SOLUTION BRIEF

Enable Resilient, Seamless, Secure Networking for the Multi-cloud Enterprise With Fortinet Secure SD-WAN

Executive Summary

Almost every organization now operates in more than one cloud, and the number of people accessing those resources remotely skyrocketed in 2020. This creates both networking and security challenges as the attack surface increases, and traffic tends to get bogged down during security checks at the central data center. Fortinet Secure software-defined wide-area networking (SD-WAN) addresses these challenges by providing scalable, resilient connections between remote users, branches, the data center, and multiple public clouds. It enables a Security-Driven Networking strategy that improves both performance and security while reducing cost. Centralized management provides full visibility and control from a single console, and integration of all networking and security solutions improves both efficiency and security.

Fortinet Security-Driven Networking consolidates SD-WAN, NGFW, advanced routing, and ZTNA Access Proxy.

Multi-cloud Networking Based on Fortinet Secure SD-WAN

Virtually every organization now operates in multiple clouds,[1] and business-critical applications and data now reside outside what was formerly known as the network perimeter. Compounding this, network traffic patterns outside the data center changed significantly when millions of people found themselves newly working from home in 2020.[2] These are two central challenges these days when it comes to networking.

These trends also bring more complexity when it comes to security. Each new cloud service that is deployed—and every remote user that is added—expands the attack surface. But with a growing share of network traffic going between remote endpoints and various clouds, routing it all through the corporate data center for security screening creates more problems than it solves. The data center becomes a chokepoint that slows performance and results in packet loss. Worse yet, if remote-user traffic is routed first to a branch office and then to the data center via a multiprotocol label switching (MPLS) connection, that increases the number of hops to get to the final destination. This adds more latency and possible packet loss.

With our Security-Driven Networking approach, Fortinet Secure SD-WAN addresses these challenges by providing seamless, secure, scalable connections between headquarters, branch offices, remote users, and multiple clouds. Built into the FortiGate Next-Generation Firewall (NGFW), Fortinet Secure SD-WAN is a part of the Fortinet Security Fabric—a broad, integrated, and automated security platform that enables centralized visibility, control, monitoring, and threat response. The integrated solution enables a secure information freeway on which traffic moves efficiently and with minimal latency.

Remote Workers, Branch Offices, and Multiple Clouds: Connecting the Dots

Early adopters of SD-WAN were mainly concerned with providing scalable, cost-effective links between headquarters and branch locations. But the same technology can help organizations with cloud security and connectivity.

With Fortinet, SD-WAN gateways can be centrally managed and orchestrated, steer applications over policy-defined links, and automatically set up and maintain Internet Protocol security (IPsec) tunnels to and across public clouds. SD-WAN can help connect branch offices to cloud services, to workloads in different virtual networks on the same public/private cloud, and even connect workloads across hybrid and multiple public clouds.

The result is a scalable, resilient, high-performance network for all users. With Fortinet Secure SD-WAN, traffic originating in branch offices can be routed over existing MPLS links or the public internet—whichever is most efficient. Traffic from remote users can be routed via broadband, Long-Term Evolution (LTE), or 5G internet connections. And administrators can set policies to prioritize critical applications and time-sensitive functions such as Voice over Internet Protocol (VoIP) and videoconferencing.

FortiManager supports network and security operations with centralized management, best practices compliance, and workflow automation to provide for secure and efficient movement of network traffic.

Public Cloud as Transit: Forging New Routes

While most public cloud use cases focus on applications and workloads, public cloud providers have built out high-speed network backbones that customers can take advantage of to improve performance, security, and speed of provisioning. For instance, an organization that needs a high-performance, low-latency connection between two geographically separated branches could leverage a cloud provider's backbone as the transport mechanism.

Similarly, Fortinet Secure SD-WAN deployed in each branch and in the public cloud can be used to set up IPsec tunnels that will transit the cloud provider's backbone. This simplifies secure cloud connectivity for the enterprise while delivering superior application experience for end users. Fortinet currently supports seamless integration with Amazon Web Services (AWS) Transit Gateway, Microsoft Azure Virtual WAN, and Google Cloud Network Connectivity Center.

Centralized Management: Improved Efficiency and Better Security

FortiManager enables administrators to manage all their FortiGate virtual and physical NGFWs—on-premises and in the cloud—from a single console. This includes centralized management of all the functionalities of Fortinet Secure SD-WAN.

Networking and security administrators can use FortiManager to provision SD-WAN capabilities, set up IPsec virtual private networks (VPNs) and static routes, and set and monitor security policies for their physical and virtual gateways—all from a single console. Once the SD-WAN infrastructure is up and running, organizations can consult the same console to get visibility into application traffic and monitor the performance of the multi-cloud overlay powered by SD-WAN.

The global view provided by FortiManager is ideal for organizations managing hybrid cloud and multi-cloud tunnels because it provides a single view into connections that might be spread across many branches and among public clouds. FortiManager also backs up device configurations, can track configuration changes, and provides role-based access control (RBAC) to ensure network and security administrators have the appropriate level of visibility and control over changes.

Integration: An Enabler of Automation

The Fortinet Security Fabric integrates security capabilities across a variety of domains, including wired and wireless networks, endpoints, web applications, the cloud, and more. It encompasses an integrated suite of security tools from Fortinet and from Fabric Partners. This integration is enabled by FortiOS, a rich open ecosystem that underlies the overall solution.

The Fortinet Security Fabric enables organizations to correlate alarms and alerts, disseminate security intelligence across the infrastructure in real time, and gain greater context into incidents. The Fabric can also orchestrate threat response across domains: for instance, updating switch and access point (AP) policies to quarantine an endpoint while launching a malware scan on that device.

Consolidation and integration of the networking and security tools required for a security-driven SD-WAN solution eliminates the complexity of a disaggregated security architecture that operates in a separate silo from the networking function. This reduces the organization's attack surface while enabling digital innovation initiatives. At the same time, it simplifies operations for both networking and security teams, enabling an organization to assign its scarce human resources to more strategic initiatives.

The Secure and Scalable Multi-cloud Freeway

The deployment of SD-WAN in branch locations to enable public cloud access is well understood. As organizations embrace a multi-cloud strategy—by design or by default—they can extend their SD-WAN investment to support hybrid cloud and multi-cloud connections. This provides efficient routing of traffic between remote endpoints, branch locations, and headquarters employees and multiple cloud-based services.

By doing this, Fortinet Secure SD-WAN with our Security-Driven Networking approach, enables a seamless, scalable, and resilient multi-cloud freeway. And unlike with physical automobile infrastructure, traffic on this freeway is always free flowing. Centralized monitoring and management enable real-time adjustments and status updates. And Fortinet's unique Fabric approach enables the entire networking and security infrastructure to be natively integrated across on-premises, private cloud, and public cloud resources.

The Fortinet Security Fabric simplifies operations and enables faster response to threats.

[1] "Flexera 2021 State of the Cloud Report," Flexera, accessed September 5, 2021.

[2] Susan Lund, et al., "The future of work after COVID-19," McKinsey Global Institute, February 18, 2021.

FORTINET

www.fortinet.com

October 6, 2021 7:18 AM
1169920-0-0-EN