SCALABLE PROTECTION ON-DEMAND FOR ELASTIC SERVICE MODELS

Fortinet VM On-Demand Program for Service Providers

INTRODUCTION

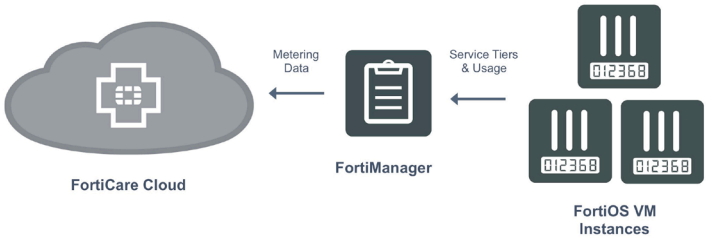
Communications service providers, cloud providers, and MSSP's are being driven by a number of enterprise data center trends, including the shift from capex to opex models as driven by IaaS/PaaS/SaaS and the need to deliver that infrastructure with more agility and elasticity to help accelerate business initiatives. Service providers in turn are looking to infrastructure suppliers, including firewall and security vendors, to help reduce capital risks and better align IT costs with recurring and on-demand service revenues.

The FortiOS virtualized security appliance and the Fortinet VM On-Demand program enable service providers to deliver award-winning Fortinet firewall and other protection in an on-demand, pay-as-you-grow model that is better aligned with the agility and elasticity in modern cloud and managed service offerings. Members of Fortinet's MSSP Partner program, as well as other qualified service providers globally, can deploy scalable virtual firewalling and advanced security services on an as-needed, per-tenant basis, with actual costs automatically and transparently measured based on actual usage.

PAY-AS-YOU-GROW PLATFORM

The VM On-Demand Program is a turnkey platform for transparent licensing, provisioning, metering, and billing of on-demand security VM's within the provider environment. A pay-as-you-grow pricing model enables providers to offer protection when and where customers and tenants need it, but pay only for actual customer usage as the platform is consumed.

Providers can flexibly spin up firewall VM instances on a per-tenant basis as needed. Elastic resource tiers support varying capacity needs, while FortiGuard threat tiers range from firewall-only to full unified-threat protection.



ON-DEMAND SECURITY USE CASES

Public IaaS Clouds

Many telco's and service providers are rolling out Infrastructure-as-a-Service (IaaS) offerings as enterprises look to migrate virtual server workloads from internal data centers to provider-hosted public clouds. Enterprises are often looking for both cost-effective opex infrastructure as well as elastic server capacity to accelerate business initiatives, and increasingly expect to be able to procure firewall and advanced security services on-demand to elastically protect their user data and privacy.

Network Function Virtualization (NFV)

The Network Function Virtualization (NFV) movement in the service provider industry takes advantage of SDN and network virtualization principles to replace monolithic physical network and security devices with virtual network functions (VNF's) encapsulated as VM's, i.e., virtualized firewalls and other appliances that can be deployed on more commoditized hardware.

KEY FEATURES AND BENEFITS

- Turnkey, out-of-the-box platform for pay-as-you-grow firewall consumption
- Seamless on-demand VM licensing, provisioning, metering, billing
- Unlimited firewall capacity available as needed for elastic clouds and workloads
- Infrastructure costs aligned with tenant/customer service revenues on a per-period basis, e.g., monthly
- Avoidance of excess capitalization from over-provisioned capacity

This interoperable, standards-based approach to service insertion and service-chaining provides an efficient, modular, scale-out approach to service delivery. NFV Management and Orchestration (MANO) enables automated instantiation of security VNF's into the service chain, and is well-complemented by opex and pay-as-you-grow firewall VNF licensing that can scale capacity with customer needs.

Virtual CPE (vCPE)
Virtual CPE (Customer Premises Equipment) replaces provider-managed broadband devices such as access routers and firewalls that traditionally sat at the network edge on customer (subscriber) premises, with virtualized network functions (VNF's) based on NFV principles. Virtual routing, switching, firewalling, and other edge services can be relocated back to the provider data center in large, pooled server hosts, or can remain on customer premises but within a low-cost CPE host – the latter approach sometimes more specifically as universal CPE (uCPE).

With a vCPE/uCPE model, access-based providers can reduce costs when provisioning managed services without requiring truck rolls to deliver/maintain/upgrade proprietary hardware devices, while additionally increasing cross-sell/upsell revenue opportunity from value-added services. On-demand advanced security for example, could enable existing firewall customers to easily add IPS, web filtering, or antimalware quickly in response to heightened hacker or advanced threat activity.

SOLUTION COMPONENTS

There are three product and technology components to the VM On-Demand Program:

	FortiOS VM	Firewall and advanced security virtual appliance running same FortiOS firmware and security engines found in award-winning FortiGate appliaces, with transparent licensing mechanism.
	FortiManager	Centralized authorization, management, and usage metering for provisioned FortiOS virtual appliances at the provider premises.
	FortiCare	SaaS-based metering account is created within FortiCare cloud portal to aggregate and report FortiManager and FortiOS virtual appliance metrics continually. Prepaid billing enables payment only as usage is consumed.

VOLUME-BASED USAGE METERING

The VM On-Demand program meters usage based on customer traffic volumes (e.g., per gigabyte of network traffic inspected), rather than on the throughput capacity of the security appliances deployed, enabling costs to be aligned with only what customers actually use. This provides efficiencies in numerous ways compared to hardware or virtual appliance perpetual licensing.

First, providers traditionally needed to budget firewall capacity upfront to meet expected capacity over the multi-year lifecycle of an appliance or chassis hardware solution based on expectation of customer/subscriber growth. In addition to fully capitalizing the hardware expense upfront, this also meant that hardware was significantly under-utilized initially. With a usage-based metering model, providers don't need to pay years ahead for capacity for anticipated customer growth.

Second, providers often must size firewall appliance capacity to handle peak loads, which means that often 80 - 90 percent of that appliance capacity is sitting idle during normal periods. With a volume-based model, there is no penalty to oversize VM capacity to handle infrequent peak traffic, as usage is charged only by actual volume.

Third, other scenarios like high availability are more attractive because a standby firewall instance in an active/standby configuration provides business continuity without incurring any added volume-based metering costs.

SUMMARY

Service providers are under increasing pressure to deliver cloud and managed services in a more agile manner, and need to be able to supply infrastructure and security capacity elastically while minimizing capital risks from overcapacity. FortiOS virtual security appliances and the Fortinet VM On-Demand program provide a unique turnkey solution for providing on-demand, pay-as-you-grow firewall capacity while aligning security infrastructure costs with actual customer cloud and managed service revenues.

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

December, 2016