Cisco Virtual Security Gateway for VMware vSphere Release Notes, Release 5.2(1)VSG2(1.2)

Release Date: August 22, 2014
Current Release: Release 5.2(1)VSG2(1.2)

This document describes the features, limitations, and caveats for Cisco Virtual Security Gateway and Cisco Prime Network Services Controller (Prime NSC) software. Use this document in combination with documents listed in the "Related Documentation" section on page 11. The following is the change history for this document.

Date	Description
June 22, 2013	Created release notes for Release 4.2(1)VSG2(1.1).
October 08, 2013	Updated release notes for open caveats for Release 4.2(1)VSG2(1.1).
Jan 31, 2014	Updated release notes for open and resolved caveats for Release 4.2(1)VSG2(1.1). Added support for VMware vSphere 5.5. Added support for Universal licensing.
August 22, 2014	Updated release notes for open and resolved caveats for Release 5.2(1)VSG2(1.2). Added support for L3 fragmentation on VSM.

Contents

This document includes the following sections:

Cisco Systems, Inc.
www.cisco.com

Introduction

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. 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, Cisco VSG ensures that access to trust zones is controlled and monitored through established security policies.

Together, 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, Cisco VSG boosts its performance through distributed vPath-based enforcement.
- Operational simplicity—You can insert 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 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 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/ESXi 5.5, 5.1, and 5.0 software.

For additional compatibility information, see the *Cisco Nexus 1000V Compatibility Information*.

VSG License

Cisco VSG license is integrated with the Nexus1000V Multi-Hypervisor License (Universal License). You need to install the Nexus1000V Multi-Hypervisor License for Cisco VSG for VMware vSphere. When the Nexus1000V Multi-Hypervisor License is installed, the license for Cisco VSG is automatically included.

The Cisco N1kv VSM is available in two modes: essential and advanced. VSG functionality is available only in the advanced mode. You need to install the Nexus1000V Multi-Hypervisor License and change the VSM mode to advanced mode.

Note If you try to access VSG services with VSM in essential mode, an error message is generated on VSM console indicating that the Nexus1000V Multi-Hypervisor License is required for VSG.

For more information about the Cisco Nexus 1000V for VMware vSphere licenses, see the *Cisco Nexus 1000V for VMware vSphere License Configuration Guide*.

Features

This section provides the following information about this release:

Product Architecture

Cisco VSG operates with the Cisco Nexus 1000V distributed virtual switch in the VMware vSphere hypervisor. 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 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 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 Cisco VSG is not inherently multitenant. It must be explicit within each tenant.

Since the 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 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 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 Prime NSC. 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 Prime NSC, 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 VMware vSphere, Release 5.2(1)VSG2(1.2).

Support for Fragmentation in Layer 3 Mode

The Cisco VSG now supports fragmentation in Layer 3(L3) mode. You can enable L3 fragmentation on VSM by using the **l3-fragment** command. Use the no form of this command to disable L3 fragmentation. When L3 fragmentation is enabled, you not need increase the uplink MTU (1500) for the additional vPath overhead. By default the L3 fragmentation is disabled on VSM. If the L3 fragmentation is disabled, you need to increase the uplink MTU to 1582 bytes for the additional vPath overhead.

VSG Models

The Cisco VSG is available in three different models based on the memory, number of virtual CPUs, and CPU speed. The following table lists the available Cisco VSG models.

VSG Models	Small	Medium	Large
Memory	2 Gb	2 Gb	2 Gb
CPU Speed	1.0 GHz	1.5 GHz	1.5 GHz
Number of Virtual CPUs	1	1	2

Condition Match Criteria for a Rule or Zone

Cisco VSG supports specifying a condition match criteria for a rule or zone. You can specify if all conditions should be true or at least one condition from a column should be true.

Support for VMware vSphere 5.5

Cisco VSG now supports VMware vSphere Release 5.5 with VMware ESXi.

Limitations and Restrictions

The Cisco Virtual Security Gateway for VMware vSphere has the following limitations and restrictions:

- If VSG version 5.2(1)VSG2(1.2) is used with Nexus 1000V, Release 5.2.(1)SV3(1.1), the max limits for N1kV are reduced to following:
  - 128 host per DVS.
  - 6000 vEthernet protected ports.
  - 512 ports per host.
- The Cisco VSG does not support multiple user accounts. It supports only the default **admin** user account.

- Jumbo frames cannot be configured for the Cisco VSG management interface.
- VMotion of the Cisco VSG is validated only for host upgrades 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. After the virtual machine is created, the port profile for these three interfaces should be changed according to the *Cisco VSG for VMware vSphere, Release 5.2(1)VSG2(1.2) and Cisco Prime NSC, Release 3.2.2b 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 62 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 62 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 1562 bytes.
- Layer 3 Mode
  - If the jumbo frames are enabled in the network, make sure the MTU of the client and server VMs are 82 bytes smaller than the uplink. For example, if the uplink MTU is 9000 bytes, set the MTU of the client and server VMs to 8918 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 in the following example:

```
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 Prime NSC:

Feature	VSG 1vCPU	VSG 2vCPU	Prime NSC
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	512	512	8,192
Security Profiles	256	256	2,048
Policies	64	64	2,048

Feature	VSG 1vCPU	VSG 2vCPU	Prime NSC
Rules	1,024	1,024	15,360
Max VSM	N/A	N/A	16
Object Groups	512	512	64K
Number of Hosts/VEMs	128	128	600

Note If VSG version 5.2(1)VSG2(1.2) is used with Nexus 1000V, Release 5.2.(1)SV3(1.1), the max limits for N1kV are reduced to following:

- 128 host per DVS.
- 6000 vEthernet protected ports.
- 512 ports per host.

Caveats

This section include the following topics:

Open Caveats—Cisco VSG Release 5.2(1)VSG2(1.2)

The following are descriptions of the caveats in Cisco Virtual Security Gateway for VMware vSphere, Release 5.2(1)VSG2(1.2). The ID links open the Cisco Bug Toolkit.

ID	Open Caveat Headline
CSCuq25165	ESXi crashes when added to Nk1v Switch.
CSCuq45489	Traffic drops after VSM switch-over and reload operation with un-used duplicate port-profiles.
CSCuq49025	VNS Agent crashes when **show vservice brief node-l3** command is run.

Open Caveats—Cisco VSG Release 4.2(1)VSG2(1.1)

The following are descriptions of the caveats in Cisco Virtual Security Gateway for VMware vSphere, Release 4.2(1)VSG2(1.1). The ID links open the Cisco Bug Toolkit.

ID	Open Caveat Headline
CSCth44688	Transaction-Per-Second value comes down for rules with action log.
CSCtz95541	Restarting VNMC puts 64 VSGs in the Failed-to-Apply state.
CSCua15679	All VM attributes are pushed to VSG when one of the attributes of a VM is changed.
CSCua77931	VNMC IP change issue.
CSCud11612	Different sizes for primary and secondary VSGs are not supported.
CSCud12188	Image upgrade from one VSG model to the other VSG model is not supported.
CSCug04393	Error when using the VSG ISSU upgrade option.

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

The following are descriptions of the caveats in Cisco Virtual Security Gateway for VMware vSphere, 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.
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.

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

The following are descriptions of the caveats in Cisco Virtual Security Gateway for VMware vSphere, 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.
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.
CSCtx49694	The **show vsn connection** command output may show inconsistent information for ping traffic with bidirectional traffic.

Resolved Caveats—Cisco VSG Release 5.2(1)VSG2(1.2)

The following table describes the resolved caveats in Cisco Virtual Security Gateway for VMware vSphere, Release 5.2(1)VSG2(1.2). The ID links open the Cisco Bug Toolkit.

ID	Resolved Caveat Headline
CSCun20852	Observed PSOD on ESX host 5.5 with fragmented traffic.
CSCuo43883	VSG becomes unresponsive due to **show tech-support** command.
CSCuo91202	Performance degrades with multiple profiles and broadcast/multicast packets.
CSCup22419	Multiple Vulnerabilities in OpenSSL.
CSCum64759	VSG trap for cefcPowerStatusChange doesn't reflect power status.
CSCuj56354	Policy Engine crashes during switchover if the VSG is configured with custom based attributes condition.

Resolved Caveats—Cisco VSG Release 4.2(1)VSG2(1.1)

The following table describes the resolved caveats in Cisco Virtual Security Gateway for VMware vSphere, Release 4.2(1)VSG2(1.1). The ID links open the Cisco Bug Toolkit.

ID	Resolved Caveat Headline
CSCtr01200	Failure occurs when copying the running configuration to the startup configuration with 1024 rules and 16 conditions each.
CSCua90578	The license not checked in after a crash and restart.
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.
CSCua13358	Zones are not classified for VM virtual Ethernet interfaces with multiple IP addresses.

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 VMware vSphere 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 VMware vSphere Release Notes, Release 5.2(1)VSG2(1.2)*
- *Cisco VSG for VMware vSphere, Release 5.2(1)VSG2(1.2) and Cisco Prime NSC, Release 3.2.2b Installation and Upgrade Guide*
- *Cisco Virtual Security Gateway for VMware vSphere Configuration Guide, Release 5.2(1)VSG2(1.2)*
- *Cisco Virtual Security Gateway for VMware vSphere Command Reference, Release 5.2(1)VSG2(1.2)*
- *Cisco Virtual Security Gateway for VMware vSphere Troubleshooting Guide, Release 5.2(1)VSG2(1.2)*
- *Cisco vPath and vServices Reference Guide for VMware vSphere*

Cisco Prime Network Services Controller Documentation

The following Cisco Prime Network Services Controller (Prime NSC) documents are available on Cisco.com at the following URL:

http://www.cisco.com/en/US/docs/net_mgmt/prime/network_services_controller/3.2/doc-overview/Cisco_Prime_Network_Svcs_Contoller_32_doc_overview.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* 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.