attacks. Often, the attack on the device is simply a jump-point to gain access to much more valuable systems on the inside. Because of this, Next Generation Firewalls (NGFW) and Internal Segmentation Firewalls (ISFW) are becoming essential.

Fortinet Secure Access Architecture

All businesses face similar access challenges – coverage, performance, reliability, BYOD onboarding and cybersecurity – but they don't always tackle the problem the same way. They differ in their preferred network architecture and topology, and organizationally in where IT roles and responsibilities fall.

While other WLAN vendors present the same solution for every problem, everyone knows one size does not fit all. Hence, Fortinet's Secure Access Architecture embraces all common WLAN topologies and deployment models, backed by the strongest access security in the industry.

Only Fortinet has three distinctly different wireless offerings: an *Infrastructure* solution made up of best-of-breed wireless, switching and security components; an *Integrated* solution in which WLAN control and security are combined on a single, high-performance appliance; and a third, *Cloud* solution that embeds security intelligence into cloud-managed access points.

Fortinet Infrastructure Wireless Solution

Fortinet's recommended secure access solution for higher education campuses is its *Infrastructure* wireless offering. It delivers high throughput and scales more easily than any competing WLAN solution. It provides everything a school needs to effortlessly onboard thousands of devices, manage application usage, and enjoy world-class threat protection.

It consists of best-of-breed components for switching, WLAN (formerly Meru Networks) and cybersecurity. The WLAN component provides a high-performance, premise-managed Wi-Fi network with a broad range of 802.11n and 802.11ac access points (APs). While FortiGate provides an access security overlay featuring a comprehensive portfolio of security services and granular application control, consolidated on a single, high-performance appliance.

The WLAN component uses a unique channel-management architecture called Virtual Cell, which differs from the traditional channel deployment approach adopted by all other vendors, while also offering a number of compelling benefits.

Virtual Cell minimizes the complex, time-consuming process of channel planning, which can take months for a large campus, through its unique single channel deployment model which avoids the challenges of planning around co-channel interference.

Figure 2: Fortinet Virtual Cell Deployment Model

All APs operate on the same channel to provide a layer of coverage across your campus. The unique Fortinet virtual cell technology effectively handles co-channel interference, even with widespread channel re-use. Because all access points in a virtual cell effectively appear to the client as a single AP, thus users enjoy a seamless roaming experience across the network.

Rapid Deployment and Scaling

The Fortinet *Infrastructure* secure access solution simplifies deployment by dispensing with site surveys, channel planning and all of that worry over cell sizes and transmit power. To increase coverage or capacity, simply plug in another AP anywhere convenient, even right next to another one, and it is ready. No channel adjustments or site surveys are required.

For serious capacity scaling or to wirelessly segment users and applications, multiple Virtual Cells can each use a different channel, while occupying the same coverage area by adding additional sets of APs. Layering cells in this way can be limited to a small zone or span your entire campus.

Layering new Virtual Cells does not require changes to existing cells, so the stability and performance of your existing environment is never at risk when you scale capacity.

Traffic Isolation

Another valuable use for channel layering is the ability to separate services at the RF level. This gives mission critical services dedicated spectrum and immunity from the risk of congestion on other channels. Schools might separate faculty and teaching resources from students or put surveillance cameras, voice services and building management control systems on different channels (see Figure 3).

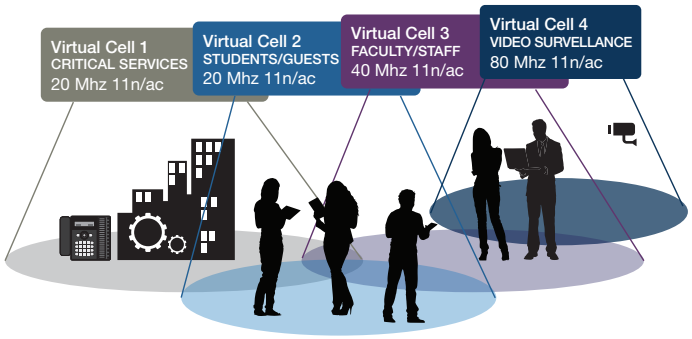

Figure 3: Campus-wide capacity scaling with channel layering

Reliable Connections

Another huge difference is that it is the network, not the client that decides when and where a client should roam for best service, resulting in a better quality of experience. This approach ensures student devices always use the optimum connection available to them, and don't drop connections as they run from class to class.

Users roam from one AP to another with zero handoff, taking only 3 ms versus the typical 120+ ms reassociation delay for traditional multi-channel deployments, where even with 802.11k and 802.11r activated on the client, best-case reconnection time is 50 ms. Zero-handoff roaming solves the all-too-common problem of voice, and other latency-sensitive real-time sessions, being dropped while roaming.

This network based traffic control enables real-time AP load balancing based on actual traffic, not crude round-robin algorithms based on station count. The network even governs station airtime so every client gets a fair turn on-air, and slow devices don't occupy all of the airtime.

Bonjour Multicast Suppression

Wherever you have a lot of Apple fans, you'll likely run into problems with Apple's Bonjour technology, which can ravage bandwidth with thousands of irrelevant multicast packets while students connect to their Apple TVs and wireless printers. The multicast advertisements may be small, but they can propagate everywhere and hit everyone.

Fortinet's Service Control feature overcomes these issues by maintaining an internal table of devices advertising services via Bonjour, and then mediates the discovery process, converting multicast probes and advertisements into unicast traffic. This approach completely neutralizes the harmful effects of AirPlay and AirPrint proliferation in student dorms, by slashing bonjour related traffic to less than 1% of its former levels.

Security and Application Control

Security and granular application control is provided as an overlay with the FortiGate appliance, which has been proven time and again to outperform all network security rivals.

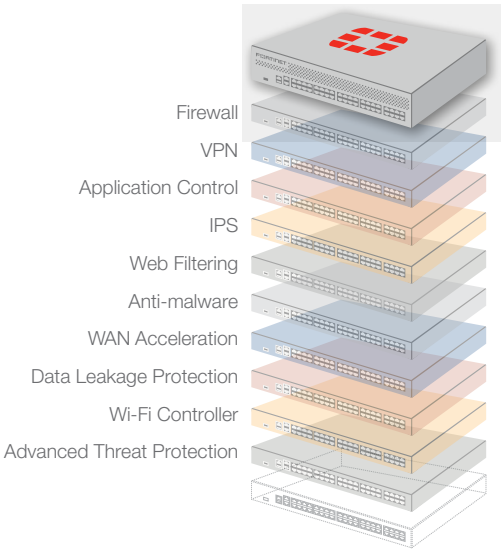

Figure 4: FortiGate consolidated security platform

FortiGate consolidates the functions of more than seven individual security devices, including Firewall, VPN Gateway, Network IPS, DLP, Anti-malware, Web Filtering and Application Control, in a single, high-performance platform.

When applications compete for limited resources, something has to give. For example, say Facilities staff use wireless VoIP handsets instead of walkie-talkies to stay in touch. FortiGate has the granularity to distinguish between VoIP calls from Facilities and a Skype call from a student, and provides the ability to apply a unique policy to each.

You can de-prioritize High-Definition YouTube, while prioritizing streaming video content from faculty servers. With signatures for over 4,000 applications, FortiGate provides detailed visibility of application usage, as well as precision controls to prioritize, throttle or block literally any application.

FortiGate security is kept up to date through frequent automated updates from FortiGuard Labs, which researches the latest attacks to provide your network with immediate protection.

Internal Segmentation

Many higher education networks are quite flat. But as cyberattacks become more sophisticated, we now know from recent documented exploits that once hackers breach perimeter defenses, they can wreak havoc on a flat network very quickly.

Multiple layers of defense is the new standard to protect against highly sophisticated attacks that are getting past border defenses. Explicit internal segmentation, with firewall policies between users and resources, limits traffic, gives you logs and helps to break the infection chain.

But software-based firewalls designed for the perimeter are too slow. Fortinet is first to market with a hardware-assisted Internal Segmentation Firewall with multi-gigabit line-rate performance.

Summary

Higher education WLANs are moving into a new era in which the coverage and bandwidth concerns that dominated the past, and still remain, are now being eclipsed by security and application-management priorities.

Thanks to a unique Wi-Fi channel-management architecture, Fortinet's *Infrastructure* access solution for higher education delivers superior throughput and more reliable connections than any competing WLAN solution, with easy deployment and scaling.

When combined with FortiGate, the performance leader in network security, universities and colleges have everything they need to effortlessly onboard thousands of devices, manage application usage and priorities, and enjoy world-class protection from current and evolving threats.

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

Jan 26, 2016