

## SOLUTION BRIEF

# Transform the Enterprise WAN with the Fortinet Security Fabric and Azure Virtual WAN

## Extend Your Fortinet Security Fabric to the Azure Cloud

### Executive Summary

Azure Virtual WAN is a Microsoft networking service that lets organizations simplify their global connectivity and benefit from the scale, speed, and resilience of the Microsoft global network. However, securing this global transit architecture requires state-of-the-art network security.

To achieve this, Microsoft offers the ability to simply and efficiently integrate Fortinet's industry-leading secure networking solutions with Azure Virtual WAN. Together, Fortinet and Microsoft enable the delivery of a converged security and connectivity platform that empowers digital agility and cyber resilience from edge to cloud.

### Transform the Enterprise WAN

Fortinet FortiGate for Azure Virtual WAN brings together Fortinet's next-generation firewall technology with Azure vWAN, ensuring secure networking through Microsoft's vWAN Hub.

### Optimize Performance and Resilience with Fortinet Secure SD-WAN

Combining FortiGate Next-Generation Firewall cybersecurity and SD-WAN, Fortinet provides a single logical SD-WAN and security overlay for Azure Virtual WAN traffic from edge to cloud.

Fortinet self-healing SD-WAN technology automatically directs traffic and optimizes flows across the Azure Virtual WAN global network in accordance with the specific needs of each application and the real-time performance of underlying connections.

### Secure the Azure vWAN Hub

Fortinet FortiGate secures SD-WAN traffic entering and leaving the Azure vWAN Hub and can secure east-west traffic traversing the vWAN. Unlike Azure's native security solutions, Fortinet provides advanced security functionality, including application awareness, data loss prevention, botnet protection, and more.

Fortinet FortiGate for Azure vWAN can be deployed through the Microsoft Commercial Marketplace and can be centrally managed using Fortinet FortiManager.



### Optimize Performance and Security for Azure Virtual WAN

Empower the modern, secure enterprise with Fortinet natively integrated solutions for Azure Virtual WAN.

- Achieve cost-effective, high-speed redundant global connectivity
- Secure north-south, east-west, and internet-bound traffic in Azure vWAN
- Orchestrate consistent network and security policies across clouds and data centers
- Gain deep analytics, central management, and self-healing of your network infrastructure
- Draw down your Microsoft Azure Consumption Commitment (MACC)



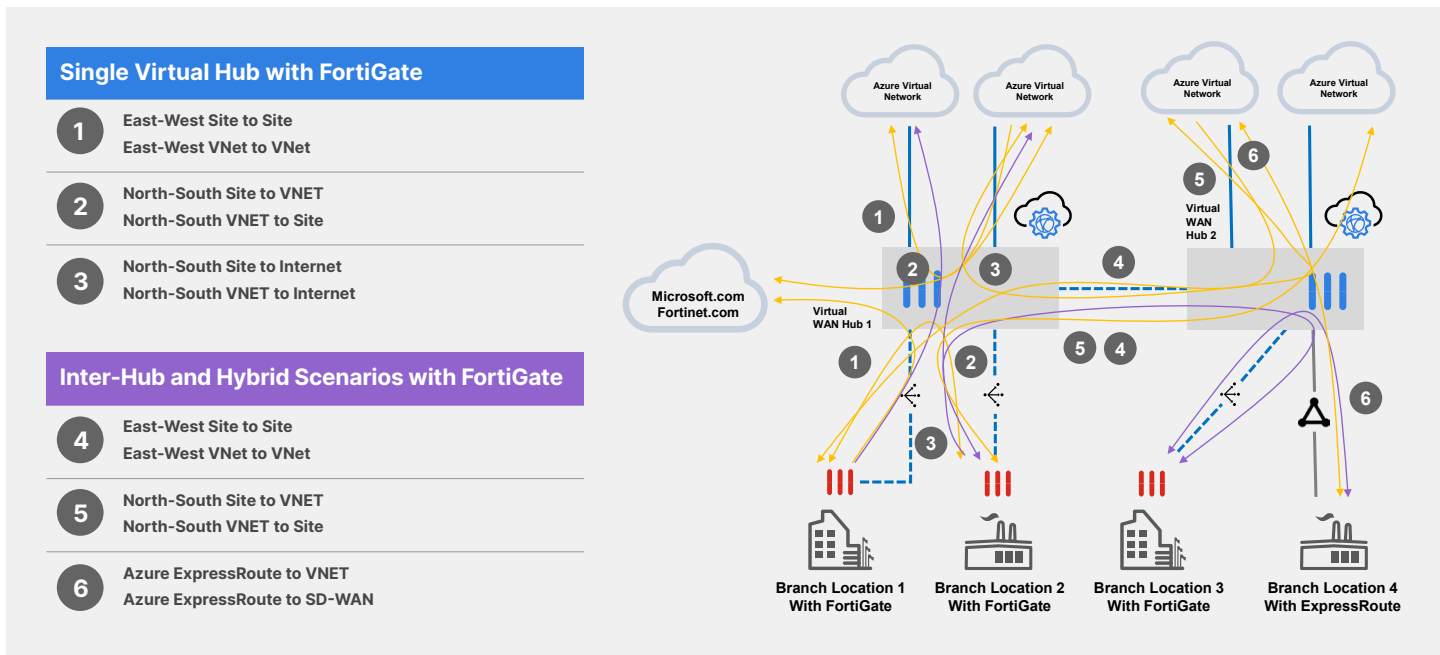


Figure 1: Fortinet secures both n-s and e-w vWAN traffic flows.

## Secure, Optimized Global Networking with Fortinet Cybersecurity and Azure Virtual WAN

The deep collaboration between Fortinet cybersecurity services and Microsoft cloud services delivers natively integrated solutions that enable organizations to:

- Simplify global connectivity**

Create a global transit network for sites, users, and cloud-hosted virtual networks with Azure vWAN—all secured with the same security solution on-premises and in the cloud.

- Secure and optimize Azure Virtual WAN traffic**

Deliver industry-leading cyber resilience and optimal digital experience with Fortinet Secure SD-WAN.

- Prevent known, unknown, and zero-day threats**

Protect all Azure Virtual WAN traffic flows with Fortinet. Powered by FortiGuard Labs, Fortinet sandboxing and FortiGate solutions harness real-time threat intelligence that utilizes machine learning and artificial intelligence to analyze billions of threat signals from millions of devices daily.

- Centrally manage on-premises and cloud security**

Simplify security and network operations across Azure and site deployments with FortiManager and FortiAnalyzer for consistent security policy management.

Whether you want to use Azure Virtual WAN as an SD-WAN backbone, for multi-cloud connectivity, or for network segmentation, Fortinet FortiGate for Azure Virtual WAN can ensure your network traffic is safe and secure.

