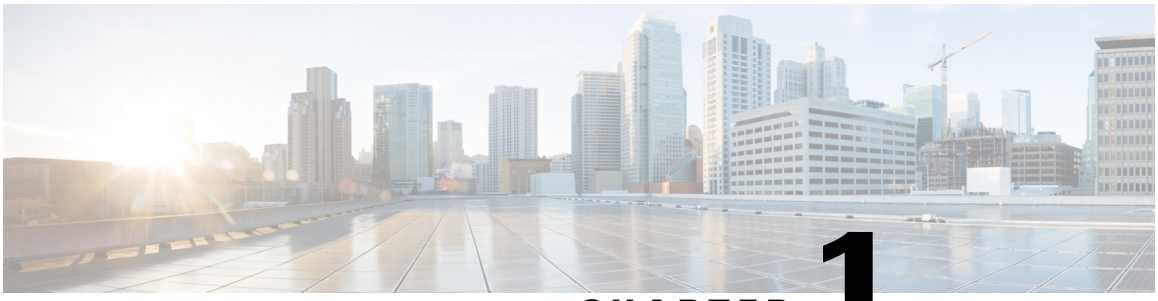
Cisco Virtual Security Gateway for KVM Configuration Guide, Release 5.2(1)VSG2(1.3)

First Published: May 26, 2015

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

Virtual Security Gateway Overview

This chapter contains the following sections:

Information About the Cisco Virtual Security Gateway

Document Conventions

Command descriptions use the following conventions:

Convention	Description
bold	Bold text indicates the commands and keywords that you enter literally as shown.
Italic	Italic text indicates arguments for which the user supplies the values.
[x]	Square brackets enclose an optional element (keyword or argument).
[x | y]	Square brackets enclosing keywords or arguments separated by a vertical bar indicate an optional choice.
{x | y}	Braces enclosing keywords or arguments separated by a vertical bar indicate a required choice.
[x {y | z}]	Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.
`variable`	Indicates a variable for which you supply values, in context where italics cannot be used.

Convention	Description
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.

Examples use the following conventions:

Convention	Description
`screen font`	Terminal sessions and information the switch displays are in screen font.
`boldface screen font`	Information 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.

Overview

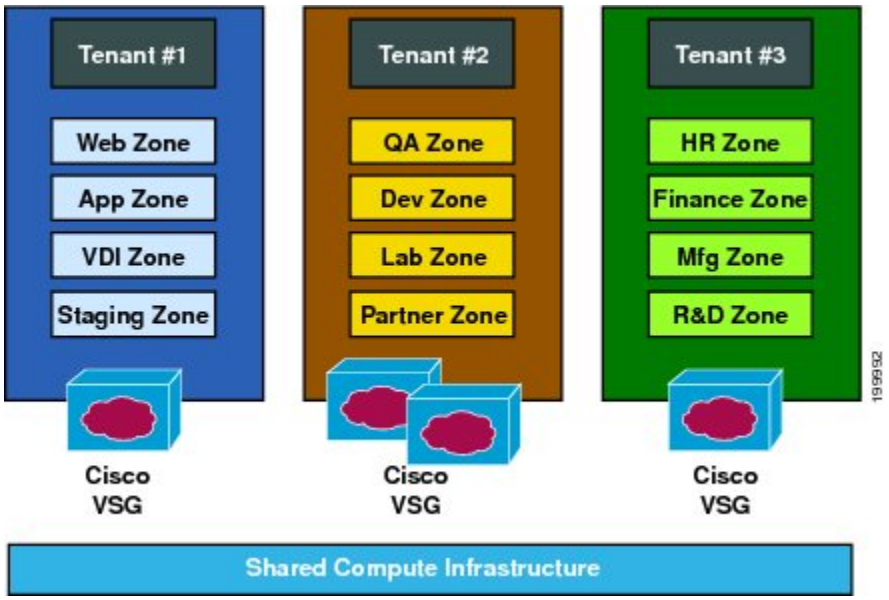
The Cisco Virtual Security Gateway (VSG) is a virtual firewall appliance that provides trusted access to virtual data center and cloud environments. The Cisco VSG enables a broad set of multi-tenant workloads that have varied security profiles to share a common compute infrastructure in a virtual data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

Integrated with either the Cisco Nexus 1000V Series switch or the Cisco Cloud Service Platform and running on the Cisco NX-OS operating system, the Cisco VSG provides the following benefits:

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

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

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



The Cisco VSG does the following:

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

VSG Models

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

Table 1: VSG Models

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

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

Product Architecture

The Cisco VSG operates with the Cisco Nexus 1000V in the KVM, and the Cisco VSG leverages the virtual network service datapath (Cisco vPath) that is embedded in the Cisco Nexus 1000V compute node.

Cisco vPath steers traffic, whether external to VM or VM to VM, to the Cisco VSG of a tenant. Initial packet processing occurs in the Cisco VSG for policy evaluation and enforcement. After the policy decision is made, the Cisco VSG off-loads the policy enforcement of remaining packets to Cisco vPath. Cisco vPath supports the following features:

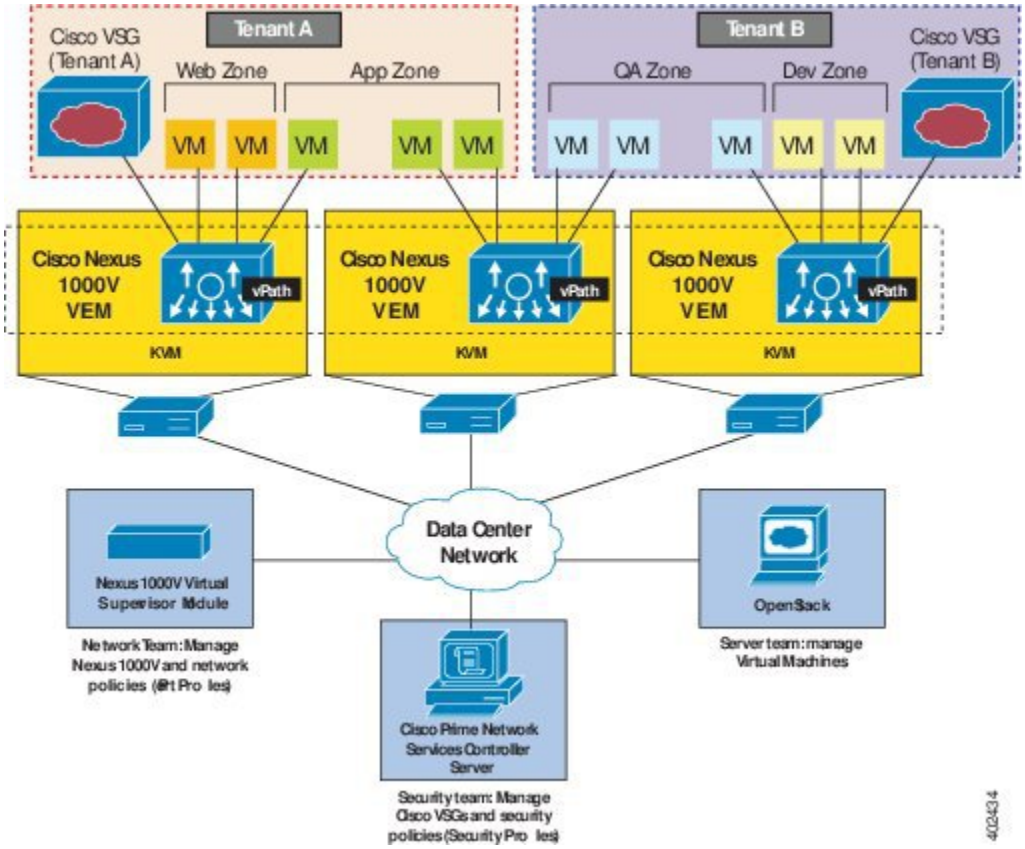
- Intelligent interception and redirection—Tenant-aware flow classification and subsequent redirection to a designated Cisco VSG tenant
- Fast-path off-load—Per-tenant policy enforcement of flows off-loaded by the Cisco VSG to Cisco vPath

The Cisco VSG and Cisco Nexus 1000V compute node provide the following benefits:

- Efficient deployment—Each Cisco VSG can protect access and traffic across multiple physical servers, which eliminates the need to deploy one virtual appliance per physical server.
- Performance optimization—By off-loading fast-path to one or more Cisco Nexus 1000V compute node vPath modules, the Cisco VSG enhances network performance through distributed vPath-based enforcement.
- Operational simplicity—The Cisco VSG can be transparently inserted in one-arm mode without creating multiple switches or temporarily migrating VMs to different switches or servers. Zone scaling is based on a security profile, not on vNICs that are limited for the virtual appliance. Zone scaling simplifies physical server upgrades without compromising security and incurring application outage.
- High availability—For each tenant, the Cisco VSG can be deployed in an active-standby mode to ensure a highly available operating environment, with vPath redirecting packets to the standby Cisco VSG when the primary Cisco VSG is unavailable.
- Independent capacity planning—The Cisco VSG can be placed on a dedicated server that is controlled by the security operations team so that maximum compute capacity can be allocated to application

workloads. Capacity planning can occur independently across server and security teams, and operational segregation across security, network, and server teams can be maintained.

Figure 2: Cisco Virtual Security Gateway Deployment Topology



Fast Path Connection Timeouts

When a compute node sees a packet for a protected VM for the first time, the compute node redirects the packet to the Cisco VSG to determine what action needs to be taken (for example, permit, drop, or reset). After the decision is made, both the Cisco VSG and compute node save the connection information and the action for a period of time. During this time, packets for this connection follow the same action without any extra policy lookup. This connection is a connection in a fast path mode. Depending on the traffic and the action, the amount of time that a connection stays in the fast path mode varies. The following table provides the timeout details for the connections in the fast path mode.

Table 2: Fast Path Connection Timeouts

Protocol	Connection State	Time Out
TCP	Close with FIN and ACKACK	Compute Node—4 secs
		VSG—4 secs
	Close with RST	Compute Node—4 secs
		VSG—4 secs
	Action drop	Compute Node—4 secs
		VSG—4 secs
	Action reset	Compute Node—4 secs
		VSG—4 secs
	Idle	Compute Node—36–60 secs
		VSG—630–930 secs
UDP	Action drop	Compute Node—4 secs
		VSG—4 secs
	Action reset	Compute Node—4 secs
		VSG—4 secs
	Idle	Compute Node—8–12 secs
		VSG—240–360 secs
	Destination Unreachable	Compute Node—4 secs
		VSG—4 secs

Protocol	Connection State	Time Out
L3/ICMP	Action drop	Compute Node—2 secs
		VSG—2 secs
	Action reset	Compute Node—2 secs
		VSG—2 secs
	Idle	Compute Node—8–12 secs
		VSG—16–24 secs

Trusted Multitenant Access

You can transparently insert a Cisco VSG into the KVM environment where the Cisco Nexus 1000V distributed virtual switch is deployed. One or more instances of the Cisco VSG is deployed on a per-tenant basis, which allows a high scale-out deployment across many tenants. Tenants are isolated from each other, so no traffic can cross tenant boundaries. You can deploy the Cisco VSG at the tenant level, at the virtual data center level, and at the vApp level.

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

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

Dynamic (Virtualization-Aware) Operation

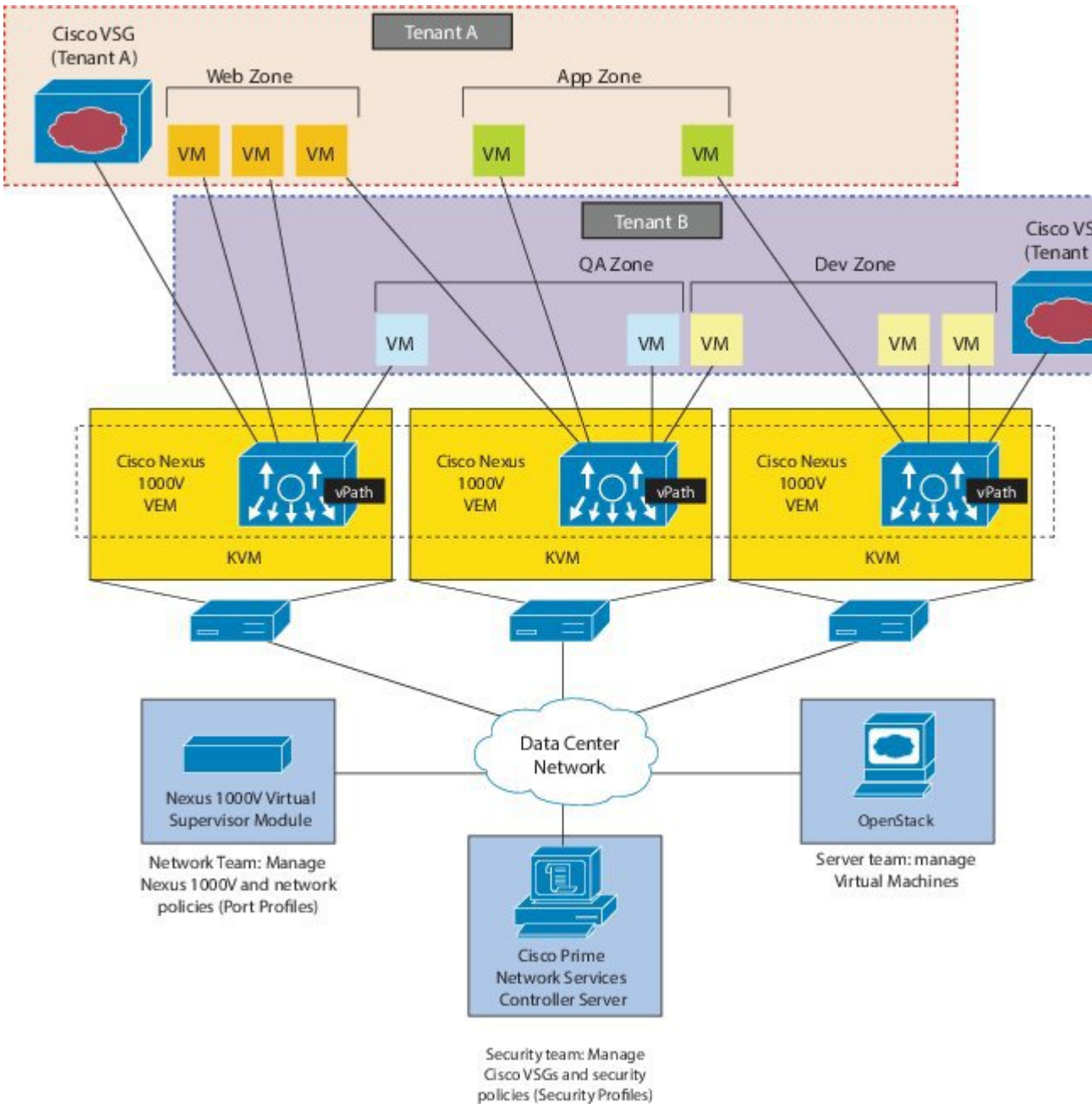
A virtualization environment is dynamic, where frequent additions, deletions, and changes occur across tenants and across VMs. Additionally, live migration of VMs can occur due to manual or programmatic VMotion events. The following figure shows how a structured environment can change over time due to this dynamic VM environment.

The Cisco VSG operating with the Cisco Nexus 1000V (and vPath) supports a dynamic VM environment. Typically, when you create a tenant on the Cisco Prime Network Services Controller (Prime NSC) with the Cisco VSG (standalone or active-standby pair), associated security profiles are defined that include trust zone definitions and access control rules. Each security profile is bound to a Cisco Nexus 1000V port profile (authored on the Cisco Nexus 1000V Virtual Supervisor Module [VSM] and published to the OpenStack dashboard). 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.

When VMotion events are triggered, VMs move across physical servers. Because the Cisco Nexus 1000V ensures that port profile policies follow the VMs, associated security profiles also follow these moving VMs, and security enforcement and monitoring remain transparent to VMotion events.

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



Cisco VSG Deployment Scenarios

The current release supports the Cisco VSG deployment in the Layer 3 mode. The compute node and the Cisco VSG communicate with each other through a special virtual network interface called the Virtual Kernel NIC (vmknic). This vmknic is created by an administrator.

Compute Node Interface for a Cisco VSG in the Layer 3 Mode

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

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-vservice** command in it. For more details, see the *Cisco Nexus 1000V System Management Configuration Guide*.

To configure the vmknic interface that the compute node uses, you can assign a port profile by using the **capability l3-vservice** command in the port-profile configuration.

To carry the Cisco VSG in the Layer 3 mode traffic over multiple uplinks (or subgroups) in server configurations where vPC-HM MAC-pinning is required, you can configure up to four vmknic.

The traffic in the Layer 3 mode that is sourced by local vEthernet interfaces and needs to be redirected to the Cisco VSG is distributed between these vmknic based on the source MAC addresses in their frames. The compute node automatically pins the multiple vmknic in the Layer 3 mode to separate uplinks. If an uplink fails, the compute node automatically repins 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 compute node does not use the KVM 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.

Cisco vPath

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

Cisco VSG Network Virtual Service

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

Cisco Virtual Security Gateway Configuration for the Network

Setting Up Cisco VSGs in Layer 2 Mode

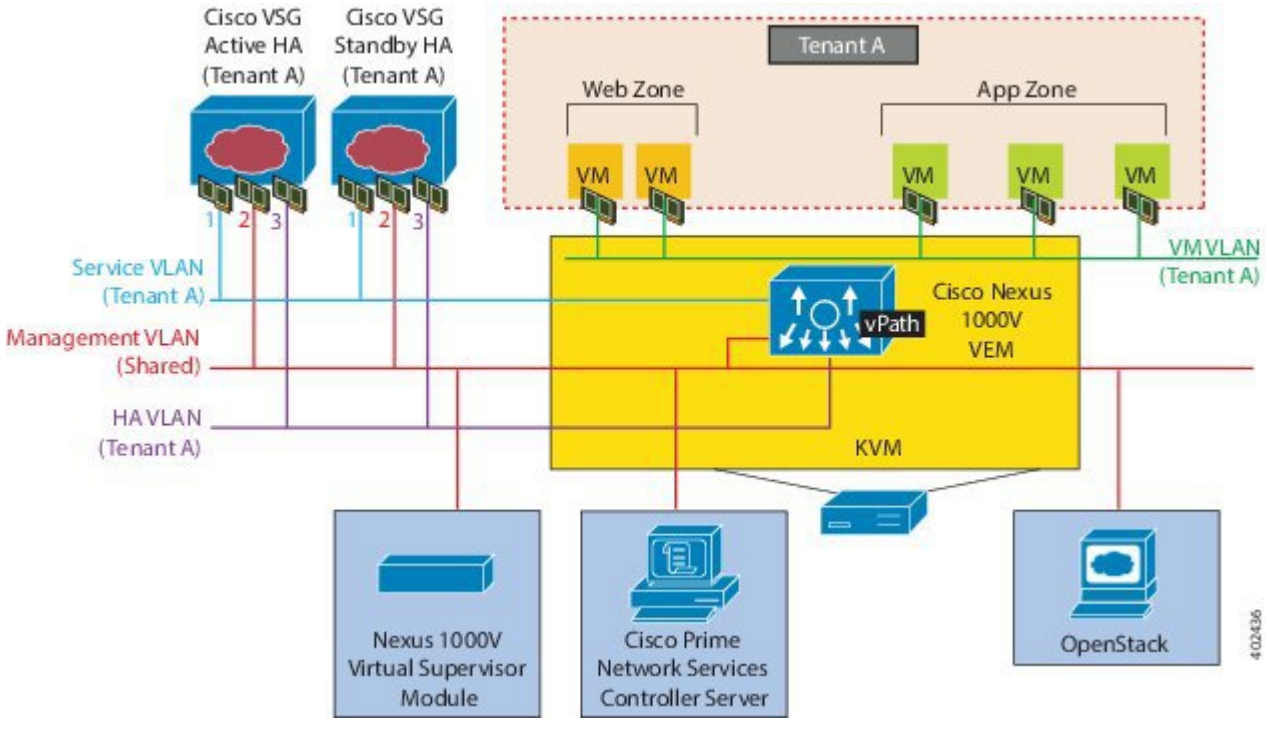
The Cisco VSG is set up so that VMs can reach a Cisco VSG irrespective of its location. The Cisco vPath component in the Cisco Nexus 1000V compute node intercepts the packets from the VM and sends them to the Cisco VSG for further processing.

The following figure 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 Cisco Prime Network Services Controller (PNSC), the Cisco Nexus 1000V VSM, and the managed Cisco VSGs.
- The Service VLAN provides communications between the Cisco Nexus 1000V compute node and Cisco VSGs. All the Cisco VSGs are part of the Service VLAN and the compute node uses this VLAN for its interaction with Cisco VSGs.
- The HA VLAN is used for the HA heartbeat mechanism and identifies the master-slave relationship.

You can allocate one or more VM Data VLAN(s) for VM-to-VM communications. In a multi-tenant environment, the Management VLAN is shared among all the tenants, and the Service VLAN, HA VLAN, and VM Data VLAN are allocated per tenant. However, when VLAN resources become scarce, you might decide to use a single VLAN for Service and HA functions.

Figure 4: Cisco Virtual Security Gateway VLAN Usages



Cisco VSG Configuration Overview

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

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

Cisco Nexus 1000V Series Switch VSM

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

Port Profile

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

The virtual Ethernet or Ethernet interfaces are assigned in the KVM Server to a port profile for the following functions:

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

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

Virtual Security Gateway

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

Security Profile

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

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

Firewall Policy

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

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

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

- Object Groups
- Zones
- Rules
- Actions

Object Groups

An object group is a set of conditions relevant to an attribute. Because 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 , such as VM attributes. 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 a zone should not have a directional sense and must be neutral.

Rules

Firewall rules can consist of multiple conditions and actions. Rules can be defined in a policy as a condition for filtering the traffic. The policy engine uses the policy as a configuration that filters the network traffic that is received on the . The policy engine uses two types of condition matching models for filtering the network traffic:

AND Model: A rule is set to matched when all the attributes in a rule match.

OR model: The attributes are classified into five different types of columns. For a rule to be true, at least one condition in each column must be true. The five columns in an OR model are:

- Source column: Attribute to identify source host.
- Destination column: Attribute to identify destination host.
- Service column: Attribute to identify service at the destination host.
- Ether type column: Attribute to identify link level protocol.
- Source port column: Attribute to identify source port.

Actions

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

- Permit
- Drop
- Reset
- Log
- Inspection

Service Firewall Logging

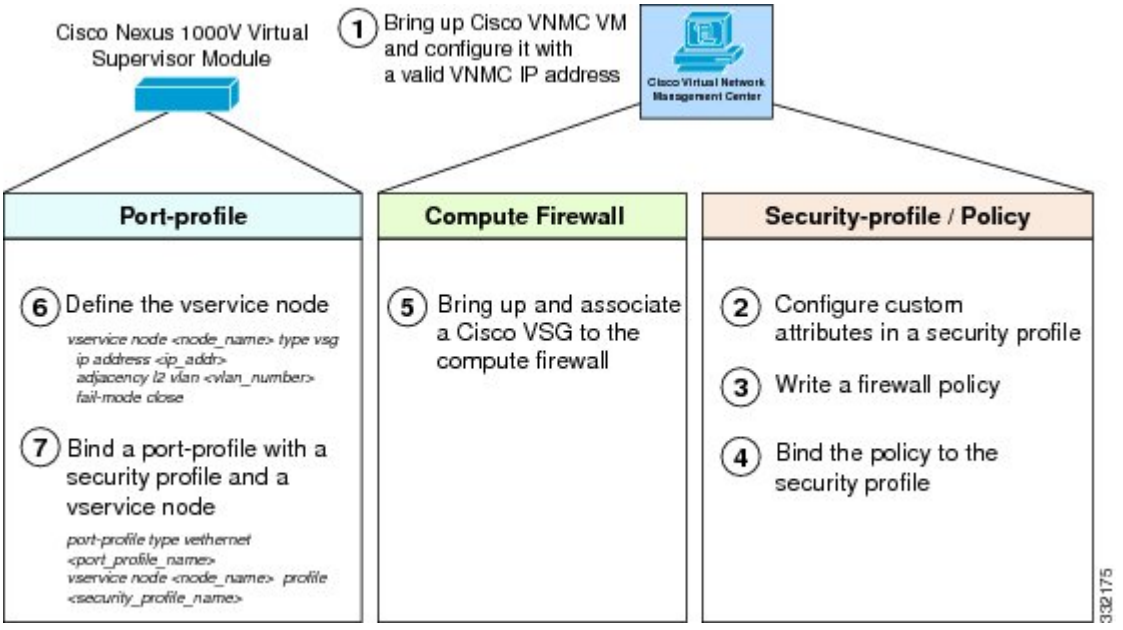
The service firewall log is a tool to test and debug the policy. During a policy evaluation, the policy engine displays the policy results of a policy evaluation. Both the users and the policy writer benefit from this tool when troubleshooting a policy.

Sequence in Configuring a Cisco VSG in the Layer 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:

1. Install and set up a Cisco Prime Network Services Controller (PNSC) service VM and configure the Cisco NSC with a valid IP address.
2. If you plan to use custom attributes in the firewall policy, create a set of custom attributes in a security profile configuration on the Cisco PNSC.
3. Write a firewall policy on the Cisco PNSC 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 PNSC. 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 PNSC.
6. Define the vservice node.
7. After the security profile and firewall policy are fully configured, you can bind the security profile and the service nodes with the VM port profiles that demand access protection provided by the Cisco VSG through the port profile management interface on the VSM.

Figure 5: Cisco Virtual Security Gateway Layer 2 Configuration Flow



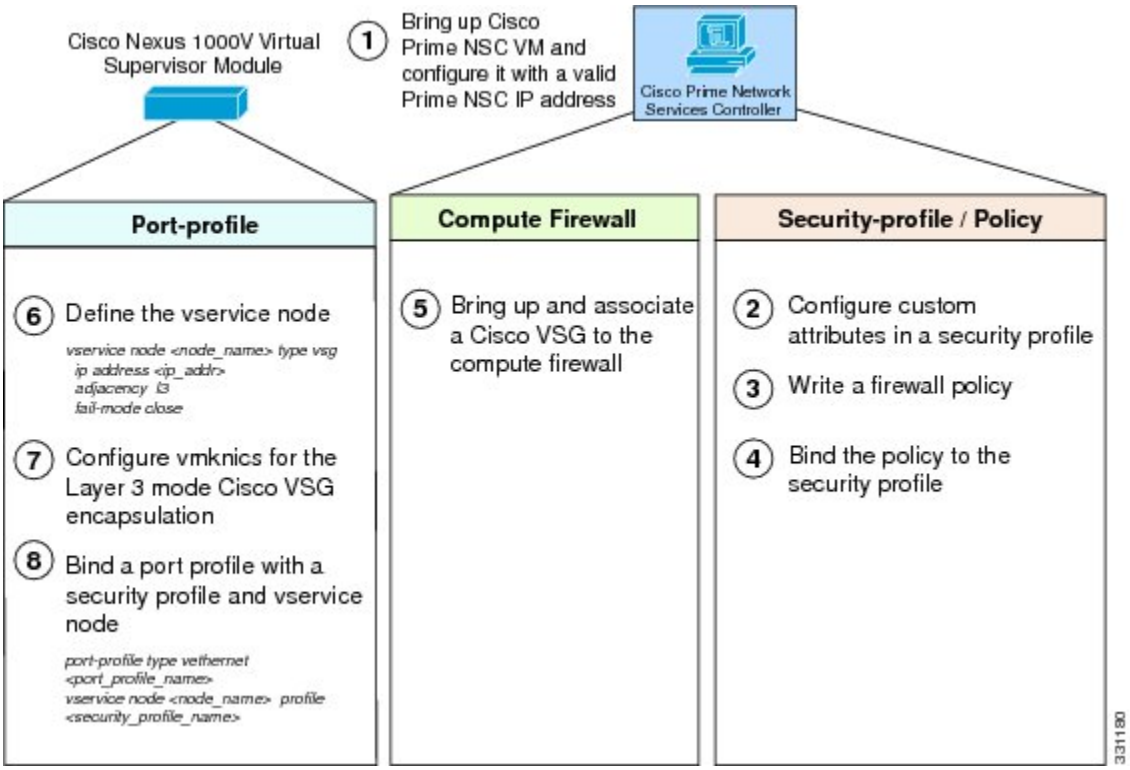
Sequence in Configuring a Cisco VSG in the Layer 3 Mode

Before configuring a Cisco VSG in Layer 3 mode, create a Layer 3 vmknic.

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

1. Install and set up a Cisco PNSC service VM and configure the Cisco PNSC 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 PNSC.
3. Write a firewall policy on the Cisco PNSC by using appropriate policy objects such as object groups, zones, rules, conditions, actions, and policies.
4. After the firewall policy is created, bind the policy to the security profile that was previously created on the Cisco PNSC.
5. Bring up a Cisco VSG and associate it to the appropriate compute firewall on the Cisco PNSC.
6. Configure the vmknic for the Layer 3 mode Cisco VSG encapsulation.
7. Configure VSG and virtual network adapter in same VLAN/network.
8. Define the vservice node.
9. After the security profile and firewall policy are fully configured, you can bind the security profile and the service node with the VM port profiles that demand access protection provided by the Cisco VSG through the port profile management interface on the VSM.

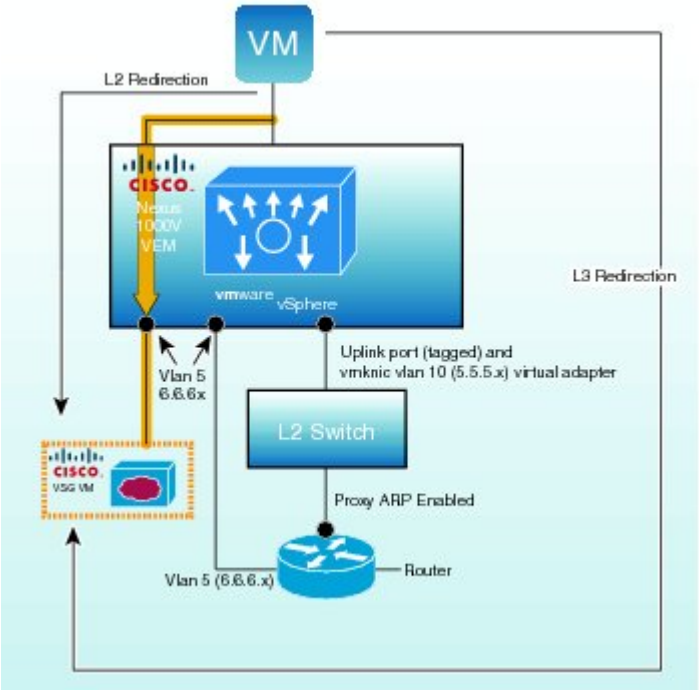
Figure 6: Cisco Virtual Security Gateway Layer 3 Configuration Flow



Layer 2 Mode to Layer 3 Mode Migration

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

Figure 7: Cisco VSG Deployment Migration from Layer 2 Mode to Layer 3 Mode



Migrating 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 4.2(1)SV2(1.1) VSM/Compute Node.

Step 1 Add Layer 3 vmknics on all compute nodes (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 with the vmknic.
d) Change the existing Layer 2 mode port profile to support Layer 3 mode or create a new Layer 3 mode port profile for each compute node host.

Step 2 Verify Layer 3 vmknic connectivity between the compute node to compute node and the compute node to Cisco VSG:

a) Perform a compute node-to-compute node vmkping from each compute node to its peers.

Example:

```
[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 compute node to the Cisco VSG connectivity.

Example:

```
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 Change the existing Layer 2 mode port profile to support Layer 3 mode or create a new Layer 3 mode port profile for each compute node host. 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. Changing the existing Layer 2 mode port profile operation has more traffic disruptions than creating a new Layer 3 mode port profile.

- 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, enter the **no vservice** command to remove the existing Layer 2 vservice configuration.
  2. Create the vservice node.

     ```
     vservice node node_name type vsg
       ip address ip_addr
       adjacency l3
     ```

     This example shows how to configure the new vservice:

     ```
     vservice node vsg1 type vsg
       ip address 106.1.1.1
       adjacency l3
     ```

  3. Bind the vservice node to the port profile.

     ```
     port-profile type vethernet vsg-profile
       switchport mode access
       switchport access vlan 1453------> access vlan for traffic VM
       vservice node vsg1 profile SP2 ----> service policy name
       org root/T2 --------> org structure
       no shutdown
       guid 26f1b883-0905-4c31-8096-cfb8330228b5
     ```

```
state enabled
publish port-profile
```

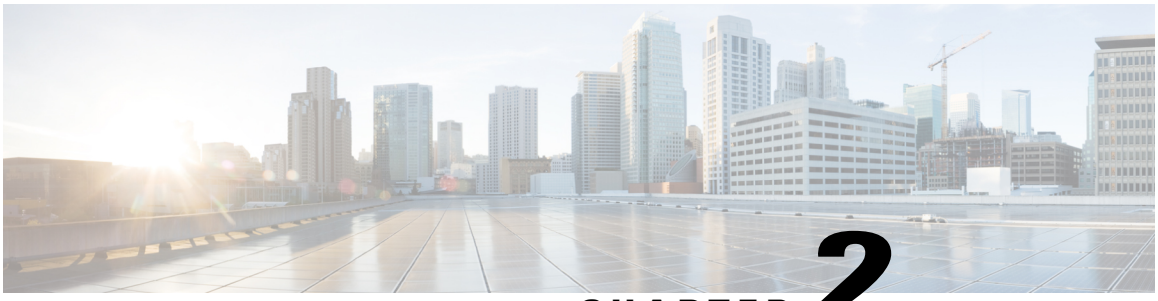
Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to vsg-docfeedback@cisco.com. We appreciate your feedback.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*, at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.



CHAPTER 2

Using the Command-Line Interface

This chapter contains the following sections:

Information About the CLI Prompt

To access , you can SSH into the management IP. After you have successfully accessed the system, the CLI prompt displays in the terminal window of remote workstation, as follows:

```
#
```

Note Use **show host name** command to display the existing hostname of the switch.

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

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.

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	Example
exit	Exits from the current configuration command mode and returns to the previous configuration command mode.	
end	Exits from the configuration command mode and returns to EXEC mode.	

Command	Purpose	Example
Ctrl-Z	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 3: Command Mode Summary

Mode	Access Method	Prompt	Exit Method
EXEC	From the login prompt, enter your username and password.		To exit to the login prompt, use the **exit** command.
Zone configuration	From global configuration mode, enter the **zone** *zone-name* command.		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 **interface data0** command.		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

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:

```
vsg(config)#copy running-config startup-config
```

Special Characters

The following table lists the characters that have special meaning in text strings and should be used only in regular expressions or other special contexts.

Table 4: Special Characters

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

Keystroke Shortcuts

The following lists command key combinations that can be used in both EXEC and configuration modes.

Key(s)	Description
Ctrl-A	Moves the cursor to the beginning of the line.

Key(s)	Description
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.
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.

Key(s)	Description
UP arrow key	Displays the previous command in the command history.
Down arrow key	Displays the next command in the command history.
Right arrow key and Left arrow key	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:
	`firewall(config)# xm<Tab>`
	`firewall(config)# xml <Tab>`
	`firewall(config)# xml server`
	This example shows how to use the tab keystroke:
	`firewall(config)# ns<Tab>`
	`nsc-policy-agent vns-binding`
	`firewall(config)# security-pr<Tab>`
	`firewall(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.

The following table lists examples of command abbreviations.

Table 5: Examples of Command Abbreviations

Command	Abbreviation
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 reenable 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.

Table 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.
UP arrow key	Use the UP arrow to have the CLI display the previous command you entered so that you can correct an error.

Syntax Error Isolation and Context-Sensitive Help

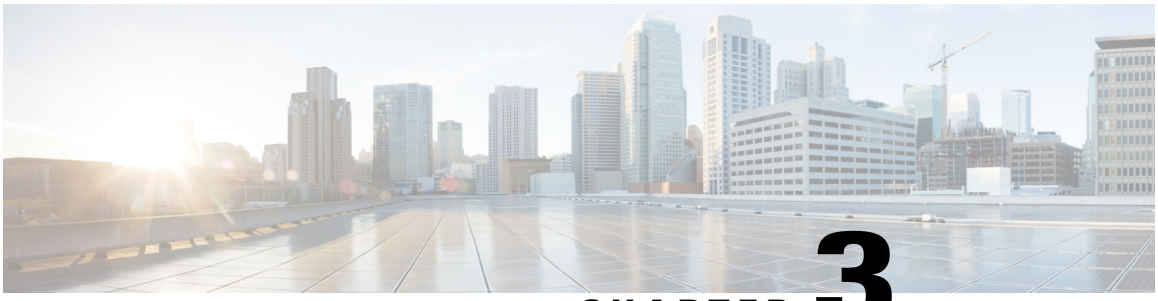
The following table describes the commands for syntax error isolation and context-sensitive help.

Command	Purpose
show interface ?	Displays the optional parameters used with the **show interface** command in EXEC mode.
show interface module ?	Displays an invalid command error message and points (^) to the syntax error.

Command	Purpose
Ctrl-P or the Up Arrow	Displays the previous command you entered so that you can correct the error.
show interface data ?	Displays the syntax for showing a data interface (data0).
show interface data0	Displays the data interface (data0).

This example shows how to use syntax error isolation and context-sensitive help.

```
firewall-40# show interface data 0
data0 Link encap:Ethernet HWaddr 3a:00:02:00:00:0a
inet addr:70.10.10.10 Bcast:70.10.10.255 Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1352 Metric:1
RX packets:2258 errors:0 dropped:0 overruns:0 frame:0
TX packets:2255 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:165730 (165.7 KB) TX bytes:211984 (211.9 KB)
firewall-40#
```



CHAPTER 3

Configuring System Management

This chapter contains the following sections:

Information About Cisco VSG System Management

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, log in to the CLI in global configuration mode.

SUMMARY STEPS

1. vsg# **configure**
2. vsg(config)# **hostname** *host-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	vsg# **configure**	Places you in global configuration mode.
Step 2	vsg(config)# **hostname** *host-name*	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
```

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, log in to the CLI in configuration mode.

SUMMARY STEPS

1. vsg# **configure**
2. vsg(config)# **banner motd** [*delimiting-character message delimiting-character*]
3. vsg(config)# **show banner motd**

DETAILED STEPS

	Command or Action	Purpose
Step 1	vsg# **configure**	Places you in global configuration mode.
Step 2	vsg(config)# **banner motd** [*delimiting-character message delimiting-character*]	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	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
```

Verifying the Cisco VSG Configuration

To verify the Cisco VSG configuration, enter the following commands:

Command	Purpose
vsg# **show version**	Displays the versions of system software and hardware that are currently running on Cisco VSG.
vsg# **show running-config**	Displays the versions of system software and hardware that are currently running on Cisco VSG.
vsg# **show running-config diff**	Displays the difference between the startup configuration and the running configuration.

Example of show version

```
vsg# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2014, 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.
kickstart: version 5.2(1)VSG2(1) [build 5.2(1)VSG2(1.398)]
system: version 5.2(1)VSG2(1) [build 5.2(1)VSG2(1.398)]
kickstart image file is: [not present on supervisor]
kickstart compile time: 07/12/2014 17:00:00
system image file is: bootflash:/nexus-1000v-mz.VSG2.1.298.bin
system compile time: 07/17/2014 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
```

Example of show running-config

```
vsg# show running-config
!Command: show running-config
!Time: Sun Jul 17 17:42:59 2014
version 5.2(1)VSG2(1.2)
no feature telnet
no feature http-server
username adminbackup password 5 $1$Oip/C5Ci$oOdx7oJSlBCFpNRmQK4na. role network-operator
username admin password 5 $1$RU5OIPU7$SYvoK9S5rOMRE9WBWZLsA. role network-admin
username vsnbetauser password 5 $1$Fg4u8MCf$xr8cSVV1gBb0ATZU8eVbB. 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
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
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.VSG2.1.2.bin sup-1
boot system bootflash:/nexus-1000v-mzg.VSG1.0.1.bin sup-1
boot kickstart bootflash:/nexus-1000v-kickstart-mzg.VSG2.1.2.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
nsc-policy-agent
policy-agent-image
registration-ip 0.0.0.0
shared-secret **********
log-level info
```

Example of show running-config diff

```
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
```

Displaying Interface Configurations

To display interface configurations, enter the following commands:

Command	Purpose
vsg# **show interface mgmt**	Displays a detailed information for a specific interface.
vsg# **show interface brief**	Displays a brief view of all interfaces.
vsg# **show running-config interface**	Displays the running configuration for all interfaces on your system.

Example of show interface

```
vsg# show interface mgmt 0
mgmt0 is up
  Hardware: Ethernet, address: 3a00.0100.000b (bia 3a00.0100.000b)
  Internet Address is 10.37.29.3/16
  MTU 1352 bytes, BW 1000000 Kbit, DLY 10 usec
  reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA
  auto-duplex, auto-speed
  Auto-Negotiation is turned on
  1 minute input rate 2672 bits/sec, 3 packets/sec
  1 minute output rate 1152 bits/sec, 1 packets/sec
  Rx
    2349928 input packets 106216 unicast packets 351159 multicast packets
    1892553 broadcast packets 182855323 bytes
  Tx
    52446 output packets 18796 unicast packets 16849 multicast packets
    16801 broadcast packets 6126844 bytes

firewall-1#
```

Example of show interface brief

```
firewall# show interface brief

--------------------------------------------------------------------------------
Port     VRF          Status IP Address                              Speed    MTU
--------------------------------------------------------------------------------
mgmt0    --           up     10.37.29.3                              --       1352

--------------------------------------------------------------------------------
Port     VRF          Status IP Address                              Speed    MTU
--------------------------------------------------------------------------------
data0 --           up     41.10.10.20                             --       9000
```

```
NOTE : * Denotes ports on modules which are currently offline on VSM
firewall#
```

Example of show running-config interface

```
vsg# show running-config interface

!Command: show running-config interface
!Time: Mon Sep 29 02:17:32 2014

version 5.2(1)VSG2(1.1)

interface mgmt0
  ip address 10.37.29.3/16

interface data0
  no snmp trap link-status
  ip address 14.10.10.20/24

firewall-1#
```

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 be logged in to the CLI in any command mode.

SUMMARY STEPS

1. vsg(config)# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	vsg(config)# **copy running-config startup-config**	Saves the running configuration to the startup configuration.

This example shows how to save a configuration.

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

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:
  - debug—Erases the debug configuration.

SUMMARY STEPS

1. vsg(config)# **write erase [debug]**

DETAILED STEPS

	Command or Action	Purpose
Step 1	vsg(config)# **write erase [debug]**	Erases the existing startup configuration and reverts all settings to their factory defaults. The running configuration is not affected.

This is an example of write erase command:

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

Displaying Intercloud Fabric Firewall Instance

You can display Intercloud Fabric(ICF) Firewall(VSG) instance.

Before You Begin

Before beginning this procedure, you must be logged in to the CLI.

SUMMARY STEPS

1. vsg# **show vsg**

DETAILED STEPS

	Command or Action	Purpose
Step 1	vsg# **show vsg**	Displays the ICF VSG model, software version and build, and the Prime Network Services Controller (PNSC) IP address.

This example shows how to display the ICF VSG model and software version and build, and the PNSC IP address:

```
firewall(config)# show vsg
Model: VSG
VSG software version: 5.2(1)VSG2(1.2) build [5.2(1)VSG2(1.2)]
NSC IP: 10.2.65.213
NSC PA version: 2.1(2a)-vsg
```

Navigating the File System

Specifying File Systems

The syntax for specifying a file system is <file system name>:[//server/].

Table 7: 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 be logged in to the CLI.

SUMMARY STEPS

1. firewall# **pwd**

DETAILED STEPS

	Command or Action	Purpose
Step 1	firewall# **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 Intercloud Fabric VSG CLI:

```
firewall# 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. vsg# **pwd**
2. vsg# **cd** *directory_name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	vsg# **pwd**	Displays the directory name of your current CLI location.
Step 2	vsg# **cd** *directory_name*	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:
```

Listing the Files in a File System

You can display the contents of a directory or file.

Before You Begin

Log in to the CLI in any command mode.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	firewall# **dir**[*directory* | *filename*]	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:

```
firewall# dir lost+found/
49241 Jan 11 09:30:00 2015 diagclient_log.2613
12861 Jan 11 09:33:04 2015 diagmgr_log.2580
31 Jan 11 09:35:21 2015 dmesg
1811 Jan 11 09:38:46 2015 example_test.2633
89 Jan 11 09:40:10 2015 libdiag.2633
42136 Jan 11 09:40:55 2015 messages
65 Jan 11 09:43:50 2015 otm.log
741 Jan 11 09:48:23 2015 sal.log
87 Jan 11 09:50:43 2015 startupdebug
Usage for log://sup-local
51408896 bytes used
158306304 bytes free
209715200 bytes total
```

Identifying Available File Systems for Copying Files

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

Before You Begin

Log in to the CLI in EXEC mode.

SUMMARY STEPS

1. vsg# **copy ?**
2. vsg# **copy filename ?**

DETAILED STEPS

	Command or Action	Purpose
Step 1	vsg# **copy ?**	Displays the source file systems available to the copy command.
Step 2	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 and how to display the destination file systems available to the copy command for the specified file name:

```
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

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.

Note Before using this procedure, you must be logged in to the CLI in EXEC mode.

Command	Purpose
vsg# **show file** *filesystem name: partial filename* <TAB>	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.
vsg# **show file** *bootflash:c* <TAB>	Completes the filename for you.

This example shows how to display a selection of available files when you press the Tab key 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.VSG2.1.2a.bin
bootflash:nexus-1000v-kickstart-mzg.VSG2.1.2a.bin
bootflash:nexus-1000v-mzg.VSG2.1.2a.bin
bootflash:nexus-1000v-mzg.VSG2.1.2a.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-----
MIICXgIBAAKBgQDSq93BrlHcg3bX1jXDMY5c9+yZSST3VhuQBqogvCPDGeLecA+j
...
...
```

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.
- 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. firewall# **copy** [*source filesystem:*] *filename* [*destination filesystem:*] *filename*

DETAILED STEPS

	Command or Action	Purpose
Step 1	firewall# **copy** [*source filesystem:*] *filename* [*destination filesystem:*] *filename*	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:

```
firewall# 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 successful
```

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 be logged in to the CLI in any command mode.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	firewall# **mkdir** {**bootflash:**	**debug:**	**volatile:**} *directory-name*	Creates a directory at the current directory level.

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

```
firewall# mkdir bootflash:test
```

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 valid only on flash file systems.
- Before you can remove it, the directory must be empty.

SUMMARY STEPS

1. firewall# **rmdir** {**bootflash:** | **debug:** | **volatile:**} *directory_name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	firewall# **rmdir** {**bootflash:** | **debug:** | **volatile:**} *directory_name*	Removes a directory as long as the directory is empty.

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

```
firewall# rmdir bootflash:test
```

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. firewall# **move** {*source_path_and_filename*} {*destination_path_and_filename*}

DETAILED STEPS

	Command or Action	Purpose
Step 1	firewall# **move** {*source_path_and_filename*} {*destination_path_and_filename*}	Moves a file from the source directory to the destination directory.

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

```
firewall# move bootflash:samplefile bootflash:mystorage/samplefile
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. firewall# **delete** [**bootflash:** | **debug:** | **log:** | **volatile:**] *filename* | *directory_name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	firewall# **delete** [**bootflash:**	**debug:**	**log:**	**volatile:**] *filename*	*directory_name*	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 and how to delete a named directory and its content:

```
firewall# delete bootflash:dns_config.cfg
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 be logged in to the CLI.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	firewall# **show** *command* **>** [*path*] *filename*	Directs show command output to a file.
Step 2	firewall# **dir**	Displays the contents of the current directory, including the new file created in the first step.
Step 3	firewall# **gzip** [*path*] *filename*	Compresses the specified file.

This example shows how to compress a specified file:

```
firewall# show system internal sysmgr event-history errors > errorsfile
firewall# dir
1480264 Jan 03 08:38:21 2015 1
77824 Jan 08 11:17:45 2015 accounting.log
4096 Jan 30 14:35:15 2015 core/
3220 Jan 09 16:33:05 2015 errorsfile
4096 Jan 30 14:35:15 2015 log/
16384 Jan 03 08:32:09 2015 lost+found/
7456 Jan 08 11:17:41 2015 mts.log
1480264 Jan 03 08:33:27 2015 nexus-1000v-dplug-mzg.VSG2.1.2a.bin
20126720 Jan 03 08:33:27 2015 nexus-1000v-kickstart-mzg.VSG2.1.2a.bin
45985810 Jan 01 14:30:00 2015 nexus-1000v-mzg.VSG2.1.2a.bin
46095447 Jan 07 11:32:00 2015 nexus-1000v-mzg.VSG2.1.2a.bin
1714 Jan 08 11:17:33 2015 system.cfg.new
4096 Jan 03 08:33:54 2015 vdc_2/
4096 Jan 03 08:33:54 2015 vdc_3/
4096 Jan 03 08:33:54 2015 vdc_4/
Usage for bootflash://
631246848 bytes used
5772722176 bytes free
6403969024 bytes total

firewall# gzip bootflash:errorsfile
firewall# dir
1480264 Jan 03 08:38:21 2015 1
77824 Jan 08 11:17:45 2015 accounting.log
4096 Jan 30 14:35:15 2015 core/
861 Jan 09 16:33:05 2015 errorsfile.gz
4096 Jan 30 14:35:15 2015 log/
16384 Jan 03 08:32:09 2015 lost+found/
7456 Jan 08 11:17:41 2015 mts.log
1480264 Jan 03 08:33:27 2015 nexus-1000v-dplug-mzg.VSG1.0.1.bin
20126720 Jan 03 08:33:27 2015 nexus-1000v-kickstart-mzg.VSG1.0.1.bin
45985810 Jan 01 14:30:00 2015 nexus-1000v-mzg.VSG1.0.1.bin
46095447 Jan 07 11:32:00 2015 nexus-1000v-mzg.VSG1.0.396.bin
1714 Jan 08 11:17:33 2015 system.cfg.new
4096 Jan 03 08:33:54 2015 vdc_2/
```

```
4096 Jan 03 08:33:54 2015 vdc_3/
4096 Jan 03 08:33:54 2015 vdc_4/
Usage for bootflash://
631246848 bytes used
5772722176 bytes free
6403969024 bytes total
```

Uncompressing Files

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

Before You Begin

Before beginning this procedure, you must be logged in to the CLI.

SUMMARY STEPS

1. firewall# **gunzip** [*path*] *filename*
2. firewall# **dir**

DETAILED STEPS

	Command or Action	Purpose
Step 1	firewall# **gunzip** [*path*] *filename*	Uncompresses the specified file.
Step 2	firewall# **dir**	Displays the contents of a directory, including the newly uncompressed file.

This example shows how to uncompress a specified file:

```
firewall# gunzip bootflash:errorsfile.gz
firewall# dir bootflash:
1480264 Jan 03 08:38:21 2015 1
77824 Jan 08 11:17:45 2015 accounting.log
4096 Jan 30 14:35:15 2015 core/
3220 Jan 09 16:33:05 2015 errorsfile
4096 Jan 30 14:35:15 2015 log/
16384 Jan 03 08:32:09 2015 lost+found/
7456 Jan 08 11:17:41 2015 mts.log
1480264 Jan 03 08:33:27 2015 nexus-1000v-dplug-mzg.VSG2.1.2a.bin
20126720 Jan 03 08:33:27 2015 nexus-1000v-kickstart-mzg.VSG2.1.2a.bin
45985810 Jan 01 14:30:00 2015 nexus-1000v-mzg.VSG2.1.2a.bin
46095447 Jan 07 11:32:00 2015 nexus-1000v-mzg.VSG2.1.296.bin
1714 Jan 08 11:17:33 2015 system.cfg.new
4096 Jan 03 08:33:54 2015 vdc_2/
4096 Jan 03 08:33:54 2015 vdc_3/
4096 Jan 03 08:33:54 2015 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 be logged in to the CLI in any command mode.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	firewall# **show running-config** > [*path*	*filename*]	Directs the output of the command to a path and filename.

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

```
firewall# show running-config > volatile:vsg1-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 be logged in to the CLI in any command mode.

SUMMARY STEPS

1. vsg# **copy** *source_path_and_file* **system:running-config**
2. vsg# **show version image** [**bootflash:** | **modflash:**| **volatile:**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	vsg# **copy** *source_path_and_file* **system:running-config**	Copies the source file to the running configuration.
Step 2	vsg# **show version image** [**bootflash:**	**modflash:**| **volatile:**]	Validates the specified image.

This example shows how to copy the source file to the running configuration and validate the specified image:

```
vsg# show version image bootflash:nexus-1000v-mz.VSG2.1.201.bin
image name: nexus-1000v-mz.VSG2.1.201.bin
bios: version unavailable
system: version 5.2(1)VSG2(1) [build 5.2(1)VSG2(1.201)]
compiled: 06/6/2014 2:00:00 [06/06/2014 15:20:50]
```

Reverting to a Previous Configuration

You can recover your configuration from a previously saved version.

Before You Begin

Before beginning this procedure, you must be 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. vsg# **copy running-config bootflash:** {*filename*}
2. vsg# **copy bootflash:** {*filename*} **startup-configure**

DETAILED STEPS

	Command or Action	Purpose
Step 1	vsg# **copy running-config bootflash:** {*filename*}	Reverts to a snapshot copy of a previously saved running configuration (binary file).
Step 2	vsg# **copy bootflash:** {*filename*} **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 and how to revert to a configuration copy that was previously saved in the bootflash: directory:

```
vsg# copy running-config bootflash:January03-Running
vsg# copy bootflash:my-configure startup-configure
```

Displaying Files

To display information about files, enter the following commands:

Command	Purpose
vsg# **show file** [**bootflash:** | **debug:** | **volatile:**] *filename*	Displays the contents of the specified file.
vsg# **pwd**	Displays the current working directory.
vsg# **dir**	Displays the contents of the directory.
vsg# **show file** *filename* [**cksum** | **md5sum**]	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.
vsg# **tail** {*path*}[*filename*] {*number-of-lines*}	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.
vsg# **show users**	Displays a list of users who are currently accessing the Cisco VSG.

Example of show file

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

Example of dir command

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

Example of show file cksum command

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

Example of show file md5sum command

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

Example of tail command

```
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
```

Example of tail command

```
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)*
```

Displaying the Current User Access

You can display all users currently accessing the Cisco VSG.

Before You Begin

Before beginning this procedure, you must be logged in to the CLI in EXEC mode.

SUMMARY STEPS

1. vsg# **show user**

DETAILED STEPS

	Command or Action	Purpose
Step 1	vsg# **show user**	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)*
```

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 be logged in to the CLI.

SUMMARY STEPS

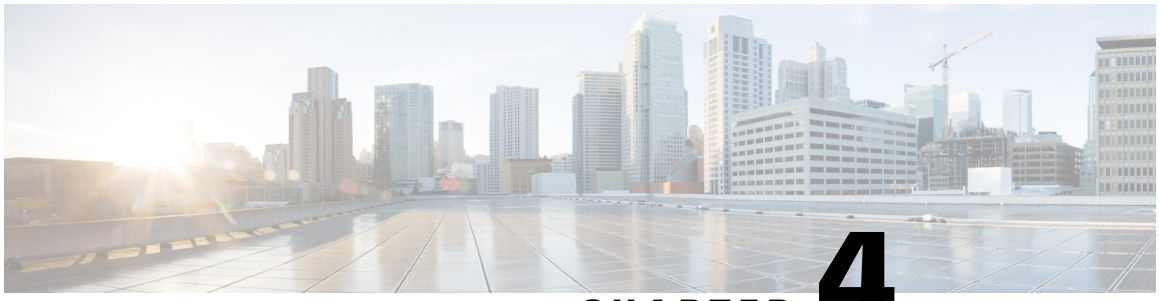
1. firewall# **send** {**session** *device*} *line*

DETAILED STEPS

	Command or Action	Purpose
Step 1	firewall# **send** {**session** *device*} *line*	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:

```
firewall# 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.
```



CHAPTER 4

Configuring SNMP

This chapter contains the following sections:

Information About SNMP

SNMP is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language used for the monitoring and management of devices in a network.

SNMP Functional Overview

The SNMP framework consists of three parts:

- An SNMP manager—The system used to control and monitor the activities of network devices using SNMP.
- An SNMP agent—The software component within the managed device that maintains the data for the device and reports these data, as needed, to manage systems. Cisco VSG supports the agent and MIB. To enable the SNMP agent, you must define the relationship between the manager and the agent.
- A managed information base (MIB)—The collection of managed objects on the SNMP agent.
- SNMP is defined in RFCs 3411 to 3418.

Note SNMP role-based access control (RBAC) is not supported. Both SNMPv1 and SNMPv2c use a community-based form of security.

SNMP Notifications

A key feature of SNMP is the ability to generate notifications from an SNMP agent. These notifications do not require that requests be sent from the SNMP manager. Notifications can indicate improper user authentication, restarts, the closing of a connection, loss of a connection to a neighbor router, or other significant events.

SNMP notifications are generated as either traps or informs. A trap is an asynchronous, unacknowledged message sent from the agent to the SNMP managers listed in the host receiver table. Informs are asynchronous messages sent from the SNMP agent to the SNMP manager which the manager must acknowledge receipt of.

Traps are less reliable than informs because the SNMP manager does not send any acknowledgment when it receives a trap. The Intercloud Fabric Firewall (VSG) cannot determine if the trap was received. An SNMP manager that receives an inform request acknowledges the message with an SNMP response protocol data unit (PDU). If the ICF Firewall never receives a response, it can send the inform request again. You can configure the ICF FIrewall to send notifications to multiple host receivers.

High Availability

Stateless restarts for SNMP are supported. After a reboot or supervisor switchover, the **running configuration** command is applied.

Guidelines and Limitations

SNMP has the following configuration guidelines and limitations:

- Read-only access to some SNMP MIBs is supported. See the Cisco NX-OS MIB support list at the following URL for more information: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.
- SNMP role-based access control (RBAC) is not supported.
- The SNMP set command is supported by the following Cisco MIBs:
  - CISCO-IMAGE-UPGRADE-MIB
  - CISCO-CONFIG-COPY-MIB

Configuring SNMP

For SNMP configuration, see the *Cisco Prime Network Services Controller GUI Configuration Guide*.

Verifying the SNMP Configuration

To display the SNMP configuration, use one of the following commands:

Table 8: SNMP Configuration Verification Commands

Command	Purpose
show running-config snmp [all]	Displays the SNMP running configuration.
show snmp	Displays the SNMP status.
show snmp community	Displays the SNMP community strings.
show snmp context	Displays the SNMP context mapping.
show snmp engineID	Displays the SNMP engine ID.
show snmp group	Displays SNMP roles.
show snmp session	Displays SNMP sessions.
show snmp trap	Displays the SNMP enabled or disabled notifications.
show snmp user	Displays SNMP users.

Standards

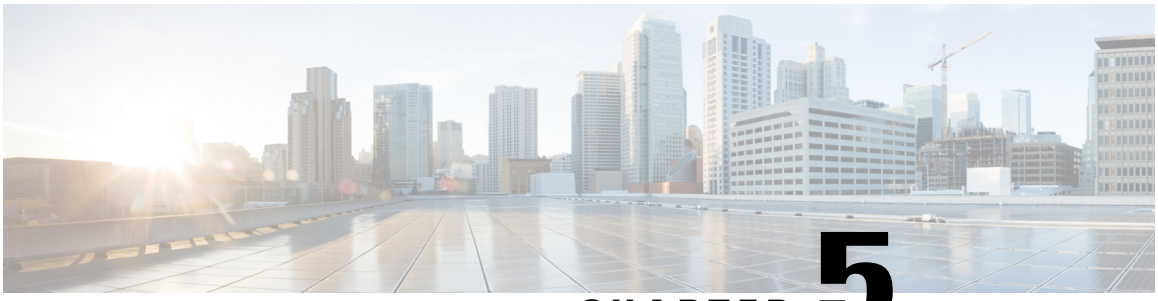
Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

Table 9: Supported MIBs

MIBs	MIBs Link
	To locate and download MIBs, go to the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

MIBs	MIBs Link
• CISCO-TC • SNMPv2-MIB • SNMP-FRAMEWORK-MIB • SNMP-FRAMEWORK-MIB • SNMP-NOTIFICATION-MIB • SNMP-TARGET-MIB • ENTITY-MIB • CISCO-ENTITY-EXT-MIB • CISCO-ENTITY-FRU-CONTROL-MIB • CISCO-FLASH-MIB • CISCO-IMAGE-MIB • CISCO-VIRTUAL-NIC-MIB • CISCO-ENTITY-VENDORTYPE-OID-MIB • NOTIFICATION-LOG-MIB • IANA-ADDRESS-FAMILY-NUMBERS-MIB • IANAifType-MIB • IANAiprouteprotocol-MIB • HCNUM-TC • CISCO-VLAN-MEMBERSHIP-MIB • CISCO-SYSTEM-MIB • CISCO-SYSTEM-EXT-MIB • ISCO-IMAGE-MIB • CISCO-IMAGE-UPGRADE-MIB • CISCO-BRIDGE-MIB • CISCO-CONFIG-COPY-MIB • CISCO-SYSLOG-EXT-MIB • CISCO-PROCESS-MIB • CISCO-AAA-SERVER-MIB • CISCO-AAA-SERVER-EXT-MIB • CISCO-COMMON-ROLES-MIB • CISCO-COMMON-MGMT-MIB • CISCO-UNIFIED-FIREWALL-MIB	



CHAPTER 5

Configuring High Availability

This chapter contains the following sections:

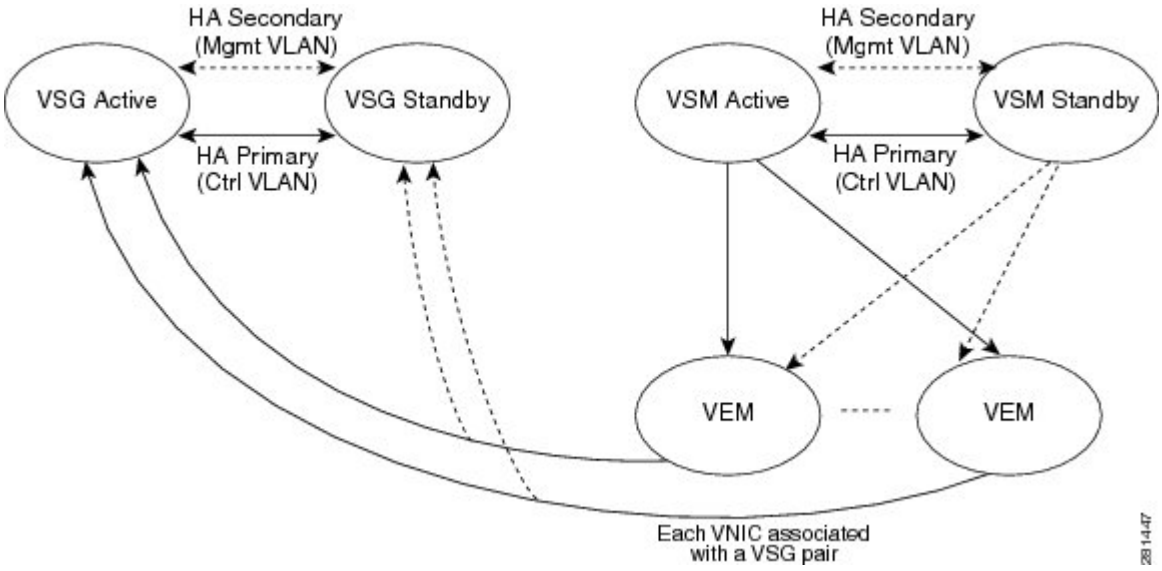
Information About High Availability

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

The following figure shows the Cisco VSG HA model.

Figure 8: Cisco VSG High Availability



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.

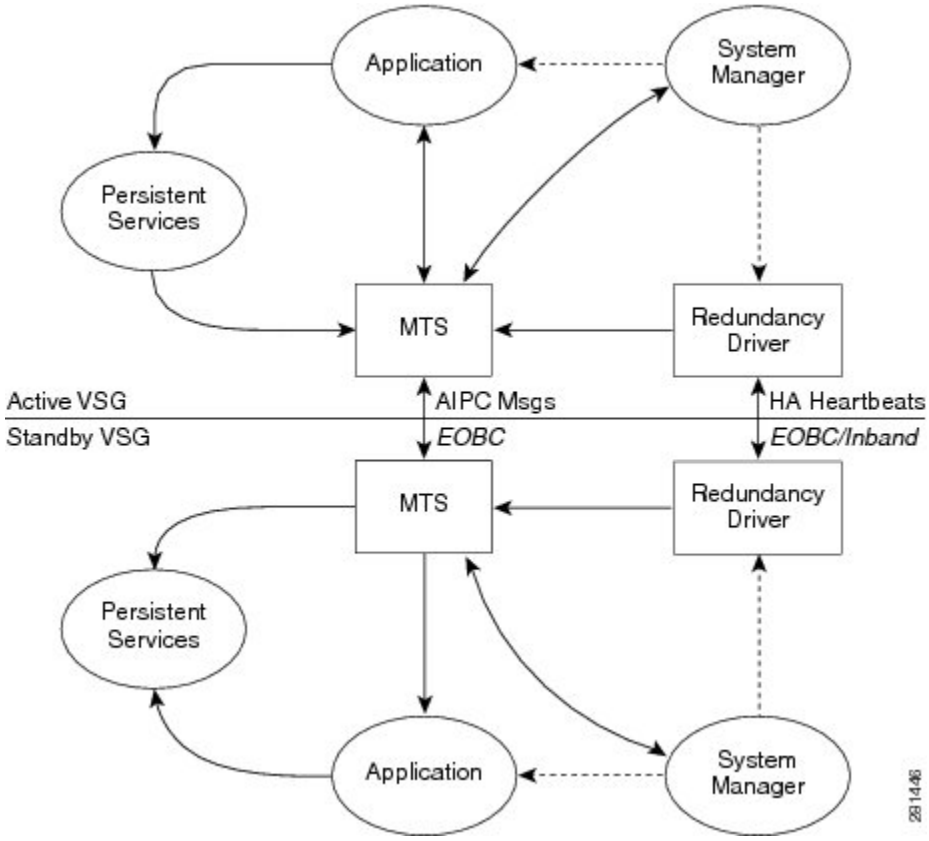
System-Control Services

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

The following figure shows the system-control services.

Figure 9: System-Control Services



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, restarting a 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 Virtual Supervisor Module (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.

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 that 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 to provide a stateful failover of most services.

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 compute nodes 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. Verify that the standby Cisco VSG is stable and is ready for a failover . After verifying that the standby Cisco VSG is stable, you can manually initiate a failover. When 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, you can improve redundancy by installing them in separate hosts and, if possible, connecting them to different upstream switches.
- The console for the standby Cisco VSG is available through the vSphere client or by entering 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. However, some **show** commands can be executed on the standby Cisco VSG. 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

Caution Changing the role of a Cisco VSG can result in a conflict between the pair. If both the primary and secondary VSG instances 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.

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

- 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.

Change a standalone Cisco VSG to a secondary Cisco VSG.

SUMMARY STEPS

1. vsg# **system redundancy role {standalone | primary | secondary}**
2. (Optional) vsg# **show system redundancy status**
3. (Optional) vsg# **copy running-config startup-config**

DETAILED STEPS

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

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

Failover 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. If the standby Cisco VSG is not in a stable state (the state must be ha-standby), a manually initiated failover cannot be done.

Command	Purpose
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

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 that verify that a cisco VSG pair is ready for a failover 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 by entering the **copy running-config startup-config** command.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	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	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	vsg# **configure**	Places you in global configuration mode.
Step 4	vsg# **copy running-config startup-config**	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

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%
```

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 be logged in to the CLI in configuration mode.

SUMMARY STEPS

1. vsg# **configure**
2. vsg(config)# **ha-pair id** {*number*}

DETAILED STEPS

	Command or Action	Purpose
Step 1	vsg# **configure**	Places you in global configuration mode.
Step 2	vsg(config)# **ha-pair id** {*number*}	Assigns an ID to an HA pair.

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

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

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.

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	vsg# **system redundancy role primary**	Changes the standalone Cisco VSG to a primary Cisco VSG. The role change occurs immediately.
Step 2	vsg# **show system redundancy status**	(Optional) Displays the current redundancy state for the Cisco VSG.
Step 3	vsg# **configure**	Places you in global configuration mode.
Step 4	vsg(config)# **copy running-config startup-config**	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

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

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

This example shows how to display the current system redundancy status for a 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# configure
vsg(config)# copy running-config startup-config
[########################################] 100%
```

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.

Note Before running the following command, you must change the single Cisco VSG role from standalone to primary.

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

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.

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.

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.

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 compute nodes 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. 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.

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 compute nodes 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 compute nodes.

Step 5 Power up the new primary Cisco VSG.
The new primary Cisco VSG starts and automatically synchronizes all configuration data with the secondary VSG, 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 of the system.

Command	Purpose
vsg# **show system redundancy status**	Displays the HA status of the system.

This example shows how to display the system redundancy status:

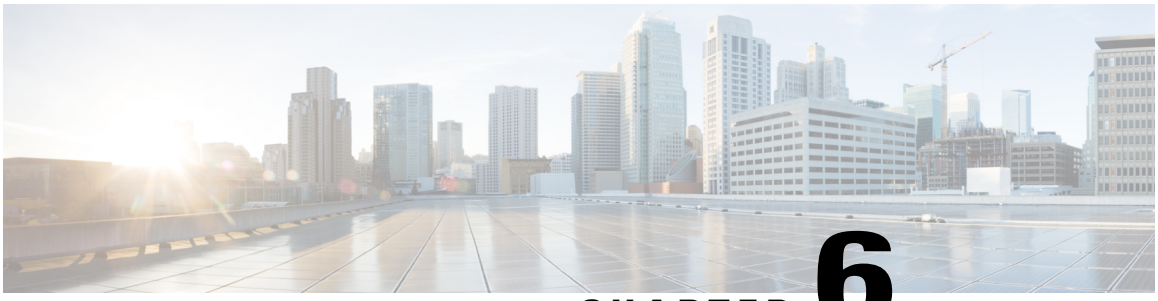
```
vsg# show system redundancy status
Redundancy role
---------------
administrative: primary
operational: primary
Redundancy mode
---------------
administrative: HA
operational: HA
This supervisor (sup-1)
-----------------------
Redundancy state: Active
Supervisor state: Active
Internal state: Active 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
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
```



CHAPTER 6

Configuring Firewall Profiles and Policy Objects

This chapter contains the following sections:

Information About Policy Objects

This section describes how you can use the Cisco Prime Network Services Controller (Prime NSC) to configure and manage the firewall policy objects on .

Note You can configure only through Cisco PNSC. Currently, we do not support out of band configuration and management of firewall policy objects.

Information About Cisco VSG Policy Objects and Firewall Profiles

Cisco VSG Policy Object Configuration Prerequisites

Cisco VSG policy objects have the following prerequisites:

- You must have the Cisco Nexus 1000V Advanced Edition license installed on the Cisco Nexus 1000V Series switch. Starting with Cisco Nexus 2.1 Release, Cisco VSG license is bundled with Cisco Nexus 1000V Advanced Edition licenses.
- 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.
- The data IP address and management IP addresses must be configured.

- 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 policy objects and firewall policies have the following configuration guidelines and limitations:

- The Management VLAN must be extended to the Cloud and configured as system VLAN.
- The 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 VSG for InterCloud and Cisco Prime NSC Installation and Upgrade Guide, for details about assigning network labels to the network adapters.

Default Settings

Table 10: Default Parameter Settings for Cisco VSG

Parameters	Default
rule policy object	drop

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 , such as VM attributes. 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 a zone should not have a directional sense and must be neutral.

Zone Example

This example shows how to display a zone in your network:

```
vsg# show running-config zone zone1
zone zone1
cond-match-criteria: match-any
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 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.

Object Group Example

This example shows how to display the object groups in your network:

```
vsg# show running-config object-group g1
object-group g1 net.port
match 10 in-range protocol 6 port 10 30
match 11 eq protocol 6 port 21 inspect ftp
```

Rules

Firewall rules can consist of multiple conditions and actions. Rules can be defined in a policy as a condition for filtering the traffic. The policy engine uses the policy as a configuration that filters the network traffic that is received on the . The policy engine uses two types of condition matching models for filtering the network traffic:

AND Model: A rule is set to matched when all the attributes in a rule match.

OR model: The attributes are classified into five different types of columns. For a rule to be true, at least one condition in each column must be true. The five columns in an OR model are:

- Source column: Attribute to identify source host.
- Destination column: Attribute to identify destination host.
- Service column: Attribute to identify service at the destination host.
- Ether type column: Attribute to identify link level protocol.
- Source port column: Attribute to identify source port.

Rule Example

This example shows how to display the rule in your network:

```
vsg# show running-config rule r2
rule r2
cond-match-criteria: match-all
   dst-attributes
     condition 10 dst.zone.name eq z1@r2
   service/protocol-attribute
```

```
condition 11 net.service eq protocol 6 port 21 inspect ftp
action permit
```

Policies

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

- Rules
- Conditions
- Actions
- Objects groups
- Zones

A policy is bound to a 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 .

Policy Examples

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

```
vsg# show running-config policy p2@root/T1
policy p2@root/T1
  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 permit
```

Cisco Virtual Security Gateway Attributes

This section describes Cisco VSG attributes.

Information About Attribute Name Notations

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 a zone 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

Attributes are used in configuring policy rules and conditions, or zone definitions.

Neutral Attributes

Because object groups and zones can be shared between various rules with different directions, the attributes used in a zone 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.

VM Attributes

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

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

The following table describes the VM attributes that are supported by Cisco VSG.

Description	Name
Name of VM	src.vm.name dst.vm.name vm.name **Note** vm.name is a neutral attribute.
Name of host parent (host)	src.vm.host-name dst.vm.host-name vm.host-name **Note** vm.host-name is a neutral attribute.

Description	Name
Full name of OS guest (includes the version)	src.vm.os-fullname dst.vm.os-fullname vm.os-fullname **Note** vm.os-fullname is a neutral attribute.
Name of port profile associated with specific vNIC	src.vm.portprofile-name dst.vm.portprofile-name vm.portprofile-name **Note** vm.portprofile-name is a neutral attribute.
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 **Note** vm.custom.xxx is a neutral attribute.

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:

```
firewall(config)# show vsg vm
VM uuid          : 852a1ff3-149d-4c75-adfa-c75e0d583d37
VM attributes :
  name                        : vm
  os-fullname               : windows server 2012 r2 datacenter
  os-hostname             : vm


Zone(s) :
```

Zone Attributes

Table 11: Zone Attributes Supported by Cisco VSG

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 **Note** zone.name is a 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-nsc-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-nsc-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
```

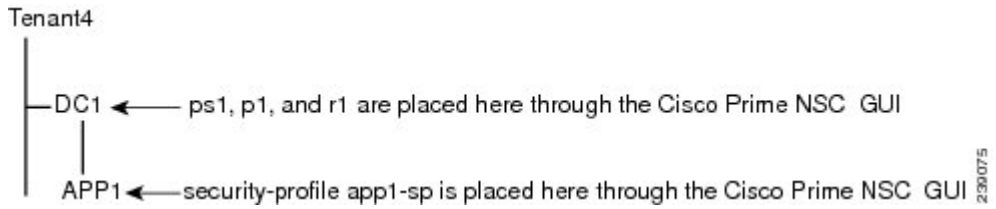
Viewing Security Profiles and Policies on the Cisco Prime NSC and the Cisco VSG

The Cisco Prime NSC GUI provides a view of the Cisco VSG security policy objects. The policy objects shown in the Cisco Prime NSC 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 Prime NSC 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.

The following figure shows the Cisco Prime NSC GUI organization structure.

Figure 10: Cisco Prime NSC Organizational Hierarchy for a Tenant, Data Center, and Application




```
security-profile app1-sp@root/tenant4/DC1/APP1
policy ps1@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 Prime NSC 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 Prime NSC organizational hierarchy.

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

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

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 Prime NSC.
- The policy p1 is located at root in the organization tree on the Cisco Prime NSC.
- The rule r1 is placed in the policy p1 on the Cisco Prime NSC (the Cisco Prime NSC 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 Prime NSC.

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

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 Prime NSC but are resolved from that location in the Cisco Prime NSC organization tree.

Configuring Service Firewall Logging

See the “Enabling Global Policy-Engine Logging” section of the .

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 2014

version 5.2(1)VSG2(1.2)
feature telnet
no feature http-server

username adminbackup password 5 $1$Oip/C5Ci$oOdx7oJSlBCFpNRmQK4na. role network-operator
username admin password 5 $1$CbPcXmpk$l31YumYWiO0X/EY1qYsFB. role network-admin
username vsnbetauser password 5 $1$mr/jBgON$hoJsM9ACdPHRWPM3KpI6/1 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
snmp-server user vsnbetauser auth md5 0x272e8099cab7365fd1649d351b953884 priv
0x272e8099cab7365fd1649d351b953884 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.VSG2.1.bin
bootflash:ukickstart
cli alias name udplug copy scp://user@<ip
address>/ws/sjc/baselard_latest/build/images/gdb/nexus-1000v-dplug-mzg.VSG2.1.bin
bootflash:ukickstart
cli alias name udplug copy scp://user@<ip
address>/ws/sjc/baselard_latest/build/images/gdb/nexus-1000v-dplug-mzg.VSG2.1.bin
bootflash:dplug
cli alias name uimage copy scp://user@<ip
address>/ws/sjc/baselard_latest/build/images/gdb/nexus-1000v-mzg.VSG2.1.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
nsc-policy-agent
 registration-ip 10.193.73.190
 shared-secret **********
 log-level info
vsg#
```

Configuration Limits

Table 12: Maximum Configuration Limits for Configuring the Cisco VSG

Feature	Maximum Limit
Zones in Cisco VSG	512

Feature	Maximum Limit
Rules per policy	1024
Policy set per Cisco VSG	16
Object Group in Cisco VSG	512
Total number of conditions	16k
Maximum rules per Cisco VSG	1024