



Virtual Security Gateway Overview

This chapter contains the following sections:

- [Information About the Cisco Virtual Security Gateway, page 1](#)
- [Cisco Virtual Security Gateway Configuration for the Network, page 10](#)
- [Feature History for Overview, page 14](#)

Information About the Cisco Virtual Security Gateway

Overview

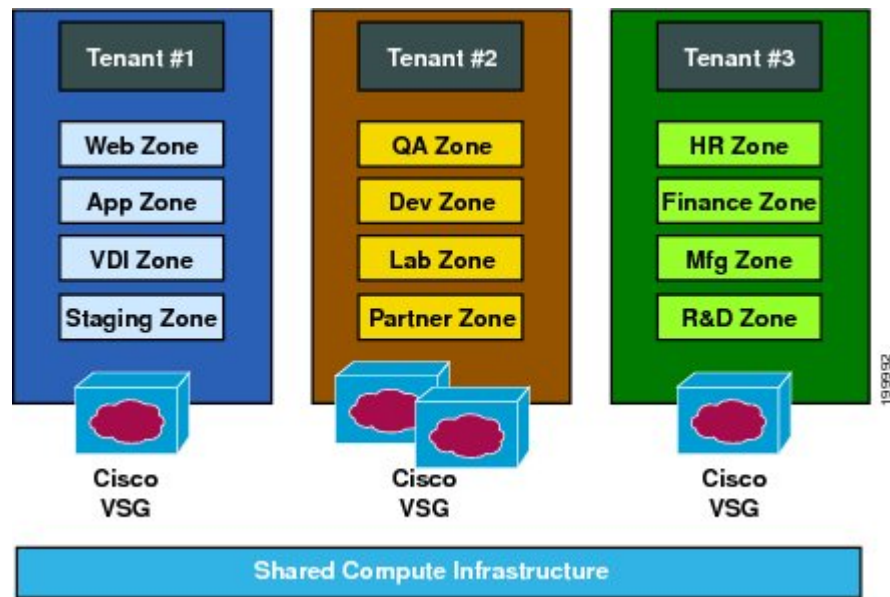
The Cisco Virtual Security Gateway (VSG) is a virtual firewall appliance that provides trusted access to virtual data center and cloud environments. The Cisco VSG enables a broad set of multitenant workloads that have varied security profiles to share a common compute infrastructure in a virtual data 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 Cloud Service Platform and running on the Cisco NX-OS operating system, the Cisco VSG provides the following benefits:

- **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: 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.

VSG Models

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

Table 1: VSG Models

VSG Models	Memory	CPU Speed	Number of Virtual CPUs	Network Adapters
Small	2 GB	1.0 GHz	1	3
Medium	2 GB	1.5 GHz	1	3
Large	2 GB	1.5 GHz	2	3

**Attention**

After you have installed a VSG instance, you should not change the VSG model. You can change the VSG model after installation using VMware vCenter. However, the VSG may not behave as expected after you change VSG model. The VSG CLI does not provide support to change the VSG model.

**Restriction**

The primary and secondary VSG models should always be same. If the primary VSG is large, the secondary VSG model should also be large type. If you configure different VSG models, VSG may not behave as expected causing the traffic to drop after a switchover or failover.

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 Cisco Nexus 1000V Virtual Ethernet Module (VEM). Cisco VSG is supported on these VMware vSphere hypervisor versions:

- vSphere 5.0
- vSphere 5.1
- vSphere 5.1U
- vSphere 5.5
- vSphere 6.0

Cisco 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. After the policy decision is made, the Cisco VSG off-loads the policy enforcement of remaining packets to vPath. vPath supports the following features:

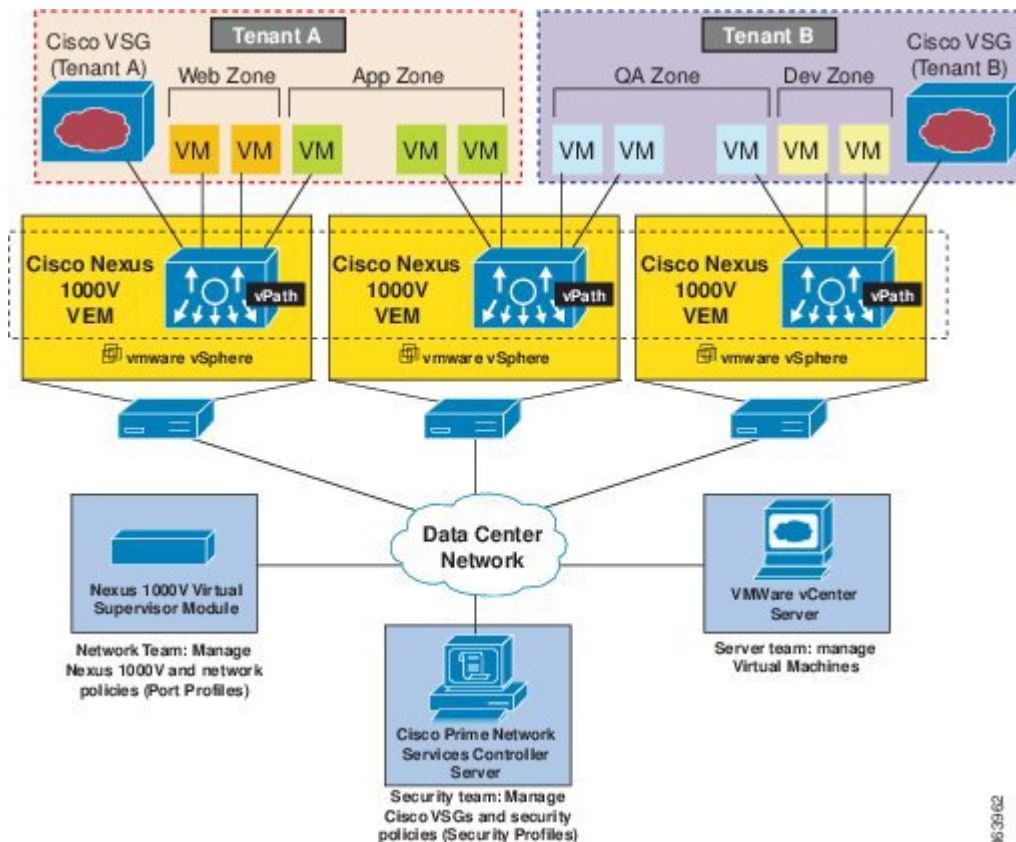
- Intelligent interception and redirection—Tenant-aware flow classification and subsequent redirection to a designated Cisco VSG tenant
- Fast-path off-load—Per-tenant policy enforcement of flows off-loaded by the Cisco VSG to vPath

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

- 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 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 2: Cisco Virtual Security Gateway Deployment Topology



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). After 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, the amount of time that a connection stays in the fast path mode varies. The following table provides the timeout details for the connections in the fast path mode.

Table 2: 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	
	Idle	VEM—36–60 secs	
		VSG—630–930 secs	
	UDP	Action drop	VEM—4 secs
			VSG—4 secs
Action reset		VEM—4 secs	
		VSG—4 secs	
Idle		VEM—8–12 secs	
		VSG—240–360 secs	
Destination Unreachable		VEM—4 secs	
		VSG—4 secs	

Protocol	Connection State	Time Out
L3/ICMP	Action drop	VEM—2 secs
		VSG—2 secs
	Action reset	VEM—2 secs
		VSG—2 secs
	Idle	VEM—8–12 secs
		VSG—16–24 secs
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 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. 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 also occur within a VLAN, 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 with an overlapping (private) IP address space, which is important in multitenant cloud environments.

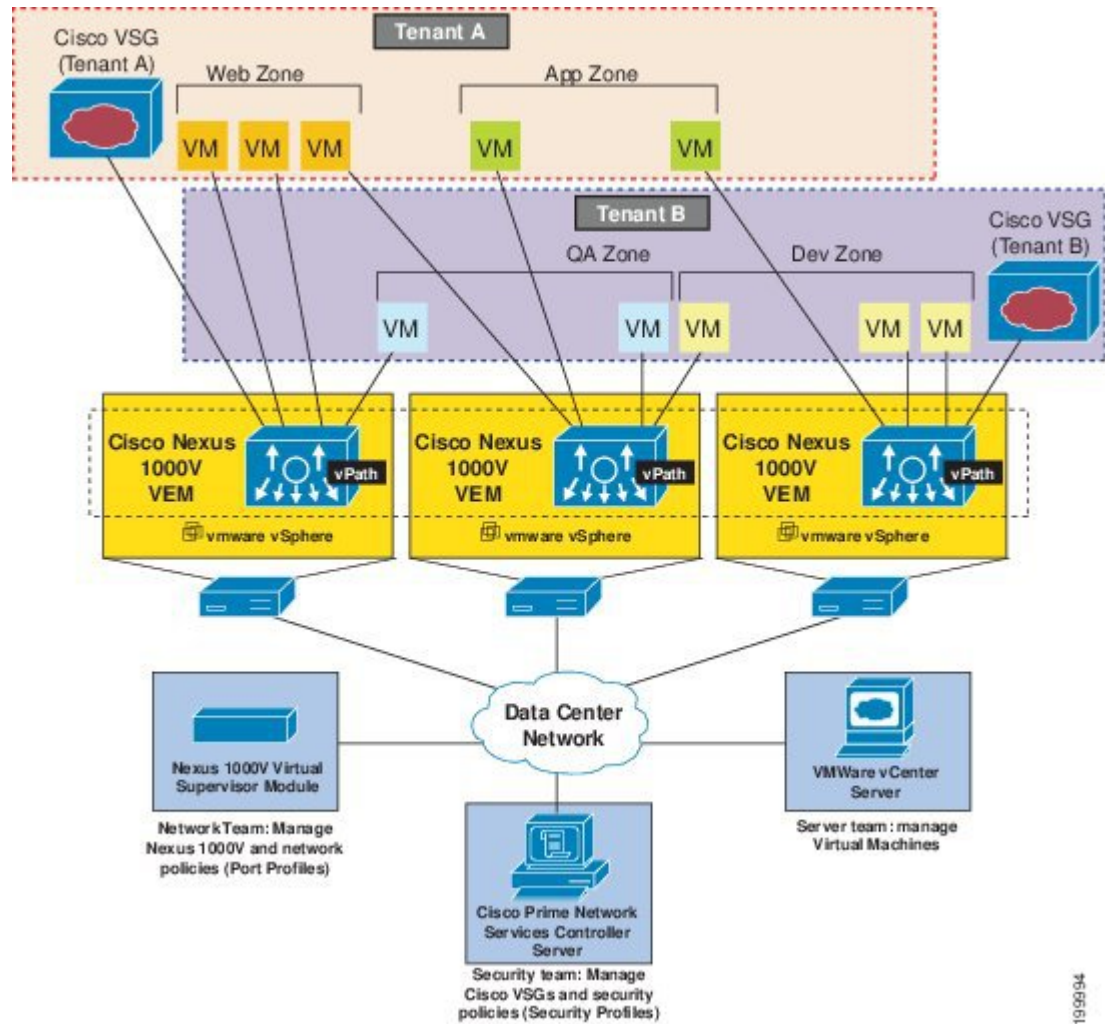
Dynamic (Virtualization-Aware) Operation

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. The following figure shows how a structured environment 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 Prime Network Services Controller (Prime NSC) 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 3: Cisco VSG Security in a Dynamic VM Environment, Including VM Live Migration



199994

Cisco VSG Deployment Scenarios

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

Layer 2 adjacency to the VEM means that vPath can talk to the Cisco VSG in 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-vservice** command in it. For more details, see the *Cisco Nexus 1000V System Management Configuration Guide*.

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

The traffic in the Layer 3 mode that is sourced by local vEthernet interfaces and needs to be redirected to the Cisco VSG is distributed between these vmknics based on the source MAC addresses 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 repins the vmknics 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.

**Note**

The Cisco VSG Layer 3 mode is not supported with the Virtual Extensible LAN (VXLAN).

Cisco vPath

vPath is embedded in the Cisco Nexus 1000V Series switch VEM. It intercepts the VM to VM traffic and then redirects the traffic to the appropriate virtual service node. For details, see the *Cisco vPath and vServices Reference Guide for VMware vSphere*.

Cisco VSG Network Virtual Service

The Cisco network virtual service (vservice) is supported by the Cisco Nexus 1000V using the vPath. It provides trusted multitenant access and supports the VM mobility across physical servers for workload balancing, availability, or scalability. For details, see the *Cisco vPath and vServices Reference Guide for VMware vSphere*.

Cisco Virtual Security Gateway Configuration for the Network

Cisco VSG Configuration Overview

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 Cisco VSG.

**Note**

For information about how to configure the Cisco VSG for the Cisco Nexus 1000V Series switch and the Cisco Cloud Service Platform Virtual Services Appliance, see the *Cisco vPath and vServices Reference Guide for VMware vSphere*.

Cisco Nexus 1000V Series Switch VSM

The VSM controls multiple VEMs as one logical modular switch. Instead of physical line cards, the VSM supports VEMs that run in software inside servers. Configurations are performed through the VSM and are 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 that are 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, which provides 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 virtual Ethernet or Ethernet interfaces are assigned in the vCenter Server to a port profile for the following functions:

- To define a port configuration by a 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 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 access control list (ACL) or quality of service (QoS) policies in the port profile. The information related to the 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 Prime NSC, and the network administrator associates it to an appropriate port profile in the 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 that are 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 multi-tenancy requirements. Different tenants can have their own Cisco VSG (or set of Cisco VSGs), which enforce 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
- Zones
- Rules
- Actions

Object Groups

An object group is a set of conditions relevant to an attribute.

Because the object groups 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. Zone definitions can be written as condition-based subnet and endpoint IP addresses.

Because zones can be shared between various rules with different directions, the attributes used in a zone 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 for filtering the traffic. The policy engine uses the policy as a configuration that filters the network traffic that is received on the Cisco VSG. The policy engine uses two types of condition matching models for filtering the network traffic:

- AND Model: A rule is set to matched when all the attributes in a rule match.
- OR model: A rule is set to matched when any one of the attributes in a rule match. The attributes are classified into five different types of columns. The five columns in an OR model are:
 - Source: Attribute to identify source host.
 - Destination: Attribute to identify destination host.
 - Service: Attribute to identify service at the destination host.
 - Ether type: Attribute to identify link level protocol.
 - Source port: Attribute to identify source port.

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
- Reset
- Log
- Inspection

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 3 Mode

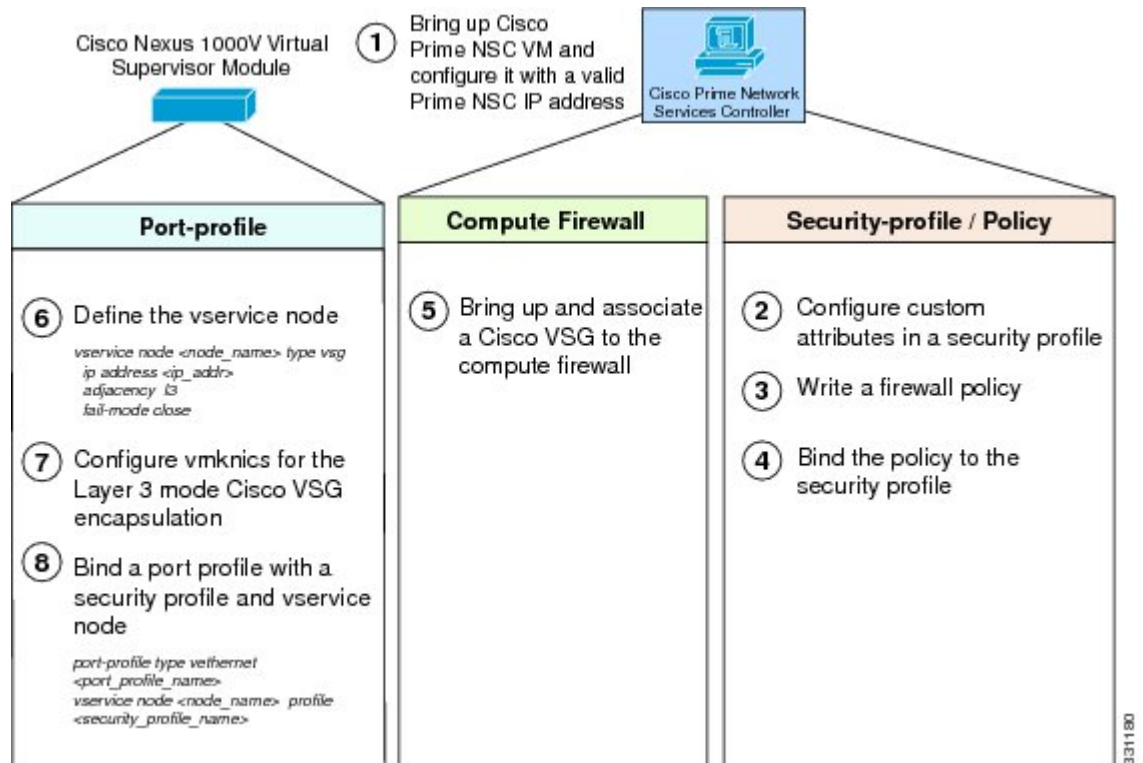
Before configuring a Cisco VSG in Layer 3 mode, create a Layer 3 vmknics

This section is an overview of the sequences that you, as an administrator, must follow when configuring a Cisco VSG in Layer 3 mode:

- 1 Install and set up a Cisco Prime NSC service VM and configure the Cisco Prime NSC 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 Prime NSC.
- 3 Write a firewall policy on the Cisco Prime NSC by using 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 Prime NSC.
- 5 Bring up a Cisco VSG and associate it to the appropriate compute firewall on the Cisco Prime NSC.
- 6 Configure the vmknics for the Layer 3 mode Cisco VSG encapsulation.
- 7 Configure VSG and virtual network adapter in same VLAN/network.
- 8 Define the vservice node.

- 9 After the security profile and firewall policy are fully configured, you can bind the security profile and the service node with the VM port profiles that demand access protection provided by the Cisco VSG through the port profile management interface on the VSM.

Figure 4: Cisco Virtual Security Gateway Layer 3 Configuration Flow



Feature History for Overview

Feature Name	Releases	Feature Information
Virtual Extensible LANs	Cisco Nexus 1000V Release 4.2(1)SV2(2.1)	Cisco Nexus 1000V supports enhanced VXLAN.
Virtual Extensible LANs	Release 4.2(1)VSG1(4)	Cisco VSG that resides in a VXLAN is supported.
Cisco vPath Service Chaining	Cisco Nexus 1000V Release 4.2(1)SV1(5.2)	The Cisco vPath supports service chaining.