Cisco Virtual Security Gateway for Cisco Nexus 1000V Series Switches

Q. What is the Cisco® Virtual Security Gateway (VSG)?

A. 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 very high performance with vPath-based policy enforcement of packets.

Q. What are the major features and benefits of Cisco VSG?

A. Table 1 provides a summary of the new features and business benefits of Cisco VSG.

Table 1. Main Features and Benefits of Cisco Virtual Security Gateway

Feature Name	Description	Benefit
Trusted access	Cisco VSG segments the virtual infrastructure into zones of trust and applies zone-based security policies to control and monitor access: • Cisco VSG applies granular, context-aware policies, based on network, custom, and virtual machine attributes. • Cisco VSG provides trusted access even in multi-tenant private and public cloud environments.	Cisco VSG secures virtualized infrastructure, strengthens compliance, simplifies audits, and lowers total cost of ownership (TCO) by helping to virtualize more workloads.
Dual-path architecture	Cisco VSG uses vPath technology embedded in the Cisco Nexus 1000V virtual Ethernet module (VEM), offering very high performance with vPath-based policy enforcement of packets: • Unknown packets are forwarded from the VEM to Cisco VSG for policy information. Cisco VSG then sends security policies to the VEM. • From there, security policies are handled in vPath by the VEM, without intervention from Cisco VSG.	Security that compromises performance is not security. The vPath-based architecture delivers the benefits of security for fully virtualized data centers without sacrificing performance.
Support for flexible virtualized data centers	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 ensures that port and security profiles follow them. Security enforcement and monitoring remains transparent to VMware vMotion events.	Support for flexible virtualized data centers delivers the benefits of simplified and scalable provisioning of security services while delivering workload agility.
Nondisruptive administration	Cisco VSG integrates with the Cisco Nexus 1000V Series, along with a separate security management solution (Cisco Prime Network Services Controller) that provides both a GUI and a web services API.	Allowing the security team to manage security policies and devices prevents accidents and errors. Automated provisioning through API integration allows rapid enablement of security services.
High availability	Cisco VSG can be deployed in active-standby mode to help ensure a highly available operating environment, with vPath redirecting packets to the secondary or standby VSG when the primary or active Cisco VSG is unavailable.	Security with high availability is achieved. Any component of the virtualized data center not delivering high availability lowers the value proposition.

Q. What are the main components of Cisco VSG?

A. The main components are:

- Cisco VSG in a virtual appliance form-factor for secure segmentation in a virtualized environment
- Cisco Prime Network Services Controller in a virtual appliance form-factor for managing the Cisco Virtual Security Gateways, creating security policies and enabling automation-based provisioning
- Tight integration with Cisco Nexus 1000V Switch that allows for intelligent traffic steering, flexible deployment and accelerated performance

Q. Where is Cisco VSG deployed?

A. Cisco VSG is deployed as a virtual appliance on VMware vSphere 4.0, 4.1, or 5.0. Cisco VSG's operation requires that virtual machines be connected to the Nexus 1000V distributed virtual switch. VMware vSphere 5.0 requires Cisco VSG release 4.2(1)VSG1(3) or later.

Q. How is Cisco VSG delivered?

A. Cisco VSG is delivered either as a downloadable Open Virtualization Format (OVF) file or as an installable ISO image.

Q. Who needs Cisco VSG?

A. Every virtualized data center that is running application workloads with varied security needs, including those requiring multiple tenants of any kind (for example, different departments of an enterprise or organization), needs Cisco VSG.

Q. Who can sell Cisco VSG?

A. Cisco sales staff, Product Sales Specialists (PSS), and channel partners can sell Cisco VSG.

Q. How is Cisco VSG licensed?

A. Cisco VSG for the Cisco Nexus 1000V Series is licensed on a per-CPU basis.

Q. How is Cisco VSG managed?

A. Cisco VSG is managed with the Cisco Prime Network Services Controller.

Q. Why does Cisco VSG require a Cisco Nexus 1000V Series Switch?

A. Cisco VSG requires a Cisco Nexus 1000V Switch to provide port-profile-to-security-profile binding, a traffic-steering element (in vPath) which makes deployment very flexible, and Vpath-based offload to accelerate performance.

Q. What is the return on investment (ROI) for Cisco VSG?

A. As with many security products, the ROI for Cisco VSG is based on:

- Prevention of expensive security breaches
- Prevention of fines resulting from noncompliance with regulations
- Reduction in audit costs
- Reduction in infrastructure costs through sharing of the same computing infrastructure across a broad set of virtualized workloads with varied security needs

Q. How does Cisco VSG support simplified deployment?

A. Delivered as a virtual appliance, Cisco VSG can be simply installed in local or remote data centers over the network and centrally managed through the GUI-based Cisco Prime Network Services Controller.

Q. Can Cisco VSG be deployed in Layer 3 hop away from Cisco Nexus 1000V VEM?

A. Yes, Cisco VSG supports both Layer 3 and Layer 2 connectivity with the Nexus 1000V VEM. Layer 3 connectivity support is available from Cisco VSG release 4.2(1)VSG1(3) or later and Cisco Nexus 1000V release 4.2(1)SV1(5) or later.

Q. How does Cisco VSG provide high availability?

A. To provide high availability, Cisco VSG can be installed in active-passive pairs. The Cisco Nexus 1000V Series vPath technology redirects packets to the secondary or standby Cisco VSG when the primary or active Cisco VSG is unavailable.

Q. Can Cisco VSG protect virtual machines on Virtual Extensible LAN (VXLAN)?

A. Yes. Cisco VSG extends zone-based firewall service to virtual machines on VXLAN, through updated segmentation features. VXLAN support is available from Cisco VSG release 4.2(1)VSG1(3) or later and Cisco Nexus 1000V release 4.2(1)SV1(5) or later.

Q. What is VXLAN?

A. Cloud computing requires support for large numbers of customers and applications and therefore demands even more scalable networks. In particular, each tenant, and each application within each tenant, requires its own network that is logically isolated from other networks. Because of this increased need for logical networks, Cisco introduced VXLAN in the Cisco Nexus 1000V Series to provide cloud networking. For more information, see the Cisco Nexus 1000V Series Switches Data Sheet.

Q. Where can I get more information about Cisco VSG?

A. Cisco VSG information and collateral are available at http://www.cisco.com/go/vsg.

Learn more about Cisco Prime Network Services Controller at http://www.cisco.com/go/services-controller.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C67-617356-02 06/13