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

This chapter contains the following sections:

- Information About Installing the Cisco Prime NSC and the Cisco VSG, page 1
- Task 1: Installing the Cisco Prime NSC from an OVA Template, page 9
- Task 2: On the Cisco Prime NSC, Setting Up VM-Mgr for vCenter Connectivity, page 11
- Task 3: On the VSM, Configuring the Cisco Prime NSC Policy Agent, page 13
- Task 4: On the VSM, Preparing Cisco VSG Port Profiles, page 14
- Task 5: Installing the Cisco VSG from an OVA Template, page 15
- Task 6: On the Cisco VSG and Cisco Prime NSC, Verifying the VNM Policy-Agent Status, page 18
- Task 7: On the Cisco Prime NSC, Configuring a Tenant and Security Profile, page 18
- Task 8: On the Cisco Prime NSC, Importing Service Image, page 20
- Task 9: On the Cisco Prime NSC, Adding a Compute Firewall, page 20
- Task 10: On the Cisco Prime NSC, Configuring a Permit-All Rule, page 23
- Task 11: On the Cisco VSG, Verifying the Permit-All Rule, page 24
- Task 12: Enabling Logging, page 24
- Task 13: Enabling the Traffic VM Port-Profile for Firewall Protection and Verifying the Communication Between the VSM, VEM, and VSG, page 25
- Task 14: Sending Traffic Flow and on the Cisco VSG Verifying Statistics and Logs, page 27

Information About Installing the Cisco Prime NSC and the Cisco VSG

This chapter describes how to install and set up a basic working configuration of the Cisco Prime NSC 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 1000V Series switch is operational, and endpoint VMs are already installed.

Cisco VSG and Cisco Prime NSC Installation Planning Checklists

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

Basic Hardware and Software Requirements

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

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

Requirement	Description
Four Virtual CPUs	1.5 GHz for each Virtual CPU
Memory	4 GB RAM for the Cisco VSG and 4 GB RAM for the Cisco Prime NSC 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	ESXi 5.0, 5.1, and 5.5

Requirement	Description
VMware vCenter	Release 5.5 (5.1 vCenter supports host version upto 5.1)
Intel Virtualization Technology (VT)	Enabled in the BIOS
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 Prime NSC, you must disable the Adobe Flash Players that are installed by default with Chrome. For more information, see Configuring Chrome for Use with Cisco Prime NSC.
Ports	Access to the Cisco Prime NSC 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 Nexus1000V Multi-Hypervisor License. You need to install the Nexus1000V Multi-Hypervisor License for Cisco VSG for VMware vSphere. The Cisco N1kv VSM is available in two modes: essential and advanced. VSG functionality is available only in the advanced mode. You need to install the Nexus1000V Multi-Hypervisor License and change the VSM mode to advanced mode. When the Nexus1000V Multi-Hypervisor License is installed, the license for Cisco VSG is automatically included.

Note If you try to access VSG services with VSM in essential mode, an error message is generated on VSM console indicating that the Nexus1000V Multi-Hypervisor License is required for VSG.

The Nexus1000V Multi-Hypervisor License is available in three different types:

- Default: The Nexus 1000v switch may be configured in Essential or Advanced mode.
  - Essential Mode: Not Supported.
  - Advanced Mode: After upgrading the software, Nexus1000V Multi-Hypervisor License is available with 1024 Socket Count and expires in 60 days.

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

- Evaluation: The Nexus 1000V switch should be in Advanced mode. After upgrading the software, Nexus1000V Multi-Hypervisor License is available with1024 Socket Count and expires in 60 days.
- Permanent: The Nexus 1000V switch should be in Advanced mode. After upgrading the software, Nexus1000V Multi-Hypervisor License is available with 1024 Socket Count and expires in 60 days.

Note You have to request for an evaluation or permanent Nexus1000V Multi-Hypervisor License.

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

VLAN Configuration Requirements

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

- You must have two VLANs that are configured on the Cisco Nexus 1000V 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 1000V 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 1000V Series switch can communicate with it)

Required Cisco Prime NSC and Cisco VSG Information

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

Type	Your Information
Cisco VSG name—Unique within the inventory folder and up to 80 characters	

Type	Your Information
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 Prime NSC instance IP address	
Mode for installing the Cisco VSG	• Standalone • HA primary • HA secondary • Manual installation
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)	
NSC DNS IP address	
NSC NTP IP address	
Cisco VSG admin password	
Cisco Prime NSC admin password	
Cisco VSM admin password	

Type	Your Information
Shared secret password (Cisco Prime NSC, Cisco VSG policy agent, Cisco VSM policy agent)	

Tasks and Prerequisites Checklist

Tasks	Prerequisites
Task 1: Installing the Cisco Prime NSC from an OVA Template, on page 9	Make sure that you know the following: • The Cisco Prime NSC OVA image is available in the vCenter. • Know the IP/subnet mask/gateway information for the Cisco Prime NSC. • 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 Prime NSC 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 Prime NSC, VSM, and Cisco VSG).
Task 2: On the Cisco Prime NSC, Setting Up VM-Mgr for vCenter Connectivity, on page 11	Make sure that you know the following: • Supported Adobe Flash Player given in System Requirements • IP address of the Cisco Prime NSC • The password for Admin user

Tasks	Prerequisites
Task 3: On the VSM, Configuring the Cisco Prime NSC Policy Agent, on page 13	Make sure that you know the following: • The Cisco Prime NSC policy-agent image is available on the VSM (for example, vnmc-vsmpa.2.1.1e.bin) **Note** The string **vsmpa** must appear in the image name as highlighted. • The IP address of the Cisco Prime NSC • The shared secret password you defined during the Cisco Prime NSC installation • That IP connectivity between the VSM and the Cisco Prime NSC 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 Prime NSC image bundle to boot from a flash drive and to complete registration with the Cisco Prime NSC.
Task 4: On the VSM, Preparing Cisco VSG Port Profiles, on page 14	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 15	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 Prime NSC 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 Prime NSC IP address • The shared secret password • The IP connectivity between Cisco VSG and Cisco Prime NSC is okay. • The Cisco VSG VNM-PA image name (vnmc-vsgpa.2.1.1b.bin) is available.
Task 6: On the Cisco VSG and Cisco Prime NSC, Verifying the VNM Policy-Agent Status, on page 18	—
Task 7: On the Cisco Prime NSC, Configuring a Tenant and Security Profile, on page 18	Make sure that you know the following: • Supported Adobe Flash Player given in System Requirements • The IP address of the Cisco Prime NSC • The password for Admin user
Task 8: On the Cisco VNMC, Assigning the Cisco VSG to the Compute Firewall	—
Task 10: On the Cisco Prime NSC, Configuring a Permit-All Rule, on page 23	—

Tasks	Prerequisites
Task 11: On the Cisco VSG, Verifying the Permit-All Rule, on page 24	—
Task 12: Enabling Logging, on page 24	—
Task 13: Enabling the Traffic VM Port-Profile for Firewall Protection and Verifying the Communication Between the VSM, VEM, and VSG, on page 25	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 (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 27	—

Host Requirements

- ESXi platform that runs VMware software release 5.0 , 5.1, and 5.5 with a minimum of 4 GB physical RAM for the Cisco VSG and 4 GB physical RAM for the Cisco Prime NSC.
- 1 processor
- Four Virtual CPUs with speed of 1.5 GHz for each virtual CPU

Obtaining the Cisco Prime NSC 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 Prime NSC software is available for download at the following URL:

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

Task 1: Installing the Cisco Prime NSC from an OVA Template

Before You Begin

Know the following:

- The Cisco Prime NSC OVA image is available in the vCenter.
- Know the IP/subnet mask/gateway information for the Cisco Prime NSC.
- 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 Prime NSC 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 Prime NSC, 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 Prime NSC VM.

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

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

Step 5 In the **OVF Template Details** window, review the details of the Cisco Prime NSC 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 Prime NSC Restore fields.

Note For choosing the shared secret password, follow the guidelines given in 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 Prime NSC is deployed.

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

Step 15 Power on the Cisco VSG VM.

Task 2: On the Cisco Prime NSC, Setting Up VM-Mgr 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 Prime NSC, on page 11
- Registering the vCenter Extension Plugin in the vCenter, on page 12
- Configuring the vCenter in VM Manager in the Cisco Prime NSC, on page 12

Downloading the vCenter Extension File from the Cisco Prime NSC

Before You Begin

Make sure that you have the following:

- Supported Adobe Flash Player given in System Requirements
- IP address of the Cisco Prime NSC
- The password for Admin user

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

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

Step 3 In the Cisco Prime NSC login window, enter the username **admin** and the admin user password. This is the password that you set when installing the Cisco Prime NSC.

Step 4 In the Cisco Prime NSC window, choose **Resource Management** > **VM Managers** > **VM Managers.**

Step 5 In the VM Managers pane, click **Export vCenter Extension**.

Step 6 Save the vCenter extension file in a directory that the vSphere Client can access, because you will need to register the vCenter extension plug-in from within the vSphere Client (see Registering the vCenter Extension Plugin in the vCenter, on page 12).

What to Do Next

Go to Registering the vCenter Extension Plugin in the vCenter, on page 12.

Registering the vCenter Extension Plugin in the vCenter

This task is completed within your client desktop vSphere client directory

Before You Begin

See Downloading the vCenter Extension File from the Cisco Prime NSC, on page 11.

Step 1 From the VMware vSphere Client, log into the vCenter server.

Step 2 In the **vSphere Client** window, choose **Plug-ins** > **Manage Plug-ins**.

Step 3 Right-click the window background and choose **New Plug-in**.

Step 4 Browse to the Cisco Prime NSC vCenter extension file that you previously downloaded and click **Register Plug-in**.
The vCenter Register Plug-in Window appears, displaying a security warning.

Step 5 In the security warning message box, click **Ignore**.
A progress indicator shows the task status.

Step 6 When the success message is displayed, click **OK**, then click **Close**.

What to Do Next

Go to Configuring the vCenter in VM Manager in the Cisco Prime NSC, on page 12.

Configuring the vCenter in VM Manager in the Cisco Prime NSC

Before You Begin

See Task 2: On the Cisco Prime NSC, Setting Up VM-Mgr for vCenter Connectivity, on page 11.

Step 1 In Cisco Prime NSC, 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 Click **OK**.

Note A successfully added VM Manager is displayed with the following information:

- Admin State of *enable*
- Operational State of *up*
- VMware vCenter version

Task 3: On the VSM, Configuring the Cisco Prime NSC Policy Agent

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

Before You Begin

Make sure that you know the following:

- The Cisco Prime NSC policy-agent image is available on the VSM (for example, vnmc-vsmpa.2.1.1e.bin)

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

- The IP address of the Cisco Prime NSC
- The shared secret password you defined during the Cisco Prime NSC installation
- That IP connectivity between the VSM and the Cisco Prime NSC 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 Prime NSC image bundle to boot from a flash drive and to complete registration with the Cisco Prime NSC.

Step 1 On the VSM, enter the following commands:

```
vsm# configure terminal
vsm(config)# vnm-policy-agent
vsm(config-vnm-policy-agent)# registration-ip 10.193.75.95
vsm(config-vnm-policy-agent)# shared-secret Example_Secret123
vsm(config-vnm-policy-agent)# policy-agent-image vnmc-vsmpa.2.1.1e.bin
vsm(config-vnm-policy-agent)# exit
vsm(config)# copy running-config startup-config
vsm(config)# exit
```

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

```
vsm# show vnm-pa status
VNM Policy-Agent status is - Installed Successfully. Version 2.1(1e)-vsm
vsm
```

The VSM is now registered with the Cisco Prime NSC.

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

```
vsm# show vnm-pa status
VNM Policy-Agent status is - Installation Failure
VNMC not reachable.
vsm#
```

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

```
vsm# show vnm-pa status
VNM 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 uplink
vsm(config-port-prof)# switchport trunk allowed vlan add 100, 200
vsm(config-port-prof)# exit
vsm(config)#
```

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 Prime NSC 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 Prime NSC IP address
- The shared secret password
- The IP connectivity between Cisco VSG and Cisco Prime NSC is okay.
- The Cisco VSG VNM-PA image name (vnmc-vsgpa.2.1.1b.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 Prime NSC.

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 Prime NSC.

i) In the **SharedSecret** field, enter the shared secret password defined during the Cisco Prime NSC installation.

j) Click **Next.**

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

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 Prime NSC 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 Prime NSC 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 Prime NSC, Verifying the VNM Policy-Agent Status

You can use the **show vnm-pa status** command to verify the VNM 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 VNM-PA configuration by entering the following command:

```
vsg# show vnm-pa status
VNM Policy-Agent status is - Installed Successfully. Version 2.1(1b)-vsg
vsg#
```

Step 3 Log in to the Cisco Prime NSC.

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

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

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

This task includes the following subtasks:

- Configuring a Tenant on the Cisco Prime NSC, on page 19
- Configuring a Security Profile on the Cisco Prime NSC, on page 19

Before You Begin

Make sure that you know the following:

- Supported Adobe Flash Player given in System Requirements
- The IP address of the Cisco Prime NSC

- The password for Admin user

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

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

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

Step 4 In the Cisco Prime NSC main window, choose **Administration** > **Service Registry** > **Clients** to check the Cisco VSG and VSM registration in the Cisco Prime NSC.
The **Clients** pane lists the Cisco VSG and VSM information.

What to Do Next

Go to Configuring a Tenant on the Cisco Prime NSC, on page 19

Configuring a Tenant on the Cisco Prime NSC

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 Prime NSC.

Step 1 In the Cisco Prime NSC, 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 Prime NSC, on page 19

Configuring a Security Profile on the Cisco Prime NSC

You can configure a security profile on the Cisco Prime NSC.

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 Prime NSC, Adding a Compute Firewall, on page 20. 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 Prime NSC, Importing Service Image, on page 20.

Task 8: On the Cisco Prime NSC, Importing Service Image

This step is required to instantiate a VSG service device from an image in Task 9: On the Cisco Prime NSC, Adding a Compute Firewall, on page 20. This step is not required for assigning a VSG or VSG pool option in Task 9: On the Cisco Prime NSC, Adding a Compute Firewall, on page 20.

Step 1 Log in to the Cisco Prime NSC.

Step 2 Choose **Resource Management** > **Resources** > **Service Devices** > **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.VSG2.1.1.ova.

Task 9: On the Cisco Prime NSC, 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 Prime NSC 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 Prime NSC. For more information, see Task 6: On the Cisco VSG and Cisco Prime NSC, Verifying the VNM Policy-Agent Status, on page 18.
- To assign a Cisco VSG pool, a Cisco VSG 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 Prime NSC. For more information on importing service images, see Task 8: On the Cisco Prime NSC, Importing Service Image, on page 20.

Step 1 Log in to the Cisco Prime NSC.

Step 2 Choose **Resource Management** > **Managed Resources** > **root** > *tenant* > **Compute Firewalls**.

Step 3 In the General tab, click **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 22, 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 22, 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 Prime NSC, Configuring a Permit-All Rule

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

Step 1 Log in to the Cisco Prime NSC.

Step 2 In the Cisco Prime NSC 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

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

```
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 24
- Enabling Global Policy-Engine Logging, on page 25

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 Prime NSC.

Step 2 In the Cisco Prime NSC 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 25.

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 Prime NSC.

Step 2 In the Cisco Prime NSC 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, VEM, and VSG

This section includes the following topics:

Enabling Traffic VM Port-Profile for Firewall Protection , on page 26
Verifying the VSM or VEM for Cisco VSG Reachability, on page 26
Checking the VM Virtual Ethernet Port for Firewall Protection, on page 27

Before You Begin

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 (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

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.

```
vsm(config)# port-profile type vethernet pp-webserver
   vmware port-group
   switchport mode access
   switchport access vlan 756
   no shutdown
   state enabled
```

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 VEM for Cisco VSG Reachability, on page 26.

Verifying the VSM or VEM for Cisco VSG Reachability

This example shows how to verify the communication between the VEM 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:Vsg215
```

```
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 VEM 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:

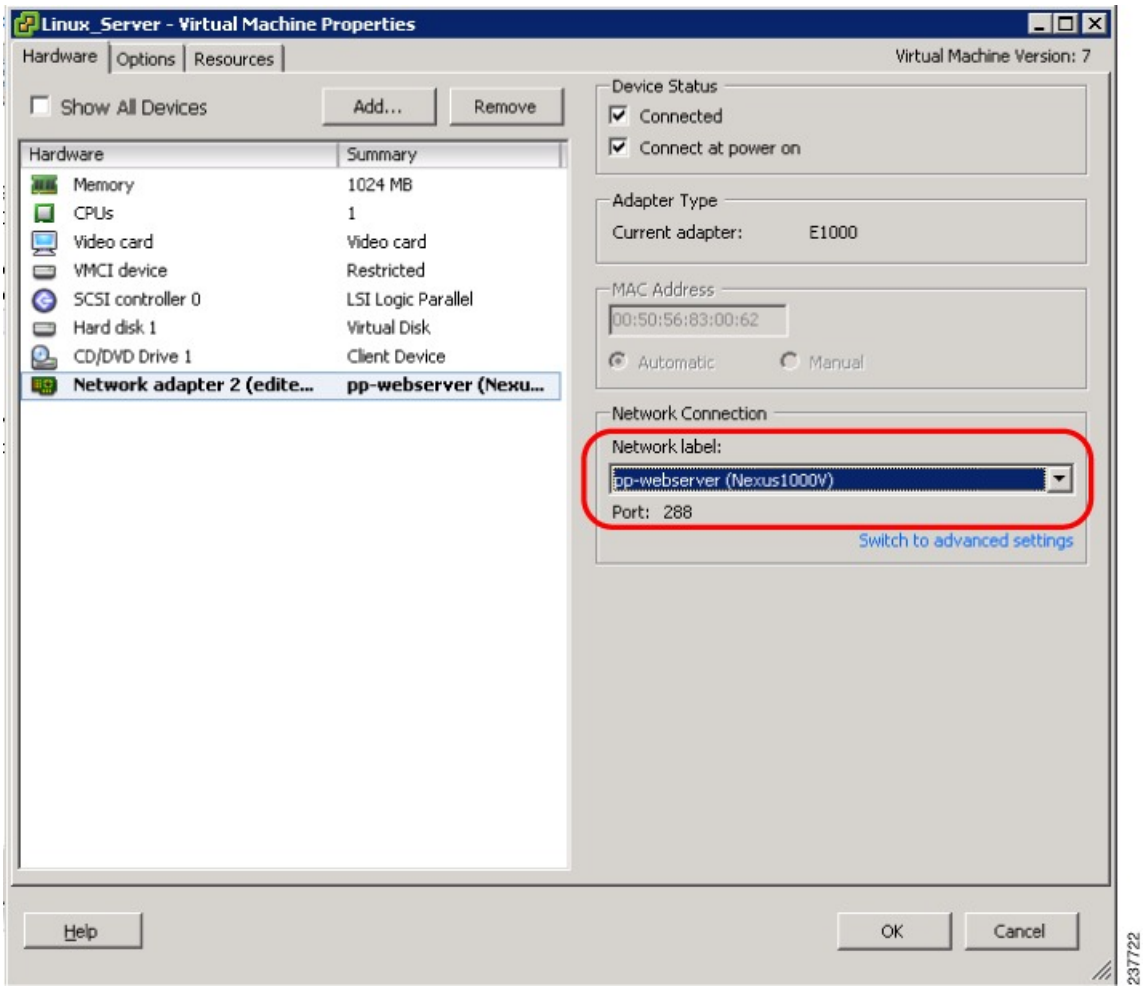
- Sending Traffic Flow, on page 28
- Verifying Policy-Engine Statistics and Logs on the Cisco VSG, on page 29

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 1: 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 29.

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
```