# Cisco Virtual Security Gateway for Nexus 1000V Series Switch Release Notes, Release 4.2(1)VSG1(1)

**Updated: July 2, 2013**
**OL-23952-01 B0**

This document describes the features, limitations, and caveats for the Cisco Virtual Security Gateway and Cisco Virtual Network Management Center software. Use this document in combination with documents listed in the "Related Documentation" section on page 6. The following is the change history for this document.

| Part Number | Revision | Date | Description |
|---|---|---|---|
| OL-23952-01 | B0 | 04-25-11 | Added open caveat CSCto35433. |
| OL-23952-01 | A0 | 02-14-11 | Added information about open virtual appliance (OVA) file installation behavior in the"Limitations and Restrictions" section on page 4. |
| OL-23952-01 | | 01-31-11 | Created release notes for Release 4.2(1)VSG1(1). |

## Contents

This document includes the following sections:



**Americas Headquarters:**
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

# Introduction

The Cisco Virtual Security Gateway (VSG) for the Cisco Nexus 1000V Series switch is a virtual firewall appliance that provides trusted access to virtual data center and cloud environments with dynamic policy-driven operation, mobility-transparent enforcement, and scale-out deployment for dense multi-tenancy. The Cisco VSG provides a broad set of multi-tenant workloads that have varied security profiles to share a common compute infrastructure. The VSG, which associates one or more virtual machines into distinct trust zones, ensures that access to trust zones is controlled and monitored through established security policies.

The Cisco VSG and Cisco Nexus 1000V Virtual Ethernet Module provide the following benefits:

- Efficient deployment—Each Cisco VSG can protect virtual machines across multiple physical servers, which eliminates the need to deploy one virtual appliance per physical server.
- Performance optimization—By off-loading Fast-Path to one or more Cisco Nexus 1000V VEM vPath modules, the Cisco VSG enhances its performance through distributed vPath-based enforcement.
- Operational simplicity—You can insert a Cisco VSG in one-arm mode without creating multiple switches or temporarily migrating VMs to different switches or servers. Zone scaling is based on security profile, not on vNICs that are limited for virtual appliances.
- High availability—For each tenant, you can deploy a Cisco VSG in an active-standby mode to ensure a highly available operating environment in which vPath redirects packets to the standby Cisco VSG when the primary Cisco VSG is unavailable.
- Independent capacity planning—You can place a Cisco VSG on a dedicated server, that is controlled by your security operations team so that maximum compute capacity can be allocated to application workloads. Capacity planning can occur independently across server and security teams, and operational segregation across security, network, and server teams can be maintained.

# Software Compatibility

The servers that run the Cisco Nexus 1000V VSM and VEM must be listed in the VMware Hardware Compatibility list, which is a requirement for running the ESX 4.0 software.

For additional compatibility information, see the *Cisco Nexus 1000V Compatibility Information, Release 4.2(1)SV1(4)*.

# Features

This section provides the following information about the VSG features:

# Product Architecture

The Cisco VSG operates with the Cisco Nexus 1000V distributed virtual switch in the VMWare vSphere hypervisor. The Cisco VSG uses the virtual network service data path (vPath) that is embedded in the Cisco Nexus 1000V Virtual Ethernet module (VEM). vPath directs traffic, whether external-to-VM or VM-to-VM, to the Cisco VSG of a tenant. A split-processing model is applied where initial packet processing occurs in the Cisco VSG for policy evaluation and enforcement. After the policy decision is made, the Cisco VSG off-loads policy enforcement of the remaining packets to vPath.

vPath supports the following features:

- Intelligent interception and redirection—Tenant-aware flow classification and subsequent redirection to a designated VSG tenant
- Fast-Path offload—Per-tenant policy enforcement of flows off-loaded by VSG to vPath

# Trusted Multi-Tenant Access

You can transparently insert a Cisco VSG into the VMware vSphere environment where the Cisco Nexus 1000V distributed virtual switch is deployed. Upon insertion, one or more instances of the Cisco VSG is deployed on a per-tenant basis. This allows a highly scaled-out deployment across many tenants. Because tenants are isolated from each other, no traffic can cross tenant boundaries. Depending on the use case, you can deploy Cisco VSG at the tenant level, at the virtual data center (vDC) level, and at the vApp level.

**Note** Cisco VSG is not inherently multi-tenant. It must be explicit within each tenant.

As VMs are instantiated for a given tenant, association to security profiles and zone membership occurs immediately through binding with the Nexus 1000V port profile. Upon instantation, each VM is placed into a logical trust zone. Security profiles contain context-aware rule sets that specify access policies for traffic that enters and exits each zone. With the VM and network contexts, you can leverage custom attributes to define zones directly through security profiles. The profiles are applied to zone-to-zone traffic and external-to-zone/zone-to-external traffic. This enforcement occurs within a VLAN because a VLAN often identifies a tenant boundary.

The Cisco VSGs evaluate access control rules and then off-load enforcement to the Cisco Nexus 1000V VEM vPath module for performance optimization. Access is permitted or denied based on policies. Cisco VSG provides policy-based traffic monitoring capability and generates access logs.

# Dynamic (Virtualization-Aware) Operation

A virtualization environment is dynamic, where frequent additions, deletions, and changes occur across tenants and across VMs. Live migration of VMs can occur due to manual or programmatic vMotion events.

A Cisco VSG operates in conjunction with the Cisco Nexus 1000V (and vPath). This supports a dynamic VM environment. Typically, a tenant is created with the Cisco VSG (standalone or active-standby pair) and on the Cisco Virtual Network Management Center (VNMC). Associated security profiles are defined that include trust zone definitions and access control rules.

Each security profile is bound to a Cisco Nexus 1000V port profile (authored on the Cisco Nexus 1000V Virtual Supervisor Module and published to the VMWare Virtual Center). When a new VM is instantiated, you can assign appropriate port profiles to the virtual Ethernet port of the VM. Because the port profile uniquely refers to a security profile and VM zone membership, security controls are immediately applied. A VM can be repurposed by assigning a different port profile or security profile.

As vMotion events occur, VMs move across physical servers. The Cisco Nexus 1000V ensures that port profile policies and associated security profiles follow the VMs. Security enforcement and monitoring remain transparent to vMotion events.

## Setting Up VSG and VLAN Usages

A Cisco VSG is set up in an overlay fashion so that VMs can reach a Cisco VSG irrespective of its location. The vPath component in the Cisco Nexus 1000V VEM intercepts the packets from the VM and sends them to the Cisco VSG for further processing.

A Cisco VSG is configured with three vNICS that are each connected to one of the VLANs. The VLANs provide these functions:

- The Management VLAN connects management platforms such as the VMware vCenter, Cisco Virtual Network Management Center, Cisco Nexus 1000V VSM, and the managed Cisco VSGs.
- The Service VLAN provides communications between the Cisco Nexus 1000V VEM and Cisco VSGs. All Cisco VSGs are part of the Service VLAN. (The VEM uses this VLAN for interaction with Cisco VSGs.)
- The HA VLAN identifies the active and standby relationship.

You can allocate one or more VM Data VLAN(s) for VM-to-VM communications. In a multitenant environment, the Management VLAN is shared among all tenants. The Service VLAN, HA VLAN, and the VM Data VLAN are allocated on a per-tenant basis. When VLAN resources are scarce, you can use a single VLAN for Service and HA functions.

# Limitations and Restrictions

The Cisco VSG for Nexus 1000V Series switch has the following limitations and restrictions:

- For better performance, increase the MTU of all links between VEM and VSG by 74 bytes to accomodate packet encapsulation, which occurs during communication between vPath and VSG.
- Jumbo frame cannot configured for VSG management interface.
- Vmotion of VSG is validated for host upgrades only, not for DRS purposes.
- Enabling firewall protection on a router virtual machine might cause problems for policies based on VM attributes; firewall protection should only be enabled for end-point virtual machines.
- The VSG objects have these maximum numbers:

| VSG Objects | Limits |
|---|---|
| Rules per policy: 256 | 256 |
| Rules per VSN: 1024 | 1024 |
| Active policies: 32 | 32 |
| Object-groups per VSN: 64 | 64 |
| Zones per VSN: 32 | 32 |

| VSG Objects | Limits |
|---|---|
| Customer attributes per security profile: 16 | 16 |
| Concurrent connections: 256 K | 256 K |

- During the open virtual appliance (OVA) file installation, the following error message might be displayed:

```
The network card VirtualE1000 has dvPort backing, which is not supported. This could
be because the host does not support vDS, or because the host is not using vDS.
```

**Workaround**: Ensure that all three network interfaces in the Cisco VSG port profile are set to **VM Network** (port profile from vSwitch) during the OVA installation. After the virtual machine is created, change the port profile for the three interfaces according to the *Cisco Virtual Security Gateway, Release 4.2(1)VSG1(1) and Cisco Virtual Network Management Center, Release 1.0.1 Installation Guide*.

# Caveats

The following table provides descriptions of the open caveats for the Cisco VSG for the Nexus 1000V Series switch, Release 4.2(1)VSG1(1). The ID links you into the Cisco Bug Toolkit.

| ID | Open Caveat Headline |
|---|---|
| CSCtf94204 | Inconsistencies appear in the slot numbering when the show commands "show system internal redundancy" are run. |
| CSCtg97333 | "Clear counters interface data0" command on VSG is not working. |
| CSCth91644 | Wrong syslog is pushed when management interface IP is changed. |
| CSCti09598 | VNSP binding for same IP in two VLANs replaces  old value in VSG. |
| CSCti11925 | Policy-engine control debugs displayed information related to data-traffic. |
| CSCti26422 | VSG information displays as Nexus-Switch or Nexus1000VF in the CDP packet sent by VSG. |
| CSCti39155 | Virtual Machine IP addresses are not learned by the VEM and VSM if the virtual machine is protected by the firewall, and no traffic has been sent from the virtual machine. |
| CSCti58398 | Same policy-engine syslog is generated multiple times for a broadcast traffic. |
| CSCti85989 | Policy-engine syslog for IPv6 packet in VSG shows incorrect information. |
| CSCti89749 | VSG HA requires domain isolation for multi-tenant setups that share a management VLAN. |
| CSCtj55534 | After several switchovers, the standby may enter the bash prompt (rare). |

| ID | Open Caveat Headline |
|---|---|
| CSCtj83214 | Traffic from virtual machines using the vApp custom attribute are evaluated by the VSG policy engine in lower case (even if a rule in VSG is written with a vApp upper case value). |
| CSCtk01744 | Policy-engine statistics and the service-path statistics won't show the right information after system switchover. |
| CSCtk62117 | Time zone changes not pushed to VSG. |
| CSCtk62820 | "Unknown" (in red text) seen during OVA install. |
| CSCtk83021 | Remove unused “show” commands on VSG. |
| CSCtl03374 | Remove unused commands on VSG. |
| CSCtl86630 | Under certain circumstances, VSG license does not get released properly. If VEM does not have any VM which is protected by VSG, then VEM should not consume a VSG license. |
| CSCto35433 | Packet drops on vPath enabled VEM in the presence of VPC-HM |

# Related Documentation

This section contains information about the documentation available for Cisco Virtual Security Gateway and related products.

## Cisco Virtual Security Gateway Documentation

*The following Cisco Virtual Security Gateway for the Nexus 1000V Series Switch documents are available on Cisco.com at the following url:*

*http://www.cisco.com/en/US/products/ps13095/tsd_products_support_series_home.html*

- *Cisco Virtual Security Gateway for Nexus 1000V Series Switch Release Notes, Release 4.2(1)VSG1(1)*
- *Cisco Virtual Security Gateway, Release 4.2(1)VSG1(1) and Cisco Virtual Network Management Center, Release 1.0.1 Installation Guide*
- *Cisco Virtual Security Gateway for Nexus 1000V Series Switch License Configuration Guide, Release 4.2(1)VSG1(1)*
- *Cisco Virtual Security Gateway for Nexus 1000V Series Switch Configuration Guide, Release 4.2(1)VSG1(1)*
- *Cisco Virtual Security Gateway for Nexus 1000V Series Switch Command Reference, Release 4.2(1)VSG1(1)*
- *Cisco Virtual Security Gateway for Nexus 1000V Series Switch Troubleshooting Guide, Release 4.2(1)VSG1(1)*

**Send document comments to vsg-docfeedback@cisco.com.**

## Cisco Virtual Network Management Center Documentation

*The following Cisco Virtual Network Management Center documents are available on Cisco.com at the following url:*

*http://www.cisco.com/en/US/products/ps11213/tsd_products_support_series_home.html*

- *Release Notes for Cisco Virtual Network Management Center, Release 1.0.1*
- *Cisco Virtual Security Gateway, Release 4.2(1)VSG1(1) and Cisco Virtual Network Management Center, Release 1.0.1 Installation Guide*
- *Cisco Virtual Network Management Center CLI Configuration Guide, Release 1.0.1*
- *Cisco Virtual Network Management Center GUI Configuration Guide, Release 1.0.1*
- *Cisco Virtual Network Management Center XML API Reference Guide, Release 1.0.1*

## Cisco Nexus 1000V Series Switch Documentation

*The Cisco Nexus 1000V Series Switch documents are available on Cisco.com at the following url:*
*http://www.cisco.com/en/US/products/ps9902/tsd_products_support_series_home.html*

# Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.

---

This document is to be used in conjunction with the documents listed above.



Internet Protocol (IP) addresses used in this document are for illustration only. Examples, command display output, and figures are for illustration only. If an actual IP address appears in this document, it is coincidental.