POINT OF VIEW

Seven Major Challenges Facing Today's Hybrid Networks

Introduction

Speed and availability are essential in today's digital marketplace, while business demands and processes are rapidly evolving. Many organizations have traded their legacy systems for hybrid networks and digital processes to remain competitive, including cloud and business application adoption. And the resulting transformation of their networks—the most significant in 40 years—has been wildly successful in terms of customer satisfaction and user productivity, empowering them to compete more effectively in today's digital marketplace.

Meeting today's digital acceleration drivers enables organizations to roll out new products and services faster, streamline time to market, optimize user experience, and meet evolving customer expectations. The ongoing objective is establishing and maintaining market differentiation by improving processes faster than competitors, allowing organizations to improve efficiency through innovation.

However, building the processes and systems that will help organizations do more faster is more complicated than it sounds. It starts by converging traditionally separate network systems to create highly efficient hybrid environments. This includes:

- Seamlessly tying physical campus and data center networks to private and public cloud environments
- Interconnecting branch offices
- Providing ubiquitous access to the rapidly growing number of remote users

Hybrid dynamic environments allow IT teams to create fast lanes for building, implementing, interconnecting, and managing critical technologies and processes, whether internal or external. They also introduce new risks that legacy security systems cannot address because they cannot adapt to a network in a constant state of flux. Because of this fundamental change in networking, security systems can no longer be designed using isolated point products deployed as a network overlay. Instead, just as different network environments need to converge, so do networking and security so they can operate as a single, responsive system.

To achieve this, organizations must overcome several challenges.

IT Has Evolved

Implementing digital innovation requires traditional IT to evolve. Static perimeters and fixed resources, the building blocks of conventional networks, have been disrupted with new applications and services. Users require greater access to critical information regardless of their device or location. Modern network architectures must interconnect traditionally fixed network environments such as campuses, data centers, and branches—and then seamlessly integrate with multi-cloud networks and their expanded hybrid workforce. By combining physical and virtual networks across private and public domains, these new hybrid networks offer true scale-on-demand capabilities to meet and protect escalating business needs end to end.

Seven Major Challenges That Can Impede Digital Acceleration

The accelerated transition to converged hybrid networks has stretched legacy security to the breaking point. Most traditional security systems, built around best-of-breed point solutions, were designed to analyze and secure predictable data at fixed points in the network. And because most network products were not designed with security in mind, these security systems operate as an overlay, almost entirely disconnected from the network it defends. So, when new networks rely on legacy security systems, gaps are created that cybercriminals are eager to exploit.

To secure your new hybrid network, there are seven critical issues you must first understand and address:

1. **Expanding attack surface:** Hybrid networks and a diverse workforce mean your network has more locations, applications, and services to protect. The solution sprawl resulting from deploying new security technologies every time another service or network segment is added has overwhelmed many IT teams—especially those coping with the ongoing cybersecurity skills gap. The challenge is to consolidate your security infrastructure while creating a security system that can span and adapt to the demands of your new hybrid network.
2. **Attacks targeting security gaps:** Today's threats target multiple points across today's distributed networks looking for the weakest link in the security chain. And once in, they exploit the lack of internal segmentation and security to spread from one area of the network to another. For example, new Internet-of-Things (IoT) and Industrial-Internet-of-Things (IIoT)-based attacks designed to target operational technology (OT) Industry 4.0, including artificial intelligence (AI) for robotics control, near-real-time digital twins, and production line automation, often enter production environments through another part of the network that is less secure.
3. **Inconsistent enforcement:** While users, devices, and applications can be anywhere, not all security solutions can say the same. And when security solutions and platforms cannot be universally deployed or centrally managed and orchestrated, it can be impossible to deliver consistent and location-agnostic security across the hybrid network. This is especially true for workflows that move between environments. End-to-end security becomes impossible when policies and enforcement are inconsistently enforced because there is no way to seamlessly hand off traffic between disparate security devices.
4. **Growing volumes of encrypted traffic:** Legacy security solutions do not have the bandwidth necessary to inspect today's high volumes of encrypted traffic without seriously impacting network performance and user experience. As a result, many IT teams are trying to combat today's threats while blindfolded. Cybercriminals exploit this known issue by targeting less secure remote and home offices and then transporting their malware into the organization through encrypted VPN tunnels they know will not be inspected.
5. **Complexity:** Given the speed of today's attacks, automated detection and response if essential. But automation is impossible with dozens of point security solutions deployed across the network. Instead, IT teams must rely on hand-correlating threat intelligence with network information to detect and respond to threats, which means things get missed, and responses are too late. And worse, today's multivector attacks exploit the inability of networking and security solutions to share and correlate threat data.
6. **Lack of integration and coordination:** The challenge goes beyond disparate security systems that do not share information. In most networks, on-premises applications and physical infrastructures also struggle to coordinate and communicate with cloud applications and networks—even though applications and workflows increasingly span multiple environments. As a result, if one gets attacked, there is no integrated mechanism to notify the other, let alone initiate appropriate protections across the network.

7. **Work from anywhere:** Most organizations, especially larger enterprises, now support a hybrid workforce. These mobile workers need seamless access to private applications in a data center or multi-cloud environment and Software-as-a-Service (SaaS) applications deployed through the cloud. Organizations must find ways to ensure consistent and secure access to all critical business resources, regardless of where employees or applications are located.

Digital Acceleration Benefits from a Hybrid Mesh Firewall Approach

Protecting today's networks requires an integrated approach to security. That starts with a hybrid mesh firewall (HMF), which converges on-premises and cloud-native deployments through unified management. It's a unified security platform that provides coordinated protection across enterprise IT, including corporate sites, branches, campuses, data centers, public and private clouds, and remote workers. And the Fortinet Security Fabric approach extends this unified management and analytics approach across our entire secure networking portfolio, resulting in unified visibility and protection against security threats. An HMF solution simplifies operations, ensures compliance, and reduces complexity with automation, increasing operational efficiency and time to respond. And it doesn't matter if you have all on-premises firewalls, all cloud firewalls, or a mix of both. The value is in having centralized and unified management across firewall deployments that can expand and adapt as your hybrid network strategy evolves.

June 12, 2023 6:39 PM

2167233-0-0-EN