FURTINET

SOLUTION BRIEF

FortiGate VM Delivers Advanced Security for OpenStack Environments

Executive Summary

OpenStack is an open-source cloud management platform specifically designed to build a low-cost private cloud for development operations (DevOps) and Infrastructure-as-a-Service (IaaS) offerings. Enterprises are increasingly turning to OpenStack for data center and cloud deployment alternatives; however, despite its popularity, OpenStack does not offer built-in security. Therefore, security architects must be able to extend their security infrastructure to include OpenStack environments. FortiGate VM on OpenStack optimizes next-generation firewall (NGFW) capabilities as a virtual machine (VM) for organizations and service providers of all sizes. FortiGate-VM offers the highest level of cyber-threat protection in the industry with its high performance, security efficacy, and deep visibility enabled by the Fortinet Security Fabric.

Critical security needs for OpenStack environments include:

- Delivering security and performance at scale
- Auto-scaling security for cloud workloads
- Multi-tenant provisioning
- Physical and virtual internal segmentation
- Scalable Security-as-a-Service
- Security that directly integrates with OpenStack

OpenStack Environments Lack Inherent Security

Networks are transitioning to models more suited to the cloud—such as software-defined networking (SDN), network function virtualization (NFV), and virtual network infrastructure. This impacts the relationships between networking, security orchestration, and policy enforcement.

OpenStack-based clouds provide an environment for elastic, on-demand, multi-tenant applications. The OpenStack framework was developed to provide infrastructure resources to consumers (e.g., developers, end-users, business units) in a rapid, self-service manner—making the platform a popular choice. The need for security with OpenStack, however, remains a problematic afterthought—sacrificing platform protection for speed and efficiency.

FortiGate VM on OpenStack

FortiGate VM on OpenStack provides a virtual NGFW for OpenStack clouds. It includes all the security and networking services common to physical FortiGate NGFW appliances. Users can deploy a mix of FortiGate hardware and virtual appliances—operating them together and managing them all from a common, centralized management platform. This flexibility allows for rapid provisioning of security infrastructure whenever and wherever it is needed.

FortiGate VM mitigates blind spots in OpenStack by implementing critical security controls within virtual infrastructures. The Fortinet OpenStack solution embraces the software-defined security framework, providing out-of-the-box integration so that advanced network security can be applied in logical and dynamic environments.

The Fortinet solution for OpenStack allows enterprises and managed security service providers (MSSPs) to expand their OpenStack cloud initiatives without the performance and scalability issues that have traditionally constrained security in virtualized environments.

FortiGate VM provides advanced security for OpenStack in several use-case scenarios:

- **Routed Firewall.** Commonly used in service provider environments, FortiGate VM can run on OpenStack as a regular in-line firewall in "routed" mode—acting as a default gateway to the network.
- **Unified Threat Management (UTM).** FortiGate VM effectively neutralizes a wide range of security threats with L4—L7 UTM capabilities, including service insertion and service chaining.

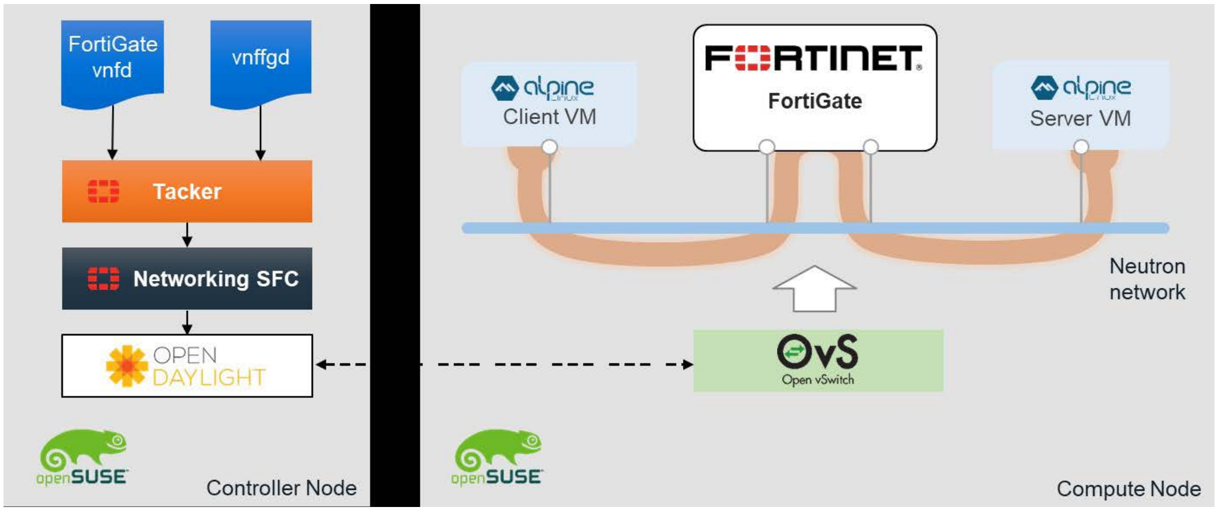

Figure 1: FortiGate VM deployed in an OpenStack Neutron environment provides "east-west" security.
FortiGate VM supports service function chaining and understands packets with network service headers (NSHs).

- **Integrated Management.** Fortinet Fabric Connectors deliver the ability to abstract security policies and provide consistent policies in dynamic, multi-vendor environments. FortiGate VM can serve as a Fabric Connector for OpenStack's Horizon dashboard—a web-based user interface to OpenStack services (e.g., Nova, Swift, Keystone).
- **Simplified Provisioning and Deployment.** In combination with Cloud Init and OpenStack Heat, FortiGate VM can be used to fully automate OpenStack deployments.
- **High-performance Threat Protection:** Since OpenStack is typically used in conjunction with kernel-based virtual machines (KVMs), FortiGate VM provides optimal threat protection performance through its virtual security processing unit (vSPU) technology.
- **Automated Workflows.** FortiGate VM FortiOS operating system automates tasks such as event-based triggers while offering customizable webhooks, AWS Lambda calls, email notifications, etc.

Benefits of FortiGate VM for OpenStack

Integrated with OpenStack, FortiGate VM provides end customers with a number of benefits:

Enhanced security. FortiGate VM protects against known exploits and malware using continuous security provided by FortiGuard Labs threat-intelligence services. It also offers advanced network traffic inspection capabilities, including the ability to automatically identify and inspect thousands of applications (including those based in the cloud). Additionally, FortiGate VM defends against unknown attacks using dynamic analysis, while providing automated mitigation to stop targeted attacks.

FortiGate VM is independently tested and validated for security effectiveness. It has received unparalleled third-party certifications from industry experts such as NSS Labs and ICSA.[1]

High performance. FortiGate VM delivers the industry's best threat protection performance[2] with vSPU and SR-IOV (single root input/output virtualization) technologies. It supports Intel QuickAssist (QAT) acceleration for throughput improvements on IPsec-VPN, enabling remote access to cloud-based applications.

Flexible deployment. Fortinet offers the ability to manage virtual appliances and physical appliances from a single-pane-of-glass management platform. FortiGate VM supports a wide array of licensing choices to fit any infrastructure requirement—including virtual domain (VDOM)-enabled models for multi-tenant environments.

Efficient management. FortiGate VM collaboratively integrates with other Fortinet products and Fabric-ready solutions from third-party vendors to provide end-to-end security across the entire attack surface. It also delivers out-of-the-box integration and orchestration with leading SDN platforms. Most importantly, centralized, single-pane-of-glass management improves visibility of multi-cloud environments while enforcing consistent policy controls across dynamic, multivendor environments. Finally, simplified operations reduce the burden on limited staff and budget resources.

Extending NGFW Protection Across Hybrid-IT Environments

FortiGate VM establishes a consistent security posture for private cloud environments based on the OpenStack platform. It shares the same advanced features of FortiGate NGFW physical appliances—enforcing security policies across all environments, protecting applications and connections, and enabling centralized security management.

As an integrated part of the Fortinet Security Fabric, FortiGate VM continuously monitors users and endpoints with automated detection and response capabilities. It automatically identifies noncompliant, suspicious, or anomalous behaviors (on- or off-network) and then rapidly sends alerts. By leveraging machine learning and advanced analytics, Fortinet's proactive approach to threat detection delivers additional protection and visibility across the entire enterprise network.

[1] "Certifications," Fortinet, accessed October 30, 2019.

[2] "FortiGate: Next Generation Firewall (NGFW)—Certifications," Fortinet, accessed October 30, 2019.