CHECKLIST

Top 6 Recommendations to Improve User Productivity with a Hybrid Architecture

The speed of business is accelerating the data center's journey toward digital transformation, requiring new hybrid network architectures that combine on-premises data centers with multiple public and private cloud deployments to form a hybrid mesh firewall (HMF) environment. However, to meet the needs of organizations expanding their digital transformation, the underlying enabling technologies must be more reliable and energy-efficient. They must also deliver consistent security across the hybrid architecture to defend against threats.

On-premises and virtual data centers are vital in today's ever-evolving network. In this new model, security is essential to protect resources and assets and to enable the network to accelerate and adapt without introducing unknown risks that can jeopardize the enterprise.

6 Things Organizations Need to do to Position Themselves for Success

☑ Invest in a Flexible Next-Generation Firewall

Organizations need to invest in a next-generation firewall that includes technologies like SD-WAN, Universal ZTNA, inline sandbox, and SOC-as-a-Service. These technologies improve WAN connectivity by providing better user experience with direct internet access, while LAN and WLAN provide faster access to local devices and users.

☑ Deploy Unified Networking and Security

Security can't be an afterthought. When security solutions are not well-integrated with each other or the underlying network, security risks and gaps arise as the attack surface expands and adapts. These blind spots are vulnerable to sophisticated multi-step attacks and are partly responsible for the dramatic rise in successful ransomware attacks. Hence, it is important to look for a unified security framework to deliver automated and reactive security that spans the HMF architecture for all firewall deployments to cover the entire attack surface. Organizations must also converge their security with networking to protect digital acceleration efforts

☑ Adopt a Secure-Networking Strategy

With new network edges being created on-premises and in the cloud, it is critical that the unified convergence of networking and security be available everywhere, combined with ZTNA to enable explicit access for applications and continuous verification of users and devices. This convergence is the heart of a secure networking strategy. Also, flexibility in providing this convergence is key in securing digital acceleration for hybrid deployments.

☑ Speed Operations with Centralized and Automated Management

The exponential growth of network edges, cloud platforms, and tools can significantly increase operational complexity. Furthermore, poor visibility and analytics gaps in the network along with tasks performed manually degrade the end-to-end digital experience.

These issues increase the time to configure, manage, and troubleshoot. They also add to operation costs and errors that can cause network outages and reduce flexibility. A hybrid mesh firewall architecture provides centralized and automated management to unify and deliver consistent security policies and network services across the organization. Removing manual configuration eliminates a major cause of downtime and security breaches.

Increase Visibility with End-to-End Digital Experience Monitoring

Traditional network performance monitoring, IT infrastructure monitoring, and application performance monitoring provide network operations center (NOC) teams with limited visibility. These types of monitoring don't provide the performance insights into critical business applications that organizations need. They also severely hinder the visibility that frontline NOC and help desk teams need to resolve issues.

A modern digital experience monitoring (DEM) platform is required to give your NOC team superior visibility. It allows for the observation of any application, starting from the end-user, across any network, and to the infrastructure the application is hosted on. It can enrich incident management and supply holistic remediation of performance issues to resolve problems before users are impacted.

Consolidate and Simplify Operations to Provide Instant ROI

Organizations adopting HMFs with unified management and integrated security achieve better ROI than those using point products with limited security. Secure networking also improves employee productivity with better user experience and simplified operations.

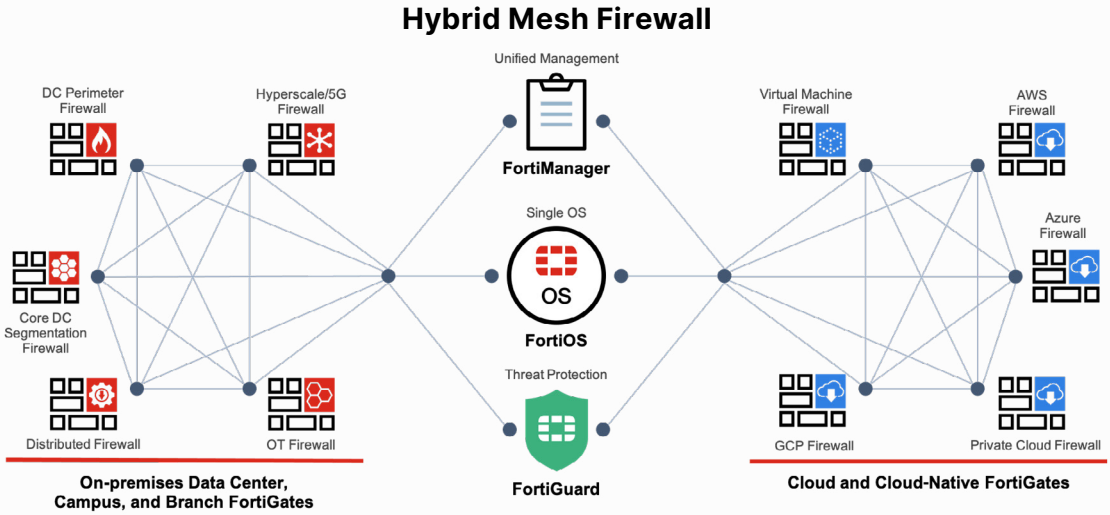

Figure 1: The Fortinet Hybrid Mesh Firewall solution

Conclusion

Many organizations still use a traditional architecture to connect offices to the data center for application access. However, with users working from anywhere and applications distributed across multi-cloud and SaaS environments, this legacy network design is an obstacle for digital acceleration and creates user experience challenges. Organizations that want to have better user productivity and secure network edges need to invest in a modern hybrid network architecture.

Fortinet is the only vendor in the industry to offer an NGFW that includes SD-WAN, Universal ZTNA, inline sandbox, and SOC-as-a-Service that can protect any edge at any scale. Offering the best convergence of networking and security, Fortinet empowers organizations to adopt modern networking technologies essential for digital acceleration. Learn more about Fortinet Secure Networking.

June 1, 2023 12:42 PM
1457355-B-0-EN