SOLUTION BRIEF

Fortinet Secure Hybrid Cloud

Executive Summary

Hybrid clouds are a mix of on-premises and public cloud services, and their use is accelerating. Security across this extended environment tends to be inconsistently enforced and complex to manage—and connections are often unsecure. The Fortinet Security Fabric solves these challenges by natively integrating with major cloud providers, centrally enforcing consistent security policies, and establishing high-speed and secure connectivity.

Secure Hybrid Cloud Protection from Fortinet:

- Single-pane-of-glass security management
- Consistent security enforcement across all environments
- Secure connections without compromising performance

Fragmented, Inconsistent Security Between On-Premises Data Centers and Clouds

Many organizations are going outside their on-premises data centers to leverage the public cloud as an additional infrastructure for developing and delivering IT solutions. Often, they develop new applications in the cloud and maintain old applications in the on-premises data center. The use of hybrid clouds is accelerating: 81% of enterprises have multi-cloud strategies, and global spending on hybrid cloud is projected to more than double from $45 billion in 2018 to $98 billion by 2023.[1]

Despite growing momentum, several barriers are slowing hybrid cloud adoption. Notably, 77% of enterprises see hybrid cloud security as a challenge.[2] Meanwhile, each cloud provider argues for the relative advantages of its own cloud security features. But the reality is that hybrid cloud adopters experience a multiplicity of disparate security technologies, platforms, and management tools. Security posture is inconsistent between on-premises data centers and each cloud deployment. Further, network visibility is poor and security management is complex.

Lack of security connectivity between and across cloud deployments creates additional security deficiencies.

Centralized, Single-Pane-of-Glass Security Management with Fortinet

The Fortinet Security Fabric addresses these challenges. It provides broad visibility across the entire digital attack surface, both on-premises and in multiple clouds. It uses native integration with each of the major cloud providers and enables automated, centralized management of the entire security infrastructure from a single pane of glass.

Following are the key Fortinet elements that protect and enable hybrid clouds:

FortiGate next-generation firewalls (NGFWs) provide secure connectivity, network segmentation, and application security for hybrid-cloud-based deployments. They help ensure centralized, consistent security policy enforcement and connect through a high-speed virtual private network (VPN) tunnel. The latter protects data without compromising performance.

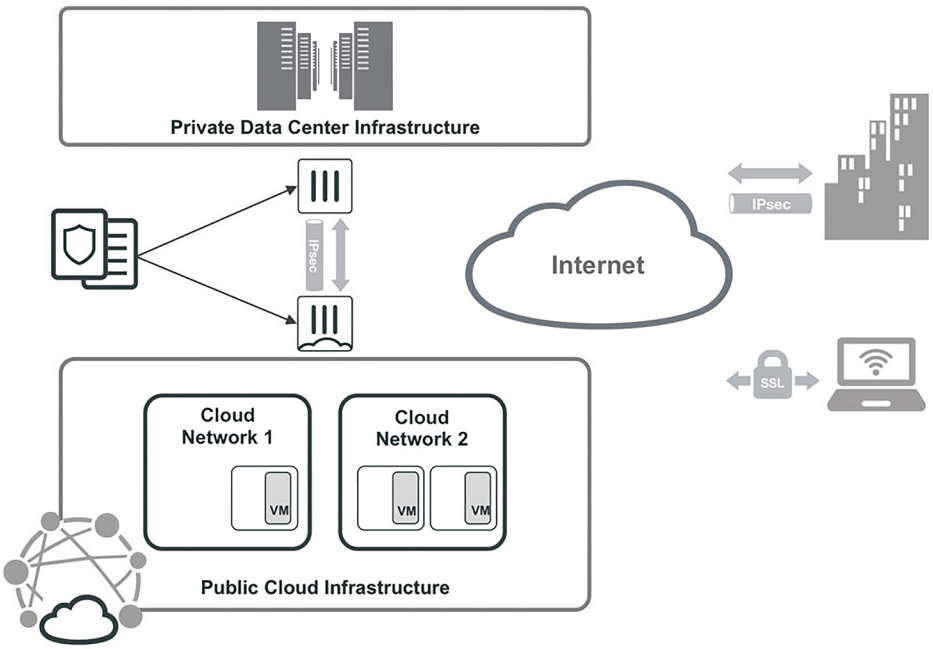

Figure 1: Security must be consistent across data center and cloud environments. Typical hybrid cloud environments increase risk through lack of visibility, inconsistent security policies, and complex security management.

Fortinet NGFWs also have the leading price-performance ratio in third-party tests among all 10 participating vendors.[3] In tests, they blocked 100% of evasions and achieved minimal performance degradation when inspecting encrypted traffic (as compared to competitive solutions). This is crucial, as over 72% of all network traffic is now encrypted, up 20 percentage points from Q3 of 2017.[4]

FortiGate-VMs are virtualized instances of FortiGate NGFWs. FortiGate VMs can securely communicate and share consistent policies with FortiGate NGFWs of any form factor that are provisioned in an on-premises data center.

FortiManager provides single-pane-of-glass management across the entire extended enterprise—including Fortinet NGFWs, switches, wireless infrastructure, and endpoints. FortiManager makes security management for enterprises easier, enabling security professionals to create and modify policies and objects with a consolidated, drag-and-drop-enabled editor. They also can manage devices in a Security Fabric group as if they were a single device, ensuring that security policies are enforced consistently across all environments. Finally, security professionals can simplify and track changes and make them auditable through integration with IT service management (ITSM) applications such as ServiceNow.

FortiAnalyzer enables organizations to analyze, report, and archive security events, network traffic, web content, and messaging data. A comprehensive suite of easily customized reports simplifies the measurement and documentation of compliance.

Protecting—and Enabling—Hybrid Clouds

Hybrid clouds give organizations new flexibility. The virtual and physical components of the Fortinet Security Fabric work together to centrally protect the resulting dynamic infrastructure and secure critical data from the customer to the cloud and back.

[1] Chaitanya Atreya, "A Closer Look At Hybrid-Cloud And Multi-Cloud Approaches," Forbes, November 26, 2018.

[2] Gary Thome, "Survey Says: Cost and Security are Top Hybrid Cloud Concerns," CIO, September 28, 2018.

[3] "Fortinet Receives Recommended Rating in Latest NSS Labs NGFW Report, Delivers High SSL Performance Suited for Encrypted Cloud Access," Fortinet, July 17, 2018.

[4] John Maddison, "Encrypted Traffic Reaches A New Threshold," Network Computing, November 28, 2018.

March 21, 2019 11:52 AM

356355-0-0-EN

D:\Fortinet\Work\March\032119\sb-secure-hybrid-cloud