FORTINET VMWARE READY™ FOR NFV SOLUTION

Security Without Compromise with Unprecedented Agility

INTRODUCTION

Network Functions Virtualization (NFV) offers unprecedented opportunities for service providers to adopt new business models, radically lower costs, and increase the speed of innovation and delivery of next-generation services. While the potential benefits of NFV are enormous, ensuring effective security is a key consideration for service providers.

Protecting these highly dynamic environments requires a Security Fabric with tightly integrated security and network technologies that share intelligence and collaborate to detect, isolate, and respond to threats in real time. Fortinet recognizes the importance of having an open system that supports and secures as many NFV solutions in the industry as needed in order to meet the requirements of service provider customers. Fortinet was the first security provider to demonstrate the integration of its virtual enterprise firewall solution, FortiGate VMX, with VMware NSX® and VMware Integrated OpenStack environments. This was a great proof point of the openness of the Fortinet Security Fabric in integrating with industry partner products and platforms.

Service providers are aware of NFV and virtualization introducing new challenges to security, including longer chains of trust, reduced isolation of network functions and other related concerns from virtualization. The Fortinet VMware Ready™ for NFV solution comprehensively addresses service provider needs for enhanced security capabilities in their NFV environments.

As a VMware Technology Alliance Partner, Fortinet has completed VMware's rigorous validation process for the solution to achieve VMware's highest level of endorsement, VMware Ready™ Status for Network Functions Virtualization, as described in the VMware Solutions Exchange (VSX). Fortinet has also achieved VMware vCloud Director compatibility certification, as indicated in the VMware Compatibility Guide. These achievements are a significant step forward in enabling service providers to offer true "security-as-a-service" delivery models on commodity CPE, while benefitting from rapid service provisioning and delivery of consolidated services.

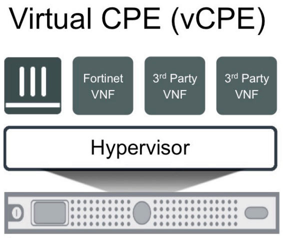
SOLUTION DESCRIPTION

The solution enables virtual network functions, such as firewall, IPS NAT, DHCP, etc., in FortiGate-VM to be deployed as customized virtual Customer Premises Equipment (vCPE) instantly, completely decoupling network security functions from the underlying hardware, and thereby gaining significantly increased flexibility. This brings unprecedented agility to network and security provisioning, combined with significant CAPEX and OPEX savings.

KEY BENEFITS

- Software-defined security automation for service life cycle.
- A variety of customizable security services on a single commodity device.
- Rapid configuration and service delivery with NFV enabled vCPE.
- Lower total cost of ownership with new security insertion rollout.
- Unparalleled security, with the industry's best-validated security protection.

FORTINET Fabric-Ready



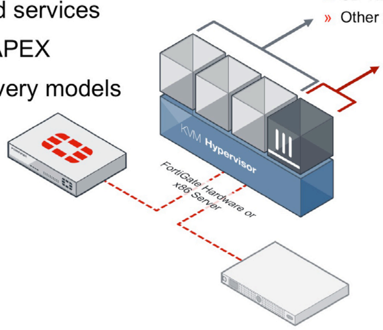
FortiGate VM – Virtual Appliance

- Virtual network function (VNF) runs on 3rd-party x86 appliance
- Supports hypervisor SR-IOV acceleration
- Supports service orchestration via VMware NFV Infrastructure

FIGURE 1: VIRTUAL CPE (VCPE)

Figure 1 illustrates the vCPE concept. The flexibility provided by the solution enables the deployment to have the same underlying x86 hardware supporting VMware vCloud NFV infrastructure, but with different FortiGate virtual network functions on the top of the stack, as illustrated in Figure 2.

- Rapid service delivery
- Consolidated services
- Reduced CAPEX
- Multiple delivery models



Third-Party VNFs
- 3rd party business applications
- SD-WAN
- Other 3rd party services

Fortinet VNFs
- Security
  - Firewall
  - UTM
  - IPS
  - SD-WAN
- Network
  - NAT
  - Routing
  - DHCP
  - ....

FIGURE 2: FORTINET VNFS IN VMWARE VCLOUD NFV INFRASTRUCTURE

SOLUTION BENEFITS

- Software-defined security automation for service life cycle.
- A variety of customizable security services on a single commodity device.
- Rapid configuration and service delivery with NFV enabled vCPE.
- Lower total cost of ownership with new security insertion rollout.
- Unparalleled security, by leveraging the industry's best validated security protection.

NFV is expected to deliver significant benefits in terms of savings that result from using general-purpose hardware and increased automation, leading to decreased time to market for new and innovative services.

The Fortinet VMware Ready™ for NFV solution comprehensively addresses security aspects in NFV environments, delivering security without compromise with unprecedented agility. The solution's benefits provided via vCPE deployments with integrated security are enormous, and help reduce the amount and cost of physical third party x86 hardware appliances required at customer premises — especially in deployments with on-demand hosting connectivity that has ever-changing, workload-driven network security requirements per tenant. Service providers can leverage Fortinet to implement security without compromise in their environments, while taking advantage of the many benefits that NFV provides.

vmware READY
NETWORK FUNCTIONS VIRTUALIZATION

FORTINET VMWARE READY™ FOR NFV CERTIFIED SOLUTION

- Fortinet FortiGate v5.4.1

The Solution is fully certified with these products from vCloud NFV 1.5:

- vSphere 6.0 U2
- vCloud Director 8.10
- NSX 6.2.2
- VMware Integrated OpenStack 2.0.3

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990

February 20, 2018 5:30 PM