Cisco Virtual Security Gateway for VMware vSphere Release Notes, Release 5.2(1)VSG2(2.2)

First Published: 01-25-2018

This document describes the features, limitations, and bugs for the Cisco Virtual Security Gateway (Cisco VSG) software. Use this document in combination with documents listed in Related Documentation, page 9. The following is the change history for this document.

Date	Description
01-25-2018	Created release notes for Release 5.2(1)VSG2(2.2).

Contents

This document includes the following sections:

Cisco Systems, Inc.
www.cisco.com

Introduction

Cisco 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 (VMs) into distinct trust zones, Cisco VSG ensures that access to trust zones is controlled and monitored through established security policies.

Together, Cisco VSG and the Cisco Nexus 1000V Virtual Ethernet Module (VEM) provide the following benefits:

- Efficient deployment—Each Cisco VSG can protect VMs 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 Cisco 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 Cisco 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 Virtual Supervisor Module (VSM) and VEM must be in the VMware Hardware Compatibility list, which is a requirement for running the ESX/ESXi 5.5, 6.0, 6.5a software. See the *Cisco Nexus 1000V and VMware Compatibility Information*.

Cisco VSG is installed on the Cisco Nexus 1000V switch and is managed using Cisco PNSC. For compatibility among the various releases of Cisco VSG, Cisco PNSC, and Cisco Nexus 1000V, see the Cisco VSG Environment Upgrade Matrix and Path.

Cisco VSG License

The Cisco VSG license is integrated with the Cisco Nexus 1000V Multi-Hypervisor License (Universal License). You must install the Cisco Nexus 1000V Multi-Hypervisor License for Cisco VSG for VMware vSphere. When the Cisco Nexus 1000V Multi-Hypervisor License is installed, the license for Cisco VSG is included automatically.

Two licenses are available for use with the Cisco Nexus 1000V switch: Essentials Edition and Advanced Edition. Cisco VSG functionality is available only with the Advanced Edition. You must install the Advanced Edition license and then configure the VSM mode to advanced mode to use the Advanced Edition license.

The Cisco Nexus 1000V VSM is available in two modes: essential and advanced. Cisco VSG functionality is available only in the advanced mode. You must install the Cisco Nexus 1000V Multi-Hypervisor License and change the VSM mode to advanced mode.

Note If you try to access Cisco VSG services on the Cisco Nexus 1000V switch with the Essentials Edition license enabled, an error message is generated on the VSM console indicating that the Cisco Nexus 1000V Multi-Hypervisor License is required for Cisco VSG.

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

Features

This section describes the key features of Cisco VSG.

Product Architecture

Cisco VSG operates with the Cisco Nexus 1000V distributed virtual switch in the VMware vSphere hypervisor. Cisco VSG leverages the Cisco virtual network service data path (vPath) that is embedded in the Cisco Nexus 1000V VEM. Cisco 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, Cisco VSG offloads policy enforcement of the remaining packets to Cisco vPath.

Cisco vPath supports:

- 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 Cisco 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 Cisco VSG instances are 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 virtual Application (vApp) level.

Note Cisco VSG is not inherently multitenant; you must configure it within each tenant.

Because 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 in 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.

Cisco VSG evaluates 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. 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.

Cisco VSG operates with the Cisco Nexus 1000V (and Cisco vPath), which supports a dynamic VM environment. Typically, a tenant is created with Cisco VSG (in a standalone or active-standby pair) and on Cisco PNSC. 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 (configured on the Cisco Nexus 1000V VSM 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

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

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 PNSC, Cisco Nexus 1000V VSM, and the managed Cisco VSGs.
- The Service VLAN provides communication 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 communication. In a multitenant environment, the management VLAN is shared among all tenants. The service VLAN, HA VLAN, and 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.

Support for Fragmentation in Layer 3 Mode

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

Cisco VSG Models

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

Cisco 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 Cisco VSG ISSU Upgrade

Starting with Cisco Nexus 1000V Release 5.2(1)SV3(1.1), you can upgrade Cisco VSG using the kickstart and system files.

Support for VMware vSphere 6.5a

Cisco VSG supports VMware vSphere Release 6.5a with VMware ESXi.

New and Changed Information

No new features are introduced for Cisco VSG for VMware vSphere, Release 5.2(1)VSG2(2.2).

Limitations and Restrictions

Cisco VSG for VMware vSphere has the following limitations and restrictions:

- If Cisco VSG Release 5.2(1)VSG2(1.3) or later is used with the Cisco Nexus 1000V Release 5.2.(1)SV3(1.3), the maximum limits for Cisco Nexus 1000V are reduced to the following:

  - 250 hosts per DVS.
  - 10,000 vEth ports with up to 6000 vEth ports protected by Cisco VSG.
- Cisco VSG supports only 512 ports per DVS.
- 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 might cause problems for policies based on VM attributes. Firewall protection should be enabled only for endpoint virtual machines.
- During OVA installation, the following error message might occur:

  ```
  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 VM 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(2.1) and Cisco PNSC, Release 3.4.2b Installation and Upgrade Guide*.
- If the VSM is down when Cisco VSG is powered on, Cisco VSG continuously tries to reboot.

  Workaround: To prevent this situation, configure the service VLAN and the HA VLAN used by 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 Cisco 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 jumbo frames are enabled in the network, make sure the MTU of the client and server VMs is 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 results 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 Release 1.3x that is newly deployed times out after 5 minutes of inactivity. The CLI session timeout does not work on Cisco VSG that has been upgraded from Release 1.0x.

  - On Cisco VSG that is upgraded from Release 1.0x, the **show running-config** consists only of the following lines:

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

  As a workaround, when you are done upgrading from Cisco VSG Release 5.2(1)VSG2(1.x) to 5.2(1)VSG2(1.3) or later, you can enable a 5-minute CLI session inactivity timeout by configuring the **exec-timeout 5** command in the line console and line vty command modes.

- VM Name Display Length Limitation

  VM names for VMs on ESX 4.1 hosts that exceed 21 characters are not displayed correctly 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 fewer display correctly. Longer VM names might truncate or append extra characters. Depending on the network adapter, the name length limitation varies. 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 fewer to avoid this issue.

Cisco VSG Scalability Matrix

The following table compares two Cisco VSGs with a different number of virtual CPUs and Cisco PNSC.

Feature	Cisco VSG 1vCPU	Cisco VSG 2vCPU	Cisco PNSC
Number of Cisco VSGs	N/A	N/A	128
Concurrent connections	256,000	256,000	N/A
New connections per second	Up to 6000	Up to 10,000	N/A
Tenants	N/A	N/A	128
Zones	512	512	8192

Feature	Cisco VSG 1vCPU	Cisco VSG 2vCPU	Cisco PNSC
Security profiles	256	256	2048
Policies	64	64	2048
Rules	1024	1024	15,360
Max VSM	N/A	N/A	16
Object groups	512	512	64,000
Number of hosts/VEMs	128	128	600
Number of protected ports/Cisco VSG	512 (on the same host or across multiple hosts)	512 (on the same host or across multiple hosts)	N/A

Bugs

The bugs are accessible through the Cisco Bug Search Tool. This web-based tool provides you with access to the Cisco bug tracking system, which maintains information about bugs and vulnerabilities in this product and other Cisco hardware and software products.

For more information about the Cisco Bug Search Tool, see the Bug Search Tool Help & FAQ.

Using the Bug Search Tool

Use the Bug Search Tool to search for a specific bug or to search for all bugs in a release.

Step 1 Go to Cisco Bug Search Tool.

Step 2 In the **Log In** screen, enter your registered Cisco.com username and password, and then click **Log In**. The Bug Search page opens.

Note If you do not have a Cisco.com username and password, you can register for them at http://tools.cisco.com/RPF/register/register.do.

Step 3 To search for a specific bug, enter the bug ID in the Search For field and press **Enter**.

Step 4 To search for bugs in the current release:

a. In the Search For field, enter appropriate release name and press **Enter**. (Leave the other fields empty.)

b. When the search results are displayed, use the filter tools to find the types of bugs you are looking for. You can search for bugs by status, severity, modified date, and so forth.

Tip To export the results to a spreadsheet, click the **Export Results to Excel** link.

Open Bugs—Cisco VSG Release 5.2(1)VSG2(2.2)

The following table lists the open bugs in Cisco VSG Release 5.2(1)VSG2(2.2).

ID	Headline
CSCvb84497	Cleanup or modification of authorization methods on PNSC are not updated on VSG.

Resolved Bugs—Cisco VSG Release 5.2(1)VSG2(2.2)

There are no resolved bugs in Cisco VSG Release 5.2(1)VSG2(2.2).

Related Documentation

This section contains information about the documentation available for Cisco VSG and related products.

Cisco Virtual Security Gateway Documentation

The Cisco VSG documentation is available at the following URL:

http://www.cisco.com/c/en/us/support/switches/virtual-security-gateway/tsd-products-support-series-home.html

Cisco Prime Network Services Controller Documentation

The Cisco Prime Network Services Controller documentation is available at the following URL:

http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-network-services-controller/tsd-products-support-series-home.html

Cisco Nexus 1000V Series Switch Documentation

The Cisco Nexus 1000V Switch for VMware vSphere documentation is available at the following URL:

http://www.cisco.com/c/en/us/support/switches/nexus-1000v-switch-vmware-vsphere/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 delivers content directly to your desktop using a reader application. The RSS feeds are a free service.