SOLUTION BRIEF

Securing and Simplifying Network Access for Higher Education

Enabling Zero-Trust Network Access Using FortiNAC

Executive Summary

Colleges and universities offer target-rich environments for cyber criminals. From financial, medical, and personal data to government and commercial research, educational networks can contain a wealth of data, numerous access points, and large volumes of endpoint access—all of which require unique security solutions. Institutions must define and implement a comprehensive security architecture that provides end-to-end network visibility, dynamic access control, and automated threat responses. FortiNAC offers an ideal network access control (NAC) solution. Part of the Fortinet Security Fabric, it offers compatibility with a wide range of third-party security solutions to help schools secure sensitive data while maximizing the value of their existing infrastructure investments.

Digital Challenges for Higher Ed—BYOD and IoT

Today's digital campuses require connectivity for numerous types of devices—from the mobile solutions of faculty, staff, and students to smart devices in classrooms and dormitories. Securing the network while enabling easy, automated access for a large volume and variety of endpoints is one of the greatest challenges for colleges and universities. Schools must balance technology controls with simplified access to ensure a productive and secure campus environment.

The quantity of devices per student has increased steadily over the last few years, rapidly expanding the number of endpoints that must be controlled. In addition to greater mobile access demands as a result of bring-your-own-device (BYOD) policies, colleges and universities are also facing a surge of new Internet-of-Things (IoT) devices that are flooding campuses. With thousands of new IoT devices introduced each year, students and campuses alike are now connecting IoT-enabled devices—such as printers, cameras, lighting, and climate controls—to the campus network. But campus IT leaders aren't keeping pace; more than 60% haven't made network security changes in two years[1] and 57% use outdated security measures, such as too-infrequent password updates.

Moreover, campus facility managers are often unintentionally complicating this already intricate network. By adding even more devices to networks without notifying campus IT and security teams, facility managers run the risk of creating new Shadow IT issues that add to the already growing risk of vulnerabilities.

On top of all of it, the shift to remote learning catalyzed by the COVID-19 pandemic has created even more of a threat from opportunistic cyber criminals. Already-prevalent attack vectors such as spam emails spiked by 26% during the first 100 days of the COVID-19 outbreak,[2] and in May 2020, the FBI and Cybersecurity and Infrastructure Security Agency (CISA) warned that COVID-19 research organizations, which include many colleges and universities, are major targets for espionage hackers.[3]

FortiNAC provides:

- Complete visibility and automated onboarding for endpoints (managed, BYOD, and IoT)
- Pre-connect and post-connect device monitoring
- Granular network access controls to enable micro-segmentation, grouping similar devices into narrow, functional slices of the network
- Device scanning for risk assessment to enforce minimum security requirements (OS, antivirus)
- Ability for custom access levels by user or role
- Automated threat responses to quarantine suspicious IoT devices, BYOD, and other endpoints
- Quick and easy scalability—each VM instance can support 25,000 concurrent devices with no upper limit on the total solution capacity
- Easily deployed across wired and wireless networks due to extensive multivendor support
- Rapid identification of devices in seconds using up to 20 different profiling methods, including active and passive means

The Need for Automation—Provisioning, Access, and Responses

Without compensating security controls, introducing countless new endpoints onto a university's network can be dangerous and expose a school to a wide variety of attacks. Universities must be able to monitor and control endpoint access, and set minimum security standards for students, faculty, contractors, and guest devices using zero-trust network access (ZTNA) principles. Schools must also ensure an automated and efficient way for these tens of thousands of devices and users to access the system with the appropriate level of access for each.

Additionally, with thousands of security alerts per day, overwhelming network traffic, and scarce IT resources, colleges and universities cannot manually review all potential issues. For effective security, schools must also automate policy-based event triage and quarantining of suspect users and devices.

"Zero trust" as a concept has become a tech industry buzzword in recent years, so it's important for administrators to understand what a true zero-trust network access strategy entails. It starts with three essential functions:

- Knowing what is on your network
- Knowing who is on your network
- Protecting assets on and off the network

Solving the Campus Security Challenge

As part of the Fortinet Security Fabric architecture, FortiNAC offers a NAC solution designed to protect networks with IoT devices. Security leaders in these environments need to be aware of each and every device and user on their networks and allow them appropriate access.

As a critical piece of the Fortinet Zero-Trust Network Access framework, FortiNAC equips security leaders with the tools they need to successfully manage and secure their complex IoT networks. The Fortinet solution provides the visibility to see everything connected to the network, as well as the ability to control those devices and users, all while providing dynamic, automated responses to threats.

With simple, centralized management, FortiNAC ensures that if a device is compromised, it can be located quickly, even if the device is in a remote location.

Visibility

With thousands of endpoint devices, identifying "who, what, when, and where" is critical to locating and securing compromised devices. FortiNAC provides the deepest level of network endpoint visibility. It profiles every endpoint and infrastructure device on the network, and provides contextual awareness about the device, user, and applications. It also tracks and monitors all activity. For IoT devices, FortiNAC identifies headless devices each time a device connects to the network. When new devices connect, it notifies the device sponsor to authorize the device onto the network and records every action taken by the device. With simple, centralized management, FortiNAC ensures that if a device is compromised, it can be located quickly, even if the device is in a remote location.

Control

FortiNAC provides contextual awareness for scalable onboarding and dynamic network access control. Network access can be assigned using automated, predefined profiles—saving a significant amount of time when onboarding large numbers of students, faculty, contractors, guests, or staff.

To manage high volumes of BYOD devices, FortiNAC helps institutions set and enforce minimum security requirements for things like current operating system patches and antivirus software. Using a pre-connect scan, FortiNAC only grants access for devices that meet requirements and can automatically direct users to a self-remediation page for those that don't qualify. FortiNAC also provides continuous post-connect scanning to look for devices and/or users that act suspiciously or fall out of network compliance.

In addition, FortiNAC provides granular control of endpoint access policies and permissions by role or by user to ensure users only receive the necessary amount of access. Integrated within the Fortinet Security Fabric, FortiNAC provides centrally managed, end-to-end control of the entire fluid network, including satellite campus locations.

Automated Threat Responses

FortiNAC supports automated threat responses including immediate quarantining of suspicious devices/users, triaging of events, and streamlining analyst reviews by delivering all contextual information along with the alert. By leveraging contextual awareness from the broader Fortinet Security Fabric, FortiNAC helps analyze and prioritize security events. It streamlines multistep workflows and integrates with ticketing systems to provide real-time endpoint containment. This speeds the time to resolution and reduces the burden on strained IT resources.

FortiNAC also acts as a compensating control for IoT devices with weak security. It monitors the devices for unusual behavior and automatically quarantines devices that act suspiciously. For example, if an IoT device starts pinging a DNS server, it will be tracked, an alert is generated, and the port can be immediately locked down while awaiting analyst review.

To manage high volumes of BYOD devices, FortiNAC helps institutions set and enforce minimum security requirements for things like current operating system patches and antivirus software.

FortiNAC supports automated threat responses including immediate quarantining of suspicious devices/users, triaging of events, and streamlining analyst reviews by delivering all contextual information along with the alert.

Summary

FortiNAC offers unparalleled visibility, control, and automated responsiveness for educational network access. Beyond those core capabilities, FortiNAC can be deployed as a hardware appliance, a virtual appliance, or a cloud service—offering school security architects a flexible, third-generation NAC solution that can adapt to the unique needs of any network environment. Designed with scalability in mind, FortiNAC also helps lower total cost of ownership by not requiring a server in every deployment location. It leverages existing directory, networking, and security infrastructures to protect existing investments and minimize disruption.

FortiNAC is a key element of the unique Fortinet approach to ZTNA. By transitioning to a ZTNA framework that identifies, segments, and continuously monitors all devices, higher education institutions can successfully replace high-risk networks, ensuring that internal resources remain secured, and data, applications, and intellectual property remain protected.

[1] Infoblox study, October 11, 2018.

[2] Robert Lemos, "Attackers Adapt Techniques to Pandemic Reality," Dark Reading, May 5, 2020.

[3] "FBI and CISA Warn Against Chinese Targeting of COVID-19 Research Organizations," FBI National Press Office, May 13, 2020.

July 24, 2020 12:30 PM

733567-0-0-EN

D:\Fortinet\Work\2020\July\072420\sb-network-access-higher-education