SOLUTION BRIEF

Fortinet Hybrid Mesh Firewall and Security Fabric for Microsoft Azure

Executive Summary

Microsoft Azure is the cloud of choice for thousands of organizations around the globe. Microsoft Azure supports a variety of security solutions and technologies to protect applications and data in the cloud. But Azure does not provide complete, enterprise-class network security. Organizations need consistent security policies across clouds and data centers as well as deep visibility and granular control wherever the compute occurs. By offering single-pane-of-glass firewall management and analytics, Fortinet simplifies security management, reduces security staff workloads, and ensures that your applications will be protected with the same security policies, whether in the cloud, the data center, or branch locations.

"Every generation of FortiGate NGFWs has brought better performance and more advanced feature sets. And the Flex-VM [now FortiFlex] billing model has been highly beneficial to our business. Being able to consume resources on the fly enables us to keep our operations lean, mean, and efficient."

Lou Corriero
Vice President of Business Development, IT Vortex

The Cloud Brings New Capabilities and Challenges

Most enterprises either have already undergone or are evaluating some form of cloud migration, including migrating to the Azure cloud. The drivers for this typically include cost reduction and greater business agility. When it comes to securing cloud environments, Microsoft does offer a firewall; however, that tool is limited and cannot be used on other clouds or on-premises.

Build a Hybrid Mesh Firewall

A hybrid mesh firewall (HMF) is a unified security platform that provides coordinated protection to multiple areas of enterprise IT, including corporate sites such as branches, campuses, and data centers; public and private clouds; and remote workers. To do this, HMFs come in various form factors, including chassis, appliances for sites both large and small, virtual machines, cloud-native firewalls, and Firewall-as-a-Service (FWaaS), and integrate with other technologies to share security context signals and automation. Fortinet FortiGate VM for Azure is designed to be integrated into your Fortinet Hybrid Mesh Firewall and into your broader Fortinet Security Fabric.

Securing an Array of Azure Public-Cloud Use Cases

As customers adopt Microsoft Azure cloud infrastructures, the need for consistent security across the organization's hybrid IT infrastructure increases. As part of the integrated Fortinet Security Fabric architecture, Fortinet solutions provide superior visibility, protection, and control for public cloud deployment options in Azure.

1. Secure hybrid cloud

FortiGate Next-Generation Firewalls (NGFWs) and cloud security solutions offer best-of-breed secure connectivity, network segmentation, and application security for hybrid cloud-based deployments. FortiGate NGFWs provide centralized, consistent security policy enforcement using high-speed VPN tunnel connections. FortiGate VMs deployed in the public cloud can securely communicate and share consistent policies with FortiGate NGFWs of any form factor provisioned in a private data center.

2. Cloud infrastructure visibility and control

Fortinet solutions monitor and track all cloud security components—such as configurations, user activity, and traffic flow logs. They also support compliance reporting requirements.

3. Secure access VPN

Remote access virtual private networks (VPNs) enable the use of cloud-based applications. The Fortinet Security Fabric delivers best-in-class performance for securing VPN traffic when remotely accessing Azure. By leveraging Azure's multiregion global infrastructure, organizations can instantaneously scale their services and offer remote access VPN termination close to the end-user.

4. Cloud security services hub

Fortinet solutions can be deployed as a transit Azure virtual network (vNET) that allows organizations to share security services to multiple networks worldwide. By leveraging the full extent of Fortinet solutions, including network visibility, VPN connectivity, NGFW, advanced web application firewall (WAF), sandboxing, and mail security, the Fortinet Security Fabric provides far more services while delivering cloud elasticity, on-demand scalability, and optimized price-performance.

5. Azure Virtual WAN integration

Fortinet solutions are tightly integrated into Azure Virtual WAN, so organizations can extend SD-WAN to the Azure cloud and secure east-west traffic between VNETs and between Virtual WAN hubs.

6. Zero-trust enforcement

Fortinet solutions, including FortiGate NGFWs and FortiWeb WAFs, enforce zero-trust policies. Zero-trust network access (ZTNA) solutions grant access on a per-session basis to individual applications only after devices and users have been verified, helping to ensure that only verified users and devices get access to each application.

7. Web application security

FortiWeb offers a purpose-built WAF that secures APIs as well as front-end web applications to ensure that applications and data remain secure. Web-based applications are vulnerable to a wide range of known and unknown attacks. FortiWeb utilizes machine learning (ML) to self-optimize application protection. FortiSandbox Cloud performs dynamic analysis, including using artificial intelligence (AI) to identify zero-day threats.

8. Intent-based segmentation

Segmenting cloud environments presents challenges because dynamic provisioning results in constantly changing IP addresses. FortiGate VMs provide intent-based segmentation, which builds rules and segments based on user identity and business logic. Rules are adjusted dynamically in response to a continuous trust assessment. As a result, FortiGate VMs can intuitively define which workloads and elements in the cloud are allowed to communicate with other workloads and elements, whether they are inside or outside the cloud.

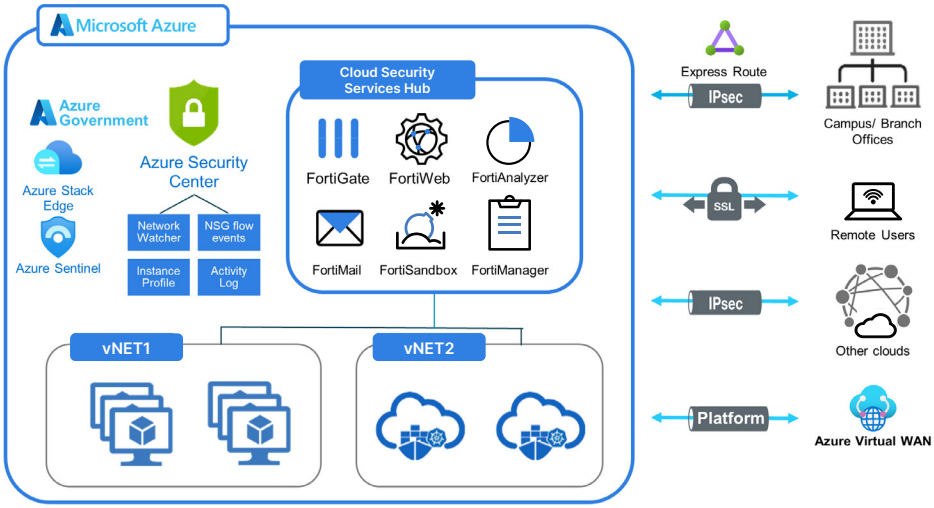

Figure 1: Fortinet secure connectivity for Microsoft Azure

How the Security Fabric Complements Azure Security

While Microsoft is responsible for securing Azure's physical cloud infrastructure (such as networking and hypervisor), it is up to the customer to ensure that other elements, such as communications, access, and applications, among others, are secured and compliant. Customers also are responsible for ensuring that security policies are consistent across clouds and their data centers.

The Fortinet Security Fabric complements Microsoft Azure security solutions. Fortinet solutions run seamlessly in Azure and integrate with Azure security services to provide transparency of security policies and events across the cloud infrastructure. Further, Fortinet's native integration with each of the major cloud providers enables seamless, automated, and centralized management across all clouds. This single-pane-of-glass management provides unified visibility, control, and policy management that can scale with additional applications and users. It also reduces the likelihood of security gaps, helps prevent misconfigurations, and ensures that the entire infrastructure is protected by state-of-the-art security.

Integrated Defenses That Span the Full Attack Spectrum

The different solutions that comprise the Fortinet Security Fabric were designed to increase end-user confidence in cloud environments. The following solutions are part of the Fortinet Security Fabric for Azure:

FortiGate VM NGFW delivers threat protection to defend against the most advanced known and unknown cyberattacks. FortiGate VM scales up and down as business needs change and is offered at various sizes to align with various supported use cases.

FortiWeb WAF protects web applications from known and unknown exploits. Using ML and AI, as well as multilayer and correlated detection methods, FortiWeb defends applications and APIs from known vulnerabilities and zero-day threats. FortiWeb is available as a service as well via pay-as-you-go (PAYG) and bring-your-own-license (BYOL) options.

FortiMail secure email gateways (SEGs) utilize the latest technologies and threat-intelligence services from FortiGuard Labs to deliver comprehensive protection from common and advanced threats while integrating robust data-protection capabilities to avoid data loss.

FortiSandbox offers a powerful combination of advanced detection, AI automated mitigation, actionable insight, and flexible deployment to stop advanced and zero-day threats.

FortiManager provides single-pane-of-glass management and policy controls across the extended enterprise for insight into networkwide, traffic-based threats. It includes features to contain advanced attacks as well as scalability to manage up to 10,000 Fortinet devices.

FortiAnalyzer collects, analyzes, and correlates data from Fortinet products for increased visibility and robust security alert information. When combined with the FortiGuard Indicators of Compromise (IOC) Service, it also provides a prioritized list of compromised hosts to allow for rapid response actions.

Fabric Connectors enable seamless, open integration of Fortinet solutions with third-party security solutions in the Fortinet Security Fabric. This provides automated firewall and network security insertion into dynamic network flows with components in a customer's existing security ecosystem.

Flexible Consumption Models

Fortinet solutions for Microsoft Azure have long been available as PAYG and BYOL licenses. Fortinet's new FortiFlex program is a points-based approach that offers organizations the flexibility to scale their security solutions and easily move them from platform to platform. Fortinet solutions for Azure also help draw down your Microsoft Azure Consumption Commitment (MACC).

Multilayer Protection That Reduces Risk

The Fortinet Security Fabric for Azure helps organizations maintain consistent security protection from on-premises to the cloud within a shared responsibility model. It delivers comprehensive, multilayer security and threat prevention for Azure users. At the same time, it streamlines operations, policy management, and visibility for improved security life-cycle management.

June 5, 2023 5:41 PM
535572-B-0-EN