Creating a Secure Network with IoT

FORTINET

Table of Contents

POINT OF VIEW

Digital Acceleration Requires Converged Security and Networking

Executive Summary

Today's businesses are under pressure to establish and maintain market differentiation by improving processes faster than competitors and delivering higher efficiency, while increasing stakeholder value. Digital acceleration is necessary to achieve these objectives. It enables organizations to roll out new products and services at the speed business requires, while delivering the optimal experience for all types of users.

For digital acceleration to succeed, however, networks must do more than they did in the past—often much more than they were originally designed to do. Pushing networks beyond their limits generally results in increased risk of network downtime and security breaches.

That's why a new approach is needed that converges networking and security into a single solution. Secure networking minimizes risk while enabling the key functions that digital acceleration requires in order to meet business goals.

"When asked about the biggest challenges to digital transformation, the top responses include: cybersecurity (37% of respondents), data interoperability (29%), and legacy technology (22%)."[2]

Increasing Demands on the Network

Digital acceleration brings many benefits, but it also negatively impacts the network, which is being asked to take on more roles than ever before.

Organizations add solutions to improve business agility, but those applications are not all structured the same way or hosted in the same location. They may be available only to those on the corporate network or available to everyone, and they may be hosted in a public or private cloud, or on-premises. This variance creates complexity for IT, and an increased risk of mis-applying permissions or security settings for these applications.

In conjunction with this, the workforce is becoming more mobile and moves between locations far more fluidly than in the past. This hybrid workforce still needs constant, secure access to resources both inside and outside the corporate network. This mobility brings more security and network access challenges than on-site workers created in the past.

Another new development is the installation of automated control systems in buildings, such as air conditioning and lighting. These systems often leverage Internet-of-Things (IoT) devices with various capabilities and security postures that are spread throughout the site. In some cases, these IoT and system footprints can start to blur the previously established lines so much that they cause challenges that were previously limited to operational technology (OT) installations beyond the carpeted space.

Compounded Risk

A key downside to digital acceleration is the increased risk to the network. Oftentimes when IT teams are moving fast, security comes as an afterthought.

Cybersecurity risk from digital acceleration comes from several factors:

Network downtime is a common occurrence, whether it stems from an attack or just something complicated going wrong with the infrastructure. This can easily happen with digital acceleration, as quite often, disparate systems are not adequately tested with one another, leading to an interoperability issue. Network downtime brings digital acceleration technologies to a screeching halt, greatly impacting productivity.

Complexity of the overall system increases as more and more new applications and technologies come online, making it difficult to maintain effective security. This increases risk to any digital acceleration initiative as there often isn't time to go back and secure everything. These insecure networks are vulnerable to attacks and data loss. IT needs the ability to set policy centrally and reliably push it to all corners of the network so settings don't drift and leave security gaps.

Internet-of-Things devices are being added in campus environments to control systems that in the past were primarily seen in only in OT deployments. These devices are notorious for their lack of security. And in situations like this, any risk to the network can also become a risk to personal comfort and (in extreme cases) personal safety.

On a more individual level, the IT team is responsible for keeping up with all these changes. If anything is missed or problems arise, jobs could be at stake. There is a level of professional risk that IT teams should be aware of as well.

Benefits of Secure Networking

By bringing together networking and security equipment in a converged solution in a hybrid mesh firewall (HMF) environment, secure networking creates unmatched efficiency and closes security gaps. Only secure networking can solve the challenges brought by digital acceleration's rapid expansion of attack surfaces, creation of new edges, and remote access requirements, while delivering a better user experience. An HMF environment:

- Provides more effective security
- Eases management of networking and security with unified management and policies
- Reduces the chances for misconfiguration
- Eliminates confusing licenses and subscriptions
- Leverages artificial intelligence (AI)-based insights
- Lowers total cost of ownership (TCO)

With secure networking, IT groups can reduce the risk to their networks by installing an intuitive architecture that includes the necessary security and management features in one centrally managed solution.

[1] "Accelerating digital: a win-win-win for customer experience, the environment, and business growth," The Economist, 2022.

[2] Ibid.

1950331-A-0-EN

CHECKLIST

5 Key IoT Capabilities to Look for in a Networking Solution

Organizations are increasingly relying on Internet-of-Things (IoT) devices to achieve business goals. Unfortunately, these devices are inherently insecure and often targeted by cybercriminals to gain entry into the network and launch attacks. As IoT devices become more important and pervasive, they must be secured.

To get the most benefit from IoT devices while minimizing their risks, you need to ensure your networking equipment has the following capabilities:

☑ **Visibility and Device Details**

You need to know more than the number and type of devices on your network. Look for solutions that can provide complete information about the manufacturer, the firmware, and known vulnerabilities for each device. This is critical to maintaining a well-functioning network.

☑ **Easy IoT Onboarding**

Joining the network may be easy for users but is often challenging for headless IoT devices. Without a user behind a device making network choices or logging in, it can be difficult for the network to place these devices in the correct security posture. Often, this is solved by network access control software that can recognize devices as they attach and configure network security settings accordingly.

☑ **Protection**

Protecting IoT devices can be problematic. IoT devices are often embedded in the network in a way that makes immediate software updates to get the latest security patches problematic. But, leaving a known vulnerability in the network is very risky. Technologies such as virtual patching can implement compensating controls over the top of devices with known vulnerabilities.

☑ **Quarantine**

Ideally, the onboarding and protection methods mentioned above will be able to keep a device from being compromised, but it's not always enough. Your solution should be able to quarantine a device into a walled garden if it becomes infected.

☑ **Automation**

With so many IoT devices in today's networks, it's crucial to automate onboarding, protection, and quarantine capabilities to reduce overhead for the IT group.

IoT devices will only continue to grow their footprint in modern networks. To mitigate the risk, any network solution must include full visibility, onboarding, protection, quarantine, and automation capabilities. IT groups can avoid being overwhelmed by IoT by deploying secure networking equipment capable of these features. Learn more about the Fortinet LAN Edge solution.

Ensure a Secure LAN Edge for All Devices

Executive Overview

The rapid growth of personal and Internet-of-Things (IoT) devices connecting to enterprise networks has increased the need for fine-grained control over what is allowed into the network and with what permissions. Network access control (NAC) solutions can ensure that only devices that should attach to the network do so and can restrict what they have access to. But many of these solutions are just as complex as the problem they are trying to solve. Ideally, NAC would be streamlined and included with the local area network (LAN) edge solution for simplicity and consistent security policy.

Fortinet has an innovative solution that enables secure onboarding of myriad devices without the complexity. This ebook covers why this is needed and how FortiLink provides this functionality.

Challenges of Ensuring a Secure LAN Edge

Onboarding devices and securing the network are often at odds. What's needed is a quick and easy method for those entering the network, but that isn't always achievable following security best practices. Network complexity is rising, but no single source can easily address it. Complexity increases for a variety of reasons, such as:

- Work-from-anywhere initiatives that result in more bring-your-own-device (BYOD) items entering the network
- On-site guests
- IoT devices

IT teams must handle large volumes of different types of devices connecting to the network, which comes with a lot more exposure than they'd like. Getting all these devices safely onto the network is more challenging since they are not all the same.

Company-owned employee devices can be trusted once they go through rigorous checks, and the endpoint state plus RADIUS or AD authentication would give that device full entry.

BYOD devices, however, require different security and access. There's still user login available, but less direct control of the devices.

IoT is even more challenging, with headless devices with limited security functionality. They won't be able to log in with a username and password, and they're notoriously easy to hack and compromise. It's extremely risky to give them access to the entire network.

The network needs a way to set the security posture of each device to the correct level at the time of connection without making the network needlessly complicated for IT or end-users. There is no need for additional wireless networks or dedicated air-gapped wired networks just to handle these devices. Users should not need to find the right SSID, go through complex captive portal arrangements, or take other complicated steps.

Historically, this is where NAC has come into play.

Effectively Gating Network Access

To ensure the network is well-protected, organizations need a solution able to scale with and handle challenges. This requires functionality that can understand what to do with a wide variety of disparate devices. This is where NAC software solutions traditionally added value. They could monitor each device entering the network and ensure that it was given the correct levels of access and permissions.

NAC solutions can encompass a large array of features and functionality, and in many cases, they offer a wider solution set than necessary to solve the access problems of most network administrators. It's understandable how this happened, as NAC providers see a need to cover each and every situation that has arisen over time. Unfortunately, this leads to complex solutions that can be costly in terms of money and the time needed to set up and manage them. Often this leads to vendor lock-in as just the thought of abandoning all the work put into finally making a solution functional to then start over is very unpleasant.

The ideal way to solve this overwhelming problem is to have basic NAC services baked into the LAN that are simple enough to not add complexity and robust enough to cover the required set of use cases.

Simple and Secure Network Access from Fortinet

Securing edges throughout the network is key to a secure enterprise. The Fortinet Security Fabric enables IT professionals to accelerate digital rollouts without hitting security roadblocks. Creating a secure LAN edge is important in increasing IT's agility to support these initiatives. An effective and efficient network access control is key to achieving a secure LAN edge.

Covering the basics with FortiLink NAC

Fortinet Secure LAN converges security and networking, in this case, to best solve the issues of network administrators needing to securely onboard devices throughout their deployment. Fortinet includes base NAC features on the FortiGate Next-Generation Firewall (NGFW) that can be used with Fortinet LAN equipment (switching and wireless). The feature is called FortiLink NAC, as the technology that converges and controls our LAN equipment with the FortiGate is called FortiLink. All Fortinet LAN Edge equipment, FortiSwitch Ethernet switches, and FortiAP Wi-Fi Access Points (APs) utilize FortiLink to extend firewall policies throughout the LAN.

What is FortiLink NAC?

FortiLink NAC is a rules-based NAC system that allows for automated onboarding of devices onto the LAN.It ensures that they are placed in the proper security context. By leveraging the consolidated security and networking controls in the FortiGate NGFW appliance, it performs NAC services for LAN devices as they attach.

How does FortiLink NAC work?

FortiLink NAC uses a set of prioritized user-configurable rules to determine what to do with a device when it attaches to the network (whether by wire or wirelessly). It places all incoming devices into an onboarding virtual LAN (VLAN) while it processes the correct posture for the device. This ensures that no traffic is passed to the wider network until the correct posture has been set.

NAC rule options

Within the FortiLink NAC system, rules can be set based on device properties (device manufacturer, operating system, and more), user groups, or EMS tags, and then the device is assigned to specific VLANs. VLAN sub-interfaces are based on interfaces that are used for the VLAN assignment.

Special considerations for IoT

As noted, IoT devices offer a special challenge for network administrators, and it's no different for a NAC system. New devices are introduced regularly. Fortinet offers an IoT service for the FortiGate that keeps a regularly updated list of devices. This service is leveraged with FortiLink NAC to offer the best functionality for NAC rules.

Going Beyond the Basics with FortiNAC

While FortiLink NAC covers the needs of an average deployment, it is not intended for complex or multivendor environments. This is where our FortiNAC offering shines. It offers support for over 2,000 different switch and access point models across a variety of vendors, as well as anomaly detection and MAC spoofing, endpoint compliance scans, and a self-remediation portal.

Conclusion

As we continue to work from anywhere, time spent on professional and personal devices becomes more fluid, and IT teams need to support more access from more BYODs. At the same time, IoT in the workplace is increasing.

The good news is that organizations can count on FortiLink NAC to deliver network access control with no expensive investment or complicated deployment and management.

1375033-B-0-EN

August 7, 2024 1:15 PM / 2806672-0-0-EN