SOLUTION BRIEF

FortiGate Secure SD-WAN Delivers Dynamic Cloud Security for Microsoft Azure

Executive Summary

As customers effectively utilize a mix of Microsoft Azure cloud infrastructures and private cloud infrastructure, the need for secure and optimized connectivity from branch offices and other corporate locations to Azure increases. FortiGate Secure SD-WAN offers an ideal branch and corporate connectivity solution for customers looking to secure and optimize their cloud on-ramp requirements. Specifically, FortiGate Secure SD-WAN for Azure Virtual WAN helps ensure ease of use, security, quality of experience (QoE), and visibility across distributed infrastructures spanning on-premises locations and Azure regional data centers.

Rapid growth of digital innovation is driving more cloud, Voice over IP (VoIP), and video traffic to the branch network. Traditional WAN deployments cannot address these branch network constraints.

Supporting an Array of Cloud Connectivity Use Cases

FortiGate Secure SD-WAN for Microsoft Azure Virtual WAN extends application awareness, security, and QoE from branch locations to the cloud. Secure SD-WAN, which is powered by FortiGate next-generation firewalls (NGFWs), selects the ideal traffic path for each application while leveraging the Azure Virtual WAN global network. An application programming interface (API) helps enable rapid rollout and modifications of infrastructure and application availability. This approach supports multiple use cases:

1. **Branch-to-Azure Virtual WAN connectivity.** As organizations migrate applications to Azure or build native applications using Azure technology, security architects must provide secure and optimized access to these applications. The combination of an on-premises, branch-based FortiGate NGFW and Azure Virtual WAN connectivity provides both security and network resilience at the branch. This also offers a globally accessible infrastructure that is easy to connect to in the cloud—delivering the most secure, optimized connectivity solution for accessing Azure infrastructures, regardless of region or application.
2. **Secure branch-to-branch connectivity.** Customers with branches in different regions can use Azure Virtual WAN to ride on top of Microsoft infrastructure for better inter-branch connectivity, while relying on Fortinet to keep those connections secure. As organizations choose to place advanced security functionality in their cloud infrastructure, security architects need to ensure that secure connectivity between branches is possible from a routing standpoint. Indeed, using the cloud as a connectivity hub becomes a good option for enabling advanced connectivity without losing visibility to global traffic flows or critical security functionality.
3. **Dynamic path selection.** Utilizing multiple connection types from branches is the norm today—whether a mix of multiprotocol label switching (MPLS)/leased lines and Azure Express route connections and broadband internet or multiple broadband internet connections. To ensure reliable performance, regardless of the connection or application in use, organizations need resilience in their branch connectivity schemes. FortiGate Secure SD-WAN dynamically steers application traffic paths in order to select the connection that will provide the best possible user experience.
4. **Custom application awareness.** Application awareness helps network teams see which applications are being used across the enterprise, which enables them to make well-informed decisions regarding SD-WAN policies. And as organizations build custom applications or run off-the-shelf applications in different Azure regions, the need for intelligent and custom application steering policies increases. FortiGate Secure SD-WAN offers teams the ability to define specific application steering logic, which complements the variety of application placements and design decisions made for global deployments.

FortiGate Secure SD-WAN for Azure Virtual WAN

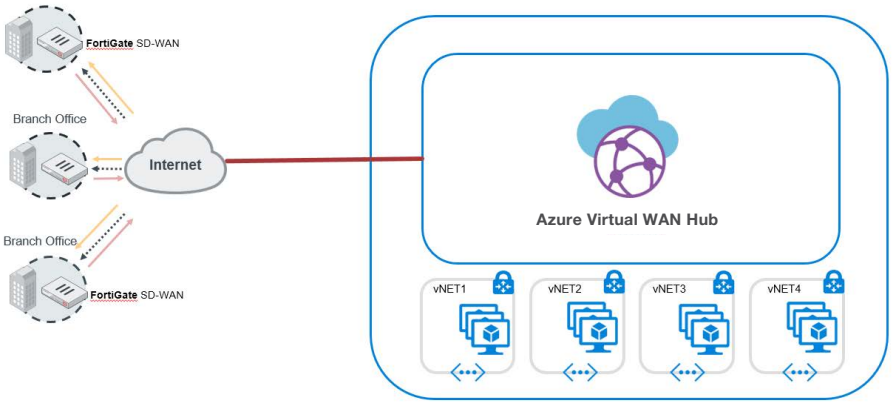

Figure 1: FortiGate Secure SD-WAN on-ramp for Azure Virtual WAN.

How FortiGate Secure SD-WAN Compliments Azure Virtual WAN

Integrated within a fully featured NGFW solution, FortiGate Secure SD-WAN offers the best-performing SD-WAN solution on the market. With respect to Azure Virtual WAN, FortiGate Secure SD-WAN delivers seamless cloud on-ramps with several critical benefits:

Reduced complexity. FortiGate Secure SD-WAN consolidates complex security and networking infrastructure. Automation and orchestration capabilities from both Fortinet and Microsoft reduce the burden on security architects and security staffs by eliminating manual workflows and simplifying operations—such as rollout of devices and creation of VPN tunnels.

Integrated security. Fortinet's unified approach to SD-WAN delivers enterprise-class security and branch networking capabilities within a single-box solution. Critical security features include secure sockets layer (SSL)/transport layer security (TLS) encryption inspection, web filtering, intrusion prevention (IPS), and artificial intelligence (AI)-powered threat intelligence.

Zero-touch deployment. FortiGate Secure SD-WAN uses FortiManager to bring a branch online in less than six minutes using zero-touch deployment capabilities. Organizations can also connect branch offices and applications running in Azure VNets with a single click of a button. Additionally, Fortinet's automation framework dynamically detects any newly added remote site and automatically connects it to the Azure vHub.

Single-pane-of-glass management. Centralized management allows security architects to manage policies and devices from a single console—while drastically reducing opportunities for configuration errors that lead to cyber-risk exposures. Enabling these capabilities, FortiManager can be leveraged to configure policies across all branch offices connected to Azure vHubs.

Compliance ready. Fortinet accelerates compliance management and reporting by simplifying infrastructure, improving visibility, and eliminating the need for many manual audit processes. FortiAnalyzer includes customizable regulatory templates as well as canned reports for multiple standards. It also provides audit logging and role-based access control (RBAC) to ensure that employees can only access the information they need to perform their jobs.

Optimized Connectivity to Azure-based Applications and Services

The combination of Microsoft Azure Virtual WAN and FortiGate Secure SD-WAN makes for a highly scalable solution across distributed organizations with multiple branch offices or remote locations. Microsoft Azure Virtual WAN simplifies the path to hybrid cloud migration for network leaders, while Fortinet helps simplify and secure dynamic cloud connectivity needs. By implementing this joint solution, organizations can achieve their desired secure connectivity with minimal operational overhead and while providing the best resilience and protection to ensure optimal productivity.

[1] Ahmed Basheer,"Software-Defined Wide Area Network Test Report: Fortinet FortiGate 61E," NSS Labs, June 19, 2019.

November 12, 2019 11:33 PM

499676-0-0-EN

D:\Fortinet\Solution Briefs\blue solution briefs\Network Leader MSFT\sb-FA-fortigate-secure-sd-wan-delivers-dynamic-cloud-security-for-microsoft-azure\sb-FA-fortigate-secure-sd-wan-delivers-dynamic-cloud-security-for-microsoft-azure