FORTINET

POINT OF VIEW

How to Achieve True Secure Connectivity: Don't Be Fooled by False Claims

Executive Summary

As networks continue to increase in complexity, integrating security becomes even more important. Network architecture must include security at its core and throughout its design. A modern LAN can only truly be secure for all users if it includes firewalling, IPS, antivirus, application control, URL filtering, and network access control (NAC). At the same time, key convergence points need to be considered on the administrative side. Otherwise, configuration may drift, making management of the network and security pieces too complicated and visibility sorely lacking. With a secure connectivity approach, key networking and security components are fully integrated and managed via one operating system, ensuring end-to-end consistency and visibility. Many networking vendors falsely claim they can do this, so knowing what to look for is important.

Because of the distributed nature of IT environments, the network is now playing a bigger role in securely connecting the enterprise.[1]

Introduction

A modern LAN network is more than just switches and access points (APs). The LAN needs deep integration with security mechanisms to ensure it continues to operate efficiently and supports key business initiatives. The goal when architecting a network is to ensure it can deliver necessary business outcomes. However, if security is not tightly integrated, the network will unlikely run smoothly for very long.

With many different aspects of the network at play, it's key that all these pieces can communicate and stay in sync. An efficient, easy-to-manage, and secure LAN is only possible with a converged networking and security solution. Using one platform for both functions enables consistency and automation throughout the network infrastructure. It also helps to ensure that security settings for the network equipment are harmonized with the security settings of the larger environment.

Firewalling

At the core of network segmentation typically sits an internal segmentation firewall. Used to control either north-south or east-west traffic, an effective internal segmentation firewall will ensure that both macrosegmentation and microsegmentation of the network are achieved.

A next-generation firewall (NGFW) platform performs these functions and additional security services. It is a protective barrier between your internal network and external, potentially untrusted networks such as the internet. Its primary purpose is to monitor and control incoming and outgoing network traffic based on predefined security rules, preventing unauthorized access and safeguarding sensitive data. When building connectivity, Ethernet and Wi-Fi equipment must operate seamlessly with the firewall and harmonize their security settings with it. Firewalls operate by inspecting data packets as they traverse the network, so make sure that your firewall can operate at line rate with the traffic in your network, even with all security settings turned on.

“As organizations build out a distributed IT infrastructure, applications, and user environments, it is critical that they have end-to-end visibility of the IT environment and eliminate any blind spots.…”[2]

Key capabilities of your NGFW should include:

Intrusion prevention system

An intrusion prevention system (IPS) safeguards the network from unauthorized access and malicious activities. IPS detects and blocks known and suspected threats before they can reach the core of your network or other devices at the edge. An advanced security layer that operates proactively to detect and mitigate potential threats, it ensures the overall integrity and confidentiality of data. IPS systems can also provide virtual patching, which protects vulnerabilities at the network level. This is especially critical for networks in which endpoint firmware and software updates are rarely performed.

Antivirus and anti-malware

Using a combination of signature- and behavior-based detection methods, antivirus and anti-malware controls detect, prevent, and remove various forms of malware. These include viruses, worms, Trojans, spyware, adware, and ransomware. Signature-based detection relies on a vast database of known malware signatures, comparing files and processes against these signatures to identify threats. On the other hand, behavior-based detection focuses on monitoring the behavior of programs and processes for unusual or malicious activities, even if the malware is previously unknown. Watching for signs of malware as it traverses the network can ensure that problems are contained before they become a threat to the operation of the network.

Application control

Application control is a must-have to achieve the desired business outcomes from a network. It lets you manage, control, and prioritize the use of specific applications and services with granular control over what applications can be accessed and how. Further, it helps enhance network security, optimize bandwidth utilization, and enforce compliance with company policies. By implementing application control, you can mitigate security risks posed by potentially harmful threats or actions, such as malware, unauthorized file transfers, or data leakage. Additionally, it prioritizes critical business applications, ensuring these apps receive sufficient network resources and performance. Given the rise of encrypted traffic, it’s important that an application control system incorporate deep packet inspection with packet decrypt and behavioral analysis techniques to accurately identify applications and manage their traffic.

Web filtering

Threats to the network’s availability and serviceability can come from various sources. To maintain compliance, web filtering manages and controls internet access to avoid web-based threats and in some industries and environments. It enables administrators to regulate the content and websites that users can access, creating a safer and more productive online environment. By using web filtering, organizations can enforce acceptable-use policies, enhance network security, and protect users from potentially harmful or inappropriate online content. Administrators can then apply policies to allow or block access to specific categories or individual websites. Additionally, web filtering systems often use real-time analysis and reputation databases to identify and block access to websites hosting malware and phishing attempts.

Network access control

Network access control (NAC) is a comprehensive security solution that governs and manages access to the network, ensuring that only authorized and compliant devices gain entry. NAC solutions identify and authenticate devices attempting to connect to the network. This can involve various factors, including user credentials, device type, security posture, and compliance with predefined policies. Devices that meet the specified criteria are granted appropriate access privileges, while those that fail to comply may be quarantined, redirected to a remediation network, or denied access altogether. NAC has particular value in network environments with IoT and OT devices, as they can present onboarding challenges.

Summary: Bringing It All Together

We ask our networks to do quite a lot, and adopting a secure connectivity approach will help ensure they can continue providing the business outcomes the company needs. The various security measures described in this paper should be part of a centralized solution that gives administrators the ability to easily deploy, configure, and manage all security, along with Ethernet and Wi-Fi equipment, from a common dashboard. As all these mechanisms are intended to protect the network, it's important that switches and APs are part of this platform and not adjacent to it. Be sure to look for networking equipment that operates as part of a larger solution that can provide all these aspects within a common framework, giving IT the power to deliver on corporate needs without creating visibility gaps or a management nightmare.

If a vendor claims it can do all of this but does not have a unified security and networking solution running on one operating system that can be managed with one console, be sure to do more research.

[1] Bob Laliberte, "The Importance of Network Visibility and Analytics and Zero Trust Initiatives," Enterprise Strategy Group, February 2023.

[2] Ibid.

FORTINET

www.fortinet.com

September 19, 2023 4:10 PM

2327518-0-0-EN