



Cisco Virtual Security Gateway for Cisco Nexus 1000V Series Switch Release Notes, Release 4.2(1)VSG1(4.1)

Release Date: August 21, 2012
Part Number: OL-27570-01
Current Release: Cisco VSG Release 4.2(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 12](#). The following is the change history for this document.

Part Number	Revision	Date	Description
OL-27570-01	E0	December 17, 2012	Added resolved caveats CSCud01427, CSCud01515, CSCud1879, and CSCud33791.
OL-27570-01	D0	November 2, 2012	Added open caveat CSCud01427.
OL-27570-01	C0	October 19, 2012	Added new features: <ul style="list-style-type: none">• Selective TCP state checks.• Configure vPath traffic to bypass the Cisco VSG nodes in a service chain, for traffic traversing between the inside and outside networks. Note The above features are supported for Cisco Nexus 1000V, Release 4.2(1)SV2(1.1) onwards.
OL-27570-01	B0	October 05, 2012	Added VSG Scalability Matrix, while deleting a table displaying limited VSG information from the Limitations and Restrictions topic.
OL-27570-01	A0	August 21, 2012	Created release notes for Release 4.2(1)VSG1(4.1).



Contents

This document includes the following sections:

- [Introduction, page 2](#)
- [Software Compatibility, page 3](#)
- [Features, page 3](#)
- [New and Changed Information, page 5](#)
- [Limitations and Restrictions, page 6](#)
- [VSG Scalability Matrix, page 8](#)
- [Open Caveats—Cisco VSG Release 4.2\(1\)VSG1\(4.1\), page 9](#)
- [Resolved Caveats—Cisco VSG Release 4.2\(1\)VSG1\(4.1\), page 11](#)
- [Related Documentation, page 12](#)
- [Obtaining Documentation and Submitting a Service Request, page 13](#)

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 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 VMware Hardware Compatibility list, which is a requirement for running the ESX 4.1 or 5.0 software.

For additional compatibility information, see the *Cisco Nexus 1000V Compatibility Information, Release 4.2(1)SVI(5.2)*.

Features

This section provides the following information about this release:

- [Product Architecture, page 3](#)
- [Trusted Multitenant Access, page 3](#)
- [Dynamic \(Virtualization-Aware\) Operation, page 4](#)
- [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 VMware vSphere hypervisor. 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 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, 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. 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 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 VMotion 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 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 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 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. In layer 2 mode 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.

New and Changed Information

This section describes the new and changed features for the Cisco Virtual Security Gateway for Nexus 1000V Series Switch, Release 4.2(1)VSG1(4.1).

New Software Features

- [Cisco vPath Service Chaining, page 5](#)
- [Selective TCP State Checks, page 5](#)
- [Service Node on VXLANs, page 5](#)
- [Multiple CPU Support, page 5](#)

Cisco vPath Service Chaining

Service chaining allows multiple service nodes to be included in a service path so that the packets that belong to a particular flow can pass through this service chain. Each service node in a chain uses the security profile specified in the **vservice** command for that node.

Cisco VSG Release 4.2(1)VSG1(4.1) supports service chaining that allows the packets on a flow to be directed to more than one service node. Cisco vPath service chaining allows two types of service nodes:

- Cisco VSG
- ASA 1000V



Note

You can configure the vPath traffic to bypass the Cisco VSG nodes in a service chain, to improve the network latency. This for only traffic traversing between the inside and outside networks, wherein only the Cisco ASA processes the traffic. This feature is supported for Cisco Nexus 1000V, Release 4.2(1)SV2(1.1) onwards.

Selective TCP State Checks

Cisco VSG Release 4.2(1)VSG1(4.1) supports the selective TCP state checks that can be configured to set the invalid-ack, seq-past-window, and window-variation parameters for the data packets.



Note

This feature is supported for Cisco Nexus 1000V, Release 4.2(1)SV2(1.1) onwards.

Service Node on VXLANs

Starting with Cisco VSG Release 4.2(1)VSG1(4.1), the virtual service node can be configured on a Virtual Extensible Local Area Network (VXLAN).

Multiple CPU Support

Starting with Cisco VSG Release 4.2(1)VSG1(4.1), Cisco VSG performance can be scaled up to two vCPUs.

Limitations and Restrictions

The Cisco Virtual Security Gateway for Nexus 1000V Series switch has the following limitations and restrictions:

- Jumbo frames cannot be configured for the Cisco VSG management interface.
- Vmotion of the Cisco VSG is validated for host upgrades only and not for DRS purposes.
- Enabling firewall protection on a router virtual machine may cause problems for policies based on VM attributes; firewall protection should be enabled only for end-point Virtual Machines.
- OVA Installation Behavior

During OVA installation, the following error message might be seen:

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 OVA installation. Once the virtual machine is created, the port profile for these three interfaces should be changed according to the *Cisco Virtual Security Gateway, Release 4.2(1)VSG1(2) and Cisco Virtual Network Management Center, Release 1.2 Installation and Upgrade Guide*.

- 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.

- Layer 2 Mode

When the VEM communicates with the Cisco VSG in the Layer 2 mode, an additional header with 74 bytes is added to the original packet. The VEM fragments the packet if it exceeds the uplink MTU.

For better performance, increase the MTU of all links between the VEM and the Cisco VSG by 74 bytes to account for packet encapsulation which occurs for communication between vPath and the Cisco VSG. For example, if the MTU values of the client and server VMs and uplink are all 1500 bytes, set the uplink MTU to 1574 bytes.

- Layer 3 Mode

- When the VEM communicates with the Cisco VSG in the Layer 3 mode, an additional header with 94 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 1594 bytes.
- If the jumbo frames are enabled in the network, make sure the MTU of the client and server VMs are 94 bytes smaller than the uplink. For example, if the uplink MTU is 9000 bytes, set the MTU of the client and server VMs to 8906 bytes.
- When encapsulated traffic that is destined to a Cisco VSG is connected to a different subnet other than the vmknic subnet, the VEM does not use the VMware host routing table. Instead, the vmknic 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 src.vm.name=sg-centos-vk-7 src.vm.host-name
=10.193.75.91 src.vm.os-fullname="red hat enterprise linux 5 (64-bit)"
dst.vm.cluster-name
="sg1-dc1-clu1 ankaa tenth" src.vm.cluster-name="sg1-dc1-clu1 ankaa tenth"
dst.vm.portprofile-name=access-3770-tenant-a
src.vm.portprofile-name=access-3770-tenant-a dst.zone.name=centos-zone@root/Tenant-A
src.zone.name=centos-zone@root/Tenant-A src.vm.os-hostname=(null)
src.vm.res-pool=(null)
```

- Cisco VSG CLI Session Timeout

The CLI session for the Cisco VSG version 1.3x that is newly deployed will time out after a period of five minutes of an inactivity. The CLI session time out does not work on Cisco VSG that has been upgraded from version 1.0x.

- On the Cisco VSG that is upgraded from version 1.0x, the show **running-config** will consist only of the following items:

```
- gold001-vsg01# sh run | i line|timeout
- line console
- gold001-vsg01#
```

As a workaround, when upgrade is done from 1.0x to 1.3 version of Cisco VSG, “exec-timeout 5” can be configured under “line console” and “line vty” command modes to enable a five minutes CLI session inactivity timeout.

- VM Name Display Length Limitation

VM names for VMs on ESX 4.1 hosts that exceed 21 characters are not displayed properly on the VSM. When you use a **show vservice** command that displays the port profile name, for example, the **show vservice port brief port-profile port-profile-name** command, only VMs with names that are 21 characters or less are displayed correctly. Longer VM names may cause the VM name to be truncated, or extra characters to be appended to the VM name. Depending on the network adapter, the name length limitation may vary. For example:

- The E1000 or VMXNET 2 network adapters allow 26-character names. At 27 characters, the word ‘.eth’ is appended to the VM name. With each addition to the VM name, a character is truncated from the word ‘.eth’. After 31 characters, the VM name is truncated.
- The VMXNET 3 network adapters allow 21-character names. At 22 characters, the word ‘ethernet’ is appended to the VM name. With each addition to the VM name, a character is truncated from the word ‘ ethernet’. After 30 characters, the VM name is truncated.

Workaround: This is a display issue with ESX Release 4.1 only. Use VM names of 21 characters or less to avoid this issue.

VSG Scalability Matrix

The following table presents a feature-based comparative analysis between two VSGs having different number of virtual CPUs and VNMC:

Feature	VSG 1vCPU	VSG 2vCPU	VNMC
Number of VSGs	N/A	N/A	128
Concurrent Connections	256,000	256,000	N/A
New Connections Per Second	6,000	10,000	N/A
Tenants	N/A	N/A	128
Zones	64	64	8192
Security Profiles	256	256	2048
Policies	32	32	2048
Rules	1024	1024	8192
Max VSM	N/A	N/A	16
Object Groups	64	64	4096
Number of Hosts/VEMs	64	64	600

Caveats

This section include the following topics:

- [Open Caveats—Cisco VSG Release 4.2\(1\)VSG1\(4.1\), page 9](#)
- [Open Caveats—Cisco VSG Release 4.2\(1\)VSG1\(3.1\), page 9](#)
- [Resolved Caveats—Cisco VSG Release 4.2\(1\)VSG1\(4.1\), page 11](#)

Open Caveats—Cisco VSG Release 4.2(1)VSG1(4.1)

The following are descriptions of the caveats in Cisco Virtual Security Gateway for Nexus 1000V Series switch, Release 4.2(1)VSG1(4.1). The ID links open the Cisco Bug Toolkit.

ID	Open Caveat Headline
CSCtz65376	vPath 1.0 Virtual Service Nodes (VSN) do not support ping from hosts that do not have any vservices enabled.
CSCua13358	Zones are not classified for VM virtual Ethernet interfaces with multiple IP addresses.
CSCua89446	The show vsg ip-binding command momentarily displays the default security profile for a VM when the port profile for a different VM is changed.
CSCua90554	The number of entries displayed by the show service-path connection command does not match the active connections displayed by the show service-path statistics command.
CSCua90578	The license not checked in after a crash and restart.

Open Caveats—Cisco VSG Release 4.2(1)VSG1(3.1)

The following are descriptions of the caveats in Cisco Virtual Security Gateway for Nexus 1000V Series switch, Release 4.2(1)VSG1(3.1). The ID links open 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.
CSCth91644	The wrong syslog is pushed when the management interface IP is changed.
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.
CSCti89749	The Cisco VSG HA requires domain isolation for multitenant setups that share a management VLAN.
CSCtk01744	Policy-engine statistics and the service-path statistics do not show the correct information after a system switchover.
CSCto89854	VMs under tenants disappear and reappear.
CSCto97454	TCP Checks: Downloading of a file stops during/after VMotion.

ID	Open Caveat Headline
CSCtr01200	Failure occurs when copying the running configuration to the startup configuration with 1024 rules and 16 conditions each.
CSCtx49694	The show vsn connection command output may show inconsistent information for ping traffic with bidirectional traffic.

Resolved Caveats—Cisco VSG Release 4.2(1)VSG1(4.1)

The following table describes the resolved caveats in Cisco Virtual Security Gateway for Nexus 1000V Series switch, Release 4.2(1)VSG1(4.1). The ID links open the Cisco Bug Toolkit.

ID	Resolved Caveat Headline
CSCtq76511	The show command displays incorrect policy and offload flags during flooding.
CSCua89127	The show vservice statistics command does not display statistics when the Cisco VSG is in a VXLAN.
CSCua99983	The show vservice port brief command displays incorrect Profile(Id) when port profile is changed to a non-existent org.
CSCub02848	When using VSG in both I2 and I3 mode, the incorrect mac address is used for encapsulated traffic, which results in traffic failure.
CSCub03360	The show vservice brief node-I3 command displays the same result as the show vservice brief command.
CSCub07106	Changes are not rolled back after a port is shut down.
CSCub08115	Zone classification issues when the cluster name is changed in VMware vCenter.
CSCub55163	After failover from a primary VM with Fault Tolerance (FT) to a secondary VM, the ip-binding learned from the primary VM is deleted.
CSCtr56196	The show license usage command displays incorrect information after port profile edit.
CSCtu22546	The show service-path connection command output does not show the VXLAN number.
CSCtg97333	The clear counters interface data0 command on the Cisco VSG is not working.
CSCti11925	Policy-engine control debugs displayed information related to the data traffic.
CSCtq44369	The show service-path connection command does not show the connection details on the destination module for a VEM to VEM connection.
CSCtr50316	Port profile org root to default SP (root) is showing as “Org not configured in Port profile”.
CSCtu18273	The show vsn connection command shows wrong information.
CSCtx08323	VNSP ID is retained even after the SP at root node is deleted from the VNMC.
CSCtx14556	The PA installation is successful with feature http_only enable and https disabled.

ID	Resolved Caveat Headline
CSCty18248	After upgrading the Cisco VSG from Release 4.2(1)VSG1(2) to Release 4.2(1)VSG1(3.1) using the install all command , any changes to the VSG configuration that are done at the Cisco VNMC do not get applied to the Cisco VSG.
CSCty33854	Zone classification may get evaluated incorrectly in a case where IP-binding is not learned before traffic reaches Cisco VSG.
CSCua59482	Traffic was being redirected to the incorrect Cisco VSG.
CSCud01427	The VSM/VEM licensing for Cisco VSG enters an unlicensed mode after you upgrade from Cisco Nexus 1000V Series switch Release 4.2(1) SV1(5.1) or Release 4.2(1) SV1(5.1a) to Release 4.2(1) SV1(5.2).
CSCud01515	A Cisco Nexus 1000V Series switch should fail close when no license is installed for Cisco VSG.
CSCud18794	PSOD related to a Cisco Nexus 1000V Series switch occurred on the ESXi host.
CSCud33791	A duplicate IP event is detected in Windows 2008 VMs in vPath when the network adapter flaps.

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(4)*
- *Cisco Virtual Security Gateway, Release 4.2(1)VSG1(4) and Cisco Virtual Network Management Center, Release 2.0 Installation and Upgrade Guide*
- *Cisco Virtual Security Gateway for Nexus 1000V Series Switch License Configuration Guide, Release 4.2(1)VSG1(4)*
- *Cisco Virtual Security Gateway for Nexus 1000V Series Switch Configuration Guide, Release 4.2(1)VSG1(4)*
- *Cisco Virtual Security Gateway for Nexus 1000V Series Switch Command Reference, Release 4.2(1)VSG1(4)*
- *Cisco Virtual Security Gateway for Nexus 1000V Series Switch Troubleshooting Guide, Release 4.2(1)VSG1(4)*

- *Cisco vPath and vServices Reference Guide*

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

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, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see [What's New in Cisco Product Documentation](#).

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the [What's New in Cisco Product Documentation RSS feed](#). 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. 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.

© 2012 Cisco Systems, Inc. All rights reserved.

