Cisco Virtual Security Gateway for Nexus 1000V Series Switch Release Notes, Release 4.2(1)VSG1(2)

Updated: July 3, 2013
OL-25347-01

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 7. The following is the change history for this document.

Part Number	Revision	Date	Description
OL-25347-01	A0	08-11-11	Added Caveat CSCto35433 and limitation and workaround for Cisco VSG continuously rebooting if powered on when VSM is down.
OL-25347-01	New	07-28-11	Created release notes for Release 4.2(1)VSG1(2).

Contents

This document includes the following sections:

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

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 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 4.0 software.

For additional compatibility information, see the *Cisco Nexus 1000V Compatibility Information, Release 4.2(1)SV1(4a)*.

Features

This section provides the following information about this release:

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 VSG tenant
- Fast-Path offload—Per-tenant policy enforcement of flows offloaded by the Cisco VSG to vPath

Trusted Multi-Tenant 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. This 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, as well as 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 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. 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 in conjunction with the Cisco Nexus 1000V (and vPath). This 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 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:

- 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. (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(2).

- TCP state-checks—Enabled by default, performs TCP state-checks on the vPath. See the *Cisco Virtual Security Gateway for Nexus 1000V Series Switch Configuration Guide, Release 4.2(1)VSG1(2)*, for more information.
- vPath Ping—Verifies the connectivity and reachability of the Cisco VSG VSNs in the vPath.

New Software Features

The Cisco VSG software is now available bundled as an optional application on the Nexus 1010 network services appliance as a virtual service blade (VSB).

Limitations and Restrictions

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

- For better performance, increase the MTU of all links between VEM and the Cisco VSG by 74 bytes to account for packet encapsulation which occurs for communication between vPath and the Cisco VSG.
- 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 router virtual machine may cause problems for policies based on VM attributes; firewall protection should be enabled only for end-point Virtual Machines.
- The maximum numbers for Cisco VSG objects are as follows:

Cisco VSG Objects	Limits
Rules per policy: 256	256
Rules per VSN: 1024	1024
Active policies: 32	32
Object-groups per VSN: 64	64
Zones per VSN: 32	32
Customer attributes per security profile: 16	16
Concurrent connections: 256K	256K

- OVA Installation Behavior

  During OVA installation, the following error message may 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 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 will continuously try 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.

Open Caveats

The following are descriptions of the caveats in Cisco Virtual Security Gateway for Nexus 1000V Series switch, Release 4.2(1)VSG1(2). 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.
CSCtg97333	"Clear counters interface data0" command on the Cisco VSG is not working.
CSCth91644	Wrong syslog is pushed when management interface IP is changed.
CSCti09598	VNSP binding for same IP in two VLANs replaces old value in the Cisco VSG.
CSCti11925	Policy-engine control debugs displayed information related to data-traffic.
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.
CSCti58398	Same policy-engine syslog is generated multiple times for a broadcast traffic.
CSCti89749	The Cisco VSG HA requires domain isolation for multi-tenant setups that share a management VLAN.
CSCtk01744	Policy-engine statistics and the service-path statistics won't show the right information after system switchover.
CSCtk83021	Remove unused commands on the Cisco VSG.
CSCto89854	VMs under tenants disappear and reappear.
CSCto97454	TCP Checks: Download of a file stops during/after vmotion.
CSCtr01200	Fail to copy running config to start-up with 1024 rules 16 conditions each.
CSCtr41120	Cisco VSG firewall getting firewalled issue.
CSCtr50316	PP org root to default SP (root) is showing as Org not configured in PP.
CSCtr55312	Large number is observed in sh vsn statistics o/p.
CSCtr56196	show license usage NEXUS_VSG_SERVICES_PKG shows incorrect information.
CSCtr71543	sh service-path conn does not show action inspect for rsh traffic.
CSCtr73966	Intermittent ICMP IP frag packet drops.
CSCtr76752	show ntp peers will periodically get stuck with VNMC DNS config changes.

Resolved Caveats

The following are descriptions of the resolved caveats in Cisco Virtual Security Gateway for Nexus 1000V Series switch, Release 4.2(1)VSG1(2). The ID links open the Cisco Bug Toolkit.

ID	Resolved Caveat Headline
CSCti26422	The Cisco VSG information displays as Nexus-Switch or Nexus1000VF in the CDP packet sent by VSG.
CSCti85989	Policy-engine syslog for IPv6 packet in the Cisco VSG shows incorrect information.
CSCtj55534	After several switchovers, the standby may enter the bash prompt (rare).
CSCtj83214	Traffic from virtual machines using the vApp custom attribute are evaluated by the Cisco VSG policy engine in lower case (even if a rule in the Cisco VSG is written with a vApp upper case value).
CSCtk62117	Time zone changes not pushed to the Cisco VSG.
CSCtl86630	Under certain circumstances, the Cisco VSG license does not get released properly. If VEM does not have any VM which is protected by the Cisco VSG, then VEM should not consume a Cisco VSG license.
CSCto35433	Packet drops on vPath enabled VEM in the presence of VPC-HM.

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(2)*
- *Cisco Virtual Security Gateway, Release 4.2(1)VSG1(2) and Cisco Virtual Network Management Center, Release 1.2 Installation and Upgrade Guide*
- *Cisco Virtual Security Gateway for Nexus 1000V Series Switch License Configuration Guide, Release 4.2(1)VSG1(2)*
- *Cisco Virtual Security Gateway for Nexus 1000V Series Switch Configuration Guide, Release 4.2(1)VSG1(2)*
- *Cisco Virtual Security Gateway for Nexus 1000V Series Switch Command Reference, Release 4.2(1)VSG1(2)*

- *Cisco Virtual Security Gateway for Nexus 1000V Series Switch Troubleshooting Guide, Release 4.2(1)VSG1(2)*

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

- *Release Notes for Cisco Virtual Network Management Center, Release 1.2*
- *Cisco Virtual Security Gateway, Release 4.2(1)VSG1(2) and Cisco Virtual Network Management Center, Release 1.2 Installation and Upgrade Guide*
- *Cisco Virtual Network Management Center CLI Configuration Guide, Release 1.2*
- *Cisco Virtual Network Management Center GUI Configuration Guide, Release 1.2*
- *Cisco Virtual Network Management Center XML API Reference Guide, Release 1.2*

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, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.

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