Cisco VSG for KVM, Release 5.2(1)VSG2(1.3) and Cisco PNSC, Release 3.4 Installation and Upgrade Guide

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

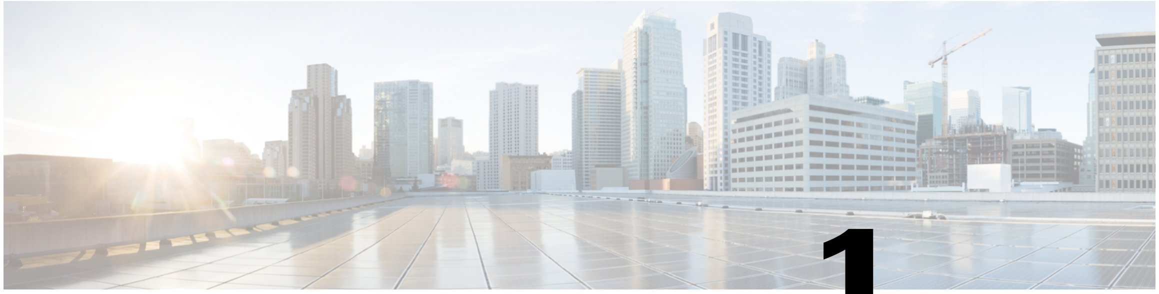
The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

CONTENTS



CHAPTER 1

Overview

This chapter contains the following sections:

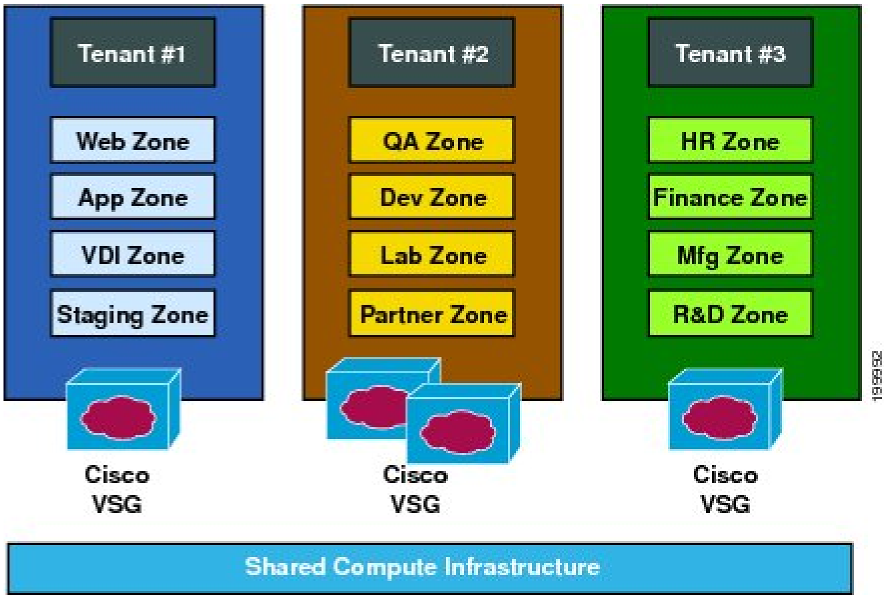
Information About Installing Cisco PNSC and Cisco VSG

You must install Cisco Prime Network Services Controller (PNSC) and Cisco VSG in a particular sequence on the Cisco Nexus 1000V switch to have a functioning virtual system.

Information About Cisco VSG

The Cisco VSG is a virtual firewall appliance that provides trusted access to virtual data center and cloud environments with dynamic policy-driven operation, mobility-transparent enforcement, and scale-out deployment for dense multitenancy. 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. The following figure shows the trusted zone-based access control that is used in per-tenant enforcement with the Cisco VSG.

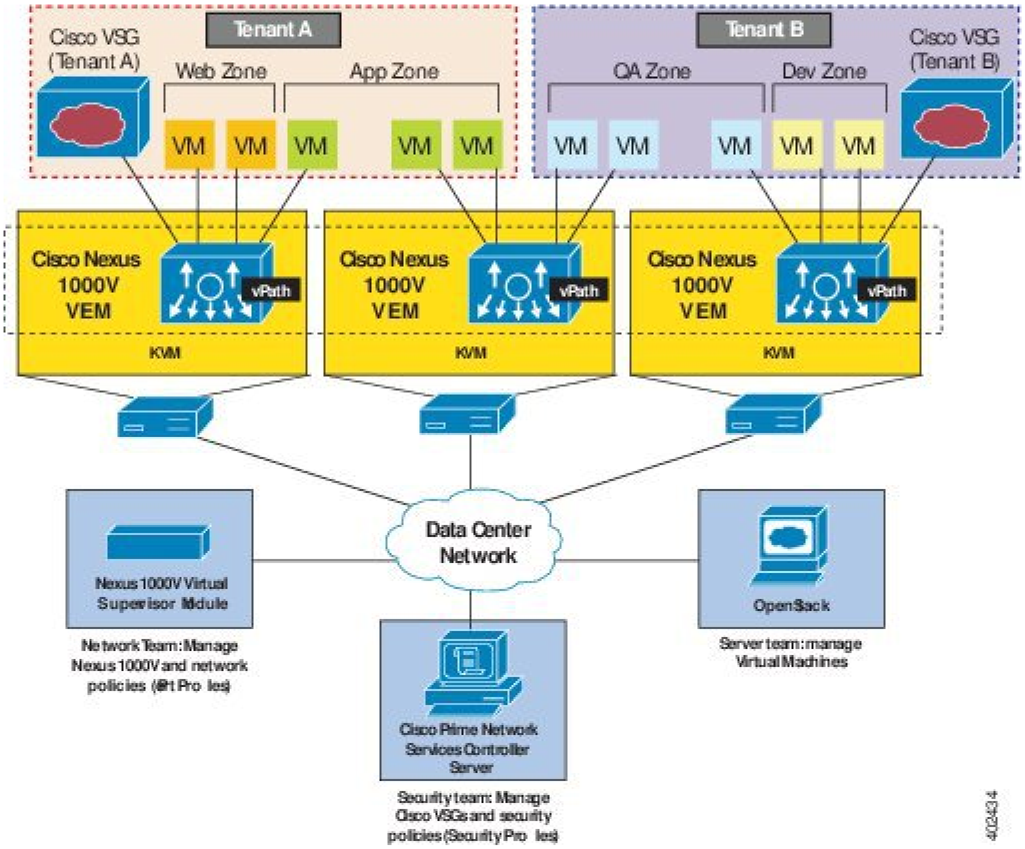
Figure 1: Trusted Zone-Based Access Control Using Per-Tenant Enforcement with the Cisco VSG



Cisco PNSC and Cisco VSG Architecture

Cisco VSG operates with Cisco Nexus 1000V Series switch on KVM on Red Hat Enterprise Linux OpenStack Platform and leverages the virtual network service data path (Cisco vPath). Cisco vPath steers traffic, whether external-to-VM or VM-to-VM, to 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 offloads policy enforcement of the remaining packets to Cisco vPath.

Figure 2: Cisco Virtual Security Gateway Deployment Topology


Tenant A
Cisco VSG (Tenant A)
Web Zone
App Zone
Tenant B
QA Zone
Dev Zone
Cisco VSG (Tenant B)
VM
Cisco Nexus 1000V VEM
vPath
KVM
Data Center Network
Nexus 1000V Virtual Supervisor Module
Network Team: Manage Nexus 1000V and network policies (Port Profiles)
Cisco Prime Network Services Controller Server
Security team: Manage Cisco VSGs and security policies (Security Profiles)
OpenStack
Server team: manage Virtual Machines
402434

vPath supports the following features:

- Tenant-aware flow classification and subsequent redirection to a designated Cisco VSG tenant.
- Per-tenant policy enforcement of flows offloaded by the Cisco VSG to Cisco vPath.

The Cisco VSG and the VEM provide the following benefits:

- Each Cisco VSG can provide protection across multiple physical servers, which eliminates the need for you to deploy a virtual appliance per physical server.
- By offloading the fast-path to one or more Cisco vPath Virtual Ethernet Modules (VEMs), the Cisco VSG enhances security performance through distributed Cisco vPath-based enforcement.
- You can use the Cisco VSG without creating multiple switches or temporarily migrating VMs to different switches or servers. Zone scaling, which is based on security profiles, simplifies physical server upgrades without compromising security or incurring application outages.
- For each tenant, you can deploy the Cisco VSG in an active-standby mode to ensure that Cisco vPath redirects packets to the standby Cisco VSG when the primary Cisco VSG is unavailable.

- You can place the Cisco VSG on a dedicated server so that you can allocate the maximum compute capacity to application workloads. This feature enables capacity planning to occur independently and allows for operational segregation across security, network, and server groups.

Trusted Multitenant Access

You can transparently insert a Cisco VSG into the KVM environment where the Cisco Nexus 1000V is deployed. One or more instances of the Cisco VSG is deployed on a per-tenant basis, which allows a highly scale-out deployment across many tenants. Tenants are isolated from each other, so no traffic can cross tenant boundaries. You can deploy a Cisco VSG at the tenant level in KVM and mange each tenant instance using OpenStack dashboard.

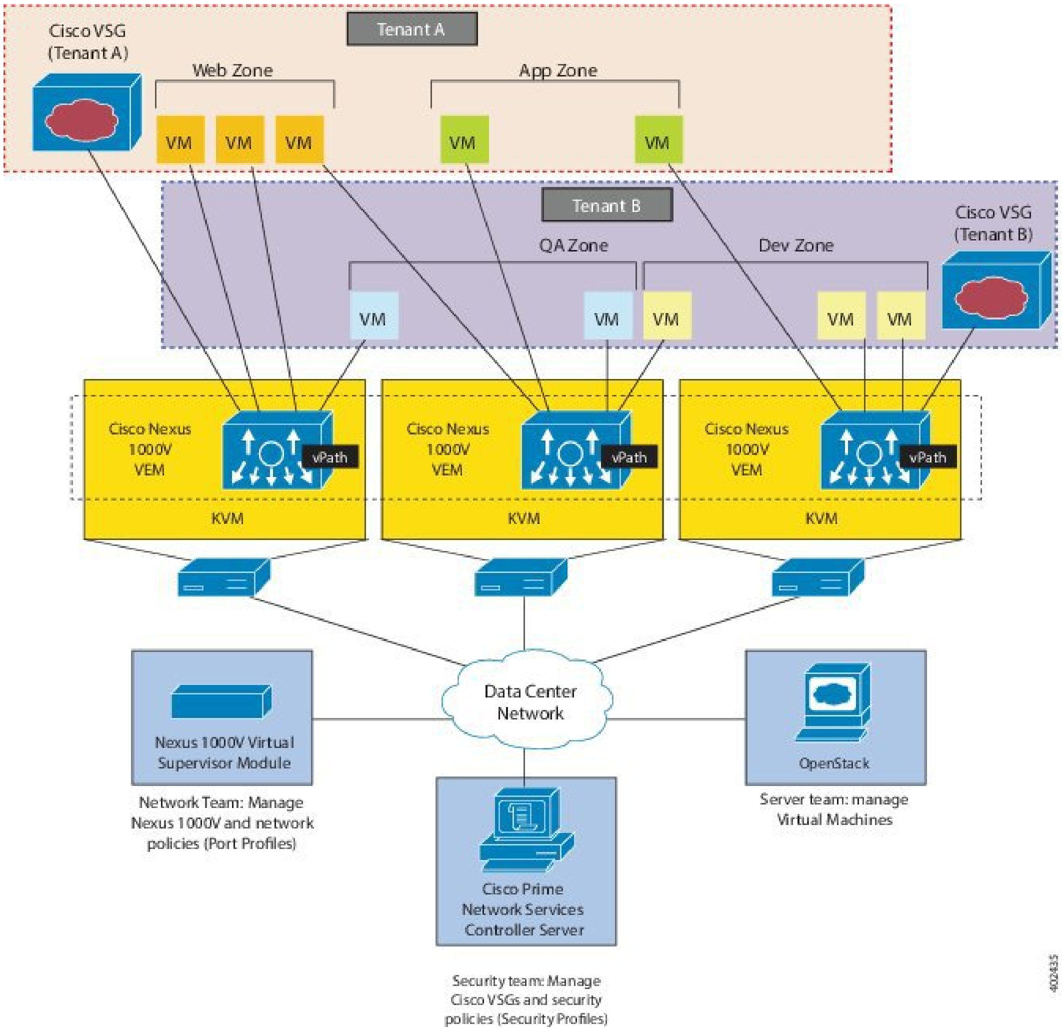
As you instantiate VMs for a given tenant, their association to security profiles (or zone membership) occurs immediately through binding with the Cisco Nexus 1000V port profile. Each VM is placed upon instantiation into a logical trust zone. Security profiles contain context-aware rule sets that specify access policies for traffic that enters and exits each zone. In addition to VM and network contexts, security administrators can also leverage custom attributes that define zones directly through security profiles. You can apply controls to zone-to-zone traffic and to external-to-zone (and zone-to-external) traffic. Zone-based enforcement occurs within a VLAN/VXLAN because a VLAN/VXLAN often identifies a tenant boundary. The Cisco VSG evaluates access control rules and then offloads enforcement to the Cisco Nexus 1000V VEM vPath module. Upon enforcement, the Cisco VSG can permit or deny access and can generate optional access logs. The Cisco VSG also provides policy-based traffic monitoring capability with access logs.

Dynamic Virtualization-Aware Operation

A virtualization environment is a dynamic environment, where frequent additions, deletions, and changes occur across tenants and across VMs. Live migration of VMs can occur due to manual or programmatic

VMotion events. The following figure shows how the structured environment can change over time due to dynamic VMs.

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



The Cisco VSG operating with the Cisco Nexus 1000V (and Cisco vPath) supports a dynamic VM environment. When you create a tenant with the Cisco VSG (standalone or active-standby pair) on the Cisco PNSC, 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 as policy profile on the OpenStack dashboard.

When a new VM is instantiated, the server administrator assigns appropriate policy profiles to the virtual Ethernet port of the VM. Because the port profile uniquely refers to a security profile and VM zone membership, the Cisco VSG immediately applies the security controls.

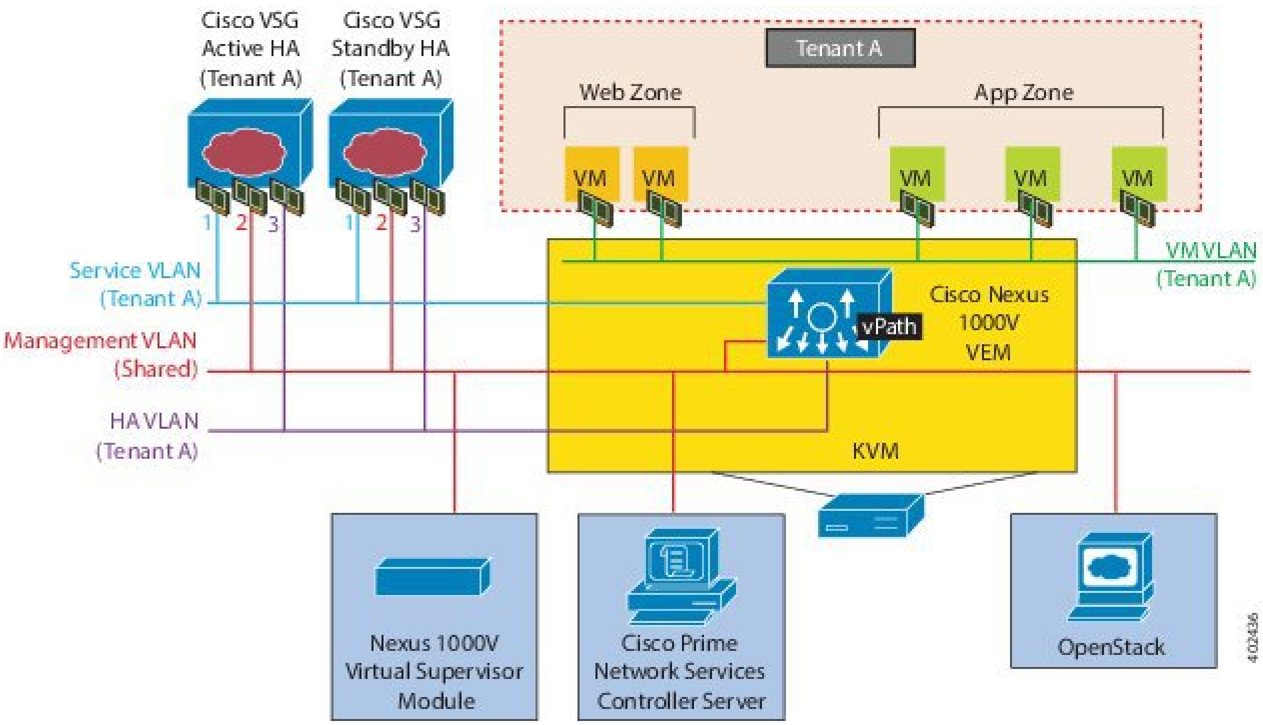
As VM migration events are triggered, VMs move across physical servers. Because Cisco Nexus 1000V ensures that port profile policies follow the VMs, associated security profiles also follow these moving VMs, and security enforcement and monitoring remain transparent to the migration events.

Setting Up the Cisco VSG and VLAN

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

In the following figure, the Cisco VSG connects to three different VLANs (service VLAN, management VLAN, and HA VLAN). A Cisco VSG is configured with three vNICS—data vNIC (1), management vNIC (2), and HA vNIC (3)—with each of the vNICs connected to one of the VLANs through a port profile.

Figure 4: Cisco Virtual Security Gateway VLAN Usages



The VLAN functions are as follows:

- The service VLAN provides communications between the Cisco Nexus 1000V VEM and Cisco VSG. All the Cisco VSG data interfaces are part of the service VLAN and the VEM uses this VLAN for its interaction withCisco VSG.
- The management VLAN connects the management platforms such as the Cisco PNSC, the Cisco Nexus 1000V VSM, and the managed Cisco VSGs. The Cisco VSG management vNIC is part of the management VLAN.

Note The VSG Management VLAN is not yet provisioned to connect to the Horizon dashboard.

- The HA VLAN provides the heartbeat mechanism and identifies the active and standby relationship between the Cisco VSGs. The Cisco VSG vNICs are part of the HA VLAN.

You can allocate one or more VM data VLANs for VM-to-VM communications. In a typical mult-itenant environment, the management VLAN is shared among all the tenants and the service VLAN, HA VLAN, and the VM data. VLANs are allocated on a per-tenant basis. However, when VLAN resources become scarce, you might decide to use a single VLAN for service and HA functions.

Information About the Cisco PNSC

The Cisco PNSC virtual appliance is based on Red Hat Enterprise Linux (RHEL), which provides centralized device and security policy management of the Cisco VSG for the Cisco Nexus 1000V Series switch. Designed for multi-tenant operation, the Cisco PNSC provides seamless, scalable, and automation-centric management for virtual data center and cloud environments. With a web-based GUI, CLI, and XML APIs, the Cisco PNSC enables you to manage Cisco VSGs that are deployed throughout the data center from a centralized location.

Note Multi-tenancy is when a single instance of the software runs on a Software-as-a-Service (SaaS) server, serving multiple client organizations or tenants. In contrast, multi-instance architecture has separate software instances set up for different client organizations. With a multi-tenant architecture, a software application can virtually partition data and configurations so that each tenant works with a customized virtual application instance.

The Cisco PNSC is built on an information model-driven architecture, where each managed device is represented by its sub-components.

Cisco PNSC Key Benefits

The Cisco PNSC provides the following key benefits:

- Rapid and scalable deployment with dynamic, template-driven policy management based on security profiles.
- Seamless operational management through XML APIs that enable integration with third-party management tools.
- Greater collaboration across security and server administrators, while maintaining administrative separation and reducing administrative errors.

Cisco PNSC Components

The Cisco PNSC architecture includes the following components:

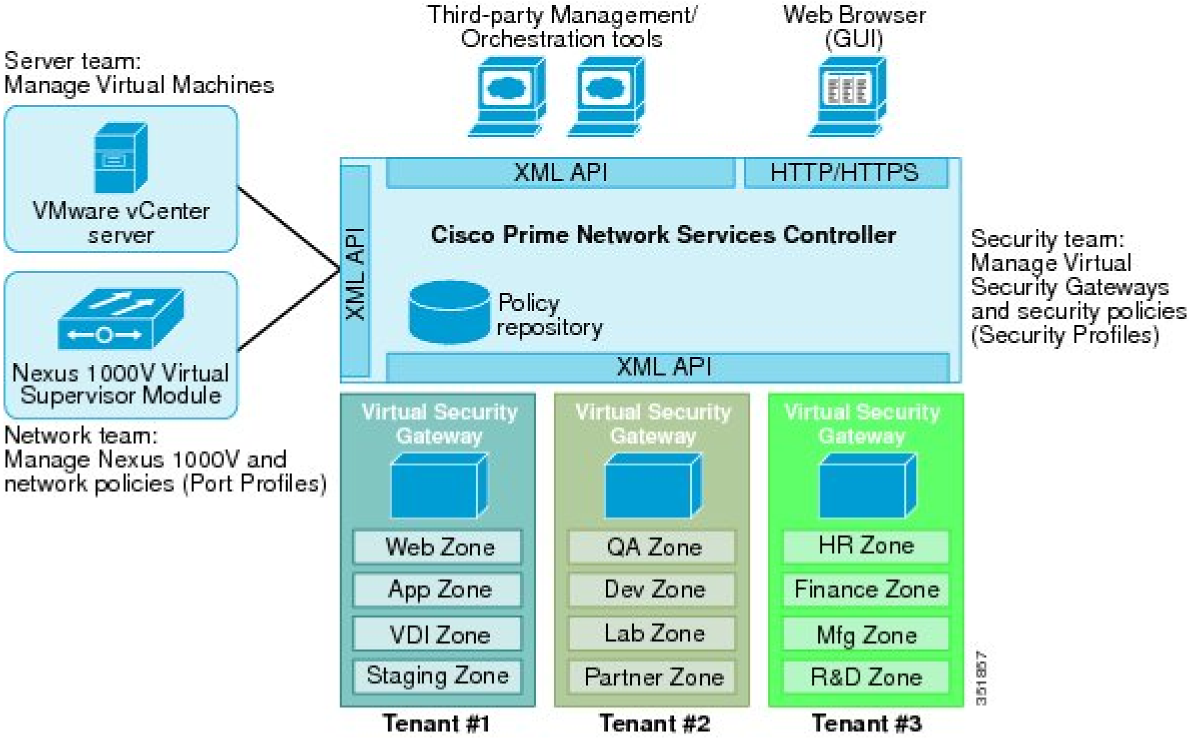
- A centralized repository for managing security policies (security templates) and object configurations that allow managed devices to be stateless.
- A centralized resource management function that manages pools of devices that are commissioned and pools of devices that are available for commissioning. This function simplifies large scale deployments as follows:
    - Devices can be pre-instantiated and then configured on demand

- ◦ Devices can be allocated and deallocated dynamically across commissioned and non-commissioned pools
- ◦ A distributed management-plane function that uses an embedded management agent on each device that allows for a scalable management framework.

Cisco PNSC Architecture

The Cisco PNSC architecture includes the components in the following figure:

Figure 5: Cisco PNSC Components

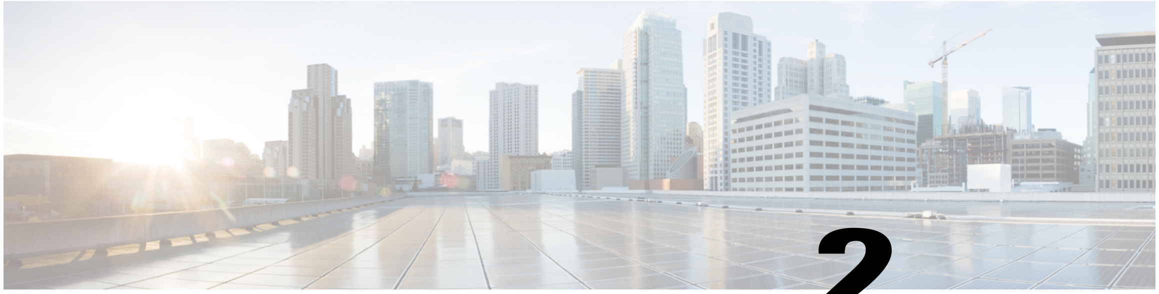

Third-party Management/ Orchestration tools
Web Browser (GUI)
Server team: Manage Virtual Machines
VMware vCenter server
Nexus 1000V Virtual Supervisor Module
Network team: Manage Nexus 1000V and network policies (Port Profiles)
XML API
HTTP/HTTPS
XML API
Cisco Prime Network Services Controller
Policy repository
XML API
Security team: Manage Virtual Security Gateways and security policies (Security Profiles)
Virtual Security Gateway
Web Zone
App Zone
VDI Zone
Staging Zone
Tenant #1
Virtual Security Gateway
QA Zone
Dev Zone
Lab Zone
Partner Zone
Tenant #2
Virtual Security Gateway
HR Zone
Finance Zone
Mfg Zone
R&D Zone
Tenant #3
351857

Cisco PNSC Security

The Cisco PNSC uses security profiles for tenant-centric template-based configuration of security policies. A security profile is a collection of security policies that are predefined and applied on an on-demand basis at the time of Virtual Machine (VM) instantiation. These profiles simplify authoring, deployment, and management of security policies in a dense multi-tenant environment, reduce administrative errors, and simplify audits.

Cisco PNSC API

The Cisco PNSC API allows you to coordinate with third-party provisioning tools for programmatic provisioning and management of Cisco VSGs. This feature allows you to simplify data center operational processes and reduce the cost of infrastructure management.



CHAPTER 2

Installing the Cisco Prime Network Services Controller

This chapter contains the following sections:

Information About the Cisco PNSC

The Cisco Prime Network Services Controller (Cisco PNSC) is a virtual appliance that provides centralized device and security policy management for Cisco virtual services. Designed to support enterprise and multiple-tenant cloud deployments, the Cisco PNSC provides transparent, seamless, and scalable management for securing virtualized data center and cloud environments.

The dynamic nature of cloud environments requires organizations to apply and enforce frequent changes to networks. These networks can consist of thousands of virtual services elements, such as firewalls, load balancers, routers, and switches. Cisco PNSC simplifies operations with centralized, automated multi-device and policy management for Cisco network virtual services.

Cisco PNSC is the primary management element for Cisco Nexus 1000V (Nexus 1000V) switches and services that can enable a transparent, scalable, and automation-centric network management solution for virtualized data center and hybrid cloud environments. Nexus 1000V switches and services deliver a highly secure multi-tenant environment by adding virtualization intelligence to the data center network. These virtual switches are built to scale for cloud networks. Support for Virtual Extensible LAN (VXLAN) helps enable a highly scalable LAN segmentation and broader virtual machine (VM) mobility.

Cisco PNSC enables the centralized management of Cisco virtual services to be performed by an administrator, through its GUI, or programmatically through its XML API. Cisco PNSC is built on an information-model architecture in which each managed device is represented by its sub-components (or objects), which are parametrically defined. This model-centric approach enables a flexible and simple mechanism for provisioning and securing virtualized infrastructure using Cisco VSG and Cisco Adaptive Security Appliance 1000V (ASA 1000V) Cloud Firewall virtual security services.

In addition, Prime Network Services Controller supports Cisco Cloud Services Router 1000V (CSR 1000V) edge routers, and Citrix NetScaler 1000V and Citrix NetScaler VPX load balancers. This combination of virtual services brings numerous possibilities to customers, enabling them to build virtual data centers with all of the required components to provide best-in-class cloud services.

For detailed information on how to install Cisco Prime Network Services Controller, see Cisco Prime Network Services Controller 3.4 Installation Guide.

Installation Requirements

Cisco PNSC System Requirements

Requirement	Description
Prime Network Services Controller Virtual Appliance	
Four Virtual CPUs	1.8 GHz
Memory	4 GB RAM
Disk Space	220 GB on shared NFS or SAN, configured on two disks as follows: • Disk 1—20 GB • Disk 2—200 GB
Management Interface	One management network interface
Processor	x86 Intel or AMD server with 64-bit processor
Prime Network Services Controller Device Adapter	
Two virtual CPUs	1.8 GHz
Memory	2 GB RAM
Disk Space	20 GB
Interfaces and Protocols	
HTTP/HTTPS	—
Lightweight Directory Access Protocol (LDAP)	—
Intel VT	
Intel Virtualization Technology (VT)	Enabled in the BIOS

Hypervisor Requirements

Cisco PNSC is a multi-hypervisor virtual appliance that can be deployed on OpenStack KVM Hypervisor. See the following links to confirm that OpenStack KVM supports your hardware platform:

- OpenStack Compute and Image System Requirements
- OpenStack for Cisco DFA Install Guide for Using the Cisco OpenStack Installer

Requirement	Description
OpenStack KVM	
KVM Hypervisor	Ubuntu 12.04 LTS server, 64-bit
KVM Kernel	Version 3.2.0-52-generic
Cisco OpenStack Installer	Havana (Standalone mode only) Cisco PNSC Release 3.4 does not support Orchestrator mode. The version depends on the installation mode: • Standalone Mode—Grizzly • Orchestrator Mode—Dynamic Fabric Automation (DFA) OpenStack

Web-Based GUI Client Requirements

Requirement	Description
Operating system	Any of the following: • Microsoft Windows • Apple Mac OS
Browser	Any of the following browsers: • Internet Explorer 10.0 or higher • Mozilla Firefox 26.0 or higher • Google Chrome 32.0 or higher
Flash Player	Adobe Flash Player plugin 11.9 or higher

Firewall Ports Requiring Access

If Cisco PNSC is protected by a firewall, the following ports on the firewall must be open so that clients can contact Cisco PNSC.

Requirement	Description
22	TCP
80	HTTP
443	HTTPS
843	Adobe Flash
6644, 6646	TCP, UDP

Cisco Nexus 1000V Series Switch Requirements

Requirement	Notes
General	
The procedures in this guide assume that the Cisco Nexus 1000V Series switch is up and running, and that endpoint Virtual Machines (VMs) are installed.	—
VLANs	
Two VLANs configured on the Cisco Nexus 1000V Series switch uplink ports: • Service VLAN • HA VLAN	Neither VLAN needs to be the system VLAN.
Port Profiles	
One port profile configured on the Cisco Nexus 1000V Series Switch for the service VLAN.	—

Information Required for Installation and Configuration

Required Information	Your Information/Notes
For Preinstallation Configuration	
ISO or OVA image location	
ISO or OVA image name	
Network / Port Profile for VM management [1]	
VM instance name	
KVM flavor name	
KVM Instance Security Group	
VMware datastore location	
For Prime Network Services Controller Installation	
IP address For OpenStack environments, use the IP address that is assigned to the Prime Network Services Controller instance in OpenStack.	
Subnet mask	
Hostname	
Domain name	
Gateway IP address	
DNS server IP address	
NTP server IP address	
Admin password	
Shared secret password for communication between Prime Network Services Controller and managed VMs. (See Shared Secret Password Criteria.)	

[1] The management port profile is the same port profile that is used for Cisco Virtual Supervisor Module (VSM). The port profile is configured in VSM and used for the Prime Network Services Controller management interface.

Shared Secret Password Criteria

A shared secret password is a password that is known only to those using a secure communication. Passwords are designated strong if they cannot be easily guessed for unauthorized access. When you set a shared secret password for communications between the Cisco PNSC, Cisco VSG, and VSM, adhere to the following criteria for setting valid, strong passwords:

Do not include the following items in passwords:

- Characters: & ' " ` ( ) < > | \ ; $
- Spaces

Create strong passwords based on the following characteristics:

Table 1: Characteristics of Strong Passwords

Strong passwords have...	Strong passwords do not have...
• At least eight characters. • Lowercase letters, uppercase letters, digits, and special characters.	• Consecutive characters, such as *abcd*. • Characters repeated three or more times, such as *aaabbb*. • A variation of the word Cisco, such as *cisco*, *ocsic*, or one that changes the capitalization of letters in the word *Cisco.* • The username or the username in reverse. • A permutation of characters present in the username or *Cisco.*

Examples of strong passwords are:

- If2CoM18
- 2004AsdfLkj30
- Cb1955S21

Configuring Chrome for Use with Cisco PNSC

To use Chrome with Cisco PNSC, you must disable the Adobe Flash Player plugins that are installed by default with Chrome.

Note Because Chrome automatically enables Adobe Flash Player plugins each time the system reboots, you must perform this procedure each time your client machine reboots.

Procedure

Step 1 In the Chrome URL field, enter **chrome://plugins**.

Step 2 Click **Details** to expand all the files associated with each plugin.

Step 3 Locate the Adobe Flash Player plugins, and disable each one.

Step 4 Download and install Adobe Flash Player plugin version 11.9 or higher.

Step 5 Close and reopen Chrome before logging in to Cisco PNSC.

OpenStack Installation Overview

You install Cisco PNSC on OpenStack by using the ISO image. The installation time varies from 10 to 20 minutes depending on the host and the storage area network load.

To install Cisco PNSC on OpenStack, complete the tasks described in the following topics:

1. Configuring OpenStack for Prime Network Services Controller
2. Installing Prime Network Services Controller on OpenStack KVM
3. Rebooting Cisco PNSC from OpenStack, on page 20

Configuring OpenStack for Cisco PNSC

To prepare OpenStack for installing Cisco PNSC using the Cisco OpenStack Installer (COI), you must create a flavor, import an image, and launch an instance. This procedure describes how to complete these tasks.

Before You Begin

In OpenStack:

- Confirm that you have met the requirements in Requirements Overview. OpenStack Havana is required for Cisco PNSC, Release 3.4 functionality.

  Note Although you can install Cisco PNSC, Release 3.4 on OpenStack Grizzly, you will not have access to release 3.4 functionality unless you use OpenStack Havana.

- Gather the information required for configuration as identified in Information Required for Configuration and Installation.
- Confirm that you have admin privileges.
- Confirm that the Cinder service is up and running.
- Create a project on which to install Cisco PNSC.
- Create a Cinder volume with the size of 20 GB.
- Configure a security group that allows TCP, UDP, and ICMP traffic with Cisco PNSC.

For information on how to configure these items, see the OpenStack documentation at docs.openstack.org.

Procedure

Step 1 In the OpenStack Dashboard, choose **Admin** > **Flavors**, and then click **Create Flavor**.

Step 2 In the Create Flavor dialog box, enter the following information, and then click **Create Flavor**:

- Name—Flavor name.
- vCPUs—Enter **4**.
- RAM MB—Enter **4096**.
- Root Disk—Enter **20 GB**.
- Ephemeral Disk—Enter **20 GB**.
- Swap Disk—Enter **400 MB**.

Step 3 Choose **Admin** > **Images**, and then click **Create An Image**.

Step 4 In the Create An Image dialog box, provide the following information, and then click **Create Image**:

- Name—Enter an image name.
- Image Source—Specify the image source.
- Image File—Use this field if the image is available on your local system.
- Format—Choose **ISO - Optical Disk Image**.
- Public—Check the check box to make the image available to all users with access to the current project.
- Protected—Check the check box to ensure that only users with permission can delete the image.

After the image has been created, it appears in the Images table at **Admin** > **Images** or **Project** > *project* > **Manage Compute** > **Images & Snapshots**.

Step 5 Choose **Project** > *project* > **Manage Compute** > **Volumes**, and click **Create Volume**.

Step 6 In the Create Volume dialog box, add a volume with the size of 20 GB, and click **Create Volume**.

Step 7 At the command line, enter the following command to launch the Cisco PNSC instance:

```
nova boot --flavor=flavor-id --image=image-id
--nic net-id=network-id,v4-fixed-ip=pnsc-ip
--block-device-mapping vdb=volume-id:::0 pnsc-image-name
```

Step 8 In the OpenStack GUI, choose **Project** > *project* > **Manage Compute** > **Instances**.

Step 9 In the Instances pane, note the IP address of the launched instance.

Step 10 Click the instance and choose **More** > **Console** to start the Cisco PNSC installation procedure.

What to Do Next

Install Cisco PNSC as described in Installing Prime Network Services Controller on OpenStack KVM.

Installing Cisco PNSC on OpenStack KVM

Before You Begin

- All system requirements are met as specified in System Requirements.
- Confirm that you have admin privileges.
- You have configured the hypervisor for the Cisco PNSC installation procedure.
- A VM has been created for Cisco PNSC and has network access.
- You can access the VM console.
- You have the IP address for the instance launched in OpenStack.

Note For information on how to configure these items, see the OpenStack documentation at docs.openstack.org.

Note For more information on how to install Cisco PNSC, see Cisco Prime Network Services Controller 3.4 Installation Guide.

Procedure

Step 1 Open the VM console if it is not already open. If you have just finished configuring the hypervisor, the Cisco PNSC installer displays within a few minutes.

Step 2 In the Network Configuration screen, click **Edit** in the Network Devices area, enter the IP address and netmask for the Cisco PNSC VM, and click **OK**.

Step 3 In the Network Configuration area, enter the hostname, domain name, and IP addresses for the gateway, DNS server, and NTP server.

Step 4 In the Modes screen, choose the required modes, and click **Next**:

- Prime Network Services Controller Operation Mode: Choose **Standalone**. This release of Cisco PNSC is available in Standalone mode only.
- Prime Network Services Controller Configuration:
  - Prime Network Services Controller Installation—Choose if this is the initial Prime Network Services Controller installation on the VM.
  - Restore Prime Network Services Controller—Choose to restore a previous Prime Network Services Controller installation.

Step 5 In the Administrative Access screen, enter the administrator and shared secret passwords with confirming entries.
For information on creating a strong password, see Shared Secret Password Criteria.

Note If you configure a weak shared secret password, no error message is generated during entry here, but the shared secret password is not usable when the VM is started during the installation process.

Step 6 In the Summary screen, confirm that the information is accurate, and then click **Finish**. Prime Network Services Controller installs on the VM. This takes a few minutes.

Step 7 When prompted, disconnect from the media source and then click **Reboot**. Prime Network Services Controller is then installed on the VM.

Step 8 To confirm that Cisco PNSC is accessible, connect to Cisco PNSC through the console for the CLI or a browser for the GUI.

What to Do Next

Reboot the Cisco PNSC from OpenStack, see *Cisco Prime Network Services Controller 3.4 Installation Guide*.

Rebooting Cisco PNSC from OpenStack

If you reboot a Cisco PNSC instance from the OpenStack Horizon UI, the reboot operation fails and the console contains a message stating that no bootable image can be found. This situation occurs for instances that were created using an ISO image, such as Cisco PNSC.

In OpenStack, the first time an instance is created by using an ISO image and rebooted, the root device name is set to /dev/hda. After the instance is created, the bootable image is located on hda. However, with the implementation of hard and soft reboot options in OpenStack, the disk definitions change. As a result, a bootable image cannot be found for the Cisco PNSC instance.

To reboot Cisco PNSC in OpenStack, use either of the following procedures:

- Rebooting Cisco PNSC Without an Image, on page 20
- Rebooting Cisco PNSC by Changing the Disk Files, on page 21

Rebooting Cisco PNSC Without an Image

Use this procedure to reboot a Cisco PNSC instance in OpenStack. For more information about OpenStack, see http://docs.openstack.org/.

Procedure

Step 1 Create a flavor with the following attributes:

- Root Disk GB—20 GB
- Ephemeral Disk GB—0 GB (no ephemeral disk)

Step 2 Using either the Horizon GUI or the CLI, create one volume (vda) for Cisco PNSC and one volume (vdb) for storing imported images.
To use the CLI, enter the following commands:

```
cinder create --display-name vda-name 20
cinder create --display-name vdb-name 200
```

Step 3 Using the CLI, boot the instance and install Cisco PNSC as follows:

a) Enter the following command:

```
nova boot --flavor=flavor-id --image=image-id
--nic net-id=network-id,v4-fixed-ip=pnsc-ip
--block-device-mapping vdb=vda-id:::0 --block-device-mapping
vdc=vdb-id:::0 pnsc-image-name
```

b) When prompted to reboot after the installation, click **Stop**.

Step 4 Terminate the instance created in Step 3 to remove the instance while retaining the required two volumes.

Step 5 To boot the Cisco PNSC instance, enter the **boot** command without the `--image` parameter and using the correct volume IDs:

```
nova boot --flavor=flavor-id
--nic net-id=network-id,v4-fixed-ip=pnsc-ip
--block-device-mapping vda=vda-id:::0 --block-device-mapping
vdb=vdb-id:::0 pnsc-image-name
```

Rebooting Cisco PNSC by Changing the Disk Files

Use this procedure to reboot a Cisco PNSC instance in OpenStack. For more information about OpenStack, see http://docs.openstack.org.

Procedure

Step 1 Create a flavor with the following attributes:

- Root Disk GB—20 GB
- Ephemeral Disk GB—20 GB

The ephemeral disk will act as the Cisco PNSC system disk.

Step 2 Using either the Horizon UI or the CLI, create one volume (vdb) for storing imported images.
To use the CLI, enter the following command:

```
cinder create --display-name vdb-name 200
```

Step 3 Using the CLI, boot the instance and install Cisco PNSC by entering the following command:

```
nova boot --flavor=flavor-id --image=image-id
--nic net-id=network-id,v4-fixed-ip=pnsc-ip
--block-device-mapping vdb=volume-id:::0 pnsc-image-name
```

Step 4 When prompted, disconnect from the media source and click **Reboot**.
Cisco PNSC is then installed on the VM.

Step 5 Change the disk files by entering the following commands:

```
mv /var/lib/nova/instance-uuid/disk /var/lib/nova/instance-uuid/disk.tmp
ln -s /var/lib/nova/instance-uuid/disk.local
/var/lib/nova/instance-uuid/disk
```

CHAPTER 3

Installing the Cisco VSG

This chapter contains the following sections:

Information About the Cisco VSG

This section describes how to install and complete the basic configuration of the Cisco VSG for Cisco Nexus 1000V Switch

- Host and VM Requirements
- Cisco VSG and Supported Cisco Nexus 1000V Series Device Terminology, on page 24

Host and VM Requirements

The Cisco VSG has the following requirements:

- KVM platform with a minimum of 4 GB RAM to host a Cisco VSG VM
- Virtual Machine (VM)
    - 32-bit VM is required and “Other 2.6.x (32-bit) Linux” is a recommended VM type.
    - 2 processors (1 processor is optional.)
    - 2-GB RAM

    - 3 NICs (E1000 type)
    - Minimum of 3 GB of SCSI hard disk with LSI Logic Parallel adapter (default)
    - Minimum CPU speed of 1 GHz

- There is no dependency on the VM hardware version, so the VM hardware version can be upgraded if required.

Cisco VSG and Supported Cisco Nexus 1000V Series Device Terminology

The following table lists the terminology is used in the Cisco VSG implementation.

Term	Description
Distributed Virtual Switch (DVS)	Logical switch that spans one or more compute nodes. It is controlled by one VSM instance.
NIC	Network interface card.
Open Virtual Appliance or Application (OVA) file	Package that contains the following files used to describe a virtual machine and saved in a single archive using .TAR packaging: • Descriptor file (.OVF) • Manifest (.MF) and certificate files (optional)
Open Virtual Machine Format (OVF)	Platform-independent method of packaging and distributing Virtual Machines (VMs).
OpenStack dashboard	Provides administrators and users a graphical interface to access, provision, and automate cloud-based resources.
Virtual Ethernet Module (VEM)/Compute node	Part of the Cisco Nexus 1000V Series switch that switches data traffic. It runs on a KVM host. Up to 64 VEMs are controlled by one VSM.
Virtual Machine (VM)	Virtualized x86 PC environment in which a guest operating system and associated application software can run. Multiple VMs can operate on the same host system concurrently.
VMotion	Practice of migrating virtual machines live from server to server. (The Cisco VSGs cannot be moved by VMotion.)
vPath	Component in the Cisco Nexus 1000V Series switch with a VEM that directs the appropriate traffic to the Cisco VSG for policy evaluation. It also acts as fast path and can short circuit part of the traffic without sending it to the Cisco VSG.

Term	Description
Virtual Security Gateway (VSG)	Cisco software that secures virtual networks and provides firewall functions in virtual environments using the Cisco Nexus 1000V Series switch by providing network segmentation.
Virtual Supervisor Module (VSM)	Control software for the Cisco Nexus 1000V Series distributed virtual device that runs on a virtual machine (VM) and is based on Cisco NX-OS.

Prerequisites for Installing the Cisco VSG Software

The following components must be installed and configured:

- On the Cisco Nexus 1000V Series switch, configure three VLANs, a service VLAN, a management VLAN, and an HA VLAN on the switch uplink ports. (The VLAN does not need to be the system VLAN.)
- On the Cisco Nexus 1000V Series switch, configure three port profiles for the Cisco VSG: one for the service VLAN, one for management VLAN, and one for the HA VLAN. (You will be configuring the Cisco VSG IP address on the Cisco VSG so that the Cisco Nexus 1000V Series switch can communicate with it.)

Details about configuring VLANs and port profiles on the Cisco Nexus 1000V Series switch are available in the Cisco Nexus 1000V Series switch documentation.

Obtaining the Cisco VSG Software

You can obtain the Cisco VSG software files at this URL:

http://www.cisco.com/en/US/products/ps13095/index.html

Installing the Cisco VSG Software

You can install the Cisco VSG software on a VM by using an open virtual appliance (OVA) file or an QCOW2 image file from the CD. Depending upon the type of file that you are installing, use one of the installation methods described in the following topics

- Installing the Cisco VSG Software on OpenStack, on page 26
- Installing the Cisco VSG Software from a QCOW2 File

Installing the Cisco VSG Software on OpenStack

You can install the Cisco VSG software on a VM by using an open virtual appliance (OVA) file or an QCOW2 image file.

Before You Begin

- Specify a name for the new Cisco VSG that is unique within the inventory folder and has up to 80 characters.
- Copy the installation file (.QCOW2 or .ova file) to the OpenStack Controller Node.
- Know the name of the host where the Cisco VSG will be installed in the inventory folder.
- Know the name of the datastore in which the VM files will be stored.
- Know the names of the network port profiles used for the VM.
- Know the Cisco VSG IP address.
- Know the mode in which you will be installing the Cisco VSG:
  - Standalone
  - HA Primary
  - HA Secondary
  - Manual Installation

Procedure

Step 1 Log in to the OpenStack Controller with OpenStack administrator credentials.

Attention If you have QCOW2 installation file, skip Step 2, which converts an OVA installation file to a QCOW2 installation file. The Cisco VSG installation on KVM requires QCOW2 installation file.

Step 2 Convert the OVA file to QCOW2 format using the **qemu-img convert** command. For example:

```
h(openstack_admin)]#qemu-img convert -f vmdk -O qcow2 nexus-1000v.5.2.1.VSG2.1.3.vmdk
nexus-1000v.5.2.1.VSG2.1.3.qcow2
```

Step 3 Create an image file using the **glance image-create** command. For example:

```
h(openstack_admin)]#glance image-create --name "VSG_qcow2" --disk-format=qcow2
--container-format=bare --property architecture=i686 --property hw_vif_model=e1000 --property
 hw_disk_bus='ide' --file nexus-1000v.5.2.1.VSG2.1.3.qcow2
```

Step 4 Display the available network lists using the **neutron net-list** command. For example:

```
h(openstack_admin)]# neutron net-list
+--------------------------------------+----------+--------------------------------------------------+
| id | name | subnets |
+--------------------------------------+----------+--------------------------------------------------+
| e4532360-6918-4360-a0ff-5df293e6f4c8 | vlan1452 | 483f9a85-f0f3-4b7d-98cf-ad144ab8d249
14.52.0.0/24 |
| 0ae7059c-4437-4ee4-b2e1-f38560ed00b4 | vlan1455 | 82bbefa3-b676-41ce-aff0-f0858faab088
14.55.0.0/24 |
| 9118659f-84c4-49d3-adb2-e5b0a01b24fc | vlan1454 | 1cc89224-8358-4f7f-961d-3b959db72c7d
```

```
14.53.0.0/24 |
| 02227127-69b9-41eb-bae4-9532f6bcb8af | vlan1453 | 351656db-83ba-48cb-bade-78feacfd4879
14.53.0.0/24 |
+--------------------------------------+----------+------------------------------------------------------------+
```

Step 5 Display the Cisco policy profile list using the **neutron cisco-policy-profile-list** command. For example:

```
h(openstack_admin)]# neutron cisco-policy-profile-list
+--------------------------------------+-------------+
| id | name |
+--------------------------------------+-------------+
| c64131c5-652b-4ac7-89b2-dfffa1a482a3 | pp3 |
| b95f931d-f09f-4236-90cf-a33df3be4437 | pp4 |
| cf394dae-7665-4b3a-88f0-99cc8517f457 | dummy |
| c336d13c-1e85-4935-9d9f-c073c22fdc08 | default-pp |
+--------------------------------------+-------------+
```

Step 6 Create a port using the **neutron port-create** *net-list_ name* **—***n1kv:profile cisco-policy-profile-list_ID* command. For example:

```
h(openstack_admin)]#neutron port-create vlan1452 --n1kv:profile
c336d13c-1e85-4935-9d9f-c073c22fdc08
Created a new port:
+--------------------+----------------------------------------------------------------------------------+
| Field | Value |
+--------------------+----------------------------------------------------------------------------------+
| admin_state_up | True |
| allowed_address_pairs | |
| binding:host_id | |
| binding:profile | {} |
| binding:vif_details | {} |
| binding:vif_type | unbound |
| binding:vnic_type | normal |
| device_id | |
| device_owner | |
| fixed_ips | {"subnet_id": "483f9a85-f0f3-4b7d-98cf-ad144ab8d249", "ip_address": "14.52.0.5"}
 |
| id | 44b424db-55bc-48a0-a7e0-f8dd679b2093 |
| mac_address | fa:16:3e:98:be:05 |
| n1kv:profile | c336d13c-1e85-4935-9d9f-c073c22fdc08 |
| name | |
| network_id | e4532360-6918-4360-a0ff-5df293e6f4c8 |
| security_groups | cb0453c4-9b79-4899-911c-68563853659f |
| status | DOWN |
| tenant_id | 24c4e9637f6f4a0589eca8b129841664 |
+----------------------+------------------------------------------------------------------------------+
```

Step 7 Launch the Cisco VSG VM on the Cisco Nexus 1000V using the **nova boot VSG-VM** command. For example:

```
h(openstack_admin)]# nova boot VSG-large-p --flavor VSG-large --image
6bc75d1e-b9e0-49dc-94da-7404f8067e8b --nic port-id=32b8862c-cc9f-4a66-ac8b-6911aeddb114
--nic port-id=bc364ae5-7218-4d56-8758-55f683ae08e1  --nic
port-id=085a0881-8774-4242-9500-7fbb9b91939f
+--------------------------------------+---------------------------------------------------+
| Property                             | Value
|
+--------------------------------------+---------------------------------------------------+
| OS-DCF:diskConfig                    | MANUAL
|
| OS-EXT-AZ:availability_zone          | nova
```

```
|
| OS-EXT-SRV-ATTR:host                 | -
|
| OS-EXT-SRV-ATTR:hypervisor_hostname  | -
|
| OS-EXT-SRV-ATTR:instance_name        | instance-0000000b
|
| OS-EXT-STS:power_state               | 0
|
| OS-EXT-STS:task_state                | scheduling
|
| OS-EXT-STS:vm_state                  | building
|
| OS-SRV-USG:launched_at               | -
|
| OS-SRV-USG:terminated_at             | -
|
| accessIPv4                           |
|
| accessIPv6                           |
|
| adminPass                            | xyJKcwTH2DbR
|
| config_drive                         |
|
| created                              | 2015-03-27T09:24:44Z
|
| flavor                               | VSG-large (08dfe7b7-f77b-424b-a4aa-6bfd4c53a227)
|
| hostId                               |
|
| id                                   | a8eb1b99-e03e-4acc-9bf3-ab17a01a07fb
|
| image                                | VSG_REL (6bc75d1e-b9e0-49dc-94da-7404f8067e8b)
|
| key_name                             | -
|
| metadata                             | {}
|
| name                                 | VSG-large-p
|
| os-extended-volumes:volumes_attached | []
|
| progress                             | 0
|
| security_groups                      | default
|
| status                               | BUILD
|
| tenant_id                            | 24c4e9637f6f4a0589eca8b129841664
|
| updated                              | 2015-03-27T09:24:44Z
|
| user_id                              | 9476dd26b5ff41bb8152124b3b9f63cb
|
+-------------------------------------+-------------------------------------------------+
[root@macf872eaa3d77e home(openstack_admin)]#
```

Step 8 Open the OpenStack GUI dashboard.

Step 9 Click **Instances**.

Step 10 In the **Instances** pane, note the IP Address of the launched VSG VM instance.

Step 11 In the **OpenStack** Dashboard, locate the newly created VM and choose **More** > **Console** to start the VSG installation procedure.

Step 12 Click the **Console** tab to view the VM console. Wait for the Install Virtual Firewall and bring up the new image to boot. See the *Configuring Initial Settings* section to configure the initial settings on the Cisco VSG.

Configuring Initial Settings

This section describes how to configure the initial settings on the Cisco VSG and configure a standby Cisco VSG with its initial settings. For configuring a standby Cisco VSG, see Configuring Initial Settings on a Standby Cisco VSG, on page 31 section.

When you power on the Cisco VSG for the first time, depending on which mode you used to install your Cisco VSG, you might be prompted to log in to the Cisco VSG to configure initial settings at the console of your OpenStack dashboard. For details about installing Cisco VSG, see Installing the Cisco VSG Software, on page 25.

Before You Begin

The following table determines if you must configure the initial settings as described in this section.

Your Cisco Virtual Security Gateway Software Installation Method	Do You Need to Proceed with “Configuring Initial Settings”?
Installing an OVA file and choosing Manually Configure Nexus 1000 VSG in the configuration field during installation.	Yes. Proceed with configuring initial settings described in this section.
Installing an OVA file and choosing any of the options other than the manual method in the configuration field during installation.	No. You have already configured the initial settings during the OVA file installation.
Installing an QCOW2 file.	Yes. Proceed with configuring initial settings described in this section.

Procedure

Step 1 Navigate to the **Console** tab in the VM.

Cisco Nexus 1000V Series switch opens the **Console** window and boots the Cisco VSG software.

Step 2 At the `Enter the password for "admin"` prompt, enter the password for the admin account and press **Enter**.

Step 3 At the prompt, confirm the admin password and press **Enter**.

Step 4 At the `Enter HA role[standalone/primary/secondary]` prompt, enter the HA role you want to use and press **Enter**.
This can be one of the following:

- standalone
- primary
- secondary

Step 5 At the `Enter the ha id(1-4095)` prompt, enter the HA ID for the pair and press **Enter**.

Note If you entered secondary in the earlier step, the HA ID for this system must be the same as the HA ID for the primary system.

Step 6 If you want to perform basic system configuration, at the `Would you like to enter the basic configuration dialog (yes/no)` prompt, enter **yes** and press **Enter**, then complete the following steps.

a) At the `Create another login account (yes/no)[n]` prompt, do one of the following:

- To create a second login account, enter **yes** and press **Enter**.
- Press **Enter**.

b) (Optional) At the `Configure read-only SNMP community string (yes/no)[n]` prompt, do one of the following:

- To create an SNMP community string, enter **yes** and press **Enter**.
- Press **Enter**.

c) At the `Enter the Virtual Security Gateway (VSG) name` prompt, enter **VSG-demo** and press **Enter**.

Step 7 At the `Continue with Out-of-band (mgmt0) management configuration? (yes/no)[y]:` prompt, enter **yes** and press **Enter**.

Step 8 At the `Mgmt IPv4 address:` prompt, enter **10.10.10.11** and press **Enter**.

Step 9 At the `Mgmt IPv4 netmask` prompt, enter **255.255.255.0** and press **Enter**.

Step 10 At the `Configure the default gateway? (yes/no)[y]` prompt, enter **yes** and press **Enter**.

Step 11 At the `Configure the DNS IPv4 address? (yes/no)[n]:` prompt, enter **no** and press **Enter**.

Step 12 At the `Enable the telnet service? (yes/no)[y]:` prompt, enter **no**.

Step 13 At the `Configure the ntp server? (yes/no)[n]` prompt, enter **no** and press **Enter**.

Step 14 At the `Continue with Policy Agent Configuration? (yes/no)[y]` prompt, enter **yes** and press **Enter**.

a) At the `vnmc IPv4 address:` prompt, enter the registration IPv4 address and press **Enter**.
b) At the `Policy agent shared secret string:` prompt, enter a secret string and press **Enter**.
c) At the `Policy agent image name[vnmc-vsgpa.2.1.3.bin]:` prompt, press **Enter**.

The following configuration will be applied:

```
hostname vsg
nsc-policy-agent
    registration-ip 16.0.9.7
    shared-secret  ******
    policy-agent-name bootflash:/vnmc-vsgpa.2.1.3.bin
no telnet server enable
ssh key rsa 2048 force
ssh server enable
feature http-server
ha-pair id 1
```

Step 15 At the `Would you like to edit the configuration? (yes/no)[n]` prompt, enter **n**and press **Enter**.

Step 16 At the `Use this configuration and save it? (yes/no)[y]`**:** prompt, enter **y** and press **Enter**.

Step 17 At the `VSG login` prompt, enter the name of the admin account you want to use and press **Enter**.
The default account name is `admin`.

Step 18 At the `Password` prompt, enter the name of the password for the admin account and press **Enter**.
You are now at the Cisco VSG node.

Configuring Initial Settings on a Standby Cisco VSG

You can add a standby Cisco VSG by logging in to the Cisco VSG you have identified as secondary and using the following procedure to configure a standby Cisco VSG with its initial settings.

Procedure

Step 1 Navigate to the **Console** tab in the VM.
Cisco Nexus 1000V Series switch opens the **Console** window and boots the Cisco VSG software.

Step 2 At the `Enter the password for "admin"` prompt, enter the password for the admin account and press **Enter**.

Step 3 At the prompt, confirm the admin password and press **Enter**.

Step 4 At the `Enter HA role[standalone/primary/secondary]` prompt, enter the secondary HA role and press **Enter**.

Step 5 At the `Enter the ha id(1-4095)` prompt, enter **25** for the HA pair id and press **Enter**.

Note The HA ID uniquely identifies the two Cisco VSGs in an HA pair. If you are configuring Cisco VSGs in an HA pair, make sure that the ID number you provide is identical to the other Cisco VSG in the pair.

Step 6 At the `VSG login` prompt, enter the name of the admin account you want to use and press **Enter**.
The default account name is `admin`.

Step 7 At the `Password` prompt, enter the name of the password for the admin account and press **Enter**.
You are now at the Cisco VSG node.

Verifying the Cisco VSG Configuration

To display the Cisco VSG configuration, perform one of the tasks:

Command	Purpose
show interface brief	Displays brief status and interface information.
show vsg	Displays the Cisco VSG and system-related information.

This example shows how to verify the Cisco VSG configurations:

```
vsg# show interface brief
--------------------------------------------------------------------------------
Port     VRF          Status IP Address                            Speed    MTU
--------------------------------------------------------------------------------
mgmt0    --           up     10.193.77.217                         1000     1500


vsg# show vsg
Model: VSG
HA ID: 111
VSG software version: 5.2(1)VSG2(1.3) build [5.2(1)VSG2(1.3)]
NSC IP: 14.52.0.9
NSC PA version: 2.1(2a)-vsg
```

Where to Go Next

After installing and completing the initial configuration of the Cisco VSG, you can configure firewall policies on the Cisco VSG through the Cisco PNSC.

CHAPTER 4

Registering Devices with the Cisco Prime NSC

This chapter contains the following sections:

Registering a Cisco VSG

You can register Cisco VSG with Cisco PNSC. Registration enables communication between the Cisco VSG and the Cisco PNSC.

Procedure

Step 1 Copy the vnmc-vsgpa.2.1.3.bin file into the Cisco VSG bootflash:

```
vsg# copy ftp://guest@172.18.217.188/n1kv/vnmc-vsgpa.2.1.3.bin bootflash
```

Step 2 Enter global configuration mode.

```
vsg# configure
```

Step 3 Enter nsc-policy-agent mode.

```
vsg (config)# nsc-policy-agent
```

Step 4 Set the Cisco PNSC registration IP address.

```
vsg (config-nsc-policy-agent)# registration-ip 209.165.200.225
```

Step 5 Specify the shared-secret of Cisco PNSC.

```
vsg (config-nsc-policy-agent)#
shared-secret ********
```

Step 6 Install the policy agent.

```
vsg (config-nsc-policy-agent)#
policy-agent-image bootflash: vnmc-vsgpa.2.1.3.bin
```

Step 7 Exit all modes.

```
vsg (config-nsc-policy-agent)# end
```

Step 8 On the Cisco VSG command line, display the NSC PA status:

```
vsg# show nsc-pa status
If registration was successful, you should see the following message:
```

```
"NSC Policy-Agent status is - Installed Successfully. Version 2.1(3)-vsg"
The Cisco VSG registration is complete.
```

Step 9 Copy the running configuration to the startup configuration:

```
vsg# copy running-config startup-config
Executing this command ensures that the registration becomes part of the basic configuration
```

Registering Cisco Nexus 1000V VSM

You can register Cisco Nexus 1000V with Cisco PNSC. Registration enables communication between the Cisco Nexus 1000V VSM and Cisco PNSC.

Procedure

Step 1 Copy the vsmcpa.3.2.2b.bin file into the VSM bootflash:

```
vsm# copy ftp://guest@172.18.217.188/n1kv/vsmcpa.3.2.2b.bin bootflash:
```

Step 2 Enter global configuration mode.

```
vsm# configure
```

Step 3 Enter config nsc-policy-agent mode.

```
vsm(config)# nsc-policy-agent
```

Step 4 Set the Cisco PNSC registration IP address.

```
vsm(config-nsc-policy-agent)# registration-ip 209.165.200.226
```

Step 5 Specify the shared-secret of Cisco PNSC.

```
vsm(config-nsc-policy-agent)# shared-secret ********
```

Step 6 Install the policy agent.

```
vsm(config-nsc-policy-agent)# policy-agent-image bootflash:vsmcpa.3.2.2b.bin
```

Step 7 Exit all modes.

```
vsm(config-nsc-policy-agent)# top
```

Step 8 Display the NSC PA status:

```
vsm# show nsc-pa status
If registration was successful, you should see the following message:
NSC Policy-Agent status is - Installed Successfully. Version 3.2(2b)-vsg
The Cisco Nexus 1000V VSM registration is complete.
```

Step 9 Copy the running configuration to the startup configuration:

```
vsm# copy running-config startup-config
Executing this command ensures that the registration becomes part of the basic configuration.
```

What to Do Next

See the *Cisco Virtual Management Center CLI Configuration Guide* for detailed information about configuring the Cisco PNSC using the CLI.