FORTINET

Creating a Secure Campus Network: 4 Vital Steps to Success

Table of Contents

Executive Overview

Building a modern campus network is not for the faint of heart. As organizations accelerate digital innovation, enterprise networks are much more complicated and dispersed, with an ever-growing number of edges.[1] Organizations increasingly need their networks to do more, so creating one that can handle all of the demands of today is not enough. It's also key to consider what tomorrow will bring, which takes careful planning. Follow the steps in this ebook to ensure secure connectivity on a smoothly running network that will be reliable for years to come.

> **"Organizations require a strategy where security and networking function as a unified framework to provide dependable connections anywhere on the network."[2]**

Step 1: Understand Your Environment

Every network needs to be built according to the physical environment it will run in. That environment is more than just the building but also who the users are, what devices they use, and what applications they need to run.

Where?

Every building is different, and over time, the way a building is used can change as well. Before deploying a new network or a network refresh, ensure that you understand the nature of the physical environment. Track where users congregate besides the conference rooms. Are there other areas, like manager's offices, break rooms, and seating areas, commonly used for collaboration? Be sure to Include additional capacity in these areas as part of the plan.

In addition, you need to be aware of the materials in use in the building and the furniture. Metal items can have a serious impact on Wi-Fi signal propagation. Once you understand where additional capacity is needed and where there are RF obstructions (or other interference sources), you can assemble a solid access point (AP) placement plan. Then, you can move upstream and ensure that switching capacity to service that number of APs and the Power over Ethernet (PoE) they will require is sufficient.

Who?

Most enterprise settings have a variety of users, from employees to visitors to contractors. It is critical to know who these people are, what level of network access they can (and should) expect, and where they can (and should) have access. Remember that building a network is also about securing it, so have a plan for where visitor network access or contractor access makes sense and where it doesn't. Ensure your network is being built for different access levels depending on user groups.

What?

Network users connect myriad devices to the network, and now, with the growth of IoT devices, the number and types of devices at a site can vary quite a bit. Understanding what these devices are and what capabilities they have (from both a network technology and security perspective) is absolutely necessary. Without this knowledge, planning a network that can appropriately support whatever may connect is very difficult. Devices that support fewer security capabilities and headless devices may require the deployment of additional security measures within the network.

It's also important to consider how often your client base typically churns. If new devices frequently enter the network or if devices tend to go more than three years between replacement cycles, different decisions should be made regarding networking standards and security measures.

How?

Key considerations include understanding who will be using what applications and how they will be accessed. Catalog the applications and compare them with the users likely to use them. Ensure that the network is designed to support any latency or jitter sensitivities among the application set.

Be sure to consider what applications and use patterns are likely to be driven by new or in-flight corporate initiatives. These may not change current network needs but could impact the network in the future, and the network being deployed today will need to support future initiatives. These application needs will drive both network and security planning in later steps.

“Internet-connected devices may be used by nefarious entities to collect personal information, steal identities, compromise financial data, and silently listen to or watch users.”[3]

Step 2: Build a Network Plan

Once all the information has been pulled together and understood, it's time to build the network plan. We'll start at the most common access layer (wireless) and move inward from there.

The wireless layer

Choose the wireless network technology that will work best based on the catalog you created that maps users and devices. When considering what standard of Wi-Fi to deploy, something to keep in mind is pricing. While newer generation standards are often more expensive, typically, the cost is not significantly higher than previous generations. If you have high turnover of client devices or expect major changes in network use in the coming years, there can be value in future-proofing with the latest technology. If your network and use patterns are more steady, there may be less need to push for the latest standards, and budget can be reserved.

To determine proper placement of APs, use site survey data of the current environment or engage in extensive planning for greenfield deployments.

Aspects of the physical environment cataloged in step one become important here, especially in new deployments. Knowledge of the building materials and what furnishings will go into the location can decide whether RF planning software gets it right or misses the mark. Most modern Wi-Fi solutions can adjust channels and power to compensate for imperfections, but significant planning problems can haunt a deployment for years if care isn't taken upfront.

The wired layer

There are several aspects to planning the wired backbone of a deployment. The typical aspects to look at are port count (the number of wired ports your deployment needs), power budgeting (especially for Wi-Fi access points and any PoE-driven phones or industrial equipment), and overall capacity. By understanding the number of types of devices and users, switch capacity can be planned and built accordingly. Be sure to include any IoT or OT devices that will need wired network connectivity.

WAN connectivity

Ensuring the proper business outcomes for employees often requires constant and reliable access to applications and data that reside off-site. Plan WAN connectivity to allow for redundancy and use technology such as SD-WAN where appropriate to ensure application performance is met. Size WAN connections for the amount of data likely to leave the site and take into account planned shifts to cloud resources that may put additional requirements on bandwidth and resiliency of the WAN.

One of the most essential components of a hybrid mesh firewall is its ability to traverse today's multi-cloud and hybrid data center environments. Hybrid mesh firewalls rely on a unified management console to coordinate protection across every IT domain (corporate sites, public and private clouds, and remote workers)."[4]

Step 3: Build a Security Plan

Traditional flat networks, even those using network-based segmentation or microsegmentation techniques, cannot detect or stop today's sophisticated attacks. Part of the problem is that many of these networks still provide authenticated users and devices with unfettered access to virtually any application. Such implicit trust policies have no boundaries and reduce visibility across the network, especially into encrypted paths.

Hybrid mesh firewall approach

A fully integrated and unified security solution is the only way to ensure consistent, adaptable threat detection and response across today's hybrid IT architectures. A hybrid mesh firewall (HMF) enables converged networking and security across on-premises and cloud infrastructure with consistent policy enforcement and unified management. This unified security platform approach provides coordinated protection across every area of enterprise IT.

Zero-trust access

A zero-trust framework is one in which nothing and nobody is trusted until verified. This applies whether the user is within the campus or working remotely, as hybrid work leads to more fluid use of on-site and off-site work locations.

Security policies must be crafted to give users access to the applications they need and restrict access to those they do not. The best way to do this is by implementing zero-trust network access (ZTNA) to control application access within a zero-trust framework.

“...organizations must implement a ‘never trust, always verify’ zero-trust model that incorporates rigorous access controls across the distributed network so that users, devices, endpoints, clouds, and infrastructure are all protected.”[5]

IoT and OT devices

A modern smart campus often has numerous IoT devices that connect to what were traditionally thought of as OT environments. These devices can be so limited in their network capabilities that they are often considered known “holes” in a ZTNA plan. Look for solutions that can ensure the easy onboarding of headless devices and those that can offer virtual patching. Virtual patching allows security systems within the ecosystem to automatically implement compensating controls when they see IoT or OT devices that have known vulnerabilities.

Step 4: Ensure Unified Management

Using numerous consoles for managing networking and security brings many challenges and consumes a lot of resources that IT teams can’t afford to spare. It’s important to be able to manage the full network (security and all) as a unified whole. This simplifies time spent on management and gives a single source of truth for resolving matters within the network. This requires networking and security equipment that can integrate together into a common framework.

Handling legacy installations

In many situations, there will be older technology in the environment that can’t be replaced immediately as part of a complete network stack overhaul. In these cases, a solution must be found to give visibility into older technology while migrating to newer ones. This can be done with network monitoring tools or NAC tools, depending on the level of oversight needed. Network monitoring tools give holistic visibility into multivendor environments and can track performance of resources that IT doesn’t manage, such as SaaS services. Multivendor NAC solutions can ensure secure connections across equipment, allowing network rollouts to happen as time and budget allow.

Tips for Avoiding a Catastrophe

Avoid these common pitfalls to promote your network’s smooth deployment and operation.

- Never assume that you know what a building is constructed of. If necessary, do some light testing with an AP on a stick to ensure you catch walls with rebar, leaded glass, or other obstacles.
- Assume there will be new applications and needs in the next few years that will push the boundaries of your network, and plan accordingly.
- Design for capacity, not coverage, in most carpeted and public spaces.
- Verify switch power budgets and include overhead for new tech.
- Pay careful attention to where applications reside (on-premises, in the data center, in a public or private cloud, or SaaS-based) and plan WAN connectivity accordingly.
- Understand all the IoT and OT devices in the installation and plan how they will be secured.
- Consider management ease during the vendor selection process, not after the fact.
- Ensure that security is layered throughout the design and look for solutions that can converge networking and security within a common framework.

Summary

The campus network continues to become more complex, so when planning a network or network refresh, IT teams must take into account several factors, including the physical environment, user locations and devices, and the applications they will use. But perhaps most importantly, security and management cannot be afterthoughts. By following the steps in this ebook, you can ensure secure connectivity with an easy-to-manage network that will accommodate your needs now and in the future.

[1] Lawrence Miller, "Zero Trust Access for Dummies," Wiley, 2022.

[2] Jonathan Nguyen-Duy, "How to Secure Your Edges Without Inhibiting Productivity," Fortinet, May 5, 2022.

[3] "Securing Wireless Networks," Cybersecurity & Infrastructure Security Agency, accessed September 5, 2023.

[4] Nirav Shah, "Using a Hybrid Mesh Firewall to Increase Network Security," Fortinet, August 4, 2023.

[5] Lawrence Miller, "Zero Trust Access for Dummies," Wiley, 2022.

FORTINET

www.fortinet.com

September 14, 2023 4:14 PM

2327553-0-0-EN