SOLUTION BRIEF

Fortinet VMware Ready™ for Telco Cloud Infrastructure 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 Telco Cloud Infrastructure 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 Marketplace Program Guide. Fortinet has also achieved VMware Telco Cloud Infrastructure 1.0 and 2.0 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., inFortiGate-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.

Joint Solution Components

- Fortinet FortiGate
- VMWare Network Functions Virtualized (NFV)

Joint 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, with the industry's best-validated security protection

FORTINET FABRIC-READY

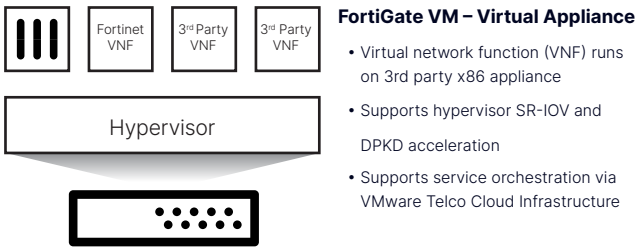

Figure 1: Virtual CPE (vCPE)

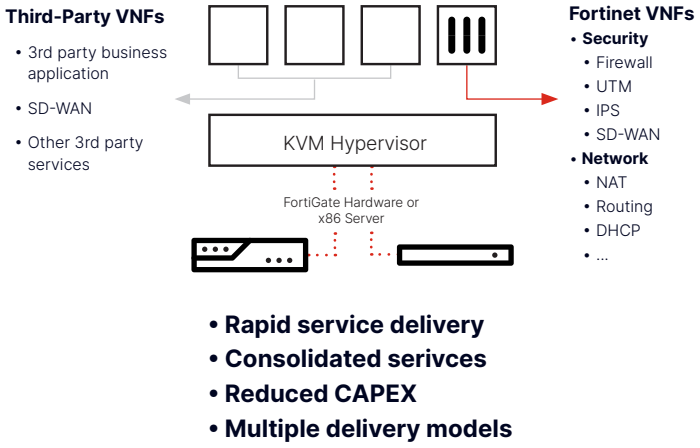

Figure 2: Fortinet VNFS in VMWare VCloud NFV Infastructure

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

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 Telco Cloud Infrastructure 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.

Fortinet VMWare Ready™ for Telco Cloud Infrastructure Certified Solution

Vendor Solution

- Fortinet FortiGate VM Ver. 7.0.1

The solution is certified with the following components from VMware Ready for Telco Cloud Infrastructure 1.0 OpenStack Edition Platform:

- VMware ESXi 6.7 EP15
- VMware vCenter Server Appliance 6.7 U3j
- VMware NSX T 3.0.2
- VMware Virtual SAN 6.7 U3
- VMware Integrated Openstack Carrier Edition 7.0
- vRealise Log Insight 4.8

The solution is certified with the following components from VMware Ready for Telco Cloud Infrastructure 2.0 OpenStack Edition Platform:

- VMware ESXi 7.0 U1b
- VMware vCenter Server Appliance 7.0 U1a
- VMware NSX-T T 3.1.0
- VMware Virtual SAN 7.0 U1
- VMware Integrated Openstack Carrier Edition 7.0.1
- VMware vRealise Log Insight 8.2

Please refer to the VMware Marketplace for additional details.

October 7, 2021 4:00 PM
sb-nfv-VMware
42853-B-0-EN