

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, page 1
- Task 1: Installing the Cisco VNMC from an OVA Template, page 7
- Task 2: On the Cisco VNMC, Setting Up VM-Mgr for vCenter Connectivity, page 16
- Task 3: On the VSM, Configuring the Cisco VNMC Policy Agent, page 21
- Task 4: On the VSM, Preparing Cisco VSG Port Profiles, page 22
- Task 5: Installing the Cisco VSG from an OVA Template, page 24
- Task 6: On the Cisco VSG and Cisco VNMC, Verifying the VNM Policy-Agent Status, page 31
- Task 7: On the Cisco VNMC, Configuring a Tenant, Security Profile, and Compute Firewall, page 32
- Task 8: On the Cisco VNMC, Assigning the Cisco VSG to the Compute Firewall, page 38
- Task 9: On the Cisco VNMC, Configuring a Permit-All Rule, page 40
- Task 10: On the Cisco VSG, Verifying the Permit-All Rule, page 43
- Task 11: Enabling Logging, page 43
- Task12: Enabling the Traffic VM Port-Profile for Firewall Protection and Verifying the Communication Between the VSM, VEM, and VSG, page 47
- Task13: Sending Traffic Flow and on the Cisco VSG Verifying Statistics and Logs, page 49

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/ps13095/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.

Туре	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	

Туре	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	Make sure that you know the following:		
an OVA Template, on page 7	• 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	Make sure that you know the following:		
VM-Mgr for vCenter Connectivity, on page 16	Install Adobe Flash Player (Version 10.1.102.64)		
r	• IP address of the Cisco VNMC		
	Admin user password		

Cisco VSG for VMware vSphere, Release 4.2(1)VSG2(1.1) and Cisco VNMC, Release 2.1 Installation and Upgrade Guide

	es de la companya de	
Make sure the	hat you know the following:	
	isco VNMC policy-agent image is available on the (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		
	P connectivity between the VSM and the Cisco C 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.	
Make sure t	hat 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 m	anagement VLAN (management).	
Note	None of these VLANs need to be system VLANs.	
	 The Cive VSM (Note) Note The IP The sh VNM(O) That II VNM(O) Note Make sure times the sure time of the sure times times the sure times the	

Tasks	Prerequisites		
Task 5: Installing the Cisco VSG from an	Make sure that you know the following:		
OVA Template, on page 24	• 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.2.1.1b.bin) is available.		
Task 6: On the Cisco VSG and Cisco VNMC, Verifying the VNM Policy-Agent Status, on page 31			
Task 7: On the Cisco VNMC, Configuring	Make sure that you know the following:		
a Tenant, Security Profile, and Compute Firewall, on page 32	• 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 38			
Task 9: On the Cisco VNMC, Configuring a Permit-All Rule, on page 40	—		

Tasks	Prerequisites
Task 10: On the Cisco VSG, Verifying the Permit-All Rule, on page 43	—
Task 11: Enabling Logging, on page 43	
Task12: Enabling the Traffic VM Port-Profile for Firewall Protection and Verifying the Communication Between the VSM, VEM, and VSG, on page 47	 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 49	

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/ps13095/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:

OL-29526-01

- 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).

SUMMARY STEPS

- 1. Choose the host on which to deploy the Cisco VNMC VM.
- 2. Choose File > Deploy OVF Template.
- **3.** In the **Source** window, do the following:
- 4. In the OVF Template Details window, review the details of the Cisco VNMC template and click Next.
- 5. In the End User License Agreement window, do the following:
- 6. In the Name and Location window, do the following:
- 7. In the Deployment Configuration window, do the following:
- 8. In the Datastore window, choose the datastore for the VM and click Next.
- **9.** In the **Disk Format** window, do the following:
- 10. In the Network Mapping window, do the following:
- 11. In the Properties window, do the following:
- 12. Click Next.
- 13. In the Ready to Complete window, review the deployment settings information and click Finish.
- 14. Click Close.
- 15. Power on the Cisco VSG VM.

Cisco VSG for VMware vSphere, Release 4.2(1)VSG2(1.1) and Cisco VNMC, Release 2.1 Installation and Upgrade

DETAILED STEPS

- **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

Deploy OVF Template Source Select the source location.		
Source OVF Template Details Name and Location Datastore Disk Format Ready to Complete	Deploy from a file or URL C:\tmp\vnnc:1.0.0.502.ova Image: 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.	
Help	≤Back Next ≥	Cancel

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

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

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.

Cisco VSG for VMware vSphere, Release 4.2(1)VSG2(1.1) and Cisco VNMC, Release 2.1 Installation and Upgrade Guide

b) Click Next.

Figure 3: Deploy OVF Template–Name and Location

itual Network Management Center e name can contain up to 80 characters and it must be unique within the in	
e name can contain up to 80 characters and it must be unique within the ir	
	wentory folder.
Barber	
11	SGI-DC1

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 8In 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.

🛃 Deploy OVF Template _ 🗆 × Disk Format In which format do you want to store the virtual disks? Source Information about the selected datastore: OVF Template Details Name: Storage1 (1) End User License Agreement 464.5 GB Capacity: Name and Location Free space: 410.8 GB Deployment Configuration Select a format in which to store the virtual machines virtual disks: Datastore Disk Format Thin provisioned format Network Mapping 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. Properties Ready to Complete Estimated disk usage: 3.8 GB C Thick provisioned format All storage is allocated immediately. Estimated disk usage: 20.0 GB Help ≤ Back Next ≥ Cancel

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.

Cisco VSG for VMware vSphere, Release 4.2(1)VSG2(1.1) and Cisco VNMC, Release 2.1 Installation and Upgrade

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.

Source DVF Template Details End User License Agreement Vame and Location Deployment Configuration Datastore Disk Format Vetwork Mapping Properties Ready to Complete	a. IP Address IPv4 Enter the VM IP in the following form: 192.168.0.10 D. 193 . 75 . 95 b. IP Netmask Netmask Enter the Subnet Mask in the following form: 255.255.255.0 255 . 255 . 248 . 0 c. Gateway IPv4Gateway	×
	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.	•

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

Deploy OVF Template		
Properties Customize the software solu	ion for this deployment.	
Source OVF Template Details End User License Agreement Name and Location Deployment Configuration Datastore Disk Format Network Mapping Properties Ready to Complete	a. IP Address IPv4 Enter the VM IP in the following form: 192.168.0.10 III . 193 . 75 . 95 b. IP Netmask Netmask Enter the Subnet Mask in the following form: 255.255.255.0 255 . 255 . 248 . 0	
	C. Gateway IPv4Gateway 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.	×
Help	≤Back Next ≥	Cancel

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

Are these the options you	u want to use?		
iource DVF Template Details	When you click Finish, the d	eployment task will be started.	
and User License Agreement	Deployment settings:		
Name and Location Deployment Configuration Datastore	OVF file: Download size: Size on disk: Name:	C:\tmp\vnmc.1.0.0.502.ova 463.8 MB 1.7 GB Virtual Network Management Center	
<u>Disk Format</u> Network Mapping Properties	Folder: Deployment Configuration: Host/Cluster:	SG1-DC1	
Ready to Complete	Datastore: Disk Format:	Storage1 (1) Thin Provisioning	
	Estimated disk usage: Network Mapping: IP Allocation:	1.7 GB "VM Network" to "Management" Fixed, IPv4	
	Property: Property:	IPv4 = 10.193.75.95 Netmask = 255.255.248.0	
	Property: Property: Property:	IPv4Gateway = 10.193.72.1 Hostname = VNMC Domainname = example.com	
	Property: Property:	DNS = 203.0.113.1 Password = Example_Password123	
	Property: Property: Property:	Secret = Example_Secret123 RestoreProto = scp RestoreIP = 0.0.0.0	
	Property: Property:	Restore File = ignore Restore Liser = ignore	_

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 16
- Registering the vCenter Extension Plugin in the vCenter, on page 18
- Configuring the vCenter in VM-Manager in the Cisco VNMC, on page 20

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

SUMMARY STEPS

- 1. To access the Cisco VNMC from your client machine, open Internet Explorer and access https://vnmc-ip/ (https://xxx.xxx.xxx).
- 2. In the Website Security Certificate window, choose Continue to this website.
- **3.** In the **Cisco VNMC Access** window, do the following:
- 4. In the VNMC Main window, choose Administration > VM Managers.
- 5. In the Cisco Virtual Network Management Center VM Managers window, do the following:

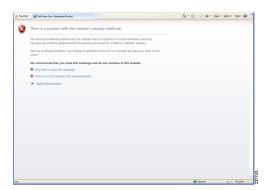
Cisco VSG for VMware vSphere, Release 4.2(1)VSG2(1.1) and Cisco VNMC, Release 2.1 Installation and Upgrade

DETAILED STEPS

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

Unite Virtual Network Mana	gement Center	(edmin)	Preferences	Log Out	About	Help
Tenant Management Resource Management	T Policy Management I Administration			-		
ccess Control Bervice Registry VNWC Profile 🚺	Managers Diagnostics Operations					
VM Managers Control Manager Control Ma	VM Managers Properties Extension Key: Cleso_VM_Manager_1799399272 Extension File Status: success Extension File Status: success Extension File Status Reason: VCenter Extension file is required to establish secure connection between vCenter and VM-Manager. Export the extension file by closing "Export vCenter Extension" and install it as plugin on all the vCenter servers.	bbA 3	VM Manager	Export vC	enter Eidens	lan
2011 Cisco Systems, Inc. All rights reserved.						

The VNMC main window opens.

- Step 4In 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 18.

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 16.

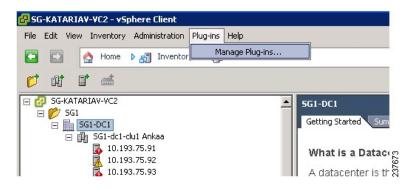
SUMMARY STEPS

- **1.** From vSphere client, log in to vCenter.
- 2. In the Vsphere Client window, choose Plug-ins > Manage Plug-ins.
- 3. Right-click in an empty space, and choose New Plug-in from the drop-down list.
- 4. In the Register Plug-in window, do the following:
- 5. On the Register Plug-in progress indicator, click OK after the successful registration message appears.
- 6. Click Close.

DETAILED STEPS

Step 1 From vSphere client, log in to vCenter.

Figure 10: vSphere Client Directory Window

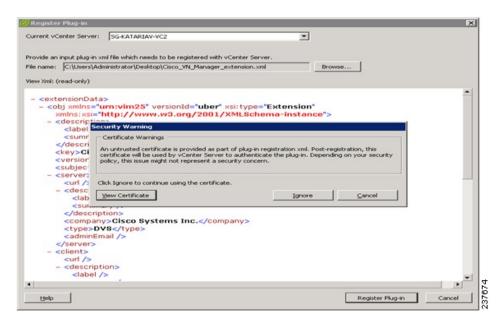


The vSphere Client Directory window opens.

- 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 20.

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 16.

SUMMARY STEPS

- 1. Go to the Cisco VNMC and click Administration > VM Managers.
- 2. In the Cisco Virtual Network Management Center window, click the VM Manager tab.
- **3.** In the left pane, choose Vm Manager > Add VM Manager.
- 4. In the Add VM Manager dialog box do the following:
- 5. Click OK.

DETAILED STEPS

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



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.

SUMMARY STEPS

- **1.** On the VSM, enter the following commands:
- 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:

DETAILED STEPS

```
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).



• None of these VLANs need to be system VLANs.

SUMMARY STEPS

- 1. On the VSM, create the VLANs by first entering global configuration mode using the following command:
- 2. Enter the following configuration commands:
- 3. Press Ctrl-Z to exit.
- **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.
- 5. Enter the following configuration commands:
- 6. Press Ctrl-Z to end the session.
- 7. Enable the Cisco VSG-ha port profile configuration mode.
- 8. Enter the following configuration commands:
- **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.
- **10.** Enter the following configuration commands:
- 11. Press Ctrl-Z to end the session.

DETAILED STEPS

 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(config) # exit
    vsm(config) # exit
    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.
- 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) # 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** Press Ctrl-Z to end the session.
- **Step 7** Enable the Cisco VSG-ha port profile configuration mode.
- 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) # 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.
- 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.2.1.1b.bin) is available.

SUMMARY STEPS

- 1. Choose the host on which to deploy the Cisco VSG VM.
- 2. Choose File > Deploy OVF Template.
- 3. In the Deploy OVF Template—Source window, do the following:
- 4. In the **Deploy OVF Template—OVF Template Details** window, review the product information including the size of the file and the VM disk.
- 5. Click Next.
- 6. In the Deploy OVF Template—End User License Agreement window, do the following:
- 7. In the Deploy OVF Template—Name and Location window, do the following:
- 8. In the **Deploy OVF Template—Deployment Configuration** window, do the following:
- **9.** In the **Deploy OVF Template—Datastore** window, choose the data store for the VM and click **Next**. The **Disk Format** window opens.
- 10. In the Deploy OVF Template—Disk Format window, do the following:
- 11. In the Deploy OVF Template-Network Mapping window, do the following:
- 12. In the Deploy OVF Template—Properties window, do the following:
- 13. Click Next. The Ready to Complete window opens.
- 14. In the Ready to Complete window, review the deployment settings information .
- 15. Click Finish. The Deploying Nexus 1000VSG dialog box opens.
- 16. Wait and click Close after the progress indicator shows that the deployment is completed successfully.
- 17. From your virtual machines, do one of the following:
- 18. In the Virtual Machine Properties window, do the following:
- 19. Power on the Cisco VSG VM.

DETAILED STEPS

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.

Cisco VSG for VMware vSphere, Release 4.2(1)VSG2(1.1) and Cisco VNMC, Release 2.1 Installation and Upgrade Guide

c) Click Next. The Deployment Configuration window opens.

Figure 12: Deploy OVF Template—Deployment Configuration Windov
--

🚰 Deploy O¥F Template		
Deployment Configuration		
Select a deployment configur	ration.	
Source		
OVF Template Details	Configuration:	
End User License Agreement Name and Location		
Deployment Configuration	Deploy medium VSG Deploy small VSG	
Storage	Deploy medium VSG edium Nexus 1000VSG	
Disk Format	Deploy large VSG	
Network Mapping Properties	2 GB memory	
Ready to Complete	1 virtual CPU (1.5 GHz)	
• •		
Help	< Back Next > Car	ncel

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

- a) From the **Configuration** drop-down list, choose **Deploy medium VSG**.
- 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

<u>purce</u> VF Template Details	Map the networks used in this OVF	template to networks in your inventory
nd User License Agreemen ame and Location		Destination Networks
eployment Configuration		
esource Pool	Data Management	VSG-Data Management
atastore	HA	VSG-HA
eady to Complete	Description:	
	Provides HA connectivity between	the Nexus 1000VSG primary and secondary. Please associate it Add to the "ha vlan" configured in the VSG.

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.

Cisco VSG for VMware vSphere, Release 4.2(1)VSG2(1.1) and Cisco VNMC, Release 2.1 Installation and Upgrade

Figure 14: Deploy OVF Template—Properties Window

Customize the software solut	ion for this deployment.	
Source OVE Template Details End User License Agreement Name and Location Deployment Configuration Host / Cluster Storage Disk Format Network Mapping Properties Ready to Complete	OVF Deployment OvfDeployment Based on the deployment, determine use of the OVF properties. Select "ignore" if manual installation is desired and disregard below options; otherwise, choose ovf and complete the property section below. vf HA Role HA Role HA Role. For secondary role, only fill out a-b below. standalone a. VSG HA ID HAid Enter the HA ID (1-4095). 1	
	b. Nexus 1000VSG Admin User Password Password Enter the password. Must contain at least one capital, one lowercase, one number. Enter password ************************************	•

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

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

- j) 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.

Cisco VSG for VMware vSphere, Release 4.2(1)VSG2(1.1) and Cisco VNMC, Release 2.1 Installation and Upgrade

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).

SUMMARY STEPS

- **1.** Log in to the Cisco VSG.
- 2. Check the status of VNM-PA configuration by entering the following command:
- 3. Log in to the Cisco VNMC. The VNMC Administration on Service Registry window opens.
- 4. Choose Administration > Service Registry > Clients > General.
- **5.** In the **Client** pane of the **VNMC Administration Service Registry** window, verify that the Cisco VSG and VSM information is listed.

DETAILED STEPS

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.

Figuro	15. VNMC	Administration	Sarvica	Ronistr	Window
riyure	IJ. VIVIVIG	Aummisuauom	Service	neyısu	

ant Management Resource Mar	agement Policy Nanagement Administ	ration					
s Control Service Registry VNMC	Profile VM Nanagers Diagnostics Operations						
Diagnostics							
Registry VNCM-favid	Clients						
Controllers	General Events						
Providers							Records:
Cilents	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-WVSW	managed-endport	10.193.75.89	registered	2010-11-26 00	1.0(0,477)
	1						

- **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 33
- Configuring a Security Profile on the Cisco VNMC, on page 35
- Configuring a Compute Firewall on the Cisco VNMC, on page 36

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

SUMMARY STEPS

- 1. For Cisco VNMC access, from your client machine, open Internet Explorer and access https://vnmc-ip/ (https://xxx.xxx.xxx).
- 2. In the Website Security Certification window, click Continue to this website.
- 3. In the Cisco VNMC Access window, log in to the Cisco VNMC:
- 4. In the Cisco VNMC main window, choose Administration > Service Registry > Clients to check the Cisco VSG and VSM registration in the Cisco VNMC.

DETAILED STEPS

Step 1 For Cisco VNMC access, from your client machine, open Internet Explorer and access https://vnmc-ip/ (https://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 33

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.

SUMMARY STEPS

- 1. From the Cisco VNMC toolbar, click the Tenant Management tab.
- 2. In the Navigation pane directory tree, right-click on **root**, and from the drop-down list, choose **Create Tenant**.
- 3. In the root pane, click the General tab and do the following:
- 4. Click OK.

DETAILED STEPS

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

Figure 16: VNMC Window Tenant Management Tab root Pane

igement Center	(adhin) Preference	s Log Out About Hel
root Fouri Sub-Coments Fauts Events Properties Name: root Description: Lovet: 0		Create Tenant
	Int i Policy Management Administration	Int i Policy Management Administration

- **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.

Guide

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

Cisco VSG for VMware vSphere, Release 4.2(1)VSG2(1.1) and Cisco VNMC, Release 2.1 Installation and Upgrade

What to Do Next

Go to Configuring a Security Profile on the Cisco VNMC, on page 35

Configuring a Security Profile on the Cisco VNMC

You can configure a security profile on the Cisco VNMC.

SUMMARY STEPS

- 1. Click the Policy Management tab in the Cisco VNMC toolbar. The Policy Management window opens.
- In the Policy Management Security Policies window, from the directory path, choose Security Policies
 root > Tenant-A > Security Profiles.
- 3. Right click in an empty space and choose Add Security Profile from the drop-down list.
- 4. In the Add Security Profile dialog box, do the following:
- 5. Click OK

DETAILED STEPS

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

Figure 17: Security Policies root Window

Usco Virtual Network Man	igement Center	(adhiki)	Preferences	Log Out	About	Help
Tenant Management Resource Manageme	t - 1 Policy Management 1 Administration					
ecurity Policies Device Configurations Capab	ites Diagnostics					
r 🗣 root						C
 Security Profiles 	root					
 Advanced 	General Sub-Elements Faults Events					
🔹 \Lambda Tenant-A	Properties					
Security Profiles	Name: root					
Mag Ad Security Profile	Description:					

- Step 2 In the Policy Management Security Policies window, from the directory path, choose Security Policies > root > Tenant-A > Security Profiles.
- Step 3Right click in an empty space and choose Add Security Profile from the drop-down list.
The Add Security Profile dialog box opens.



Add Security Profile Attibutes Name: \$p-web Description: Policy set: Belect Policy Set Belect Policy Set: Image: Add Policy Set Resolved Policy Set: Image: Add Policy Set Image: Policy Set: Image: Source Condition Policy Set: Image: Source Condition Image: Policy Image: Source Condition Image: Source Condition Image: Policy Image: Policy Image: Policy Image: Policy Image: Policy Image: Policy Image: Policy Image:							del
Name: \$	0					ty Profile	d Securi
Policy set: Select Policy Set: S							Attributes
escription: Policy Set: Belect Policy Set Corp.root/pasel-default soolwed Policies (Un)assign Policy Source Condition Destination Condition Protocol Ethertype Action						eb	Name: Sp-We
Policy set: Select Policy Set Add Policy Set Resolved Policy Set: org-root/pasel-default (Un)assign Policy The Source Condition Name Source Condition Destination Condition							Numo.
Select Policy Set Image: Contraction Condition Protocol Ethertype Action Name Source Condition Destination Condition Protocol Ethertype Action							Policy set: D
Solved Policies 1 (Un)assign Policy The second sec							Sele
(Un)assign Policy The second seco					et-default	wed Policy Set: 0ra-root/p:	Reso
(Un)assign Policy The second seco							solved Policies
	Records: 1				Ł	11 至 余 平 3	
a default	Description	Action	Ethertype	Protocol	Destination Condition	Source Condition	
							default
OF							

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 36

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.

Cisco VSG for VMware vSphere, Release 4.2(1)VSG2(1.1) and Cisco VNMC, Release 2.1 Installation and Upgrade

36

SUMMARY STEPS

- 1. From the Cisco VNMC, choose Resource Management > Managed Resources.
- 2. On the left-pane directory tree, choose root > Tenant-A > Compute Firewall.
- 3. From the drop-down list, choose Add Compute Firewall. The Add Compute Firewall dialog box opens.
- 4. In the Add Compute Firewall dialog box, do the following:
- 5. Click OK.

DETAILED STEPS

 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

	inagement Center		Preferences	Log Out	Abold	
art Management Resource Manage	ment T Policy Management I Administration	_	_			
ged Resources Resources Capabilite:	s Diagnestics					
Intual Security Gateways Proof © Compute Firewaits ⊕ Pools ■ TenantA ■ 100 Compute Firewaits	root General Sub-Elements Faults Events Properties Name: root Description:					
- Pools Add Com	pute Firewall					

- **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

Create			⊐ ×
Add Compute	Firewall		0
neral			
Name: CFW-VSG- Description: Config State: not-applied			
Firewall Settings Device Profile:	default	৬ Select	
Management Hostname:	firewall		
Data IP Address:	10 . 10 . 10 . 200		
Data IP Subnet:	255 . 255 . 255 . 0		
		ОК	Cancel

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.

SUMMARY STEPS

- 1. Choose Resource Management > Managed Resources. The Deploy OVF Template window opens.
- 2. In the Deploy OVF Template window, choose root > Tenant-A > Compute Firewalls.
- 3. Right-click in the Compute Firewalls pane and choose Assign VSG from the drop-down list.
- 4. From the Name drop-down list, choose the Cisco VSG IP address.
- 5. Click OK.

DETAILED STEPS

- 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

enan: Nanacemen: 🕴 Hesource Manag	emant Folicy Management Administration		and the second se	STREET, STREET
maged Resources Pean mea Capability	es Diagonatios			
Virtual Scenity Galeways	💿 root 🕨 🙏 Tenent-A 🕨			C
 mor Gomoute Firmalis 	Compute Firewalls			
- To s	General Fault:	Auvign Pool 👌 Jacourus VSG/Pool	Ma Edit 💼 Dalaia	Rescrise: 1
	Name	Description	Device Profile	Crudiy State
🗼 🍌 Tenarità 🔹 🥳 Annoide Firewalls	CEWIVEG A			
CEONAED-6	11 ES:			
ends ≣ents	Avsign VEG			
B	🦡 Assign Poo			
	Urassign VSG/Poci			
	1 Delete			
				10.0

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

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

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.

SUMMARY STEPS

- **1.** Log in to the Cisco VSG.
- Choose Policy Management > Service Policies. The Cisco VNMC Policy Management Security Policies window opens.
- 3. In the Cisco VNMC Policy Management Security Policies, window do the following:
- 4. Click Add Policy. The Add Policy dialog box opens.
- 5. In the Add Policy dialog box, do the following:
- 6. In the Add Rule dialog box, do the following:
- 7. In the Add Policy dialog box, click OK.
- 8. In the Add Policy Set dialog box, click OK.
- 9. In the Security Profile window, click Save.

DETAILED STEPS

- **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

n.Manacement Resource Man	Cabir ent Pulley Managemo	i Administration						-
A Pulkies Device Configurations	Capabilities Diagnostics							
ICO.	🔮 roct 🕨 🥂 Tona'	I-A 🕨 🚺 Scenity Profiles 🕨						
📕 Security Partiles	sp-web							
🚳 Arkanced	General Philadas	Peents						
A Tenarità								
🐖 🌆 Feaulity Profiles	Name:	s percela						
sp-weit	Descriptions							
e- 🚱 Advancer	Policy set: U	Object Policy Oel	 Acid Pictury Sct 					
		Resolved Policy Set: 20-10020	set-default	**				
	Resolved Policie	Resolved Policy Set: 20-10026		•				
		Resolved Policy Set: 25-15825	set-default	•			Recards	: 1
	Recoived Policie	Resolved Policy Set: <u>20-5522</u> 5 8 0	And Policy to	Protocol	Fihertype	Action	Pecarde Description	
	Resolved Policie	Resolved Pelicy Set: 35:15:02 6 D Hits T T T	And Policy 5		Fiherfype	Action		
	Resolved Policie	Resolved Pelicy Set: 35:15:02 6 D Hits T T T	And Policy 5		Fitherlype	Action		
	Resolved Policie	Resolved Pelicy Set: 35:15:02 6 D Hits T T T	And Policy 5		Fitherstypes	Action		
	Resolved Policie	Resolved Pelicy Set: 35:15:02 6 D Hits T T T	And Policy 5		Fibesbype	Jacien		
	Resolved Policie	Resolved Pelicy Set: 35:15:02 6 D Hits T T T	And Policy 5		Ftherfype	Action		
	Resolved Policie	Resolved Pelicy Set: 35:15:02 6 D Hits T T T	And Policy 5		Fihedype	Action		
	Resolved Policie	Resolved Pelicy Set: 35:15:02 6 D Hits T T T	And Policy 5		Fiberbyre	Action		
	Resolved Policie	Resolved Pelicy Set: 35:15:02 6 D Hits T T T	And Policy 5		Fiberlype	Action		
	Resolved Policie	Resolved Pelicy Set: 35:15:02 6 D Hits T T T	And Policy 5		Fiherfype	Action		

- 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

lindu tisco Virtual Netw	vork Management C						
Service Profiles Service Polic		apabilities Diagnostics					
Add	A						
Add ACL Polic	у						0
General							
Name: Policy Description:							
Rule Table	+ +						Records: 0
	Match Criteria Source Cond	ition Destination Condition	Service/Protocol	EtherType	Action	Descript	
🗄 Add Rule 🏻 🕋 🎓	Match Source Cond	ition Destination Condition	Service/Protocol	EtherType	Action		
🗄 Add Rule 🏻 🕋 🎓	Match Source Cond		Service.Protocol	EtherType	Action		
🗄 Add Rule 🏻 🕋 🎓	Match Source Cond		Service/Protocol	EtherType	Action		
🗄 Add Rule 🏻 🕋 🎓	Match Source Cond		Service/Protocol	EtherType	Action		
🗄 Add Rule 🛛 🕋 🎓	Match Source Cond		Service.Protocol	Ether Type	Action	Descript	ion

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 7In 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 43
- Enabling Global Policy-Engine Logging, on page 45

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.

SUMMARY STEPS

- **1.** Log in to the Cisco VNMC.
- 2. Choose Policy Management > Device Configurations.
- 3. In the Device Configuration window, do the following:
- 4. In the Edit Syslog dialog box, do the following:
- 5. In the Edit (Primary) Syslog Server dialog box, do the following:
- 6. Click OK.

DETAILED STEPS

- **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

enart Vanagement 🔰 Resource Managemen	it Policy Management Administration		
urity Policies Device Configurations Capabil	Nes Diagnostics		
👻 raat	😌 cost 🕨 🐺 Advancest 🕨 🇯 Dences Policies 🕨		
🖡 🎯 Device Prafiles	Syslog		
🛛 🎡 Advanced	General Faults		
· Device Policies	🖬 Add Systop 🛛 👪 Edit 👚 Delete		Records: 1
- S Core File	Name	Part	Description
► S Fault ► S Log File	default	514 Systop	Service
SINMP	🚓 Edit Syslog	□ ×	
👻 🚨 Systop	Edit (default)	0	
- 🖉 default	Eun (deraun)	U	
🖌 🙏 Tenant-A	General Servers Local Destinations Events		
	Name: defaut		
	Profiles.		
	Description: Syslog Senice		
	Port: 514		
		OK Apply Cancel	

Cisco VSG for VMware vSphere, Release 4.2(1)VSG2(1.1) and Cisco VNMC, Release 2.1 Installation and Upgrade Guide

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

Figure 26: Edit Syslog Dialog Box

Edit Syslog					• ×
Edit (def	ault)				0
eneral Servers l	Local Destinations Ever	nts			
🗄 Add Syslog Se	erver 🔀 Edit 🖞	🕆 Delete			Records: 3
Server Type 1 🔺	Hostname	Admin State	Severity	Forwarding Fa	cility
orimary	none	disabled	critical (2)	localO	
secondary	none	disabled	critical (2)	local0	
ertiary	none	disabled	critical (2)	local0	

- 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 45.

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.

SUMMARY STEPS

- **1.** Log in to the Cisco VNMC.
- In the Virtual Network Management Control window, choose Policy Management > Device Configurations > Device Configurations > root > Device Profiles > default. The default Device Profile window opens.
- 3. In the default window, do the following:
- 4. Click Save.

DETAILED STEPS

Step 1 Log in to the Cisco VNMC.

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

	ment Policy Management	Administration			
ity Policies Device Configurations Cap root	Second Provide	- 5			-
- 🕜 Device Profiles	default				L L
🧟 default	General Policies Events				
 Advanced A Tenanté 	DNS Servers		NTP Servers		
► A Tenant-A	Add DNS Server	· 중 술 후 호 Rec	cords: 1 🔠 Add NTP Server 🕴	F 🛊 🖶 Records: 0	
		IP Address		Hostname	
	171.70.168.183				
	DNS Domains 🚹		SNMP 0	Syslog 🖪	
	🗄 Add Domain	Records: 1	default * El Add SNM		
	Name	Domain			-
	default	cisza.com	Resolved Policy: org-root/snmp-default	Resolved Policy: org-root/syslog-default	
	General		Fault 🛙	Core File 0	
	delaut				1 Core F
	Cerear.	and a start and a start	Select Fault Policy 🔻 📑 Add Fault	Policy Select Core File Policy 🔹 🖬 Adv	
	CONTROL 1			Policy Select Core File Policy 🔹 🖬 Adv	
	United in the second se	11110.0111	Select Fault Policy 🔻 📑 Add Fault	Policy Select Core File Policy 🔹 🖬 Adv	
		1010.0111	Select Fault Policy Add Fault Resolved Policy: 979-root/fault-policy-de	Policy Select Core File Policy	
			Select Faut Policy Add Faut Resolved Policy: Ora-root/Sulf-colloy-de Policy Agent Log File	Policy Select Core File Policy Select Core File Policy Resolved Policy: Policy Engine Legging B gging Policy Engine Legging B Core	

- 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:

Enabling Traffic VM Port-Profile for Firewall Protection, on page 47 Verifying the VSM or VEM for Cisco VSG Reachability, on page 48 Checking the VM Virtual Ethernet Port for Firewall Protection, on page 48

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.

SUMMARY STEPS

1. Verify the traffic VM port profile before firewall protection.

DETAILED STEPS

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 to Verifying the VSM or VEM for Cisco VSG Reachability, on page 48.

Verifying the VSM or VEM for Cisco VSG Reachability

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

			License Inform	ation		
Type vsg asa	In-Use-Lic-Count 4 0	UnLice	nsed-Mod		 	
			Node Informati		 	
ID Name 1 vsg1		Туре	IP-Address 40.40.40.40	Mode		
			Path Informati	 on 	 	
			Port Informati	on	 	
Org:root/	le:pp-webserver Tenant-A (40.40.40.40)		file(Id):SP_web		-Name vml	

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

Cisco VSG for VMware vSphere, Release 4.2(1)VSG2(1.1) and Cisco VNMC, Release 2.1 Installation and Upgrade

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, on page 49
- Verifying Policy-Engine Statistics and Logs on the Cisco VSG, on page 51

Sending Traffic Flow

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

SUMMARY STEPS

- **1.** Ensure that you have the VM (Server-VM) that is using the port profile (pp-webserver) configured for firewall protection.
- 2. In the Virtual Machine Properties window, do the following:
- 3. Check the policy-engine statistics and log on the Cisco VSG.

DETAILED STEPS

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

.inux_Server - Virtual Machine F dware Options Resources	roperties	Virtual Machine Version: 7
		Device Status
Show All Devices	Add Remove	Connected
rdware	Summary	Connect at power on
Memory	1024 MB	
CPUs	1	Adapter Type
Video card	Video card	Current adapter: E1000
VMCI device	Restricted	
SCSI controller 0	LSI Logic Parallel	MAC Address
Hard disk 1	Virtual Disk	00:50:56:83:00:62
CD/DVD Drive 1	Client Device	C Automatic C Manual
Network adapter 2 (edite	pp-webserver (Nexu	
		Network Connection
		Network label:
		pp-webserver (Nexus1000V)
		Port: 288
		Switch to advanced settings
		Switch to advanced settings

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 51.

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:

<pre>vsg# show policy-engine stats</pre>			
Policy Match Stats:			
default@root :	0		
<pre>default/default-rule@root :</pre>	0	(Drop)	
NOT_APPLICABLE :	0	(Drop)	
<pre>PS_web@root/Tenant-A : pol_web/permit-all@root/Tenar NOT_APPLICABLE</pre>	1 nt-A : :	1 (Log, Permit) 0 (Drop)	
<pre>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</pre>			