Staying Ahead of Cyberthreats: Leveraging the Power of Secure Networking

Executive Overview

While digital acceleration delivers many benefits, such as reduced costs, faster growth, and better user experience, it has also led to a rapid expansion of attack surfaces and new network edges. These include the local area network (LAN), the wide area network (WAN), 5G, remote workers, and clouds.

The overarching challenge of digital acceleration is that rapid IT changes often result in new vulnerabilities, which are outpacing the security team's ability to protect them from cyberthreats.

Networks today are the center of innovation and enable digital acceleration using network modernization. Adopting a secure networking strategy helps fortify organizations so they can be safe and successful in their digital acceleration efforts.

Components to Achieve Secure Digital Acceleration

A modern enterprise network needs solutions spanning three areas to achieve robust, secure networking: robust security at the edges and for remote users, innovative networking solutions that can adapt to evolving business demands, and a unified and simplified network operations solution to address issues before they become a disruption.

Hybrid mesh firewall architecture: unified security and management across the organization

Today's cybercriminals exploit the lack of consistent security and visibility across various distributed network segments found in most enterprises. Because data centers, campuses, multi-cloud, and branch environments are now interconnected, east-west traffic across the network has increased. This allows a successful breach in one area of the network to quickly spread to others. The most effective way to address this challenge is to deploy consistent security in every part of the network—but differences between various network ecosystems have made that difficult.

Hybrid mesh firewalls (HMFs) are designed to consistently integrate critical next-generation firewall (NGFW) features across your network, including campus, data center, and public and private cloud environments, as well as Firewall-as-a-Service and secure access service edge (SASE) to secure remote users and locations—all run under a centralized and cohesive management solution. This approach creates a single, integrated platform that spans, scales, and adapts to today's dynamic and distributed networks. An HMF approach coordinates protection across IT domains (corporate sites, public and private clouds, and remote workers) from a unified management console. This integration allows IT teams to automate threat detection and response, orchestrate configurations, and enforce policies without investing needless manual hours, especially when the cybersecurity skills gap is already constraining resources.

Security for Edges and Users

Powerful next-generation firewalls

Next-generation firewalls, especially HMF solutions, are essential for modern enterprises needing to secure their increasing attack surface driven by the growth in network edges. But today's advanced firewalls must also utilize artificial intelligence (AI) and machine learning (ML) to enhance threat intelligence and accelerate the prevention, detection, and response to various attacks, including zero-day attacks, APTs, and unknown threats.

And with the majority of internet traffic being encrypted, these firewalls must also be able to inspect encrypted traffic without performance loss, especially as users rely on latency-sensitive business applications. To ensure robust automated protection, they must provide comprehensive visibility and threat detection, even through SSL/Transport Layer Security (TLS 1.3) encrypted traffic. They must also be optimized for flexibility, enabling them to be deployed consistently across various enterprise environments, including distributed branches, campuses, data centers, and cloud infrastructures, supporting a unified, holistic security posture.

In addition to proven security controls, a cutting-edge NGFW should encompass:

1. **Unified management:** Integration of on-site and cloud security under a single HMF system for streamlined operations
2. **Dynamic segmentation:** Adaptive structuring to safeguard essential applications and user groups through dynamic segmentation of the network
3. **Embedded access control:** Real-time validation of user and device access to maintain continuous security integrity
4. **Microsegmentation:** Detailed oversight and defense mechanisms tailored to specific applications and data flows to enhance security within network segments

Encrypted traffic has hit 95%.[2]

Cloud-delivered SASE for hybrid work security

Over the past several years, organizations have been expanding their multi-edge networking strategies to enable new work-from-anywhere (WFA) realities and support workers as they become increasingly dependent on cloud applications and environments to do their jobs. However, as these networks grow to meet new business demands, the attack surface increases. The result is a growing gap between network functionality and security coverage that inherently exposes organizations to more points of compromise and degrades the user experience of those remote workers who still rely on the conventional, virtual private network (VPN)-only solutions to access the network. This is usually because all their application traffic still needs to be backhauled through the network to receive security protections and access controls. Secure access service edge solutions have been developed to address these issues, enabling organizations to rapidly converge and scale out their security and networking strategies. With SASE, they can securely deliver an expanding and dynamic set of new network edges as well as meet the new demands of a hybrid workforce distributed between on- and off-network users.

An efficient SASE solution provides:

- **A single-vendor SASE architecture:** SASE is designed to deliver secure, cloud-based connectivity. However, very few enterprise networks are cloud-only. Even though many enterprises have a multi-cloud strategy, most still have physical networks. This means that cloud-only security is, by definition, incomplete security. Organizations need to insist on SASE services that are integrated with—or can be deployed as a seamless extension of—the extended network, including SD-WAN security. This is called the single-vendor SASE approach.
- **Enterprise-grade security everywhere:** When assessing any SASE solution, the functionality and performance of its security elements need to be effective. The SASE solution should include components that fully secure all applications and edges and provide secure access to the internet, SaaS applications, and corporate applications, wherever they are located.
- **Seamless convergence between networking and security with unified tools:** Legacy equipment is here to stay. SASE integration with on-premises solutions is essential for streamlined operations and to facilitate change. Seamless integration between on-premises security (SD-WAN and NGFW) and cloud security is key for operations simplification, compliance requirements, and consistent security posture among all users. A SASE solution also extends the convergence of networking and security from the network edge to remote users with unified management, a unified agent, and digital experience monitoring (DEM) for streamlined operations.

Fortinet Secure Networking

Fortinet has an innovative approach to securing digital acceleration with the convergence of enterprise-class security and networking. This unique platform approach ensures secure access to critical applications and resources, whether users are on-premises or accessing resources remotely. Our secure networking approach, including our unique combination of purpose-built ASICs, a universal operating system (FortiOS), cloud-delivered security solutions, and integrated networking equipment, enables superior user experience combined with coordinated threat protection for every network edge.

With FortiOS at its core, Fortinet Secure Networking tackles one of the most persistent challenges facing today's IT teams: extending enterprise-grade security and granular access control throughout the network and at all levels, from campus to branch to remote workers. Fortinet's solution solves user experience, point networking and security technology, and implicit trust challenges that create obstacles for organizations undergoing digital acceleration.

[1] "Gartner Says 89% of Board Directors Say Digital is Embedded in All Business Growth Strategies," Gartner, October 19, 2023.

[2] "HTTPS encryption on the web," Google Transparency Report, accessed May 22, 2023.

[3] Scott Anderson, "Is Your Network Operations Center Outdated? Here's What You Need to Know," LinkedIn, March 28, 2023

[4] Rahul Awati, "What is a network operations center (NOC)?" TechTarget, accessed January 26, 2023.

FORTINET

January 4, 2024 12:35 PM

1934260-B-0-EN