



# Cisco Virtual Security Gateway for Microsoft Hyper-V Release Notes, Release 5.2(1)VSG1(4.1)

---

Release Date: June 3, 2013

Current Release: Cisco VSG Release 5.2(1)VSG1(4.1)

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-28942-01 |          | June 03, 2013 | Created release notes for Release 5.2(1)VSG1(4.1). |

## Contents

This document includes the following sections:

- [Introduction, page 2](#)
- [Software Compatibility, page 2](#)
- [Features, page 2](#)
- [Limitations and Restrictions, page 4](#)
- [Open Caveats—Cisco VSG Release 5.2\(1\)VSG1\(4.1\), page 6](#)
- [Related Documentation, page 6](#)
- [Obtaining Documentation and Submitting a Service Request, page 7](#)



# Introduction

The Cisco Virtual Security Gateway (VSG) for Microsoft Hyper-V platform 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 multitenancy. The Cisco VSG enables a broad set of multitenant workloads that have varied security profiles to share a common compute infrastructure. By associating one or more Virtual Machines into distinct trust zones, the Cisco VSG ensures that access to trust zones is controlled and monitored through established security policies.

Together, 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 offloading Fast-Path to one or more Cisco Nexus 1000V VEM vPath modules, the Cisco VSG boosts 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 with vPath redirecting 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, controlled by the 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 in the Microsoft Server Hardware Compatibility list, which is a requirement for running the Microsoft Hyper-V software.

For additional compatibility information, see the *Cisco Nexus 1000V Compatibility Information, Release 4.2(1)SV2(2.1)*.

## Features

This section provides the following information about this release:

- [Product Architecture, page 3](#)
- [Trusted Multitenant Access, page 3](#)
- [Dynamic \(Virtualization-Aware\) Operation, page 3](#)
- [Setting Up Cisco VSG and VLAN Usages, page 4](#)

## Product Architecture

The Cisco VSG operates with the Cisco Nexus 1000V distributed virtual switch in the Microsoft Hyper-V. The Cisco VSG leverages the virtual network service data path (vPath) that is embedded in the Cisco Nexus 1000V Virtual Ethernet module (VEM). vPath steers 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 remaining packets to vPath.

vPath supports the following features:

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

## Trusted Multitenant Access

You can transparently insert a Cisco VSG into the Microsoft Hyper-V 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, which 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, or at the vApp level.



Note

---

The Cisco VSG is not inherently multitenant. 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 Cisco Nexus 1000V port profile. Upon instantiation, 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. 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 offloads enforcement to the Cisco Nexus 1000V VEM vPath module for performance optimization. Access is permitted or denied based on policies. The 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 especially across VMs. Live migration of VMs can occur due to manual or programmatic VM motion events.

A Cisco VSG operates with the Cisco Nexus 1000V (and vPath), which 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 Microsoft SCVMM). 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 VM motion 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 VM motion events.

## Setting Up Cisco 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 VLAN functions are as follows:

- The Management VLAN connects management platforms such as the Microsoft SCVMM, 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 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 Virtual Security Gateway for Nexus 1000V Series switch has the following limitations and restrictions:

- Cisco VSG is supported on HyperV VEM via a layer 3 interface
  - If the layer 3 interface is configured via Virtual machine router (VM Router), then the VM Router should not be present on the same VEM host as the VSG protected virtual machines.
- SNMP is not supported on Cisco VSG on Nexus Cloud Services Platform.
- Jumbo frames cannot be configured for the Cisco VSG management interface.
- If the VSM is down when the Cisco VSG is powered on, the Cisco VSG continuously tries to reboot.
 

Workaround: To prevent this situation, configure the Service VLAN and the HA VLAN used by the Cisco VSG as **system vlan *vlan\_number*** in the uplink port profile.
- VSG on Microsoft Hyper-V does not support jumbo frames.
- Layer 3 Mode

- When the VEM communicates with the Cisco VSG in the Layer 3 mode, an additional header with 82 bytes is added to the original packet. The VEM does not support fragmentation in Layer 3 mode and the ports/network-elements (which carry vPath encapsulated packets) must be configured in such a way that the vPath overhead is accommodated. For example, if MTU values of client and server VMs and uplink are all 1500 bytes, set the uplink MTU to 1582 bytes.
  - When encapsulated traffic that is destined to a Cisco VSG is connected to a different subnet other than the virtual network adapter subnet, the VEM does not use the Hyper-V host routing table. Instead, the virtual network adapter initiates an ARP for the remote Cisco VSG IP addresses. You must configure the upstream router to respond by using the proxy ARP feature.
  - The VEM does not support a routing functionality and it is assumed that the upstream switch/router is configured with the proxy-ARP configuration.
- **Configuring a Rule with a Reset Action**

Configuring a rule with a reset action for the non-TCP/UDP protocol will result in dropped traffic. However, the syslog generated for this traffic shows that the action performed for the traffic is reset as shown below:

```
2011 June 16 07:19:56 VSG-Fw %POLICY_ENGINE-6-POLICY_LOOKUP_EVENT:
policy=ps-web@root/Tenant-A rule=pol-B/udp-rule@root/Tenant-A action=Reset
direction=ingress src.net.ip-address=172.31.2.107 dst.net.ip-address=172.31.2.101
net.protocol=1 net.ethertype=800
```

- Ensure that MAC spoofing is enabled for VSG data interface.

## Caveats

This section include the following topics:

- [Open Caveats—Cisco VSG Release 5.2\(1\)VSG1\(4.1\), page 6](#)

## Open Caveats—Cisco VSG Release 5.2(1)VSG1(4.1)

The following are descriptions of the caveats in Cisco Virtual Security Gateway for Microsoft Hyper-V, Release 5.2(1)VSG1(4.1). The ID links open the Cisco Bug Toolkit.

| ID                         | Open Caveat Headline  |
|----------------------------|---|
| <a href="#">CSCUh02928</a> | Logical Switch may get automatically removed from the host properties in VMM.                       |
| <a href="#">CSCUg18779</a> | User not able to set VSG data interface to up or down.  |
| <a href="#">CSCUg85088</a> | Show interface command on VSG results in "error: get_port_channel_info failed" error message.       |
| <a href="#">CSCUe55369</a> | Show interface command returns Data IP of VSG as Control0 IP.                                       |
| <a href="#">CSCUh03470</a> | Show system internal event-log all command returns error with no such event log file.               |
| <a href="#">CSCUh05236</a> | Terminal event-logs are seen on first session even after enabling event-logs on the second session. |
| <a href="#">CSCUg88821</a> | Changed VSG data0 MAC address on SCVMM does not reflect correctly on VSG.                           |
| <a href="#">CSCUg18779</a> | User not able to set VSG data interface to up or down state.  |
| <a href="#">CSCUh17265</a> | VM may get stuck in modifying state when user changes the port-profile.                             |
| <a href="#">CSCUh15723</a> | VSG enabled VEM module may be seen as unlicensed on VSM.  |
| <a href="#">CSCUh24743</a> | Log message is truncated when the rule, policy, or zone name is long.                               |

## 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/ps11208/tsd\\_products\\_support\\_model\\_home.html](http://www.cisco.com/en/US/products/ps11208/tsd_products_support_model_home.html)

- *Cisco Virtual Security Gateway, Release 5.2(1)VSG1(4.1) and Cisco Virtual Network Management Center, Release 2.0 Installation Guide*
- *Cisco Virtual Security Gateway for Microsoft Hyper-V License Configuration Guide, Release 5.2(1)VSG1(4.1)*

- *Cisco Virtual Security Gateway for Microsoft Hyper-V Configuration Guide, Release 5.2(1)VSG1(4.1)*
- *Cisco Virtual Security Gateway for Microsoft Hyper-V Command Reference, Release 5.2(1)VSG1(4.1)*
- *Cisco Virtual Security Gateway for Microsoft Hyper-V Troubleshooting Guide, Release 5.2(1)VSG1(4.1)*
- *Cisco vPath and vServices Reference Guide for Microsoft Hyper-V for Microsoft Hyper-V*

## 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](http://www.cisco.com/en/US/products/ps11213/tsd_products_support_series_home.html)

## 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](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, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: <http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html>.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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.

© 2013 Cisco Systems, Inc. All rights reserved.

