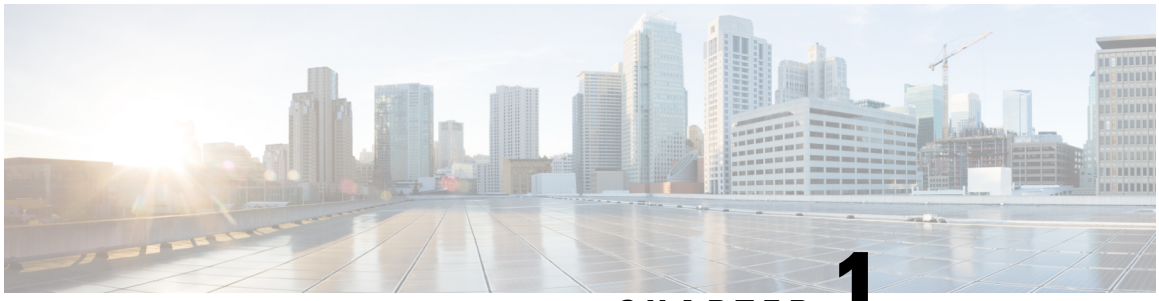
Cisco VSG for VMware vSphere, Release 5.2(1)VSG2(2.2) and Cisco Prime NSC, Release 3.5.1a Installation Guide

First Published: 2018-07-10

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

Overview

This chapter contains the following sections:

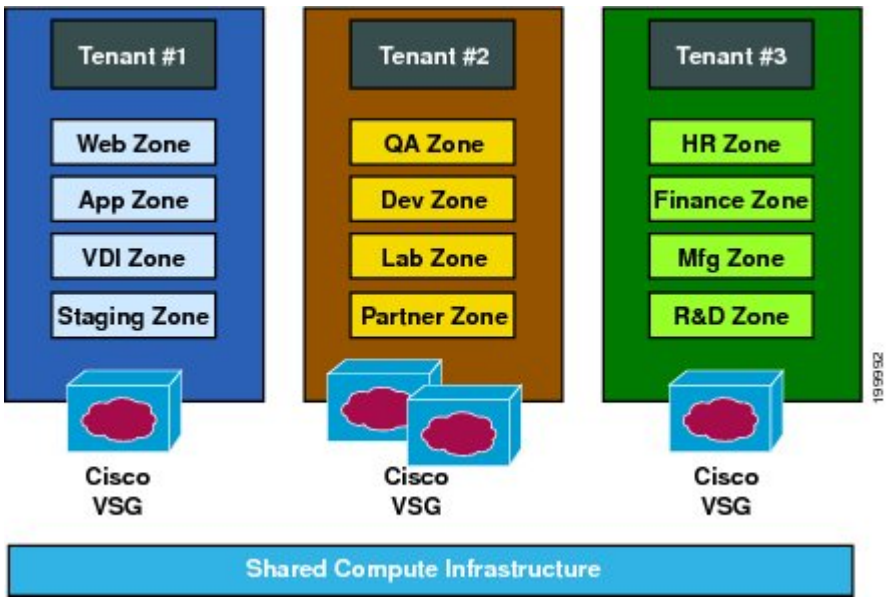
Information About Installing the Cisco PNSC and the Cisco VSG

You must install the Cisco Prime Network Services Controller (Cisco PNSC) and the Cisco Virtual Security Gateway (Cisco VSG) in a particular sequence on the Cisco Nexus 1000VE switch in order to have a functioning virtual system. For the critical sequence information that you need for a successful installation on the Cisco Nexus 1000VE switch, see Chapter 2, *Installing the Cisco VSG and the Cisco PNSC Quick Start*. .

Information About Cisco VSG

The Cisco VSG is a virtual firewall appliance that provides trusted access to virtual data center 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.

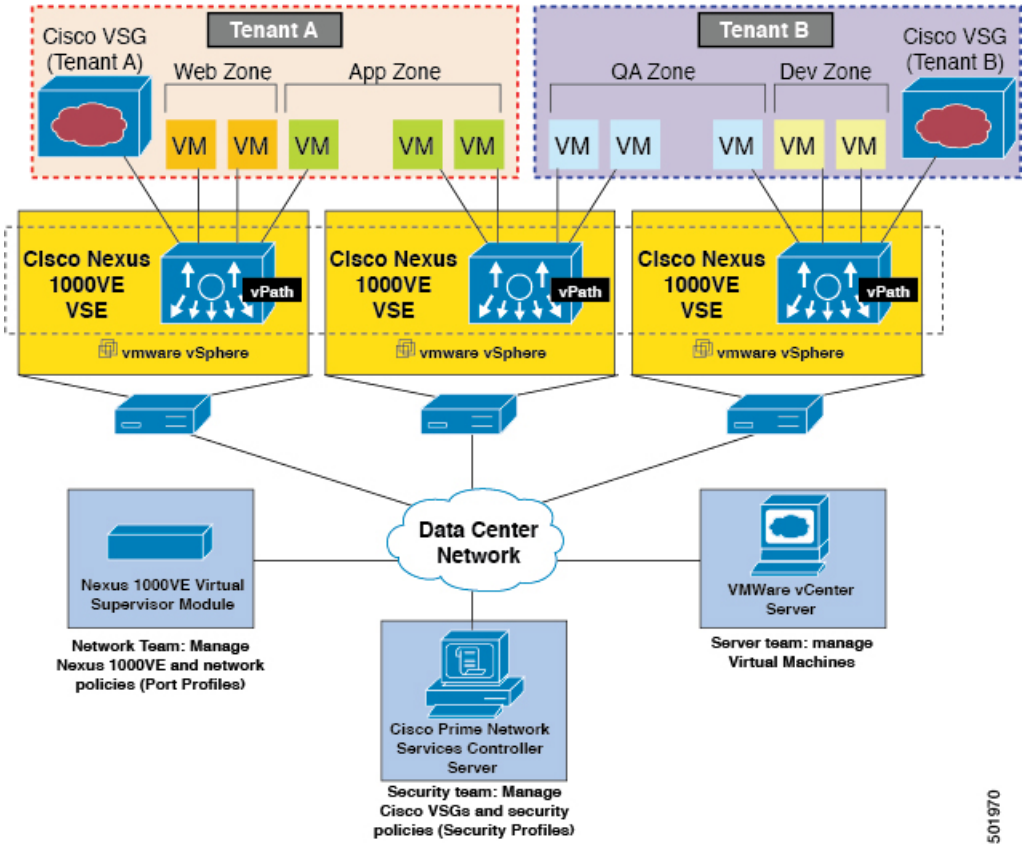
Figure 1: Trusted Zone-Based Access Control Using Per-Tenant Enforcement with the Cisco VSG



Cisco PNSC and Cisco VSG Architecture

The Cisco VSG operates with the Cisco Nexus 1000VE Series switch in the VMware vSphere Hypervisor and the Cisco VSG leverages the virtual network service data path (Cisco vPath). 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 offloads policy enforcement of the remaining packets to vPath.

Figure 2: Cisco Virtual Security Gateway Deployment Topology



Cisco 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 VSE 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 vPath Virtual Service Engine(VSEs), the Cisco VSG enhances security performance through distributed 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

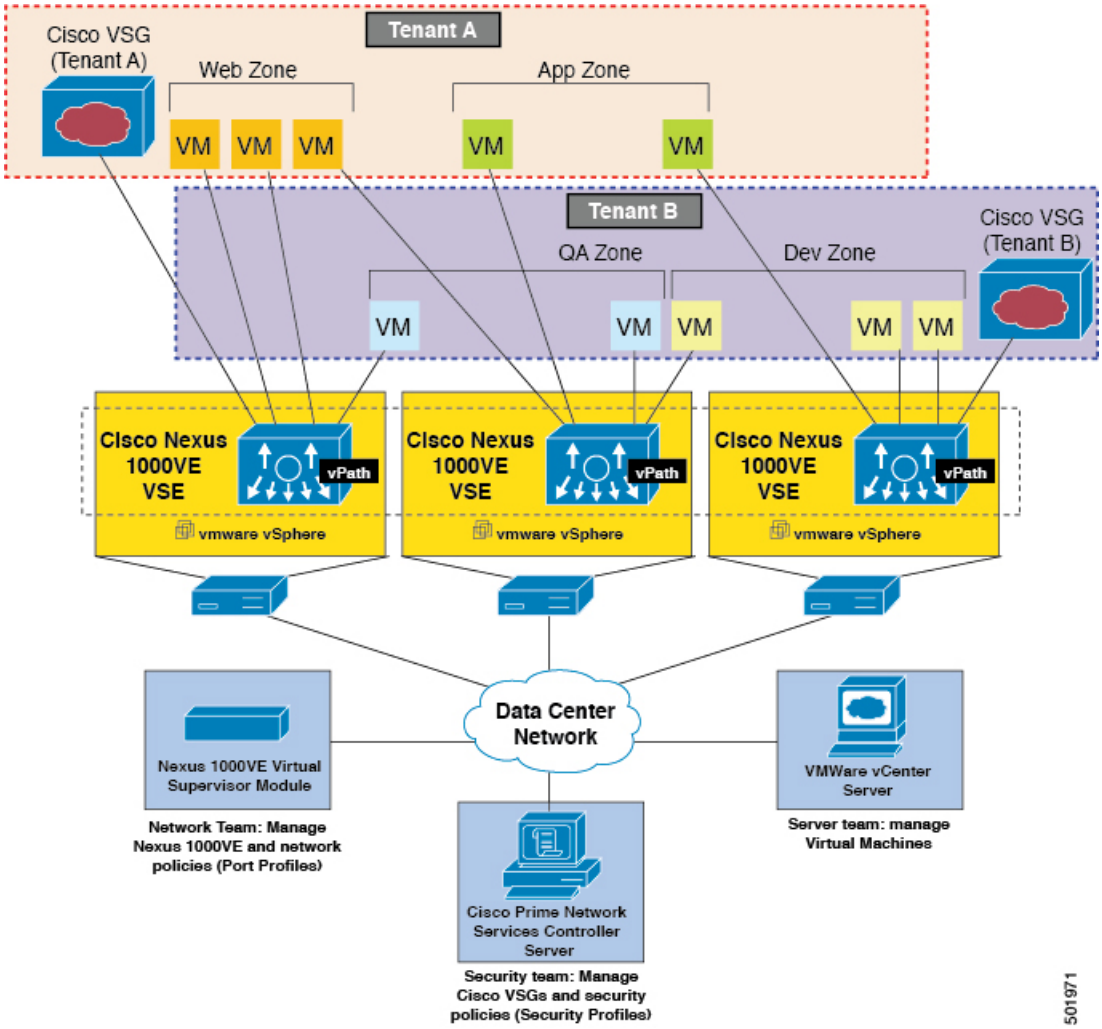
You can transparently insert a Cisco VSG into the VMware vSphere environment where the Cisco Nexus 1000VE is deployed. One or more instances of the Cisco VSG is deployed on a per-tenant basis, which allows a highly scale-out deployment across many tenants. Tenants are isolated from each other, so no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

As you instantiate VMs for a given tenant, their association to security profiles (or zone membership) occurs immediately through binding with the Cisco Nexus 1000VE protected 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 because a VLAN often identifies a tenant boundary. The Cisco VSG evaluates access control rules and then offloads enforcement to the Cisco Nexus 1000VE VSE vPath module. Upon enforcement, the Cisco Nexus 1000VE 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 dynamic, 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 1000VE (and 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 1000VE port profile (authored on the Cisco Nexus 1000VE Virtual Supervisor Module (VSM) and published to the VMware vCenter.

When a new VM is instantiated, the server administrator assigns appropriate port 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. You can repurpose a VM by assigning it to a different port profile or security profile.

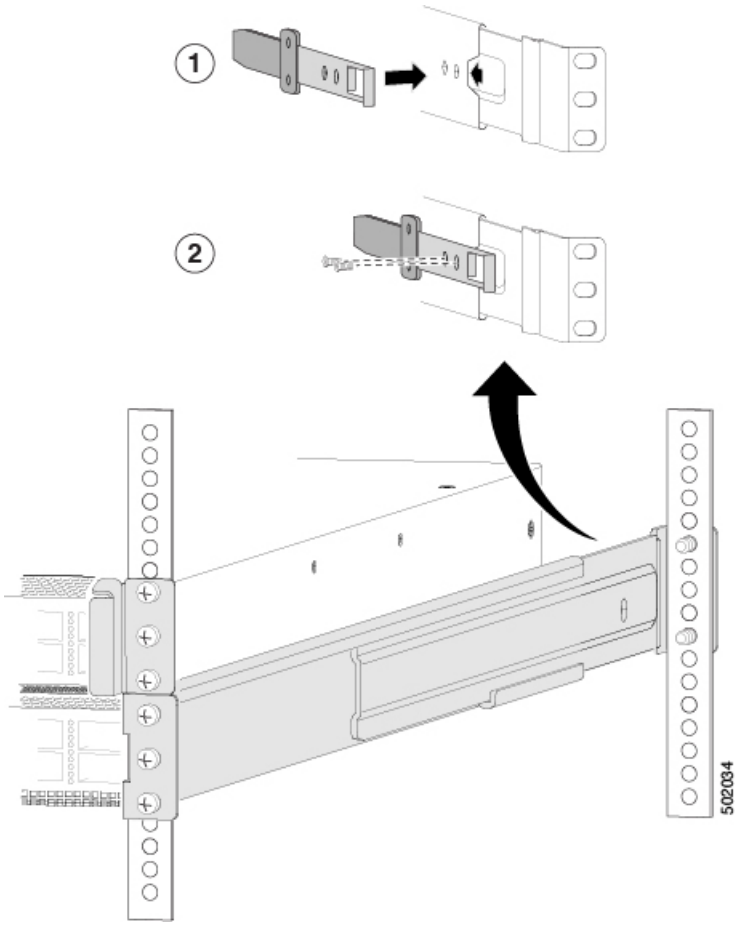
As VMotion events are triggered, VMs move across physical servers. Because the Cisco Nexus 1000VE ensures that port profile policies follow the VMs, associated security profiles also follow these moving VMs, and security enforcement and monitoring remain transparent to VMotion events.

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 vPath component in the Cisco Nexus 1000VE VSE 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 1000VE VSE and Cisco VSG. All the Cisco VSG data interfaces are part of the service VLAN and the VSE uses this VLAN for its interaction with Cisco VSG.
- The management VLAN connects the management platforms such as the VMware vCenter, the Cisco PNSC, the Cisco Nexus 1000VE VSM, and the managed Cisco VSGs. The Cisco VSG management vNIC is part of the management VLAN.
- 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 multitenant 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 1000VE Series switch. Designed for multitenant 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 Multitenancy 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 multitenant 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 subcomponents.

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:

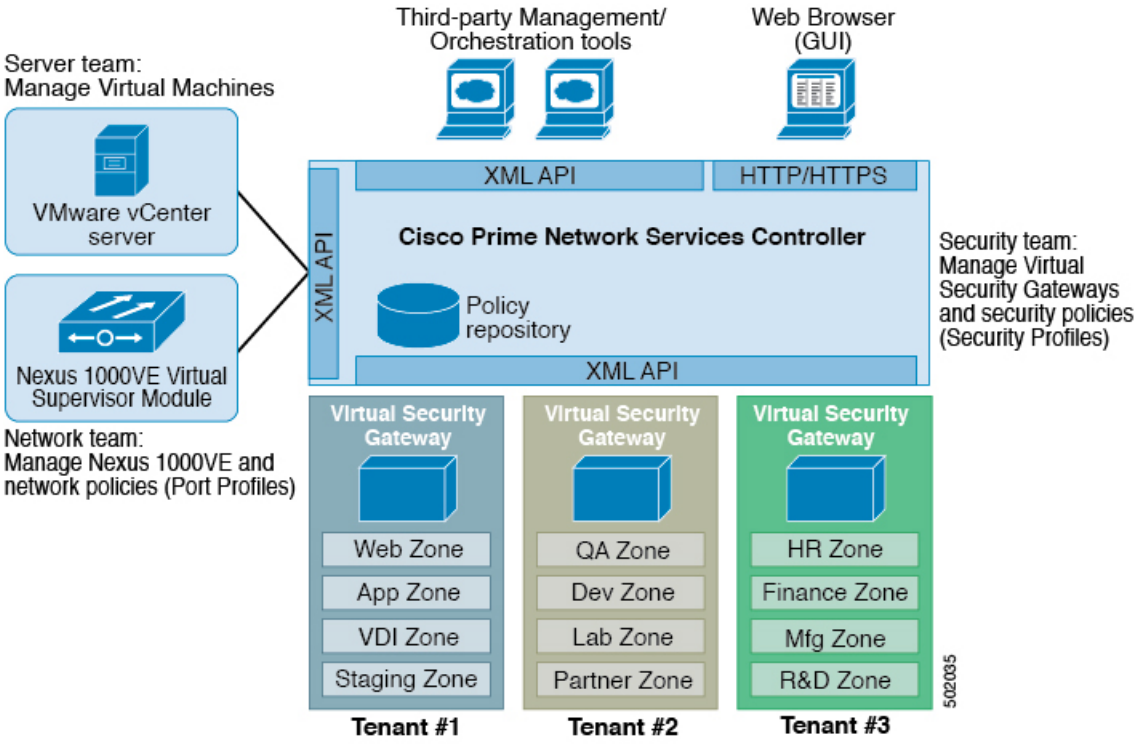
- A centralized repository for managing security policies (security templates) and object configurations that allow managed devices to be stateless.
- A centralized resource management function that manages pools of devices that are commissioned and pools of devices that are available for commissioning.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



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 multitenant 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.

Cisco PNSC and Cisco VSG

The Cisco PNSC operates with the Cisco Nexus 1000VE Series VSM to achieve the following scenarios:

- Security administrators who author and manage security profiles as well as manage Cisco VSG instances. Security profiles are referenced in Cisco Nexus 1000VE Series port profiles through the Cisco PNSC interface.
- Network administrators who author and manage port profiles as well as manage Cisco Nexus 1000VE Series switches. Port profiles are referenced in the vCenter through the Cisco Nexus 1000VE Series VSM interface.
- Server administrators who select the appropriate port profiles in the vCenter when instantiating a virtual machine.

System Requirements

For Cisco PNSC installation system requirement, see Installing Cisco Prime Network Services Controller, on page 43.

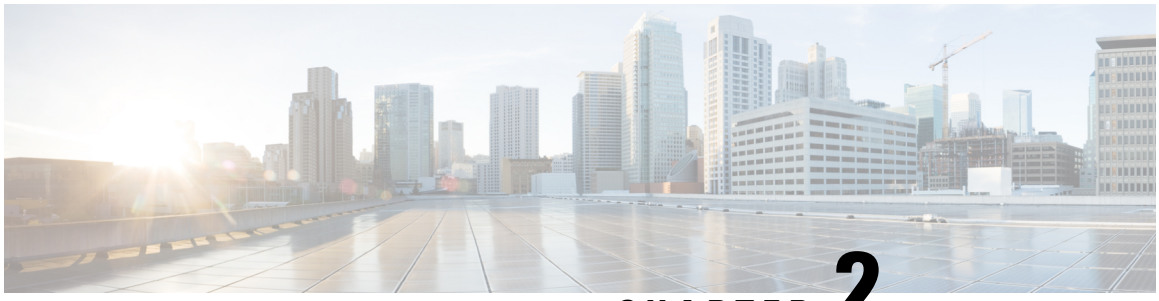
Information About High Availability

VMware high availability (HA) provides a base level of protection for a Cisco VSG VM by restarting it on another host in the HA cluster. With VMware HA, data is protected through a shared storage. The Cisco PNSC services can be restored in a few minutes. Transient data such as user sessions is not preserved in the service transfer. Existing users or service requests must be reauthenticated.

Requirements for supporting VMware HA in Cisco PNSC are as follows:

- At least two hosts per HA cluster
- VM and configuration files located on the shared storage and hosts are configured to access that shared storage

For additional details, see the VMware guides for HA and fault tolerance.



CHAPTER 2

Installing the Cisco VSG and the Cisco Prime NSC-Quick Start

This chapter contains the following sections:

Information About Installing the Cisco PNSC and the Cisco VSG

This chapter describes how to install and set up a basic working configuration of the Cisco PNSC and Cisco VSG. The example in this chapter uses the OVF template method to install the OVA files of the software. The steps assume that the Cisco Nexus 1000VE Series switch is operational, and endpoint VMs are already installed.

Cisco VSG and Cisco PNSC Installation Planning Checklists

Planning the arrangement and architecture of your network and equipment is essential for a successful operation of the Cisco PNSC and Cisco VSG.

Basic Hardware and Software Requirements

The following table lists the basic hardware and software requirements for Cisco VSG and Cisco PNSC installation.

The Cisco VSG software is available for download at http://www.cisco.com/en/US/products/ps13095/index.html and the Cisco PNSC software is available for download at http://www.cisco.com/en/US/products/ps13213/index.html.

Requirement	Description
Two Virtual CPUs	1.5 GHz for each Virtual CPU
Memory	4 GB RAM for the Cisco VSG and 4 GB RAM for the Cisco PNSC or 8 GB for both

Disk Space	One of the following, depending on InterCloud functionality:
	• With InterCloud functionality, 220 GB on shared network file storage (NFS) or storage area network (SAN), and configured on two disks as follows:
	  • Disk 1: 20 GB
	  • Disk 2: 200 GB
	• Without InterCloud functionality, 40 GB on shared NFS or SAN, and configured on two disks as follows:
	  • Disk 1: 20 GB
	  • Disk 2: 20 GB

Processor	x86 Intel or AMD server with a 64-bit processor listed in the VMware compatibility matrix. **Note** You can find VMware compatibility guides at http://www.vmware.com/resources/compatibility/search.php.
VMware vSphere	Cisco VSG is supported on ESXi 6.5
VMware vCenter	Release 6.5
Intel Virtualization Technology (VT)	Enabled in the BIOS

Requirement	Description
Browser	Any of the following browsers: • Internet Explorer 9.0 or higher • Mozilla Firefox 23.0 or higher • Google Chrome 29.0 or higher **Note** If you are running Firefox or IE and do not have Flash, or you have a version of Flash that is older than 11.2, a message displays asking you to install Flash and provides a link to the Adobe website. **Note** Before using Google Chrome with Cisco PNSC, you must disable the Adobe Flash Players that are installed by default with Chrome.
Ports	Access to the Cisco PNSC application using a web browser and the following ports (if the deployment uses a firewall, make sure to permit the following ports): • 443 (HTTPS) • 80 (HTTP/TCP) • 843 (Adobe Flash)
Flash Player	Adobe Flash Player plugin 11.2 or higher

License Requirements

Cisco VSG license is integrated with the Nexus1000VE Multi-Hypervisor License. You need to install the Nexus1000VE Multi-Hypervisor License for Cisco VSG for VMware vSphere. The Cisco Nexus1000VE VSM is available in two modes: essential and advanced. VSG functionality is available only in the advanced mode. You need to install the Nexus1000VE Multi-Hypervisor License and change the VSM mode to advanced mode. When the Nexus1000VE Multi-Hypervisor License is installed, the license for Cisco VSG is automatically included.

The Nexus1000VE Multi-Hypervisor License is available in three different types:

- Default: The Nexus 1000VE switch may be configured in Essential or Advanced mode.
  - Essential Mode: Not Supported.
  - Advanced Mode: After upgrading the software, Nexus1000VE Multi-Hypervisor License is available with 1024 Socket Count and expires in 60 days.

Note You have to request for an evaluation or permanent Nexus1000VE Multi-Hypervisor License.

Note You must install either the evaluation or the permanent (NEXUS1000VE_LAN_SERVICES_PKG) license prior to upgrading to the latest software.

- Evaluation: The Nexus 1000VE solution should be in Advanced mode. After upgrading the software, Nexus1000VE Multi-Hypervisor License is available with1024 Socket Count and expires in 60 days.
- Permanent: The Nexus 1000VE switch should be in Advanced mode. After upgrading the software, Nexus1000VE Multi-Hypervisor License is available with 1024 Socket Count and expires in 60 days.

For more information about the Cisco Nexus 1000VE for VMware vSphere licenses, see the *Cisco Nexus 1000VE for VMware vSphere License Configuration Guide*.

VLAN Configuration Requirements

Follow these VLAN requirements to prepare the Cisco Nexus 1000VE Series switch for further installation processes:

- You must have two VLANs that are configured on the Cisco Nexus 1000VE Series switch uplink ports: the service VLAN and an HA VLAN (the VLAN does not need to be the system VLAN).
- You must have two port profiles that are configured on the Cisco Nexus 1000VE Series switch: one port profile for the service VLAN and one port profile for the HA VLAN (you will be configuring the Cisco VSG IP address on the Cisco VSG so that the Cisco Nexus 1000VE Series switch can communicate with it)

Required Cisco PNSC and Cisco VSG Information

The following information can be used later during the Cisco PNSC and Cisco VSG installation.

Type	Your Information
Cisco VSG name—Unique within the inventory folder and up to 80 characters	
Hostname—Where the Cisco VSG will be installed in the inventory folder	
Datastore name—Where the VM files will be stored	
Cisco VSG management IP address	
VSM management IP address	
Cisco PNSC instance IP address	

Type	Your Information
Mode for installing the Cisco VSG	• Standalone • HA primary • HA secondary
Cisco VSG VLAN number • Service (1) • Management (2) • High availability (HA) (3)	
Cisco VSG port profile name • Data (1) • Management (2) • High availability (HA) (3) **Note** The numbers indicate the VSG port profile that must be associated with the VSG VLAN number.	
HA pair ID (HA domain ID)	
DNS IP address	
NTP IP address	
Cisco VSG admin password	
Cisco PNSC admin password	
Cisco VSM admin password	
Shared secret password (Cisco PNSC, Cisco VSG policy agent, Cisco VSM policy agent)	

Tasks and Prerequisites Checklist

Tasks	Prerequisites
Task 1: Installing the Cisco PNSC from an OVA Template, on page 19	Make sure that you know the following: • The Cisco PNSC OVA image is available in the vCenter. • Know the IP/subnet mask/gateway information for the Cisco PNSC. • Know the admin password, shared_secret, hostname that you want to use. • Know the DNS server and domain name information. • Know the NTP server information. • Know the management port-profile name for the Virtual Machine (VM) (management). **Note** The management port profile is the same port profile that is used for the Virtual Supervisor Module (VSM). The port profile is configured in the VSM and is used for the Cisco PNSC management interface. • Make sure that all system requirements are met as specified in System Requirements. • A shared secret password is available (this password enables communication between the Cisco PNSC, VSM, and Cisco VSG).
Task 2: On the Cisco PNSC, Setting Up VM-Manager for vCenter Connectivity, on page 21	Make sure that you know the following: • Supported Adobe Flash Player given in System Requirements, on page 9 • IP address of the Cisco PNSC • The password for Admin user

Tasks	Prerequisites
Task 3: On the VSM, Configuring the Cisco PNSC Policy Agent, on page 21	Make sure that you know the following: • The Cisco PNSC policy-agent image is available on the VSM (for example, vsmcpa.3.2.3a.bin) **Note** The string **vsmcpa** must appear in the image name as highlighted. • The IP address of the Cisco PNSC • The shared secret password you defined during the Cisco PNSC installation • That IP connectivity between the VSM and the Cisco PNSC is working **Note** If you upgrade your VSM, you must also copy the latest Cisco VSM policy agent image. This image is available in the Cisco PNSC image bundle to boot from a flash drive and to complete registration with the Cisco PNSC.
Task 4: On the VSM, Preparing Cisco VSG Port Profiles, on page 23	Make sure that you know the following: • The uplink port-profile name. • The VLAN ID for the Cisco VSG data interface (for example,100). • The VLAN ID for the Cisco VSG-ha interface (for example, 200). • The management VLAN (management). **Note** None of these VLANs need to be system VLANs.

Tasks	Prerequisites
Task 5: Installing the Cisco VSG from an OVA Template, on page 24	Make sure that you know the following: • The Cisco VSG OVA image is available in the vCenter. • Cisco VSG-Data and Cisco VSG-ha port profiles are created on the VSM. • The management port profile (management) **Note** The management port profile is the same port profile that is used for the VSM. The port profile is configured in the VSM and is used for the Cisco PNSC management interface. • The Cisco VSG-Data port profile: VSG-Data • The Cisco VSG-ha port profile: VSG-ha • The HA ID • The IP/subnet mask/gateway information for the Cisco VSG • The admin password • 2 GB RAM and 3 GB hard disk space are available • The Cisco PNSC IP address • The shared secret password • The IP connectivity between Cisco VSG and Cisco PNSC is okay. • The Cisco VSG NSC-PA image name (nsc-vsgpa.2.1.3i.bin) is available.
Task 6: On the Cisco VSG and Cisco PNSC, Verifying the NSC Policy-Agent Status, on page 27	—
Task 7: On the Cisco PNSC, Configuring a Tenant and Security Profile, on page 27	Make sure that you know the following: • Supported Adobe Flash Player given in System Requirements, on page 9 • The IP address of the Cisco PNSC • The password for Admin user
Task 8: On the Cisco PNSC, Importing Service Image, on page 32	—
Task 10: On the Cisco PNSC, Configuring a Permit-All Rule, on page 35	—

Tasks	Prerequisites
Task 11: On the Cisco VSG, Verifying the Permit-All Rule, on page 36	—
Task 12: Enabling Logging, on page 36	—
Task 13: Enabling the Traffic VM Port-Profile for Firewall Protection and Verifying the Communication Between the VSM, VSE, and VSG, on page 37	Make sure that you know the following: • The server virtual machine that runs with an access port profile (for example, web server) • The Cisco VSG data IP address (for example, 10.10.10.200) and VLAN ID (100) • The security profile name (for example, sp-web) • The organization (Org) name (for example, root/Tenant-A) • The port profile that you would like to edit to enable firewall protection • That one active port in the port-profile with vPath configuration has been set up
Task 14: Sending Traffic Flow and on the Cisco VSG Verifying Statistics and Logs, on page 39	—

Host Requirements

- ESXi platform that runs VMware software release 6.5 with a minimum of 4 GB physical RAM for the Cisco VSG and 4 GB physical RAM for the Cisco PNSC.
- 1 processor
- Four Virtual CPUs with speed of 1.5 GHz for each virtual CPU

Obtaining the Cisco PNSC and the Cisco VSG Software

The Cisco VSG software is available for download at the following URL:

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

The Cisco PNSC software is available for download at the following URL:

http://www.cisco.com/en/US/products/ps13213/index.html

Task 1: Installing the Cisco PNSC from an OVA Template

Before you begin

Know the following:

- The Cisco PNSC OVA image is available in the vCenter.

- Know the IP/subnet mask/gateway information for the Cisco PNSC.
- Know the admin password, shared_secret, hostname that you want to use.
- Know the DNS server and domain name information.
- Know the NTP server information.
- Know the management port-profile name for the Virtual Machine (VM) (management).

Note The management port profile is the same port profile that is used for the Virtual Supervisor Module (VSM). The port profile is configured in the VSM and is used for the Cisco PNSC management interface.

- Make sure that all system requirements are met as specified in System Requirements.
- A shared secret password is available (this password enables communication between the Cisco PNSC, VSM, and Cisco VSG).

Step 1 Use the VMware vSphere Client to log into the vCenter server.

Step 2 Choose the host on which to deploy the Cisco PNSC VM.

Step 3 From the File menu, choose **Deploy OVF Template**.

Step 4 In the **Source** window, choose the Cisco PNSC OVA, then click **Next**.

Step 5 In the **OVF Template Details** window, review the details of the Cisco PNSC template, and then click **Next**.

Step 6 In the **End User License Agreement** window, click **Accept** after reviewing the End User License Agreement, and then click **Next**.

Step 7 In the **Name and Location** window, provide the required information, and then click **Next**.

The name can contain up to 80 characters and must be unique within the inventory folder.

Step 8 In the **Deployment Configuration** window, choose **Installer** from the Configuration drop-down list, then click **Next**.

Step 9 In the **Datastore** window, select the data store for the VM, and then click **Next**.

Note The storage can be local or shared remote such as the network file storage (NFS) or the storage area network (SAN). If only one storage location is available for an ESXi host, this window does not display and you are assigned to the one that is available.

Step 10 In the **Disk Format** window, click either **Thin provisioned format** or **Thick provisioned format** to store the VM vdisks, and then click **Next**.

The default is thick provisioned. If you do not want to allocate the storage immediately, use thin provisioned.

Step 11 In the **Network Mapping** window, select the management network port group for the VM, then click **Next**.

Step 12 In the **Properties** window, provide the required information, address any errors described in the red text messages below the selection box, and then click **Next**. If needed, you can enter placeholder information as long as your entry meets the field requirements.

Note You can safely ignore the Cisco PNSC Restore fields.

Note For choosing the shared secret password, see the *Shared Secret Password Criteria*.

Step 13 In the **Ready to Complete** window, review the deployment settings information, and then click **Finish**.

Caution Any discrepancies can cause VM booting issues. Carefully review the IP address, subnet mask, gateway, and DNS and NTP IP address information.

A progress indicator shows the task progress until Cisco PNSC is deployed.

Step 14 After Cisco PNSC is successfully deployed, click **Close**.

Step 15 Power on the Cisco VSG VM.

Task 2: On the Cisco PNSC, Setting Up VM-Manager for vCenter Connectivity

Perform the following tasks in the same order as listed below to set up the VM-manager for vCenter connectivity:

- Downloading the vCenter Extension File from the Cisco PNSC
- Registering the vCenter Extension Plugin in the vCenter
- Registering and Configuring the vCenter in VM Manager in the Cisco PNSC, on page 21

Registering and Configuring the vCenter in VM Manager in the Cisco PNSC

Step 1 In Cisco PNSC, choose **Resource Management** > **VM Managers** > **VM Managers**.

Step 2 In the VM Managers pane, click the **Add VM Manager** tab.

Step 3 In the Add VM Manager dialog box, do the following:

a) In the **Name** field, enter the vCenter name (no spaces allowed).

b) In the **Description** field, enter a brief description of the vCenter.

c) In the **Hostname/IP Address** field, enter the vCenter IP address.

Step 4 Select the option, **`vCenter 6.5 and greater`** option.

Step 5 Enter user name and password for vCenter.

Step 6 Click **OK**.

Task 3: On the VSM, Configuring the Cisco PNSC Policy Agent

After installing the Cisco PNSC, you must register the VSM with the Cisco PNSC policy.

Before you begin

Make sure that you know the following:

- The Cisco PNSC policy-agent image is available on the VSM (for example, vsmcpa.3.2.3a.bin)

Note The string **vsmcpa** must appear in the image name as highlighted.

- The IP address of the Cisco PNSC
- The shared secret password you defined during the Cisco PNSC installation
- That IP connectivity between the VSM and the Cisco PNSC is working

Note If you upgrade your VSM, you must also copy the latest Cisco VSM policy agent image. This image is available in the Cisco PNSC image bundle to boot from a flash drive and to complete registration with the Cisco PNSC.

Step 1 On the VSM, enter the following commands:

```
vsm# configure terminal
vsm(config)# nsc-policy-agent
vsm(config-nsc-policy-agent)# registration-ip 10.193.75.95
vsm(config-nsc-policy-agent)# shared-secret Example_Secret123
vsm(config-nsc-policy-agent)# policy-agent-image vsmcpa.3.2.3a.bin
vsm(config-nsc-policy-agent)# exit
vsm(config)# copy running-config startup-config
vsm(config)# exit
```

Note Use PNSC IP address for the **registration-ip** command.

Step 2 Check the status of the NSC policy agent configuration to verify that you have installed the Cisco PNSC correctly and it is reachable by entering the **show nsc-pa status** command. This example shows that the Cisco PNSC is reachable and the installation is correct:

```
vsm# show nsc-pa status
NSC Policy-Agent status is - Installed Successfully. Version 3.4(2)-vsm
vsm
```

The VSM is now registered with the Cisco PNSC.

Example

This example shows that the Cisco PNSC is unreachable or an incorrect IP is configured:

```
vsm# show nsc-pa status
NSC Policy-Agent status is - Installation Failure
PNSC not reachable.
vsm#
```

This example shows that the NSC policy-agent is not configured or installed:

```
vsm# show nsc-pa status
NSC Policy-Agent status is - Not Installed
```

Task 4: On the VSM, Preparing Cisco VSG Port Profiles

To prepare Cisco VSG port profiles, you must create the VLANs and use the VLANs in the Cisco VSG data port profile and the Cisco VSG-ha port profile.

Before you begin

Make sure that you know the following:

- The uplink port-profile name.
- The VLAN ID for the Cisco VSG data interface (for example,100).
- The VLAN ID for the Cisco VSG-ha interface (for example, 200).
- The management VLAN (management).

Note None of these VLANs need to be system VLANs.

Step 1 On the VSM, create the VLANs by first entering global configuration mode using the following command:

```
vsm# configure
```

Step 2 Enter the following configuration commands:

```
vsm(config)# vlan 100
vsm(config-vlan)# no shutdown
vsm(config-vlan)# exit
vsm(config)# vlan 200
vsm(config-vlan)# no shutdown
vsm(config-vlan)# exit
vsm(config)# exit
vsm# configure
vsm(config)# copy running-config startup-config
vsm(config)# exit
```

Step 3 Press **Ctrl-Z** to exit.

Step 4 Create a Cisco VSG data port profile and a Cisco VSG-ha port profile by first enabling the Cisco VSG data port-profile configuration mode. Use the **configure** command to enter global configuration mode.

```
vsm# configure
```

Step 5 Enter the following configuration commands:

```
vsm(config)# port-profile VSG-Data
vsm(config-port-prof)# vmware port-group
vsm(config-port-prof)# switchport mode access
vsm(config-port-prof)# switchport access vlan 100
vsm(config-port-prof)# no shutdown
```

```
vsm(config-port-prof)# state enabled
vsm(config-port-prof)# exit
vsm(config)#
vsm(config)# copy running-config startup-config
vsm(config)# exit
```

Step 6 Press **Ctrl-Z** to end the session.

Step 7 Enable the Cisco VSG-ha port profile configuration mode.

```
vsm# configure
```

Step 8 Enter the following configuration commands:

```
vsm(config)# port-profile VSG-HA
vsm(config-port-prof)# vmware port-group
vsm(config-port-prof)# switchport mode access
vsm(config-port-prof)# switchport access vlan 200
vsm(config-port-prof)# no shutdown
vsm(config-port-prof)# state enabled
vsm(config-port-prof)# exit
vsm(config)# copy running-config startup-config
vsm(config)# exit
```

Step 9 Add the VLANs created for the Cisco VSG data and Cisco VSG-ha interfaces as part of the allowed VLANs into the uplink port profile. Use the **configure** command to enter global configuration mode.

```
vsm# configure
```

Step 10 Enter the following configuration commands:

```
vsm(config)# port-profile type ethernet outside_trunk_port
vsm(config-port-prof)#  switchport mode trunk
vsm(config-port-prof)#  switchport trunk allowed vlan add 100,200
vsm(config-port-prof)#  no shutdown
vsm(config-port-prof)#  state enabled
vsm(config-port-prof)#  vmware port-group
```

Step 11 Press **Ctrl-Z** to end the session.

Task 5: Installing the Cisco VSG from an OVA Template

Before you begin

Make sure that you know the following:

- The Cisco VSG OVA image is available in the vCenter.
- Cisco VSG-Data and Cisco VSG-ha port profiles are created on the VSM.
- The management port profile (management)

Note The management port profile is the same port profile that is used for the VSM. The port profile is configured in the VSM and is used for the Cisco PNSC management interface.

- The Cisco VSG-Data port profile: VSG-Data
- The Cisco VSG-ha port profile: VSG-ha
- The HA ID
- The IP/subnet mask/gateway information for the Cisco VSG
- The admin password
- 2 GB RAM and 3 GB hard disk space are available
- The Cisco PNSC IP address
- The shared secret password
- The IP connectivity between Cisco VSG and Cisco PNSC is okay.
- The Cisco VSG NSC-PA image name (nsc-vsgpa.2.1.3i.bin) is available.

Step 1 Choose the host on which to deploy the Cisco VSG VM.

Step 2 Choose **File** > **Deploy OVF Template**.

Step 3 In the **Deploy OVF Template—Source** window, browse to the path to the Cisco VSG OVA file, and then click **Next**.

Step 4 In the **Deploy OVF Template—OVF Template Details** window, review the product information including the size of the file and the VM disk, and then click **Next**.

Step 5 In the **Deploy OVF Template—End User License Agreement** window, click **Accept** after reviewing the end user license agreement and then click **Next**.

Step 6 In the **Deploy OVF Template—Name and Location** window, do the following:

a) In the **Name** field, enter a name for the Cisco VSG that is unique within the inventory folder and has up to 80 characters.

b) In the **Inventory Location** pane, choose the location that you would like to use for hosting the Cisco VSG.

c) Click **Next**.

Step 7 In the **Deploy OVF Template—Deployment Configuration** window, from the **Configuration** drop-down list, choose **Deploy medium VSG**, and then click **Next**.

Step 8 In the **Deploy OVF Template—Datastore** window, choose the data store for the VM and click **Next**.

The storage can be local or shared remote such as the network file storage (NFS) or the storage area network (SAN).

Note If only one storage location is available for an ESXi host, this window does not display and you are assigned to the one that is available.

Step 9 In the **Deploy OVF Template—Disk Format** window, do the following:

a) Click either **Thin provisioned format** or **Thick provisioned format** to store the VM vdisks.

The default is thick provisioned. If you do not want to allocate the storage immediately, use thin provisioned. Ignore the red text in the window.

b) Click **Next**.

Step 10 In the **Deploy OVF Template—Network Mapping** window, do the following:

a) Choose **VSG Data** for the data interface port profile.

b) Choose **Management** for the management interface port profile.

c) Choose **VSG-ha** for the HA interface port profile .
d) Click **Next**.

Note In this example, for Cisco VSG-Data and Cisco VSG-ha port profiles created in the previous task, the management port profile is used for management connectivity and is the same as in the VSM and Cisco PNSC.

Step 11 In the **Deploy OVF Template—Properties** window, do the following:

a) In the **OvfDeployment** field, select **ovf** to continue the configuration. Select **ignore** for manual configuration.
b) From the **HARole** drop-down list, choose HA role.
c) In the **HAid** field, enter the high-availability identification number for a Cisco VSG pair (value from 1 through 4095).
d) In the **Password** field, enter a password that contains at least one uppercase letter, one lowercase letter, and one number.
e) In the **ManagementIpV4** field, enter the IP address for the Cisco VSG.
f) In the **ManagementIpV4 Subnet** field, enter the subnet mask.
g) In the **Gateway** field, enter the gateway name.
h) In the **VnmcIpV4** field, enter the IP address of the Cisco PNSC.
i) In the **SharedSecret** field, enter the shared secret password defined during the Cisco PNSC installation.
j) Click **Next.**

Note For the shared secret password guidelines, see *Shared Secret Pasword* section.

Note In the following step, make sure that red text messages do not appear before you click **Next**. If you do not want to enter valid information in the red-indicated fields, use null values to fill those fields. If those fields are left empty or filled with invalid null values, the application does not power on. Ignore the Cisco PNSC Restore fields.

Step 12 In the **Ready to Complete** window, review the deployment settings information .

Note Review the IP/mask/gateway information carefully because any discrepancies might cause the VM to have bootup issues.

Step 13 Click **Finish**. The **Deploying Nexus 1000VSG** dialog box opens.

The progress bar in the **Deploying Nexus 1000VSG** dialog box shows how much of the deployment task is completed before the Cisco PNSC is deployed.

Step 14 Wait and click **Close** after the progress indicator shows that the deployment is completed successfully.

Step 15 From your virtual machines, do one of the following:

a) Right click and choose **Edit Settings**.
b) Click the **Getting Started** tab from the menu bar and then click the link **Edit Virtual Machine Settings**.

Step 16 In the **Virtual Machine Properties** window, do the following:

a) From the **CPUs** drop-down list, choose the appropriate vCPU number.

For older version of ESXi hosts, you can directly select a number for the vCPUs.

b) From the **Number of Virtual Sockets** drop down list, choose the appropriate socket with cores.

For the latest version of ESXi hosts, you can directly select a number for the vCPUs.

Choosing 2 CPUs results in a higher performance.

Step 17 Power on the Cisco VSG VM.

Task 6: On the Cisco VSG and Cisco PNSC, Verifying the NSC Policy-Agent Status

You can use the **show nsc-pa status** command to verify the NSC policy-agent status (which can indicate that you have installed the policy-agent successfully).

Step 1 Log in to the Cisco VSG.

Step 2 Check the status of NSC-PA configuration by entering the following command:

```
vsg# show nsc-pa status
NSC Policy-Agent status is - Installed Successfully. Version 2.1(3i)-vsg
vsg#
```

Step 3 Log in to the Cisco PNSC.

Step 4 Choose **Resource Management** > **Resources** > **VSG**.

Step 5 Confirm that the table in the Clients window contains the registered value in the **Oper Status** column for the Cisco VSG and VSM entries.

Task 7: On the Cisco PNSC, Configuring a Tenant and Security Profile

This task includes the following subtasks:

- Configuring a Tenant on the Cisco PNSC, on page 28
- Configuring a Security Profile on the Cisco PNSC, on page 28

Before you begin

Make sure that you know the following:

- Supported Adobe Flash Player given in System Requirements, on page 9
- The IP address of the Cisco PNSC
- The password for Admin user

Step 1 In your browser, enter https://*server-ip-address* where *server-ip-address* is the Cisco PNSC IP address.

Step 2 In the **Website Security Certificate** window, choose **Continue to this website**.

Step 3 In the Cisco PNSC login window, enter the username **admin** and the admin user password.

Step 4 In the Cisco PNSC main window, choose **Resource Management** > **Resources** to check the Cisco VSG and VSM registration in the Cisco PNSC.

What to do next

Go to Configuring a Tenant on the Cisco PNSC, on page 28

Configuring a Tenant on the Cisco PNSC

Tenants are entities (businesses, agencies, institutions, and so on) whose data and processes are hosted on VMs on the virtual data center. To provide firewall security for each tenant, the tenant must first be configured in the Cisco PNSC.

Step 1 In the Cisco PNSC, choose **Tenant Management** > **root**.

Step 2 In the upper-right corner of the Tenant Management Root pane, click **Create Tenant**.

The tenant name can contain 1 to 32 alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is created. The newly created tenant is listed in the navigation pane under root.

What to do next

Go to Configuring a Security Profile on the Cisco PNSC, on page 28

Configuring a Security Profile on the Cisco PNSC

You can configure a security profile on the Cisco PNSC.

Step 1 Choose **Policy Management** > **Service Profiles** > **root** > *tenant* > **Compute Firewall** > **Compute Security Profiles** where *tenant* is the required tenant.

Step 2 In the General tab, click **Add Compute Security Profile**.

Step 3 In the **Add Compute Security Profile** dialog box, enter a name and description for the security profile, and then click **OK**.

What to do next

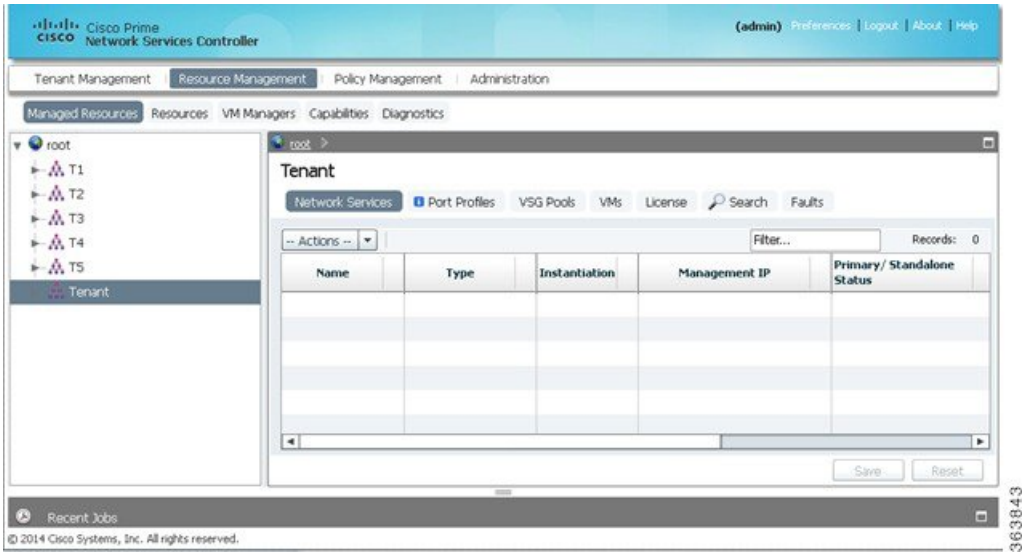
Next, you need to add a compute firewall as described in Task 9: On the Cisco PNSC, Adding a Compute Firewall, on page 33. While adding a compute firewall, you either instantiate a VSG service device from an image or assign a VSG or VSG pool. To instantiate a VSG service device from an image, you first need to import the VSG service image as described in Task 8: On the Cisco PNSC, Importing Service Image, on page 32.

Configuring a Compute Firewall on the Cisco PNSC

The compute firewall is a logical virtual entity that contains the device profile that you can bind (assign) to a Cisco VSG VM. The device policy in the device profile is then pushed from the Cisco PNSC to the Cisco VSG. Once this is complete, the compute firewall is in the applied configuration state on the Cisco PNSC.

Step 1 From the Cisco PNSC, choose **Resource Management** > **Managed Resources> Tenant**.

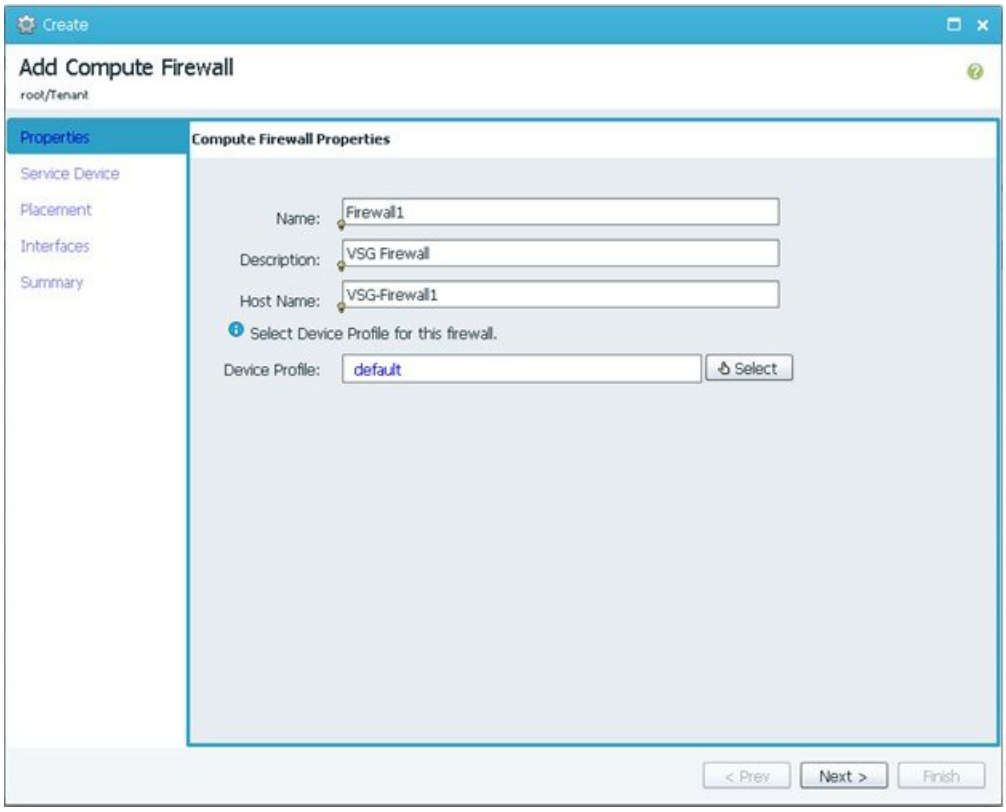
Figure 6: PNSC Resource Management, Managed Resources, Firewall Profiles Window



Step 2 On the right-pane on the Network Services Tab, click **Actions** drop-down list.

Step 3 From the drop-down list, choose **Add Compute Firewall**. The **Add Compute Firewall** dialog box opens.

Figure 7: Add Compute Firewall - Compute Firewall Properties

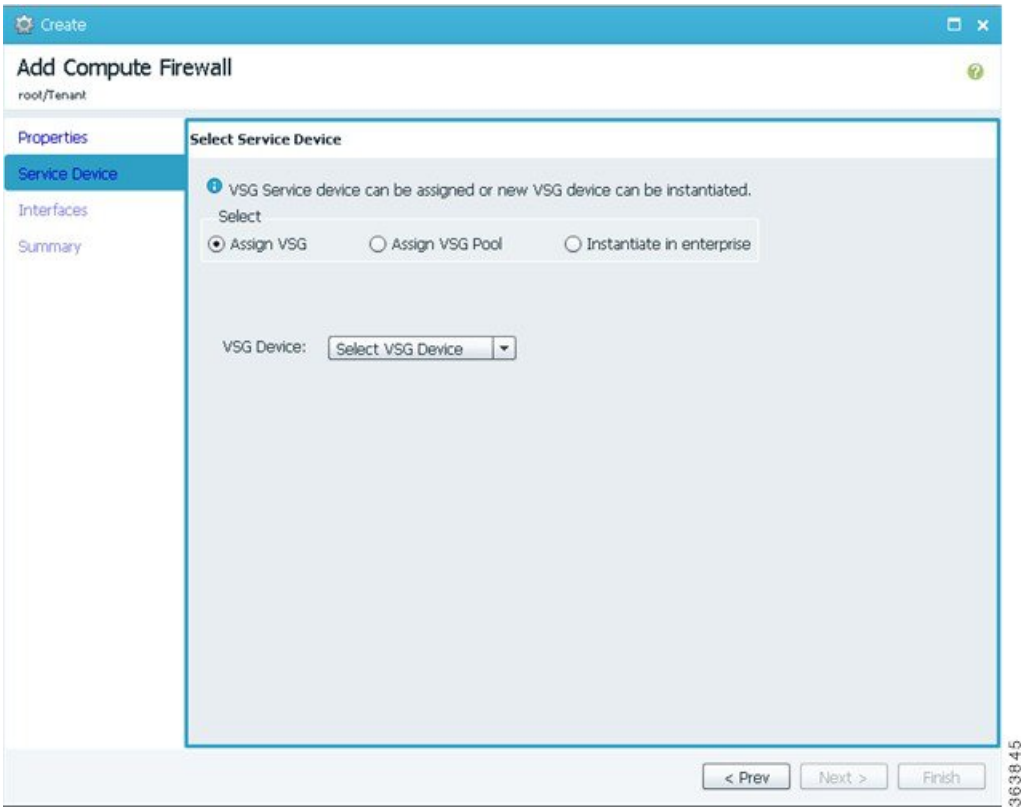


Step 4 In the **Add Compute Firewall** dialog box, do the following:

a) In the **Name** field, enter a name for the compute firewall.
b) In the **Description** field, enter a brief description of the compute firewall.
c) In the **Host Name** field, enter the name for your Cisco VSG.

Step 5 Click **Next**, the Select Service Device page opens.

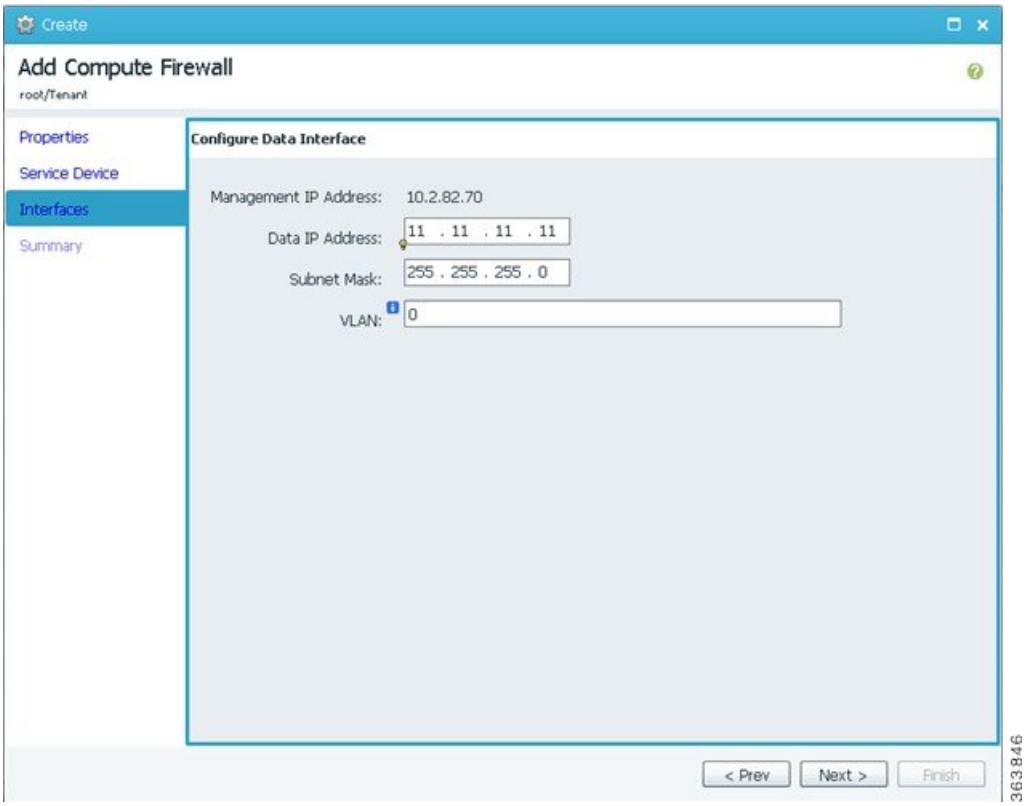
Figure 8: Add Compute Firewall - Select Service Device



Step 6 On **Select Service Device** page, choose **Assign VSG** option and select a VSG device from the **Select VSG Device** drop-down list.

Step 7 Click **Next**, the **Configure Data Interface** page opens.

Figure 9: Add Compute Firewall - Configure Data Interface



Step 8 On the **Configure Data Interface** page, do the following:

a) In the **Data IP Address** field, enter IP address for the data interface for the compute firewall.

b) In the **Subnet Mask** field, enter subnet mask for the data interface for the compute firewall.

Step 9 Click **Next**, the **Summary** page opens.

Step 10 Verify the details you entered for configuring the compute firewall and click **Finish** to complete the firewall configuration.

The new **Compute Firewall** pane displays with the information that you provided.

Task 8: On the Cisco PNSC, Importing Service Image

This step is required to instantiate a VSG service device from an image in Task 9: On the Cisco PNSC, Adding a Compute Firewall, on page 33. This step is not required for assigning a VSG or VSG pool option in Task 9: On the Cisco PNSC, Adding a Compute Firewall, on page 33.

Step 1 Log in to the Cisco PNSC.

Step 2 Choose **Resource Management** > **Resources** > **Images**.

Step 3 Click **Import Service Image**.

Step 4 In the Import Service Image dialog box, do the following:

a) Enter a name and description for the image you are importing.
b) In the **Type** field, select **VSG**.
c) In the **Version** field, enter a version to assign to the image.
d) In the **Protocol** field, choose a protocol.
e) In the **Hostname / IP Address** field, enter the hostname or IP address of the remote host to which you downloaded the images.
f) In the **User Name** field, enter the account username for the remote host.
g) In the **Password** field, enter the account password for the remote host.
h) In the **Remote File** field, enter the absolute path and filename of the service image, starting with a slash, such as /mnt/nexus-1000v.5.2.1.VSG2.2.2.ova.

Task 9: On the Cisco PNSC, Adding a Compute Firewall

You can add a compute firewall and assign it to a Cisco VSG, thereby placing the Cisco VSG in service. A wizard walks you through the configuration process, which includes assigning a Cisco VSG, assigning profiles, and configuring interfaces.

When you add a new compute firewall, the firewall data IP address can be the same as the data IP address of an existing compute firewall in Cisco PNSC as long as the firewalls have different organizational paths. That is, as long as the firewalls do not reside in the same organization, including parent and child organizations.

Before you begin

To place a Cisco VSG in service, at least one of the following must exist:

- To assign a Cisco VSG, an available Cisco VSG must be registered in Cisco PNSC. For more information, see Task 6: On the Cisco VSG and Cisco PNSC, Verifying the NSC Policy-Agent Status, on page 27.
- To assign a Cisco VSG pool, a Cisco PNSC pool must have at least one available Cisco VSG.
- To instantiate a Cisco VSG service device, a VM service image must be imported and VM Manager must be configured in the Cisco PNSC. For more information on importing service images, see Task 8: On the Cisco PNSC, Importing Service Image, on page 32.

Step 1 Log in to the Cisco PNSC.

Step 2 Choose **Resource Management** > **Managed Resources** > **root** > ***tenant*** > **Network Services**.

Step 3 From the **Actions** drop-down list, select **Add Compute Firewall**.
The Add Compute Firewall Wizard opens.

Step 4 In the Properties window, supply the information as described in the Properties Window, on page 34, and then click **Next**.

Step 5 In the Service Device window, select the required VSG service device as described in the Service Device Window, on page 34, and then click **Next**.

Step 6 (Instantiate option only) If you instantiate a VSG service device from an image, do one or both of the following in the Placement screen, then click **Next**:

- Navigate to and choose the host or resource pool to use for the VSG instance.

- If you enabled high availability, either check the **Same as Primary** check box, or navigate to and choose the host or resource pool to use for the secondary VSG instance.

Step 7 In the Interfaces window, configure interfaces as follows, and then click **Next**:

- If you assigned a VSG, enter the data IP address and subnet mask.
- If you assigned a VSG pool, enter the data IP address and subnet mask.
- If you instantiated a VSG service device without high availability, add management and data interfaces.
- If you instantiated a VSG service device with high availability, add management, data, and HA interfaces.

For field-level help when configuring the interfaces, see the online help.

Step 8 In the Summary window, confirm that the information is correct, and then click **Finish**.

Properties Window

Field	Description
Name	Compute firewall name. This name can contain 1 to 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is created.
Description	Compute firewall description.
Host Name	Management hostname of the firewall.
Device Configuration Profile	Do either of the following: • Click the profile name to view or optionally modify the currently assigned device configuration profile. • Click **Select** to choose a different device configuration profile.

Service Device Window

Field	Description
Assign VSG	Assign a VSG to the compute firewall. In the **VSG Device** drop-down list, choose the required service device.
Assign VSG Pool	Assign a VSG pool to the compute firewall. In the **VSG Pool** field, either choose the required pool from the drop-down list or click **Add Pool** to add a new pool.

Field	Description
Instantiate	Instantiate a VSG service device from an available image. 1. In the list of available images, select the image to use to instantiate a new VSG service device. 2. In the High Availability field, check the **Enable HA** check box to enable high availability. 3. In the VM Access password fields, enter the password for the admin user account.

Task 10: On the Cisco PNSC, Configuring a Permit-All Rule

You can configure a permit-all rule in the Cisco PNSC.

Step 1 Log in to the Cisco PNSC.

Step 2 In the Cisco PNSC window, choose **Policy Management** > **Service Profiles**.

Step 3 In the **Service Profile** window, choose **root** > ***tenant*** > **Compute Security-Profiles** > **SP1**.

Step 4 In the right pane, click **Add ACL Policy Set**.

Step 5 In the Add ACL Policy Set dialog box, enter a name and description for the policy set, and then click **Add ACL Policy**.

Step 6 In the **Add ACL Policy** dialog box, enter a name and description for the policy, and then click **Add Rule** above the **Name** column.

Step 7 In the **Add ACL Policy Rule** dialog box, do the following:

a) In the **Name** field, enter the rule name.
b) In the **Description** field, enter a description for the rule.
c) In the **Action To Take** area, choose **permit**.
d) In the **Condition Match Criteria** field, select a matching condition.
e) In the **Source Conditions** field, enter the source condition of the rule.
f) In the **Destination Conditions** field, enter the destination condition of the rule.
g) In the **Service** field, enter the service expression.
h) In the **Protocol** tab, select a protocol for the rule.
i) In the **Ether Type** tab, specify the ether type for the rule.
j) Click **OK**.

Step 8 In the **Add ACL Policy** dialog box, click **OK**.

The newly created policy is displayed in the **Assigned** field.

Step 9 In the **Add ACL Policy Set** dialog box, click **OK**.

Step 10 In the **Security Profile** window, click **Save**.

Task 11: On the Cisco VSG, Verifying the Permit-All Rule

SUMMARY STEPS

1. You can verify the rule presence in the Cisco VSG, by using the Cisco VSG CLI and the **show** commands.

DETAILED STEPS

	Command or Action	Purpose

Step 1	You can verify the rule presence in the Cisco VSG, by using the Cisco VSG CLI and the **show** commands.
	Example:
	`vsg# show running-config | begin security`
	`security-profile SP_web@root/Tenant-A`
	`  policy PS_web@root/Tenant-A`
	`  custom-attribute vnsporg "root/tenant-a"`
	`security-profile default@root`
	`  policy default@root`
	`  custom-attribute vnsporg "root"`
	`rule Pol_web/permit-all@root/Tenant-A`
	`cond-match-criteria: match-all`
	`  action permit`
	`  action log`
	`rule default/default-rule@root cond-match-criteria:`
	` match-all`
	`  action drop`
	`Policy PS_web@root/Tenant-A`
	`  rule Pol_web/permit-all@root/Tenant-A order 101`
	`Policy default@root`
	`  rule default/default-rule@root order 2`	

Task 12: Enabling Logging

To enable logging follow these procedures:

- Enabling Policy-Engine Logging in a Monitor Session, on page 36
- Enabling Global Policy-Engine Logging, on page 37

Enabling Policy-Engine Logging in a Monitor Session

Configuring a syslog policy enables you to specify the level of syslog messages to log and where to log the messages.

Step 1 Log in to the Cisco PNSC.

Step 2 In the Cisco PNSC window, choose **Policy Management** > **Device Configurations** > **root** > **Policies** > **Syslog**.

Step 3 In the Syslog table, select **default**, then click **Edit**.

Step 4 In the **Edit Syslog** dialog box, click the **Servers** tab.

Step 5 In the Syslog Policy table, select the primary server type, then click **Edit**.

Step 6 In the **Edit Syslog Client** dialog box, provide the following information, then click **OK** in the open dialog boxes:

- Hostname/IP Address—Enter the syslog server IP address or hostname.
- Severity—Choose **information (6)**.
- Admin State—Choose **enabled**.

What to do next

Go to Enabling Global Policy-Engine Logging, on page 37.

Enabling Global Policy-Engine Logging

Logging enables you to see what traffic is going through your monitored VM. This logging is helpful for verifying that you have a proper configuration and to help in troubleshooting.

Step 1 Log in to the Cisco PNSC.

Step 2 In the Cisco PNSC window, choose **Policy Management** > **Device Configurations** > **root** > **Device Profiles** > **default**. The **default** Device Profile window opens.

Step 3 In the Device Profiles pane, click the **Policies** tab.

Step 4 In the Policy Engine Logging area at the lower-right of the Policies tab, click **Enabled**, and then click **Save**.

Task 13: Enabling the Traffic VM Port-Profile for Firewall Protection and Verifying the Communication Between the VSM, VSE, and VSG

Make sure that you know the following:

- The server virtual machine that runs with an access port profile (for example, web server)
- The Cisco VSG data IP address (for example, 10.10.10.200) and VLAN ID (100)
- The security profile name (for example, sp-web)
- The organization (Org) name (for example, root/Tenant-A)
- The port profile that you would like to edit to enable firewall protection
- That one active port in the port-profile with vPath configuration has been set up

This section includes the following topics:

Checking the VM Virtual Ethernet Port for Firewall Protection, on page 39

Enabling Traffic VM Port-Profile for Firewall Protection

You can enable a traffic VM port profile for traffic protection.

Verify the traffic VM port profile before firewall protection.

Configuring vservice node in vsm that will be attached to port-profile pp-webserver.

```
vsm(config)# vservice node vsg1 type vsg
vsm(config-vservice-node)# ip address 11.11.11.11
vsm(config-vservice-node)# adjacency l3
vsm(config-vservice-node)# fail-mode close
vsm(config-vservice-node)# copy running-config startup-config
```

Enable firewall protection.

```
VSM(config)# port-profile pp-webserver
VSM(config-port-prof)# vservice node vsg1 profile SP_web
VSM(config-port-prof)# org root/Tenant-A
```

Verify the traffic VM port profile after firewall protection.

```
VSM(config)# port-profile type vethernet pp-webserver
  vmware port-group
  switchport mode access
  switchport access vlan 756
  org root/Tenant-A
  vservice node vsg1 profile SP_web
  no shutdown
  state enabled
```

What to do next

Go toVerifying the VSM or VSE for Cisco VSG Reachability, on page 38.

Verifying the VSM or VSE for Cisco VSG Reachability

This example shows how to verify the communication between the VSE and the VSG:

```
vsm(config)# show vservice brief
------------------------------------------------------------------------------
License Information
------------------------------------------------------------------------------
Type In-Use-Lic-Count UnLicensed-Mod
asa 0

------------------------------------------------------------------------------
Node Information
------------------------------------------------------------------------------
ID Name Type IP-Address Mode State Module
2 VSG-L2-V vsg 10.1.1.251 v-920 Alive 3,6,

------------------------------------------------------------------------------
```

```
Path Information
------------------------------------------------------------------------------
------------------------------------------------------------------------------
Port Information
------------------------------------------------------------------------------
PortProfile:Vsg220
Org:root/T1
Node:VSG-L2-V(10.1.1.251) Profile(Id):sp11(5)
Veth Mod VM-Name vNIC IP-Address
9 6 inside_vm 1 10.1.1.81
19 3 outside_vm 1 10.1.1.82
```

A display showing the MAC-ADDR Listing and Up state verifies that the VSE can communicate with the Cisco VSG.

Note In order to see the above status, one active port in the port profile with vPath configuration needs to be up.

Checking the VM Virtual Ethernet Port for Firewall Protection

This example shows how to verify the VM Virtual Ethernet port for firewall protection:

```
VSM(config)# show vservice port brief vethernet 23
------------------------------------------------------------------------------
                                  Port Information
------------------------------------------------------------------------------
PortProfile:pp-webserver
Org:root/Tenant-A
Node:vsg1(40.40.40.40)                          Profile(Id):SP_web(29)
Veth Mod VM-Name                                vNIC IP-Address
 23  4     vm1                                    2   14.14.14.21
```

Note Make sure that your VNSP ID value is greater than 1.

Task 14: Sending Traffic Flow and on the Cisco VSG Verifying Statistics and Logs

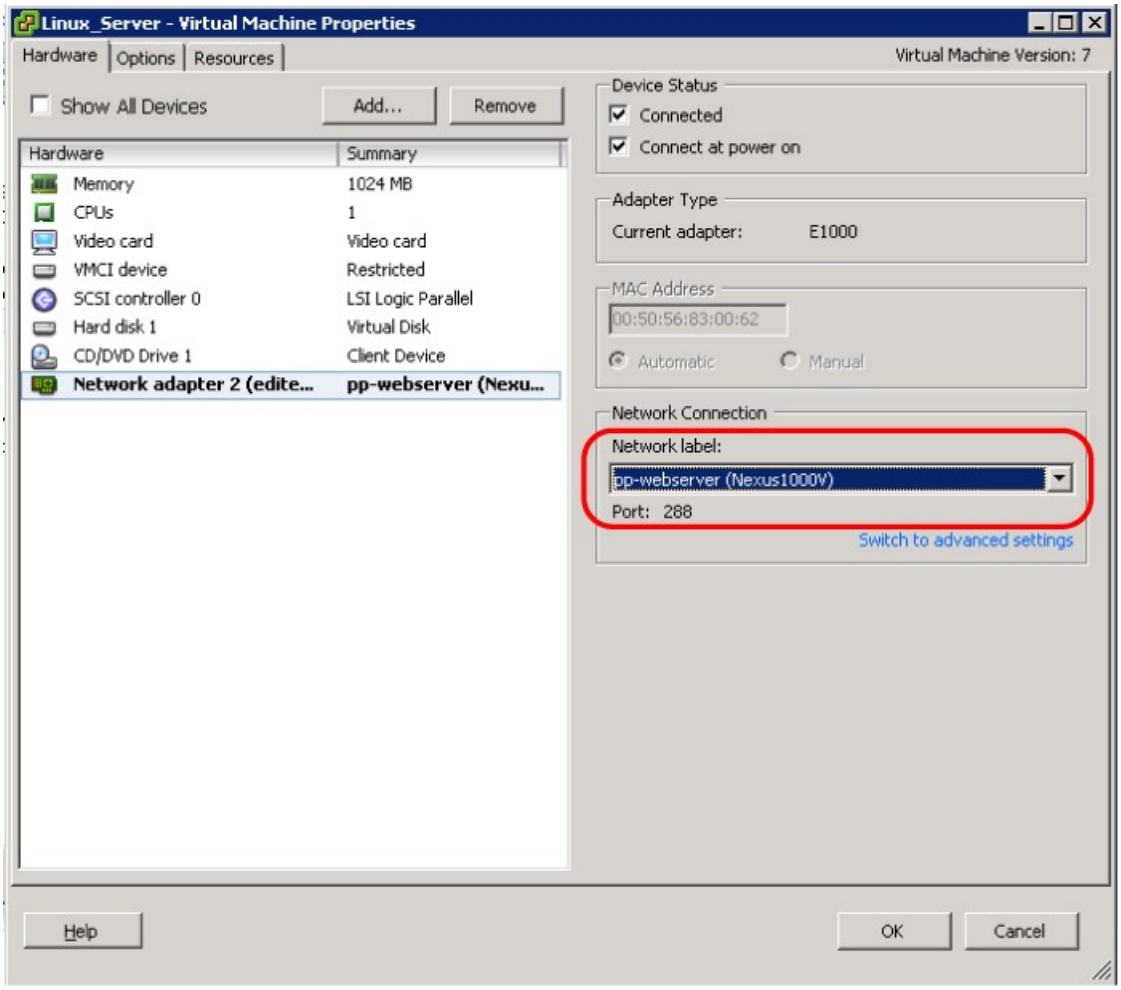
This section includes the following topics:

Sending Traffic Flow

You can send traffic flow through the Cisco VSG to ensure that it is functioning properly.

Step 1 Ensure that the VM (Server-VM) is using the port profile (pp-webserver) configured for firewall protection.

Figure 10: Virtual Machine Properties Window



Step 2 In the **Virtual Machine Properties** window, do the following:

a) Log in to any of your client virtual machine (Client-VM).

b) Send traffic (for example, HTTP) to your Server-VM.

```
[root@]# wget http://172.31.2.92/
--2010-11-28 13:38:40--  http://172.31.2.92/
Connecting to 172.31.2.92:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 258 [text/html]
Saving to: `index.html'

100%[======================================================================>] 258         --.-K/s
  in 0s

2010-11-28 13:38:40 (16.4 MB/s) - `index.html' saved [258/258]

[root]#
```

Step 3 Check the policy-engine statistics and log on the Cisco VSG.

What to do next

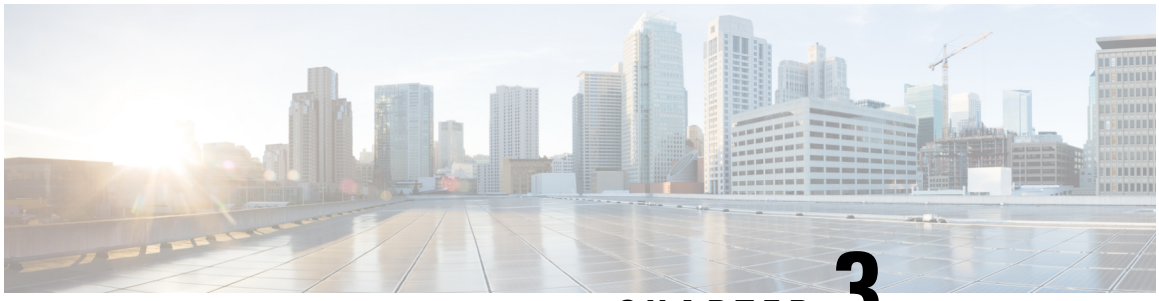
Go to Verifying Policy-Engine Statistics and Logs on the Cisco VSG, on page 41.

Verifying Policy-Engine Statistics and Logs on the Cisco VSG

Log in to the Cisco VSG and check the policy-engine statistics and logs.

This example shows how to check the policy-engine statistics and logs:

```
vsg# show policy-engine stats
Policy Match Stats:
default@root                  :         0
  default/default-rule@root   :         0 (Drop)
  NOT_APPLICABLE              :         0 (Drop)

PS_web@root/Tenant-A :         1
  pol_web/permit-all@root/Tenant-A :         1 (Log, Permit)
  NOT_APPLICABLE                :         0 (Drop)

vsg# terminal monitor
vsg# 2010 Nov 28 05:41:27 firewall %POLICY_ENGINE-6-POLICY_LOOKUP_EVENT:
policy=PS_web@root/Tenant-A rule=pol_web/permit-all@root/Tenant-A action=Permit
direction=egress src.net.ip-address=172.31.2.91 src.net.port=48278
dst.net.ip-address=172.31.2.92 dst.net.port=80 net.protocol=6 net.ethertype=800
```



CHAPTER 3

Installing 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.

Installation Requirements

Cisco PNSC System Requirements

Requirement	Description
Virtual Appliance	
Four Virtual CPUs	1.8 GHz for each virtual CPU
Memory	4 GB RAM

Requirement	Description

Disk Space	One of the following, depending on InterCloud functionality:
	• With InterCloud functionality, 220 GB on shared network file storage (NFS) or storage area network (SAN), and configured on two disks as follows:
	  • Disk 1: 20 GB
	  • Disk 2: 200 GB
	• Without InterCloud functionality, 40 GB on shared NFS or SAN, and configured on two disks as follows:
	  • Disk 1: 20 GB
	  • Disk 2: 20 GB

Management interface	One management network interface
Processor	x86 Intel or AMD server with 64-bit processor listed in the VMware compatibility matrix. **Note** You can find VMware compatibility guides at http://www.vmware.com/resources/compatibility/search.php.
VMware	
VMware vSphere	6.0, and 6.5a with VMware ESXi (English only)
VMware vCenter	6.5u2 with VMware ESXi (English only)
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 VMware vSphere.

For more information on VMware compatibility with your hardware platform, see the VMware Compatibility Guide.

Table 1: Hypervisor Requirements

Requirement	Description
VMware	
VMware vSphere	6.0, and 6.5a with VMware ESXi (English only)
VMware vCenter	6.5u2 with VMware ESXi (English only)

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 **Note** If you are running Firefox or IE and do not have Flash, or you have a version of Flash that is older than 11.9, a message displays asking you to install Flash and provides a link to the Adobe website. **Note** Before using Google Chrome with Cisco PNSC, you must disable the Adobe Flash Players that are installed by default with Chrome. For more information, see Configuring Chrome for Use with Prime Network Services Controller.
Flash Player	Adobe Flash Player plugin 11.9 or higher

Firewall Ports Requiring Access

Requirement	Description
22	TCP
80	HTTP/TCP
443	HTTPS

Requirement	Description
843	Adobe Flash

Cisco Nexus 1000VE Series Switch Requirements

Requirement	Notes
General	
The procedures in this guide assume that the Cisco Nexus 100VE Series switch is up and running, and that endpoint Virtual Machines (VMs) are installed.	—
VLANs	
Two VLANs configured on the Cisco Nexus 100VE 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 100VE Series Switch for the service VLAN.	—

Information Required for Configuration and Installation

Before installation, collect the following information:

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 name	
VMware datastore Location	
For Prime Network Services Controller Installation	

Required Information	Your Information/Notes
IP address • One management IP address • Two IP addresses on the same subnet (that is, one IP address for each node in an HA pair)	
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, on page 47.)	

[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 to only those using a secure communication channel. Passwords are designated as strong if they cannot be easily guessed for unauthorized access. When you set a shared secret password for communications between Prime Network Services Controller, Cisco VSG, and VSM, adhere to the following criteria for setting valid, strong passwords:

- Do not include special characters or spaces.
- Make sure your password contains the characteristics of strong passwords and avoids the characteristics of weak passwords as described in the following table:

Strong Passwords	Weak Passwords
• At least eight characters. • Contain characters from at least three of the following classes: lowercase letters, uppercase letters, and numbers.	• Consecutive alphanumeric characters, such as *abcd* or *123*. • 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
- Es1955Ap

Configuring Chrome for Use with Cisco Prime Network Services Controller

To use Chrome with Prime Network Services Controller, 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.

SUMMARY STEPS

1. In the Chrome URL field, enter **chrome://plugins**.
2. Click **Details** to expand all the files associated with each plugin.
3. Locate the Adobe Flash Player plugins, and disable each one.
4. Download and install Adobe Flash Player plugin version 11.9 or higher.
5. Close and reopen Chrome before logging in to Prime Network Services Controller.

DETAILED STEPS

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 Prime Network Services Controller.

ESXi Server Requirement

You must set the clock to the correct time on all ESXi servers that will run Cisco PNSC, ASA 1000V instances, Cisco VSG, or VSM. If you do not set the correct time on the server, the Cisco PNSC CA certificate that is created when the Cisco PNSC VM is deployed might have an invalid time stamp. An invalid time stamp can prevent you from successfully registering ASA 1000V instances to the Cisco PNSC.

After you set the clock to the correct time on all ESXi servers that run the Cisco PNSC, you can, as an option, set the clock on the Cisco PNSC as follows:

- If you set the clock manually, be sure to enter the correct time zone as a Coordinated Universal Time (UTC) offset.
- If you set the clock by synchronizing with the Network Time Protocol (NTP), you can select the UTC time zone.

VMware Installation Overview

You can install Prime Network Services Controller on VMware by using either an ISO or an OVA image. The installation time varies from 10 to 20 minutes, depending on the host and the storage area network load.

To install Prime Network Services Controller on VMware, complete the following tasks:

Task	Comments
1. Configuring VMware for Prime Network Services Controller, on page 52	Required for ISO installations only.
2. Installing Prime Network Services Controller	Use the procedure appropriate for your environment: • Installing Prime Network Services Controller Using the ISO Image, on page 54 • Installing Prime Network Services Controller Using the OVA Image
3. Performing VMware Post-Installation Tasks	Required for all installations.

Installing Prime Network Services Controller Using the OVA Image

This procedure describes how to deploy the Prime Network Services Controller OVA image on VMware.

Before you begin

- Set your keyboard to United States English.
- Confirm that the Prime Network Services Controller OVA image is available from the VMware vSphere Client.
- Make sure that all system requirements are met.
- Gather the information identified in Information Required for Configuration and Installation, on page 46.

SUMMARY STEPS

1. Using the VMware vSphere Client, log in to the vCenter server.
2. Choose the host on which to deploy the Prime Network Services Controller VM.
3. Right-click **Host** and select **Deploy OVF Template** from the Pop-up menu.
4. In the wizard, provide the information as described in the following table:
5. Click **Finish**.
6. After Prime Network Services Controller is successfully deployed, click **Close**.
7. Power on the Prime Network Services Controller VM.

DETAILED STEPS

Step 1 Using the VMware vSphere Client, log in to the vCenter server.

Step 2 Choose the host on which to deploy the Prime Network Services Controller VM.

Step 3 Right-click **Host** and select **Deploy OVF Template** from the Pop-up menu.

Step 4 In the wizard, provide the information as described in the following table:

Screen	Action
Source	Choose the Prime Network Services Controller OVA.
OVF Template Details	Review the details.
End User License Agreement	Review the agreement and click **Accept**.
Name and Location	Enter a name and choose a location for the template.
Deployment Configuration	Choose **Installer**.
Datastore	Select the data store for the VM. The storage can be local or shared remote, such as NFS or SAN.
Disk Format	Choose either **Thin provisioned format** or **Thick provisioned format** to store the VM virtual disks.
Network Mapping	Choose the management network port group for the VM.
Properties Address any errors that are indicated in red colored text below a selection box. You can enter placeholder information as long as your entry meets the field requirements.	

Screen	Action
A. IP Address	VM management IP address.
B. IP Netmask	VM subnet mask.
C. Gateway	Gateway IP address.
D. DNS	• VM hostname • VM domain • DNS server IP address
E. NTP	NTP server IP address.
F. Operation Mode	• Standalone—Operates as a standalone VM. • Orchestrator—Integrates through an orchestrator with a northbound application.
G. Passwords	• Administrator password • Shared secret password
H. Restore	You can safely ignore the Restore fields.
Ready to Complete	Review the deployment settings. **Caution** Any discrepancies can cause VM booting issues. Carefully review the IP address, subnet mask, and gateway information for accuracy.

Step 5 Click **Finish**.
A progress indicator shows the task progress until Prime Network Services Controller is deployed.

Step 6 After Prime Network Services Controller is successfully deployed, click **Close**.

Step 7 Power on the Prime Network Services Controller VM.

Installing Prime Network Services Controller Using an ISO Image

To install Prime Network Services Controller in a VMware environment using an ISO image, complete the tasks described in the following topics:

1. Configuring VMware for Prime Network Services Controller, on page 52
2. Installing Prime Network Services Controller Using the ISO Image, on page 54

Configuring VMware for Prime Network Services Controller

Before you install Prime Network Services Controller (PNSC) on VMware using an ISO image, you must configure a VM for Prime Network Services Controller. This procedure describes how to configure the VM so that you can install Prime Network Services Controller on it.

Before you begin

- Confirm that the system requirements have been met.
- Gather the information required for configuration as identified in Information Required for Configuration and Installation, on page 46.

SUMMARY STEPS

1. Download a Prime Network Services Controller ISO image to your client machine. In case of vSphere 6.5 and greater, upload the PNSC ISO image to datastore.
2. Open the Web client (version 6.5u2).
3. Right-click the host on which to install the ISO image, and then choose **New Virtual Machine**.
4. Create a new VM by providing the information as described in the following table:
5. For VMware vSphere version 6.5, in the Ready to Complete screen, review the information for accuracy, check the **Edit the Virtual Machine Settings Before Completion** check box, and then click **Continue**.
6. In the Virtual Machine Properties dialog box in the Hardware tab, do the following:
7. In the **Options** tab, choose **Boot Options**, check the **Force BIOS Setup** check box, and then click **Finish**.
8. After the new VM is created, power it on.
9. For VMware vSphere 6.5, mount the ISO to the VM CD ROM drive as follows:

DETAILED STEPS

Step 1 Download a Prime Network Services Controller ISO image to your client machine. In case of vSphere 6.5 and greater, upload the PNSC ISO image to datastore.

Step 2 Open the Web client (version 6.5u2).

Step 3 Right-click the host on which to install the ISO image, and then choose **New Virtual Machine**.

Step 4 Create a new VM by providing the information as described in the following table:

Screen	Action
Configuration	Choose **Custom**.
Name and Location	Enter a name and choose a location for the VM.
Storage	Choose the data store.
Virtual Machine Version	Choose **Version 8**.
Guest Operating System	Choose **Linux** and **Red Hat Enterprise Linux 5 (64-bit)**.
CPUs	Set the number of virtual sockets to **4**.
Memory	Set the memory to **4 GB**.

Screen	Action
Network	1. Set the number of NICs to **1**. A single NIC is required for Prime Network Services Controller. 2. Choose a NIC. 3. From the Adapter drop-down list, choose **E1000**. Prime Network Services Controller supports only E1000 adapters.
SCSI Controller	Choose **LSI Logic Parallel**.
Select a Disk	Choose **Create a new virtual disk**.
Create a Disk	1. Disk Size—Enter a minimum of 20 GB. 2. Disk Provisioning—Choose **Thin Provision** or **Thick Provision**. 3. Location—Specify the location of the data store.
Advanced Options	Specify options as needed.

Step 5 For VMware vSphere version 6.5, in the Ready to Complete screen, review the information for accuracy, check the **Edit the Virtual Machine Settings Before Completion** check box, and then click **Continue**.

Step 6 In the Virtual Machine Properties dialog box in the Hardware tab, do the following:

a) Click **Memory** and in the Memory Size field, choose **4 GB**.
b) Click **CPUs** and in the Number of Virtual Sockets field, choose **4**.
c) Click **New Hard Disk** and then click **Add** to create a new hard disk.
d) Create an additional hard disk with 200 GB memory with thin provisioning. For VMware vSphere 6.5 webclient, choose the **Network** and **ISO disk** from the datastore and select the **Connect** check box.
e) After you supply the information in the Add Hardware Wizard, click **Finish** to create the new disk and to return to the Virtual Machine Properties dialog box.
f) For VMware vSphere 6.5 webclient, choose the Network for the VM. For the Image choose your uploaded ISO disk from datastore.

Step 7 In the **Options** tab, choose **Boot Options**, check the **Force BIOS Setup** check box, and then click **Finish**.

Step 8 After the new VM is created, power it on.

Step 9 For VMware vSphere 6.5, mount the ISO to the VM CD ROM drive as follows:

a) Right-click the VM and choose **Open Console**.
b) From the VM console, click **Connect/Disconnect the CD/DVD Devices of the virtual machine**.
c) Choose **CD/DVD Drive 1**.
d) Choose **Connect to ISO Image on Local Disk**.
e) Choose the ISO image that you downloaded in Step 1.

What to do next

Install Prime Network Services Controller as described in Installing Prime Network Services Controller Using the ISO Image, on page 54.

Installing Prime Network Services Controller Using the ISO Image

This procedure describes how to install the ISO image on a VM that has been configured for Prime Network Services Controller.

Before you begin

Confirm the following items:

- All system requirements are met.
- You have the information identified in Information Required for Configuration and Installation, on page 46.
- You have configured the hypervisor for the Prime Network Services Controller installation procedure.
- A VM has been created for Prime Network Services Controller and has network access.
- You can access the VM console.

SUMMARY STEPS

1. Open the VM console if it is not already open.
2. In the Network Configuration screen, click **Edit** in the Network Devices area, enter the IP address and netmask for the Prime Network Services Controller VM, and click **OK**.
3. In the Network Configuration area, enter the hostname, domain name, and IP addresses for the gateway, DNS server, and NTP server.
4. In the Modes screen, choose the required modes, and click **Next**:
5. In the Administrative Access screen, enter the administrator and shared secret passwords with confirming entries.
6. In the Summary screen, confirm that the information is accurate, and then click **Finish**.
7. When prompted, disconnect from the media source and then click **Reboot**. For vSphere 6.5a Webclient, you need to power off the VM and edit the configuration to uncheck the **Connect** check box for ISO disk and then power on the VM again to complete the reboot.
8. To confirm that Prime Network Services Controller is accessible, connect to Prime Network Services Controller through the console for the CLI or a browser for the GUI.

DETAILED STEPS

Step 1 Open the VM console if it is not already open.

If you have just finished configuring the hypervisor, the Prime Network Services Controller 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 Prime Network Services Controller 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 Prime Network Services Controller 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.

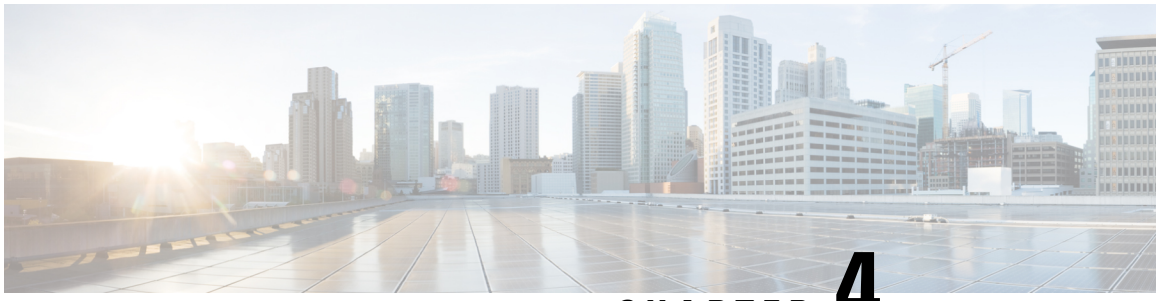
For information on creating a strong password, see Shared Secret Password Criteria, on page 47.

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**. For vSphere 6.5a Webclient, you need to power off the VM and edit the configuration to uncheck the **Connect** check box for ISO disk and then power on the VM again to complete the reboot.
Prime Network Services Controller is then installed on the VM.

Step 8 To confirm that Prime Network Services Controller is accessible, connect to Prime Network Services Controller through the console for the CLI or a browser for the GUI.



CHAPTER 4

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 VMware vSphere software.

Host and VM Requirements

The Cisco VSG has the following requirements:

- ESXi platform running VMware software release 5.x and requiring 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 (1 of type VMXNET3 and 2 of type E1000)
  - 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 1000VE 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 VMware ESX servers. It is controlled by one VSM instance.
ESXi	Virtualization platform used to create the virtual machines as a set of configuration and disk files.
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).
vCenter Server	Service that acts as a central administrator for VMware ESXi hosts that are connected on a network. vCenter Server directs actions on the VMs and the VM hosts.
Virtual Service Engine (VSE)	Part of the Cisco Nexus 1000VE Series switch that switches data traffic. It runs on a ESX/ESXi host. Up to 64 VSEs are controlled by one VSM. All the VSEs that form a switch domain should be in the same virtual data center as defined by the VMware vCenter Server.
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 1000VE Series switch with a VSE 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.
Virtual Security Gateway (VSG)	Cisco software that secures virtual networks and provides firewall functions in virtual environments using the Cisco Nexus 1000VE Series switch by providing network segmentation.

Term	Description
Virtual Supervisor Module (VSM)	Control software for the Cisco Nexus 1000VE 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 1000VE Series switch, configure two VLANs, a service VLAN, and an HA VLAN on the switch uplink ports. (The VLAN does not need to be the system VLAN.)
- On the Cisco Nexus 1000VE Series switch, configure two port profiles for the Cisco VSG: one for the service VLAN and the other for the HA VLAN. (You will be configuring the Cisco VSG IP address on the Cisco VSG so that the Cisco Nexus 1000VE Series switch can communicate with it.)

Details about configuring VLANs and port profiles on the Cisco Nexus 1000VE Series switch are available in the Cisco Nexus 1000VE 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 ISO 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 from an OVA File, on page 59
- Installing the Cisco VSG Software from an ISO File, on page 61

Installing the Cisco VSG Software from an OVA File

To install the Cisco VSG software from an OVA file, obtain the OVA file and either install it directly from the URL or copy the file to the local disk from where you connect to the vCenter Server.

Before you begin

- Specify a name for the new Cisco VSG that is unique within the inventory folder and has up to 80 characters.
- 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

Step 1 Choose the host on which to deploy the Cisco VSG VM.

Step 2 Choose **File** > **Deploy OVF Template**.

Step 3 In the **Deploy OVF Template—Source** window, do the following:

a) Browse to the path to the Cisco VSG OVA file in the **Deploy from a file or URL** field.
b) Click **Next**. The **Deploy OVF Template—OVF Template Details** window opens.

Step 4 In the **Deploy OVF Template—OVF Template Details** window, review the product information including the size of the file and the VM disk and then click **Next**.

Step 5 In the **Deploy OVF Template—End User License Agreement** window, click **Accept** after reviewing the end user license agreement, and then click **Next**.

Step 6 In the **Deploy OVF Template—Name and Location** window, do the following:

a) In the **Name** field, enter a name for the Cisco VSG that is unique within the inventory folder and has up to 80 characters.
b) In the **Inventory Location** pane, choose the location that you would like to use for hosting the Cisco VSG.
c) Click **Next**.

Step 7 In the **Deploy OVF Template—Deployment Configuration** window, do the following:

a) From the **Configuration** drop-down list, choose **Standalone**.
b) Click **Next**.

Note The Standalone Installation for this document is an example in this publication. If you chose Manual Installation mode, you would choose the default values for the following steps. In Standalone mode, be sure to fill in all the fields indicated (they will be indicated on the GUI with red type).

Step 8 In the **Disk Format** dialog box, choose the radio button for the selected format and click **Next**.

Step 9 In the **Host or Cluster** window, choose the host where the Cisco VSG will be installed, and then click **Next**.

Step 10 From the **Select a datastore** field in which to store the VM files pane, choose your datastore, and then click **Next**.

Step 11 Click the drop-down arrows for Data (Service), Management, and HA to associate port profiles, and then click **Next**.

Step 12 In the **Deploy OVF Template—Properties** window, do the following:

a) In the **HaId** field, enter the high-availability identification number for a Cisco VSG pair (value from 1 through 4095).
b) In the **Password** field, enter a password that contains at least one uppercase letter, one lowercase letter, and one number.

c) In the **ManagementIpV4** field, enter the IP address for the Cisco VSG.
d) In the **ManagementIpV4 Subnet** field, enter the subnet mask.
e) In the **Gateway** field, enter the gateway name.
f) In the **VnmcIpV4** field, enter the IP address of the Cisco PNSC.
g) In the **SharedSecret** field, enter the shared secret password defined during the Cisco PNSC installation.
h) In the **ImageName** field, enter the VSG VNM-PA image name (nsc-vsgpa.2.1.3i.bin).
i) Click **Next**.

Note In the following step, make sure that red text messages do not appear before you click **Next**. If you do not want to enter valid information in the red-indicated fields, use null values to fill those fields. If those fields are left empty or filled with invalid null values, the application does not power on. Ignore the Cisco PNSC Restore fields.

Step 13 In the **Ready to Complete** window, review the deployment settings information.

Note Review the IP/mask/gateway information carefully because any discrepancies might cause the VM to have bootup issues.

Step 14 Click **Finish**. The **Deploying Nexus 1000VSG** dialog box opens.

The progress bar in the **Deploying Nexus 1000VSG** dialog box shows how much of the deployment task is completed before the Cisco PNSC is deployed.

Step 15 Wait and click **Close** after the progress indicator shows that the deployment is completed successfully.

Step 16 Power on the Cisco VSG VM.

Step 17 If you chose the Standalone mode for installation earlier, you now see the Cisco VSG login prompt. Log in with your Cisco VSG administration password. You may now proceed with configuring the Cisco Virtual Security Gateway. For details, see the *Cisco Virtual Security Gateway for VMware vSphere Configuration Guide*.

Step 18 If you chose the manual installation in the Configuration field earlier, see Configuring Initial Settings, on page 63 to configure the initial settings on the Cisco VSG.

Note If you are installing high availability (HA), you must configure the software on the primary Cisco VSG before installing the software on the secondary Cisco VSG.

Installing the Cisco VSG Software from an ISO File

You can install the Cisco VSG from an ISO 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.
- 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.

Step 1 Upload the Cisco Virtual Security Gateway ISO image to the vCenter datastore.

Step 2 From the data center in the vSphere Client menu, choose your ESXi host where you want to install the Cisco VSG and choose **New Virtual Machine**.

For VM requirements, see the Host and VM Requirements, on page 57.

For detailed information about how to create a VM, see the VMware documentation.

Step 3 In the **Create New Virtual Machine** dialog box, do the following:

a) Click **Custom** to create a virtual machine.
b) Click **Next**.

Step 4 In the **Create New Virtual Machine** dialog box, do the following:

a) In the **Name** field, add a name for the Cisco VSG.

The Cisco VSG name must be a unique name within the inventory folder and should be up to 80 characters.

b) In the **Inventory Location** field, choose your data center and click **Next**.

Step 5 In the **Datastore** dialog box, choose your datastore from the **Select a datastore** and then click **Next**.

Step 6 In the **Virtual Machine Version** dialog box, click the **Virtual Machine Version**.

Note Keep the selected virtual machine version.

Step 7 In the **Guest Operating System** dialog box, do the following:

a) Click the **Linux** radio button.
b) In the **Version** field, choose **Other 2.6x Linux (32-bit)** from the drop-down list and click **Next**.

Step 8 In the **CPUs** dialog box, choose 1 socket with 2 cores or 2 sockets each with one core, and then click **Next**.

By default, the Cisco VSG virtual machine deployed with OVA has only one1 vCPU. You can choose 2 vCPUs. For an older version of the ESX hosts, you can directly select the number of vCPUs.

Step 9 In the **Memory** dialog box, choose **2 GB** memory size, and then click **Next**.

Step 10 In the **Create Network Connectors** dialog box, do the following:

a) In the **How many NICs do you want to connect?** field, choose **3** from the drop-down list.
b) In the Network area, choose **service**, **management**, and **HA** port profiles in that sequence for the NIC 1, NIC 2, and NIC 3 from the drop-down list. Choose **VMXNET3** for the adapter type for NIC 1. Choose **E1000** for the adapter type for NIC 2 and NIC 3.

Step 11 Click **Next**. The **SCSI Controller** dialog box opens.

The radio button for the default SCSI controller is chosen.

Step 12 Click **Next**. The **Select a Disk** dialog box opens.

The radio button for the default disk is chosen.

Step 13 Click **Next**. The **Create a Disk** dialog box opens.

The default virtual disk size and policy is chosen.

Step 14 Click **Next**. The **Advanced Options** dialog box opens.

The default options are chosen.

Step 15 Click **Next**. The **Ready to Complete** dialog box opens.

Step 16 Review your settings in the **Settings for the new virtual machine** area.

Step 17 Check the **Edit the virtual machine before completion** check box and click **Continue** to open a dialog box with the device details.

Step 18 In the Work pane, choose your **New CD/DVD (adding)** in the **Hardware** area.

Step 19 Click **Datastore ISO File**, and select your ISO file from the drop-down list.

Step 20 In the work pane, check the **Connect at power on** check box and click **Finish**.The **Summary tab** window opens.

The **Create virtual machine status** completes.

Step 21 From the **vSphere Client** menu, choose your recently installed VM.

Step 22 In the work pane, click **Power on the virtual machine**.

Step 23 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.

Note To allocate additional RAM, right-click the **VM** icon to power off the VM and then choose **Power** > **Power Off** from the dialog box. After the VM is powered down, edit the configuration settings on the VM for controlling memory resources.

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 65 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 on your vSphere Client. For details about installing Cisco VSG, see Installing the Cisco VSG Software, on page 59 in this chapter.

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.

Your Cisco Virtual Security Gateway Software Installation Method	Do You Need to Proceed with "Configuring Initial Settings"?
Installing an ISO file.	Yes. Proceed with configuring initial settings described in this section.

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

Cisco Nexus 1000VE 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 `Enable the telnet service? (yes/no)[y]:` 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**.

The following configuration will be applied:

```
Interface mgmt0
ip address 10.10.10.11 255.255.255.0
no shutdown
vrf context management
ip route 0.0.0.0/10.10.11.1
no telnet server enable
ssh key rsa 768 force
ssh server enable
no feature http-server
ha-pair id 25
```

Step 14 At the `Would you like to edit the configuration? (yes/no)[n]` prompt, enter **n**and press **Enter**.

Step 15 At the `Use this configuration and save it? (yes/no)[y]:` prompt, enter **y**and press **Enter**.

Step 16 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 17 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.

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

Cisco Nexus 1000VE 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:

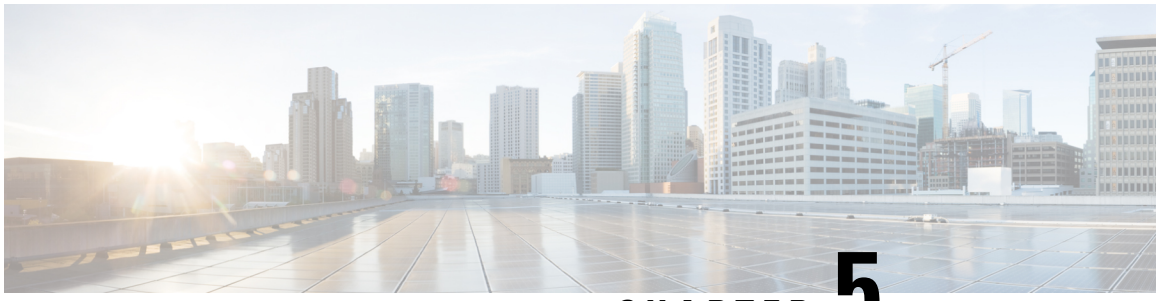
Command	Purpose
show interface brief	Displays brief status and interface information.
show vsg	Displays the Cisco VSG and system-related information.

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: 3437
VSG software version: 5.2(1)VSG2(2.2) build [5.2(1)VSG2(2.2)]
PNSC IP: 10.193.75.73
```

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 5

Registering Devices With the Cisco Prime NSC

This chapter contains the following sections:

Registering a Cisco VSG

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

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

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

Step 2 On the command line, enter configuration mode.

```
vsg# configure
```

Step 3 Enter the config-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: nsc-vsgpa.2.1.3i.bin
```

Step 7 Exit all modes.

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

Step 8 On the Cisco VSG command line, enter the **show nsc-pa status** command:

```
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(3i)-vsg"
The Cisco VSG registration is complete.
```

Step 9 Save the change persistently through reboots and restarts by copying 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 a Cisco Nexus 1000VE VSM

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

Step 1 Copy the vsmcpa.3.2.3a.bin file into the VSM bootflash:

```
vsm# copy ftp://guest@172.18.217.188/n1kv/vsmcpa.3.2.3a.bin bootflash:
```

Step 2 On the command line, enter 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.3.2.3a.bin
```

Step 7 Exit all modes.

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

Step 8 On the command line, enter the following command:

```
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(3a)-vsm
The Cisco Nexus 1000V VSM registration is complete.
```

Step 9 On the command line, enter the following command:

```
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 Prime Network Services Controller CLI Configuration Guide* for detailed information about configuring the Cisco PNSC using the CLI.

Registering vCenter 6.0

Step 1 Log into Cisco PNSC.
Step 2 Choose **Resource Management** > **VM Managers**.
Step 3 In the **Navigation** pane, right-click **VM Managers**.
Step 4 Choose **Export vCenter Extension**.
Step 5 In the dialog box that appears, choose the appropriate extension, and click **Save**.
Step 6 Log into **vSphere**.
Step 7 In your vSphere client, log into **vCenter**.
Step 8 Choose **Plug-ins** > **Manage Plug-ins**.
Step 9 Right-click the empty space and click **New Plug-in**.
Step 10 Browse to the Cisco PNSC vCenter extension file, and then click **Register Plug-in**.
Step 11 Click **Ignore** for any security warning.

You should see a message that reports a successful registration.

Step 12 Log into the Cisco PNSC and choose **Resource Management** > **VM Managers**.
Step 13 In the **Navigation** pane, right-click **VM Managers**.
Step 14 Click **Add VM Manager**.
Step 15 Enter the vCenter name and IP address information and click **OK**.

Note The Successful Addition State field should display the word Enabled, and the Operational State field should display the version information.

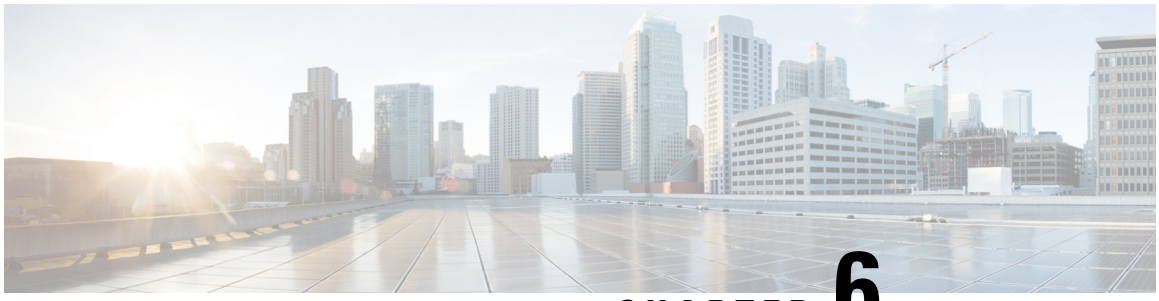
vCenter is registered.

Registering vCenter 6.5

Step 1 Log into the Cisco PNSC and choose **Resource Management** > **VM Managers**.
Step 2 In the **Navigation** pane, right-click **VM Managers**.
Step 3 Click **Add VM Manager** on the pop-up menu.
Step 4 In the **Add VM Manager** window, enter the vCenter name and IP address in the **Name** and **Hostname/IP Address** textfields.
Step 5 Select **vCenter 6.5 and greater** option and enter vCenter username and password in the **User-Name/Domain-Name** and **Password** text-fields.
Step 6 Click **OK**

Note On the **VM Managers** tab, the **Operational State** field should display the word up, and the**Version** field should display the version information.

vCenter is registered.



CHAPTER 6

Upgrading the Cisco Prime NSC

This chapter contains the following sections:

Complete Upgrade Procedure

For information on the migration of Cisco Nexus 1000V with VSG to Cisco Nexus 1000VE with VSG, see the *Cisco Nexus 1000VE Installation Guide, Release 5.2(1)SV5(1.1)*

Information About Cisco Prime NSC Upgrades

When you upgrade the Cisco PNSC software, all current command-line interface (CLI) and graphical user interface (GUI) sessions are interrupted, which means that you must restart any CLI or GUI sessions.

PNSC Upgrade Matrix and Path

Migration of Nexus 1000V to Nexus 1000VE includes upgrading PNSC to version 3.5.1a. The following table lists the compatibility information for the PNSC upgrade.

Table 2: Cisco VNMC/PNSC Upgrade Path

Initial Version	Intermediate State(s)	Final Version
3.4.2c	NA	3.5.1a
3.4.2d	NA	3.5.1a

Note For detailed information about Upgrading PNSC, see Upgrading Prime Network Services Controller.

Upgrade Procedure for Cisco PNSC Release 3.4.2d to Release 3.5.1

Upgrading Cisco Prime NSC 3.4.2d to Cisco Prime NSC 3.5.1a

Before you begin

- You are logged in to the CLI in EXEC mode.
- You have backed up the new software files to a remote server and have verified that the backup file was created on the remote server.
- You must have the Cisco PNSC Release 3.5.1 downloaded.

SUMMARY STEPS

1. nsc# **connect local-mgmt**
2. (Optional) nsc (local-mgmt)# **show version**
3. (Optional) nsc (local-mgmt)# **copy scp://user@***example-server-ip/example-dir/filename* **bootflash:/**
4. nsc (local-mgmt)# **dir bootflash:/**
5. nsc (local-mgmt)# **update bootflash:/***filename*
6. (Optional) nsc (local-mgmt)# **service status**
7. (Optional) nsc (local-mgmt)# **show version**

DETAILED STEPS

	Command or Action	Purpose
Step 1	nsc# **connect local-mgmt**	Places you in local management mode.
Step 2	(Optional) nsc (local-mgmt)# **show version**	Displays the version information for the Cisco PNSC software.
Step 3	(Optional) nsc (local-mgmt)# **copy scp://user@***example-server-ip/example-dir/filename* **bootflash:/**	Copies the Cisco PNSC software file to the VM.
Step 4	nsc (local-mgmt)# **dir bootflash:/**	Verifies that the desired file is copied in the directory.
Step 5	nsc (local-mgmt)# **update bootflash:/***filename*	Begins the update of the Cisco PNSC software.
Step 6	(Optional) nsc (local-mgmt)# **service status**	Allows you to verify that the server is operating as desired.
Step 7	(Optional) nsc (local-mgmt)# **show version**	Allows you to verify that the Cisco PNSC software version is updated.

	Command or Action	Purpose
		Note After you upgrade to Cisco PNSC Release 3.5.1, you might see the previous version of Cisco PNSC in your browser. To view the upgraded version, clear the browser cache and browsing history in the browser. This note applies to all supported browsers: Internet Explorer, Mozilla Firefox, and Chrome. **Note** For detailed information about Upgrading PNSC, see Upgrading Prime Network Services Controller.

Configuration Example

The following example shows how to connect to the local-mgmt mode:

```
nsc# connect local-mgmt
Cisco Prime Network Services Controller
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2018, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
```

The following example shows how to display version information for the Cisco PNSC:

```
nsc(local-mgmt)# show version

Name Package Version GUI
---- ------- ------- ----
core Base System 3.4(2b) 3.4(2b) service-reg
Service Registry 3.4(2b) 3.4(2b) policy-mgr
Policy Manager 3.4(2b) 3.4(2b) resource-mgr
Resource Manager 3.4(2b) 3.4(2b) vm-mgr
VM manager 3.4(2b) none vsm-service
VSM Service 3.4(2d) none cloudprovider-mgr
Cloud Provider Mgr 3.4(2d) none
localhost(local-mgmt)#
```

The following example shows how to copy the Cisco PNSC software to the VM:

```
nsc(local-mgmt)# copy scp://<user@example-server-ip>/example1-dir/nsc.3.5.1.bin bootflash:/
Enter password:
100%  143MB  11.9MB/s   00:12
```

The following example shows how to see the directory information for Cisco PNSC:

```
nsc(local-mgmt)# dir bootflash:/

    1.1G Dec 05 00:57 nsc.3.5.1.bin

Usage for bootflash://
```

```
             6359716 KB used
            10889320 KB free
            18187836 KB total
```

The following example shows how to start the update for the Cisco PNSC:

```
nsc(local-mgmt)# update bootflash:/nsc.3.5.1.bin
It is recommended that you perform a full-state backup before updating any VNMC component.
  Press enter to continue or Ctrl-c to exit.
```

The following example shows how to display the updated version for the Cisco PNSC:

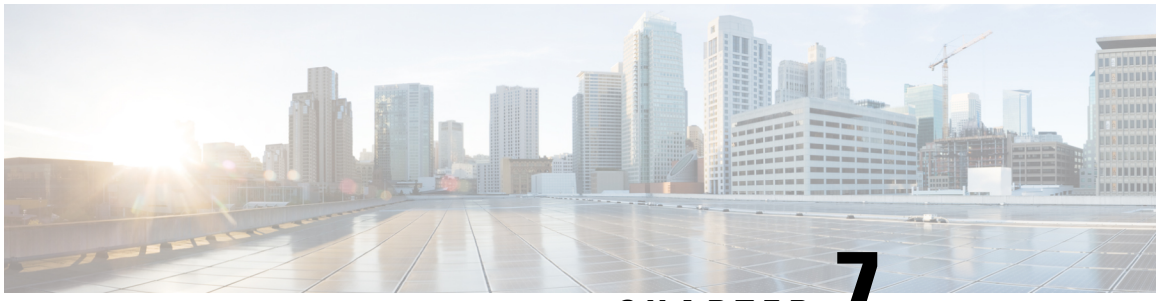
```
nsc(local-mgmt)# show version

Name                Package             Version        GUI
---- ------- ------- ----
core                Base System         3.5.1        3.5.1
service-reg         Service Registry    3.5.1        3.5.1
policy-mgr          Policy Manager      3.5.1        3.5.1
resource-mgr        Resource Manager    3.5.1        3.5.1
vm-mgr              VM manager          3.5.1        none
cloudprovider-mgr   Cloud Provider Mgr  3.5.1        none
```

What to do next

After the migration from Cisco Prime NSC 3.4.2d to Cisco Prime NSC 3.5.1a, VM names are not displayed under PNSC and as a result there is traffic drop for rules with VM name information.

Follow the below workaround to overcome the issue:

1. Upgrade from existing PNSC 3.4.2c/d with PNSC 3.5.1a VSM and VSG.
2. Register Policy Agent (PA) of PNSC 3.5.1a VSM and VSG to PNSC 3.4.2c/d.
3. Create Firewall object for PNSC 3.5.1a VSG with different data IP (to be later configured on PNSC 3.5.1a VSM) on PNSC 3.4.2c/d.
4. Migrate to PNSC 3.5.1a VSG with data IP (to be provided in the migration config text field).
5. After migration is complete, PNSC 3.4.2c/d is now attached to PNSC 3.5.1a VSM and VSG. This leads to VM Info loss in PNSC.
6. Upgrade PNSC 3.4.2 c/d to PNSC 3.5.1a . The VM Info gets populated on PNSC.
7. Re-register PNSC 3.5.1a VSM and VSG Policy Agent (PA) and the traffic is restored.



CHAPTER 7

Examples of Cisco Prime NSC OVA Template Deployment and Cisco Prime NSC ISO Installations

This chapter contains the following sections:

OVA Installation Using vSphere Installer 6.0 and Later

Before you begin

- Ensure that you have the Virtual Supervisor Module (VSM) IP address available
- Ensure that you have all the proper networking information available, including the IP address you will use for your Cisco PNSC instance
- Ensure that you have the Cisco Prime NSC ova image

Step 1 Open your vSphere client.

Step 2 Click **Hosts and Clusters** and choose an ESXi host.

Step 3 (Optional) For 6.5 and later, right-click ESXi host and from the pop-up menu, choose **Deploy OVF Template**.

Step 4 In the **Deploy OVF Template** dialog box, click **Browse** to choose an .ova file on your local machine, or choose a file from another location (URL).

Step 5 From the **Open** dialog box, choose the appropriate .ova file and click **Open**.

Step 6 Click **Next**.

The **OVF Template Details** dialog box appears inside the **Deploy OVF Template** dialog box. The **OVF Template Details** dialog box is the first of ten pages in the **Deploy OVF Template** dialog box that you use to set parameters for the Cisco? PNSC instance.

Step 7 View your template details and click **Next**.

Step 8 In the **User License Agreement** window, view the license and click **Accept**.

Step 9 Click **Next**.

Step 10 In the **Name and Location** window, do the following:

a) In the **Name** field, enter a template name.
b) In the **Inventory Location** area, choose the appropriate folder and click **Next**.

Step 11 In the **Deploy Configuration** window, from the Configuration drop-down list, choose **NSC Installer** and click **Next**.

Step 12 In the **Resource Pool** window, choose the appropriate location to deploy the Cisco PNSC and click **Next**.

Step 13 In the **Storage** window, choose an appropriate location to store the virtual machine files and click **Next**.

Step 14 In the **Display Format** window, keep default settings and click **Next**.

Step 15 In the **Network Mapping** window, choose an appropriate configured management network VLAN for Cisco PNSC and click **Next**.

Step 16 In the **Properties** window, in the **IP Address** area, do the following:

a) Enter an IP address in the **IPv4 IP Address** field.
b) Enter an IP netmask in the **IPv4 IP Netmask** field.
c) Enter a gate address in the **IPv4 Gateway** field.

Note The netmask is defaulted to 255.255.255.0.

Step 17 In the **NSC DNS** area, do the following:

a) Enter the host name in the **Host Name** field.
b) Enter an IP address in the **NSC IP** field.

Step 18 In the **NSC NTP** area, enter the NTP server IP address in the **NTP server** field.

Step 19 In the **NSC Password** area, enter a password in the **NSC Password** field or the **NSC Secret** field.

Note You enter the admin password in the **Password** field.

Step 20 Click **Next**.

Step 21 In the **Ready to Complete** window, verify the configuration details for Cisco PNSC and click **Finish** to deploy Cisco PNSC on the selected ESXi host.

Note Select **Power on after deployment** check box to start Cisco PNSC immediately after the deployment completes.

The progress dialog box appears. Once the virtual machine is installed, the **Deployment Completed Successfully** dialog box opens.

Step 22 Click **Close**.

The Cisco PNSC instance is created.

PNSC Installation Using an ISO Image

Step 1 Download a Cisco PNSC ISO to your client machine.

Step 2 Open a vCenter client.

Step 3 Create a virtual machine on the appropriate host as follows:

a) Ensure your virtual machine size is 220 GB split into two disks (Disk1 having 20GB and Disk2 having 200GB).
b) Ensure your virtual machine has 4 GB of RAM.
c) Choose **Red Hat Enterprise Linux 5 64-bit** as your operating system.

Step 4 Power on your virtual machine.

Step 5 Mount the ISO to the virtual machine CD ROM drive as follows:

a) Right-click the virtual machine and choose **Open the VM Console**.
b) From the virtual machine console, click Connect/Disconnect CD/DVD Devices.
c) Choose **CD/DVD Drive1**.
d) Choose **Connect to ISO Image on Local Disk**.
e) Choose the ISO image that you downloaded.

Step 6 Reboot the VM using VM, Guest, and press **Ctrl-Alt-Del**.

Step 7 In the ISO installer, enter the appropriate values in the **ISO installer** field.

Step 8 Once installation is completed, click **Reboot** to create the Cisco PNSC instance.