Cisco Virtual Security Gateway for Nexus 1000V Series Switch Configuration Guide, Release 4.2(1)VSG1(3.1)

March 21, 2014

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide.
Addresses, phone numbers, and fax numbers
are listed on the Cisco website at
www.cisco.com/go/offices.

CONTENTS

Preface

This preface describes the audience, organization, and conventions of the *Cisco Virtual Security Gateway for Nexus 1000V Series Switch Configuration Guide, Release 4.2(1)VSG1(3.1)* . It also provides information about how to obtain related documentation.

This preface includes the following sections:

Audience

This publication is for those who have an understanding of virtualization and experience with using VMware tools to create virtual machines and have the following responsibilities:

- Security Administration—Define and administer security policies and rules.
- Network Administration—Manage and associate the security policies to particular port profiles.
- ESX Server Administration—Select the appropriate port-group (Cisco Nexus 1000V equivalent port-profile) for the particular virtual machines (VM).

Note Knowledge of VMware vNetwork Distributed Switch is not a prerequisite.

Document Organization

This document is organized as follows:

Chapter and Title	Description
Chapter 1, "Cisco Virtual Security Gateway Overview"	Provides an overview of the Cisco Virtual Security Gateway.
Chapter 2, "Cisco Virtual Security Gateway Command-Line Interface"	Describes how to use the CLI on a Cisco Virtual Security Gateway.

Chapter and Title	Description
Chapter 3, "Configuring the Cisco Virtual Security Gateway"	Describes how to configure the Cisco Virtual Security Gateway port profile on the Cisco Nexus 1000V Series switch for protecting network traffic.
Chapter 4, "Cisco Virtual Security Gateway System Management"	Describes CLI configurable aspects of the Cisco Virtual Security Gateway.
Chapter 5, "Cisco Virtual Security Gateway High Availability"	Describes Cisco Virtual Security Gateway high availability concepts and configuration.
Chapter 6, "Cisco Virtual Security Gateway Firewall Profiles and Policy Objects"	Describes how to verify Cisco Virtual Security Gateway firewall policy configurations.

Document Conventions

Command descriptions use these conventions:

Convention	Description
boldface font	Commands and keywords are in boldface.
italic font	Arguments for which you supply values are in italics.
{ }	Elements in curly brackets are required.
[ ]	Elements in square brackets are optional.
[x	y	z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.

Screen examples use these conventions:

`screen font`	Terminal sessions and information that the switch displays are in screen font.
`boldface screen font`	Information that you must enter is in boldface screen font.
`italic screen font`	Arguments for which you supply values are in italic screen font.
< >	Nonprinting characters, such as passwords, are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

This document uses the following conventions:

Note Means reader *take note*. Notes contain helpful suggestions or references to material not covered in the manual.

> ⚠️
>
> **Caution** Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

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(3.1)*

- *Cisco Virtual Security Gateway, Release 4.2(1)VSG1(3.1) and Cisco Virtual Network Management Center, Release 1.3 Installation and Upgrade Guide*

- *Cisco Virtual Security Gateway for Nexus 1000V Series Switch License Configuration Guide, Release 4.2(1)VSG1(3.1)*

- *Cisco Virtual Security Gateway for Nexus 1000V Series Switch Configuration Guide, Release 4.2(1)VSG1(3.1)*

- *Cisco Virtual Security Gateway for Nexus 1000V Series Switch Command Reference, Release 4.2(1)VSG1(3.1)*

- *Cisco Virtual Security Gateway for Nexus 1000V Series Switch Troubleshooting Guide, Release 4.2(1)VSG1(3.1)*

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

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 and Cisco currently supports RSS version 2.0.

New and Changed Information

This chapter provides release-specific information for each new and changed feature in the *Cisco Virtual Security Gateway for Nexus 1000V Series Switch Configuration Guide, Release 4.2(1)VSG1(3.1)*. The latest version of this document is available at the following Cisco website: http://www.cisco.com/go/techdocs.

To check the additional information about Release 4.2(1)VSG1(3.1), see the *Cisco Virtual Security Gateway for Nexus 1000V Series Switch Release Notes, Release 4.2(1)VSG1(3.1)* available at the following Cisco website: http://www.cisco.com/go/techdocs.

Table 1 summarizes the new and changed features for the *Cisco Virtual Security Gateway for Nexus 1000V Series Switch Configuration Guide, Release 4.2(1)VSG1(3.1)*.

Table 1   New and Changed Information in Release 4.2(1)VSG1(3.1)

Feature	Description	Changed in Release	Where Documented
Cisco VSG support in the Layer 2 and Layer 3 mode	Time out for the fast connection between the CIsco VSG and VEM.	Release 4.2(1)VSG1(3.1)	Fast Path Connection Timeouts, page 1-4
	The Cisco VSG deployment in the Layer 3 mode. The VEM and the Cisco VSG communicate with each other through a vmknic.		Cisco VSG Deployment Scenarios, page 1-8
	The sequencse to follow when configuring a Cisco VSG in the Layer 2 and Layer 3 mode.		• 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
	The sequences to follow when migrating the Cisco VSG deployment from Layer 2 to Layer 3 mode.		Migrating from Layer 2 Mode to Layer 3 Mode, page 1-15
	Configurtion of the IP address and the security port-profile on the VSM for a Cisco VSG in the Layer 2 and Layer 3 mode.		• Configuring the Port Profile on the VSM for a Cisco VSG in the Layer 2 Mode, page 3-1 • Configuring the Port Profile on the VSM for a Cisco VSG in the Layer 3 Mode, page 3-3

Table 1　　　*New and Changed Information in Release 4.2(1)VSG1(3.1) (continued)*

Feature	Description	Changed in Release	Where Documented
Cisco VSG support in the Layer 2 and Layer 3 mode	The vPath ping command examples to verify various connections and reachable attributes of the VSG VSN in the Layer 3 mode.	Release 4.2(1)VSG1 (3.1)	vPath Ping Command for the Layer 3 Mode, page 3-11
TCP state-checks	Enabled by default, performs TCP state-checks on the vPath.	4.2(1)VSG1 (2)	Configuring TCP State-Checks for All Cisco VSG VSNs in a vPath, page 3-7
vPath Ping	Verifies the connectivity and reachability of the VSG VSNs in the vPath.	4.2(1)VSG1 (2)	Verifying the Cisco VSG Configuration, page 3-9

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

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

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**
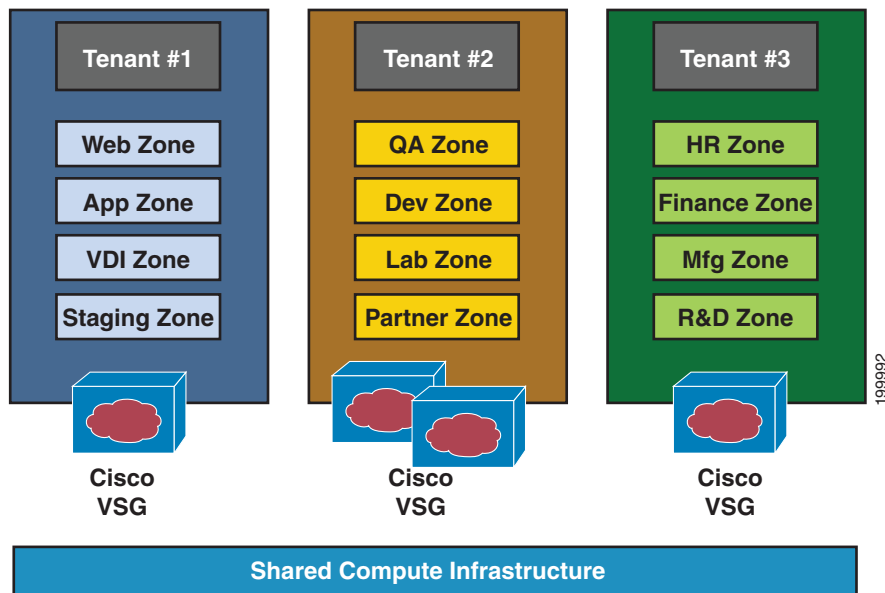
The Cisco VSG does the following:

- 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
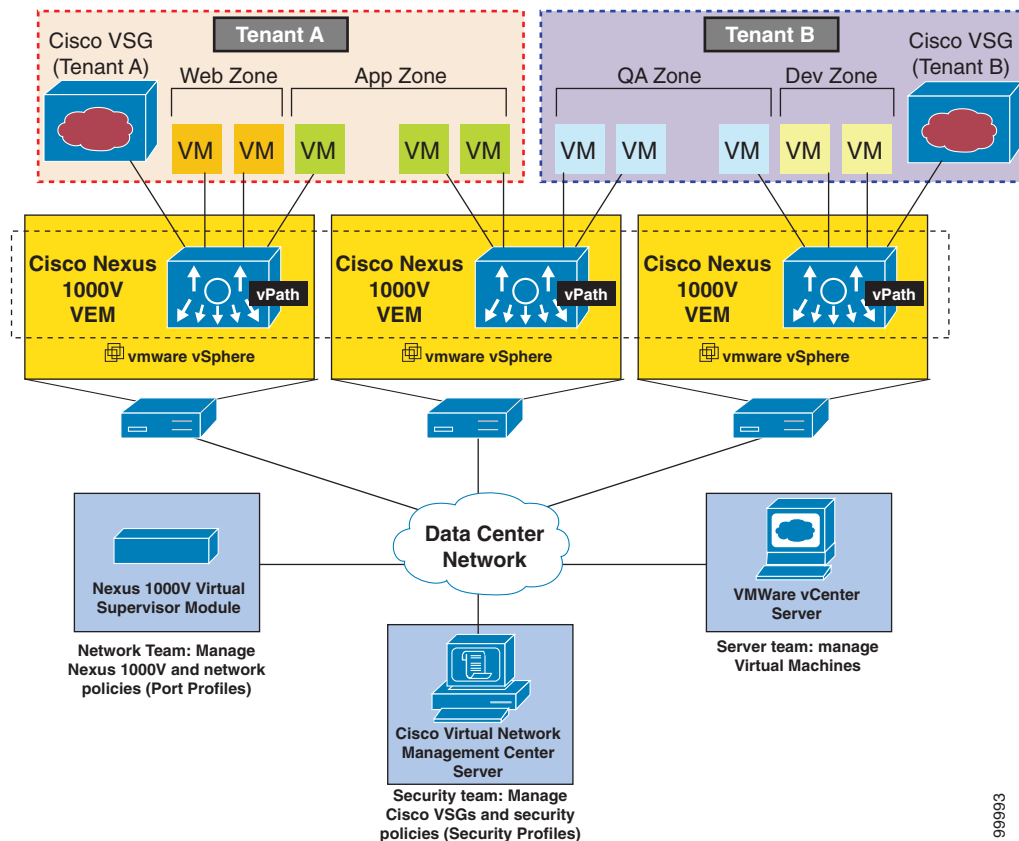
Fast Path Connection Timeouts

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
	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
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

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
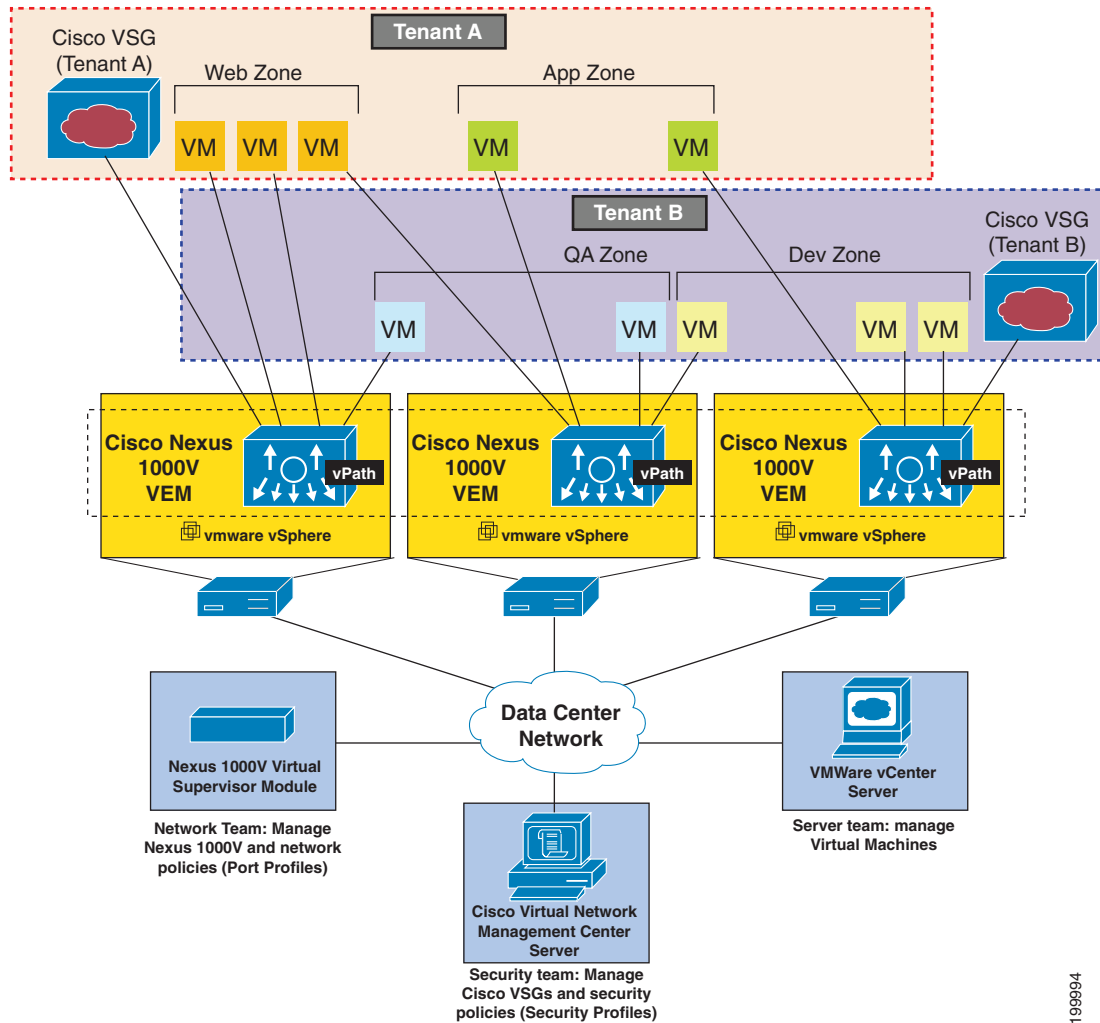
Cisco VSG on the Cisco Nexus 1010 Virtual Services Appliance

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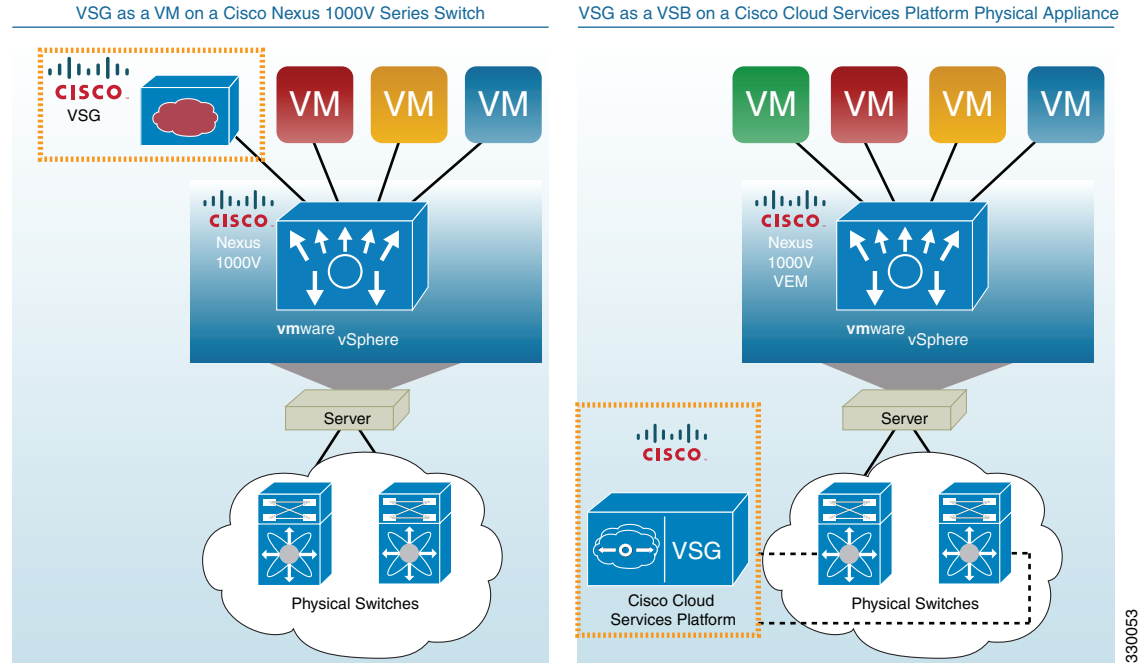
Figure 1-5 shows the Cisco Nexus 1010 software components and how they relate to the Cisco VSG.

Figure 1-5   *Cisco Nexus 1010 Software Components*
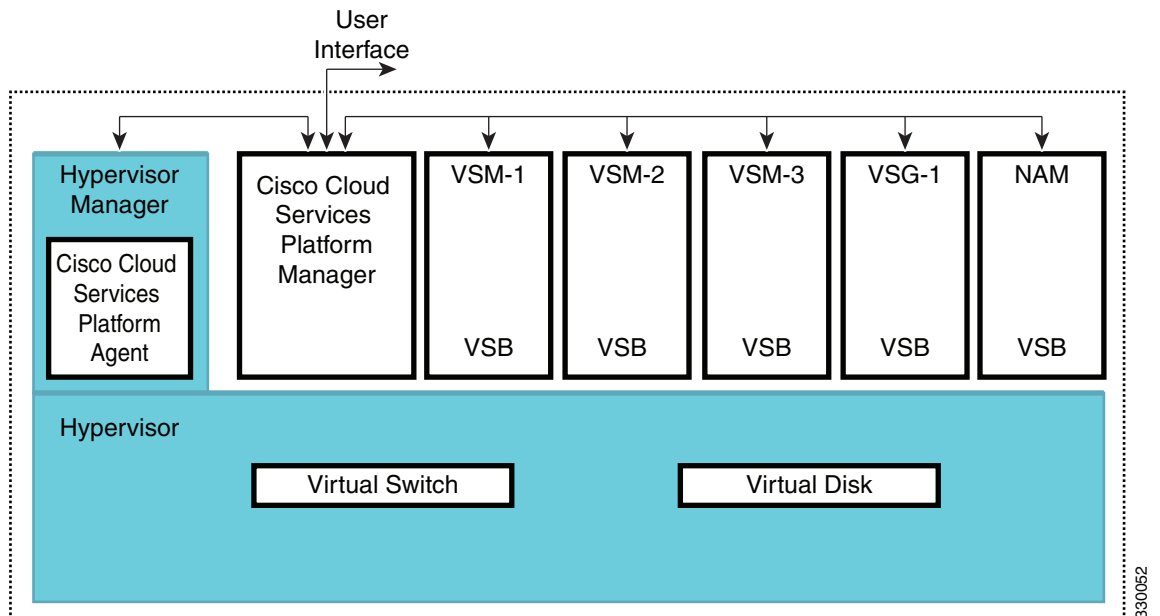
For more information about the *Cisco Nexus 1010,* see the *Cisco Nexus 1010 Software Configuration Guide*.

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 vnmknic 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 l3-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)SV1(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 l3-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 l3-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

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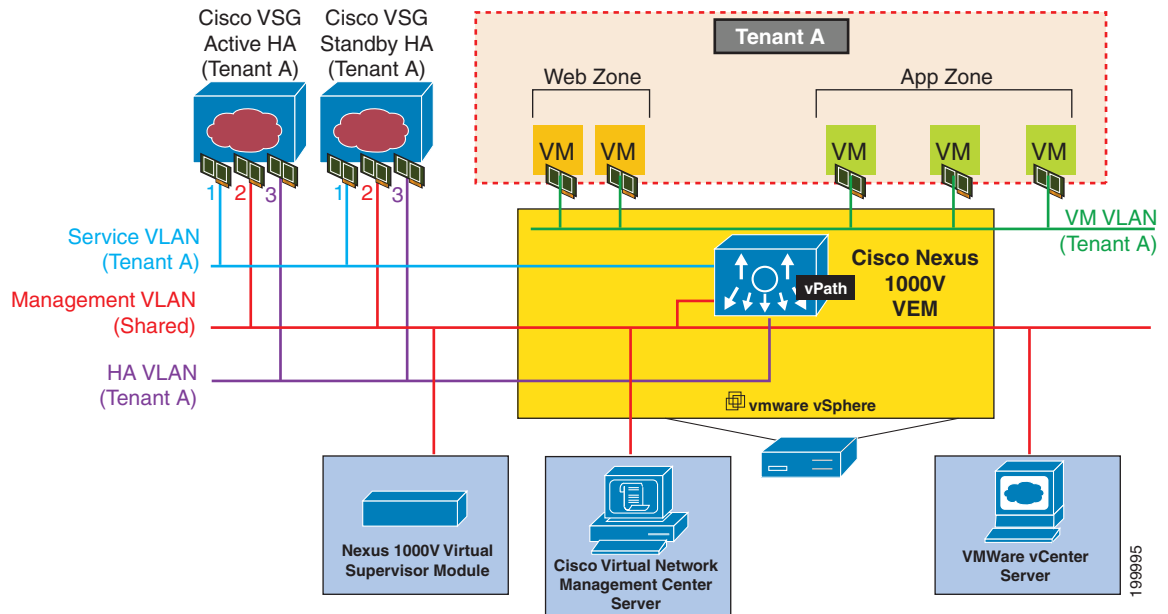
Note   The Cisco VSG will not be on a VXLAN. The Cisco VSG supports the VXLAN data traffic only . For details, see the *Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.2(1)SV1(5.1)*.

Cisco VSG Configuration Overview

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

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
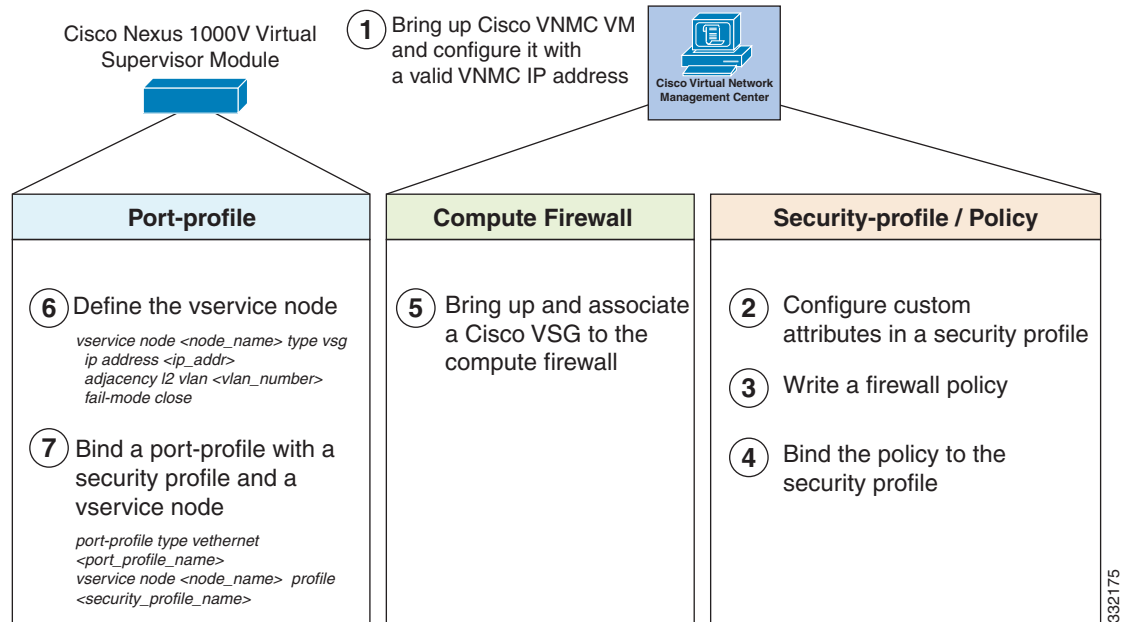
Sequence in Configuring a Cisco VSG in the Layer 3 Mode

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***

Prime NSC IP address   Services Controller

Port-profile	Compute Firewall	Security-profile / Policy
⑥ Define the vservice node *vservice node <node_name> type vsg* *ip address <ip_addr>* *adjacency l3* *fail-mode close* **⑦ Configure vmknics for the Layer 3 mode Cisco VSG encapsulation** **⑧ Bind a port profile with a security profile and vservice node** *port-profile type vethernet* *<port_profile_name>* *vservice node <node_name> profile* *<security_profile_name>*	**⑤ Bring up and associate a Cisco VSG to the compute firewall**	**② Configure custom attributes in a security profile** **③ Write a firewall policy** **④ Bind the policy to the security profile**

331180

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 theVEM- 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).

CHAPTER 2

Cisco Virtual Security Gateway Command-Line Interface

This chapter describes the Cisco Virtual Security Gateway (VSG) command-line interface (CLI).

This chapter includes the following sections:

Note   Information about the Cisco VSG CLI is provided in this chapter. For information about the Cisco Nexus 1000V Series switch CLI or the Cisco Nexus 1010 Virtual Services Appliance CLI, see the respective product's documentation.

Information About the CLI Prompt

Once you have successfully accessed the system, the CLI prompt displays in the terminal window of your console port or remote workstation, as follows:

```
switch#
```

You can change this switch prompt to another name or leave it as it is.

```
switch# configure
switch(config)# switchname vsg100
switch(config)# exit
vsg100#
```

From the CLI prompt, you can do the following:

- Use CLI commands for configuring features.
- Access the command history.

- Use command parsing functions.

Command Modes

This section includes the following topics:

- Information About Command Modes, page 2-2
- EXEC Command Mode, page 2-3
- Global Configuration Command Mode, page 2-3
- Exiting a Configuration Mode, page 2-3
- Command Mode Summary, page 2-4

Information About Command Modes

The CLI is divided into command modes that define the actions available to the user. Command modes are "nested" and are accessed in sequence. When you first log in, you are placed in CLI EXEC mode.

As you navigate from EXEC mode to global configuration mode, a larger set of commands is available to you. To transition to global configuration mode, enter the following command:

config t

Table 2-1 shows how command access builds from user EXEC to global configuration mode.

Table 2-1   Accessing the Global Configuration Mode

Command Mode	Prompt	Description
EXEC	`vsg#`	• Connect to remote devices. • Temporarily change terminal line settings. • Do basic tests. • List system information (show).
Global configuration	`vsg(config)#`	Includes access to EXEC commands. • Connect to remote devices. • Temporarily change terminal line settings. • Perform basic tests. • List system information (show).

All commands in EXEC command mode are accessible from the global configuration command mode. For example, the **show** commands are available from any command mode.

EXEC Command Mode

When you first log in, you are placed into EXEC mode. The commands available in EXEC mode include the **show** commands that display device status and configuration information, the **clear** commands, and other commands that perform actions that you do not save in the device configuration.

Global Configuration Command Mode

Global configuration mode provides access to the widest range of commands, including those commands used to make configuration changes that are saved by the device and can be stored and applied when the device is rebooted.

Commands entered in global configuration mode update the running configuration file as soon as they are entered, but must also be saved into the startup configuration file by using the following command:

copy running-config startup-config

In global configuration mode, you can access protocol-specific, platform-specific, and feature-specific configuration modes.

Exiting a Configuration Mode

To exit from any configuration mode, use one of the following commands:

Command	Purpose
exit **Example:** vsg(config-rule)# exit vsg(config)#	Exits from the current configuration command mode and returns to the previous configuration command mode.
end **Example:** vsg(config)# end vsg#	Exits from the configuration command mode and returns to EXEC mode.
Ctrl-z **Example:** vsg(config)# ^z vsg#	Exits the current configuration command mode and returns to EXEC mode. ⚠️ **Caution** If you press **Ctrl-Z** at the end of a command line in which a valid command has been typed, the CLI adds the command to the running configuration file. We recommend that you exit a configuration mode using the **exit** or **end** command.

Command Mode Summary

Table 2-2 summarizes information about command modes.

Table 2-2   Command Mode Summary

Mode	Access Method	Prompt	Exit Method
EXEC	From the login prompt, enter your username and password.	`VSG#`	To exit to the login prompt, use the **exit** command.
Global configuration	From EXEC mode, enter the command, **configure**.	`VSG(config)#`	To exit to EXEC mode, use the **end** or **exit** command or press **Ctrl-Z**.
Zone configuration	From global configuration mode, enter the command, **zone** *zone-name*.	`VSG(config-zone)#`	To exit to global configuration mode, use the **exit** command. To exit to EXEC mode, use the **end** command or press **Ctrl-Z**.
Data0 interface configuration	From global configuration mode, enter the command **interface data0**	`VSG(config-if)#`	To exit to global configuration mode, use the **exit** command. To exit to EXEC mode, use the **end** command or press **Ctrl-Z**.

Saving CLI Configuration Changes

This section describes how to save CLI configuration changes and includes the following topics:

- Running Configuration, page 2-4
- Startup Configuration, page 2-4
- Copying the Running Configuration to the Startup Configuration, page 2-5

Running Configuration

The running configuration is the configuration that is currently running on the device. It includes configuration changes from commands entered since the last time the device was restarted. If the device is restarted, the running configuration is replaced with a copy of the startup configuration. Any changes that were made to the running configuration but were not copied to the startup configuration are discarded.

Startup Configuration

The startup configuration is the configuration that is saved and that will be used by the device when you restart it. When you make configuration changes to the device, they are automatically saved in the running configuration. If you want configuration changes saved permanently, you must copy them to the startup configuration so that they are preserved when the device is rebooted or restarted.

Copying the Running Configuration to the Startup Configuration

To copy changes you have made to the running configuration into the startup configuration so that they are saved persistently through reboots and restarts, use the following command:

	Command	Purpose

Step 1	`copy running-config startup-config`
	
	Example:
	`vsg(config)# copy running-config`
	`startup-config`
		(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Special Characters

Table 2-3 lists the characters that have special meaning in text strings and should be used only in regular expressions or other special contexts.

Table 2-3   Special Characters

Character	Description
|	Vertical bar
< >	Less than or greater than

Keystroke Shortcuts

Table 2-4 lists command key combinations that can be used in both EXEC and configuration modes.

Table 2-4   Keystroke Shortcuts

Key(s)	Description
Ctrl-**A**	Moves the cursor to the beginning of the line.
Ctrl-**B**	Moves the cursor one character to the left. When you enter a command that extends beyond a single line, you can press the Left Arrow or Ctrl-B keys repeatedly to scroll back toward the system prompt and verify the beginning of the command entry, or you can press the Ctrl-A key combination.
Ctrl-**C**	Cancels the command and returns to the command prompt.
Ctrl-**D**	Deletes the character at the cursor.
Ctrl-**E**	Moves the cursor to the end of the line.
Ctrl-**F**	Moves the cursor one character to the right.
Ctrl-**G**	Exits to the previous command mode without removing the command string.
Ctrl-**K**	Deletes all characters from the cursor to the end of the command line.
Ctrl-**L**	Redisplays the current command line.
Ctrl-**R**	Redisplays the current command line.

Table 2-4   Keystroke Shortcuts (continued)

Key(s)	Description
Ctrl-T	Transposes the character to the left of the cursor with the character located to the right of the cursor.
Ctrl-U	Deletes all characters from the cursor to the beginning of the command line.
Ctrl-W	Deletes the word to the left of the cursor.
Ctrl-X, H	Lists history. When using this key combination, press and release the Ctrl and X keys together before pressing H.
Ctrl-Y	Recalls the most recent entry in the buffer (press keys simultaneously).
Ctrl-Z	Ends a configuration session, and returns you to EXEC mode. When used at the end of a command line in which a valid command has been typed, the resulting configuration is first added to the running configuration file.
↑	Displays the previous command in the command history.
↓	Displays the next command in the command history.
→ ←	Moves your cursor through the command history directionally to locate a command string.
?	Displays a list of available commands.

Tab	Completes the word for you after you enter the first characters of the word and then press the Tab key. All options that match are presented. Used to complete: - Command names - Scheme names in the file system - Server names in the file system - File names in the file system This example shows how to use the tab keystroke:
	`vsg(config)# xm<Tab>`
	`vsg(config)# xml <Tab>`
	`vsg(config)# xml server`
	
	This example shows how to use the tab keystroke:
	
	`vsg(config)# vn<Tab>`
	`vnm-policy-agent vns-binding`
	
	`vsg(config)# security-pr<Tab>`
	`vsg(config)# security-profile`

Abbreviating Commands

You can abbreviate commands and keywords by entering the first few characters of a command. The abbreviation must include enough characters to make it unique from other commands or keywords. If you are having trouble entering a command, check the system prompt and enter the question mark (?) for a list of available commands. You might be in the wrong command mode or using incorrect syntax.

Table 2-5 lists examples of command abbreviations.

Table 2-5   Examples of Command Abbreviations

Command	Abbreviation
configure	conf
copy running-config startup-config	copy run start
show running-config	sho run

Using the no Form of a Command

Almost every configuration command has a **no** form that can be used to disable a feature or function. For example, to remove a VLAN, use the **no vlan** command. To re-enable it, use the **vlan** command form.

For example, if you use the **boot** command in global configuration mode, you can then use the **no boot** command to undo the results:

```
vsg(config)# boot system bootflash: svs1.bin
vsg(config)# no boot system bootflash: svs1.bin
```

Using Help

The CLI provides the following help features (see Table 2-6 and Table 2-7).

Table 2-6   CLI Help Features

Feature	Description
?	Type the question mark (?) to list the valid input options.
^	The CLI prints the caret (^) symbol below a line of syntax to point to an input error in the command string, keyword, or argument.
↑	Use the up arrow to have the CLI display the previous command you entered so that you can correct an error.

The example in Table 2-7 describes how to use syntax error isolation and context-sensitive help.

Table 2-7   Using Syntax Error Isolation and Context-Sensitive Help on the CLI

	Command	Purpose
Step 1	`show interface ?` **Example:** `vsg# show interface ?` `  <CR>` `  >                Redirect it to a file` `  >>               Redirect it to a file in append mode` `  brief            Show brief info of interface` `  capabilities     Show interface capabilities information` `  counters         Show interface counters` `  data             Data interface` `  debounce         Show interface debounce time information` `  description      Show interface description` `  ethernet         Ethernet IEEE 802.3z` `  fcoe (no abbrev) Show FCoE info for interface` `  loopback         Loopback interface` `  mac-address      Show interface MAC address` `  mgmt             Management interface` `  port-channel     Port Channel interface` `  snmp-ifindex     Show snmp ifindex list` `  status           Show interface line status` `  switchport       Show interface switchport information` `  transceiver      Show interface transceiver information` `  trunk            Show interface trunk information` `  vethernet        Virtual ethernet interface` `  virtual          Show virtual interface information` `	Pipe command output to filter`  `vsg#`	Displays the optional parameters used with the **show interface** command in EXEC mode.

Step 2	`show interface module ?`
	
	Example:
	`vsg# show interface module ?`
	`                    ^`
	`Invalid command (interface name) at '^' marker.`
	`?`
	`vsg#`
		Displays an invalid command error message and points (^) to the syntax error.

Step 3	`Ctrl-P` or the Up Arrow
	
	Example:
	`vsg# <Ctrl-P>`
	`vsg# show interface data0`
		Displays the previous command you entered so that you can correct the error.

Step 4	`show interface data ?`
	
	Example:
	`vsg# show interface data ?`
	`  <0-0>  Data interface number`
	`vsg#`
		Displays the syntax for showing a data interface (data0).

Table 2-7 **Using Syntax Error Isolation and Context-Sensitive Help on the CLI (continued)**

	Command	**Purpose**

Step 5	`show interface data0`
	
	Example:
	`vsg# show interface data0`
	`control0 is up`
	`  Hardware: Ethernet, address: 0050.5691.53b6 (bia`
	`0050.5691.53b6)`
	`  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,`
	`    reliability 255/255, txload 1/255, rxload 1/255`
	`  Encapsulation ARPA`
	`  full-duplex, 1000 Mb/s`
	`  Auto-Negotiation is turned on`
	`  1 minute input rate 1920 bits/sec, 0 packets/sec`
	`  1 minute output rate 24 bits/sec, 0 packets/sec`
	`  Rx`
	`    91082 input packets 0 unicast packets 2935 multicast`
	`packets`
	`    88147 broadcast packets 20642956 bytes`
	`  Tx`
	`    21968 output packets 0 unicast packets 21968 multicast`
	`packets`
	`    0 broadcast packets 5228289 bytes`
	
	`vsg#`
		Displays the data interface (data0).

Configuring the Cisco Virtual Security Gateway

This chapter describes how to configure the Cisco Virtual Security Gateway (VSG) for the Cisco Nexus 1000V Series switch and the Cisco Nexus 1010 Virtual Services Appliance.

This chapter includes the following sections:

For additional details about the Cisco Nexus 1000V Series switch port profiles, see the *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(5.1)*.

Configuring the Port Profile on the VSM for a Cisco VSG in the Layer 2 Mode

BEFORE YOU BEGIN

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

- You have the Cisco VSG software installed and the basic installation completed. For details, see the *Cisco Virtual Security Gateway, Release 4.2(1)VSG1(3.1) and Cisco Virtual Network Management Center, Release 1.3 Installation and Upgrade Guide.*

- You must have the NEXUS_VSG_SERVICES_PKG license installed on the switch. Ensure that you have enough licenses to cover the number of Virtual Ethernet Modules (VEMs) you want to protect.

- The data IP address and management IP addresses should be configured. To configure the data IP address, see the *Cisco Virtual Security Gateway, Release 4.2(1)VSG1(3.1) and Cisco Virtual Network Management Center, Release 1.3 Installation and Upgrade Guide*.

- You have completed creating the Cisco VSG port profiles for the service and high-availability (HA) interface. see the"Cisco VSG Configuration Guidelines and Limitations" section on page 6-2

- You are logged in to the switch CLI in EXEC mode.

SUMMARY STEPS

1. **configure**

2. **port-profile** *port-profile-name*

3. **org** *org-name*

4. **vn-service ip-address** *ip-address* **vlan** *vlan-id* [**fail** {**open** | **close**}] [**security-profile** *security-profile-name*]

5. (Optional) **copy running-config startup-config**

6. **exit**

DETAILED STEPS

	Command	Purpose

Step 1	`configure`
	
	Example:
	`n1000v# configure`
	`n1000v(config)#`
		Places you in global configuration mode.

Step 2	`port-profile` *port-profile-name*
	
	Example:
	`n1000v(config-port-prof)# port-profile`
	`host-profile`
	`n1000v(config-port-prof)#`
		Enters the port profile configuration mode for the named port profile. If the port profile does not exist, it is created using the following characteristics:
		
		port-profile-name—The port profile name can be up to 80 alphanumeric characters and must be unique for each port profile on the Cisco VSG.

Step 3	`org` *org-name*
	
	Example:
	`n1000v(config-port-prof)# org`
	`root/Tenant-A`
	`n1000v(config-port-prof)#`
		Designates an organization name for the Cisco VSG port profile.

Step 4	`vn-service ip-address` *ip-address* `vlan`
	vlan-id [`fail` {`open`
		`close`}]
		[`security-profile` *security-profile-name*]
		
		Example:
		`n1000v(config-port-prof)# vn-service ip`
		`100.1.1.100 vlan 1000 profile vnsp-1`
		`n1000v(config-port-prof)#`
			Configures the IP address, VLAN ID, and profile for the Cisco VSG, and optionally allows a fail-safe configuration.
			
			Note The IP address must match the data interface (data0) IP address on the Cisco VSG.
			
			Note If you do not pick a security profile name, the default name is assumed. The security profile name must match the security profile created on the Cisco VSG.

Step 5	`copy running-config startup-config`
	
	Example:
	`n1000v(config-port-prof)# copy`
	`running-config startup-config`
	`n1000v(config-port-prof)#`
		(Optional) Saves configuration changes.

Step 6	`exit`
	
	Example:
	`n1000v(config-port-prof)# exit`
	`n1000v(config)#`
		Exits the configuration mode and returns you to the global configuration mode.

Configuring the Port Profile on the VSM for a Cisco VSG in the Layer 3 Mode

BEFORE YOU BEGIN

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

- You have the Cisco VSG software installed and the basic installation completed. For details, see the *Cisco Virtual Security Gateway, Release 4.2(1)VSG1(3.1) and Cisco Virtual Network Management Center, Release 1.3 Installation and Upgrade Guide*.

- You must have the NEXUS_VSG_SERVICES_PKG license installed on the switch. Ensure that you have enough licenses to cover the number of Virtual Ethernet Modules (VEMs) you want to protect.

- You have configured the data IP and management IP addresses. To configure the data IP address, see the *Cisco Virtual Security Gateway, Release 4.2(1)VSG1(3.1) and Cisco Virtual Network Management Center, Release 1.3 Installation and Upgrade Guide.*

- When VEM communicates with the Cisco VSG in the Layer 3 mode, an additional header with 94 bytes is added to the original packet. You must have set the MTU to a minimum of 1594 bytes to accommodate this extra header for any network interface through which the traffic passes between the Cisco Nexus 1000V and the Cisco VSG. These interfaces can include the uplink port profile, the proxy ARP router, a virtual switch or other interfaces.

- If jumbo frames are enabled in the network, you must have set the MTU of the client and server VMs to at least 94 bytes smaller than the uplink port profile MTU. For example, if the uplink port profile MTU is set to 9000 bytes, the MTU of the VMs must be 8906 bytes or less.

- You have completed creating the Cisco VSG port profiles for the service and high-availability (HA) interface. For details, see the "Cisco VSG Configuration Guidelines and Limitations" section on page 6-2.

- You are logged in to the switch CLI in EXEC mode.

SUMMARY STEPS

1. **configure**

2. **port-profile** *port-profile-name*

3. **org** *org-name*

4. **vn-service ip-address** *ip-address* **l3-mode** [**fail** {**open** | **close**}] [**security-profile** *security-profile-name*]

5. (Optional) **copy running-config startup-config**

6. **exit**

DETAILED STEPS

	Command	Purpose

Step 1	`configure`
	
	Example:
	`n1000v# configure`
	`n1000v(config)#`
		Places you in global configuration mode.

Step 2	`port-profile` *port-profile-name*
	
	Example:
	`n1000v(config-port-prof)# port-profile`
	`host-profile`
	`n1000v(config-port-prof)#`
		Enters the port profile configuration mode for the named port profile. If the port profile does not exist, it is created using the following characteristics:
		
		port-profile-name—The port profile name can be up to 80 alphanumeric characters and must be unique for each port profile on the Cisco VSG.

Step 3	`org` *org-name*
	
	Example:
	`n1000v(config-port-prof)# org`
	`root/Tenant-A`
	`n1000v(config-port-prof)#`
		Designates an organization name for the Cisco VSG port profile.

Step 4	`vn-service ip-address` *ip-address* `l3-mode`
	[`fail` {`open` │ `close`}] [`security-profile`
	security-profile-name]
	
	Example:
	`n1000v(config-port-prof)# vn-service ip`
	`100.1.1.100 l3-mode profile vnsp-1`
	`n1000v(config-port-prof)#`
		Configures the IP address, Layer 3 mode, and port profile for the Cisco VSG, and optionally allows a fail-safe configuration.
		
		Note The IP address must match the data interface (data0) IP address on the Cisco VSG.
		
		Note If you do not pick a security profile name, the default name is assumed. The security profile name must match the security profile created on the Cisco VSG.

Step 5	`copy running-config startup-config`
	
	Example:
	`n1000v(config-port-prof)# copy`
	`running-config startup-config`
	`n1000v(config-port-prof)#`
		(Optional) Saves configuration changes.

Step 6	`exit`
	
	Example:
	`n1000v(config-port-prof)# exit`
	`n1000v(config)#`
		Exits the configuration mode and returns you to the global configuration mode.

Configuring vmknics for the Layer 3 Mode VSG Encapsulation

You can configure vmknics for a Cisco VSG in the Layer 3 mode encapsulation by running the following procedure.

BEFORE YOU BEGIN

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

- Identify a VLAN to be used for transporting the Cisco VSG in the Layer 3 mode-encapsulated traffic. Ensure that VLAN is configured on the uplink port profile for all VEMs on which the Cisco VSG in Layer 3 mode can be configured.

SUMMARY STEPS

1. **configure terminal**

2. **port-profile** *profilename*

3. **vmware port-group** *name*

4. **switchport mode access**

5. **switchport access vlan** *id*

6. **capability l3-vn-service**

7. **no shutdown**

8. **state enabled**

9. (Optional) **show port-profile name** *profilename*

10. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	Enters global configuration mode.

Step 2	**port-profile** *profilename*
	
	Example:
	switch(config)# port-profile vmknic-pp
	switch(config-port-prof)
		Enters port profile configuration mode for the named port profile. If the port profile does not already exist, it is created using the following characteristics:
		
		• *profilename*—The port profile name can be up to 80 characters and must be unique for each port profile on the Cisco Nexus 1000V.
		
		Note If a port profile is configured as an Ethernet type, it cannot be used to configure VMware virtual ports.

Step 3	**vmware port-group** *name* **Example:** switch(config-port-prof)# vmware port-group switch(config-port-prof)#	Designates the port profile as a VMware port group. The port profile is mapped to a VMware port group of the same name unless you specify a name. When you connect the VSM to vCenter Server, the port group is distributed to the virtual switch on the vCenter Server.
Step 4	**switchport mode access** **Example:** switch(config-port-prof)# switchport mode access switch(config-port-prof)#	Designates the interfaces as switch access ports (the default).

	Command	Purpose

Step 5	`switchport access vlan` *`id`*
	
	Example:
	`switch(config-port-prof)# switchport access vlan 100`
	`switch(config-port-prof)`
		Assigns a VLAN ID to this port profile.

Step 6	`capability l3-vn-service`
	
	Example:
	`switch(config-port-prof)# capability l3-vn-service`
	`switch(config-port-prof)`
		Assigns the capability **l3-vn-service** to the port profile to ensure that the interfaces that inherit this port profile are used as sources for the Cisco VSG in Layer 3 mode encapsulated traffic.

Step 7	`no shutdown`
	
	Example:
	`switch(config-port-prof)# no shutdown`
	`switch(config-port-prof)`
		Administratively enables all ports in the profile.

Step 8	`state enabled`
	
	Example:
	`switch(config-port-prof)# state enabled`
	`switch(config-port-prof)`
		Sets the operational state of a port profile.

Step 9	`show port-profile name` *`profilename`* **Example:** `switch# show port-profile vmknic-pp`	(Optional) Displays the port profile configuration.

Step 10	`copy running-config startup-config`
	
	Example:
	`switch# copy running-config startup-config`
		(Optional) Copies the running configuration to the startup configuration.

Configuring the Cisco VSG with the vsn type Command

The Cisco VSG is a virtual service node (VSN). To configure the VSN for Cisco VSG functionality, use the **vsn type vsg global** command to enter the global configuration mode for the Cisco VSG.

BEFORE YOU BEGIN

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

- You have the Cisco VSG software installed and the basic installation completed. For details, see the *Cisco Virtual Security Gateway, Release 4.2(1)VSG1(3.1) and Cisco Virtual Network Management Center, Release 1.3 Installation and Upgrade Guide*.

- You must have the NEXUS_VSG_SERVICES_PKG license installed on the switch. Ensure that you have enough licenses to cover the number of VEMs that you want to protect.

- You must configure the data IP address and management IP addresses. To configure the data IP address, see the *Cisco Virtual Security Gateway, Release 4.2(1)VSG1(3.1) and Cisco Virtual Network Management Center, Release 1.3 Installation and Upgrade Guide.*

- You have completed creating the Cisco VSG port profiles for the service and HA interface.

- You are logged in to the switch CLI in EXEC mode.

SUMMARY STEPS

1. **configure**
2. **vsn type vsg global**

DETAILED STEPS

	Command	Purpose

Step 1	`configure`
	
	`Example:`
	`vsm# configure`
	`vsm(config)#`
		Places you in global configuration mode.

Step 2	`vsn type vsg global`
	
	`Example:`
	`vsm(config)# vsn type vsg global`
	`vsm(config-vsn)#`
		Enters VSN configuration mode.

Configuring TCP State-Checks for All Cisco VSG VSNs in a vPath

Although the TCP state-checks for Cisco VSGs on a vPath feature is enabled by default, there may be times when you want to disable this feature, such as when you do not want the information generated by this feature to hide other information in which you are specifically interested.

BEFORE YOU BEGIN

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

- You have the Cisco VSG software installed and the basic installation completed. For details, see the *Cisco Virtual Security Gateway, Release 4.2(1)VSG1(3.1) and Cisco Virtual Network Management Center, Release 1.3 Installation and Upgrade Guide.*

- You must have the NEXUS_VSG_SERVICES_PKG license installed on the switch. Ensure that you have enough licenses to cover the number of VEMs that you want to protect.

- You must configure the data IP address and management IP addresses. To configure the data IP address, see the *Cisco Virtual Security Gateway, Release 4.2(1)VSG1(3.1) and Cisco Virtual Network Management Center, Release 1.3 Installation and Upgrade Guide.*

- You have completed creating the Cisco VSG port profiles for the service and HA interface.

- You are logged in to the switch CLI in EXEC mode.

SUMMARY STEPS

1. **configure**
2. **vsn type vsg global**
3. **tcp state-checks**
4. **no tcp state-checks**
5. **exit**
6. **exit**

DETAILED STEPS

	Command	Purpose

Step 1	`configure`
	
	`Example:`
	`vsm# configure`
	`vsm(config)#`
		Places you in global configuration mode.

Step 2	`vsn type vsg global`
	
	`Example:`
	`vsm(config)# vsn type vsg global`
	`vsm(config-vsn)#`
		Enters VSN configuration mode.

Step 3	`tcp state-checks`
	
	`Example:`
	`vsm(config-vsn)# tcp state-checks`
	`vsm(config-vsn)#`
		Enables TCP state checks for all Cisco VSG VSNs in the vPath. (This is the default status.)

Step 4	`no tcp state-checks`
	
	`Example:`
	`vsm(config-vsn)# no tcp state-checks`
	`vsm(config-vsn)#`
		Disables the TCP state-checks feature.

Step 5	`exit`
	
	`Example:`
	`vsm(config-vsn)# exit`
	`vsm(config)#`
		Exits the VSN configuration mode and returns you to the global configuration mode.

Step 6	`exit`
	
	`Example:`
	`vsm(config)# exit`
	`vsm#`
		Exits the global configuration mode and returns you to EXEC mode.

Verifying the Cisco VSG Configuration

To display information related to a Cisco VSG, perform one of the following tasks on the switch CLI:

Show Commands

Command	Purpose

`show license usage`
 	
Example:
`vsm# show license usage`
	Displays a table with the Cisco VSG license usage information for the Cisco Nexus 1000V Series switch.

`show license usage NEXUS_VSG_SERVICES_PKG`
 	
Example:
`vsm# show license usage`
`NEXUS_VSG_SERVICES_PKG`
	Displays the usage information for the license package NEXUS_VSG_SERVICES_PKG.

`show vsn {statistics	brief	{detail [{{vlan vlan-num [ip ip-addr]}	module module-num}]}}`  **Example:** `vsm# show vsn statistics detail vlan 1`	Displays information about the configuration, MAC address, state of associated Cisco VSG and Virtual Ethernet Module (VEM), Veths to which Cisco VSGs are bound, and Virtual Service Node (VSN) statistics for all VEM modules associated with Cisco VSGs.

For detailed information about the fields in the output from these commands, see the *Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(5.1).*

vPath Ping Command for the Layer 2 Mode

To verify various connections and reachable attributes of the Cisco VSG VSN, you can use the vPath **ping** command.

The vPath **ping** command for Layer 2 mode has the following syntax:

ping vsn {**all** | {**ip** *ip-addr* [**vlan** *vlan-num*]}} **src-module** {**all** | **vpath-all** | *module-num*} [**timeout** *secs*] [**count** {*count* | **unlimited**}]

Examples

The following example shows how to see the VSN connections and if they are reachable:

```
VSM-1# ping vsn all src-module all
ping vsn 106.1.1.1 vlan 54 from module 3 5, seq=0 timeout=1-sec
  module(usec)   :  3(156)  5(160)
ping vsn 110.1.1.1 vlan 54 from module 3 5, seq=0 timeout=1-sec
  module(failed) :  3(VSN ARP not resolved)  5(VSN ARP not resolved)

ping vsn 106.1.1.1 vlan 54 from module 3 5, seq=1 timeout=1-sec
  module(usec)   :  3(230)  5(151)
ping vsn 110.1.1.1 vlan 54 from module 3 5, seq=1 timeout=1-sec
  module(failed) :  3(VSN ARP not resolved)  5(VSN ARP not resolved)

ping vsn 106.1.1.1 vlan 54 from module 3 5, seq=2 timeout=1-sec
  module(usec)   :  3(239)  5(131)
ping vsn 110.1.1.1 vlan 54 from module 3 5, seq=2 timeout=1-sec
```

```
   module(failed) :  3(VSN ARP not resolved)  5(VSN ARP not resolved)

ping vsn 106.1.1.1 vlan 54 from module 3 5, seq=3 timeout=1-sec
  module(usec)   :  3(248)  5(153)
ping vsn 110.1.1.1 vlan 54 from module 3 5, seq=3 timeout=1-sec
  module(failed) :  3(VSN ARP not resolved)  5(VSN ARP not resolved)

ping vsn 106.1.1.1 vlan 54 from module 3 5, seq=4 timeout=1-sec
  module(usec)   :  3(259)  5(126)
ping vsn 110.1.1.1 vlan 54 from module 3 5, seq=4 timeout=1-sec
  module(failed) :  3(VSN ARP not resolved)  5(VSN ARP not resolved)
```

This example shows how VSN ping options are displayed:

```
VSM-1# ping vsn ?
  all   All VSNs associated to VMs
  ip    IP Address
  vlan  VLAN Number
```

This example shows how VSN ping options are displayed for all source modules:

```
VSM-1# ping vsn all src-module ?
  <3-66>     Module number
  all        All modules in VSM
  vpath-all  All modules having VMs associated to VSNs
```

This example shows how to set up a ping for all source modules from a specified IP address:

```
VSM-1# ping vsn ip 10.1.1.60 src-module all
ping vsn 10.1.1.60 vlan 501 from module 4 5 7, seq=0 timeout=1-sec
  module(usec)   :  4(301)  5(236)
  module(failed) :  7(VSN ARP not resolved)

ping vsn 10.1.1.60 vlan 501 from module 4 5 7, seq=1 timeout=1-sec
  module(usec)   :  4(241)  5(138)  7(270)

ping vsn 10.1.1.60 vlan 501 from module 4 5 7, seq=2 timeout=1-sec
  module(usec)   :  4(230)  5(155)  7(256)

ping vsn 10.1.1.60 vlan 501 from module 4 5 7, seq=3 timeout=1-sec
  module(usec)   :  4(250)  5(154)  7(284)

ping vsn 10.1.1.60 vlan 501 from module 4 5 7, seq=4 timeout=1-sec
  module(usec)   :  4(231)  5(170)  7(193)
```

This example shows to set up a ping for all Vpath source modules for a specified IP address:

```
VSM-1# ping vsn ip 10.1.1.60 src-module vpath-all
ping vsn 10.1.1.60 vlan 501 from module 4 5, seq=0 timeout=1-sec
  module(usec)   :  4(223)  5(247)

ping vsn 10.1.1.60 vlan 501 from module 4 5, seq=1 timeout=1-sec
  module(usec)   :  4(206)  5(167)

ping vsn 10.1.1.60 vlan 501 from module 4 5, seq=2 timeout=1-sec
  module(usec)   :  4(241)  5(169)
```

This example shows how to set up a ping for all source modules of a specified IP address with a time-out and a count:

```
VSM-1# ping vsn ip 10.1.1.60 src-module all timeout 2 count 3
ping vsn 10.1.1.60 vlan 501 from module 4 5 7, seq=0 timeout=2-sec
  module(usec)   :  4(444)  5(238)  7(394)

ping vsn 10.1.1.60 vlan 501 from module 4 5 7, seq=1 timeout=2-sec
```

```
          module(usec)   :  4(259)  5(154)  7(225)


ping vsn 10.1.1.60 vlan 501 from module 4 5 7, seq=2 timeout=2-sec
          module(usec)   :  4(227)  5(184)  7(216)
```

vPath Ping Command for the Layer 3 Mode

Examples

```
vsm# ping vsn ip 10.1.1.40 src-module vpath-all
ping vsn 10.1.1.40 vlan 0 from module 9 11 12, seq=0 timeout=1-sec
  module(usec)   :  9(698) 11(701) 12(826)

ping vsn 10.1.1.40 vlan 0 from module 9 11 12, seq=1 timeout=1-sec
  module(usec)   :  9(461) 11(573) 12(714)

ping vsn 10.1.1.40 vlan 0 from module 9 11 12, seq=2 timeout=1-sec
  module(usec)   :  9(447) 11(569) 12(598)

ping vsn 10.1.1.40 vlan 0 from module 9 11 12, seq=3 timeout=1-sec
  module(usec)   :  9(334) 11(702) 12(559)

ping vsn 10.1.1.40 vlan 0 from module 9 11 12, seq=4 timeout=1-sec
  module(usec)   :  9(387) 11(558) 12(597)

vsm#


vsm# ping vsn all src-module all
ping vsn 10.1.1.44 vlan 501 from module 9 10 11 12, seq=0 timeout=1-sec
  module(usec)   :  9(508)
  module(failed) : 10(VSN ARP not resolved) 11(VSN ARP not resolved)
                   12(VSN ARP not resolved)
ping vsn 10.1.1.40 vlan 0 from module 9 10 11 12, seq=0 timeout=1-sec
  module(usec)   :  9(974) 11(987) 12(1007)
  module(failed) : 10(VSN ARP not resolved)

ping vsn 10.1.1.44 vlan 501 from module 9 10 11 12, seq=1 timeout=1-sec
  module(usec)   :  9(277) 10(436) 11(270) 12(399)
ping vsn 10.1.1.40 vlan 0 from module 9 10 11 12, seq=1 timeout=1-sec
  module(usec)   :  9(376) 10(606) 11(468) 12(622)

ping vsn 10.1.1.44 vlan 501 from module 9 10 11 12, seq=2 timeout=1-sec
  module(usec)   :  9(272) 10(389) 11(318) 12(357)
ping vsn 10.1.1.40 vlan 0 from module 9 10 11 12, seq=2 timeout=1-sec
  module(usec)   :  9(428) 10(632) 11(586) 12(594)

ping vsn 10.1.1.44 vlan 501 from module 9 10 11 12, seq=3 timeout=1-sec
  module(usec)   :  9(284) 10(426) 11(331) 12(387)
ping vsn 10.1.1.40 vlan 0 from module 9 10 11 12, seq=3 timeout=1-sec
  module(usec)   :  9(414) 10(663) 11(644) 12(698)

ping vsn 10.1.1.44 vlan 501 from module 9 10 11 12, seq=4 timeout=1-sec
  module(usec)   :  9(278) 10(479) 11(334) 12(469)
ping vsn 10.1.1.40 vlan 0 from module 9 10 11 12, seq=4 timeout=1-sec
  module(usec)   :  9(397) 10(613) 11(560) 12(593)

vsm#
```

Where to Go Next

After you have completed configuring the Cisco VSG port profile on the switch for protection, proceed to assign port profiles to your VMs for Cisco VSG firewall protection on the vCenter.

CHAPTER 4

Cisco Virtual Security Gateway System Management

This chapter describes how to manage the Cisco Virtual Security Gateway (VSG).

This chapter includes the following sections:

Information About VSG System Management

The Cisco Virtual Security Gateway (VSG) enables you to use command-line interface (CLI) configuration commands to do standard system management functions such as the following:

- Changing the hostname
- Configuring messages of the day
- Displaying, saving, and erasing configuration files
- Providing a single interface to all file systems including:
  - Flash memory
  - FTP and TFTP
  - Running configuration
  - Any other endpoint for reading and writing data
- Identifying users connected to the Cisco VSG
- Sending messages to single users or all users

Changing the Cisco VSG Instance Name

You can change the Cisco VSG instance name or prompt. If you have multiple instances of Cisco VSGs, you can use this procedure to uniquely identify each Cisco VSG.

BEFORE YOU BEGIN

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

- You are logged in to the CLI in global configuration mode.

SUMMARY STEPS

1. **configure**
2. **hostname**

DETAILED STEPS

	Command	Purpose

Step 1	`configure`
	
	`Example:`
	`vsg# configure`
		Places you in global configuration mode.

Step 2	`hostname host-name`
	
	`Example:`
	`vsg(config)# hostname vsg100`
		Changes the host prompt. The *host-name* argument can have a maximum of 32 alphanumeric characters.

This example shows how to change the hostname (name of the Cisco VSG):

```
vsg# configure
vsg(config)# hostname metro
vsg(config)# exit
metro#
```

Configuring a Message of the Day

You can configure a message of the day (MOTD) to display at the login prompt.

- The banner message can be up to 40 lines with up to 80 characters per line.
- Use the following guidelines when choosing your delimiting character:
  – Do not use the delimiting-character in the message string.
  – Do not use **"** and **%** as delimiters.
- The following tokens can be used in the message of the day:
  – `$(hostname)` displays the hostname for the switch.
  – `$(line)` displays the vty or tty line or name.

BEFORE YOU BEGIN

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

- You are logged in to the CLI in configuration mode.

SUMMARY STEPS

1. **configure**
2. **banner motd**
3. **show banner motd**

DETAILED STEPS

	Command	Purpose

Step 1	`configure`
	
	Example:
	`vsg# configure`
		Places you in global configuration mode.

Step 2	`banner motd` [*delimiting-character message delimiting-character*] **Example:** `vsg(config)# banner motd #Hello#`	Configures an MOTD with the following limits: • Up to 40 lines • Up to 80 characters per line • Enclosed in a delimiting character, such as # • Can span multiple lines • Can use tokens

Step 3	`show banner motd`
	
	Example:
	`vsg(config)# show banner motd`
		Displays the configured banner message.

This example shows how to configure an MOTD:

```
vsg# configure
vsg(config)# banner motd #December 12, 2010 Welcome to the VSG#
vsg(config)# show banner motd
December 12, 2010 Welcome to the VSG
vsg(config)#
```

Verifying the Cisco VSG Configuration

This section includes the following topics on verifying the Cisco VSG configuration:

Verifying the Software and Hardware Versions

You can view the versions of software and hardware on your system.

BEFORE YOU BEGIN

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

- You are logged in to the CLI in any command mode.

SUMMARY STEPS

    1. **show version**

DETAILED STEPS

	Command	Description
Step 1	**show version** **Example:** vsg# show version	Displays the versions of system software and hardware that are currently running on the Cisco VSG.

This example shows how to display and verify the system software and hardware version information for the Cisco VSG:

```
vsg# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2011, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license.
Some parts of this software are covered under the GNU Public
License. A copy of the license is available at
http://www.gnu.org/licenses/gpl.html.

Software
  loader:    version unavailable [last: image booted through mgmt0]
  kickstart: version 4.2(1)VSG1(2) [build 4.2(1)VSG1(2.398)]
  system:    version 4.2(1)VSG1(2) [build 4.2(1)VSG1(2.398)]
  kickstart image file is: [not present on supervisor]

  kickstart compile time:  07/12/2011 17:00:00
  system image file is:    bootflash:/nexus-1000v-mz.VSG1.0.398.bin
  system compile time:     07/17/2011 17:00:00 [07/17/2011 13:03:38]

Hardware
  cisco Nexus 1000VF Chassis ("Nexus VSN Virtual Firewall")
  Intel(R) Xeon(R) CPU        with 1944668 kB of memory.
  Processor Board ID T5056BB0072

  Device name: vsg
  bootflash:    2059572 kB

Kernel uptime is 1 day(s), 5 hour(s), 47 minute(s), 4 second(s)

plugin
  Core Plugin, Virtualization Plugin, Ethernet Plugin
```

Verifying the Running Configuration

You can view the configuration currently running on the system.

BEFORE YOU BEGIN

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

- You are logged in to the CLI in any command mode.

SUMMARY STEPS

   1. **show running-config**

DETAILED STEPS

	Command	Description
Step 1	**show running-config** **Example:** vsg# show running-config	Displays the versions of system software and hardware that are currently running on the Cisco VSG.

This example shows how to display the versions of system software and hardware running on the Cisco VSG:

```
vsg# show running-config

!Command: show running-config
!Time: Sun Jul 17 17:42:59 2011

version 4.2(1)VSG1(2)
no feature telnet
no feature http-server

username admin password 5 $1$RU5OIPU7$SYvoK9S5rOMRE9WBWZLsA.  role network-admin

banner motd #Nexus VSN#

ssh key rsa 2048
ip domain-lookup
ip domain-lookup
hostname vsg
snmp-server user admin network-admin auth md5 0x5ed3cfea7c44550ac3d18475f28b118b priv
0x5ed3cfea7c44550ac3d18475f28b118b localizedkey

vrf context management
  ip route 0.0.0.0/0 10.193.72.1
vlan 1
port-channel load-balance ethernet source-mac
port-profile default max-ports 32

vdc vsg id 1
  limit-resource vlan minimum 16 maximum 2049
  limit-resource monitor-session minimum 0 maximum 2
  limit-resource vrf minimum 16 maximum 8192
  limit-resource port-channel minimum 0 maximum 768
  limit-resource u4route-mem minimum 32 maximum 32
  limit-resource u6route-mem minimum 16 maximum 16
```

```
        limit-resource m4route-mem minimum 58 maximum 58
        limit-resource m6route-mem minimum 8 maximum 8

interface mgmt0
   ip address 10.193.73.118/21

interface data0
   ip address 118.1.1.1/8
line console
boot kickstart bootflash:/nexus-1000v-kickstart-mzg.VSG1.0.1.bin sup-1
boot system bootflash:/nexus-1000v-mzg.VSG1.0.1.bin sup-1
boot kickstart bootflash:/nexus-1000v-kickstart-mzg.VSG1.0.1.bin sup-2
boot system bootflash:/nexus-1000v-mzg.VSG1.0.1.bin sup-2
   ha-pair id 23

security-profile sp1
   policy p1
rule r1
   action 10 permit
policy p1
   rule r1 order 10
vnm-policy-agent
   policy-agent-image
   registration-ip 0.0.0.0
   shared-secret **********
   log-level info

vsg#
```

Comparing the Startup and Running Configurations

You can view the differences between the startup configuration and running configuration.

BEFORE YOU BEGIN

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

- You are logged in to the CLI in any command mode.

SUMMARY STEPS

   1. show running-config diff

DETAILED STEPS

	Command	Description

Step 1	`show running-config diff`
	
	Example:
	`vsg# show running-config diff`
		Displays the difference between the startup configuration and the running configuration.

This example shows how to display the difference between the startup configuration and the running configuration:

```
vsg# show running-config diff
*** Startup-config
```

```
--- Running-config
***************
*** 14,34 ****
  banner motd #Nexus VSG#

  ssh key rsa 2048
  ip domain-lookup
  ip domain-lookup
! switchname G-VSG-116-1
  snmp-server user admin network-admin auth md5 0x5ed3cfea7c44550ac3d18475f28b118b priv
0x5ed3cfea7c44550ac3d18475f28b118b localizedkey
  snmp-server user vsnbetauser network-admin auth md5 0x11d89525029e4148a2a494a8e131f9ed
priv 0x11d89525029e4148a2a494a8e131f9ed localizedkey

  vrf context management
    ip route 0.0.0.0/0 10.193.72.1
  vlan 1
  port-channel load-balance ethernet source-mac
  port-profile default max-ports 32

! vdc G-VSG-116-1 id 1
    limit-resource vlan minimum 16 maximum 2049
    limit-resource monitor-session minimum 0 maximum 2
    limit-resource vrf minimum 16 maximum 8192
    limit-resource port-channel minimum 0 maximum 768
    limit-resource u4route-mem minimum 32 maximum 32
--- 13,33 ----
  banner motd #Nexus VSG#

  ssh key rsa 2048
  ip domain-lookup
  ip domain-lookup
! hostname vsg
  snmp-server user admin network-admin auth md5 0x5ed3cfea7c44550ac3d18475f28b118b priv
0x5ed3cfea7c44550ac3d18475f28b118b localizedkey
  snmp-server user vsnbetauser network-admin auth md5 0x11d89525029e4148a2a494a8e131f9ed
priv 0x11d89525029e4148a2a494a8e131f9ed localizedkey

  vrf context management
    ip route 0.0.0.0/0 10.193.72.1
  vlan 1
  port-channel load-balance ethernet source-mac
  port-profile default max-ports 32

! vdc vsg id 1
    limit-resource vlan minimum 16 maximum 2049
    limit-resource monitor-session minimum 0 maximum 2
    limit-resource vrf minimum 16 maximum 8192
    limit-resource port-channel minimum 0 maximum 768
    limit-resource u4route-mem minimum 32 maximum 32
vsg#
```

Displaying Interface Configurations

This section includes the following procedures:

Displaying a Brief View of a Specific Interface Configuration

You can display a brief view of a specific interface configuration.

BEFORE YOU BEGIN

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

- You are logged in to the CLI in any command mode.

SUMMARY STEPS

1. **show interface brief**

DETAILED STEPS

	Command	Description

Step 1	`show interface {type} {name} brief`
	
	Example:
	`vsg# show interface brief`
		Displays a brief view of a specific interface configuration.

This example shows how to display a brief view of a specific interface configuration:

```
vsg# show interface brief

--------------------------------------------------------------------------------
Port    VRF         Status IP Address                                Speed   MTU
--------------------------------------------------------------------------------
mgmt0   --          up     10.193.73.10                              1000    1500


--------------------------------------------------------------------------------
Port    VRF         Status IP Address                                Speed   MTU
--------------------------------------------------------------------------------
data0   --          up     10.10.10.10                               1000    1500
vsg#
--------------------------------------------------------------------------------
```

Displaying a Detailed View of a Specific Interface Configuration

You can display a detailed view of a specific interface configuration.

BEFORE YOU BEGIN

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

- You are logged in to the CLI in any command mode.

SUMMARY STEPS

1. **show interface**

DETAILED STEPS

	Command	Description
Step 1	**show interface** {*type*} {*name*} **Example:** vsg# show interface mgmt 0	Displays a detailed version of a specific interface connection.

This example shows how to display a detailed version of a specific interface connection:

```
vsg# show interface mgmt 0
mgmt0 is up
  Hardware: Ethernet, address: 0050.5689.3321 (bia 0050.5689.3321)
  Internet Address is 172.23.232.141/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA
  full-duplex, 1000 Mb/s
  Auto-Negotiation is turned on
    4961 packets input, 511995 bytes
    0 multicast frames, 0 compressed
    0 input errors, 0 frame, 0 overrun, 0 fifo
    245 packets output, 35853 bytes
    0 underrun, 0 output errors, 0 collisions
    0 fifo, 0 carrier errors
vsg#
```

Displaying a Brief View of All Interfaces

You can display a brief view of all interfaces.

BEFORE YOU BEGIN

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

- You are logged in to the CLI in any command mode.

SUMMARY STEPS

1. **show interface brief**

DETAILED STEPS

	Command	Description
Step 1	**show interface brief** **Example:** vsg# show interface brief	Displays a brief view of all interfaces.

This example shows how to display a brief view of all the interfaces on the Cisco VSG:

```
vsg# show interface brief

--------------------------------------------------------------------------------
Port    VRF         Status IP Address                Speed    MTU
```

```
--------------------------------------------------------------------------------
mgmt0      --           up    10.23.232.141                 1000    1500
--------------------------------------------------------------------------------
Ethernet     VLAN   Type Mode   Status  Reason                  Speed    Port
Interface                                                                Ch #
--------------------------------------------------------------------------------
Eth3/2       1      eth  trunk  up      none                     1000(D) --
Eth3/3       262    eth  access up      none                     1000(D) --
--------------------------------------------------------------------------------
Interface    VLAN   Type Mode   Status  Reason                  MTU
--------------------------------------------------------------------------------
Veth81       630    virt access up      none                    1500
Veth82       630    virt access up      none                    1500
Veth224      631    virt access up      none                    1500
Veth225      1      virt access nonPcpt nonParticipating        1500
vsg#
```

Verifying the Running Configuration for All Interfaces

You can verify the running configuration for all interfaces.

✎

Note   The output for the **show running-config interface** command differs from that of the **show interface** command.

BEFORE YOU BEGIN

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

- You are logged in to the CLI in any command mode.

SUMMARY STEPS

     1.   **show running-config interface**

DETAILED STEPS

	Command	Description

Step 1	`show running-config interface`
	
	Example:
	`vsg# show running-config interface`
		Displays the running configuration for all interfaces on your system.

This example shows how to display the running configuration for all the interfaces on the Cisco VSG:

```
vsg# show running-config interface

!Command: show running-config interface
!Time: Sun Jul 17 16:29:08 2011

version 4.2(1)VSG1(2)

interface mgmt0
  ip address 10.193.73.10/16

interface data0
```

```
    ip address 10.10.10.10/24

vsg#
```

Saving a Configuration

You can save the running configuration to the startup configuration, so that your changes are retained in the startup configuration file the next time you start up the Cisco VSG.

BEFORE YOU BEGIN

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

- You are logged in to the CLI in any command mode.

SUMMARY STEPS

1. **copy running-config startup-config**

DETAILED STEPS

	Command	Description
Step 1	**copy running-config startup-configure** **Example:** vsg# copy running-config startup-configure	Saves the running configuration to the startup configuration.

This example shows how to save the running configuration to your startup configuration:

```
vsg(config)# copy running-config startup-config
[#####################################] 100%
vsg(config)#
```

Erasing a Configuration

You can erase a startup configuration.

⚠

Caution   The **write erase** command erases the entire startup configuration with the exception of loader functions.

BEFORE YOU BEGIN

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

- You are logged in to the CLI.
- The following parameters are used with this command:
  - **boot**—Erases the boot variables and the mgmt0 IP configuration.
  - **debug**—Erases the debug configuration.

SUMMARY STEPS

1. **write erase [boot | debug]**

DETAILED STEPS

	Command	Description
Step 1	**write erase** [**boot** | **debug**] **Example:** vsg# write erase debug	Erases the existing startup configuration and reverts all settings to their factory defaults. The running configuration is not affected.

This example shows how to erase a debug startup configuration:

```
vsg(config)# write erase debug
Warning: This command will erase the startup-configuration.
Do you wish to proceed anyway? (y/n)  [y]
[#####################################] 100%
vsg(config)#
```

Displaying a Cisco VSG Instance

You can display a Cisco VSG instance.

BEFORE YOU BEGIN

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

- You are logged in to the CLI.

SUMMARY STEPS

> **1. show vsg**

DETAILED STEPS

	Command	Description

Step 1	`show vsg`
	
	Example:
	`vsg# show vsg`
		Displays the particulars of the Cisco VSG—including the model, the high availability (HA) ID, the Cisco VSG software version and build, and the Cisco Virtual Network Management Center (VNMC) IP address.
		The running configuration is not affected.

This example shows how to display the Cisco VSG model, HA ID, software version and build, and the Cisco VNMC IP address:

```
vsg# show vsg
Model: VSG
HA ID: 10
VSG Software Version: 4.2(1)VSG1(1) build [4.2(1)VSG1(0.396)]
VNMC IP: 10.193.20.12
vsg#
```

Navigating the File System

This section describes how to navigate the file system.

This section includes the following topics:

- Specifying File Systems, page 4-13
- Identifying Your Current Working Directory, page 4-14
- Changing Your Directory, page 4-14
- Listing the Files in a File System, page 4-15
- Identifying Available File Systems for Copying Files, page 4-16
- Using Tab Completion, page 4-17

Specifying File Systems

The syntax for specifying a file system is `<file system name>`**:**[**//**`server`**/**]. Table 4-1 describes the file system syntax.

Table 4-1   File System Syntax Components

File System Name	Server	Description
bootflash:	sup-active sup-local sup-1 module-1	Internal memory located on the active supervisor used for storing system images, configuration files, and other miscellaneous files. The CLI defaults to the bootflash: file system.
	sup-standby sup-remote sup-2 module-2	Internal memory located on the standby supervisor used for storing system images, configuration files, and other miscellaneous files.
volatile:	—	Volatile random-access memory (VRAM) located on a supervisor module used for temporary or pending changes.

Identifying Your Current Working Directory

You can display the directory name of your current location in the CLI.

BEFORE YOU BEGIN

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

- You are logged in to the CLI.

SUMMARY STEPS

1. **pwd**

DETAILED STEPS

	Command	Purpose
Step 1	**pwd** **Example:** vsg# pwd	Displays the directory name of your current location in the CLI.

This example shows how to display the directory name of your current location in the Cisco VSG CLI:

```
vsg# pwd
bootflash:
```

Changing Your Directory

You can change directories in the CLI.

BEFORE YOU BEGIN

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

- You are logged in to the CLI in any command mode.

- The Cisco VSG CLI defaults to the bootflash: file system.

Note Any file saved in the volatile: file system is erased when the Cisco VSG reboots.

SUMMARY STEPS

1. **pwd**
2. **cd** *directory_name*

DETAILED STEPS

	Command	Purpose

Step 1	`pwd`
	
	Example:
	`vsg# pwd`
		Displays the directory name of your current CLI location.

Step 2	`cd` *directory_name* **Example:** `vsg# cd bootflash:`	Changes your CLI location to the specified directory.

This example shows how to display the directory name of the current Cisco VSG CLI location and how to change the CLI location to the specified directory:

```
vsg# pwd
bootflash:
vsg# cd volatile:
vsg# pwd
volatile:
vsg#
```

Listing the Files in a File System

You can display the contents of a directory or file.

BEFORE YOU BEGIN

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

- You are logged in to the CLI in any command mode.

SUMMARY STEPS

1. **dir** [*directory* | *filename*]

DETAILED STEPS

	Command	Purpose
Step 1	`dir` [*directory* | *filename*] **Example:** `vsg# dir TenantA/`	Displays the contents of a directory or file. Ending an argument with a slash indicates a directory and displays the contents of that directory.

This example shows how to display the contents of a directory:

```
vsg# dir lost+found/
    49241    Jul 01 09:30:00 2008  diagclient_log.2613
    12861    Jul 01 09:29:34 2008  diagmgr_log.2580
       31    Jul 01 09:28:47 2008  dmesg
     1811    Jul 01 09:28:58 2008  example_test.2633
       89    Jul 01 09:28:58 2008  libdiag.2633
    42136    Jul 01 16:34:34 2008  messages
       65    Jul 01 09:29:00 2008  otm.log
      741    Jul 01 09:29:07 2008  sal.log
       87    Jul 01 09:28:50 2008  startupdebug

Usage for log://sup-local
   51408896 bytes used
  158306304 bytes free
  209715200 bytes total
vsg#
```

Identifying Available File Systems for Copying Files

You can identify the file systems that you can copy to or from.

BEFORE YOU BEGIN

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

- You are logged in to the CLI in EXEC mode.

SUMMARY STEPS

1. **copy ?**
2. **copy filename ?**

DETAILED STEPS

	Command	Purpose

Step 1	`copy ?`
	
	Example:
	`vsg# copy ?`
		Displays the source file systems available to the **copy** command.

Step 2	`copy filename ?`
	
	Example:
	`vsg# copy filename ?`
		Displays the destination file systems available to the **copy** command for a specific file.

This example shows how to display the source file systems available to the **copy** command:

```
vsg# copy ?
bootflash: Select source filesystem
core: Select source filesystem
debug: Select source filesystem
ftp: Select source filesystem
licenses Backup license files
log: Select source filesystem
nvram: Select source filesystem
running-config Copy running configuration to destination
scp: Select source filesystem
sftp: Select source filesystem
startup-config Copy startup configuration to destination
system: Select source filesystem
tftp: Select source filesystem
volatile: Select source filesystem
```

This example shows how to display the destination file systems available to the **copy** command for the specific file named:

```
vsg# copy filename ?
  bootflash:      Select destination filesystem
  debug:          Select destination filesystem
  ftp:            Select destination filesystem
  log:            Select destination filesystem
  modflash:       Select destination filesystem
  nvram:          Select destination filesystem
  running-config  Copy from source to running configuration
  scp:            Select destination filesystem
  sftp:           Select destination filesystem
  startup-config  Copy from source to startup configuration
  system:         Select destination filesystem
  tftp:           Select destination filesystem
  volatile:       Select destination filesystem
```

Using Tab Completion

You can have the CLI complete a partial filename in a command.

BEFORE YOU BEGIN

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

- You are logged in to the CLI in EXEC mode.

SUMMARY STEPS

1. **show file** *filesystem name: partial filename* **<Tab>**
2. **show file** *bootflash:c* **<Tab>**

DETAILED STEPS

	Command	Purpose
Step 1	**show file** *filesystem name: partial filename* **<Tab>** **Example:** vsg# show file bootflash:sanfrancisc	Completes the filename when Tab is pressed, if the characters you typed are unique to a single file. If not, the CLI lists a selection of filenames that match the characters you typed. You can then retype enough characters to make the filename unique. The CLI completes the filename for you.
Step 2	**show file bootflash:c <Tab>** **Example:** vsg# show file bootflash:c	Completes the filename for you.

This example shows how to display a selection of available files when you press Tab after you have typed enough characters that are unique to a file or set of files:

```
VSG# show file bootflash:nex<Tab>
bootflash:nexus-1000v-dplug-mzg.VSG1.0.1.bin
bootflash:nexus-1000v-kickstart-mzg.VSG1.0.1.bin
bootflash:nexus-1000v-mzg.VSG1.0.1.bin
bootflash:nexus-1000v-mzg.VSG1.0.2.bin
```

This example shows how to complete a command by pressing the Tab key when you have already entered the first unique characters of a command:

```
vsg# show file bootflash:c<Tab>
-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKBgQDSq93Br1Hcg3bX1jXDMY5c9+yZSST3VhuQBqogvCPDGeLecA+j
...
...
vsg#
```

Copying and Backing Up Files

You can copy a file, such as a configuration file, to save it or reuse it at another location. If your internal file systems are corrupted, you could potentially lose your configuration. Save and back up your configuration files periodically. Also, before installing or migrating to a new software configuration, back up the existing configuration files.

BEFORE YOU BEGIN

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

- You are logged in to the CLI in any command mode.

- If you are copying to a remote location, make sure that your device has a route to the destination. Your device and the remote destination must be in the same subnetwork if you do not have a router or default gateway to route traffic between subnets.

- Using the **ping** command to make sure that your device has connectivity to the destination.

- Make sure that the source configuration file is in the correct directory on the remote server.

- Make sure that the permissions on the source file are set correctly. Permissions on the file should be set to world-read.

> **Note** Use the **dir** command to ensure that enough space is available in the destination file system. If enough space is not available, use the **delete** command to remove unneeded files.

SUMMARY STEPS

1. **copy** [*source filesystem*:] *filename* [*destination filesystem*:] *filename*

DETAILED STEPS

	Command	Purpose
Step 1	**copy** [*source filesystem*:] *filename* [*destination filesystem*:] *filename* **Example:** vsg# copy system:running-config tftp://10.10.1.1./home/configs/vsg2.cfg	Copies a file from the specified source location to the specified destination location.

This example shows how to copy a file from a specified source location and move it to a specified destination location:

```
vsg# copy system:running-config tftp://10.10.1.1/home/configs/vsg3-run.cfg
Enter vrf (If no input, current vrf 'default' is considered):
Trying to connect to tftp server......
Connection to Server Established.
TFTP put operation succesful
vsg#
```

Creating a Directory

You can create a directory at the current directory level or at a specified directory level.

BEFORE YOU BEGIN

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

- You are logged in to the CLI in any command mode.

SUMMARY STEPS

1. **mkdir** {**bootflash:** | **debug:** | **volatile:**} *directory-name*

DETAILED STEPS

	Command	Purpose
Step 1	`mkdir {bootflash:	debug:	volatile:}` *directory-name*  **Example:** `vsg# mkdir bootflash:new-directory`	Creates a directory at the current directory level.

This example shows how to create a directory called test in the bootflash: directory:

```
vsg# mkdir bootflash:test
vsg#
```

This example shows how to create a directory called test at the current directory level:

```
vsg# mkdir test
vsg#
```

Removing an Existing Directory

You can remove an existing directory from the flash file system.

BEFORE YOU BEGIN

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

- You are logged in to the CLI.
- This command is only valid on flash file systems.
- Before you can remove it, the directory must be empty.

SUMMARY STEPS

1. **rmdir** {**bootflash:** | **debug:** | **volatile:**} *directory*

DETAILED STEPS

	Command	Purpose
Step 1	`rmdir {bootflash:	debug:	volatile:}` *directory*  **Example:** `vsg# rmdir bootflash:new-directory`	Removes a directory as long as the directory is empty.

This example shows how to remove the directory called test in the bootflash: directory:

```
vsg# rmdir bootflash:test
vsg#
```

This example shows how to remove the directory called test at the current directory level:

```
vsg# rmdir test
vsg#
```

Moving Files

You can move a file from one location to another location.

BEFORE YOU BEGIN

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

- You are logged in to the CLI.

- The copy does not complete if there is not enough space in the destination directory.

⚠
Caution   If a file with the same name already exists in the destination directory, that file is overwritten by the file that you move.

SUMMARY STEPS

    1. **move** {*source path and filename*} {*destination path and filename*}

DETAILED STEPS

	Command	Purpose
Step 1	**move** {*source path and filename*} {*destination path and filename*} **Example:** `vsg# move bootflash:file1 bootflash:mystuff/file1`	Moves a directory.

This example shows how to move a file from one directory to another in the same file system:

```
vsg# move bootflash:samplefile bootflash:mystorage/samplefile
```

This example shows how to move a file from one directory to another in the current file system:

```
vsg# move samplefile mystorage/samplefile
```

Deleting Files or Directories

You can delete files or directories on a Flash memory device.

BEFORE YOU BEGIN

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

- If you try to delete the configuration file or image specified by the CONFIG_FILE or BOOTLDR environment variable, the system prompts you to confirm the deletion.

- If you try to delete the last valid system image specified in the BOOT environment variable, the system prompts you to confirm the deletion.

SUMMARY STEPS

1. **delete** [**bootflash:** | **debug:** | **log:** | **volatile:**] *filename or directory name*

DETAILED STEPS

	Command	Purpose
Step 1	`delete [bootflash:	debug:	log:	volatile:] filename or directory name`  `Example:` `vsg# delete log:test-log`	Deletes a specified file or directory and everything in the directory.

This example shows how to delete the named file from the current working directory:

```
vsg# delete bootflash:dns_config.cfg
```

This example shows how to delete the named directory and its contents:

```
vsg# delete log:my-log
```

Compressing Files

You can compress (zip) a specified file using LZ77 coding.

BEFORE YOU BEGIN

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

*   You are logged in to the CLI.

SUMMARY STEPS

1. **show** *command* > [*path*] *filename*
2. **dir**
3. **gzip** [*path*] *filename*

DETAILED STEPS

	Command	Purpose

Step 1	`show command > [path] filename`
	
	`Example:`
	`vsg# show pwd > pwdfile`
		Directs **show** command output to a file.

	Command	Purpose

Step 2	`dir`
	
	Example:
	`vsg# dir`
		Displays the contents of the current directory, including the new file created in the first step.

Step 3	`gzip` [*path*] *filename* **Example:** `vsg# gzip bootflash:errorsfile`	Compresses the specified file.

This example shows how to display and then compress a specified file:

```
vsg# show system internal sysmgr event-history errors > errorsfile
vsg# dir
    1480264    Nov 03 08:38:21 2001  1
      77824    Dec 08 11:17:45 2001  accounting.log
       4096    Nov 30 14:35:15 2001  core/
       3220    Dec 09 16:33:05 2001  errorsfile
       4096     Nov 30 14:35:15 2001  log/
      16384    Nov 03 08:32:09 2001  lost+found/
       7456    Dec 08 11:17:41 2001  mts.log
    1480264    Nov 03 08:33:27 2001  nexus-1000v-dplug-mzg.VSG1.0.1.bin
   20126720    Nov 03 08:33:27 2001  nexus-1000v-kickstart-mzg.VSG1.0.1.bin
   45985810    Dec 01 14:30:00 2001  nexus-1000v-mzg.VSG1.0.1.bin
   46095447    Dec 07 11:32:00 2001  nexus-1000v-mzg.VSG1.0.396.bin
       1714    Dec 08 11:17:33 2001  system.cfg.new
       4096    Nov 03 08:33:54 2001  vdc_2/
       4096    Nov 03 08:33:54 2001  vdc_3/
       4096    Nov 03 08:33:54 2001  vdc_4/

Usage for bootflash://
  631246848 bytes used
5772722176 bytes free
6403969024 bytes total
```

This example shows how to compress the specified file:

```
vsg# gzip bootflash:errorsfile
vsg# dir
    1480264    Nov 03 08:38:21 2001  1
      77824    Dec 08 11:17:45 2001  accounting.log
       4096    Nov 30 14:35:15 2001  core/
        861    Dec 09 16:33:05 2001  errorsfile.gz
       4096     Nov 30 14:35:15 2001  log/
      16384    Nov 03 08:32:09 2001  lost+found/
       7456    Dec 08 11:17:41 2001  mts.log
    1480264    Nov 03 08:33:27 2001  nexus-1000v-dplug-mzg.VSG1.0.1.bin
   20126720    Nov 03 08:33:27 2001  nexus-1000v-kickstart-mzg.VSG1.0.1.bin
   45985810    Dec 01 14:30:00 2001  nexus-1000v-mzg.VSG1.0.1.bin
   46095447    Dec 07 11:32:00 2001  nexus-1000v-mzg.VSG1.0.396.bin
       1714    Dec 08 11:17:33 2001  system.cfg.new
       4096    Nov 03 08:33:54 2001  vdc_2/
       4096    Nov 03 08:33:54 2001  vdc_3/
       4096    Nov 03 08:33:54 2001  vdc_4/

Usage for bootflash://
  631246848 bytes used
5772722176 bytes free
6403969024 bytes total
vsg#
```

Uncompressing Files

You can uncompress (unzip) a specified file that is compressed using LZ77 coding.

BEFORE YOU BEGIN

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

• You are logged in to the CLI.

SUMMARY STEPS

1. **gunzip** [*path*] *filename*

2. **dir**

DETAILED STEPS

	Command	Purpose

Step 1	`gunzip` `[path]` `filename`
	
	Example:
	`vsg# gunzip`
	`bootflash:errorsfile.gz`
		Uncompresses the specified file.

Step 2	`dir`
	
	Example:
	`vsg# dir`
		Displays the contents of a directory, including the newly uncompressed file.

This example shows how to uncompress a specified file:

```
vsg# gunzip bootflash:errorsfile.gz
vsg# dir bootflash:
   1480264     Nov 03 08:38:21 2001  1
     77824     Dec 08 11:17:45 2001  accounting.log
      4096     Nov 30 14:35:15 2001  core/
      3220     Dec 09 16:33:05 2001  errorsfile
      4096     Nov 30 14:35:15 2001  log/
     16384     Nov 03 08:32:09 2001  lost+found/
      7456     Dec 08 11:17:41 2001  mts.log
   1480264     Nov 03 08:33:27 2001  nexus-1000v-dplug-mzg.VSG1.0.1.bin
  20126720     Nov 03 08:33:27 2001  nexus-1000v-kickstart-mzg.VSG1.0.1.bin
  45985810     Dec 01 14:30:00 2001  nexus-1000v-mzg.VSG1.0.1.bin
  46095447     Dec 07 11:32:00 2001  nexus-1000v-mzg.VSG1.0.396.bin
      1714     Dec 08 11:17:33 2001  system.cfg.new
      4096     Nov 03 08:33:54 2001  vdc_2/
      4096     Nov 03 08:33:54 2001  vdc_3/
      4096     Nov 03 08:33:54 2001  vdc_4/

Usage for bootflash://sup-local
  631246848 bytes used
5772722176 bytes free
6403969024 bytes total
```

Directing Command Output to a File

You can direct command output to a file.

BEFORE YOU BEGIN

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

- You are logged in to the CLI in any command mode.

SUMMARY STEPS

1. **show running-config >** [*path* | *filename*]

DETAILED STEPS

	Command	Purpose

Step 1	`show running-config >` [*path* | *filename*]
	
	Example:
	`vsg# show running-config >`
	`bootflash:vsg1-run.cfg`
		Directs the output of the command to a path and file name.

This example shows how to direct the output of the command to the file vsg1-run.cfg in the volatile: directory:

```
vsg# show running-config > volatile:vsg1-run.cfg
```

This example shows how to direct the output of the command to the file vsg2-run.cfg in the bootflash: directory:

```
vsg# show running-config > bootflash:vsg2-run.cfg
```

Verifying a Configuration File Before Loading

You can verify the integrity of an image before loading it.

> **Note** The **copy** command can be used for both the system and kickstart images.

BEFORE YOU BEGIN

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

- You are logged in to the CLI in any command mode.

SUMMARY STEPS

1. **copy** *source path and file* **system:running-config**
2. **show version image** [**bootflash:** | **modflash:** |**volatile:**]

DETAILED STEPS

	Command	Purpose
Step 1	**copy** *source path and file* **system:running-config** **Example:** vsg# copy tftp://10.10.1.1./home/configs/vsg1-run.cfg system:running-config	Copies the source file to the running configuration.
Step 2	**show version image** [**bootflash:** | **modflash:** |**volatile:**] **Example:** vsg# show version image	Validates the specified image.

This example shows how to copy the source file to the running configuration:

```
vsg# copy tftp://10.10.1.1/home/configs/vsg1-run.cfg system:running-config
```

This example shows how to validate the specified image:

```
vsg# show version image bootflash:nexus-1000v-mz.VSG1.0.401.bin
  image name: nexus-1000v-mz.VSG1.0.401.bin
  bios:      version unavailable
  system:    version 4.2(1)VSG1(1) [build 4.2(1)VSG1(0.401)]
  compiled:  12/9/2010 2:00:00 [12/09/2010 15:20:50]
vsg#
```

Reverting to a Previous Configuration

You can recover your configuration from a previously saved version.

BEFORE YOU BEGIN

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

- You are logged in to the CLI in any command mode.

✎

Note Each time that you enter the **copy running-config startup-config** command, a binary file is created and the ASCII file is updated. A valid binary configuration file reduces the overall boot time significantly. A binary file cannot be uploaded, but its contents can be used to overwrite the existing startup configuration. Enter the **write erase** command to clear the binary file.

SUMMARY STEPS

1. **copy running-config bootflash:** {*filename*}
2. **copy bootflash:** {*filename*} **startup-configure**

DETAILED STEPS

	Command	Purpose

Step 1	`copy running-config bootflash:` `{filename}`
	
	 Example:
	 `vsg# copy running-config` `bootflash:Jan24-running`
		Reverts to a snapshot copy of a previously saved running configuration (binary file).

Step 2	`copy bootflash: {filename}` `startup-configure`
	
	 Example:
	 `vsg# copy bootflash:my-configure` `startup-configure`
		Reverts to a configuration copy that was previously saved in the bootflash: file system (ASCII file).

This example shows how to revert to a snapshot copy of a previously saved running configuration:

```
vsg# copy running-config bootflash:January03-Running
```

This example shows how to revert to a configuration copy that was previously saved in the bootflash: directory:

```
vsg# copy bootflash:my-configure startup-configure
```

Displaying Files

This section describes how to display information about files and includes the following topics:

Displaying File Contents

You can display the contents of a specified file.

BEFORE YOU BEGIN

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

- You are logged in to the CLI in EXEC mode.

SUMMARY STEPS

1. **show file** [**bootflash:** | **debug:** | **volatile:**] *filename*

DETAILED STEPS

	Command	Purpose
Step 1	`show file [bootflash:	debug:	volatile:] filename`  **Example:** `vsg# show file bootflash:sample_file.txt`	Displays the contents of the specified file.

This example shows how to displays the contents of the specified file:

```
vsg# show file bootflash:sample_file.txt
security-profile sp1
  policy p1
rule r1
  action 10 permit
policy p1
  rule r1 order 10

vsg#
```

Displaying Directory Contents

You can display the contents of a directory or file system.

BEFORE YOU BEGIN

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

- You are logged in to the CLI in EXEC mode.

SUMMARY STEPS

1. **pwd**
2. **dir**

DETAILED STEPS

	Command	Purpose

Step 1	`pwd`
	
	Example:
	`vsg# pwd`
		Displays the current working directory.

Step 2	`dir`
	
	Example:
	`vsg# dir`
		Displays the contents of the directory.

This example shows how to display your current working directory:

```
vsg# pwd
bootflash:
```

This example shows how to display the contents of a directory:

```
vsg# dir
Usage for volatile://
         0 bytes used
  20971520 bytes free
  20971520 bytes total
vsg#
```

Displaying File Checksums

You can display checksums for checking file integrity.

BEFORE YOU BEGIN

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

- You are logged in to the CLI in EXEC mode.

SUMMARY STEPS

1. **show file** *filename* [**cksum** | **md5sum**]

DETAILED STEPS

	Command	Purpose
Step 1	**show file** *filename* [**cksum**	**md5sum**] **Example:** vsg# show file bootflash:sample_file.txt chksum	Provides the checksum or Message-Digest Algorithm 5 (MD5) checksum of the file for comparison with the original file. MD5 is an electronic fingerprint for the file.

This example shows how to provide the checksum or MD5 checksum of the file for comparison with the original file.

```
vsg# show file bootflash:sample_file.txt cksum
750206909
vsg#
```

This example shows how to provide the MD5 checksum of the file:

```
vsg# show file bootflash:sample_file.txt md5sum
aa163ec1769b9156614c643c926023cf
vsg#
```

Displaying the Last Lines in a File

You can display the last lines of a specified file.

BEFORE YOU BEGIN

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

- You are logged in to the CLI in EXEC mode.

SUMMARY STEPS

1. **tail** {*path*}[*filename*] {*number-of-lines*}

DETAILED STEPS

	Command	Purpose

Step 1	`tail {path}[filename] {number-of-lines}`
	
	`Example:`
	`vsg# tail bootflash:errorsfile 5`
		Displays the requested number of lines from the end of the specified file.
		
		The range for the number-of-lines argument is from 0 to 80.

This example shows how to display the requested number of lines from the end of a specified file:

```
vsg# tail bootflash:errorsfile 5
(20) Event:E_DEBUG, length:34, at 171590 usecs after Tue Jul  1 09:29:05 2008
    [102] main(326): stateless restart
vsg#
```

Displaying the Current User Access

You can display all users currently accessing the Cisco VSG.

BEFORE YOU BEGIN

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

*   You are logged in to the CLI in EXEC mode.

SUMMARY STEPS

1. **show users**

DETAILED STEPS

	Command	Description

Step 1	`show users`
	
	`Example:`
	`vsg# show users`
		Displays a list of users who are currently accessing the Cisco VSG.

This example shows how to display a list of users who are currently accessing the Cisco VSG:

```
vsg# show users
NAME     LINE        TIME           IDLE          PID COMMENT
admin    pts/0       Jul  1 04:40 03:29          2915 (::ffff:64.103.145.136)
admin    pts/2       Jul  1 10:06 03:37          6413 (::ffff:64.103.145.136)
admin    pts/3       Jul  1 13:49   .            8835 (171.71.55.196)*
vsg#
```

Sending a Message to Users

You can send a message to all active users currently using the Cisco VSG.

BEFORE YOU BEGIN

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

- You are logged in to the CLI.

SUMMARY STEPS

1. **send** {**session** *device*} *line*

DETAILED STEPS

	Command	Description
Step 1	**send** {**session** *device*} *line* **Example:** `vsg# send System Shutdown in 10 Minutes`	Sends a message to users currently logged in to the system. You can use the following keyword and argument: - **session**: sends the message to a specified pts/tty device type. - *line* is a message of up to 80 alphanumeric characters.

This example shows how to send a message to all users:

```
vsg# send Hello. Shutting down the system in 10 minutes.
Broadcast Message from admin@vsg (/dev/pts/34) at 8:58 ...
Hello. Shutting down the system in 10 minutes.
vsg#
```

Cisco Virtual Security Gateway High Availability

This chapter describes how to configure high availability (HA) for the Cisco Virtual Security Gateway (VSG).

This chapter includes the following sections:

Information About High Availability

Cisco VSG HA is a subset of the Cisco NX-OS HA. Redundancy or HA is provided by one active Cisco VSG and one standby Cisco VSG. The active Cisco VSG runs and controls all the system applications. Applications are started and initialized in standby mode on the standby Cisco VSG as they are synchronized and updated on the active Cisco VSG. When a failover occurs, the standby Cisco VSG takes over for the active Cisco VSG. The following HA features minimize or prevent traffic disruption in the event of a failure:

- Redundancy—HA pairing of devices
- Isolation of processes—Software component isolation
- Supervisor and Cisco VSG failover—HA pairing of the active/standby Cisco VSG

Figure 5-1 shows the Cisco VSG HA model.

Figure 5-1   *Cisco VSG High Availability*
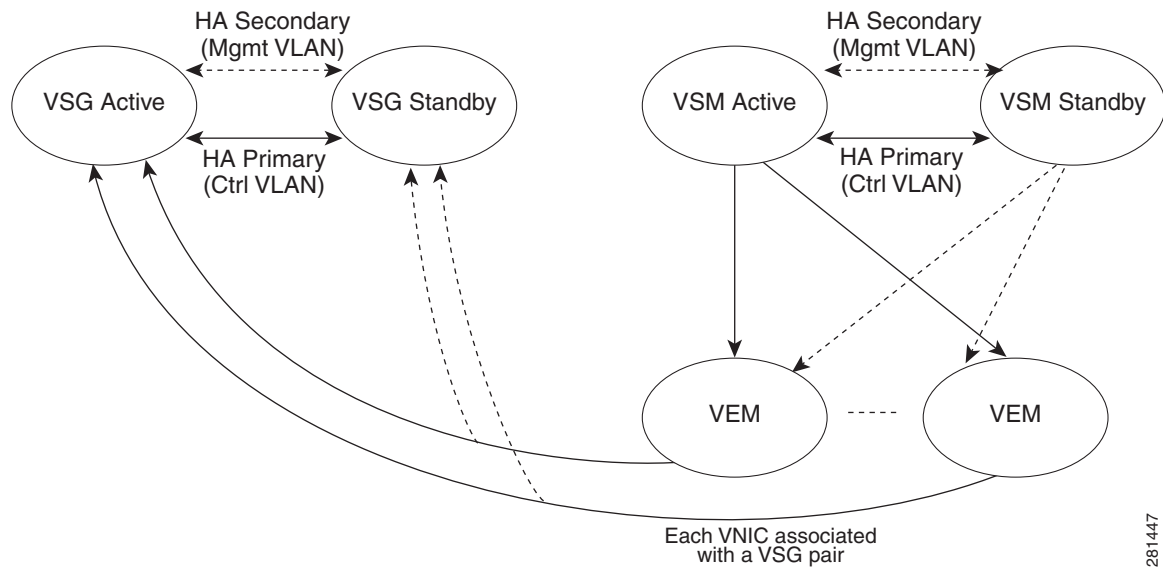
This section includes the following topics:

- Redundancy, page 5-2
- Isolation of Processes, page 5-2
- Cisco VSG Failover, page 5-3

Redundancy

Cisco VSG redundancy is equivalent to HA pairing. The possible redundancy states are active and standby. An active Cisco VSG is paired with a standby Cisco VSG. HA pairing is based on the Cisco VSG ID. Two Cisco VSGs that are assigned the identical ID are automatically paired. All processes running in the Cisco VSG are critical on the data path. If one process fails in an active Cisco VSG, a failover to the standby Cisco VSG occurs instantly and automatically.

Isolation of Processes

The Cisco VSG software contains independent processes, known as services, that perform a function or set of functions for a subsystem or feature set. Each service and service instance runs as an independent, protected process. This way of operating provides a highly fault-tolerant software infrastructure and fault isolation between services. A failure in a service instance does not affect any other services that are running at that time. Additionally, each instance of a service can run as an independent process, which means that two instances of a routing protocol can run as separate processes.

Cisco VSG Failover

When a failover occurs, the Cisco VSG HA pair configuration allows uninterrupted traffic forwarding by using a stateful failover. For information about a Cisco VSG failover, see the "Cisco VSG HA Pair Failover" section on page 5-6.

System-Control Services

The Cisco VSG allows stateful restarts of most processes and services. Back-end management of processes, services, and applications is handled by the following high-level system-control services:

- System Manager
- Persistent Storage Service
- Message and Transaction Service
- HA Policies

Figure 5-2 shows the system-control services.

Figure 5-2   System-Control Services
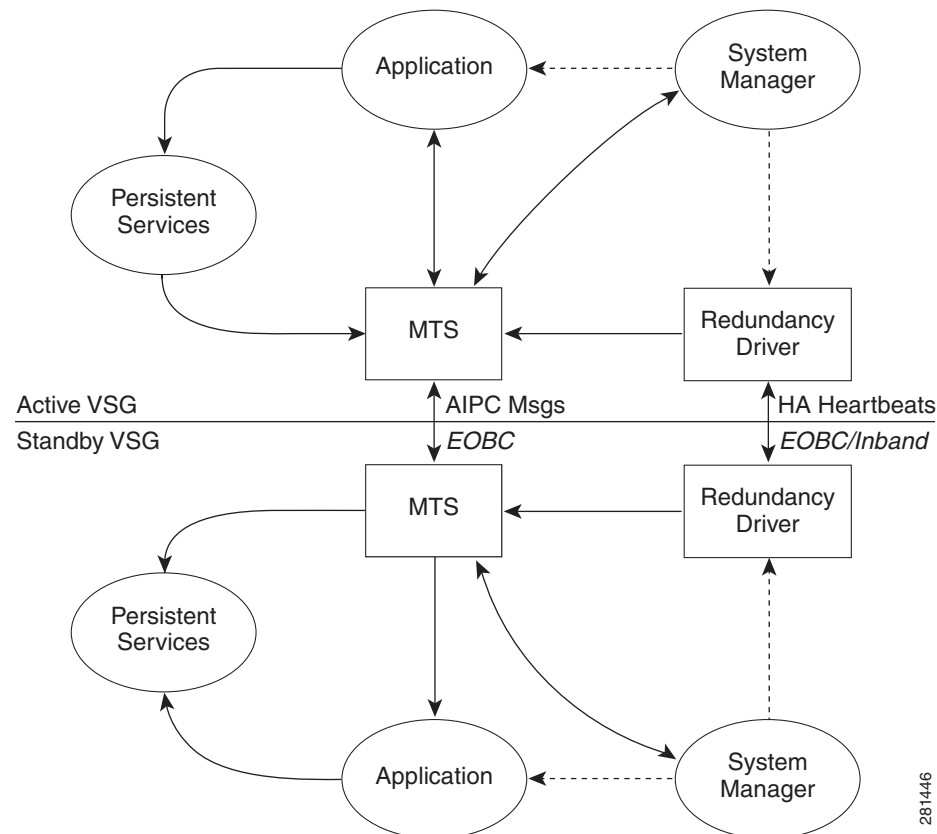
This section includes the following topics:

- System Manager, page 5-4
- Persistent Storage Service, page 5-4

- Message and Transaction Service, page 5-4
- HA Policies, page 5-4

System Manager

The System Manager (SM) directs overall system function, service management, and system health monitoring, and enforces high-availability policies. The SM is responsible for launching, stopping, monitoring, and restarting service, and for initiating and managing the synchronization of service states and supervisor states.

Persistent Storage Service

The Persistent Storage Service (PSS) stores and manages the operational run-time information and configuration of platform services. The PSS component works with system services to recover states if a service restart occurs. It functions as a database of state and run-time information, which allows services to make a checkpoint of their state information whenever needed. A restarting service can recover the last known operating state that preceded a failure.

Each service that uses PSS can define its stored information as private (it can be read only by that service) or shared (the information can be read by other services). If the information is shared, the service can specify that it is local (the information can be read only by services on the same supervisor) or global (it can be read by services on either supervisor or on modules).

Message and Transaction Service

The message and transaction service (MTS) is an interprocess communications (IPC) message broker that specializes in high-availability semantics. The MTS handles message routing and queuing between services on and across modules and between supervisors. The MTS facilitates the exchange of messages, such as event notification, synchronization, and message persistency, between system services and system components. The MTS can maintain persistent messages and logged messages in queues for access even after a service restart.

HA Policies

The Cisco NX-OS software usually allows each service to have an associated set of internal HA policies that define how a failed service is restarted. When a process fails on a device, System Manager either performs a stateful restart, a stateless restart, or a failover.

Note   Only processes that are borrowed by a Cisco VSG from a VSM restart. Processes that are native to a Cisco VSG, such as policy engine or inspect, do not restart. A failed native Cisco VSG process causes an automatic failover.

Cisco VSG HA Pairs

Cisco VSG HA pairs have the following characteristics:

- Redundancy is provided by one active Cisco VSG and one standby Cisco VSG.
- The active Cisco VSG runs and controls all the system applications.
- Applications are started and initialized in standby mode on the standby Cisco VSG.
- Applications are synchronized and updated on the standby Cisco VSG.
- When a failover occurs, the standby Cisco VSG takes over for the active Cisco VSG.

This section includes the following topics:

- Cisco VSG Roles, page 5-5
- HA Pair States, page 5-5
- Cisco VSG HA Pair Synchronization, page 5-5

Cisco VSG Roles

The Cisco VSG roles are as follows:

- Standalone—This role does not interact with other Cisco VSGs. You assign this role when there is only one Cisco VSG in the system. This role is the default.
- Primary—This role coordinates the active/standby state with the secondary Cisco VSG. It takes precedence during bootup when negotiating the active/standby mode. That is, if the secondary Cisco VSG does not have the active role at bootup, the primary Cisco VSG takes the active role. You assign this role to the first Cisco VSG that you install in an HA Cisco VSG system.
- Secondary—This role coordinates the active/standby state with the primary Cisco VSG. You assign this role to the second Cisco VSG that you add to a Cisco VSG HA pair.

HA Pair States

The Cisco VSG HA pair states are as follows:

- Active—This state indicates the Cisco VSG is active and controls the system. It is visible to the user through the **show system redundancy status** command.
- Standby—This state indicates that the Cisco VSG has synchronized its configuration with the active Cisco VSG so that it is continuously ready to take over in case of a failure or manual switchover.

Cisco VSG HA Pair Synchronization

The active and standby Cisco VSGs automatically synchronize when the internal state of one is active and the internal state of the other is standby.

If the output of the **show system redundancy status** command indicates that the operational redundancy mode of the active Cisco VSG is none, the active and standby Cisco VSGs are not synchronized.

This example shows the internal state of Cisco VSG HA pair when they are synchronized:

```
vsg# show system redundancy status
Redundancy role
---------------
      administrative:   primary
         operational:   primary


Redundancy mode
---------------
      administrative:   HA
         operational:   HA


This supervisor (sup-1)
-----------------------
    Redundancy state:   Active
    Supervisor state:   Active
      Internal state:   Active with HA standby


Other supervisor (sup-2)
-----------------------
    Redundancy state:   Standby
Supervisor state: HA standby
Internal state: HA standby
vsg#
```

Cisco VSG HA Pair Failover

The Cisco VSG HA pair configuration allows uninterrupted traffic forwarding using a stateful failover when a failure occurs. The pair operates in an active/standby capacity in which only one is active at any given time, while the other acts as a standby backup. The two Cisco VSGs constantly synchronize the state and configuration in order to provide a stateful failover of most services.

This section includes the following topics:

- Failover Characteristics, page 5-6
- Automatic Failovers, page 5-6
- Manual Failovers, page 5-7

Failover Characteristics

A failover occurs when the active Cisco VSG fails and it has the following characteristics:

- It is stateful, or nondisruptive, because control traffic is not affected.
- It does not disrupt data traffic because the Virtual Ethernet Modules (VEMs) are not affected.

Automatic Failovers

When a stable standby Cisco VSG detects that the active Cisco VSG has failed, it initiates a failover and transitions to active. When a failover begins, another failover cannot be started until a stable standby Cisco VSG is available. If a standby Cisco VSG that is not stable detects that an active Cisco VSG has failed, then instead of initiating a failover, it tries to restart the pair.

Manual Failovers

Before you can initiate a manual failover from the active to the standby Cisco VSG, the standby Cisco VSG must be stable. To find out if it is, see the "Verifying that a Cisco VSG Pair is Ready for a Failover" section on page 5-9. Once you have verified that the standby Cisco VSG is stable, you can manually initiate a failover. To find out if it is, see the "Manually Switching the Active Cisco VSG to Standby" section on page 5-10. Once a failover process begins, another failover process cannot be started until a stable standby Cisco VSG is available.

Cisco VSG HA Guidelines and Limitations

HA pairs have the following configuration guidelines and limitations:

*   Although primary and secondary Cisco VSGs can reside in the same host, to improve redundancy install them in separate hosts and, if possible, connect them to different upstream switches.

*   The console for the standby Cisco VSG is available through the vSphere client or by using the **attach module** [*1 | 2*] command depending on whether the primary is active or not, but configuration is not allowed and many commands are restricted. The **attach module** [*1 | 2*] command must be executed at the console of the active Cisco VSG.

Changing the Cisco VSG Role

You can change the role of a Cisco VSG to one of the following after it is already in service:

*   Standalone

*   Primary

*   Secondary

BEFORE YOU BEGIN

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

⚠ **Caution**   Changing the role of a Cisco VSG can result in a conflict between the pair. If a primary and secondary see each other as active at the same time, the system resolves this problem by resetting the primary Cisco VSG. If you are changing a standalone Cisco VSG to a secondary Cisco VSG, be sure to first isolate it from the other Cisco VSG in the pair to prevent any interaction with the primary Cisco VSG during the change. Power the Cisco VSG off before reconnecting it as standby.

*   You are logged into the CLI in EXEC mode.

*   To activate a change from a primary to a secondary Cisco VSG, you must reload the primary Cisco VSG by doing one of the following:

    –   Enter the **reload** command.

    –   Power the Cisco VSG off and then on from the vSphere Client.

*   A change from a standalone to a primary Cisco VSG takes effect immediately.

To change a standalone Cisco VSG to a secondary Cisco VSG, see the "Pairing a Second Cisco VSG with an Active Cisco VSG" section on page 5-13.

SUMMARY STEPS

1. (Optional) **system redundancy role** {**standalone** | **primary** | **secondary**}

2. (Optional) **show system redundancy status**

3. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**system redundancy role** {**standalone** | **primary** | **secondary**} **Example:** vsg# system redundancy role primary	Specifies the HA role of a Cisco VSG.
Step 2	**show system redundancy status** **Example:** vsg# show system redundancy status	(Optional) Displays the current redundancy status for the Cisco VSG.
Step 3	**copy running-config startup-config** **Example:** vsg# copy running-config startup-configure	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

EXAMPLES

This example shows how to specify the HA role of a Cisco VSG:

```
vsg# system redundancy role standalone
vsg#
```

This example shows how to display the system redundancy status of a standalone Cisco VSG:

```
vsg# show system redundancy status
Redundancy role
---------------
      administrative:   standalone
         operational:   standalone

Redundancy mode
---------------
      administrative:   HA
         operational:   None

This supervisor (sup-1)
-----------------------
   Redundancy state: Active
   Supervisor state: Active
   Internal state: Active with no standby

Other supervisor (sup-2)
-----------------------
   Redundancy state:   Not present
vsg#
```

This example shows how to copy the running configuration to the startup configuration:

```
vsg# copy running-config startup-config
[#######################################] 100%
vsg#
```

Configuring a Failover

This section includes the following topics:

- Guidelines and Limitations, page 5-9
- Verifying that a Cisco VSG Pair is Ready for a Failover, page 5-9
- Manually Switching the Active Cisco VSG to Standby, page 5-10

Guidelines and Limitations

Failovers have the following configuration guidelines:

- When you manually initiate a failover, system messages are generated that indicate the presence of two Cisco VSGs and identify which one is becoming active.
- A failover can only be done when both Cisco VSGs are functioning.

Verifying that a Cisco VSG Pair is Ready for a Failover

You can verify that both an active and standby Cisco VSG are in place and operational before proceeding with a failover.

BEFORE YOU BEGIN

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

- You are logged into the CLI in EXEC mode.
- If the standby Cisco VSG is not in a stable state (the state must be **ha-standby**), a manually initiated failover cannot be done.

SUMMARY STEPS

1. **show system redundancy status**

DETAILED STEPS

	Command	Purpose

Step 1	`show system redundancy status`
	
	Example:
	`vsg# show system redundancy status`
		Displays the current redundancy status for the Cisco VSG(s).
		
		If the output indicates the following, you can proceed with a system failover, if needed:
		
		• The presence of an active Cisco VSG
		
		• The presence of a standby Cisco VSG in the HA standby redundancy state

EXAMPLES

This example shows how to verify that a Cisco VSG pair is ready for a failover:

```
vsg# show system redundancy status
Redundancy role
---------------
     administrative:   primary
         operational:   primary

Redundancy mode
---------------
     administrative:   HA
         operational:   None

This supervisor (sup-1)
-----------------------
   Redundancy state:   Active
   Supervisor state:   Active
     Internal state:   Active with no standby

Other supervisor (sup-2)
-----------------------
   Redundancy state:   Active
   Supervisor state:   Active
     Internal state:   Active with no standby
```

Manually Switching the Active Cisco VSG to Standby

You can manually switch an active Cisco VSG to standby in an HA pair.

BEFORE YOU BEGIN

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

• You are logged in to the active Cisco VSG CLI in EXEC mode.

• You have completed the steps in the "Verifying that a Cisco VSG Pair is Ready for a Failover" section on page 5-9 and have found the system to be ready for a failover.

• A failover can be performed only when two Cisco VSGs are functioning.

• If the standby Cisco VSG is not in a stable state, you cannot initiate a manual failover and you see the following error message:

```
Failed to switchover (standby not ready to takeover in vdc 1)
```

- Once you enter the **system switchover** command, you cannot start another failover process on the same system until a stable standby Cisco VSG is available.
- Any unsaved running configuration that was available in the active Cisco VSG is still unsaved in the new active Cisco VSG. You can verify this unsaved running configuration by using the **show running-config diff** command. Save that configuration, if needed, as you would do in the other Cisco VSG by entering the **copy running-config startup-config** command.

SUMMARY STEPS

1. **system switchover**
2. (Optional) **show running-config diff**
3. **configure**
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**system switchover** **Example:** vsg# system switchover	Initiates a manual failover from the active Cisco VSG to the standby Cisco VSG. **Note** Once you enter this command, you cannot start another failover process on the same system until a stable standby Cisco VSG is available. **Note** Before proceeding, wait until the switchover completes and the standby supervisor becomes active.
Step 2	**show running-config diff** **Example:** vsg# show running-config diff	(Optional) Verifies the difference between the running and startup configurations. Any unsaved running configuration in an active Cisco VSG is also unsaved in the Cisco VSG that becomes active after a failover. Save that configuration in the startup if needed.
Step 3	**configure** **Example:** vsg# configure	Places you in global configuration mode.
Step 4	**copy running-config startup-config** **Example:** vsg# copy running-config startup-config	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

EXAMPLES

This example shows how to switch an active Cisco VSG to the standby Cisco VSG and displays the output that appears on the standby Cisco VSG as it becomes the active Cisco VSG:

```
vsg# system switchover
--------------------------
```

```
2011 Jan 18 04:21:56 n1000v %$ VDC-1 %$ %SYSMGR-2-HASWITCHOVER_PRE_START:
This supervisor is becoming active (pre-start phase).
2011 Jan 18 04:21:56 n1000v %$ VDC-1 %$ %SYSMGR-2-HASWITCHOVER_START:
This supervisor is becoming active.
2011 Jan 18 04:21:57 n1000v %$ VDC-1 %$ %SYSMGR-2-SWITCHOVER_OVER: Switchover completed.
2011 Jan 18 04:22:03 n1000v %$ VDC-1 %$ %PLATFORM-2-MOD_REMOVE: Module 1 removed (Serial
number )
```

This example shows how to display the difference between the running and startup configurations:

```
vsg# show running-config diff
*** Startup-config
--- Running-config
***************
*** 1,38 ****
  version 4.0(4)SV1(1)
  role feature-group name new
  role name testrole
  username admin password 5 $1$S7HvKc5G$aguYqHl0dPttBJAhEPwsy1  role network-admin
  telnet server enable
  ip domain-lookup
```

This example shows how to copy the running configuration to the startup configuration:

```
vsg# configure
vsg(config)# copy running-config startup-config
[#####################################] 100%
vsg(config)#
```

Assigning IDs to HA Pairs

You can create Cisco VSG HA pairs. Each HA pair is uniquely identified by an identification (ID) called an HA pair ID. The configuration state synchronization between the active and standby Cisco VSGs occurs between those Cisco VSG pairs that share the same HA pair ID.

BEFORE YOU BEGIN

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

- You are logged in to the CLI in configuration mode.

SUMMARY STEPS

1. **configure**
2. **ha-pair id** {*number*}

DETAILED STEPS

	Command	Purpose
Step 1	**configure** **Example:** vsg# configure	Places you in global configuration mode.

	Command	Purpose

Step 2	`ha-pair id {number}`
	
	Example:
	`vsg(config-svs-domain)# ha-pair id 10`
		Assigns an ID to an HA pair.

EXAMPLES

This example shows how to assign an ID to an HA pair:

```
vsg# configure
vsg(config)# ha-pair id 10
vsg(config)#
```

Pairing a Second Cisco VSG with an Active Cisco VSG

You can change a standalone Cisco VSG into an HA pair by adding a second Cisco VSG.

This section includes the following topics:

BEFORE YOU BEGIN

Before adding a second Cisco VSG to a standalone system, you must know or do the following:

- You are logged into the CLI in EXEC mode.
- Although primary and secondary Cisco VSGs can reside in the same host, you can improve redundancy by installing them in separate hosts and, if possible, connecting them to different upstream switches.
- When installing the second Cisco VSG, assign it with the secondary role.
- Set up the port groups for the dual Cisco VSG VMs with the same parameters in both hosts.
- After the secondary Cisco VSG is paired, the following occurs automatically:
  - The secondary Cisco VSG is reloaded and added to the system.
  - The secondary Cisco VSG negotiates with the primary Cisco VSG and becomes the standby Cisco VSG.
  - The standby Cisco VSG synchronizes its configuration and state with the primary Cisco VSG.

Changing the Standalone Cisco VSG to a Primary Cisco VSG

You can change the role of a Cisco VSG from standalone to primary in a Cisco VSG HA pair.

BEFORE YOU BEGIN

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

- You are logged into the CLI in EXEC mode.
- A change from a standalone to a primary takes effect immediately.

SUMMARY STEPS

1. **system redundancy role primary**
2. **show system redundancy status**
3. **configure**
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	`system redundancy role primary`
	
	`Example:`
	`vsg# system redundancy role primary`
		Changes the standalone Cisco VSG to a primary Cisco VSG.
		
		The role change occurs immediately.

Step 2	`show system redundancy status`
	
	`Example:`
	`vsg# show system redundancy status`
		Displays the current redundancy state for the Cisco VSG.

Step 3	`configure`
	
	`Example:`
	`vsg# configure`
		Places you in global configuration mode.

Step 4	`copy running-config startup-config`
	
	`Example:`
	`vsg(config)# copy running-config startup-config`
		(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

EXAMPLES

This example shows how to change the standalone Cisco VSG to a primary Cisco VSG:

```
vsg# system redundancy role primary
vsg#
```

This example shows how to display the current system redundancy status for a Cisco VSG:

```
vsg# show system redundancy status
Redundancy role
---------------
      administrative:   primary
         operational:   primary


Redundancy mode
---------------
      administrative:   HA
         operational:   None

This supervisor (sup-1)
-----------------------
    Redundancy state:   Active
    Supervisor state:   Active
      Internal state:   Active with no standby

Other supervisor (sup-2)
-----------------------
    Redundancy state:   Not present
```

This example shows how to copy the running configuration to the startup configuration:

```
vsg# configure
vsg(config)# copy running-config startup-config
[#########################################] 100%
vsg(config)#
```

Verifying the Change to a Cisco VSG HA Pair

You can verify a change from a single Cisco VSG to a Cisco VSG HA pair.

BEFORE YOU BEGIN

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

- You are logged into the CLI in EXEC mode.
- You have already changed the single Cisco VSG role from standalone to primary. See the "Changing the Standalone Cisco VSG to a Primary Cisco VSG" section on page 5-13.

SUMMARY STEPS

1. **show system redundancy status**

DETAILED STEPS

	Command	Purpose
Step 1	**show system redundancy status** **Example:** vsg# show system redundancy status	Displays the current redundancy status for Cisco VSGs in the system.

EXAMPLES

This example shows how to display the current redundancy status for Cisco VSGs in the system. In this example, the primary and secondary Cisco VSGs are shown following a change from a single Cisco VSG system to a dual Cisco VSG system.

```
vsg# show system redundancy status
    Redundancy role
    ---------------
    administrative: primary
    operational: primary
    Redundancy mode
    ---------------
    administrative: HA
    operational: HA
```

```
        This supervisor (sup-1)
        -----------------------
        Redundancy state: Active
        Supervisor state: Active
        Internal state: Active with HA standby
Other supervisor (sup-2)
-----------------------
Redundancy state: Standby
Supervisor state: HA standby
Internal state: HA standby
```

Replacing the Standby Cisco VSG in an HA Pair

You can replace a standby/secondary Cisco VSG in an HA pair.

> **Note**   Equipment Outage—This procedure requires that you power down and reinstall a Cisco VSG. During this time, your system will be operating with a single Cisco VSG.

PROCEDURE

Step 1   Power off the standby Cisco VSG.

Step 2   Install the new Cisco VSG as a standby, with the same domain ID as the existing Cisco VSG.

After the new Cisco VSG is added to the system, it synchronizes with the existing Cisco VSG.

Replacing the Active Cisco VSG in an HA Pair

You can replace an active/primary Cisco VSG in an HA pair.

BEFORE YOU BEGIN

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

- You are logged into the CLI in EXEC mode.
- You must configure the port groups so that the new primary Cisco VSG cannot communicate with the secondary Cisco VSG or any of the VEMs during the setup. Cisco VSGs with a primary or secondary redundancy role have built-in mechanisms for detecting and resolving the conflict between two Cisco VSGs in the active state. In order to avoid these mechanisms during the configuration of the new primary Cisco VSG, you must isolate the new primary Cisco VSG from the secondary Cisco VSG.

> **Note**   Equipment Outage—This procedure requires powering down and reinstalling a Cisco VSG. During this time, your system will be operating with a single Cisco VSG.

PROCEDURE

Step 1   Power off the active Cisco VSG.

The secondary Cisco VSG becomes active.

Step 2   On a vSphere Client, change the port group configuration for the new primary Cisco VSG to prevent communication with the secondary Cisco VSG and the VEMs during setup.

Step 3   Install the new Cisco VSG as the primary, with the same domain ID as the existing Cisco VSG.

Step 4   On the vSphere Client, change the port group configuration for the new primary Cisco VSG to permit communication with the secondary Cisco VSG and the VEMs.

Step 5   Power up the new primary Cisco VSG.

The new primary Cisco VSG starts and automatically synchronizes all configuration data with the secondary, which is currently the active Cisco VSG. Because the existing Cisco VSG is active, the new primary Cisco VSG becomes the standby Cisco VSG and receives all configuration data from the existing active Cisco VSG.

Verifying the HA Status

You can display and verify the HA status.

SUMMARY STEPS

    1. **show system redundancy status**

DETAILED STEPS

	Command	Purpose
Step 1	**show system redundancy status** **Example:** vsg# show system redundancy status	Displays the HA status of the system.

EXAMPLES

This example shows how to display the system redundancy status:

```
vsg# show system redundancy status
Redundancy role
---------------
administrative: primary
operational: primary
Redundancy mode
---------------
administrative: HA
operational: HA
```

```
This supervisor (sup-1)
-----------------------
Redundancy state: Active
Supervisor state: Active
Internal state: Active with HA standby
Other supervisor (sup-2)
-----------------------
Redundancy state: Standby
Supervisor state: HA standby
Internal state: HA standby
```

This example shows how to display the state and start count of all processes:

```
vsg# show processes
PID    State PC        Start_cnt   TTY    Process
-----  ----- --------  ----------- ----   ------------
    1     S  b7f8a468            1   -    init
    2     S         0            1   -    ksoftirqd/0
    3     S         0            1   -    desched/0
    4     S         0            1   -    events/0
    5     S         0            1   -    khelper
   10     S         0            1   -    kthread
   18     S         0            1   -    kblockd/0
   35     S         0            1   -    khubd
  188     S         0            1   -    pdflush
  189     S         0            1   -    pdflush
  190     S         0            1   -    kswapd0
  191     S         0            1   -    aio/0
  776     S         0            1   -    kseriod
  823     S         0            1   -    kide/0
  833     S         0            1   -    ata/0
  837     S         0            1   -    scsi_eh_0
 1175     S         0            1   -    kjournald
 1180     S         0            1   -    kjournald
 1740     S         0            1   -    kjournald
 1747     S         0            1   -    kjournald
 1979     S  b7f6c18e            1   -    portmap
 1992     S         0            1   -    nfsd
 1993     S         0            1   -    nfsd
 1994     S         0            1   -    nfsd
 1995     S         0            1   -    nfsd
 1996     S         0            1   -    nfsd
 1997     S         0            1   -    nfsd
 1998     S         0            1   -    nfsd
 1999     S         0            1   -    nfsd
 2000     S         0            1   -    lockd
 2001     S         0            1   -    rpciod
 2006     S  b7f6e468            1   -    rpc.mountd
 2012     S  b7f6e468            1   -    rpc.statd
 2039     S  b7dd2468            1   -    sysmgr
 2322     S         0            1   -    mping-thread
 2323     S         0            1   -    mping-thread
 2339     S         0            1   -    stun_kthread
 2340     S         0            1   -    stun_arp_mts_kt
 2341     S         0            1   -    stun_packets_re
 2376     S         0            1   -    redun_kthread
 2377     S         0            1   -    redun_timer_kth
 2516     S         0            1   -    sf_rdn_kthread
 2517     S  b7f37468            1   -    xinetd
 2518     S  b7f6e468            1   -    tftpd
 2519     S  b79561b6            1   -    syslogd
 2520     S  b7ecc468            1   -    sdwrapd
 2522     S  b7da3468            1   -    platform
 2527     S         0            1   -    ls-notify-mts-t
```

Cisco Virtual Security Gateway for Nexus 1000V Series Switch Configuration Guide, Release 4.2(1)VSG1(3.1)

```
2541     S   b7eabbe4            1    -   pfm_dummy
2549     S   b7f836be            1    -   klogd
2557     S   b7c09be4            1    -   vshd
2558     S   b7e4f468            1    -   stun
2559     S   b7b11f43            1    -   smm
2560     S   b7ea1468            1    -   session-mgr
2561     S   b7cd1468            1    -   psshelper
2562     S   b7f75468            1    -   lmgrd
2563     S   b7e6abe4            1    -   licmgr
2564     S   b7eb5468            1    -   fs-daemon
2565     S   b7e97468            1    -   feature-mgr
2566     S   b7e45468            1    -   confcheck
2567     S   b7ea9468            1    -   capability
2568     S   b7cd1468            1    -   psshelper_gsvc
2576     S   b7f75468            1    -   cisco
2583     S   b779f40d            1    -   clis
2586     S   b76e140d            1    -   port-profile
2588     S   b7d07468            1    -   xmlma
2589     S   b7e69497            1    -   vnm_pa_intf
2590     S   b7e6e468            1    -   vmm
2591     S   b7b9c468            1    -   vdc_mgr
2592     S   b7e73468            1    -   ttyd
2593     R   b7edb5f5            1    -   sysinfo
2594     S   b7d07468            1    -   sksd
2596     S   b7e82468            1    -   res_mgr
2597     S   b7e49468            1    -   plugin
2598     S   b7bb9f43            1    -   npacl
2599     S   b7e93468            1    -   mvsh
2600     S   b7e02468            1    -   module
2601     S   b792c40d            1    -   fwm
2602     S   b7e93468            1    -   evms
2603     S   b7e8d468            1    -   evmc
2604     S   b7ec4468            1    -   core-dmon
2605     S   b7e11468            1    -   bootvar
2606     S   b769140d            1    -   ascii-cfg
2607     S   b7ce5be4            1    -   securityd
2608     S   b77de40d            1    -   cert_enroll
2609     S   b7ce2468            1    -   aaa
2611     S   b7b0bf43            1    -   l3vm
2612     S   b7afef43            1    -   u6rib
2613     S   b7afcf43            1    -   urib
2615     S   b7e05468            1    -   ExceptionLog
2616     S   b7daa468            1    -   ifmgr
2617     S   b7ea5468            1    -   tcap
2621     S   b763340d            1    -   snmpd
2628     S   b7f02d39            1    -   PMon
2629     S   b7c00468            1    -   aclmgr
2646     S   b7b0ff43            1    -   adjmgr
2675     S   b7b0bf43            1    -   arp
2676     S   b793b896            1    -   icmpv6
2677     S   b79b2f43            1    -   netstack
2755     S   b77ac40d            1    -   radius
2756     S   b7f3ebe4            1    -   ip_dummy
2757     S   b7f3ebe4            1    -   ipv6_dummy
2758     S   b78e540d            1    -   ntp
2759     S   b7f3ebe4            1    -   pktmgr_dummy
2760     S   b7f3ebe4            1    -   tcpudp_dummy
2761     S   b784640d            1    -   cdp
2762     S   b7b6440d            1    -   dcos-xinetd
2765     S   b7b8f40d            1    -   ntpd
2882     S   b7dde468            1    -   vsim
2883     S   b799340d            1    -   ufdm
2884     S   b798640d            1    -   sal
2885     S   b795940d            1    -   pltfm_config
```

```
2886     S   b787640d              1    -   monitor
2887     S   b7d71468              1    -   ipqosmgr
2888     S   b7a4827b              1    -   igmp
2889     S   b7a6640d              1    -   eth-port-sec
2890     S   b7b7e468              1    -   copp
2891     S   b7ae940d              1    -   eth_port_channel
2892     S   b7b0a468              1    -   vlan_mgr
2895     S   b769540d              1    -   ethpm
2935     S   b7d3a468              1    -   msp
2938     S   b590240d              1    -   vms
2940     S   b7e8d468              1    -   vsn_service_mgr
2941     S   b7cc0468              1    -   vim
2942     S   b7d57468              1    -   vem_mgr
2943     S   b7d25497              1    -   policy_engine
2944     S   b7e6a497              1    -   inspect
2945     S   b7d33468              1    -   aclcomp
2946     S   b7d1c468              1    -   sf_nf_srv
2952     S   b7f1deee              1    -   thttpd.sh
2955     S   b787040d              1    -   dcos-thttpd
3001     S   b7f836be              1    1   getty
3003     S   b7f806be              1    S0  getty
3004     S   b7f1deee              1    -   gettylogin1
3024     S   b7f836be              1    S1  getty
15497    S   b7a3840d              1    -   in.dcos-telnetd
15498    S   b793a468              1    20  vsh
19217    S   b7a3840d              1    -   in.dcos-telnetd
19218    S   b7912eee              1    21  vsh
19559    S   b7f5d468              1    -   sleep
19560    R   b7f426be              1    21  more
19561    R   b7939be4              1    21  vsh
19562    R   b7f716be              1    -   ps
   -     NR      -                 0    -   tacacs
   -     NR      -                 0    -   dhcp_snoop
   -     NR      -                 0    -   installer
   -     NR      -                 0    -   ippool
   -     NR      -                 0    -   nfm
   -     NR      -                 0    -   private-vlan
   -     NR      -                 0    -   scheduler
   -     NR      -                 0    -   vbuilder
vsg#
```

Cisco Virtual Security Gateway Firewall Profiles and Policy Objects

This chapter describes how to configure the Cisco Virtual Security Gateway (VSG) firewall profiles and policy objects.

This chapter includes the following sections:

Information About Cisco VSG Firewall Policy Objects

Use the Cisco Virtual Network Management Center (VNMC) to do all configuration and management of the Cisco VSG.

Note When the policy-agent (PA) is installed, the command-line interface (CLI) is unavailable for configuring policy-related objects on the Cisco VSG. When the PA is uninstalled (removed), you can again configure the policies (and policy objects) from the CLI; however, we recommend that you use the Cisco VNMC for all configuration and management of the Cisco VSG firewall policy objects.

Cisco VSG Firewall Policy Objects

This section includes the following topics:

Cisco VSG Policy Object Configuration Prerequisites

Cisco VSG policy objects have the following prerequisites:

• You must have the NEXUS_VSG_SERVICES_PKG license installed on the Cisco Nexus 1000V Series switch.

• Ensure that you have enough licenses to cover the number of ESX hosts (VEMs) you want to protect.

• Create port profiles for the service and HA interfaces of Cisco VSG on the Virtual Supervisor Module (VSM).

• You have the Cisco VSG software installed and the basic installation completed. For details, see the *Cisco Virtual Security Gateway, Release 4.2(1)VSG1(3.1) and Cisco Virtual Network Management Center, Release 1.3 Installation and Upgrade Guide*.

• The data IP address and management IP addresses must be configured. To configure the data IP address, see the *Cisco Virtual Security Gateway, Release 4.2(1)VSG1(3.1) and Cisco Virtual Network Management Center, Release 1.3 Installation and Upgrade Guide*.

• You have the attribute details required for your security policies.

• You are logged in to the Cisco VSG CLI in EXEC mode.

Cisco VSG Configuration Guidelines and Limitations

The Cisco VSG has the following configuration guidelines and limitations:

• The Management VLAN must be on the VM network vSwitch.

• The HA and Service VLANs are configured on the uplink ports. (They are not required to be on the system VLAN.)

• Do not configure the same network IP address on the management and data interfaces (data0) of the Cisco VSG.

For any configuration and management tasks, the following requirements must be met:

• The Cisco VSG software must be operating with three network adapters. The network labels are as follows:

  – Service (Eth0) as the port-profile

  – Mgmt (Eth1) as the management VLAN

  – HA (Eth2) as the port-profile

• You have the Cisco VSG VM powered on and the data interface IP address (for data0) and management interface IP address configured.

See the *Cisco Virtual Security Gateway, Release 4.2(1)VSG1(3.1) and Cisco Virtual Network Management Center, Release 1.3 Installation and Upgrade Guide*, for details about assigning network labels to the network adapters.

Default Settings

Table 6-1 lists the default setting for the Cisco VSG parameters.

Table 6-1   Default Parameter

Parameters	Default
rule policy object	drop

Zones

A zone is a logical group of virtual machines (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 attributes.

This example shows how the zone is expressed in the **show running-config** command output:

```
vsg# show running-config zone zone1
zone zone1
   condition 1 net.ip-address eq 1.1.1.1
   condition 2 net.port eq 80
```

Object Groups

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

This example shows how the object groups are expressed in the **show running-config** command output:

```
vsg# show running-config object-group g1
object-group g1 net.port
  match 1 eq 80
  match 2 eq 443
```

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 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

This example shows how the rule is expressed in the **show running-config** command output:

```
vsg# show running-config rule r2
rule r2
  condition 1 dst.net.ip-address eq 2.2.2.2
  condition 2 src.net.ip-address eq 1.1.1.1
  condition 3 src.net.port eq 100
  condition 4 dst.net.port eq 80
  condition 5 net.protocol eq 6
  action 1 permit
```

Policies

Firewall policies bind rules to a given policy, creating a rank among the rules. A policy enforces network traffic on a Cisco VSG and is constructed by using the following set of policy objects:

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

A policy is bound to a Cisco VSG 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.

This example shows how the policy is expressed in the **show running-config** command output:

```
vsg# show running-config policy p2
policy p2
  rule r2 order 10
```

This example shows how conditions are expressed in the **show running-config** command output:

```
condition 1 dst.net.ip-address eq 2.2.2.2
condition 2 src.net.ip-address eq 1.1.1.1
```

This example shows how an action is expressed in the **show running-config** command output:

```
action 1 permit
```

Cisco Virtual Security Gateway Attributes

This section describes Cisco Virtual Security Gateway attributes.

This section includes the following topics:

- Information About Attribute Name Notations, page 6-4
- Attribute Classes, page 6-5

Information About Attribute Name Notations

This section includes the following topics:

- Directional Attributes, page 6-5
- Neutral Attributes, page 6-5

Directional Attributes

A firewall policy is direction sensitive with regard to incoming or outgoing packets. An attribute in a rule condition requires that you have specified if the attribute is relevant to a source or a destination. The prefixes src., dst., or an attribute name are used to provide the sense of direction.

Neutral Attributes

Because object groups and zones can be shared between various rules with different directions, the attributes used in an object group should not have a directional sense. Attributes without a directional sense (that do not provide a direction prefix such as src. or dst.) are called neutral attributes.

Two rule conditions with different directions can share the same object group definition. A neutral attribute and net.ip-address used in the object-group can be associated with the directional attributes, such as src.net.ip-address and dst.net.ip-address, used in the different rules.

Attribute Classes

Cisco VSG attributes are classified into the following classes:

- Network Attributes, page 6-5
- VM Attributes, page 6-6
- Zone Attributes, page 6-7

Attributes are used in configuring policy rules and conditions, or zone definitions. Zones can be defined using VM attributes.

Network Attributes

This section describes the VSG network attributes (see Table 6-2).

.

Table 6-2   Network Attributes

Description	Name
Source IP address	src.net.ip-address
Source port	src.net.port
Destination IP address	dst.net.ip-address
Destination port	dst.net.port
IP address[1]	net.ip-address
Port[1]	net.port
IP Protocols 9[1]	net.protocol
EtherType of the Layer 2 mode frame[1]	net.ethertype

1. Neutral attribute

VM Attributes

The VM attributes are attributes that are related to the virtual machine infrastructure and include the following classes of VM attributes:

- Virtual infrastructure attributes—These attributes are obtained from the VMware vCenter and are mapped to the names listed in Table 6-3.
- Port profile attributes—These attributes are associated with port profiles.
- Custom attributes—These attributes can be configured under a service profile.

Table 6-3 describes the VM attributes supported.

Table 6-3   VM Attributes

Description	Name
Name of VM	src.vm.name
	dst.vm.name
	vm.name[1]
Name of host parent (ESX host)	src.vm.host-name
	dst.vm.host-name
	vm.host-name[1]
Full name of OS guest (includes the version)	src.vm.os-fullname
	dst.vm.os-fullname
	vm.os-fullname[1]
Name of associated virtual application	src.vm.vapp-name
	dst.vm.vapp-name
	vm.vapp-name[1]
Name of associated cluster	src.vm.cluster-name
	dst.vm.cluster-name
	vm.cluster.name[1]
Inventory path of the VM	src.vm.inventory-path
	dst.vm.inventory-path
	vm.inventory-path[1]
Name of port profile associated with specific vNIC	src.vm.portprofile-name
	dst.vm.portprofile-name
	vm.portprofile-name[1]
Custom attributes from security profile of associated port group. **Note** For every unique custom-attribute xxx, the synthesized attribute name is src.vm.custom.xxx or dst.vm.custom.xxx. The policy uses the synthesized attribute name.	src.vm.custom.xxx
	dst.vm.custom.xxx
	vm.custom.xxx[1]

1. Neutral attributes

Custom VM attributes are user-defined attributes that can be configured under a service profile.

This example shows how to verify the VM attributes on a Cisco VSG:

```
vsg# show vsg vm

VM uuid           : 421c2a2d-5e7c-3bdb-51e7-f7528163b021
VM attributes :
    name                        : centos5.3_3_vem1_clone
    vapp-name                   : apps
    os-fullname                 : red hat enterprise linux 4 (32-bit)
    tools-status                : installed
    host-name                   : 10.193.75.20
    cluster-name                : dc_dm1_clu1
```

Zone Attributes

Table 6-4 lists the zone attributes supported by the Cisco VSG.

Table 6-4   Zone Attributes

Description	Name
Zone name. This is a multi-valued attribute and can belong to multiple zones at the same time.	src.zone.name
	dst.zone.name
	zone.name[1]

1. Neutral attribute

Security Profiles

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.

This example shows how to verify the security profile on a Cisco VSG:

```
vsg_d3338(config-vnm-policy-agent)# show vsg security-profile table
--------------------------------------------------------------------------------
        Security-Profile Name            VNSP ID      Policy Name
--------------------------------------------------------------------------------
default@root                             1        default@root
sp10@root/tenant_d3338                   9        ps9@root/tenant_d3338
sp9@root/tenant_d3338                    10       ps9@root/tenant_d3338
sp2@root/tenant_d3338                    11       ps1@root/tenant_d3338
sp1@root/tenant_d3338                    12       ps1@root/tenant_d3338
```

This example shows how to verify the security profile on a Cisco VSG:

```
vsg_d3338(config-vnm-policy-agent)# show vsg security-profile
VNSP            : sp10@root/tenant_d3338
VNSP id         : 9
Policy Name     : ps9@root/tenant_d3338
Policy id       : 3
Custom attributes :
    vnsporg                     : root/tenant_d3338

VNSP            : default@root
VNSP id         : 1
Policy Name     : default@root
Policy id       : 1
```

```
Custom attributes :
    vnsporg                  : root

VNSP           : sp1@root/tenant_d3338
VNSP id        : 12
Policy Name    : ps1@root/tenant_d3338
Policy id      : 2
Custom attributes :
    vnsporg                  : root/tenant_d3338
    location                 : losangeles
    color9                   : test9
    color8                   : test8
    color7                   : test7
    color6                   : test6
    color5                   : test5
    color4                   : test4
    color3                   : test3
    color2                   : test2
    color13                  : test13
    color12                  : test12
    color11                  : test11
    color10                  : test10
    color1                   : test1
    color                    : red

VNSP           : sp2@root/tenant_d3338
VNSP id        : 11
Policy Name    : ps1@root/tenant_d3338
Policy id      : 2
Custom attributes :
    vnsporg                  : root/tenant_d3338
    location                 : sanjose
    color                    : blue

VNSP           : sp9@root/tenant_d3338
VNSP id        : 10
Policy Name    : ps9@root/tenant_d3338
Policy id      : 3
Custom attributes :
    vnsporg                  : root/tenant_d3338
```

Viewing Security Profiles and Policies on the Cisco VNMC and the Cisco VSG

The Cisco VNMC GUI provides a view of the Cisco VSG security policy objects. The policy objects shown in the Cisco VNMC GUI are not necessarily shown in the same organizational path location as they appear in the Cisco VSG CLI when you enter the **show running-config** command.

For example, in the Cisco VNMC GUI, if the virtual data center DC1 is under the tenant and the application APP1 is under DC1, the vnsp app1-sp in the APP1 level is pointing to the policy set ps1 at the DC level.

Figure 6-1 shows the Cisco VNMC GUI organization structure.

Figure 6-1   Cisco VNMC Organizational Hierarchy for a Tenant, Data Center, and Application

Tenant4

├── DC1 ◄────── ps1, p1, and r1 are placed here through the Cisco Prime NSC GUI
│
    APP1 ◄──── security-profile app1-sp is placed here through the Cisco Prime NSC GUI

239075
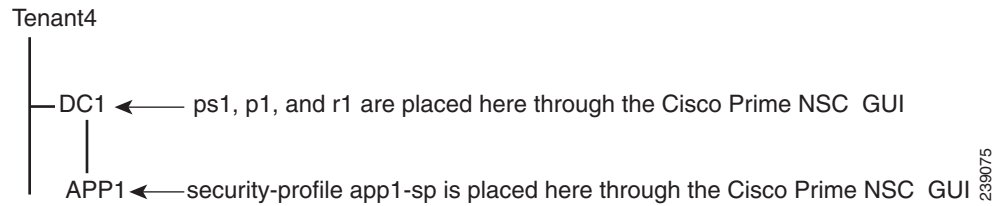
```
security-profile app1-sp@root/tenant4/DC1/APP1
  policy ps1@root/tenant4/DC1/APP1
  custom-attribute loc "sunnyvale"
  custom-attribute vnsporg "root/tenant4/dc1/app1"
```

The output of the **show running-config** command shows that the policy set and its objects are resolved from the APP1 level where the security profile is defined. The actual location of the objects in the Cisco VNMC GUI is at the DC1 level.

```
policy ps1@root/tenant4/DC1/APP1
rule p1/r1@root/tenant4/DC1/APP1 order 101
```

The policy object DNs that are shown in the Cisco VSG **show running-config** command output are shown with a DN relative to where they are resolved *from*. The policy object DNs are not where the actual policy objects are in the Cisco VNMC organizational hierarchy.

However, security profiles are shown with the DN where the actual security profile is created on the Cisco VNMC organizational hierarchy.

Policy objects are resolved upwards from where the security profile is located in the Cisco VNMC organizational hierarchy.

EXAMPLE

In the following example, the Cisco VSG is configured with the following specifications:

- The security profile (VNSP) sp1 has policy-set ps1 in which there is a policy p1 that includes a rule, r1.
- The policy-set ps1 is located at root in the organization tree on the Cisco VNMC.
- The policy p1 is located at root in the organization tree on the Cisco VNMC.
- The rule r1 is placed in the policy p1 on the Cisco VNMC (the Cisco VNMC does not allow you to create a rule object in and of itself).
- The security profile sp1 is placed in tenant_d3337/dc1 on the Cisco VNMC.

All Cisco VSGs in the tenant_d3337 have the following **show-running config** command output (this configuration is replicated to all Cisco VSGs in the leaf path):

```
security-profile sp1@root/tenant_d3337/dc1
  policy ps1@root/tenant_d3337/dc1
  custom-attribute vnsporg "root/tenant_d3337/dc1"

policy p1@root/tenant_d3337/dc1
  rule p1/r1@root/tenant_d3337/dc1 order 101
```

Note   The policy objects above do not actually exist at the DC1 level of the organization tree on the Cisco VNMC but are resolved from that location in the Cisco VNMC organization tree.

Configuring Service Firewall Logging

See "Enabling Global Policy-Engine Logging" section of *Cisco Virtual Security Gateway, Release 4.2(1)VSG1(3.1) and Cisco Virtual Network Management Center, Release 1.3 Installation and Upgrade Guide*

Verifying the Cisco VSG Configuration

To display the Cisco VSG configuration, use the **show running-config** command.

```
vsg# show running-config

!Command: show running-config
!Time: Wed Jan 26 15:39:57 2011

version 4.2(1)VSG1(1)
feature telnet
no feature http-server

username admin password 5 $1$CbPcXmpk$l31YumYWiO0X/EY1qYsFB.  role network-admin

banner motd #Nexus VSN#

ssh key rsa 2048
ip domain-lookup
ip domain-lookup
hostname vsg
snmp-server user admin auth md5 0x0b4894684d52823092c7a7c0b87a853d priv
0x0b4894684d52823092c7a7c0b87a853d localizedkey engineID 128:0:0:9:
3:0:0:0:0:0:0

vrf context management
  ip route 0.0.0.0/0 10.193.72.1
vlan 1
port-channel load-balance ethernet source-mac
port-profile default max-ports 32

vdc vsg id 1
  limit-resource vlan minimum 16 maximum 2049
  limit-resource monitor-session minimum 0 maximum 2
  limit-resource vrf minimum 16 maximum 8192
  limit-resource port-channel minimum 0 maximum 768
  limit-resource u4route-mem minimum 32 maximum 32
  limit-resource u6route-mem minimum 16 maximum 16
  limit-resource m4route-mem minimum 58 maximum 58
  limit-resource m6route-mem minimum 8 maximum 8

interface mgmt0
  ip address 10.193.73.185/21

interface data0
```

```
                    cli alias name ukickstart copy scp://user@<ip
                    address>/ws/sjc/baselard_latest/build/images/gdb/nexus-1000v-kickstart-mzg.VSG1.1.bin
                    bootflash:ukickstart
                    cli alias name udplug copy scp://user@<ip
                    address>/ws/sjc/baselard_latest/build/images/gdb/nexus-1000v-dplug-mzg.VSG1.1.bin
                    bootflash:ukickstart
                    cli alias name udplug copy scp://user@<ip
                    address>/ws/sjc/baselard_latest/build/images/gdb/nexus-1000v-dplug-mzg.VSG1.1.bin
                    bootflash:dplug
                    cli alias name uimage copy scp://user@<ip
                    address>/ws/sjc/baselard_latest/build/images/gdb/nexus-1000v-mzg.VSG1.1.bin
                    bootflash:user_bin
                    line console
                    boot kickstart bootflash:/ukickstart sup-1
                    boot system bootflash:/user_bin sup-1
                    boot kickstart bootflash:/ukickstart sup-2
                    boot system bootflash:/user_bin sup-2
                    mgmt-policy TCP permit protocol tcp
                      ha-pair id 25

                    security-profile profile1
                      policy p2

                    security-profile profile2
                      policy p1
                      custom-attribute state "texas"
                    object-group g1 net.port
                      match 1 eq 80
                      match 2 eq 443
                    zone zone1
                      condition 1 net.ip-address eq 1.1.1.1
                      condition 2 net.port eq 80
                      condition 2 net.port eq 80
                    rule r2
                      condition 1 dst.net.ip-address eq 2.2.2.2
                      condition 2 src.net.ip-address eq 1.1.1.1
                      condition 3 src.net.port eq 100
                      condition 4 dst.net.port eq 80
                      condition 5 net.protocol eq 6
                      action 1 permit
                    rule r5
                      condition 1 net.ethertype eq 0x800
                      action 1 inspect ftp
                    rule r6
                    rule r7
                    policy p2
                      rule r2 order 10
                    policy p1
                      rule r2 order 10
                    service firewall logging enable
                    vnm-policy-agent
                      registration-ip 10.193.73.190
                      shared-secret **********
                      log-level info

                    vsg#
```

Configuration Limits

Table 6-5 lists the maximum configuration limits for configuring the Cisco VSG.

Table 6-5   Maximum Configuration Limits

Feature	Maximum Limits
Zones in Cisco VSG	512 counts
Rules per policy	1024 counts
Policy set per Cisco VSG	16 counts
Object Group in Cisco VSG	512
Total number of conditions	16K
Maximum rules per Cisco VSG	1024