FORTINET | vmware

SOLUTION BRIEF

Scale and Segment for VMware Integrated OpenStack (VIO)

Executive Summary

Enterprises have been able to use the power of virtualization to streamline operations and to drive up operational efficiency. With the introduction of VMware NSX, enterprises are able to take this simplification to a new level. They are also able to secure granular microservices with automated security policy grouping.

Highlights

- Delivers cohesive enterprise security, control, and visibility for VMware-powered OpenStack cloud
- Fortinet Security Fabric enables instant and transparent compatibility with NSX microsegmentation for a heterogeneous data center
- Scales out control plane for HA control throughout NSX-enabled hypervisors

VMware Integrated OpenStack (VIO)

VMware Integrated OpenStack is a VMware-supported OpenStack distribution designed and built to be deployed atop existing VMware infrastructure. VMware Integrated OpenStack empowers VMware administrators to easily deliver and operate an enterprise production-grade OpenStack cloud on a VMware base. It empowers enterprises to take advantage of all VMware vSphere features like HA, DRS, or VSAN for an OpenStack cloud.

In VIO, VMware NSX serves as a virtual networking platform powering the OpenStack production environment by playing the role of the networking engine behind Neutron. It brings enterprise-grade capabilities to the OpenStack production environment including:

- The distributed systems architecture of the NSX Controller Cluster
- The core functionality and behavior of NSX primary system components
- High-availability deployments
- The logical networking devices and NSX security tools

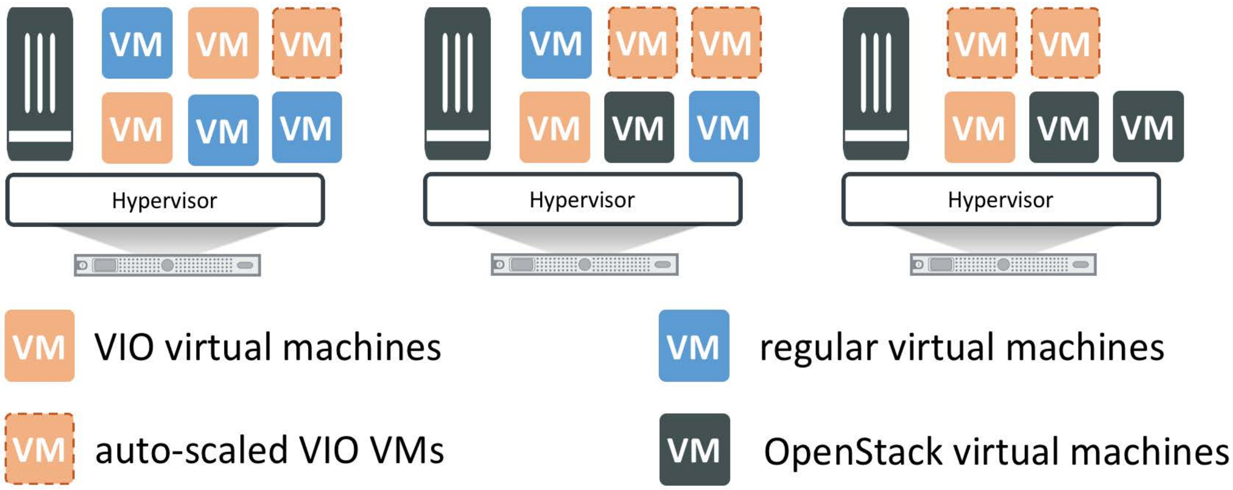

FIGURE 1: Protecting VIO Data Center with FortiGate-VMX.

Enterprises and managed service providers want to harness the power of this integration between OpenStack and VMware NSX. They greatly value the flexibility and orchestration OpenStack brings to the table. The power of OpenStack to facilitate agile deployments and simplified scaling and growth is especially invaluable to them. Fortinet is in an ideal position to provide a powerful security solution to protect this integrated deployment.

With the advent of VMware Integrated OpenStack (VIO) version 2.5, VMware has introduced support for a tightly knit integration with VMware NSX. VIO mirrors OpenStack security groups into NSX automatically. As a part of this integration with VMware NSX-V, you can leverage the power of NSX-integrated security solutions to automate L4-L7 advanced security controls backed by FortiOS. FortiGate-VMX is in a unique position to be able to bring in the security effectiveness organizations have come to expect from FortiGate physical and virtualized appliances to the VIO data center.

Today, VMware, through their NSX APIs, virtualizes networking functions such as routing and switching with the same expertise they have applied to storage and compute infrastructure for years. FortiGate-VMX, then, integrates with these NSX APIs to provide best-in-class security to the software-defined data center (SDDC).

Advantages

Simplified Scaling

The solution consists of the FortiGate Service Manager, which coordinates with VMware NSX Manager to provision a FortiGate NSX security node on each hypervisor in the cluster. This ensures that FortiGate-VMX security nodes will automatically protect every workload in this environment, including any newly created or migrated workloads. Through the use of NSX automation, FortiGate Service Manager can ensure that the same sets of policies are deployed on all security nodes without the need for manual intervention after VM migration.

East-West Protection

Simply using a traditional firewall sitting at the edge protecting north-south traffic isn't enough. True east-west protection is essential to prevent the lateral spread of any threats that do happen to get through the boundary firewalls (or are propagated from within the network). Using microsegmentation, FortiGate-VMX security nodes are also able to protect eastwest migration of threats between VMs within the data center while still being able to keep up with modern performance demands. This comes from the added performance benefits that VMware NSX architecture brings.

Virtual Segmentation Function – Fortinet's VM Portfolio, including the FortiGate-VMX using **patented virtual domain technology (VDOM)**, is the ONLY virtual security product to support multi-tenancy and security function virtualization. This is a great benefit to both **managed services providers** and **enterprises.**

Managed services providers using VDOMs are able to provide complete segmentation of tenants while providing them administrative autonomy over their security requirements.

- MSSPs can provision one VDOM per tenant
- Each VDOM can be configured with a tailored set of security features that best suit the individual tenant
- Each tenant can then securely be provided with complete autonomy over the security policies of their VDOM

Enterprises could choose to use VDOMs in order to segment their security architectures to differentiate policies and services by department, application, etc.

- Enterprises can create VDOMs for each department (e.g., Human Resources, InfoSec, or Marketing)
- Security services provided for each of these VDOMs can then be tailored to suit the department

Security posture is one of the key design considerations when it comes to both building new deployments and expanding existing ones. Fortinet has been protecting both OpenStack and VMware NSX deployments for a while now, and the FortiGate-VMX continues to be a leader when it comes to protecting your VMware Integrated OpenStack deployment.

FORTINET

www.fortinet.com