

# Quick Start Guide for the Cisco Virtual Security Gateway and the Cisco Virtual Network Management Center

This chapter provides a Quick Start reference for installing and completing the basic configuration for the Cisco Virtual Network Management Center (VNMC) and the Cisco Virtual Security Gateway (VSG) software.

This chapter includes the following sections:

- Information About Installing Cisco VNMC and Cisco VSG, page 2-2
- Host Requirements, page 2-6
- Obtaining the Cisco VNMC and the Cisco VSG Software, page 2-6
- Task 1—Installing Cisco VNMC Software from an OVA Template, page 2-6
- Task 2-On the Cisco VNMC, Setting Up VM-Mgr for vCenter Connectivity, page 2-15
- Task 3—On the VSM, Configuring the Cisco VNMC Policy-Agent, page 2-21
- Task 4—On the VSM, Preparing Cisco VSG Port Profiles, page 2-22
- Task 5—Installing the Cisco VSG from an OVA Template, page 2-23
- Task 6—On the Cisco VSG and Cisco VNMC, Verifying the VNM Policy Agent Status, page 2-34
- Task 7—On the Cisco VNMC, Configuring a Tenant, Security Profile, and Compute Firewall, page 2-35
- Task 8—On the Cisco VNMC, Assigning the Cisco VSG to the Compute Firewall, page 2-43
- Task 9-On the Cisco VNMC, Configuring a Permit-All Rule, page 2-45
- Task 10—On the Cisco VSG, Verifying the Permit-All Rule, page 2-51
- Task 11—Enabling Logging, page 2-52
- Task 12—Enabling the Traffic VM's Port-Profile for Firewall Protection and Verifying the Communication Between the VSM, VEM, and VSG, page 2-56
- Task 13—Sending Traffic Flow and on the Cisco VSG Verifying Statistics and Logs, page 2-57

Information About Installing Cisco VNMC and Cisco VSG

Send document comments to vsg-docfeedback@cisco.com

# **Information About Installing Cisco VNMC and Cisco VSG**

This chapter presents an example of an effective way 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 is up and running 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 successful operation of the Cisco VNMC and Cisco VSG. This section provides some planning and information checklists to assist you in installing the Cisco VNMC and Cisco VSG.

This section includes the following checklists:

- Table 2-1Basic Hardware and Software Requirements, page 2-2
- Table 2-2Preparation of the Cisco Nexus 1000V Series Switch for Further Installation Processes, page 2-3
- Table 2-3Your Cisco VNMC and Cisco VSG Information for Use Later During Installation, page 2-3
- Table 2-4Tasks, Descriptions, and Prerequisites Checklist, page 2-4

#### Table 2-1 Basic Hardware and Software Requirements

ltem	Do You Have?	Your Information
1	x86 Intel or AMD server with 64-bit processor listed in the VMware compatibility matrix	
2	Intel VT enabled in the BIOS	
3	VMware ESX 4.0, 4.0 U1, 4.0 U2 or 4.1	
4	ESX/ESXi platform that runs VMware software release 4.0.0 or 4.1.0 with a minimum of 4-GB physical RAM for the Cisco VSG and similar for the Cisco VNMC or 6-GB for both.	
5	VMware vSphere Hypervisor	
6	VMware vCenter 4.0, 4.0 U1, 4.0 U2 or 4.1	
7	1 processor	
8	CPU speed of 1.5 Ghz	
9	Datastore with at least 25-GB disk space available on shared NFS/SAN storage when the Cisco VNMC is deployed in an HA cluster	
10	Internet Explorer 7.0 or Mozilla Firefox 3.6.x on Windows	
11	Flash 10.0 or 10.1	
12	Cisco VSG software available for download at the following URL:	
	http://www.cisco.com/en/US/products/ps13095/tsd_products_support_series_home.html	
13	Cisco VNMC software available for download at the following URL:	
	http://www.cisco.com/en/US/products/ps11213/index.html	

#### Table 2-2 Preparation of the Cisco Nexus 1000V Series Switch for Further Installation Processes

ltem	Requirement	Your Information
1	Two VLANs that are configured on the Cisco Nexus 1000V Series switch uplink ports: the service VLAN and an HA VLAN (the VLAN do not need to be the system VLAN)	
2	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)	

#### Table 2-3 Your Cisco VNMC and Cisco VSG Information for Use Later During Installation

ltem	Туре	Your Information
1	Cisco VSG name—unique within the inventory folder and up to 80 characters long	
2	Hostname—where the Cisco VSG will be installed in the inventory folder	
3	Datastore name—where the VM files will be stored	
4	Cisco VSG management IP address	
5	VSM management IP address	
6	Cisco VNMC instance IP address	
7	Mode for installing the Cisco VSG	• Standalone
		• HA primary
		• HA secondary
		Manual installation
8	Cisco VSG VLAN number	
	Service (1)	
	Management (2)	
	High availability (HA) (3)	
9	Cisco VSG port profile name	
	Data (1)	
	Management (2)	
	High availability (HA) (3)	
10	HA pair ID (HA domain ID)	
11	Cisco VSG admin password	
12	Cisco VNMC admin password	
13	Cisco VSM admin password	
14	Shared secret password (Cisco VNMC, Cisco VSG policy agent, Cisco VSM policy agent)	

Information About Installing Cisco VNMC and Cisco VSG

### Send document comments to vsg-docfeedback@cisco.com

#### Table 2-4 Tasks, Descriptions, and Prerequisites Checklist

Task	Description	scription Prerequisites					
1	Installing the Cisco VNMC	Before starting the procedure, know or do the following:					
	software from an OVA template	• Verify that the Cisco VNMC OVA image is available in the vCenter					
	template	• IP/subnet mask/gateway information for Cisco VNMC					
		• The admin password and hostname that you want to use					
		• The shared secret password that you want to use (this password is what enables communication between the Cisco VNMC, VSM, and Cisco VSG)					
		• The DNS server and domain name information					
		• The management port-profile name for the virtual machine (VM) (management)					
		<b>Note</b> 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.					
		• Make sure that the host has 2-GB RAM and 25-GB available hard-disk space					
2	On the Cisco VNMC, setting up VM-Mgr for vCenter connectivity	Before starting the procedure, know or do the following:					
		• Install Adobe Flash Player (Version 10.1.102.64 or later versions)					
		• The IP address of the Cisco VNMC					
		• The admin user password					
3	On the VSM, configuring the Cisco VNMC policy agent	Before starting the procedure, know or do the following:					
		• The Cisco VNMC policy-agent image is available on the VSM (for example, vnmc- <b>vsmpa</b> .1.0.1j.bin)					
		<b>Note</b> The string <b>vsmpa</b> must appear in the image name as highlighted.					
		• The IP address of the Cisco VNMC					
		• The shared secret password that you defined during the Cisco VNMC installation					
		• IP connectivity between the VSM and the Cisco VNMC is okay.					
4	On the VSM, preparing the	Before starting the procedure, know or do the following:					
	Cisco VSG port profiles	• 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)					
		None of these VLANs need to be system VLANs.					

Task	Description	Prerequisites	Completed
5	Installing the Cisco VSG	Before starting the procedure, know or do the following:	
	from an OVA template	• Make sure that the Cisco VSG OVA image is available in the vCenter	
		Cisco VSG-data and Cisco VSG-HA port profile are created on the VSM	
		• Management port profile (management)	
		<b>Note</b> 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.	
		HA pair ID	
		• IP/subnet mask/gateway information for the Cisco VSG	
		Admin password	
		• 2-GB RAM and 3-GB hard disk space are available	
		Cisco VNMC IP	
		Shared secret password	
		• IP connectivity between the Cisco VSG and the Cisco VNMC is okay	
		• Cisco VSG VNM-PA image name (vnmc-vsgpa.1.0.1j.bin)	
6	On the Cisco VSG, verifying the VNM policy-agent Status		
7	On the Cisco VNMC,	Before starting the procedure, know or do the following:	
	configuring a tenant and security profile	• Install Adobe Flash Player (Version 10.1.102.64)	
	security prome	• IP address of the Cisco VNMC	
		Admin user password	
8	On the Cisco VNMC, assigning the Cisco VSG to the compute firewall		
9	On the Cisco VNMC, configuring a permit-all rule	_	
10	On the Cisco VSG, verifying the permit-all rule		
11	Enabling logging		

Task	Description	Prerequisites	Completed
12	Preparing Traffic VM's Port-Profile for Firewall Protection and Verifying the VSM/VEM	<ul> <li>Make sure you have the following:</li> <li>Cisco VSG data IP (10.10.10.200) and VLAN ID (100)</li> <li>Security profile name (for example, sp-web)</li> <li>Organization (Org) name (for example, root/Tenant-A)</li> </ul>	
		<ul> <li>The port profile that you will edit to enable firewall protection</li> </ul>	
13	Sending Traffic Flow and on the Cisco VSG Verifying Statistics and Logs	<ul> <li>Make sure that you have the VM (Server-VM) that is using the port profile (pp-webserver) configured for firewall protection.</li> <li>Log in to only of your client VM (Client VM) and cond traffic (for a server of your client VM) and cond traffic (for a server).</li> </ul>	
		• Log in to any of your client VM (Client-VM) and send traffic (for example, HTTP) to your Server-VM.	
		• Check the policy-engine statistics and log on the Cisco VSG.	

## **Host Requirements**

The Cisco VSG and Cisco VNMC installations have the following host requirements:

- ESX/ESXi platform that runs VMware software release 4.0.0 or 4.1.0 with a minimum of 4-GB physical RAM for the Cisco VSG and 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/ps13095/tsd\_products\_support\_series\_home.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 Cisco VNMC Software from an OVA Template

As with most software application installations, there is an order of installation for the Cisco VNMC and the Cisco VSG that must be followed to ensure that all components work and communicate properly. This first task involves using an OVA Template to install the Cisco VNMC software.

#### **BEFORE YOU BEGIN**

Before starting the procedure, know or do the following:

- Verify that the Cisco VNMC OVA image is available in the vCenter
- IP/subnet mask/gateway information for the Cisco VNMC

#### Send document comments to vsg-docfeedback@cisco.com

- The admin password, shared\_secret, hostname that you want to use
- The DNS server and domain name information
- 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 VSM. The port profile is configured in the VSM and is used for the Cisco VNMC management interface.

- Make sure that the host has 2-GB RAM and 25-GB available hard-disk space
- Have a shared secret password available (this password is what enables communication between the Cisco VNMC, VSM, and Cisco VSG)

#### PROCEDURE

Γ

- **Step 1** Choose the host on which to deploy the Cisco VNMC VM.
- Step 2 From the File menu, choose Deploy OVF Template.

The Deploy OVF Template window opens. See Figure 2-1.

#### 🛃 Deploy O¥F Template \_ 🗆 🗡 Source Select the source location Source OVF Template Details Name and Location Datastore Disk Format Deploy from a file or URL Ready to Complete C:\tmp\vnmc.1.0.0.502.ova -Browse... Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive. <u>H</u>elp <u><</u> Back Next $\geq$ Cancel

Figure 2-1 Deploy OVF Template—Source Window

Step 3 In the Deploy from a file or URL field, enter the path to the Cisco VNMC OVA file and click Next. The OVF Template Details window opens. See Figure 2-2.

#### Send document comments to vsg-docfeedback@cisco.com

#### Figure 2-2 Deploy OVF Template – OVF Template Details Window

eploy OVF Template		
DVF Template Details Verify OVF template details.		
<u>Source</u> DYF Template Details End User License Agreement	Product:	Virtual Network Management Center
Name and Location Deployment Configuration	Version:	1.0(0.502)
Datastore Disk Format	Vendor:	Cisco Systems, Inc.
Network Mapping Properties	Publisher:	No certificate present
Ready to Complete	Download size:	463.8 MB
	Size on disk:	1.7 GB (thin provisioned) 20.0 GB (thick provisioned)
	Description:	Cisco Virtual Network Management Center
<u>H</u> elp		≤Back Next ≥ Cancel

**Step 4** Review the details of the Cisco VNMC template and click Next.

The End User License Agreement window opens. See Figure 2-3.

#### Figure 2-3 Deploy OVF Template – End User License Agreement Window

Source		
OVF Template Details End User License Agreeme Name and Location Deployment Configuration	End User License Agreement IMPORTANT: PLEASE READ THIS END USER LICENSE AGREEMENT CAREFULLY. DOWNLOADING, INSTALLING OR USING CISCO OR CISCO-SUPPLIED SOFTWARE CONSTITUTES ACCEPTANCE OF	-
Datastore Disk Format Network Mapping Properties	THIS AGREEMENT. CISCO SYSTEMS, INC. OR ITS SUBSIDIARY LICENSING THE SOFTWARE INSTEAD OF CISCO SYSTEMS, INC. ("CISCO") IS WILLING TO LICENSE ITS SOFTWARE TO YOU ONLY UPON THE	
Ready to Complete	CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS END USER LICENSE AGREEMENT PLUS ANY ADDITIONAL LIMITATIONS ON THE LICENSE SET FORTH IN A SUPPLEMENTAL LICENSE AGREEMENT ACCOMPANYING THE PRODUCT (COLLECTIVELY THE "AGREEMENT"). TO THE EXTENT OF ANY CONFLICT BETWEEN THE TERMS OF THIS END USER LICENSE AGREEMENT AND ANY SUPPLEMENTAL LICENSE AGREEMENT, THE SUPPLEMENTAL LICENSE AGREEMENT AND ANY SUPPLEMENTAL LICENSE AGREEMENT, THE SUPPLEMENTAL LICENSE MAREEMENT AND ANY SUPPLEMENTAL LICENSE MAREEMENT, THE SUPPLEMENTAL LICENSE BINDING YOURSELF AND THE BUSINESS ENTITY THAT YOU REPRESENT	
	(COLLECTIVELY, "CUSTOMER") TO THE AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THE AGREEMENT, THEN CISCO IS UNWILLING TO LICENSE THE SOFTWARE TO YOU AND (A) YOU MAY NOT DOWNLOAD, JINSTALL OR USE THE SOFTWARE, AND (B) YOU MAY RETURN THE SOFTWARE (INCLUDING ANY UNOPENED CD PACKAGE AND ANY WRITTEN MATERIALS) FOR A FULL REFUND, OR, JF THE SOFTWARE AND WRITTEN MATERIALS ARE SUPPLIED AS PART OF ANOTHER PRODUCT, YOU MAY RETURN THE ENTIRE PRODUCT FOR A FULL REFUND. YOUR RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM CISCO OR AN AUTHORIZED CISCO RESELLER, AND APPLIES ONLY JF YOU ARE THE ORIGINAL END USER PURCHASER.	-
Þ	Accept	_

Step 5 Click Accept to accept the End User License Agreement and click Next.

#### Send document comments to vsg-docfeedback@cisco.com

The Name and Location window opens. See Figure 2-4.

Name: Virtual Network Management: Center	
Nirtual Network Management Center	
,	folder.
Terrenken i senkine	
Dol-DC1	
	The name can contain up to 80 characters and it must be unique within the inventory f Inventory Location: SG1-DC1

Figure 2-4 Deploy OVF Template – Name and Location

- **Step 6** In the Name field, enter the name of the Cisco Virtual Network Management Center. The name can contain up to 80 characters and i must be unique within the inventory folder.
- Step 7 In the Inventory Location pane, choose the location that you would like to use and click Next.The Deployment Configuration window opens. See Figure 2-5.

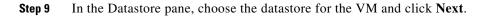
#### Send document comments to vsg-docfeedback@cisco.com

#### Figure 2-5 Deploy OVF Template – Deployment Configuration Window

P Deploy OVF Template	
Deployment Configuration Select a deployment configur	ation.
Source OVF Template Details	
End User License Agreement	Configuration:
Name and Location	VNMC Installer
Deployment Configuratior	
Datastore	Use this deployment option to configure the VNMC using the installer application. If this option is
Disk Format Network Mapping	selected, please enter the properties as prompted in the Properties section ahead.
Properties	
Ready to Complete	
• · · · ·	
Help	<u>≤</u> Back Next ≥ Cancel

Step 8 From the Configuration drop-down list, choose VNMC Installer and click Next.The Datastore window opens. See Figure 2-6.

Where do you want to -	store the virtual machine fil	es?					
innoro do you nane co.							
Source	Select a datastore in w	hich to store th	e VM files:				
OVF Template Details End User License Agreemen	Name	Capacity	Provisioned	Free	Туре	Thin Provisioning	Ac
Name and Location	[SG_PR_LUN	49.75 GB	48.20 GB	1.55 GB	VMFS	Supported	Mu
Deployment Configuration	[SG_PR_LUN	66.50 GB	56.31 GB	10.19 GB	VMFS	Supported	Mu
Datastore	[Storage1 (1)]	464.50 GB	127.05 GB	402.14 GB	VMFS	Supported	Sin
Disk Format	[SG_PR_LUN	49.75 GB	39.41 GB	10.34 GB	VMFS	Supported	Mu
Network Mapping	[SG_PR_LUN	49.75 GB	34.61 GB	15.14 GB	VMFS	Supported	Mu
Properties Ready to Complete	[SG_PR_LUN	49.75 GB	32.02 GB	17.73 GB	VMFS	Supported	Mu
Ready to Complete	[SG_PR_LUN	49.75 GB	46.62 GB	3.13 GB	VMFS	Supported	Mu
	•						
	Compatibility:						



#### Send document comments to vsg-docfeedback@cisco.com



**Note** 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.

The Disk Format window opens. See Figure 2-7.



🛃 Deploy O¥F Template		
Disk Format In which format do you war	nt to store the virtual disks?	
Source OVF Template Details End User License Agreement Name and Location Deployment Configuration Datastore Disk Format Network Mapping Properties Ready to Complete	Information about the selected datastore: Name: Storage1 (1) Capacity: 464.5 GB Free space: 410.8 GB Select a format in which to store the virtual machines virtual disks: Thin provisioned format The storage is allocated on demand as data is written to the virtual disks. This is supported only on VMFS3 and newer datastores. Other types of datastores might create thick disks. Estimated disk usage: 3.8 GB Thick provisioned format All storage is allocated immediately. Estimated disk usage: 20.0 GB	
Help	≤ Back Next ≥	Cancel

Step 10 Click either Thin provisioned format or Thick provisioned format to store the VM vdisks and click Next.

#### 

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

# <u>Note</u>

Ignore the red text in the window.

The Network Mapping window opens. See Figure 2-8.

#### Figure 2-8 Deploy OVF Template – Network Mapping Window

letwork Mapping What networks should I	he deployed template use?		
iource DVF Template Details ind User License Agreemer		template to networks in your inventory	
lame and Location	Source Networks	Destination Networks	
Deployment Configuration Datastore	VM Network	Management	
leady to Complete	Description: This network provides connectivity	to this virtual machine.	<u></u>
			<u>_</u>

Step 11 In the network mapping pane, choose the management network port profile for the VM and click Next. The Properties window opens. See Figure 2-9.

Deploy OVF Template		
Properties Customize the software solu	tion for this deployment.	
Source OVF Template Details		
End User License Agreement Name and Location Deployment Configuration Datastore Disk Format	a. IP Address IPv4 Enter the VM IP in the following form: 192.168.0.10 ID , 193 , 75 , 95	
Network Mapping Properties Ready to Complete	b. IP Netmask Netmask Enter the Subnet Mask in the following form: 255.255.255.0	
	255 , 255 , 248 , 0 c. Gateway IPy4Gateway	
	Enter the gateway in the following form: 192.168.0.1 Not all properties have valid values. The vApp will not be able to power on.	1
Help	≤ Back Next ≥	Cancel

**Step 12** Do the following:

- a. In the IPv4 field, enter the IP address.
- **b.** In the Netmask field, enter the subnet mask.
- c. In the IPv4Gateway field, enter the gateway.
- d. In the Hostname section:
  - In the DomainName field, enter the domain name.
  - In the DNS field, enter the domain name server name.
- e. In the Passwords section:
  - In the Password field, enter the admin password.
  - In the Secret field, enter the shared secret password.
- Step 13 Click Next.

# <u>Note</u>

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.

# <u>Note</u>

Ignore the VNMC Restore fields.

The Ready to Complete window opens. See Figure 2-10.

#### Figure 2-10 Deploy OVF Template – Ready to Complete Window

Are these the options you	want to use?		
Source OVF Template Details	When you click Finish, the de	eployment task will be started.	
End User License Agreement Name and Location Deployment Configuration Datastore Disk Format Network: Mapping Properties Ready to Complete	OVF file: Download size: Size on disk: Name: Folder: Deployment Configuration: Host/Cluster: Datastore: Disk Format: Estimated disk usage: Network Mapping: IP Allocation: Property: Prope	C:\tmp\vmc.1.0.0.502.ova 463.8 MB 1.7 GB Virtual Network Management Center SG1-DC1 VNMC Installer 10.193.75.94 Storage1 (1) Thin Provisioning 1.7 GB "VM Network" to "Management" Fixed, IPv4 IPv4 = 10.193.75.95 Netmask = 255.255.248.0 IPv4Gateway = 10.193.72.1 Hostname = VNMC Domainname = example.com DNS = 203.0.113.1 Password = Example_Secret123 RestoreProto = scp RestoreFibe = signore Pactoral locations = com Pactoral locations = com Pactora	

**Step 14** Review the deployment settings information and click **Finish**.

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

The Deploying Virtual Network Management Center progress indicator opens. See Figure 2-11.

The progress bar in Figure 2-11 shows how much of the deployment task is completed before the Cisco VNMC is deployed.

#### Figure 2-11 Deploying Virtual Network Management Center—Deploying Disk Files Progress Indicator

🛃 5% Deploying Virtual Network Management Cent	er 💶 🗙
Deploying Virtual Network Management Center	
Deploying disk 1 of 1 from C:\tmp\vnmc.1.0.0.502-disk1.vm	dk
	Cancel
1 minute and 13 seconds remaining	050
	227

The progress indicator in Figure 2-12 shows that the deployment has completed successfully.

#### Send document comments to vsg-docfeedback@cisco.com

Figure 2-12 Deployment Completed Successfully Progress Indicator

Deployment Completed Successfully	
Deploying Virtual Network Management Center	
Completed Successfully	
	Close

- Step 15 Click Close.
- **Step 16** Power on the Cisco VNMC VM.

# Task 2—On the Cisco VNMC, Setting Up VM-Mgr for vCenter Connectivity

This section includes the following topics:

- Downloading the vCenter Extension File from the Cisco VNMC, page 2-15
- Registering the vCenter Extension Plugin in the vCenter, page 2-18
- Configuring the vCenter in VM-Manager in the Cisco VNMC, page 2-19

#### **BEFORE YOU BEGIN**

Before doing this procedure, know or do the following:

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

### Downloading the vCenter Extension File from the Cisco VNMC

You can download the vCenter extension file from the Cisco VNMC.

#### PROCEDURE

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

A Website Security Certification window opens. See Figure 2-13.

#### Send document comments to vsg-docfeedback@cisco.com

Figure 2-13	Website Security	Certification	Window
-------------	------------------	---------------	--------

🚖 Favorites	Certificate Error: Navigation Blocked	🦄 🔹 🗔 👘 🖾 👼 👻 Bage 👻 Safety + Tools + 🔞 +	"
	There is a problem with this website's security certificate.		~
$\mathbf{i}$			
	The security certificate presented by this website was not issued by a trusted certificate presented by this website was issued for a different website?		
	Security certificate problems may indicate an attempt to fool you or intercept any d server.	data you send to the	
	We recommend that you close this webpage and do not continue to this web	absite.	
	Ø Click here to close this webpage.		
	Continue to this website (not recommended).		
	O More information		
Done		🕥 Internet 🦛 + 🔍 100% +	2

Step 2 On the certificate warning window, click Continue to this website.

The Cisco VNMC Access window opens. See Figure 2-14.

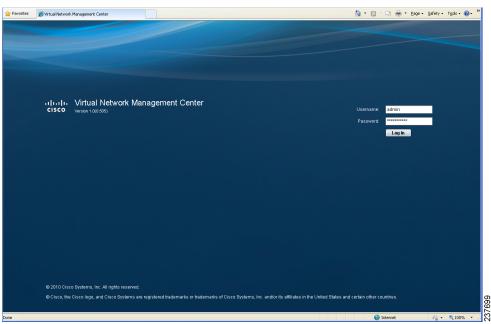


Figure 2-14 VNMC Access Window

**Step 3** Log in to the Cisco VNMC with the username "admin" and your password that you set when installing the application. The VNMC Main window opens. See Figure 2-15.

330067

#### Send document comments to vsg-docfeedback@cisco.com

#### Figure 2-15 Cisco Virtual Network Management Center—Opening Window

cisco Virtual Network Mana	gement Center	(adhiri)	Preferences	Log Out	About	нар
Tenant Management   Resource Management	Folicy Management   Administration		_			
Realisability Matrix	root General Out-Elements Fauto Events Properties Name: root Description: Lovst: 0			C (	Treate Tens	
2011 Cisco Systems, Inc. All rights reserved.						

**Step 4** Choose Administration > VM Managers. The Cisco Virtual Network Management Center VM Managers window opens. See Figure 2-16.

#### Figure 2-16 Cisco VNMC Administration VM Managers Window

Tenark Management   Resource Management   Policy Management   Administration					
Access Control Bervice Registry VNIMC Profile VM Managers Diagnostics Operations					
2 VM Managers					
Add VM Manager VM Managers	🗄 Add VM Mar	nager 🍝	Export vCer	ter Extensio	n
Export vCenter Extension General Will Managers Events Properties					
Extension Key: Cisco_VVLManager_1789399272					
Extension File Status: success					
Extension File Status Reason:					
vCenter Eidension file is required to establish secure connection between vCenter and VM-Manager. Export the extension file by cilcking "Export vCenter Extension" and install it as plugin on all the vCenter servers.					
5 2011 Cisco Systems, Inc. All rights reserved					

**Step 5** From VM Managers, right-click and choose **Export vCenter Extension**, and save the file on your vCenter Desktop.

330069

#### Send document comments to vsg-docfeedback@cisco.com

**Step 6** The vCenter Desktop displays as shown in Figure 2-17.

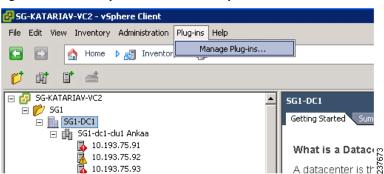
### **Registering the vCenter Extension Plugin in the vCenter**

This task is completed from within your client desktop vSphere client directory.

#### PROCEDURE

**Step 1** From vSphere client, log in to vCenter. See Figure 2-17.

Figure 2-17 vSphere Client Directory Window



- **Step 2** Choose **Plug-ins** > **Manage Plug-ins**.
- Step 3 Right-click in an empty space, and in the drop-down list, choose New Plug-in.

The Register Plug-in window that contains the vSphere client and vCenter directory for managing plug-ins opens. See Figure 2-18.

Figure 2-18 vSphere Client and vCenter Directory for Managing Plug-ins with Security Warning

Register Plug-in			E
Current vCenter Server:	SG-KATARIAV-VC2	2	
	and file which needs to be registered with vCentr		
File name: C:\Users\Ad	ministrator\Desktop\Cisco_VN_Manager_extens	ion.xml Browse	
View Xml: (read-only)			
xmins: xsi="	urn:vim25" versionId="uber" xsi:t http://www.w3.org/2001/XML		Î
	Certificate Warnings		
<key>Ci</key>	An untrusted certificate is provided as part of p	henticate the plug-in. Depending on your security	
- <server:< td=""><td></td><td></td><td></td></server:<>			
- <desc -<="" td=""><td>lick Ignore to continue using the certificate.</td><td>and the second se</td><td></td></desc>	lick Ignore to continue using the certificate.	and the second se	
<lab< td=""><td>Yew Certificate</td><td>Ignore ⊆ancel</td><td></td></lab<>	Yew Certificate	Ignore ⊆ancel	
<sui< td=""><td></td><td></td><td></td></sui<>			
	y>Cisco Systems Inc.VS	>	
- <client></client>			
<url></url>			
- <descript <label< p=""></label<></descript 			
<laber <="" td=""><td>· · ·</td><td></td><td></td></laber>	· · ·		

237674

#### Send document comments to vsg-docfeedback@cisco.com

- Step 4 Browse to the Cisco VNMC vCenter extension file and click Register Plug-in.
- **Step 5** On the security warning that displays, click **Ignore**.

The Register Plug-in progress indicator opens. When the registration has completed successfully, the successful registration message will display. See Figure 2-19.

Figure 2-19 Register Plug-in Progress Success Indicator

egister Plug-in	-
The plug-in "Cisco_VN_Manager_1846481687" is vCenter Server sg-katariav-vc2.	successfully registered on
	ОК

Step 6 Click OK.

Step 7 Click Close.

### **Configuring the vCenter in VM-Manager in the Cisco VNMC**

You can configure the vCenter in VM-Manager in the Cisco VNMC.

#### PROCEDURE

Step 1 Return to the Cisco VNMC and click Administration > VM Managers. The Cisco VNMC Administration VM Managers window opens. See Figure 2-20.

#### Send document comments to vsg-docfeedback@cisco.com

Figure 2-20

20 Cisco VNMC Administration VM Managers Window

cisco Virtual Network Manag	ement Center	(admin)	Preferences	Log Out	About	нар
Tenant Management Resource Management			_			
Access Control Service Registry VNMC Profile VII	Managers Diagnostics Operations					
VM Managers	VM Managers	🚦 Add Vi	N Manager	🚡 Export v Cer	nter Extensi	on 🗆
Export vCerifer Extension	Greek VM Managers Events Properties Extension Kiry: Cisco_VA_Manager_1799399272 Extension File Status: success Extension File Status Reaser: vCenter Extension Tile is required to astabilish secure connection between v Export the extension file by citking Export vCenter Extension" and install it a					
@ 2011 Cince Systems, Inc. All rights reserved						_

**Step 2** Choose VM Managers > Add VM Manager.

The Add VM Manager dialog box opens. See Figure 2-21.



🚖 Add VM Manager		□ ×
Add VM Man	ager	0
Name:	vCenter-Server	
Description:	vCenter Server	
Hostname / IP Address:	10.103.75.70	
	ОК	Cancel

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

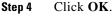
a. In the Name field, enter the vCenter name (no spaces allowed).

- **b.** In the Description field, enter a brief description of the vCenter.
- c. In the Hostname/IP Address field, enter the vCenter IP address.

330070

Task 3—On the VSM, Configuring the Cisco VNMC Policy-Agent

#### Send document comments to vsg-docfeedback@cisco.com





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 you have the Cisco VNMC installed, you must register the Virtual Supervisor Module (VSM) with the Cisco VNMC policy agent.

#### **BEFORE YOU BEGIN**

Before starting the procedure, know or do the following:

• Make sure that the Cisco VNMC policy-agent image is available on the VSM (for example, vnmc-vsmpa.1.0.1j.bin)



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 Cisco VNMC installation
- Make sure that IP connectivity between the VSM and the Cisco VNMC is okay.

Note

If you have upgraded your VSM to 1.4, you need to copy the VSM policy agent image, available in VNMC image bundle, to bootflash to complete registration with VNMC.

#### PROCEDURE

L

**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.1.0.1j.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 1.0(1j)-vsm
vsm#
```

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

#### Send document comments to vsg-docfeedback@cisco.com

The VSM is now registered with the Cisco VNMC.

#### **EXAMPLES**

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**

Before starting the procedure, know or do 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)



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** To exit, press **Ctrl-Z**.

Chapter 2 Quick Start Guide for the Cisco Virtual Security Gateway and the Cisco Virtual Network Management

#### Send document comments to vsg-docfeedback@cisco.com

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)#
vsm(config)# copy running-config startup-config
vsm(config)# exit
```

- **Step 6** To end the session, press **Ctrl-Z**.
- **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)#
vsm(config)#
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)#
```

To end the session, press Ctrl-Z.

# Task 5—Installing the Cisco VSG from an OVA Template

Once you have installed the Cisco Virtual Network Management Center (Cisco VNMC), configured the Cisco VNM policy agent on the VSM, and prepared the Cisco VSG port profiles by creating the VLANs that will be used, you now must install the Cisco VSG.

For this example, the OVF Template is used to install a Cisco VSG in standalone mode.

Task 5—Installing the Cisco VSG from an OVA Template

#### Send document comments to vsg-docfeedback@cisco.com

#### **BEFORE YOU BEGIN**

Before starting the procedure, know or do the following:

- Make sure that the Cisco VSG OVA image is available in the vCenter
- Cisco VSG-data and Cisco VSG-HA port profile created on VSM
- Management port-profile (management)



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.

- HA ID
- IP/subnet mask/gateway information for the Cisco VSG
- Admin password
- 2-GB RAM and 3-GB hard disk space
- Cisco VNMC IP
- Shared secret
- IP connectivity between Cisco VSG and Cisco VNMC is okay
- Cisco VSG VNM-PA image name (vnmc-vsgpa.1.0.1j.bin)

#### PROCEDURE

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

**Step 2** From the File menu, choose **Deploy OVF Template**.

The Source window opens. See Figure 2-22.



🚰 Deploy OVF Template		
Source Select the source location.		
Source OVF Template Details Name and Location Resource Pool Datastore Disk Format Ready to Complete	Deploy from a file or URL C:\tmp\nexus-1000v.V5G1.0.375.ova Ther a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.	
Help	< Back Next >	Cancel 590 Cancel

**Step 3** In the Deploy from a file or URL field, enter the path to the Cisco VSG OVA file and click **Next**. The OVF Template Details window opens. See Figure 2-23.

Figure 2-23 Deploy OVF Template – OVF Template Details Window

Deploy OVF Template					
OVF Template Details Verify OVF template details.					
Source OVF Template Details End User License Agreement Name and Location Deployment Configuration Resource Pool Datastore Disk Format Network Mapping Properties Ready to Complete	Product: Version: Vendor: Publisher: Download size: Size on disk:	Nexus1000VSG 4.2(1)VSG1(1) Cisco Systems Inc No certificate present 65.9 MB Unknown (thin provisioned) 3.0 GB (thick provisioned)			
	Description:	Cisco Nexus 1000V5G			
Help			< Back	Next >	Cancel

Cisco Virtual Security Gateway, Rel. 4.2(1)VSG1(2) and Cisco Virtual Network Management Center, Rel. 1.2 Installation and Upgrade Guide

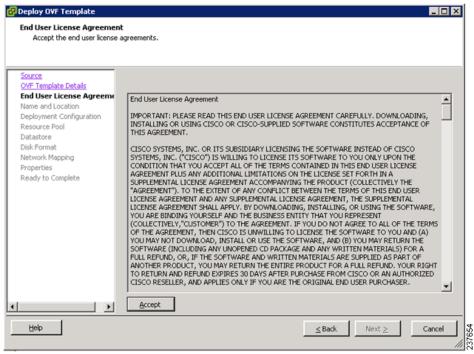
Task 5—Installing the Cisco VSG from an OVA Template

#### Send document comments to vsg-docfeedback@cisco.com

**Step 4** Review the details of the Cisco VSG template and click **Next**.

The End User License Agreement window opens. See Figure 2-24.

Figure 2-24	Deploy OVF Template – End	d User License Agreement Window
-------------	---------------------------	---------------------------------



Step 5 Click Accept to accept the End User License Agreement.

#### Step 6 Click Next.

The Name and Location window opens. See Figure 2-25.

#### Send document comments to vsg-docfeedback@cisco.com

iource WF Template Details Ind User License Agreement Jame and Location	Name: Nexus1000V/SG The name can contain up to 80 characters and it must be unique within the inventory folder.	
eployment Configuration tesource Pool Vatastore Visk Format Jetwork Mapping roperties teady to Complete	Inventory Location:	
cody to complete		

#### Figure 2-25 Deploy OVF Template – Name and Location Window

- **Step 7** In the Name field, enter the name that you want to use for the Cisco VSG.
- **Step 8** In the Inventory Location field, choose the location that you want to use for hosting the Cisco VSG.
- Step 9 Click Next.

The Deployment Configuration window opens. See Figure 2-26.

Task 5—Installing the Cisco VSG from an OVA Template

#### Send document comments to vsg-docfeedback@cisco.com

#### Figure 2-26 Deploy OVF Template – Deployment Configuration Window

Peploy OVF Template	
Deployment Configuration Select a deployment configur	ation.
source a copie, ment comiga	
Source	
OVF Template Details	Castin wation
End User License Agreement	Configuration:
Name and Location	Deploy Nexus 1000VSG as Standalon
Deployment Configuration Resource Pool	Deploy Nexus 1000VSG as Standalone
Datastore	Deploy Nexus 1000VSG as Primary Deploy Nexus 1000VSG as a standalone system. If this option is compted in the Properties section alread
Disk Format	Deploy Nexus 1000VSG as Secondary Manually Configure Nexus 1000VSG
Network Mapping	
Properties	
Ready to Complete	
<b>▲</b>	
Help	≤Back Next ≥ Cancel

Step 10 From the Configuration drop-down list, choose Deploy Nexus 1000V as Standalone and click Next. The Datastore window opens. See Figure 2-27.

#### Send document comments to vsg-docfeedback@cisco.com

Source	Select a datastore in w	hich to store th	e VM files:			
OVF Template Details End User License Agreement	Name	Capacity	Provisioned	Free Typ	e Thin Provisioning	Acc
Name and Location	[SG_PR_LUN	49.75 GB	48.20 GB	1.55 GB VM	=S Supported	Muli
Deployment Configuration	[SG_PR_LUN	66.50 GB	56.31 GB	10.19 GB VM	=S Supported	Muli
Datastore	[Storage1 (1)]	464.50 GB	127.05 GB	402.14 GB VM	=S Supported	Sing
Disk Format	[SG_PR_LUN	49.75 GB	39.41 GB	10.34 GB VM	=S Supported	Muli
Network Mapping	[SG_PR_LUN	49.75 GB	34.61 GB	15.14 GB VM	=S Supported	Muli
Properties Ready to Complete	[SG_PR_LUN	49.75 GB	32.02 GB	17.73 GB VM	=S Supported	Muli
Ready to Complete	[SG_PR_LUN	49.75 GB	46.62 GB	3.13 GB VM	Supported	Mul
	•					
	Compatibility:					

#### Figure 2-27 Deploy OVF Template – Datastore Window

**Step 11** In the Select a datastore in which to store the VM files pane, choose the datastore for the VM and click **Next**.

Note

Storage can be local or shared-remote such as a network file storage (NFS) or a 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 storage location that is available.

The Disk Format window opens. See Figure 2-28.

Task 5—Installing the Cisco VSG from an OVA Template

#### Send document comments to vsg-docfeedback@cisco.com

#### Figure 2-28 Deploy OVF Template – Disk Format Window

Deploy OVF Template Disk Format In which format do you wai	nt to store the virtual disks?	
Source OVF Template Details End User License Agreement Name and Location Deployment Configuration Resource Pool Datastore Disk Format Network Mapping Properties Ready to Complete	Information about the selected datastore: Name: datastore1-91 Capacity: 464.5 G8 Free space: 364.0 GB Select a format in which to store the virtual machines virtual disks: The storage is allocated on demand as data is written to the virtual disks. This is supported only on VMFS3 and newer datastores. Other types of datastores might create thick disks. Estimated disk usage: Unknown Thick provisioned format All storage is allocated immediately. Estimated disk usage: 3.0 GB	
Help	≤ Back Next ≥	Cancel

- Step 12 Click either Thin provisioned format or Thick provisioned format to store the VM vdisks and click Next.

**Note** 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.

The Network Mapping window opens. See Figure 2-29.

#### Send document comments to vsg-docfeedback@cisco.com

#### Figure 2-29 Deploy OVF Template – Network Mapping Window

Deploy OVF Template Network Mapping What networks should th	e deployed template use?	
Source OVF Template Details End User License Agreement	Map the networks used in this OVF	- template to networks in your inventory
Name and Location	Source Networks	Destination Networks
Deployment Configuration	Data	VSG-Data
Resource Pool	Management	Management
<u>Datastore</u> Disk Format	HA	VSG-HA
Ready to Complete	Description:	
		n the Nexus 1000VSG primary and secondary. Please associate it Adds to the "ha vlan" configured in the VSG.
Help		≤ Back Next ≥ Cancel

- **Step 13** Choose the data interface port profile as **VSG-Data**, choose the management interface port profile as **Management**, and choose the HA interface port profile as **VSG-HA**.
- Step 14 Click Next.



In this example, for VSG-Data and VSG-HA port profiles created in Task 4—On the VSM, Preparing Cisco VSG Port Profiles, page 2-22, the management port profile is used for management connectivity and is the same as in the VSM and Cisco VNMC.

The Properties window opens. See Figure 2-30.

#### Figure 2-30 Deploy OVF Template – Properties Window

<b>Properties</b> Customize the software so	lution for this deployment.	
Source OVF Template Details End User License Agreement Name and Location Deployment Configuration Resource Pool Datastore Disk Format Network Mapping Properties Ready to Complete	a. VSG HA Id         HaId         Enter the HA Id (1-4095).         \$503         b. Nexus 1000VSG Admin User Password         Password         Enter the password. Must contain at least one capital, one lowercase, one number.         Example_Password123         c. Management IP Address         Management IPV4         Enter the VSG Ip in the following form: 192.168.0.10         10 , 193 , 75 , 101	
Help	≤Back Next ≥	Cancel

#### **Step 15** Do the following:

- **a.** In the Hald 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 Management IP Address section, do the following:
  - In the ManagementIpV4 field, enter the IP address for the Cisco VSG.
  - In the ManagementIpV4 Subnet field, enter the subnet mask.
- d. In the Gateway field, enter the gateway name.
- e. In the VnmcIpV4 field, enter the IP address of the Cisco VNMC.
- f. In the SharedSecret field, enter the shared secret password defined during the Cisco VNMC installation.
- g. In the ImageName field, enter the VSG VNM-PA image name (vnmc-vsgpa.1.0.1j.bin)

Step 16 Click Next.



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.

The Ready to Complete window opens. See Figure 2-31.

#### Send document comments to vsg-docfeedback@cisco.com

#### Figure 2-31 Deploy OVF Template—Ready to Complete Window

Ready to Complete Are these the options you Source				
OVF Template Details	When you click Finish, the do Deployment settings:	eployment task will be started.		
End User License Agreement Name and Location Deployment Configuration Resource Pool Datastore Disk Format Network Mapping Properties Ready to Complete	OVF file: Download size: Size on disk: Name: Folder: Deployment Configuration: Host/Cluster: Datastore: Disk Format: Estimated disk usage: Network Mapping: Network Mapping: IP Allocation: Property: Property: Property: Property: Property: Property: Property: Property: Property: Property: Property: Property: Property: Property: Property: Property: Property: Property:	C:\tmp\nexus-1000v.V5G1.0.375.ova 82.5 MB Unknown Nexus1000V5G SG1-DC1 Deploy Nexus 1000V5G as Standalone SG1-dC1-clu1 Ankaa Storage1 Thin Provisioning Unknown "Data" to "VSG-Data" "Management" to "Management" "HA" to "VSG-HA" Fixed, IPv4 HaId = 3501 Password = Example_Password123 ManagementIpV4 = 10.193.75.101 ManagementIpV4 = 10.193.75.101 ManagementIpV4 = 10.193.75.95 SharedSecret = Example_Secret123 ImageName = vnmc-vsgpa.1.0.1d.bin		
Help	1	<u>≤</u> Back	Finish	Cancel

**Step 17** Review the deployment settings information and click **Finish**.

Note

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

The Deploying Nexus1000VSG Progress Indicator opens. See Figure 2-32.

The progress bar in Figure 2-32 shows how much of the deployment task is completed before the Cisco VSG is deployed.

#### Figure 2-32 Deploying Nexus1000VSG—Deploying Disk Files Progress Indicator

🛃 56% Deploying Nexus1000¥5G	
Deploying Nexus1000VSG	
Deploying disk 1 of 1 from C:\tmp\nexus-1000v.VSG1.0.375.disk1.vmdk	
Cancel	
14 seconds remaining	8
	237720

The progress indicator in Figure 2-33 shows that the deployment has completed successfully.

Chapter 2 Quick Start Guide for the Cisco Virtual Security Gateway and the Cisco Virtual Network Management

Task 6—On the Cisco VSG and Cisco VNMC, Verifying the VNM Policy Agent Status

#### Send document comments to vsg-docfeedback@cisco.com

Deploying Nexus1000VSG
Completed Successfully

**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 VNM 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 1.0(1j)-vsg
vsg#
```

- **Step 3** Log in to the Cisco VNMC.
- Step 4 Choose Administration > Service Registry > Clients > General. The VNMC Administration Service Registry Window opens. See Figure 2-34.

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

#### Send document comments to vsg-docfeedback@cisco.com

Figure 2-34

VNMC Administration Service Registry Window

	ement I Policy Nanagement I Administ	Tauun	and the second	and the second			
ss Control Service Registry VNMC Pri	ofile VM Managers Diagnostics Operations						
🚡 Diagnostics							
Registry VNCM-favid	Clients						
Controllers	General Events						
Providers							
Clients	Name	Capability	Туре	IP Address	Oper State	Last Poll	Version
	Firewall	vm-fw	managed-endport	10.193.75.101	registered	2010-11-26 00	1.0(0,477)
	sg-vtm vk-1	VII-VVSW	managed-endport	10.193.75.89	registered	2010-11-26 00	1.0(0,477)

Step 5

5 In the Clients pane, 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.

#### **BEFORE YOU BEGIN**

Before doing this procedure, know or do the following:

- Install Adobe Flash Player (Version 10.1.102.64 or later)
- IP address of the Cisco VNMC
- 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).

A Website Security Certification window opens. See Figure 2-35.

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

#### Send document comments to vsg-docfeedback@cisco.com

avorites	Certificate Error: Navigation Blocked		🏠 * 🔝 🛸 🖶 👘 * Page + Safety + Tools + 🔞
8	There is a problem with this websit		
		site was not issued by a trusted certificate authority. site was issued for a different website's address.	
	Security certificate problems may indicate an server.	attempt to fool you or intercept any data you send to the	
	We recommend that you close this webp		
	🥙 Click here to close this webpage.		
	Sontinue to this website (not recommend		
	More information		

#### Step 2 On the certificate warning, click Continue to this website.

The Cisco VNMC Access window opens. See Figure 2-36.

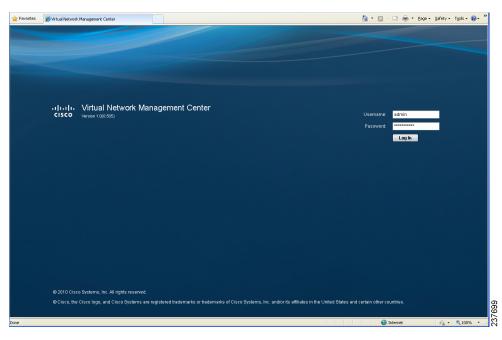


Figure 2-36 VNMC Access Window

Step 3 Log in to the Cisco VNMC with the username "admin" and your password.

### Send document comments to vsg-docfeedback@cisco.com

**Step 4** The Cisco VNMC Main window opens. See Figure 2-37.

Figure 2-37

t Management   Resource N	nagement   Policy Management   Administration	
kvallability Mattix ooot	root General Sul-Elements Fauts Events Properties Name: root Description: Lowit: 0	Create Tenor
	LUWE U	

Cisco Virtual Network Management Center-Opening Page

Step 5 Choose Administration > Service Registry > Clients to check the Cisco VSG and VSM registration in the Cisco VNMC.

The Clients pane of the Cisco VNMC opens. See Figure 2-38.

#### Figure 2-38 VNMC Administration Service Registry Window Clients Pane

	gement i Policy Nanagement i Administ						
	ofie VM Nanagers Diagnostics Operations						-
Diagnostics Registry VNCM-favid	Clients						
Controllers							
Providers	General Events						
Clients	Name	Capability	Туре	IP Address	Oper State	Last Poll	Records: 0 Version
	Firewall	vn-fw	managed-endport	10.193.75.101	registered	2010-11-26 00	1.0(0,477)
	sg-vtm vk-1	VII-WVSW	managed-endport	10.193.75.89	registered	2010-11-26 00 2010-11-26 00	1.0(0,477)
	age the start of	PIT-S Faile	The segme encloses	The Faller Part and	- again as	2010-11-20-00	1.00(00,4711)

Cisco Virtual Security Gateway, Rel. 4.2(1)VSG1(2) and Cisco Virtual Network Management Center, Rel. 1.2 Installation and Upgrade Guide

## Send document comments to vsg-docfeedback@cisco.com

The Cisco VSG and VSM information should be listed in the Clients pane.

# **Configuring a Tenant in the Cisco VNMC**

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

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

The root pane opens. See Figure 2-39.

	nagement Center	(schin) Preference	es Log Out About
nt Management   Resource Manage	ment Folicy Management   Administration		and the second se
Availability Matrix: Tool	root Crentral Out-Elements Faults Events Properties Name: root Description: Level: 0		Create Tessart

Figure 2-39 VNMC Window Tenant Management Tab root Pane

Step 2 In the left pane directory tree right-click on Root, and from the drop-down list, choose Create Tenant.The Create Tenant dialog box opens. See Figure 2-40.

## Send document comments to vsg-docfeedback@cisco.com

Figure	2-40
riguic	2 70

Create Tenant Dialog Box

🔺 Create		□ ×
Create	Tenant	0
Name: Description:	Tenant-A TenantA Organization	
		OK Cancel

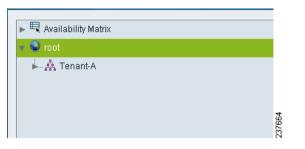
#### **Step 3** Do the following:

- **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 now listed in the left-side pane under root. See Figure 2-41.

Figure 2-41 Cisco VNMC VSG Configuration Directory Tree Pane



# **Configuring a Security Profile in the Cisco VNMC**

You can configure a security profile on the Cisco VNMC.

#### PROCEDURE

**Step 1** In the Cisco VNMC top row toolbar, click the **Policy Management** tab. The Policy Management Security Policies window opens. See Figure 2-42.

## Send document comments to vsg-docfeedback@cisco.com

Figure 2-42

2 VNMC Policy Management Security Policies Window

cisco Virtual Network Man	agement Center	(schin) Preferences	Log Out	About	Help
Tenant Management   Resource Managem	nt Policy Menagement Administration				
Security Policies Device Configurations Capal	ities Disgnostics				
	root General Sub-Elements Faults Events Properties Name: root Description:				
D 2011 Cisco Systems, Inc. All rights reserved.					

**Step 2** From the directory path, choose **Security Policies** > **root** > **Tenant-A** > **Security Profiles**. Right-click in an empty space and from the drop-down list, choose **Add Security Profile**.

The Add Security Profile dialog box opens. See Figure 2-43.

ral Attributes							
Name: sp-w	den						
escription:							
Policy set: 🚺 👝	lect Policy Set	<ul> <li>Add Policy Set</li> </ul>					
Sel							
Sel	olved Policy Set: 010-1001/0:	set-default					
Reso	olved Policy Set: 010-1000/0	ael-default					
Resolved Policies	olved Policy Set: <u>010-1001/0</u>					Records:	1
Sel	olved Policy Set: <u>010-1001/0</u>	eel-default  Destination Condition	Protocol	Ethertype	Action	Records: Description	1
solved Policies  (Un)assign Policy	olved Policy Set: oro-rooto:	ŧ	Protocol	Ethertype	Action	1	1
solved Policies 0 (Un)assign Policy Name	olved Policy Set: oro-rooto:	ŧ	Protocol	Ethertype	Action	1	1
solved Policies 0 (Un)assign Policy Name	olved Policy Set: oro-rooto:	ŧ	Protocol	Ethertype	Action	1	1
solved Policies 0 (Un)assign Policy Name	olved Policy Set: oro-rooto:	ŧ	Protocol	Ethertype	Action	1	1

Figure 2-43 Add Security Profile Dialog Box

- **Step 3** Do the following:
  - **a.** In the Name field, enter a name for the security profile; for example, *sp-web*.

### Send document comments to vsg-docfeedback@cisco.com

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

Step 4 Click OK.

## **On the Cisco VNMC, Configuring a Compute Firewall**

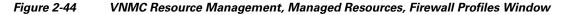
The compute firewall is a logical virtual entity that contains the device profile that you can bind (assign) to a Cisco VSG virtual machine. The device policy in the device profile is then pushed from the Cisco VNMC to the Cisco VSG. Once this is complete, the compute firewall is in the *applied* configuration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

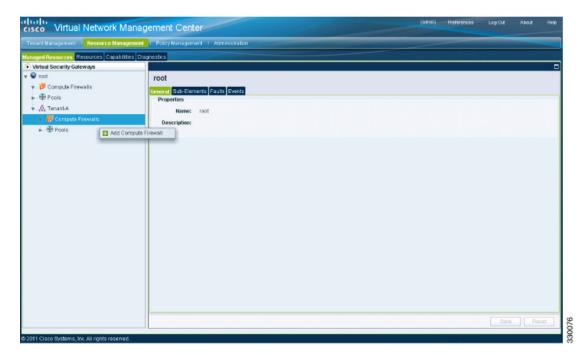
#### PROCEDURE

Γ

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

The VNMC Resource Management, Managed Resources, Firewall Profiles window opens. See Figure 2-44.





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. See Figure 2-45.

Chapter 2 Quick Start Guide for the Cisco Virtual Security Gateway and the Cisco Virtual Network Management

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

## Send document comments to vsg-docfeedback@cisco.com

Figure 2-45	Add Compute	Firewall	Dialoa	Вох
i igaio 🖬 io	/ aa oompato	i nonan	Dialog	

			□ ×
Add Compute	Firewall		0
neral			
Name: CFW-VSG- Description: Config State: not-applied	۸		
Firewall Settings			
Firewall Settings Device Profile:	default	د & Select	
Device Profile:	default firewall	ন্ট Select	
Device Profile:		৬ Select	
Device Profile: Management Hostname:	firewall	ও Select	

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

- In the Name field, enter a name for the compute firewall.
- In the Decription field, enter a brief description of the compute firewall.
- In the Management Hostname field, enter the name for your Cisco VSG.
- In the Data IP Address field, enter the Data IP address, if it is different from what is the default.

#### Step 5 Click OK.

The new Compute Firewall pane displays with the information that you provided. See Figure 2-46.

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

### Send document comments to vsg-docfeedback@cisco.com

Figure 2

2-46 Compute Firewall	Pane
-----------------------	------

Virtual Network Manag	ement Center	(adhin)	Preferences	Log Out Abou	a Holp
Tenant Nanagement Resource Management	Folicy Management   Administration		_		
anaged Resources Resources Capabilities Dia	prostes				
Virtual Security Gateways	💐 root 🕨 🏯 Tenent-A 🕨 👹 Connote Firewalls 🕨				(
root	CFW-VSG-A	🛶 Assign VSG	🥪 Assign Pool	👌 Unassign V	
<ul> <li></li></ul>	General Faults Events				
* A Tenant-A	Name: CFW-VSG-A				
Formula Firewalls CFW-V80-A	Description:	]			
- 🕀 Pools	Config State: not applied				
	Association State: unassociated				
	Pool Name: none				
	Firewall Settings				
	Device Profile: default & Select				
	Management Hostname: 0 frewal				
	Data IP Address: 0 10 10 200				
	Data IP Subnet: 255 . 255 . 0				
				Save	Reset
2011 Cisco Systems, Inc. All rights reserved.					

# 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.

You can assign the Cisco VSG to the compute firewall on the Cisco VNMC.

#### PROCEDURE

Step 1 Choose **Resource Management > Managed Resources**.

> The VNMC Resource Management Managed Resources Compute Firewalls window opens. See Figure 2-47.

Figure 2-47 VNMC Resource Management Managed Resources Compute Firewalls Window

non: Manacement    Hesource Manag	cmart Policy Management I Administration		and the second	Statement of the local division in which the
aged Resources Pern mes Capabiliti	es Diagonarios			
Virtual Socurity Galeways	🌻 root: 🕨 🙏 Tenent-A. 🕨			
v 🔮 100	Compute Firewalls			
- 🤔 Comade Firenals	General Faults			
- 🕀 Pros	🚦 Add Company Friveral 👘 Assign VEG 🧠	🖌 Avvign Pool 🌐 👌 Jaw valign VSG(Pool	🚺 Edi 👚 Daha	Reparce:
🔁 Hertautt	Name	Description	Device Profile	Crudiy State
- A Tenart-A	CFW/VEG/L		tefault	act-applied
Portpute Firewalls     Portpute Firewalls	10% C.S.			
	🚙 Avsign VEG			
P 00 -0.14	sp Assign Pco	1		
	😁 Unassign VSG/Poci			
	1 Delete	1		

**Step 2** Choose **root > Tenant-A > Compute Firewalls**.

Step 3 Right-click Compute Firewalls, and from the drop-down list, choose Assign VSG.The Assign VSG dialog box opens. See Figure 2-48.

🚖 Assign	□ ×
Assign VSG	0
Name: Select a VSG T 10.193.75.101	
	OK Cancel

Figure 2-48 Assign VSG Dialog Box

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

Step 5 Click OK.



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

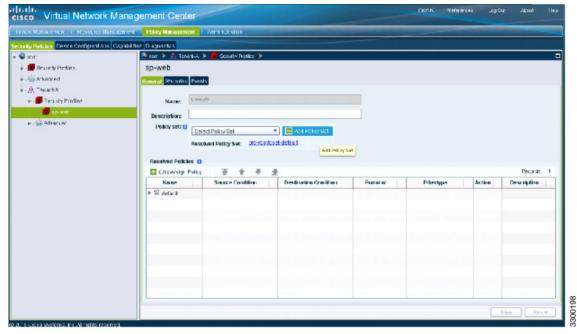
You can configure a permit-all rule in the Cisco VNMC.

#### PROCEDURE

**Step 1** Log in to the Cisco VNMC and choose **Policy Management > Security Policies**.

The Cisco VNMC Policy Management Security Policies window opens. See Figure 2-49.

#### Figure 2-49 Cisco Virtual Network Management Center—Policy Management Security Policies Window



- Step 2 Choose root > Tenant-A > Security-Profile > sp-web.
- **Step 3** From the button to the right of the sp-web pane Policy sets field, click **Add policy set**.

The Add Policy Set dialog box opens. See Figure 2-50.

Figure 2-50

## Send document comments to vsg-docfeedback@cisco.com

Add Policy Set Dialog Box

eral						
Name:	PS_web					
escription:						
Policies: 🚺	🕂 Add Policy 📑 Ed	t				
	Available : Add Poli		Assigned :			
	Add Poli	oy	至 余	+	Ŧ	
	default					
		>>				
		>				
		<				
		~				

Step 4 Click Add Policy. The Add Policy dialog box appears. See Figure 2-51.

Cisco Virtual Security Gateway, Rel. 4.2(1)VSG1(2) and Cisco Virtual Network Management Center, Rel. 1.2 Installation and Upgrade Guide

330200

### Send document comments to vsg-docfeedback@cisco.com

Name: Description:	pol_web				
ules					
ules Add Rule	1				Records:
	Source Condition	Destination Condition	Protocol	Ethertype	Records: Action
Add Rule	Source Condition	1 1	Protocol	Ethertype	-

Figure 2-51 Add Policy Dialog Box

**Step 5** 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.

The Add Rule dialog box displays. See Figure 2-52.

## Send document comments to vsg-docfeedback@cisco.com

Figure 2	2-52
----------	------

2 VNMC Add Rule Dialog Box

Name:	permikall		_			
Description:	\$ 					
ction to take: 🚺	0.000	terra				
	C drop  permit C	re set				
Protocol: 🖪						
	IN THE					
	T					
Ether Type: 🚺	✓ Any					
Ether Type: 0	🗹 Any		Destination Conditions	D		
Ether Type: 🚺	🗹 Any	Kecords: U	Destination Conditions	D	Hecords:	U
Ether Type: 🛛 ource Conditions	∉ Any s D	Kecords: U Attribute Value		D Operator	Hacorda: Attribute Value	U
Ether Type: O ource Conditions Adc	∉ Any s D		Add			U
Ether Type: 0 ource Conditions Adc	∉ Any s D		Add			U
Ether Type: 0 ource Conditions Adc	∉ Any s D		Add			U
Ether Type: O ource Conditions Adc	∉ Any s D		Add			U

- **Step 6** In the Name field, enter the rule name.
- **Step 7** In the Description field, enter a brief description of the rule.
- **Step 8** From the Action to Take buttons, choose the rule action that you want this rule to have; in this case, **permit**.
- **Step 9** Click **OK** in this Add Rule dialog box.

The Add Policy dialog box reappears showing a policy with the new rule. See Figure 2-53.

### Send document comments to vsg-docfeedback@cisco.com

Add					□ >
Add P	olicy				0
neral					
Nam	e: pol_web				
Description	*				
Description	d.				
Rules 🗄 Add Rul	•   Ŧ ★ + ]	Ł			Records: 1
	le 🛛 🖀 🛊 🚽 Source Condition	Destination Condition	Protocol	Ethertype	Records: 1
Add Rul			Protocol Any	Ethertype Any	
Add Rul	Source Condition	Destination Condition			Action
Add Rul	Source Condition	Destination Condition			Action
	Source Condition	Destination Condition			Action

Figure 2-53 VNMC Add Policy Dialog Box

- **Step 10** Click **OK** in the Add Policy dialog box.
- Step 11 Click OK in the Add Policy Set dialog box. The newly created policy is displayed in the Assigned: field. See Figure 2-54.

Figure 2-54

## Send document comments to vsg-docfeedback@cisco.com

Add Policy Set Dialog Box

📥 Add						□ ×
Auu Auu						· · ·
Add Pol	icy Set					0
General						
Name:	PS_web					
Description:						
Policies: 🚺	🛨 Add Policy 🛛 🗒	Edit				
	Available :		Assigned :			
			<b>王</b> 十	÷ ±		
	default		pol_web			
		>>				
		>				
		<				
		*				
					OK	Cancel

**Step 12** Click **OK** in the Add Policy Set dialog box.

**Step 13** Click **Save** in the Security Profile window. See Figure 2-55.

Task 10—On the Cisco VSG, Verifying the Permit-All Rule

#### Send document comments to vsg-docfeedback@cisco.com

Figure 2-55

Cisco Virtual Network Management Center—Policy Management Window

sco Virtual Network Man	agement Center				(acron) Prefers	arcas	v: Alcovi	lleg
encin: Monacomenti III. Roscenco Manciapir e	Policy Management	Administration						
uilly Pulicies Device Configurations Capat	il ties Diagnostics							
• ICO.	🙁 roc: 🕨 🙏 Tenani-A	🕨 💼 Sceurity Profiles 🕨						
- 📴 Security Partiles	sp-web							
- 🏠 Atkanced	General Phianles Pres	łs						
-A Tenario				-				
w- 🗾 Feaulty Profiles	Name: 53-6	1979						
S sp-web	Descriptions							
In - 🚱 Advancer	Holloy sets 🖬	_web	<ul> <li>Acti Policy Sct</li> </ul>					
		olved Policy Set: 30-rco/s						
		avera runny ave.						
	Resolved Policies							
	Chowsig Policy		*				Pecarite	1
	Name	Source Condition	Destination Condition	Protocol	Ethertype	Action	Description	
	ien_hq ≌ ∢							
								_
								_
						1	The Re	s at
L' Il Cicleo Bystema, Ine. All rights reperced.								

# Task 10—On the Cisco VSG, Verifying the Permit-All Rule

To verify the rule presence in the Cisco VSG, use the Cisco VSG CLI and the show commands.

#### PROCEDURE

```
Step 1
        Log in to the Cisco VSG and enter the following commands:
        vsg# show running-config | begin security
        security-profile default@root
          policy default@root
          custom-attribute vnsporg "root"
        security-profile sp-web@root/Tenant-A
          policy PS_web@root/Tenant-A
          custom-attribute vnsporg "root/Tenant-A"
        rule default/default-rule@root
          action 10 drop
        rule pol_web/permit-all@root/Tenant-A
          action 10 log
          action 11 permit
        policy default@root
          rule default/default-rule@root order 2
        policy PS_web@root/Tenant-A
          rule pol_web/permit-all@root/Tenant-A order 101
```

Cisco Virtual Security Gateway, Rel. 4.2(1)VSG1(2) and Cisco Virtual Network Management Center, Rel. 1.2 Installation and Upgrade Guide

# Task 11—Enabling Logging

This section includes the following topics:

- Enabling Logging Level 6 for Policy-Engine Logging, page 2-52
- Enabling Global Policy-Engine Logging, page 2-55

## **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 sesson.

#### PROCEDURE

**Step 1** Log in to the Cisco VNMC.

**Step 2** Choose **Policy Management > Device Configurations**. See Figure 2-56.

Figure 2-56 Cisco Virtual Network Management Center—Device Configurations Window

cisco Virtual Network Management Center	(ninin)	Preferences		Help
Tenant Management I. Resource Management Pulicy Management I. Administration				
Security Policies Device Configurations, Capabilities Diagnostics				
root root root root root Beginted States and the second states and				

**Step 3** From the left pane navigation tree, choose **root** > **Advanced** > **Device Policies** > **Syslog**.

**Step 4** From the Syslog panel on the right, choose **Default** and click **Edit**.

## Send document comments to vsg-docfeedback@cisco.com

#### Figure 2-57

Cisco Virtual Network Management Center Syslog Pane Edit Syslog Dialog Box

Tenant Management   Resource Managem	ent Policy Management   Administration			
ecurity Policies Device Configurations Capa	bilities Diagnostics			
r 🝚 raat	😤 cost 🕨 🏟 Astrancest 🕨 🇯 Dennce Policies 🕨			
🕨 🏈 Device Profiles	Syslog			
🔻 🎡 Advanced	General Faults			
👻 🎬 Device Policies	🗄 Add Systog 🛛 🚟 Edit 👘 Delete			Records:
- S Core File	Name	Part	De	escription
Fault	default	514	Syslog Service	
<ul> <li>S Log File</li> <li>S SNMP</li> </ul>	+ Edit System		<b>C</b> ×	
<ul> <li>System</li> </ul>				
S default	Edit (default)		•	
► A Tenant-A	General Servers Local Destinations Events			
	Name: defaut			
	Description: Syslog Senice			
	Port: 614			
		<u>ок</u>	Apply Cancel	

**Step 5** Click on **Servers** tab. See Figure 2-58.



🕂 Add Syslog S	erver   🔀 Edit 👔	🕆 Delete			Records: 3
Server Type 1 🔺	Hostname	Admin State	Severity	Forwar	ding Facility
primary	none	disabled	critical (2)	localO	
econdary	none	disabled	critical (2)	local0	
ertiary	none	disabled	critical (2)	local0	

**Step 6** From the **Server Type** column, choose the primary server type from the displayed list and from the pane toolbar, click **Edit**. See Figure 2-59.

#### Figure 2-59

Edit Syslog Server Dialog Box

👗 Edit Syslog Server		<b>×</b>
Edit (primary	/)	0
General Events		
Server Type:	primary 👻	
Hostname / IP Address:	10.193.77.25	
Severity:	information (6)	
Forwarding Facility:	local0	
Admin State:	disabled  disabled enabled	
	ОКС	ancel

Step 7 In the Hostname/IP address field, enter the syslog server IP address.

Step 8 From the Severity drop-down list, choose **Information(6)**.

- From the Admin State drop-down list, choose Enabled. Step 9
- Click OK. Step 10

Figure 2-60 E	dit Syslog	Dialog Box
---------------	------------	------------

Edit (de					
+ Add Syslog 8	Local Destinations Eve Server 🛛 🖽 Edit	ents 🕆 Delete			Records: 3
Server Type	Hostname	Admin State	Severity	Forward	ling Facility
orimary	10.193.77.25	disabled	information (6)	local0	
secondary	none	disabled	critical (2)	local0	
ertiary	none	disabled	critical (2)	local0	

### Send document comments to vsg-docfeedback@cisco.com

Step 11 Click OK.

# **Enabling Global 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 global policy-engine logging.

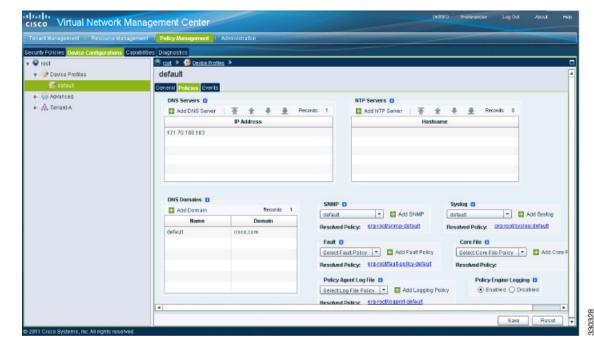
#### PROCEDURE

Step 1 Log in to the Cisco VNMC and choose Policy Management > Device Configurations > root > Device Profiles > default.

The Cisco VNMC Policy Management window opens.

**Step 2** In the Device Profiles pane, choose **Policies**. See Figure 2-61.





**Step 3** In the Policy Engine Logging area at the bottom of the pane, click **Enabled**.

**Step 4** Click **Save** to save the configuration.

# Task 12—Enabling the Traffic VM's Port-Profile for Firewall Protection and Verifying the Communication Between the VSM, VEM, and VSG

This section includes the following topics:

- Enabling Traffic VM's Port-Profile for Firewall Protection, page 2-56
- Verifying the VSM/VEM for Cisco VSG Reachability, page 2-56
- Checking the VM Veth Port for Firewall Protection, page 2-57

#### **BEFORE YOU BEGIN**

Make sure you have the following:

- Cisco VSG data IP (10.10.10.200) and VLAN ID (100)
- Security profile name (for example, sp-web)
- Organization (Org) name (for example, root/Tenant-A)
- The port-profile that you would like to edit to enable firewall protection

## **Enabling Traffic VM's Port-Profile for Firewall Protection**

This example shows the traffic VM port profile before firewall protection:

```
port-profile type vethernet pp-webserver
vmware port-group
switchport mode access
switchport access vlan 3770
no shutdown
state enabled
```

This example shows how to enable firewall protection:

```
vsm(config)# port-profile pp-webserver
vsm(config-port-prof)# vn-service ip-address 10.10.10.200 vlan 100 security-profile sp-web
vsm(config-port-prof)# org root/Tenant-A
```

This example shows the traffic VM port profile after firewall protection:

```
port-profile type vethernet pp-webserver
vmware port-group
switchport mode access
switchport access vlan 3770
vn-service ip-address 10.10.10.200 vlan 100 security-profile sp-web
org root/Tenant-A
no shutdown
state enabled
```

## Verifying the VSM/VEM for Cisco VSG Reachability

This example show how to verify VEM/VSG communication:

```
vsm# show vsn brief
```

Chapter 2 Quick Start Guide for the Cisco Virtual Security Gateway and the Cisco Virtual Network Management

Task 13—Sending Traffic Flow and on the Cisco VSG Verifying Statistics and Logs

#### Send document comments to vsg-docfeedback@cisco.com

```
VLAN IP-ADDR MAC-ADDR FAIL-MODE STATE MODULE
100 10.10.10.200 00:50:56:83:00:46 Close Up 3
vsm#
```

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

## Checking the VM Veth Port for Firewall Protection

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

```
vsm# show vsn port vethernet16
Veth
                : Veth16
VM Name
                : sg-allrun-centos2
VM uuid
                : 42 03 d1 ab 29 20 fd 01-57 89 80 1a 6f fe 04 8b
DV Port
                : 2112
DVS unid
                : 40 f2 03 50 4b b3 50 eb-2e 13 bc 0c 82 ee 54 58
                : 0x148
Flags
VSN Data IP
               : 10.10.10.200
Security Profile : sp-web
Org
               : root/Tenant-A
VNSP id
                : 2
IP addresses:
    172.31.2.92
```

Note

Make sure that your VNSP ID value is more than 1.

# Task 13—Sending Traffic Flow and on the Cisco VSG Verifying Statistics and Logs

This section includes the following topics:

- Sending Traffic Flow, page 2-57
- On the Cisco VSG, Verifying Policy-Engine Statistics and Logs, page 2-59

## **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. See Figure 2-62.

Task 13—Sending Traffic Flow and on the Cisco VSG Verifying Statistics and Logs

## Send document comments to vsg-docfeedback@cisco.com

#### Figure 2-62

2 Virtual Machine Properties Window

	x_Server - ¥irtual Machine P	roperties	
Hardwa	re Options Resources		Virtual Machine Version: 7
E sh	ow All Devices	Add Remove	Device Status
101 011	- a Devices		Connected
Hardwa	are	Summary	Connect at power on
MIK M	lemory	1024 MB	Adaptas Tura
🔲 🤇	PUs	1	Adapter Type
🖳 V	ideo card	Video card	Current adapter: E1000
	MCI device	Restricted	
🌀 s	CSI controller 0	LSI Logic Parallel	MAC Address
😀 Н	lard disk 1	Virtual Disk	00:50:56:83:00:62
💁 c	D/DVD Drive 1	Client Device	C Automatic C Manual
19 N	etwork adapter 2 (edite	pp-webserver (Nexu	
			Network label: pp-webserver (Nexus1000V) Port: 288 Switch to advanced settings
He	lp		OK Cancel

Step 2 Log in to any of your client VM (Client-VM) and send traffic (for example, HTTP) to your Server-VM.

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

Task 13—Sending Traffic Flow and on the Cisco VSG Verifying Statistics and Logs

### Send document comments to vsg-docfeedback@cisco.com

# **On the Cisco VSG, Verifying Policy-Engine Statistics and Logs**

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:

<pre>vsg# show policy-engine stat Policy Match Stats:</pre>	S	
default@root	:	0
default/default-rule@root	:	0 (Drop)
NOT_APPLICABLE	:	0 (Drop)
PS_web@root/Tenant-A : pol_web/permit-all@root/Te NOT_APPLICABLE	1 nant-A : :	1 (Log, Permit) 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 Task 13—Sending Traffic Flow and on the Cisco VSG Verifying Statistics and Logs

Send document comments to vsg-docfeedback@cisco.com