Installing the Cisco VSG and the Cisco VNMC-Quick Start

This chapter contains the following sections:

Information About Installing the Cisco VNMC and the Cisco VSG

This chapter describes how to install and set up a basic working configuration of the Cisco VNMC 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 VNMC Installation Planning Checklists

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

Basic Hardware and Software Requirements

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

- x86 Intel or AMD server with 64-bit processor listed in the VMware compatibility matrix
- Intel VT enabled in the BIOS
- VMware ESX 4.1, 5.0, or 5.1
- ESX or ESXi platform that runs VMware software release 4.1. or 5.0 with a minimum of 4-GB physical RAM for the Cisco VSG and similar for the Cisco VNMC or 6 GB for both.
- VMware vSphere Hypervisor
- VMware vCenter 5.0 (4.1 VMware supports only 4.1 host)
- 1 processor
- CPU speed of 1.5 Ghz
- Datastore with at least 25-GB disk space available on shared NFS/SAN storage when the Cisco VNMC is deployed in an HA cluster
- Internet Explorer 8.0 or Mozilla Firefox 3.6.x on Windows
- Flash 10.0 or 10.1
- Cisco VSG software available for download at http://www.cisco.com/en/US/products/ps11208/index.html
- Cisco VNMC software available for download at http://www.cisco.com/en/US/products/ps11213/index.html

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 VNMC and Cisco VSG Information

The following information can be used later during the Cisco VNMC 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 VNMC 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)	
Cisco VSG admin password	
Cisco VNMC admin password	

Type	Your Information
Cisco VSM admin password	
Shared secret password (Cisco VNMC, Cisco VSG policy agent, Cisco VSM policy agent)	

Tasks and Prerequisites Checklist

Tasks	Prerequisites
Task 1: Installing the Cisco VNMC from an OVA Template, on page 7	Make sure that you know the following: • The Cisco VNMC OVA image is available in the vCenter. • Know the IP/subnet mask/gateway information for the Cisco VNMC. • Know the admin password, shared_secret, hostname that you want to use. • Know the DNS server and domain name 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 VNMC management interface. • The host has 2-GB RAM and 25-GB available hard-disk space. • A shared secret password is available (this password enables communication between the Cisco VNMC, VSM, and Cisco VSG).
Task 2: On the Cisco VNMC, Setting Up VM-Mgr for vCenter Connectivity, on page 15	Make sure that you know the following: • Install Adobe Flash Player (Version 10.1.102.64) • IP address of the Cisco VNMC • Admin user password

Tasks	Prerequisites
Task 3: On the VSM, Configuring the Cisco VNMC Policy Agent, on page 19	Make sure that you know the following: • The Cisco VNMC policy-agent image is available on the VSM (for example, vnmc-vsmpa.2.1.1b.bin) **Note** The string **vsmpa** must appear in the image name as highlighted. • The IP address of the Cisco VNMC • The shared secret password you defined during the Cisco VNMC installation • That IP connectivity between the VSM and the Cisco VNMC 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 VNMC image bundle to boot from a flash drive and to complete registration with the Cisco VNMC.
Task 4: On the VSM, Preparing Cisco VSG Port Profiles, on page 20	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 22	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 VNMC 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 VNMC IP address • The shared secret password • The IP connectivity between Cisco VSG and Cisco VNMC is okay. • The Cisco VSG VNM-PA image name (vnmc-vsgpa.2.0.1a.bin) is available.
Task 6: On the Cisco VSG and Cisco VNMC, Verifying the VNM Policy-Agent Status, on page 27	—
Task 7: On the Cisco VNMC, Configuring a Tenant, Security Profile, and Compute Firewall, on page 28	Make sure that you know the following: • Adobe Flash Player (Version 10.1 or later) has been installed • The IP address of the Cisco VNMC • The admin user password
Task 8: On the Cisco VNMC, Assigning the Cisco VSG to the Compute Firewall, on page 33	—
Task 9: On the Cisco VNMC, Configuring a Permit-All Rule, on page 35	—

Tasks	Prerequisites
Task 10: On the Cisco VSG, Verifying the Permit-All Rule, on page 38	—
Task 11: Enabling Logging, on page 38	—
Task12: Enabling the Traffic VM Port-Profile for Firewall Protection and Verifying the Communication Between the VSM, VEM, and VSG, on page 41	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
Task13: Sending Traffic Flow and on the Cisco VSG Verifying Statistics and Logs, on page 43	—

Host Requirements

- ESX or ESXi platform that runs VMware software release 4.1, 5.0 , 5.1 with a minimum of 4 GB physical RAM for the Cisco VSG and similar requirements for the Cisco VNMC, or 6 GB for both.
- 1 processor
- CPU speed of 1.5 GHz

Obtaining the Cisco VNMC and the Cisco VSG Software

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

http://www.cisco.com/en/US/products/ps11208/index.html
The Cisco VNMC software is available for download at the following URL:

http://www.cisco.com/en/US/products/ps11213/index.html

Task 1: Installing the Cisco VNMC from an OVA Template

Before You Begin

Know the following:

- The Cisco VNMC OVA image is available in the vCenter.
- Know the IP/subnet mask/gateway information for the Cisco VNMC.
- Know the admin password, shared_secret, hostname that you want to use.
- Know the DNS server and domain name 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 VNMC management interface.

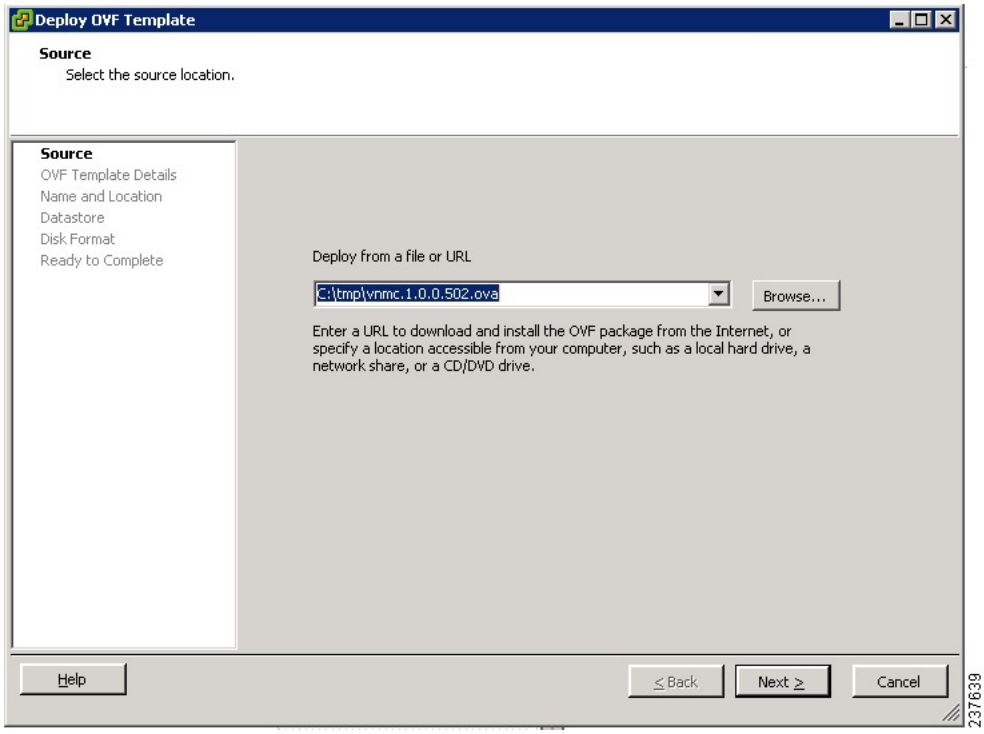
- The host has 2-GB RAM and 25-GB available hard-disk space.
- A shared secret password is available (this password enables communication between the Cisco VNMC, VSM, and Cisco VSG).

Procedure

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

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

Figure 1: Deploy OVF Template—Source Window



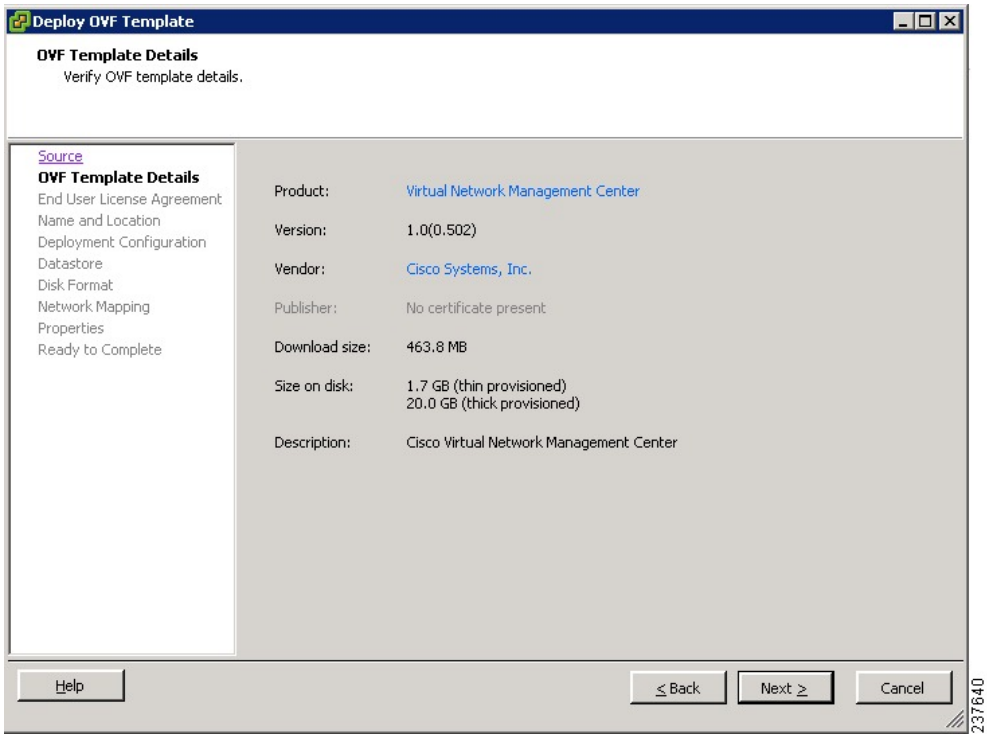
The **Source** window opens.

Step 3 In the **Source** window, do the following:

a) Enter the path to the Cisco VNMC OVA file in the **Deploy from a file or URL** field.

b) Click **Next**.

Figure 2: Deploy OVF Template–OVF Template Details Window



The **OVF Template Details** window opens.

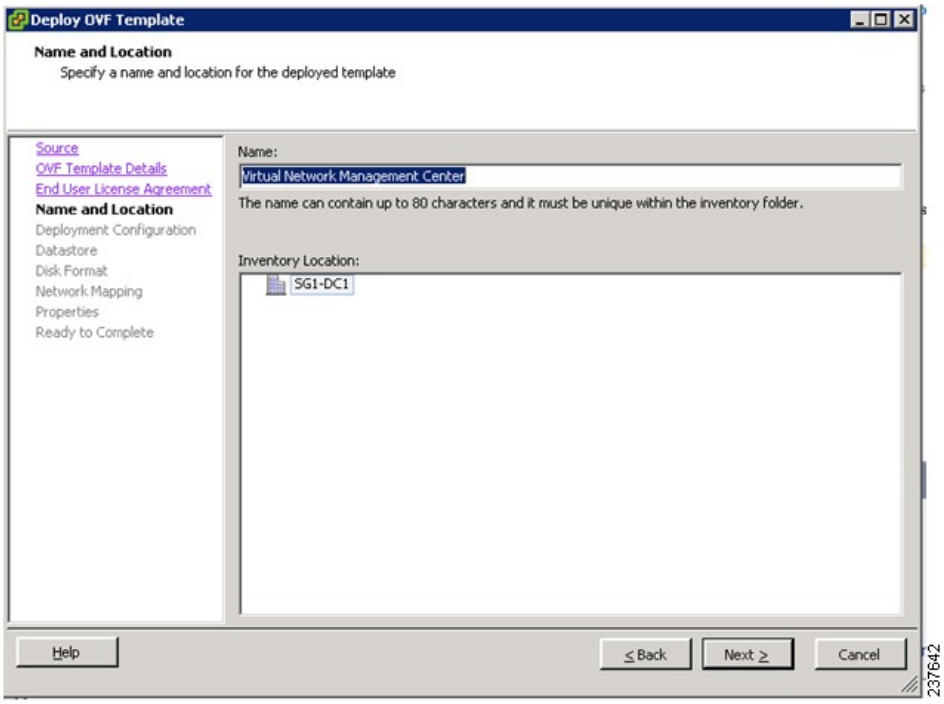
Step 4 In the **OVF Template Details** window, review the details of the Cisco VNMC template and click **Next**. The **End User License Agreement** window opens.

Step 5 In the **End User License Agreement** window, do the following:

a) Review the End User License Agreement and click **Accept**.

b) Click **Next**.

Figure 3: Deploy OVF Template–Name and Location



The **Name and Location** window opens.

Step 6 In the **Name and Location** window, do the following:

a) In the **Name** field, enter the name of the Cisco Virtual Network Management Center.
The name can contain up to 80 characters and must be unique within the inventory folder.

b) In the Work pane, choose the **Inventory location** that you would like to use.

c) Click **Next**.

Step 7 In the **Deployment Configuration** window, do the following:

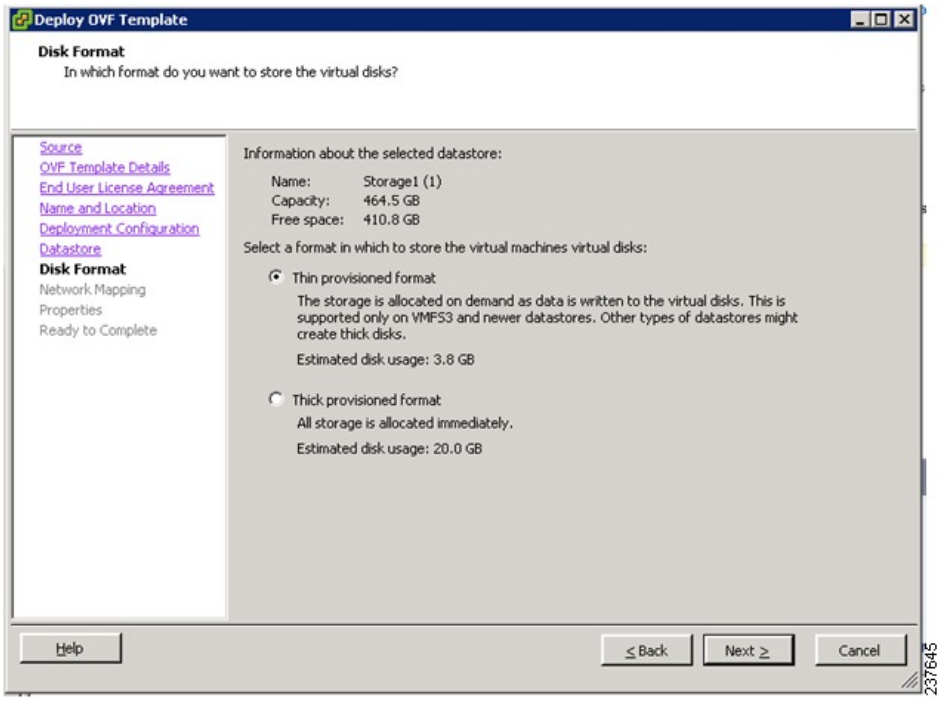
a) From the **Configuration** drop-down list, choose **VNMC Installer**.

b) Click **Next**.

Step 8 In the **Datastore** window, choose the **datastore** for the VM and click **Next**.
The **Disk Format** window opens.

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 ESX host, this window does not display and you are assigned to the one that is available.

Figure 4: Deployment OVF Template–Disk Format



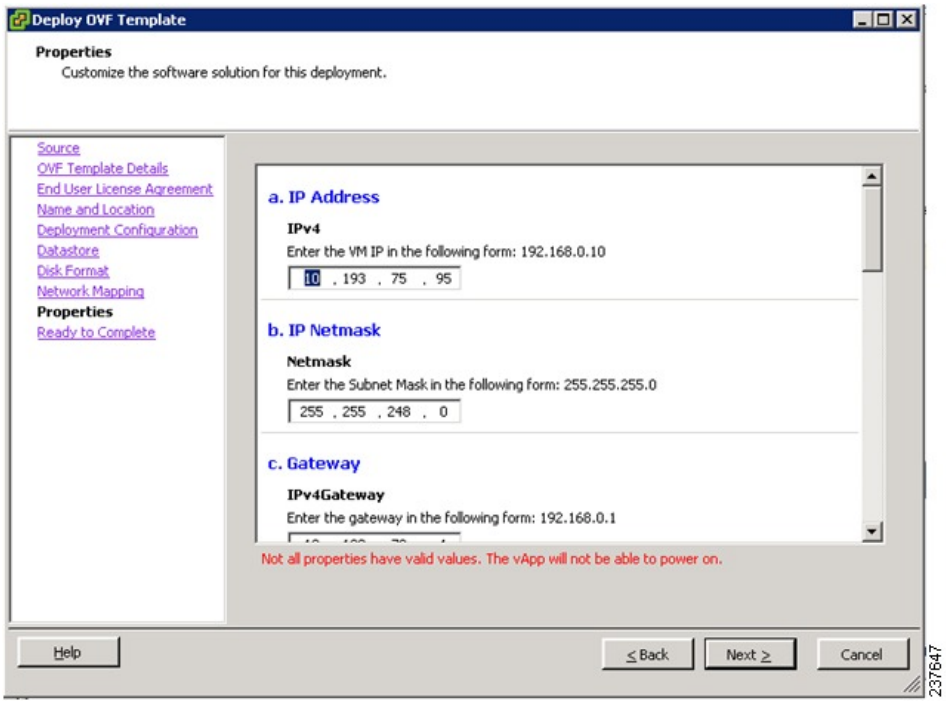
Step 9 In the **Disk Format** window, do the following:

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

b) Click **Next**.
The **Network Management** window opens.

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.

Figure 5: Deploy OVF Template–Network Mapping Window

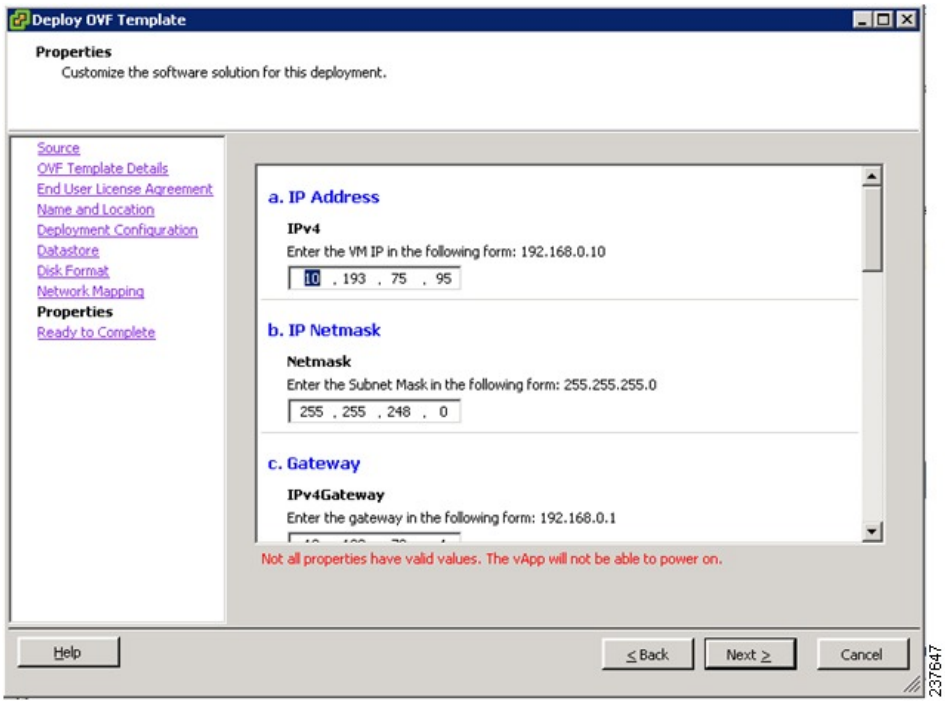


Step 10 In the **Network Mapping** window, do the following:

a) Choose the management network port profile for the VM in the **Network Mapping** pane.

b) Click **Next**.

Figure 6: Deploy OVF Template–Properties Window



The **Properties** window opens.

Step 11 In the **Properties** window, do the following:

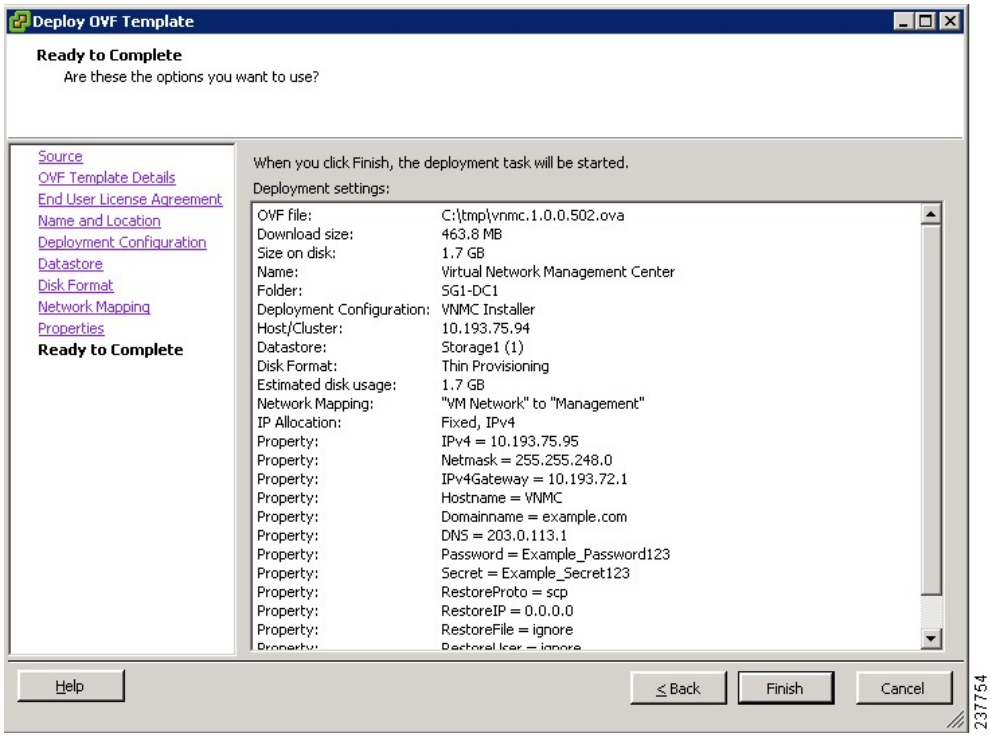
a) In the **IPv4** field, enter the IP address
b) In the **Netmas** field, enter the subnet mask
c) In the **IPv4Gateway** field, enter the gateway.
d) In the **DomainName** field, enter the domain name.
e) In the **DNS** field, enter the domain name server name.
f) In the **Password** field, enter the admin password.
g) In the **Secret** field, enter the shared secret password.

Note Follow these parameters for choosing the shared secret password:

- The password must be more than eight characters.
- Characters not supported for shared secret password: $ & ' " ` ( )< >| \ characters and all other characters supported on the keyboard.
- The password should contain lowercase letters, uppercase letters, digits, and special characters.
- The password should not contain characters repeated three or more times consecutively.
- The new shared secret passwords should not repeat or reverse the username.
- The password should not be cisco, ocsic, or any variant obtained by changing the capitalization of letters.
- The password should not be formed by easy permutations of characters present in the username or Cisco.

Step 12 Click **Next**.

Figure 7: Deploy OVF Template–Ready to Complete Window



Note 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 VNMC Restore fields.

The **Ready to Complete** window opens.

Step 13 In the **Ready to Complete** window, review the deployment settings information and click **Finish**.
The progress bar in the **Deploying Virtual Network Management Center** window shows how much of the deployment task is completed before the Cisco VNMC is deployed.

Wait for the **Deployment completed Successfully** window.

Step 14 Click **Close**.

Step 15 Power on the Cisco VSG VM.

Task 2: On the Cisco VNMC, 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 VNMC, on page 15
- Registering the vCenter Extension Plugin in the vCenter, on page 17
- Configuring the vCenter in VM-Manager in the Cisco VNMC, on page 18

Downloading the vCenter Extension File from the Cisco VNMC

Before You Begin

Make sure that you know the following:

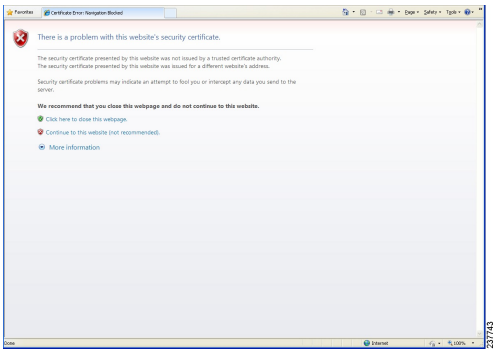
- Install Adobe Flash Player (Version 10.1.102.64)
- IP address of the Cisco VNMC
- Admin user password

Procedure

Step 1 To access the Cisco VNMC from your client machine, open Internet Explorer and access https://vnmc-ip/ (https://xxx.xxx.xxx.xxx).

The **Website Security Certificate** window opens.

Figure 8: Website Security Certification Window



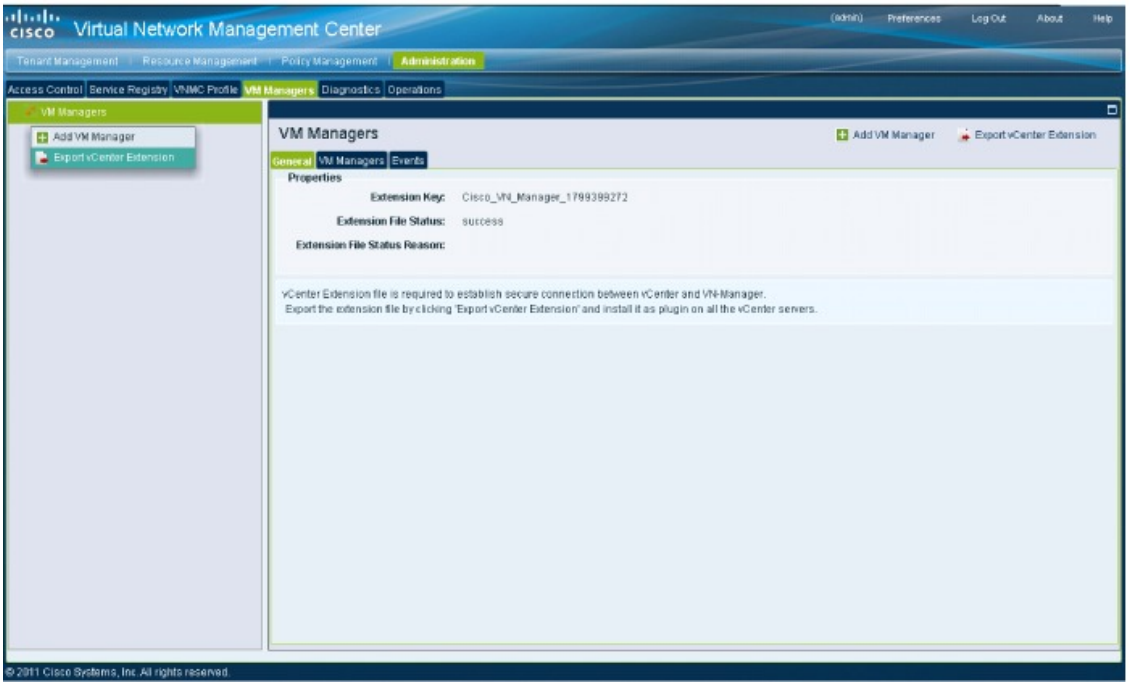
Step 2 In the **Website Security Certificate** window, choose **Continue to this website**.

Step 3 In the **Cisco VNMC Access** window, do the following:

a) Enter the login name admin.

b) Enter the password that you set when installing the application.

Figure 9: Cisco VNMC Window



The VNMC main window opens.

Step 4 In the **VNMC Main** window, choose **Administration** > **VM Managers.**

The **VM Managers** window opens.

Step 5 In the **Cisco Virtual Network Management Center VM Managers** window, do the following:

a) Right-click and choose **Export vCenter Extension** from the **VM Managers** pane.

b) Save the file on your vCenter desktop.

What to Do Next

Go to Registering the vCenter Extension Plugin in the vCenter, on page 17.

Registering the vCenter Extension Plugin in the vCenter

This task is completed within your client desktop vSphere client directory

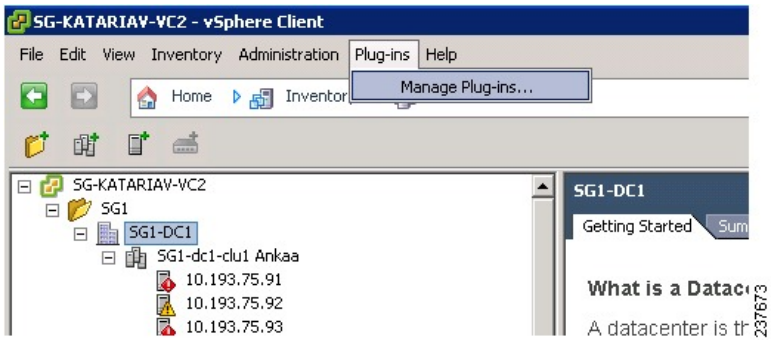
Before You Begin

See Downloading the vCenter Extension File from the Cisco VNMC, on page 15.

Procedure

Step 1 From vSphere client, log in to vCenter.

Figure 10: vSphere Client Directory Window



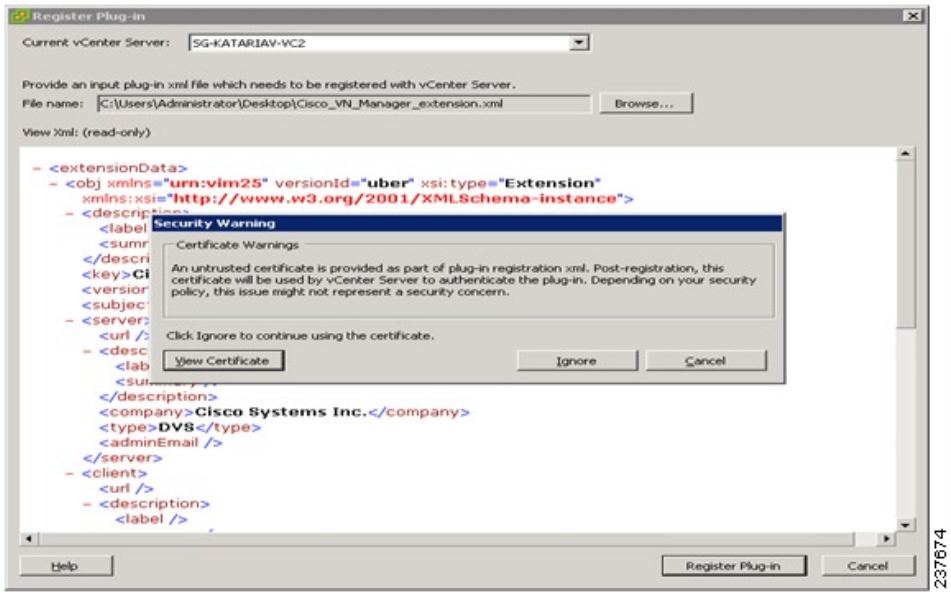
The **vSphere Client Directory** window opens.

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

Step 3 Right-click in an empty space, and choose **New Plug-in** from the drop-down list.

The **Register Plug-in** window that contains the vSphere client and vCenter directory for managing plug-ins opens.

Figure 11: vSphere Client and vCenter Directory for Managing Plug-ins with Security Warning



Step 4 In the **Register Plug-in** window, do the following:

a) Browse to the Cisco VNMC vCenter extension file and click **Register Plug-in.**

b) On the **Security Warning** dialog box, click **Ignore**.

Step 5 On the **Register Plug-in** progress indicator, click **OK** after the successful registration message appears.

Step 6 Click **Close**.

What to Do Next

Go to Configuring the vCenter in VM-Manager in the Cisco VNMC, on page 18.

Configuring the vCenter in VM-Manager in the Cisco VNMC

Before You Begin

See Task 2: On the Cisco VNMC, Setting Up VM-Mgr for vCenter Connectivity, on page 15.

Procedure

Step 1 Go to the Cisco VNMC and click **Administration** > **VM Managers**.

Step 2 In the **Cisco Virtual Network Management Center** window, click the **VM Manager** tab.

Step 3 In the left pane, choose **Vm Manager** > **Add VM Manager**.

Step 4 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 5 Click **OK**.

Note The successful addition should display the Admin State as enable and the Operational State as up with the version information.

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

Once the Cisco VNMC is installed, you must register the VSM with the Cisco VNMC policy.

Before You Begin

Make sure that you know the following:

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

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

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

Procedure

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.2.1.1b.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 VNMC correctly and it is reachable by entering the **show vnm-pa status** command. This example shows that the Cisco VNMC is reachable and the installation is correct:

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

The VSM is now registered with the Cisco VNMC.

This example shows that the Cisco VNMC 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.

Procedure

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 VNMC 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 VNMC IP address
- The shared secret password
- The IP connectivity between Cisco VSG and Cisco VNMC is okay.
- The Cisco VSG VNM-PA image name (vnmc-vsgpa.2.0.1a.bin) is available.

Procedure

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**.

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.

Step 5 Click **Next**.

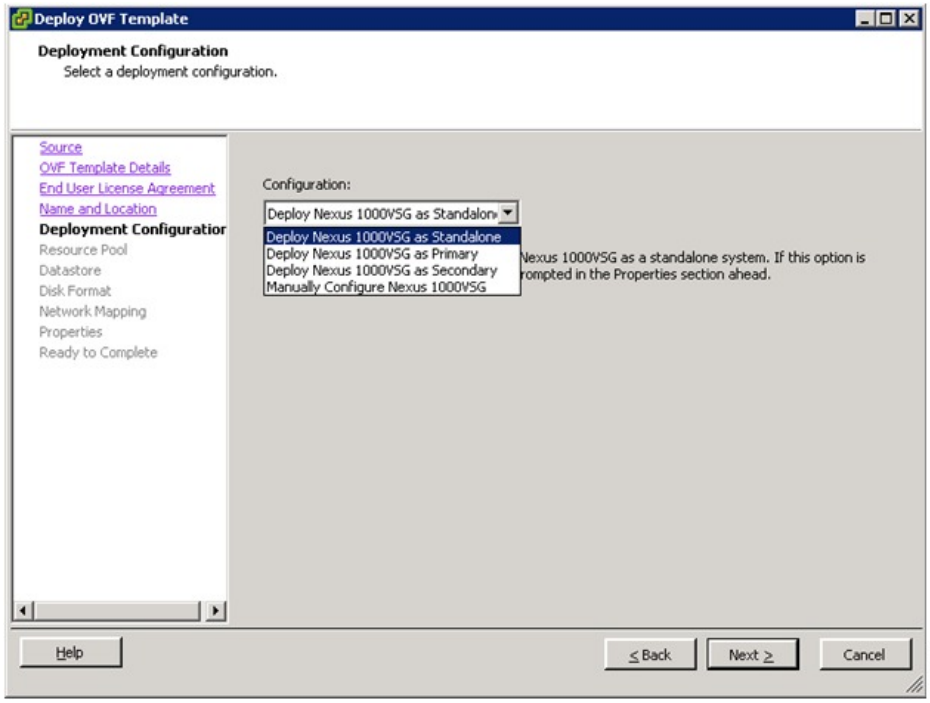
Step 6 In the **Deploy OVF Template—End User License Agreement** window, do the following:

a) Review the end user license agreement and click **Accept**.
b) Click **Next**. The **Name and Location** window opens.

Step 7 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**. The **Deployment Configuration** window opens.

Figure 12: Deploy OVF Template—Deployment Configuration Window



q

Step 8 In the **Deploy OVF Template—Deployment Configuration** window, do the following:

a) From the **Configuration** drop-down list, choose **Deploy Nexus 1000V as Standalone**.
b) Click **Next**. The **Datastore** window opens.

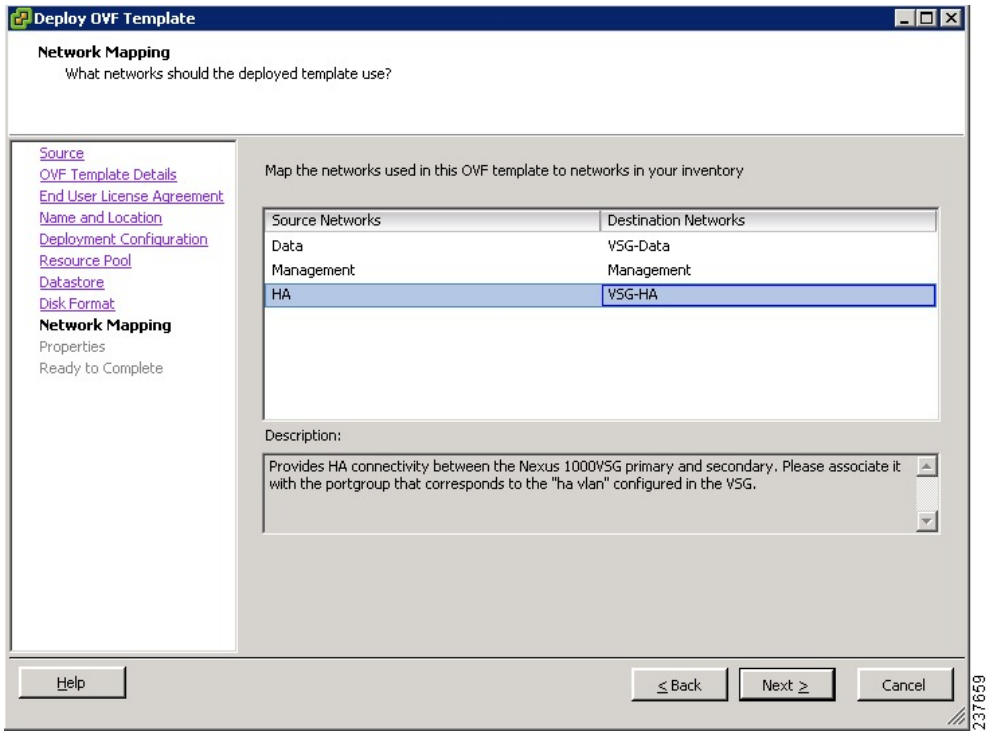
Step 9 In the **Deploy OVF Template—Datastore** window, choose the data store for the VM and click **Next**. The **Disk Format** window opens.
The storage can be local or shared remote such as the network file storage (NFS) or the storage area network (SAN).

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

Step 10 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.
b) Click **Next**. The **Network Mapping** window opens.
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.

Figure 13: Deploy OVF Template—Network Mapping



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

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

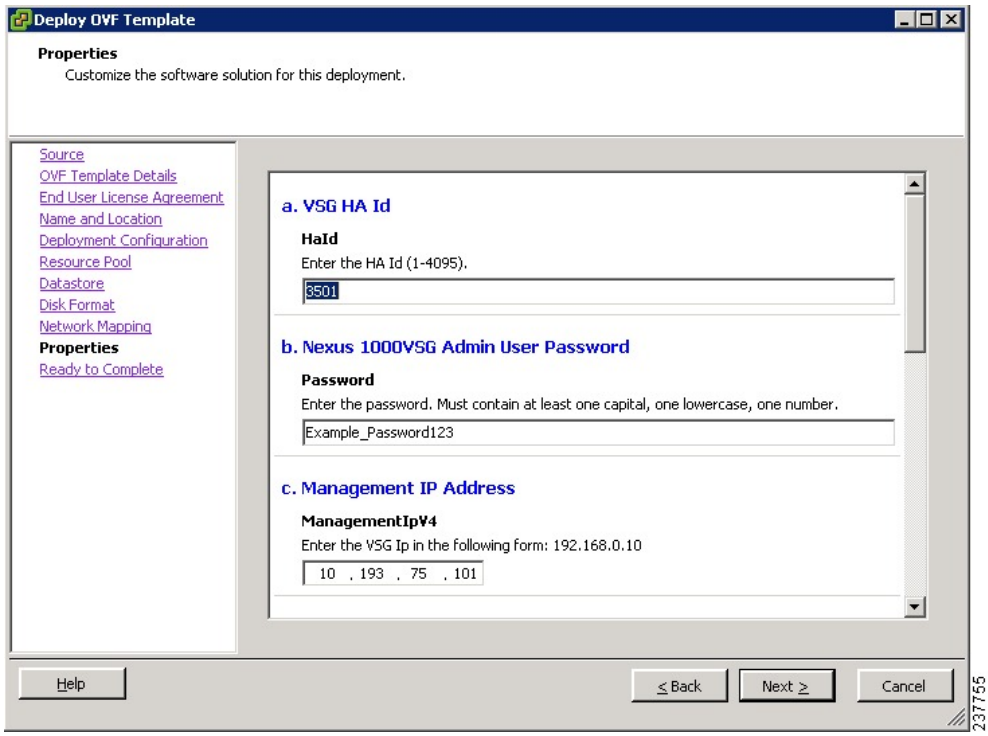
b) Choose **Management** for the management interface port profile.

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

d) Click **Next**. The **Properties** window opens.

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 VNMC.

Figure 14: Deploy OVF Template—Properties Window



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 VNMC.
g) In the **SharedSecret** field, enter the shared secret password defined during the Cisco VNMC installation.
h) In the **ImageName** field, enter the VSG VNM-PA image name (vnmc-vsgpa.2.0.1a.bin).

Note Follow these parameters for choosing the shared secret password:

- The password must be more than eight characters.
- Characters not supported for the shared secret password: & ' " ` ( )< >| \ characters and all other characters supported on the keyboard.
- The password should contain lowercase letters, uppercase letters, digits, and special characters.
- The password should not contain characters, repeated three or more times consecutively.
- The new shared secret passwords should not repeat or reverse the username
- The password should not be cisco, ocsic, or any variant obtained by changing the capitalization of letters.
- The password should not be formed by easy permutations of characters present in the username or Cisco.

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 VNMC Restore fields.

Step 13 Click **Next**. The **Ready to Complete** window opens.

Step 14 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 15 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 VNMC is deployed.

Step 16 Wait and click **Close** after the progress indicator shows that the deployment is completed successfully.

Step 17 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**. The **Virtual Machine Properties** window opens.

Step 18 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 19 Power on the Cisco VSG VM.

Task 6: On the Cisco VSG and Cisco VNMC, 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).

Procedure

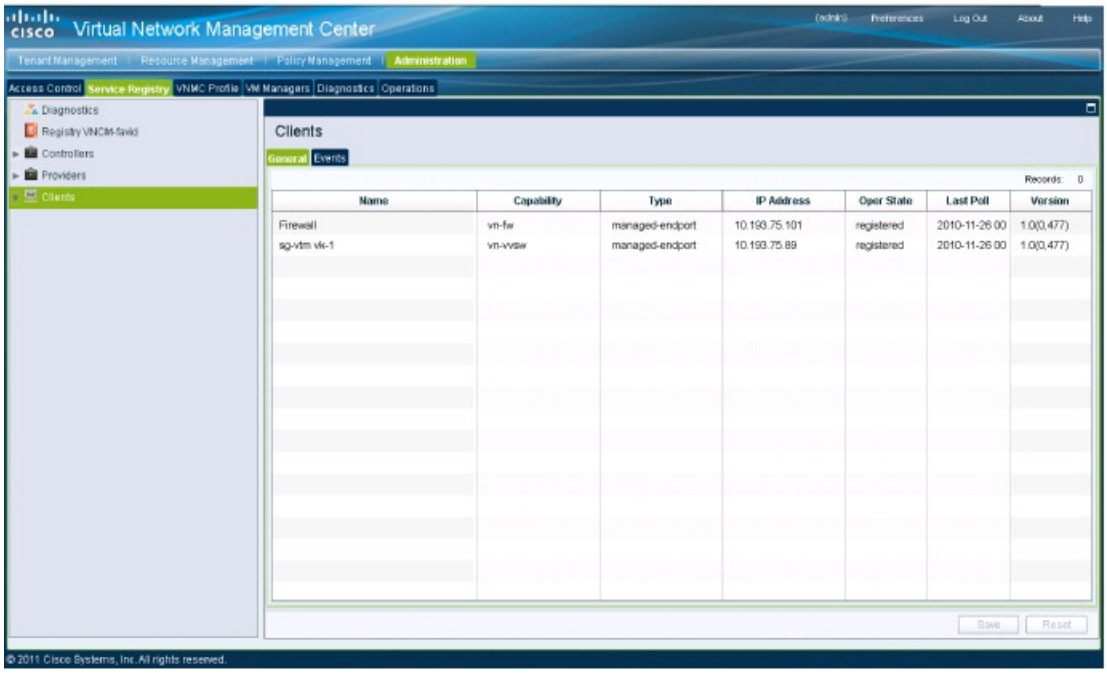
Step 1 Log in to the Cisco VSG.

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 2.0(1a)-vsg
vsg#
```

Step 3 Log in to the Cisco VNMC. The **VNMC Administration on Service Registry** window opens.

Figure 15: VNMC Administration Service Registry Window



Step 4 Choose **Administration** > **Service Registry** > **Clients** > **General**.

Step 5 In the **Client** pane of the **VNMC Administration Service Registry** window, verify that the Cisco VSG and VSM information is listed.

Task 7: On the Cisco VNMC, Configuring a Tenant, Security Profile, and Compute Firewall

Now that you have the Cisco VNMC and the Cisco VSG successfully installed with the basic configurations (completed through the OVA File Template wizard), you should configure some of the basic security profiles and policies.

This task includes the following subtasks:

- Configuring a Tenant on the Cisco VNMC, on page 28
- Configuring a Security Profile on the Cisco VNMC, on page 29
- Configuring a Compute Firewall on the Cisco VNMC, on page 31

Before You Begin

Make sure that you know the following:

- Adobe Flash Player (Version 10.1 or later) has been installed
- The IP address of the Cisco VNMC
- The admin user password

Procedure

Step 1 For Cisco VNMC access, from your client machine, open Internet Explorer and access https://vnmc-ip/ (https://xxx.xxx.xxx.xxx).

Step 2 In the **Website Security Certification** window, click **Continue to this website**.

Step 3 In the **Cisco VNMC Access** window, log in to the Cisco VNMC:

a) Enter the username admin.

b) Enter your password.

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

What to Do Next

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

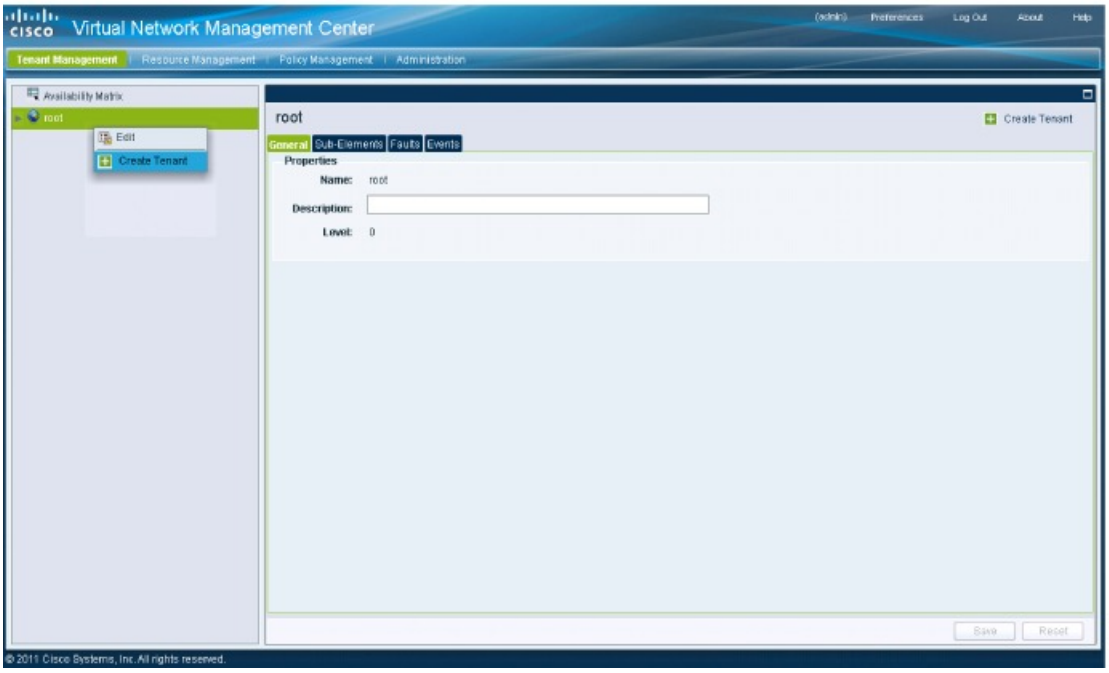
Configuring a Tenant on the Cisco VNMC

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 VNMC.

Procedure

Step 1 From the Cisco VNMC toolbar, click the **Tenant Management** tab.

Figure 16: VNMC Window Tenant Management Tab root Pane



Step 2 In the Navigation pane directory tree, right-click on **root**, and from the drop-down list, choose **Create Tenant**.

Step 3 In the **root** pane, click the **General** tab and do the following:

a) In the **Name** field, enter the tenant name; for example, Tenant-A.

b) In the **Description** field, enter a description for that tenant.

Step 4 Click **OK**.

Notice that the tenant you just created is listed in the left-side pane under root.

What to Do Next

Go to Configuring a Security Profile on the Cisco VNMC, on page 29

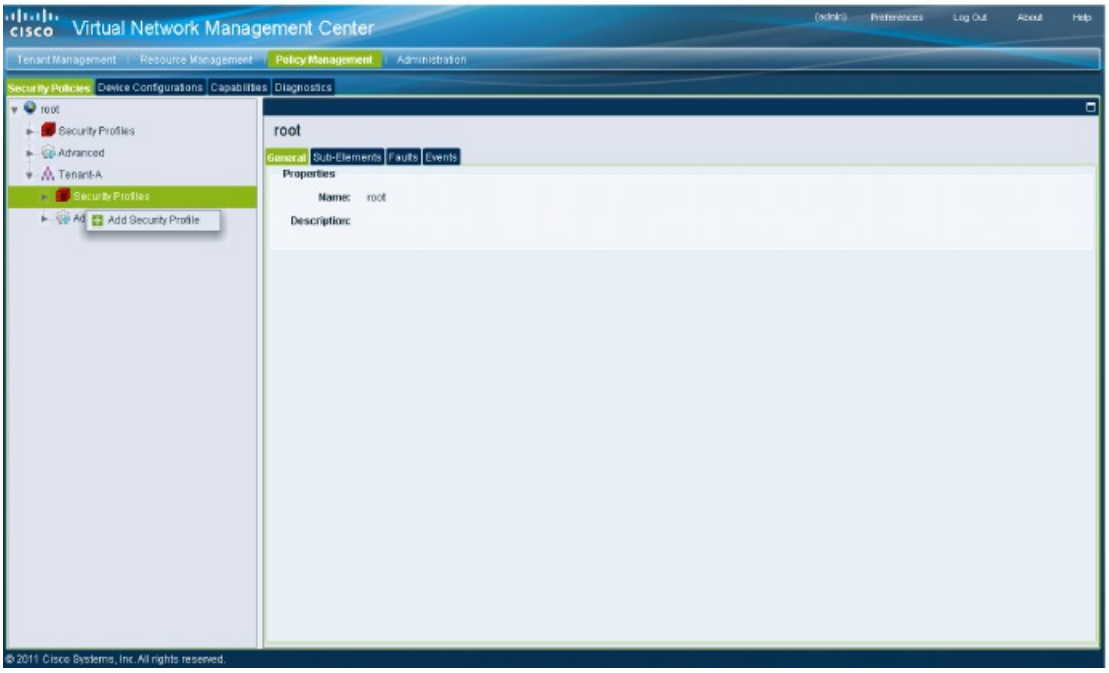
Configuring a Security Profile on the Cisco VNMC

You can configure a security profile on the Cisco VNMC.

Procedure

Step 1 Click the **Policy Management** tab in the Cisco VNMC toolbar. The **Policy Management** window opens.

Figure 17: Security Policies root Window

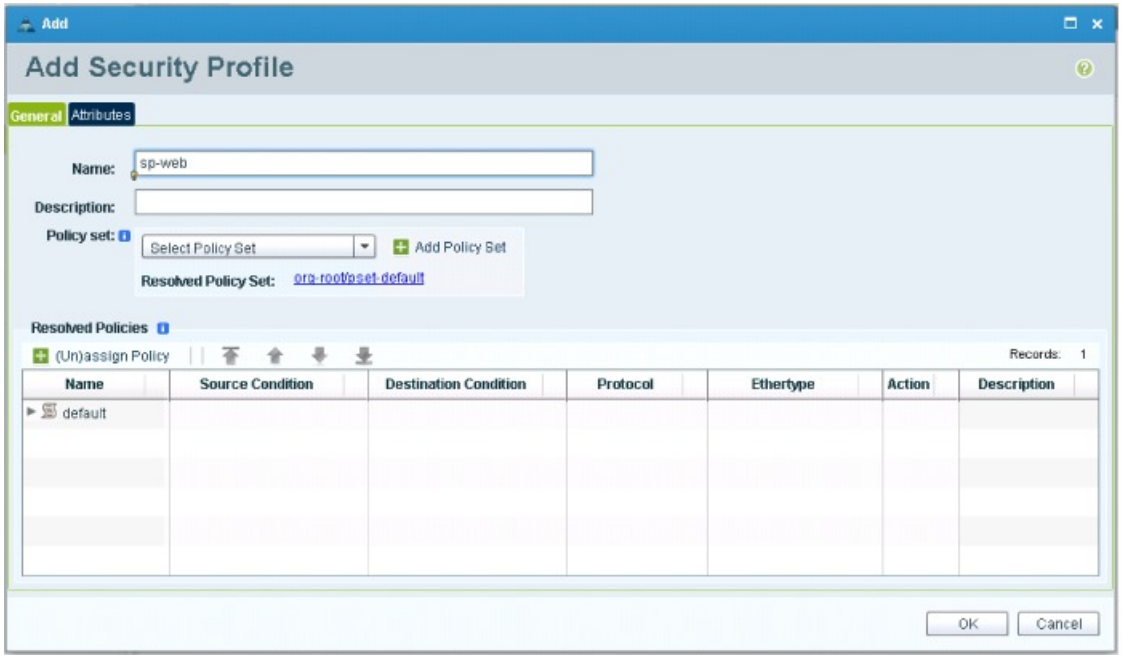


Step 2 In the **Policy Management Security Policies** window, from the directory path, choose **Security Policies** > **root** > **Tenant-A** > **Security Profiles**.

Step 3 Right click in an empty space and choose **Add Security Profile** from the drop-down list.

The **Add Security Profile** dialog box opens.

Figure 18: Add Security Profile Dialog Box



Step 4 In the Add Security Profile dialog box, do the following:

a) In the **Name** field, enter a name for the security profile; for example, sp-web.

b) In the **Description** field, enter a brief description of this security profile.

Step 5 Click **OK**

What to Do Next

Go to Configuring a Compute Firewall on the Cisco VNMC, on page 31

Configuring a Compute Firewall on the Cisco VNMC

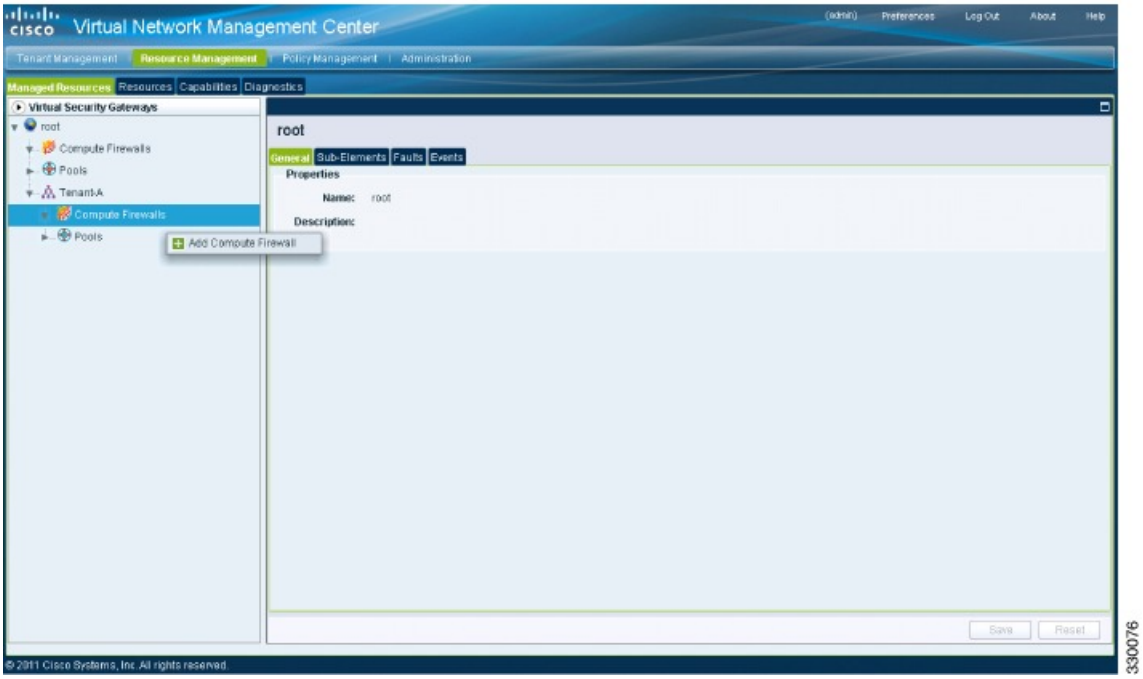
The compute firewall is a logical virtual entity that contains the device profile that you can bind (assign) to a Cisco VSG VM. The device policy in the device profile is then pushed from the Cisco VNMC to the Cisco VSG. Once this is complete, the compute firewall is in the applied configuration state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

Procedure

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

The Firewall Profiles window opens.

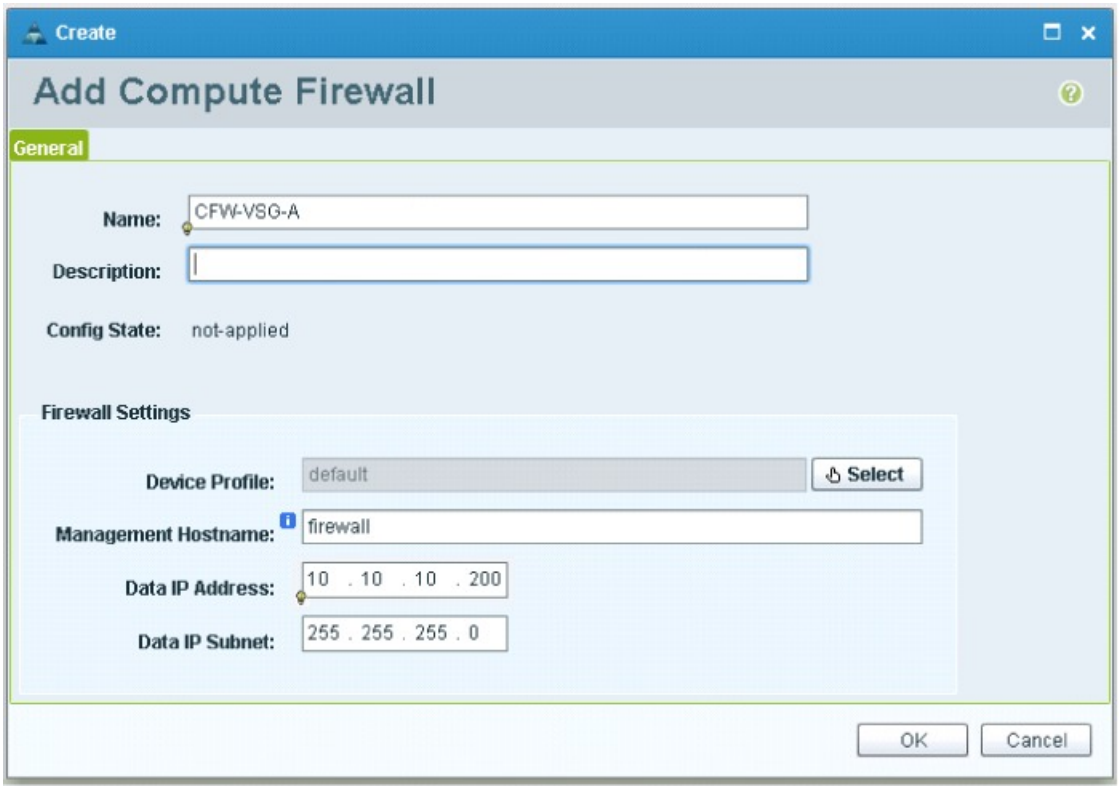
Figure 19: VNMC Resource Management, Managed Resources, Firewall Profiles Window



Step 2 On the left-pane directory tree, choose **root** > **Tenant-A** > **Compute Firewall**.

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

Figure 20: Add Compute Firewall Dialog Box



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 **Management Hostname** field, enter the name for your Cisco VSG.
d) In the **Data IP Address** field, enter the data IP address.

Step 5 Click **OK**.
The new Compute Firewall pane displays with the information that you provided.

Task 8: On the Cisco VNMC, Assigning the Cisco VSG to the Compute Firewall

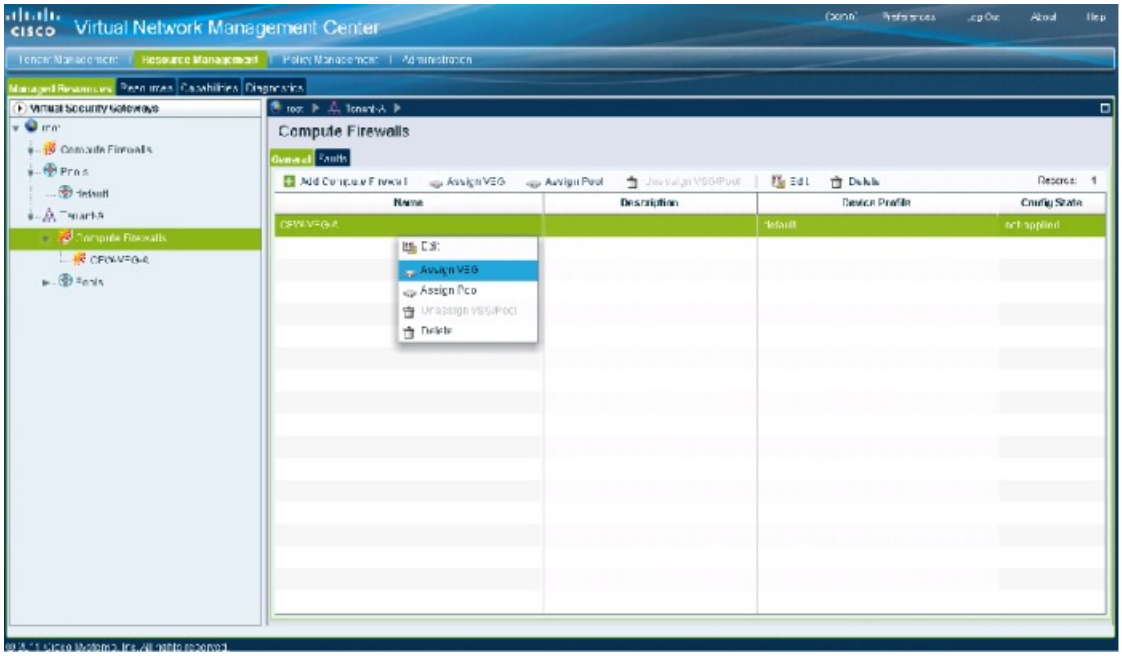
The compute firewall is a logical virtual entity that contains the device profile that can be later bound to the device for communication with the Cisco VNMC and VSM.

Procedure

Step 1 Choose **Resource Management** > **Managed Resources**.The **Deploy OVF Template** window opens.

Step 2 In the **Deploy OVF Template** window, choose **root** > **Tenant-A** > **Compute Firewalls**.

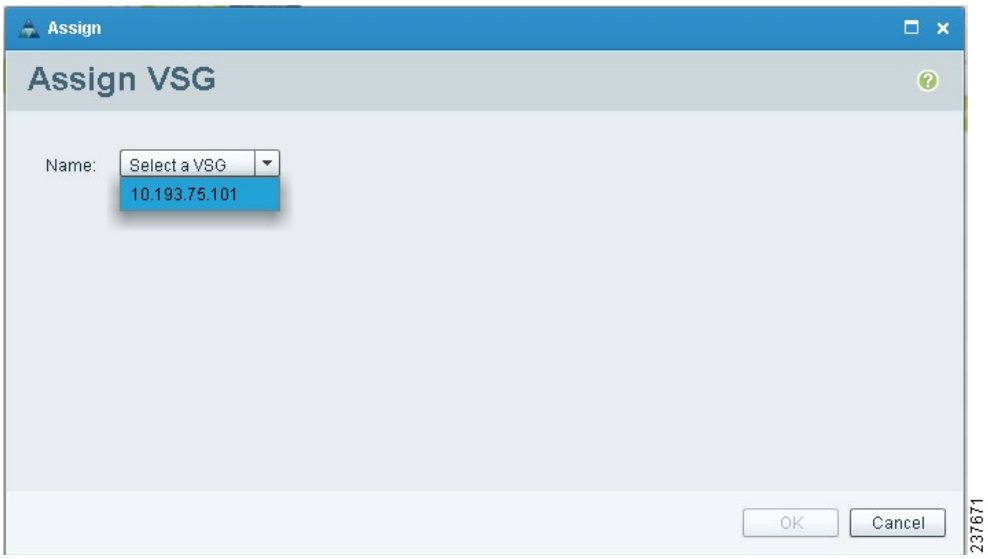
Figure 21: VNMC Resource Management Resources Compute Firewalls Window



Step 3 Right-click in the **Compute Firewalls** pane and choose **Assign VSG** from the drop-down list.

The **Assign VSG** dialog box opens.

Figure 22: Assign VSG Dialog Box



Step 4 From the **Name** drop-down list, choose the Cisco VSG IP address.

Step 5 Click **OK**.

Note The Config State status changes from "not-applied" to "applying" and then to "applied."

Task 9: On the Cisco VNMC, Configuring a Permit-All Rule

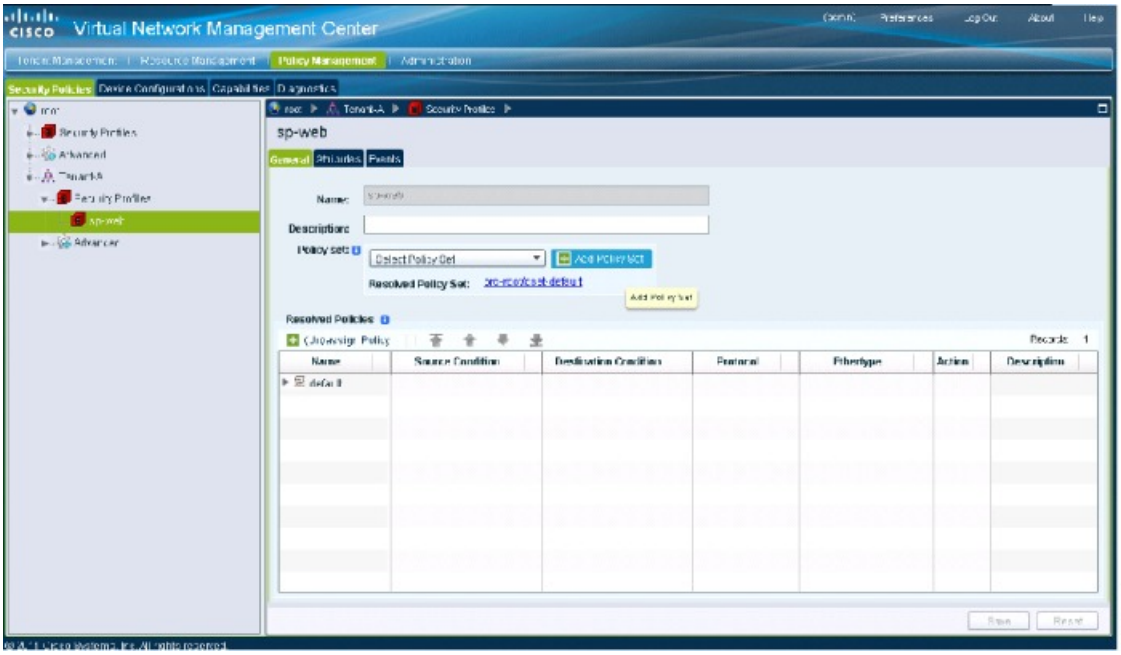
You can configure a permit-all rule in the Cisco VNMC.

Procedure

Step 1 Log in to the Cisco VSG.

Step 2 Choose **Policy Management** > **Service Policies**. The **Cisco VNMC Policy Management Security Policies** window opens.

Figure 23: Cisco VNMC Policy Management Security Policies Window



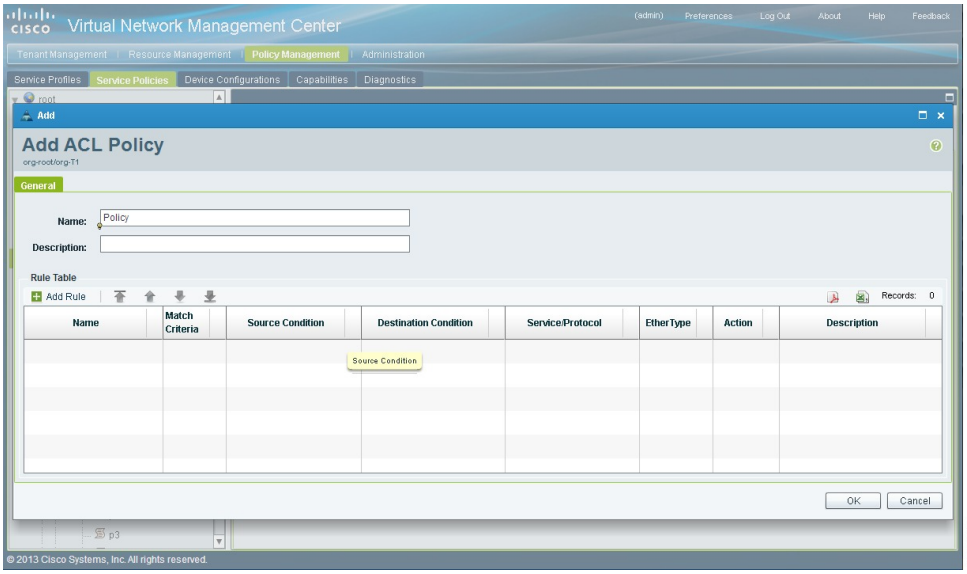
Step 3 In the **Cisco VNMC Policy Management Security Policies**, window do the following:

a) Choose **root** > **Tenant-A** > **Security-Profile** > **sp-web**.

b) In the right pane, click **Add policy set**.

Step 4 Click **Add Policy**. The **Add Policy** dialog box opens.

Figure 24: Add Policy Dialog Box



Step 5 In the **Add Policy** dialog box, do the following:

a) In the **Name** field, enter the security policy name.
b) In the **Description** field, enter a brief description of the security policy.
c) Above the **Name** column, click **Add Rule**.

Step 6 In the **Add Rule dialog** box, do the following:

a) In the **Name** field, enter the rule name.
b) In the **Match Criteria** field, select the matching condition.
c) In the **Source Condition** field, enter the source condition of the rule.
d) In the **Destination Condition** field, enter the destination of the rule.
e) In the **Service/Protocol** field, select a service or protocol for the rule.
f) In the **EtherType** field, specify ethertype for the rule.
g) Under the **Action** button, choose an action that you want this rule to have in this case, **permit**.
h) Click **OK**.

Step 7 In the **Add Policy** dialog box, click **OK**.
The newly created policy is displayed in the **Assigned** field.

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

Step 9 In the **Security Profile** window, click **Save**.

Task 10: 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 11: Enabling Logging

To enable logging follow these procedures:

- Enabling Logging level 6 for Policy-Engine Logging, on page 38
- Enabling Global Policy-Engine Logging, on page 40

Enabling Logging level 6 for Policy-Engine Logging

Logging enables you to see what traffic is going through your monitored virtual machine. This logging is helpful for verifying that you have a proper configuration and to help in troubleshooting. You can enable Logging Level 6 for policy-engine logging in a monitor session.

Procedure

Step 1 Log in to the Cisco VNMC.

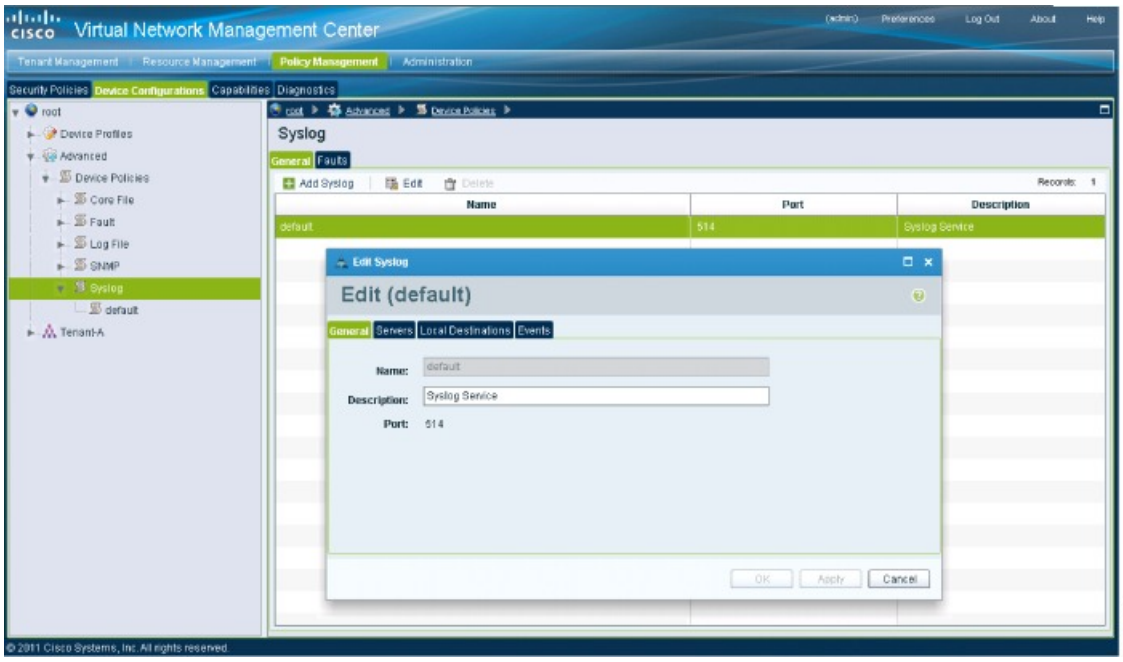
Step 2 Choose **Policy Management** > **Device Configurations**.

Step 3 In the **Device Configuration** window, do the following:

a) In the **Navigation** pane, choose **root** > **Advanced** > **Device Policies** > **Syslog**.

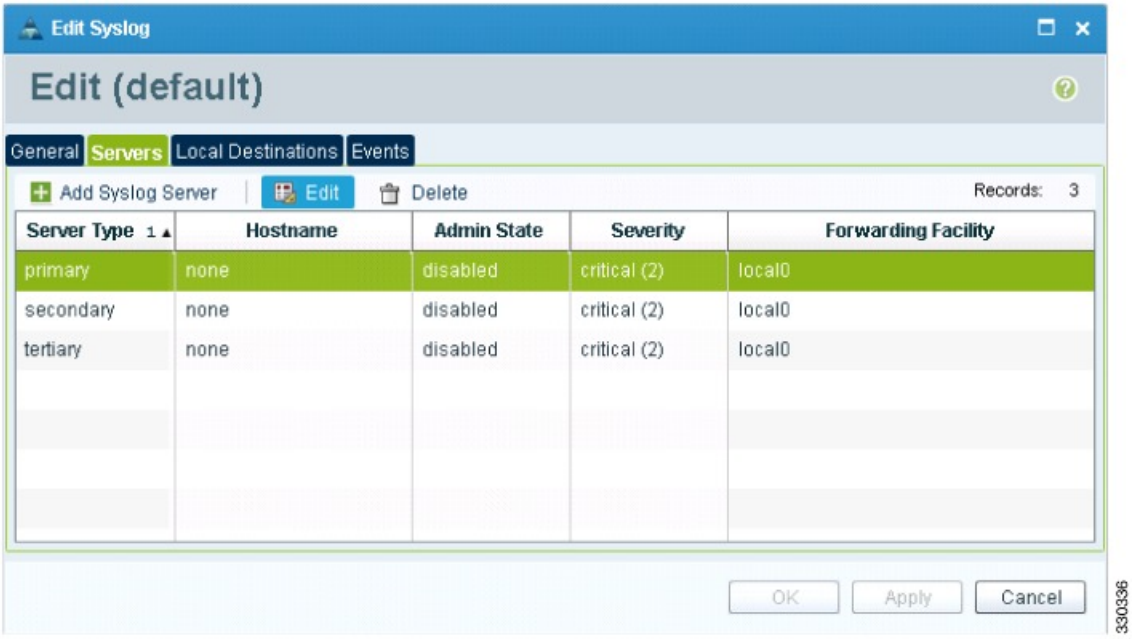
b) In the **Work** pane, choose **Default** and click **Edit**.
The **Edit (default)** dialog box opens.

Figure 25: Cisco Virtual Network Center Syslog Pane



Step 4 In the **Edit Syslog** dialog box, do the following:

Figure 26: Edit Syslog Dialog Box



a) Click the **Servers** tab.

b) From the **Server Type** column, choose the **primary** server type from the displayed list.
c) From the pane toolbar, click **Edit.**

Step 5 In the **Edit (Primary) Syslog Server** dialog box, do the following:

a) In the **Hostname/IP address** field, enter the syslog server IP address.
b) From the **Severity** drop-down list, choose **Information(6).**
c) From the **Admin State** drop-down list, choose **Enabled.**
d) Click **OK**.

Step 6 Click **OK**.

What to Do Next

Go to Enabling Global Policy-Engine Logging, on page 40.

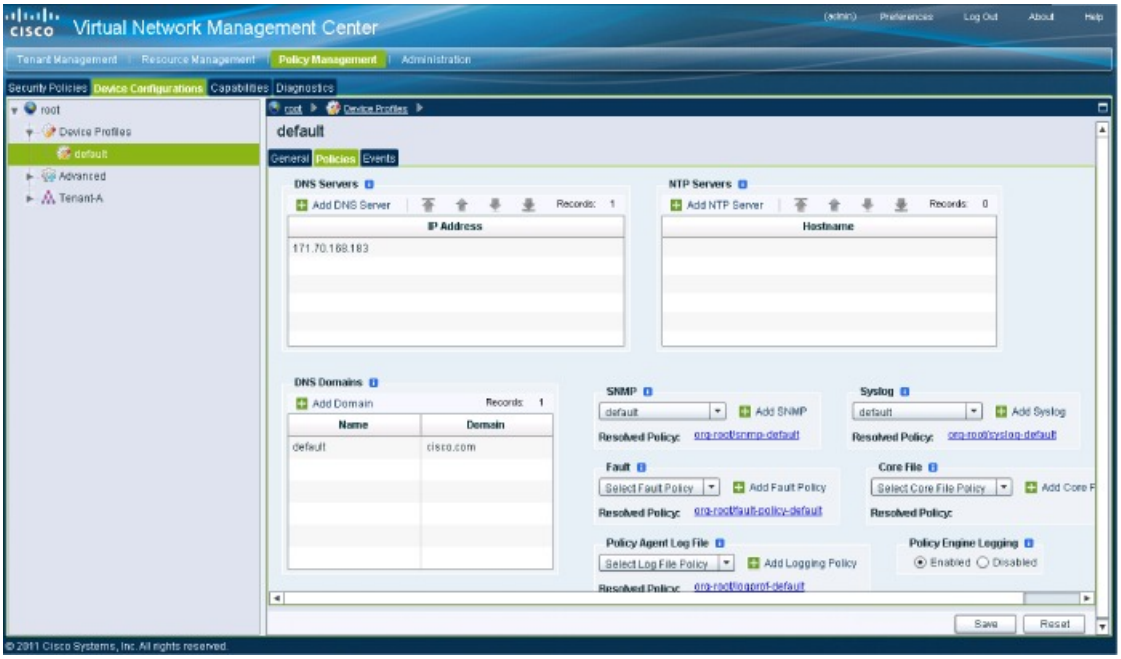
Enabling Global Policy-Engine Logging

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.

Procedure

Step 1 Log in to the Cisco VNMC.

Figure 27: Cisco Virtual Management Center Policy management Device Configuration Profiles Pane



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

Step 3 In the **default** window, do the following:

a) In the **Work** pane, click the **Policies** tab.

b) At the bottom of the **Work** pane, under the **Policy Engine Logging** field, click **Enabled**.

Step 4 Click **Save**.

Task12: 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:

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.

Procedure

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 42.

Verifying the VSM or VEM for Cisco VSG Reachability

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

```
vsm# show vservice brief
------------------------------------------------------------------------------
                                License Information
------------------------------------------------------------------------------
Type      In-Use-Lic-Count  UnLicensed-Mod
vsg                     4
asa                     0

------------------------------------------------------------------------------
                                Node Information
------------------------------------------------------------------------------
 ID Name                    Type   IP-Address      Mode   State   Module
  1 vsg1                    vsg    40.40.40.40     l3     Alive   4,5,

------------------------------------------------------------------------------
                                Path Information
------------------------------------------------------------------------------
------------------------------------------------------------------------------
                                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
```

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.

Task13: Sending Traffic Flow and on the Cisco VSG Verifying Statistics and Logs

This section includes the following topics:

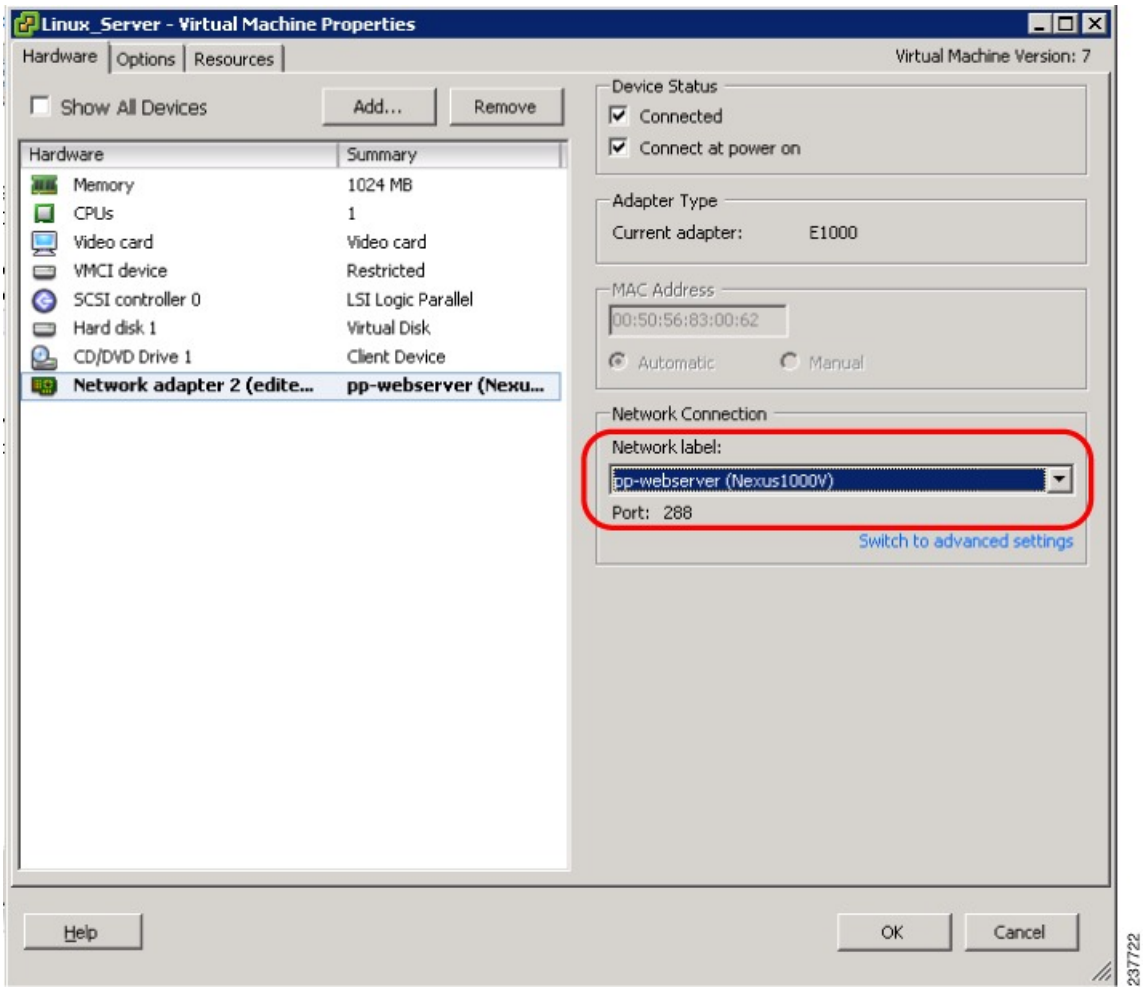
Sending Traffic Flow

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

Procedure

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

Figure 28: 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 45.

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
```