Cisco Virtual Security Gateway for Cisco Nexus 1000V Series Switches

Security and Compliance for Virtual Computing

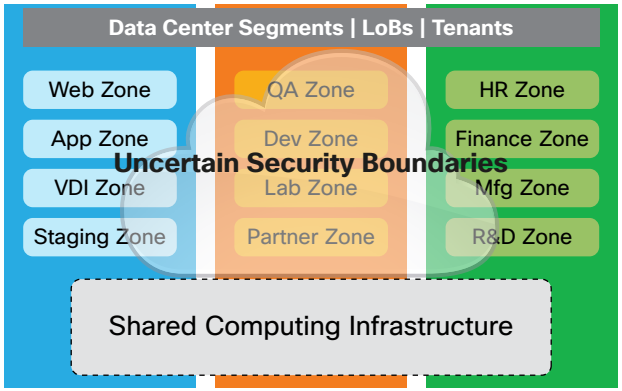
Cisco Virtual Security Gateway (VSG) for Cisco Nexus® 1000V Series Switches delivers security, compliance, and trusted access for virtual data center and cloud computing environments.

The Virtual Computing Security Challenge

As virtualization continues its rapid penetration of information technology infrastructure, security, data protection, and privacy compliance rules, historically formulated for the physical server, can be compromised (Figure 1). With virtualization enabling multiple operating systems to share a single physical server, a way to replicate traditional security and segmentation for virtualized servers is required. Attributes of enterprise private cloud and public cloud architectures include:

- Multiple lines of business or tenants, each of which requires a protected and trusted virtual computing environment
- Workload elasticity, in which virtual servers are rapidly instantiated to address increased workloads and periodically stopped or removed to support data center efficiency and green computing
- An elevated requirement for high availability

Figure 1. Virtualization Creates Obscured and Uncertain Security Boundaries



Cisco VSG Solution

Cisco VSG for Cisco Nexus 1000V Series Switches is a virtual appliance that delivers security and compliance for virtual computing environments. Cisco VSG uses virtual network service data path (vPath) technology embedded in the Cisco Nexus 1000V Series virtual Ethernet module (VEM), offering transparent insertion, efficient deployment, and very high performance with vPath-based distributed enforcement of packets (Figure 2).

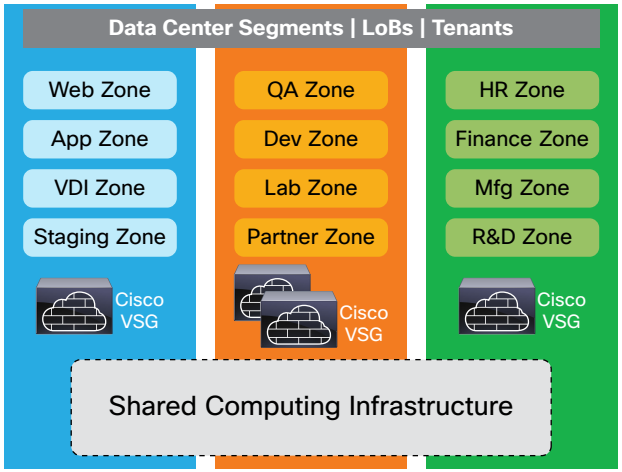
Cisco VSG works with the Cisco Nexus 1000V virtual supervisor module (VSM) and with the new Cisco Prime Network Services Controller. Together they allow security, network, and server teams to collaborate while simultaneously helping ensure administrative segregation to meet compliance and audit requirements and reduce administrative errors. Security team continues to be responsible for creating and managing security profiles through the Cisco Prime Network Services Controller.

Cisco VSG supports dynamic virtualization environments. Security profiles are bound to Cisco Nexus 1000V Series port profiles. The Cisco Nexus 1000V Series manages and enforces port and security profiles for each virtual machine virtual Ethernet port. A virtual machine can be repurposed by assigning a different port and security profile. Similarly, as VMware vMotion operations move virtual machines across physical servers, the Cisco Nexus 1000V Series helps ensure that port and security profiles follow them. Security enforcement and monitoring remains transparent to VMware vMotion events.

Main Benefits of Cisco VSG

- Reduced IT costs by enabling secure virtualized workloads across multiple tenants on a shared computing infrastructure for virtual data centers or for private or public cloud computing environments
- Comprehensive support for security for changing workloads
- Enhanced compliance with industry standards and government regulations
- Simplified auditing processes for virtualized environments

Figure 2. Secure Virtualization with Multiple Tenants and Clear and Certain Security Boundaries



Why Cisco?

As Cisco continues to add value to the enterprise data center, network, and user community, we continue to innovate while we listen to needs. With the Cisco Unified Computing System™ the technology leader in servers and the Cisco Nexus Family the technical leader in networking, Cisco VSG adds highly differentiated value to the virtualized data center. These Cisco solutions in combination with Cisco world-leading technical support and Cisco Advanced Services offerings help lead the way to optimized IT.

For more information, visit http://www.cisco.com/go/vsg and http://www.cisco.com/go/nexus.

C45-617364-01 06/13