Cisco Virtual Security Gateway for KVM Release Notes, Release 5.2(1)VSG2(1.3)

First Published: May 26, 2015

This document describes the features, limitations, and caveats for Cisco Virtual Security Gateway (VSG) and Cisco Prime Network Services Controller (PNSC) software for KVM. Use this document in combination with documents listed in the Related Documentation, page 8. The following is the change history for this document.

Date	Description
May 26, 2015	Created release notes for Release 5.2(1)VSG2(1.3).

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 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 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 Cisco Nexus 1000V VSM and VEM must be running in Red Hat Enterprise Linux (RHEL), OSP 6.0.

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

VSG License

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

The Cisco Nexus 1000V VSM is available in two modes: essential and advanced. VSG functionality is available only in the advanced mode. You need to install the Cisco Nexus 1000V 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 the VSM console indicating that the Cisco Nexus 1000V Multi-Hypervisor License is required for VSG.

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 RHEL OSP6 hypervisor. Cisco VSG leverages the virtual network service data path (vPath) that is embedded in the Cisco Nexus 1000V VEM. The 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, the Cisco VSG off-loads policy enforcement of remaining packets to Cisco vPath.

The Cisco 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 KVM 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 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 (authored on the Cisco Nexus 1000V Virtual Supervisor Module. 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 Cisco PNSC, 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.

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 two 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	Large
Memory	2 Gb	2 Gb
CPU speed	1.0 GHz	1.5 GHz
Number of virtual CPUs	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.

Limitations and Restrictions

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

- If VSG version 5.2(1)VSG2(1.3) is used with Nexus 1000V, Release 5.2.(1)SV3(1.3), the max limits for Cisco Nexus 1000V are reduced to following:
  - 250 host per DVS.
  - 10,000 vEth ports with up to 6000 vEth ports protected by VSG.
  - 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.
- 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 KVM 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 that is newly deployed will time out after a period of five minutes of an inactivity.

  - 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 KVM 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: 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 with a different number of virtual CPUs and Cisco PNSC.

Feature	VSG 1 vCPU	VSG 2 vCPU	PNSC
Number of VSGs	—	—	128
Concurrent connections	256,000	256,000	—
New connections per second	Up to 6,000	Up to 10,000	—
Tenants	—	—	128
Zones	512	512	8,192
Security profiles	256	256	2,048
Policies	64	64	2,048
Rules	1,024	1,024	15,360
Max VSM	—	—	16
Object groups	512	512	64K
Number of hosts/VEMs	128	128	600

If VSG Release 5.2(1)VSG2(1.3) is used with Cisco Nexus 1000V Release 5.2.(1)SV3(1.4), the maximum limits for Cisco Nexus 1000V are reduced to following:

- 250 host per DVS.
- 10,000 vEth ports with up to 6000 vEth ports protected by VSG.
- 512 ports per host.

Caveats

Caveats 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

This topic explains how to 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 the 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 Caveats

The following table describes the open caveats in Cisco VSG Release 5.2(1)VSG2(1.3).

ID	Headline
CSCut77418	NTPd related vulnerabilities.
CSCuu30603	VSG running with 1 vCPU might cause a CPU spike.
CSCuu36018	VSG Management and Data IP addresses are not reachable after switchover from VSG primary to VSG secondary.

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 documents are available:

- *Cisco VSG for KVM, Release 5.2(1)VSG2(1.3) and Cisco Prime NSC, Release 3.4.1b Installation Guide*
- *Cisco Virtual Security Gateway for KVM Configuration Guide, Release 5.2(1)VSG2(1.3)*
- *Cisco Virtual Security Gateway for KVM Troubleshooting Guide, Release 5.2(1)VSG2(1.3)*

Cisco Prime Network Services Controller Documentation

The Cisco Prime Network Services Controller (PNSC) documents are 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 Series Switch documents are 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.