SOLUTION BRIEF

Fortinet Secure Remote Access for Multi-Cloud Environments

Executive Summary

Organizations are rapidly increasing their use of cloud-based computing. Cloud-specific spending is expected to grow six times faster than general IT spending through next year. This makes it increasingly difficult for security teams to protect data moving to, from, and within clouds. Fortinet FortiGate VM next-generation firewalls (NGFWs) offer the flexibility to be deployed as NGFWs and/or VPN gateways in the cloud. They enable high-performance VPN connections across multiple on-premises and cloud environments, and they protect data in motion: within clouds, across multiple clouds, and between clouds and on-premises data centers.

Consistent, Fast, and Secure Connectivity:

- Flexible, fast, centralized deployment across multiple environments
- The best of data-in-motion security and networkwide threat protection
- Low-latency, always-on connectivity to business applications

Cloud Access Must Be Fast *and* Secure

Organizations need global, on-demand, secure access to cloud resources. They get this from FortiGate VMs, full-featured FortiGate NGFWs that are packaged as virtual appliances.

A FortiGate VM is ideal for monitoring and enforcing virtual traffic on leading virtualization, cloud, and software-defined network (SDN) platforms. These include VMware vSphere, Hyper-V, Xen, KVM, and Amazon Web Services (AWS). FortiGate VMs can be orchestrated in SDN environments to provide agile and elastic network security services—including high-performance VPNs—to virtual workloads. The FortiGate VMs can be flexibly scaled up and down, with options that include instance sizes starting from two cores per instance to 32 cores per instance.

FortiGate VM NGFWs enable an organization to simplify the deployment of secure multi-cloud connections. As a starting point, security architects need to build configuration templates that enable secure remote access termination in the public cloud. Then, they can dynamically provision FortiGate VM instances, which are preconfigured, with these templates globally. This enables mobile workforces, customers, and business partners to connect to the public cloud. It also connects the cloud network to business applications through high-performance VPN tunnels, whether they are deployed in the cloud or on-premises. All FortiGate virtual and physical NGFWs can be managed remotely from a single pane of glass.

Security architects can also leverage **FortiClient** on host servers in the cloud to enable security sockets layer (SSL)/transport layer security (TLS) and IPsec VPN connectivity between VMs on those hosts and FortiGate VMs to secure data in motion. FortiClient also integrates with FortiSandbox, which can analyze suspected but unknown threats before they impact the business. FortiSandbox exchanges threat intelligence in real time with other Fortinet Security Fabric elements such as FortiGate VM to block unknown (zero-day), advanced, and targeted threats.

Secure and Fast Connections That Multi-Clouds Require

Users should have a consistent experience, regardless of where an application is located. To support a consistent experience, FortiGate NGFWs and FortiGate VMs enable low-latency, always-on connectivity to business applications through the closest entry point into the network, as well as provide a full range of high-speed VPN solutions that protect data in motion. And they can support a global high-availability design, eliminating the potential impact of a network single point of failure.

The result is secure remote access to multi-cloud environments through VPNs, as well as broad visibility, threat-intelligence sharing, and high-performance threat protection in a single system—a foundation for meeting the demands of increasing multi-cloud use.

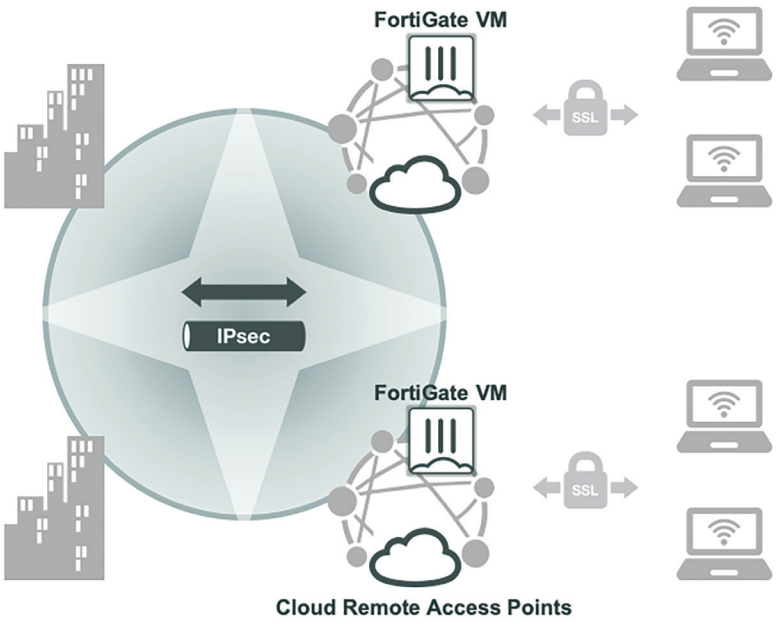

Figure 1: Secure remote access. Multi-cloud environments require fast and secure data transfer.

July 27, 2019 6:48 PM

357275-0-0-EN

D:\Fortinet\Work\2019\July\072719\Task 9 sb secure remote access\sb-secure-remote-access-for-multicloud-environments