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 software.

This chapter includes the following sections:

Information About the Cisco Virtual Security Gateway

This section provides an overview of the Cisco VSG for the Cisco Nexus 1000V Series switch and includes the following sections:

Overview

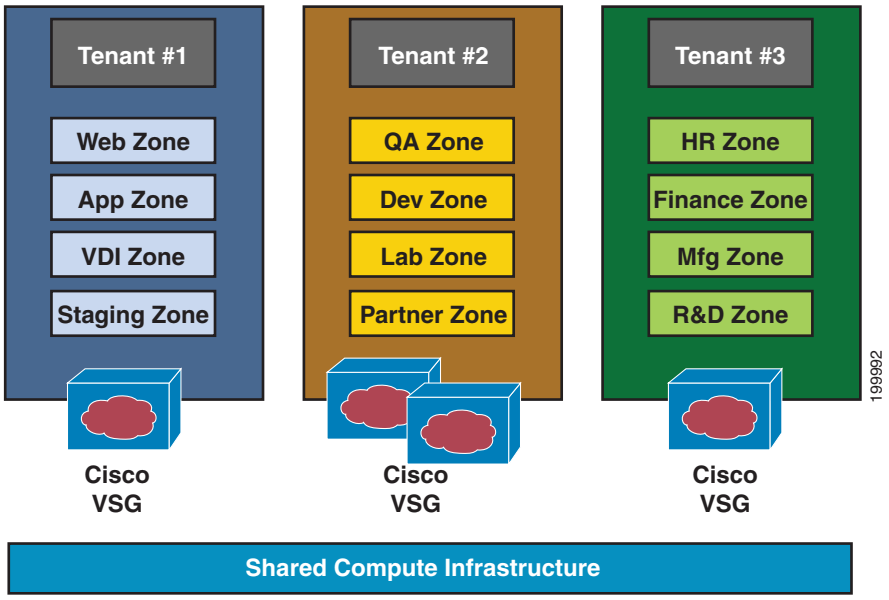
The Cisco Virtual Security Gateway (VSG) is a virtual firewall appliance that provides trusted access to virtual data center and cloud environments. The Cisco VSG enables a broad set of multitenant workloads that have varied security profiles to share a common compute infrastructure in a virtual data 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 the Cisco Nexus 1000V Series switch and running on the Cisco NX-OS operating system, the Cisco VSG provides the following benefits (see Figure 1-1):

- Trusted Multitenant Access—Granular, zone-based control and monitoring with context-aware security policies applied 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 while enhancing collaboration, eliminating administrative errors, and simplifying audits.

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



The Cisco VSG provides the following advantages:

- Enhances compliance with industry regulations
- Simplifies audit processes in virtualized environments
- Reduces cost by securely deploying a broad set of 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 distributed virtual switch 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:

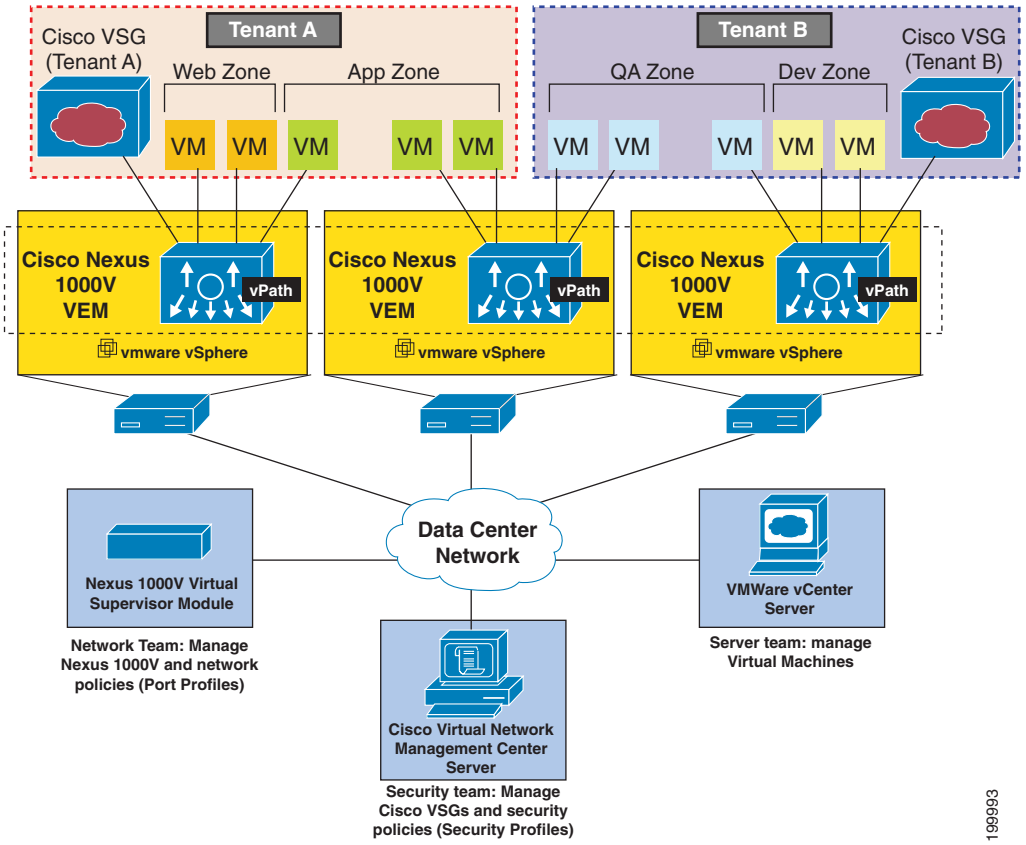
- Intelligent interception and redirection—Tenant-aware flow classification and subsequent redirection to a designated Cisco VSG tenant
- Fast-path off-load—Per-tenant policy enforcement of flows off-loaded by the Cisco VSG to vPath

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



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 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.

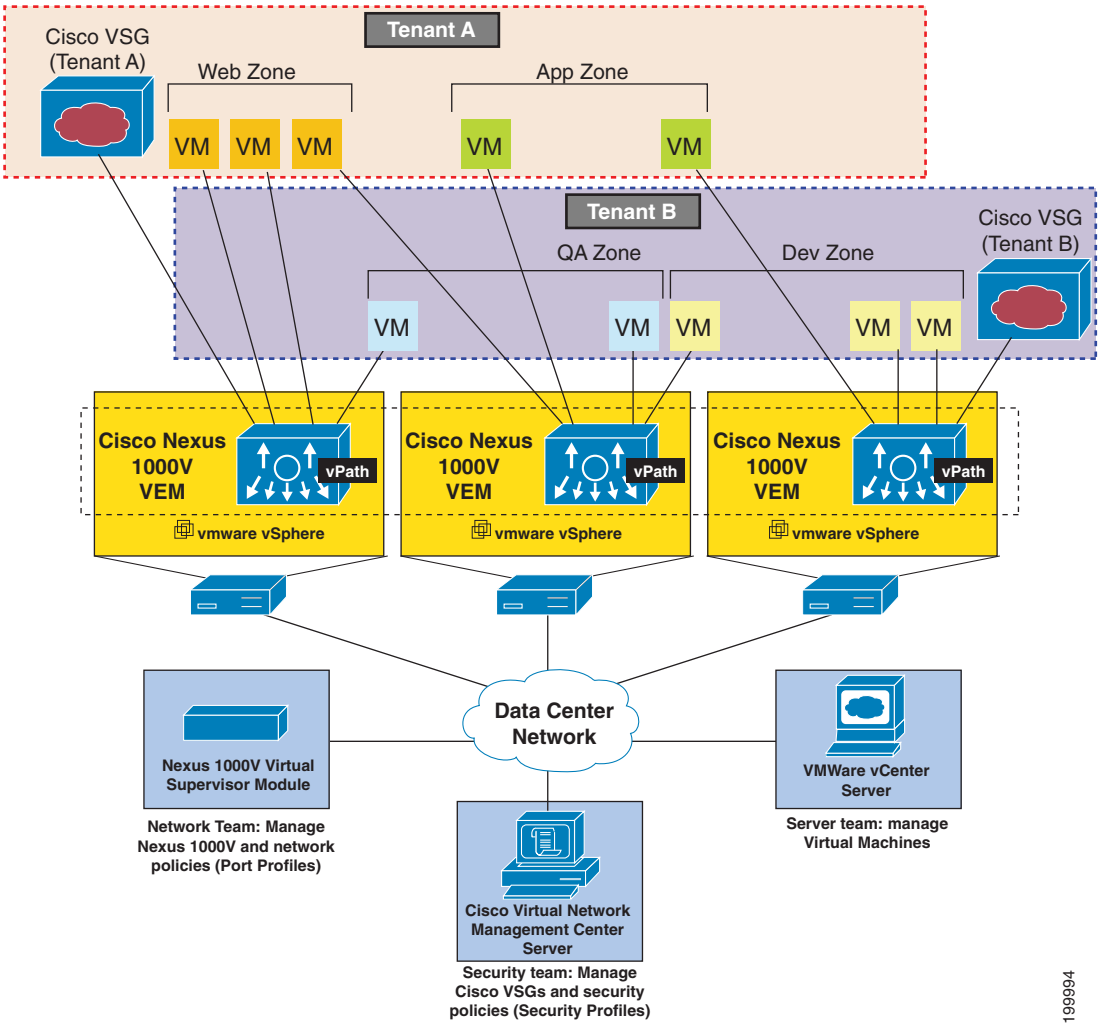
Dynamic (Virtualization-Aware) Operation

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



Cisco Virtual Security Gateway Configuration for the Network

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

- Setting Up Cisco VSGs and VLANs, page 1-5
- Cisco VSG Configuration Overview, page 1-6
- Sequence in Configuring a Cisco VSG, page 1-9

Setting Up Cisco VSGs and VLANs

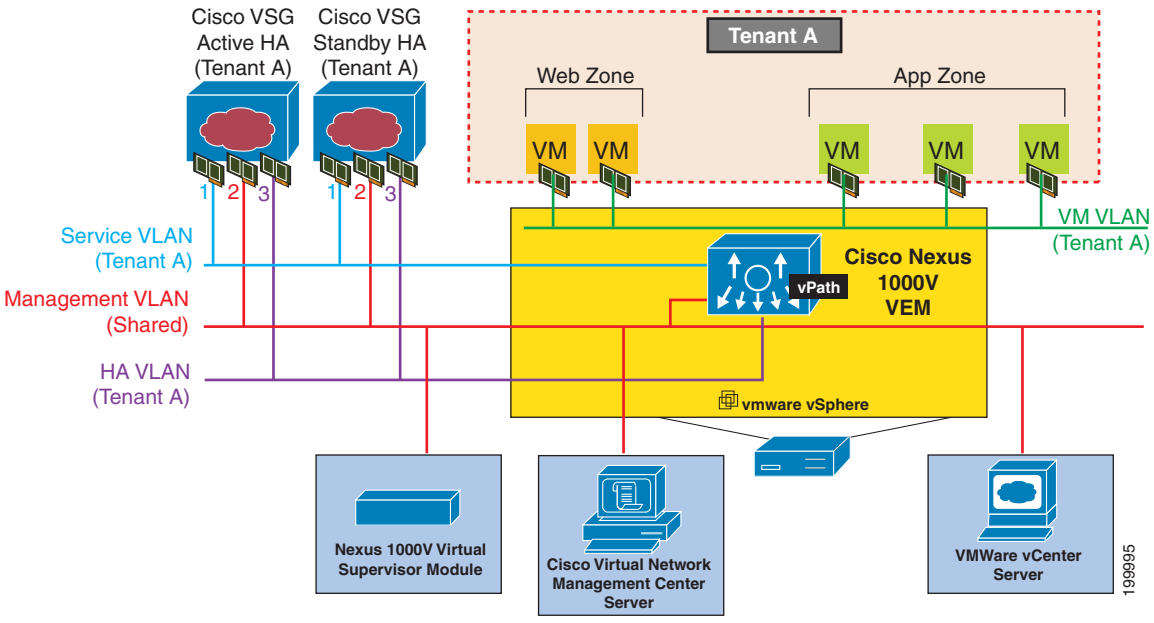
The Cisco VSG is set up so that VMs can reach a Cisco VSG irrespective of its location. The vPath component in the Cisco Nexus 1000V VEM intercepts the packets from the VM and sends them to the Cisco VSG for further processing.

Figure 1-4 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 the 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 1-4 Cisco Virtual Security Gateway VLAN Usages



Cisco VSG Configuration Overview

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

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 itself.

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 running 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

A firewall policy is used to enforce network traffic on a Cisco VSG. A key component operating on the Cisco VSG is the policy engine. The policy engine uses the policy as a configuration and executes it when enforced against 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 1-8
- Zones, page 1-8
- Rules, page 1-8
- Actions, page 1-8
- Policies, page 1-9

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
- 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

This section is an overview of the sequence to follow in configuring a Cisco VSG:

1. Install and set up a Cisco VSG service VM and configure the Cisco VSG with a valid IP address.
2. As 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 VSG.
3. As administrator, write a firewall policy on the Cisco VSG by using appropriate policy objects such as object-group, zones, rules, conditions, actions, and policies.
4. After the firewall policy is created, as administrator, bind the policy to the security profile previously created. This step is done with the security profile management interface.
5. After the security profile and firewall policy are fully developed, as 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 administrator, you must also bind the Cisco VSG with the set of VM port profiles.

Figure 1-5 Cisco Virtual Security Gateway Configuration Flow