



Cisco Virtual Security Gateway Overview

This chapter provides an overview of the Cisco Virtual Security Gateway (VSG) features for the Cisco Nexus 1000V Series switch and Cisco Nexus 1010 Virtual Services Appliance.

This chapter includes the following sections:

- [Information About the Cisco Virtual Security Gateway, page 1-1](#)
- [Cisco Virtual Security Gateway Configuration for the Network, page 1-9](#)

Information About the Cisco Virtual Security Gateway

This section provides an overview of the Cisco VSG and includes the following topics:

- [Overview, page 1-1](#)
- [Product Architecture, page 1-2](#)
- [Fast Path Connection Timeouts, page 1-4](#)
- [Trusted Multitenant Access, page 1-5](#)
- [Dynamic \(Virtualization-Aware\) Operation, page 1-5](#)
- [Cisco VSG on the Cisco Nexus 1010 Virtual Services Appliance, page 1-6](#)
- [Cisco VSG Deployment Scenarios, page 1-8](#)

Overview

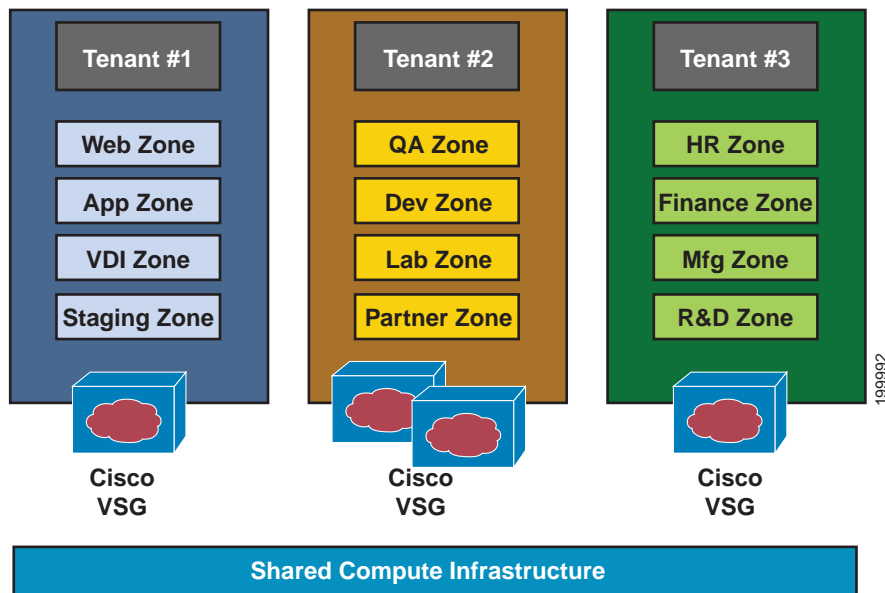
The Cisco Virtual Security Gateway (VSG) is a virtual firewall appliance that provides trusted access to virtual data center and cloud environments. The Cisco VSG enables a broad set of multitenant workloads that have varied security profiles to share a common compute infrastructure in a virtual data center private cloud or in a public cloud. By associating one or more virtual machines (VMs) into distinct trust zones, the Cisco VSG ensures that access to trust zones is controlled and monitored through established security policies.

Integrated with either the Cisco Nexus 1000V Series switch or the Cisco Nexus 1010 and running on the Cisco NX-OS operating system, the Cisco VSG provides the following benefits (see [Figure 1-1](#)):

- Trusted multitenant access—Zone-based control and monitoring with context-aware security policies in a multitenant (scale-out) environment to strengthen regulatory compliance and simplify audits. Security policies are organized into security profile templates to simplify their management and deployment across many Cisco VSGs.

- Dynamic operation—On-demand provisioning of security templates and trust zones during VM instantiation and mobility-transparent enforcement and monitoring as live migration of VMs occur across different physical servers.
- Nondisruptive administration—Administrative segregation across security and server teams that provides collaboration, eliminates administrative errors, and simplifies audits.

Figure 1-1 Trusted Zone-Based Access Control Using Per-Tenant Enforcement with the Cisco VSG



The Cisco VSG does the following:

- Provides compliance with industry regulations.
- Simplifies audit processes in virtualized environments.
- Reduces costs by securely deploying virtualized workloads across multiple tenants on a shared compute infrastructure, whether in virtual data centers or private/public cloud computing environments.

Product Architecture

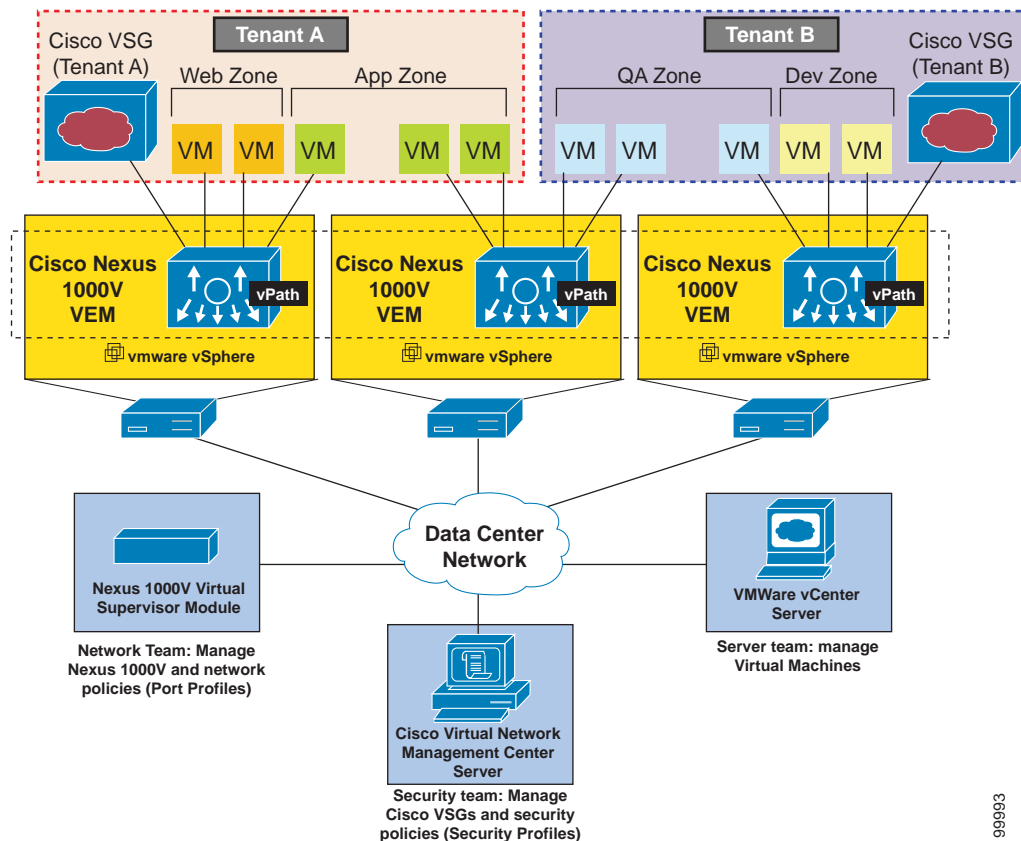
The Cisco VSG operates with the Cisco Nexus 1000V in the VMware vSphere hypervisor, and the Cisco VSG leverages the virtual network service datapath (vPath) that is embedded in the Nexus 1000V Virtual Ethernet Module (VEM) (see [Figure 1-2](#)). vPath steers traffic, whether external to VM or VM to VM, to the Cisco VSG of a tenant. Initial packet processing occurs in the Cisco VSG for policy evaluation and enforcement. Once the policy decision is made, the Cisco VSG off-loads the 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 off-load—Per-tenant policy enforcement of flows off-loaded by the Cisco VSG to vPath

The Cisco VSG and Nexus 1000V VEM provide the following benefits (see [Figure 1-3](#)):

- Efficient deployment—Each Cisco VSG can protect access and traffic across multiple physical servers, which eliminates the need to deploy one virtual appliance per physical server.
- Performance optimization—By off-loading fast-path to one or more Cisco Nexus 1000V VEM vPath modules, the Cisco VSG enhances network performance through distributed vPath-based enforcement.
- Operational simplicity—The Cisco VSG can be transparently inserted in one-arm mode without the need for creating multiple switches or temporarily migrating VMs to different switches or servers. Zone scaling is based on a security profile, not on vNICs that are limited for the virtual appliance. Zone scaling simplifies physical server upgrades without compromising security and incurring application outage.
- High availability—For each tenant, the Cisco VSG can be deployed 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—The Cisco VSG can be placed on a dedicated server that is 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.

Figure 1-2 Cisco Virtual Security Gateway Deployment Topology



199993

Fast Path Connection Timeouts

When a VEM sees a packet for a protected VM for the first time, the VEM redirects the packet to the Cisco VSG to determine what action needs to be taken (for example, permit, drop, or reset). Once the decision is made, both the Cisco VSG and VEM save the connection information and the action for a period of time. During this time, packets for this connection follow the same action without any extra policy lookup. This connection is a connection in a fast path mode. Depending on the traffic and the action, how long a connection stays in fast path mode varies. [Table 1-1](#) provides the timeout details for the connections in the fast path.

Table 1-1 Fast Path Connection Timeouts

Protocol	Connection State	Time Out
TCP	Close with FIN and ACKACK)	VEM—4 secs
		VSG—4 secs
	Close with RST	VEM—4 secs
		VSG—4 secs
	Action drop	VEM—4 secs VSG—4 secs
Action reset	VEM—4 secs VSG—4 secs	
UDP	Idle	VEM—36–60 secs
		VSG—630–930 secs
	Action drop	VEM—4 secs VSG— 4 secs
	Action reset	VEM—4 secs VSG—4 secs
L3/ICMP	Destination Unreachable	VEM—8–12 secs
		VSG—240–360 secs
	Action drop	VEM—4 secs VSG—4 secs
		VEM—2 secs VSG—2 secs
Action reset	VEM—2 secs VSG—2 secs	
	Idle	VEM—8–12 secs VSG—16–24 secs

Table 1-1 Fast Path Connection Timeouts (continued)

Protocol	Connection State	Time Out
L2 (for example, IPv6)	Action drop	VEM—2 secs
		VSG—2 secs
	Action reset	VEM—2 secs
VSG—2 secs		
Idle		VEM—8–12 secs
		VSG—12–18 secs

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. One or more instances of the Cisco VSG is deployed on a per-tenant basis, which allows a high scale-out deployment across many tenants. Tenants are isolated from each other, so no traffic can cross tenant boundaries. You can deploy the Cisco VSG at the tenant level, at the virtual data center (VDC) level, and at the vApp level.

As VMs are instantiated for a given tenant, their association to security profiles and zone membership occurs immediately through binding with the Cisco Nexus 1000V port profile. Each VM is placed upon instantiation into a logical trust zone (see [Figure 1-2](#)). Security profiles contain context-aware rule sets that specify access policies for traffic that enters and exits each zone. In addition to VM and network contexts, security administrators can also use custom attributes to define zones directly through security profiles. Controls are applied to zone-to-zone traffic as well as to external-to-zone (and zone-to-external) traffic. Zone-based enforcement can occur within a VLAN also, as a VLAN often identifies a tenant boundary. The Cisco VSG evaluates access control rules and then, if configured, off-loads enforcement to the Cisco Nexus 1000V VEM vPath module. The Cisco VSG can permit or deny access and optional access logs can be generated. The Cisco VSG also provides a policy-based traffic monitoring capability with access logs.

A Cisco VSG tenant can protect its VMs that span multiple hypervisors. Each tenant can also be assigned an overlapping (private) IP address space, which is important in multitenant cloud environments.

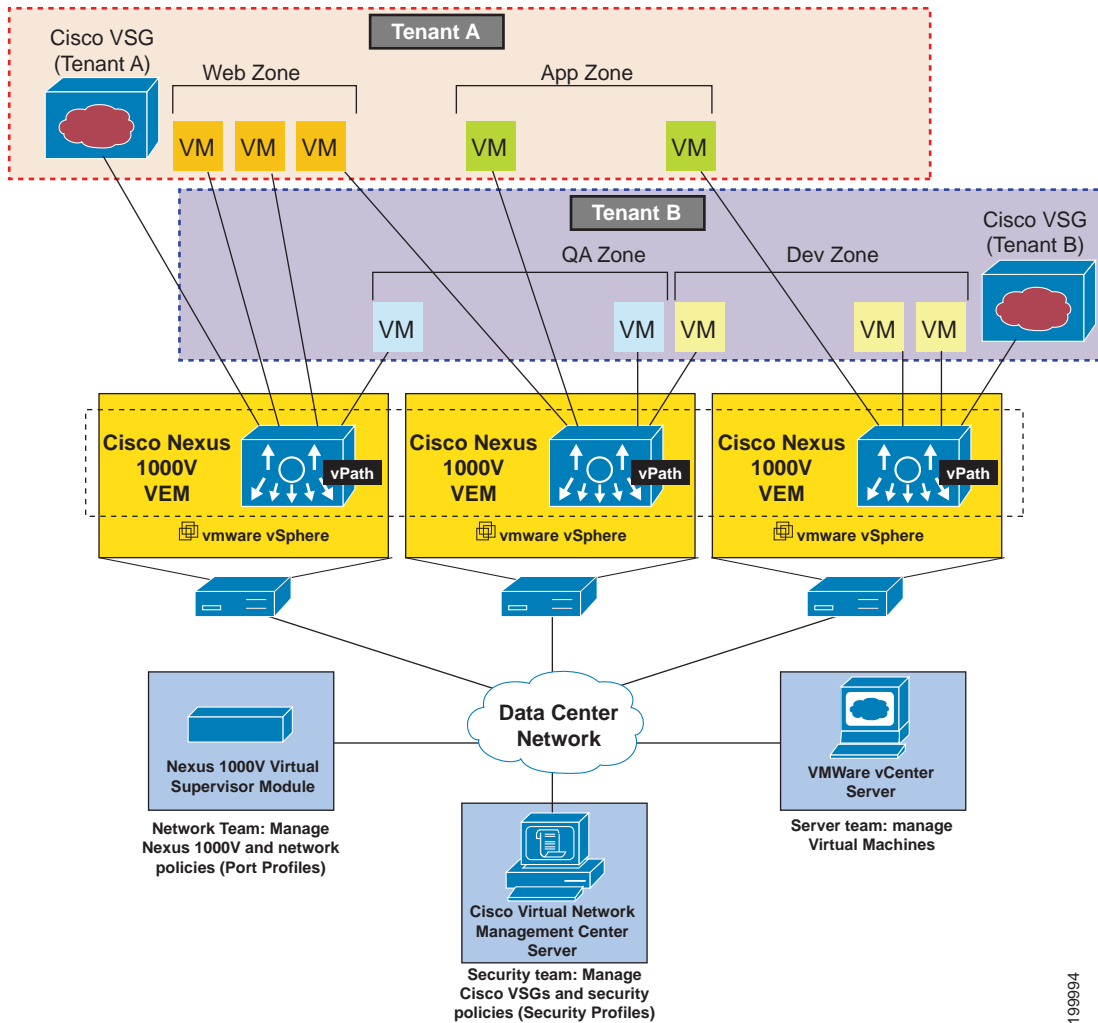
Dynamic (Virtualization-Aware) Operation

A virtualization environment is dynamic, where frequent additions, deletions, and changes occur across tenants and across VMs. Additionally, live migration of VMs can occur due to manual or programmatic vMotion events. [Figure 1-3](#) shows how a structured environment (see [Figure 1-2](#)) can change over time due to this dynamic VM environment.

The Cisco VSG operating with the Cisco Nexus 1000V (and vPath) supports a dynamic VM environment. Typically, when you create a tenant on the Cisco Virtual Network Management Center (VNMC) with the Cisco VSG (standalone or active-standby pair), 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 [VSM] and published to the VMware Virtual Center). When a new VM is instantiated, the server administrator assigns 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 are triggered, VMs move across physical servers. Because the Cisco Nexus 1000V ensures that port profile policies follow the VMs, associated security profiles also follow these moving VMs, and security enforcement and monitoring remain transparent to vMotion events.

Figure 1-3 Cisco VSG Security in a Dynamic VM Environment, Including VM Live Migration



199994

Cisco VSG on the Cisco Nexus 1010 Virtual Services Appliance

The Cisco Virtual Security Gateway (VSG) can be hosted on a Cisco Nexus 1010 Virtual Services Appliance. The Cisco Nexus 1010 hosts up to six virtual service blades (VSBs) that can be configured as a Cisco Network Analysis Module (NAM), a Virtual Supervisor Module (VSM), or a Cisco VSG. VSMs that had been hosted on VMware virtual machines can be hosted on the Cisco Nexus 1010, as can the Cisco VSG.

Software for the Cisco VSG comes bundled with the other software for the Cisco Nexus 1010, which includes the kickstart image and a hypervisor. The software for implementing the Cisco VSG on the Cisco Nexus 1010 is included with the software for creating the VSB and is stored in the bootflash repository.

Figure 1-4 compares running the VSM and Cisco VSG on a Cisco Nexus 1010 with running the VSM and Cisco VSG on a virtual machine.

Figure 1-4 VM and Cisco Nexus 1010 Comparison

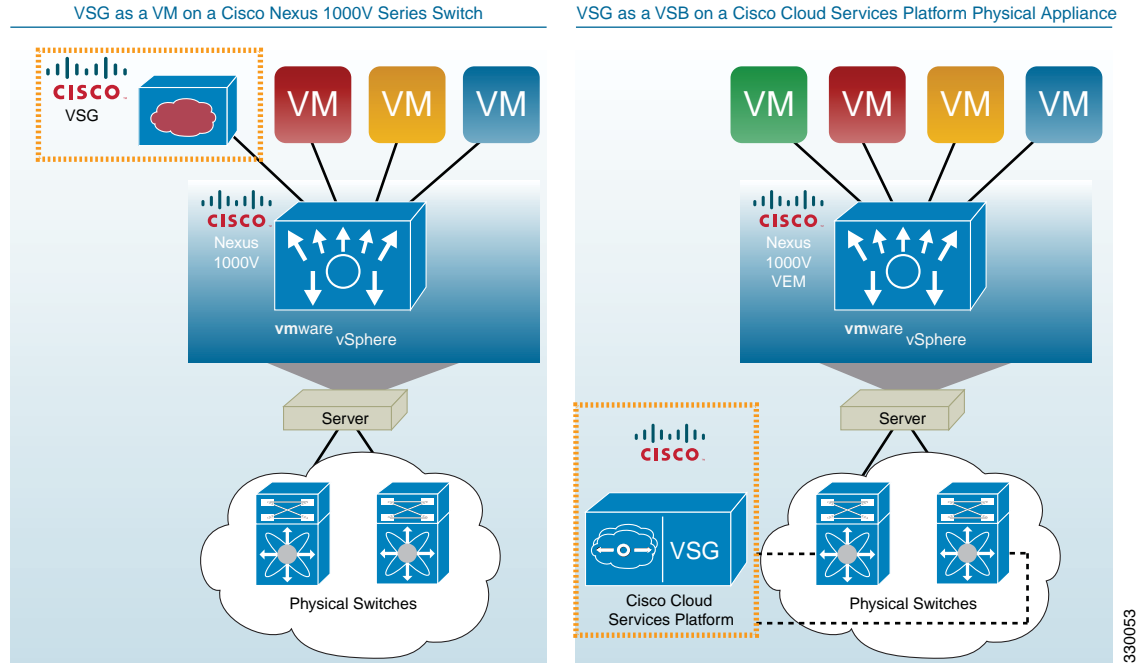
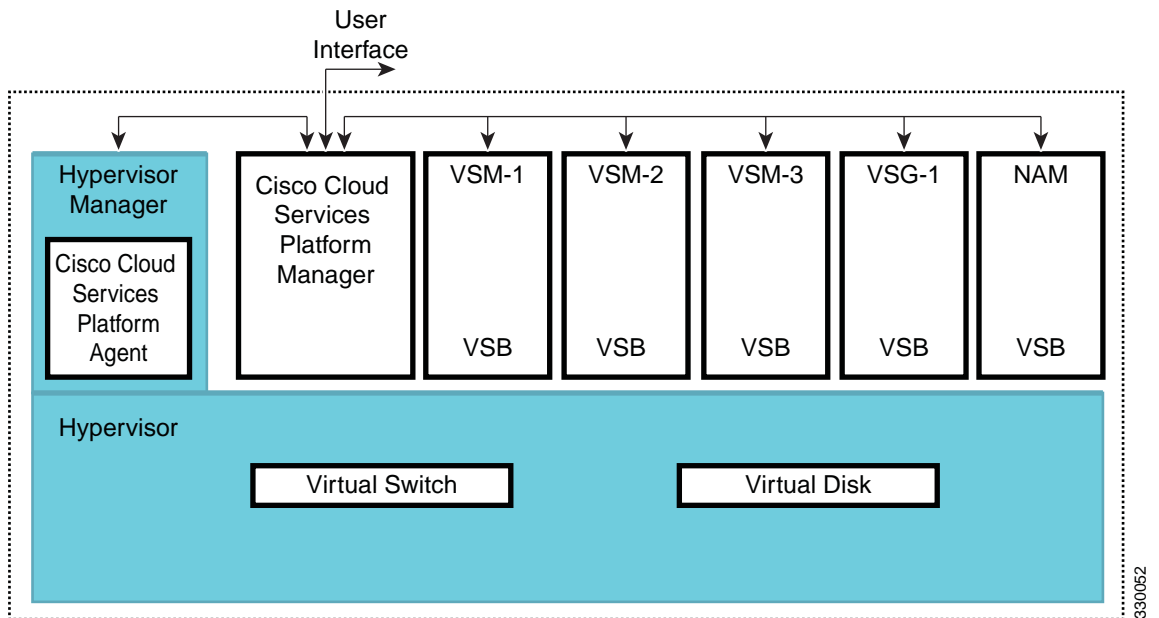


Figure 1-5 shows the Cisco Nexus 1010 software components and how they relate to the Cisco VSG.

Figure 1-5 Cisco Nexus 1010 Software Components



For more information about the *Cisco Nexus 1010*, see the *Cisco Nexus 1010 Software Configuration Guide*.

Cisco VSG Deployment Scenarios

Prior to Release 4.2(1)VSG1(3.1), the Cisco VSG must be deployed in the Layer 2 adjacency to a VEM. Throughout this document, the Cisco VSG is called operating in the Layer 2 mode when deployed this way.

The current release supports the Cisco VSG deployment in the Layer 3 mode. The Cisco VSG and the VEM are no longer required to be in the same Layer 2 network. The VEM and the Cisco VSG communicate with each other through a special virtual network interface called the Virtual Kernel NIC (vmknic). This vmknic is created by an administrator.



Note

Adjacency to the VEM means that vPath can talk to the Cisco VSG in the Layer 2 without a router because vPath and the Cisco VSG belong to the same Layer 2 network.

VEM Interface for a Cisco VSG in the Layer 3 Mode

When a VEM has a VM that is protected by the Cisco VSG in the Layer 3 mode, the VEM requires at least one IP/MAC pair to terminate the Cisco VSG packets in the Layer 3 mode. The VEM acts as an IP host (not a router) and supports only the IPv4 addresses.

Similar to how VEM Layer 3 Control is configured, the IP address to use for communication with the Cisco VSG in the Layer 3 mode is configured by assigning a port profile to a vmknic that has the **capability I3-vn-service** command in it. For more details, see the “Creating a Port Profile for Layer 3 Control” section of the *Cisco Nexus 1000V System Management Configuration Guide, Release 4.2(1)SVI(5.1)* at http://www.cisco.com/en/US/docs/switches/datacenter/nexus1000/sw/4_2_1_s_v_1_5_1/system_management/configuration/guide/n1000v_system_3domain.html#wp1055053.

To configure the vmknic interface that VEM uses, you can assign a port profile by using the **capability I3-vn-service** command in the port-profile configuration.

To carry the Cisco VSG in the Layer 3 mode traffic over multiple uplinks (or subgroups) in server configurations where vPC-HM MAC-pinning is required, you can configure up to four vmknics. We recommend that you assign all the vmknics in the Layer 3 mode within the same ESX/ESXi host to the same port profile by using the **capability I3-vn-service** command.

The traffic in the Layer 3 mode that is sourced by local vEthernet interfaces and needs to be redirected to Cisco VSG is distributed between these vmknics based on the source MAC in their frames. The VEM automatically pins the multiple vmknics in the Layer 3 mode to separate uplinks. If an uplink fails, the VEM automatically respins the vmknic to a working uplink.

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 to a VSG IP address ARP request by using the Proxy ARP feature.

Virtual Extensible LANs

In the current release, Cisco Nexus 1000V supports Virtual Extensible LAN (VXLAN) feature that defines a 24-bit LAN segment identifier to provide segmentation at a cloud scale.

The VXLAN enables the following:

- Logical networks to be extended among virtual machines placed in different subnets.
- New servers to be added in different subnets.
- The virtual machines to be migrated between servers in different subnets.

The VMs that reside in the VXLAN can be protected by the Cisco VSG.



Note

The Cisco VSG must reside in the VLAN.

Cisco Virtual Security Gateway Configuration for the Network

This section describes the Cisco Virtual Security Gateway configuration for your network and includes the following topics:

- [Setting Up Cisco VSGs and VLANs, page 1-9](#)
- [Cisco VSG Configuration Overview, page 1-10](#)
- [Sequence in Configuring a Cisco VSG in the Layer 2 Mode, page 1-13](#)
- [Sequence in Configuring a Cisco VSG in the Layer 3 Mode, page 1-14](#)
- [Migrating from Layer 2 Mode to Layer 3 Mode, page 1-15](#)

Setting Up Cisco VSGs and VLANs

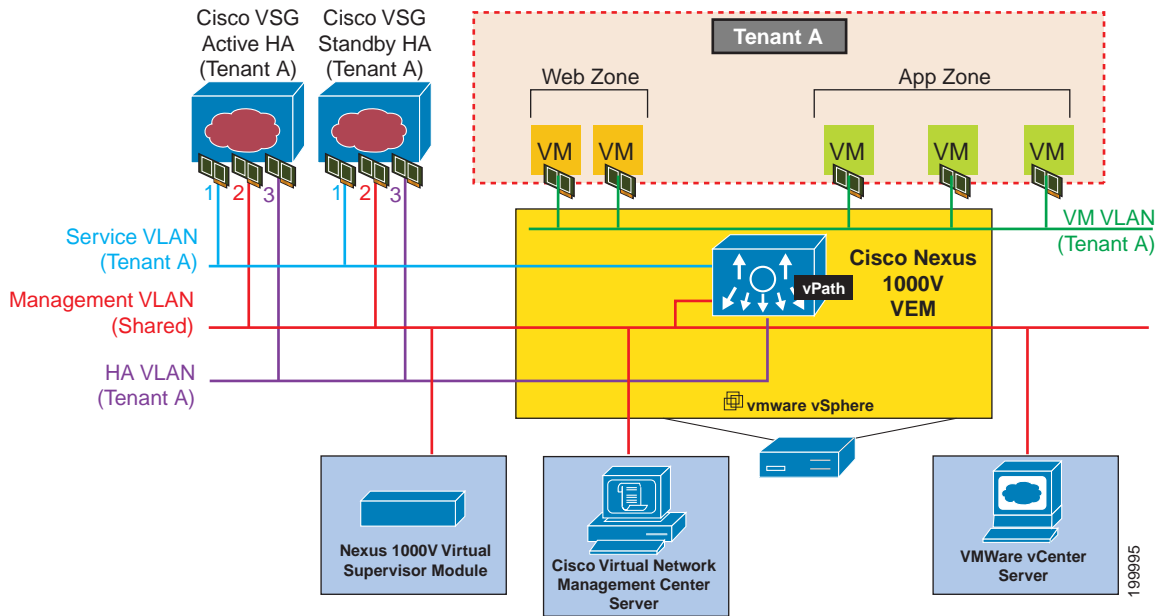
The Cisco VSG is set up so that VMs can reach a Cisco VSG irrespective of its location. The vPath component in the Cisco Nexus 1000V VEM intercepts the packets from the VM and sends them to the Cisco VSG for further processing.

Figure 1-6 shows a Cisco VSG. In the figure, the Cisco VSG has connectivity to three different VLANs (Management VLAN, Service VLAN, and HA VLAN). A Cisco VSG is configured with three vNICs with each of the vNICs connected to one of the VLANs. The VLAN functions are as follows:

- The Management VLAN connects management platforms such as the VMware vCenter, the Cisco Virtual Network Management Center, and the Cisco Nexus 1000V VSM and the managed Cisco VSGs.
- The Service VLAN provides communications between the Cisco Nexus 1000V VEM and Cisco VSGs. All the Cisco VSGs are part of the Service VLAN and the VEM uses this VLAN for its interaction with Cisco VSGs.
- The HA VLAN is used for the HA heart-beat mechanism and identifies the master-slave 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 the tenants, and the Service VLAN, HA VLAN, and VM Data VLAN are allocated on a per-tenant basis. However, when VLAN resources become scarce, you may decide to use a single VLAN for Service and HA functions.

Figure 1-6 Cisco Virtual Security Gateway VLAN Usages

**Note**

The Cisco VSG will not be on a VXLAN. The Cisco VSG supports the VXLAN data traffic only. For details, see the *Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.2(1)SV1(5.1)*.

Cisco VSG Configuration Overview

This section provides an overview of the Cisco VSG configuration and includes the following topics:

- [Cisco Nexus 1000V Series Switch VSM, page 1-10](#)
- [Port Profile, page 1-11](#)
- [Virtual Security Gateway, page 1-11](#)
- [Security Profile, page 1-11](#)
- [Firewall Policy, page 1-11](#)

When you install a Cisco VSG on a virtualized data center network, you must change the configuration of the Cisco Nexus 1000V Series switch VSM and the configuration of the Cisco VSG.

Cisco Nexus 1000V Series Switch VSM

The VSM controls multiple VEMs as one logical modular switch. Instead of physical line-card modules, the VSM supports VEMs that runs in software inside servers. Configurations are performed through the VSM and automatically propagated to the VEMs. Instead of configuring soft switches inside the hypervisor on one host at a time, you can define configurations for immediate use on all VEMs being managed by the VSM.

Port Profile

In the Cisco Nexus 1000V Series switch, you use port profiles to configure interfaces. Through a management interface on the VSM, you can assign a port profile to multiple interfaces—providing all of them with the same configuration. Changes to the port profile can be propagated automatically to the configuration of any interface assigned to it.

In the VMware vCenter Server, a port profile is represented as a port group. The vEthernet or Ethernet interfaces are assigned in the vCenter Server to a port profile for the following functions:

- To define port configuration by policy.
- To apply a single policy across many ports.
- To support both vEthernet and Ethernet ports.

Port profiles that are not configured as uplinks can be assigned to a VM virtual port. When binding with a security profile and a Cisco VSG IP address, a VM port profile can be used to provision security services (such as for VM segmentation) provided by a Cisco VSG.

Virtual Security Gateway

The Cisco VSG for the Cisco Nexus 1000V Series switch is a virtual firewall appliance that provides trusted access to the virtual data center and cloud environments. Administrators can install a Cisco VSG on a host as a service VM and configure it with security profiles and firewall policies in order to provide VM segmentation and other firewall functions to protect the access to VMs.

Security Profile

The Cisco Nexus 1000V Series switch port profile dynamically provisions network parameters for each VM. The same policy provisioning carries the network service configuration information so that each VM is dynamically provisioned with the network service policies when the VM is attached to the port profile. This process is similar to associating ACL or QoS policies in the port profile. The information related to network service configuration is created in an independent profile called the security profile and is attached to the port profile. The security administrator creates the security profile in the Cisco VSG, and the network administrator associates it to an appropriate port profile in VSM.

The security profile defines custom attributes that can be used to write policies. All the VMs tagged with a given port profile inherit the firewall policies and custom attributes defined in the security profile associated with that port profile. Each custom attribute is configured as a name value pair, such as state = CA. The network administrator also binds the associated Cisco VSG for a given port profile. The Cisco VSG associated with the port profile enforces firewall policies for the network traffic of the application VMs bound to that port profile. The same Cisco VSG is used irrespective of the location of the application VM. As a result, the policy is consistently enforced even during the VMotion procedures. You can also bind a specific policy to a service profile so that if any traffic is bound to a service profile, the policy associated with that service profile is executed. Both the service plane and the management plane support multitenancy requirements. Different tenants can have their own Cisco VSG (or set of Cisco VSGs), enforcing the policy defined by them. The vPath in each ESX host can intelligently redirect tenant traffic to the appropriate Cisco VSG.

Firewall Policy

You can use a firewall policy to enforce network traffic on a Cisco VSG. A key component of the Cisco VSG is the policy engine. The policy engine uses the policy as a configuration that filters the network traffic that is received on the Cisco VSG.

A policy is bound to a Cisco VSG by using a set of indirect associations. The security administrator can configure a security profile and then refer to a policy name within the security profile. The security profile is associated with a port profile that has a reference to a Cisco VSG.

A policy is constructed using the following set of policy objects:

- [Object Groups, page 1-12](#)
- [Zones, page 1-12](#)
- [Rules, page 1-12](#)
- [Actions, page 1-12](#)
- [Policies, page 1-12](#)

Object Groups

An object group is a set of conditions relevant to an attribute. As object groups and zones can be shared between various rules with different directions, the attributes used in an object group condition should not have a directional sense and must be neutral. An object group is a secondary policy object that assists in writing firewall rules. A rule condition can refer to an object group by using an operator.

Zones

A zone is a logical group of VMs or hosts. Zones simplify policy writing by allowing users to write policies based on zone attributes using zone names. The zone definitions map the VMs to the zones. The logical group definition can be based on the attributes associated with a VM or a host, such as VM attributes defined in the vCenter. Zone definitions can be written as condition-based subnet and endpoint IP addresses.

Because zones and object groups can be shared between various rules with different directions, the attributes used in an object group should not have a directional sense and must be neutral.

Rules

Firewall rules can consist of multiple conditions and actions. Rules can be defined in a policy as a condition-based subnet or endpoint IP addresses and VM attributes.

Actions

Actions are the result of a policy evaluation. You can define and associate one or more of the following actions within a specified rule:

- Permit
- Drop packet
- Reset
- Log
- Inspection

Policies

A policy enforces network traffic on a Cisco VSG. A key component operating on the Cisco VSG is the policy engine. The policy engine takes the policy as configuration and executes it when enforced against the network traffic that is received on the Cisco VSG. A policy is constructed by using the following set of policy objects:

- Rules
- Conditions
- Actions
- Object-groups
- Zones

A policy is bound to a Cisco VSG by using a set of indirect associations. The security administrator can configure a security profile and then refer to a policy name within the security profile. The security profile is associated with a port profile that has a reference to a Cisco VSG.

Service Firewall Logging

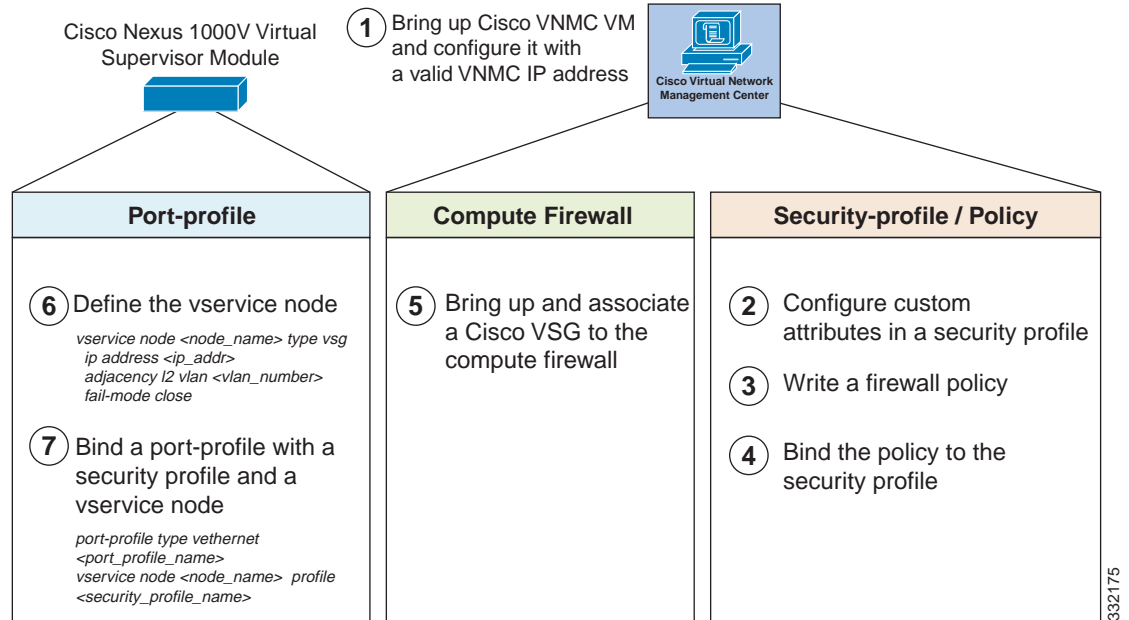
The service firewall log is a tool to test and debug the policy. During a policy evaluation, the policy engine displays the policy results of a policy evaluation. Both the users and the policy writer benefit from this tool when troubleshooting a policy.

Sequence in Configuring a Cisco VSG in the Layer 2 Mode

This section is an overview of the sequence that you, as an administrator, must follow when configuring a Cisco VSG in Layer 2 mode (see [Figure 1-7](#)):

1. Install and set up a Cisco VNMC service VM and configure the Cisco VNMC with a valid IP address.
2. If you plan to use custom attributes in the firewall policy, create a set of custom attributes in a security profile configuration on the Cisco VNMC.
3. Write a firewall policy on the Cisco VNMC by using the appropriate policy objects such as object groups, zones, rules, conditions, actions, and policies.
4. After the firewall policy is created, bind the policy to the security profile that was previously created on the Cisco VNMC. This step is done with the security profile management interface.
5. Bring up a Cisco VSG and associate it to the appropriate compute firewall on the Cisco VNMC.
6. After the security profile and firewall policy are fully developed, you can bind the security profile with the VM port profiles that demand access protection provided by the Cisco VSG through the port profile management interface on the VSM. You must also bind the Cisco VSG with the set of VM port profiles.

Figure 1-7 Cisco Virtual Security Gateway Layer 2 Configuration Flow



Sequence in Configuring a Cisco VSG in the Layer 3 Mode

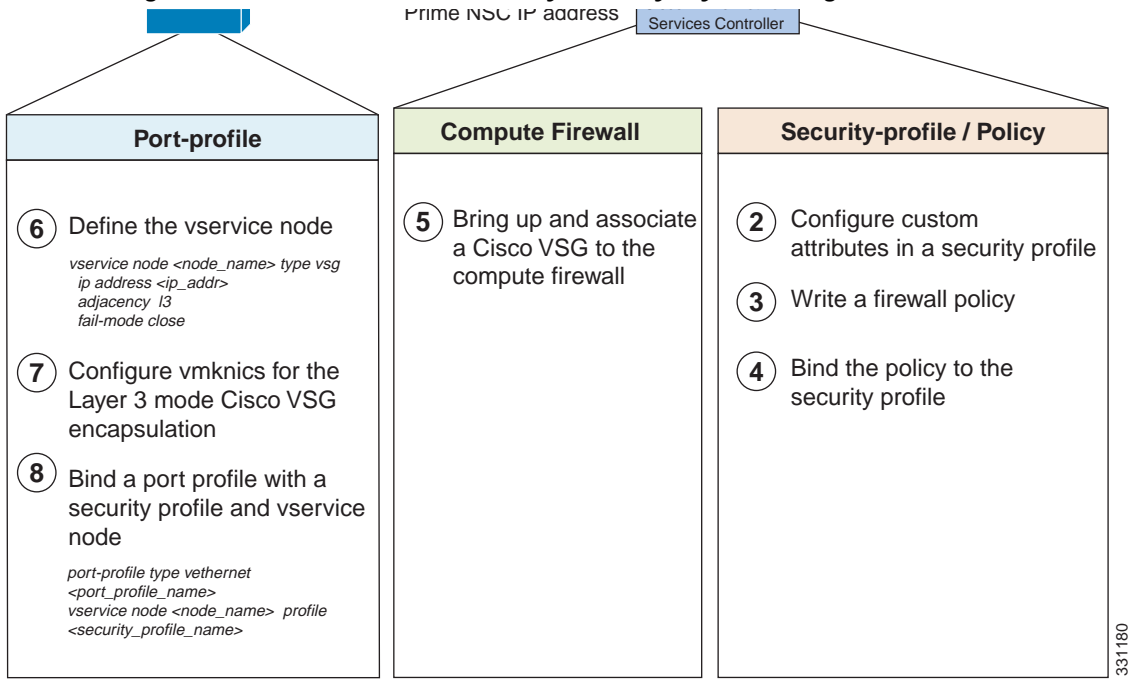
Before configuring a Cisco VSG in Layer 3 mode, create a Layer 3 vmknic. For details, see the [“Configuring vmknics for the Layer 3 Mode VSG Encapsulation”](#) section on page 3-4.

This section is an overview of the sequences that you, as an administrator, to follow in configuring a Cisco VSG in Layer 3 mode (see [Figure 1-8 on page 1-15](#)):

1. Install and set up a Cisco VNMC service VM and configure the Cisco VNMC with a valid IP address.
2. As an administrator, if you plan to use custom attributes in the firewall policy, create a set of custom attributes in a security profile configuration on the Cisco VNMC.
3. As an administrator, write a firewall policy on the Cisco VNMC by using appropriate policy objects such as object groups, zones, rules, conditions, actions, and policies.
4. After the firewall policy is created, as an administrator, bind the policy to the security profile that was previously created on the Cisco VNMC.
5. Bring up a Cisco VSG and associate it to the appropriate compute firewall on the Cisco VNMC
6. After the security profile and firewall policy are fully developed, as an administrator, you can bind the security profile with the VM port profiles that demand access protection provided by the Cisco VSG through the port profile management interface on the VSM. As an administrator, you must also bind the Cisco VSG with the set of VM port profiles.

Figure 1-8

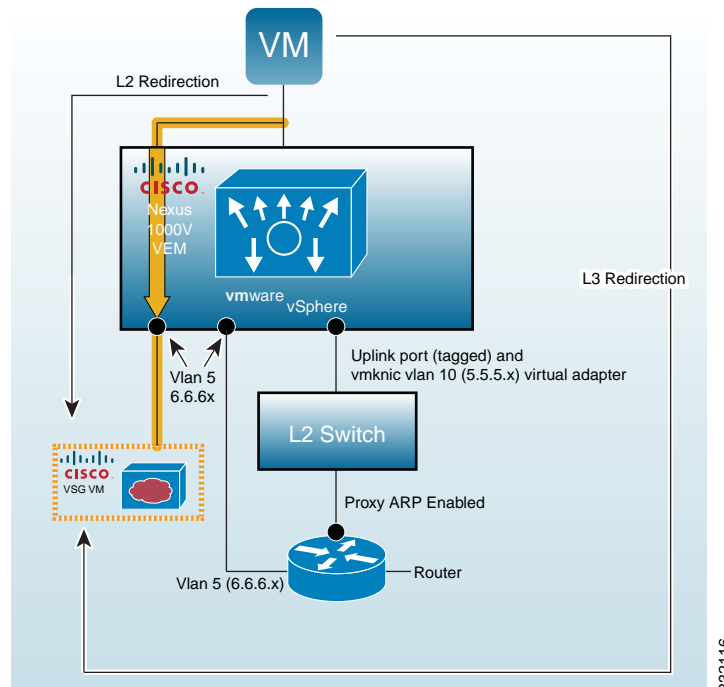
Cisco Virtual Security Gateway Layer 3 Configuration Flow



Migrating from Layer 2 Mode to Layer 3 Mode

This section provides an overview of the sequence to follow when migrating the Cisco VSG deployment from Layer 2 mode to Layer 3 mode. See Figure 1-9.

Figure 1-9 Cisco VSG Deployment Migration from Layer 2 Mode to Layer 3 Mode



BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- The virtual or real router contains two interfaces:
 - One interface resides in the Layer 3 vmknic VLAN (VLAN 10) 5.5.5.x network.
 - One interface resides in the existing Layer 2 Cisco VSG service VLAN (VLAN 5) 6.6.6.x network.
- Proxy ARP is enabled on the VLAN 10 interface of the router.
- You have upgraded to the 1.3 VNMC, 1.3 Cisco VSG, and CN VSM/VEM.

PROCEDURE

-
- Step 1** Add Layer 3 vmknics on all VEMs (VLAN 10) as follows:
- a. Provision the Layer 3 vmknic VLAN on the uplink ports.
 - b. Create a port profile with Layer 3 capability and VLAN 10.
 - c. Create the vmknic and associate the port profile created in [Step b](#) with the vmknic.
 - d. Repeat [Step 3](#) for each VEM host.

- Step 2** Verify Layer 3 vmknic connectivity between the VEM-to-VEM and the VEM-to-Cisco VSG:

- a. Perform a VEM-to-VEM vmkping from each VEM to its peers.

```
[root@sg-dmastrop-sd4 Storage1 (1)]# vmkping 5.5.5.2
PING 5.5.5.2 (5.5.5.2): 56 data bytes
64 bytes from 5.5.5.2: icmp_seq=0 ttl=64 time=0.467 ms
```

- b. Perform a ping vsn on the VSM to check the VEM to the Cisco VSG connectivity.

```
vsm-d16-bl434(config-vnm-policy-agent)# ping vsn ip 6.6.6.99 src-module all
ping vsn 6.6.6.99 vlan 0 from module 3 4, seq=0 timeout=1-sec
  module(usec)    : 3(434) 4(434)
```

```
ping vsn 6.6.6.99 vlan 0 from module 3 4, seq=1 timeout=1-sec
  module(usec)    : 3(356) 4(481)
```

```
ping vsn 6.6.6.99 vlan 0 from module 3 4, seq=2 timeout=1-sec
  module(usec)    : 3(341) 4(448)
```

```
ping vsn 6.6.6.99 vlan 0 from module 3 4, seq=3 timeout=1-sec
  module(usec)    : 3(368) 4(466)
```

```
ping vsn 6.6.6.99 vlan 0 from module 3 4, seq=4 timeout=1-sec
  module(usec)    : 3(346) 4(414)
```


Step 3 Proceed to either Step [a](#) or Step [b](#). During this step, there will be a disruption of traffic for the new traffic flows from the VMs using the port profile. Existing flows will not be disrupted. The operation in Step [a](#) has more traffic disruptions than in Step [b](#).

a. Change the existing Layer 2 mode port profile to support Layer 3 mode (new sessions will be disrupted):

1. Under the Layer 2 mode port profile, do a no-vn-service to remove the existing Layer 2 vn-service configuration.
2. Configure the new vn-service as follows:

```
VSM(config-port-prof)# Vn-service <same ip address> l3-mode security-profile <same security-profile name>
```

The following example shows how to configure the new vn-service:

```
VSM(config-port-prof)# vn-service ip-address 6.6.6.99 l3-mode security-profile L3mode2
```

b. Create a new Layer 3 mode port profile and leave the existing Layer 2 mode port profile:

1. Create a new Layer 3 mode port profile.

The following example shows how to create a new Layer 3 mode port profile and leave the existing layer 2 mode port profile:

```
port-profile type vethernet L3_vlan121_VM
  vmware port-group
  switchport mode access
  switchport access vlan 121 <<< access vlan for the traffic VM
  org root/L3_mode/dc2
  no shutdown
  vn-service ip-address 6.6.6.99 l3-mode security-profile L3mode2
  state enabled
```

2. Change the port profile on the traffic VMs to the new Layer 3 mode port profile (new sessions will be disrupted).

