CHAPTER 3

Setting Up the ASA 1000V Using VNMC Mode

You must configure the ASA 1000V with Cisco VNMC information so that the ASA 1000V can connect to the Cisco VNMC. You must perform this task for both Cisco VNMC and ASDM management modes.

This section includes the following topics:

Registering the ASA 1000V with the Cisco VNMC

Prerequisites

The registration address provided for the Cisco VNMC must be reachable via the management0/0 interface. Additionally, the ASA 1000V must be able to connect to the Cisco VNMC via HTTPS.

You must synchronize the clocks on the ASA 1000V and the Cisco VNMC. You can manually synchronize the clock on the ASA 1000V by using the **clock set** command. When ASA 1000V is powered on for the first time, it gets its clock settings from the ESX/ESXi host. You can set the clock on the ESX/ESXi hosts to the correct value before starting ASA 1000V and Cisco VNMC.

Detailed Steps

Step 1 From the Hosts and Clusters view, choose the ASA 1000V instance that you deployed, and click the **Console** tab.

Step 2 Enter the following Cisco VNMC configuration on the console:

```
ASA1000V(config)# vnmc policy-agent
ASA1000V(config-vnmc-policy-agent)# registration host ip_address
```

Where *ip_address* is the IP address or hostname of the host on which the Cisco VNMC is running. The IP address may have already been provided through OVF deployment.

```
ASA1000V(config-vnmc-policy-agent)# shared-secret key
```

Where *key* is the shared secret for authentication of the ASA 1000V connection to the Cisco VNMC.

Note The IP address and shared secret you specify must match what was configured in Cisco VNMC.

Step 3 Save the configuration to startup by entering the **write mem** command.

Adding the ASA 1000V as an Edge Firewall in the Cisco VNMC

Perform this task only when configuring ASA 1000V for the VNMC management mode.

From the VMware vSphere Client, obtain the IP address that you entered for the host running the ASA 1000V VM. You set this IP address when you configured the ASA 1000V management IP address in the Deploy OVF Template wizard. See the "Deploying the ASA 1000V Using the VMware vSphere Client" section on page 2-8.

Note In the Cisco VNMC, you must have already created the tenant on which you want to associate the ASA1000V. See the Cisco VNMC documentation for instructions.

Detailed Steps

Step 1 Log into the Cisco VNMC.

Step 2 Choose **Resource Management** > **Managed Resources** > **Firewalls** > **root** > *tenant* > **Edge Firewalls**; where *tenant* is the logical entity under which you want to associate the ASA 1000V as an edge firewall.

In the Cisco VNMC, multitenancy enables the division of large physical infrastructures into logical entities. You can assign unique resources to each tenant through the related organization in the multitenant environment. See the Cisco VNMC documentation for tenant management information.

Note To perform this step, you must have at least one tenant defined in the Cisco VNMC.

Step 3 In the Edge Firewalls pane, click **Add Edge Firewall**.

The Add Edge Firewall dialog box appears.

Step 4 Name the logical edge firewall.

Step 5 Under Interfaces, click **Add Data Interface** to add the inside and outside data interfaces for the logical edge firewall. For the outside interface, enable and select an edge profile that applies to all traffic coming in and going out of the outside interface. For the inside interface, there is no need for an edge profile. See the Cisco VNMC documentation for data interface information.

Step 6 Click **OK** to close the Add Data Interfaces dialog box and save the interface.

The ASA 1000V edge firewall instance appears in the right pane under the ASA 1000V tenant.

Step 7 Enable and select a device profile if required in the Firewall Settings pane.

Step 8 Enable and select an edge device profile, if required, in the Firewall Settings pane.

Step 9 In the left pane, select the logical edge firewall you have added, and click **Assign ASA 1000V** in the right pane.

The Assign ASA 1000V dialog box appears.

Step 10 Choose the Virtual-ASA Management IP address from the drop-down list, then click **OK**.

The IP address appears in the drop-down list because you entered the ASA 1000V **vnmc policy-agent** command in the "Registering the ASA 1000V with the Cisco VNMC" section on page 3-1. You must set the virtual ASA management IP address to specify under which tenant to deploy the ASA 1000V.

Step 11 (Recommended) Verify that the ASA 1000V is configured to communicate with the Cisco VNMC by selecting the logical edge firewall instance in the left pane, then from the General tab, check these fields for the following values:

- Config State: applied
- Association Status: associated
- Reachable: yes

Verify that the Operational State is OK by clicking the Task link in the right-hand side under ASA 1000V Details, then click the **General** tab.

Configuring Security Profiles in VSM

For each port profile in the VSM, you configure a vservice that determines which ASA 1000V the Cisco Nexus 1000V switch uses for that port profile and which edge security profile to apply to all the VMs that belong to the port profile. The Cisco VNMC generates a unique security profile ID (SPID) for each edge security profile. The VEM determines which edge security profile to apply for a given packet based on the port profile configuration.

The vservice configured for a port profile controls which SPID to use and to which ASA 1000V to forward packets. The ASA 1000V uses the SPID in the packet to know which policies to apply to the packet.

Detailed Steps

Step 1 Log into the VMware vSphere Client.

Step 2 Choose the VSM from the Hosts and Clusters view, then click the **Console** tab. The VSM is the control software for the Cisco Nexus 1000V.

The VSM is also deployed as a VM.

Step 3 Match the IP address of the inside interface for the ASA 1000V with the IP address configured on the VSM for the vservice of the port profiles. Match these IP addresses by entering the following commands in configuration mode:

```
switch(config)# vservice node vservice_name type asa
```

Where *vservice_name* is the name of the ASA 1000V.

```
switch(config)# ip address inside_interface_ip_address
```

Where *inside_interface_ip_address* is the inside IP address of the ASA 1000V.

These IP addresses must match so that packets are correctly forwarded to the ASA 1000V by the Cisco Nexus 1000V.

Step 4 Set up the VLAN on which the ASA 1000V's inside interface is connected by entering the following command:

```
switch(config)# adjacency l2 vlan vlan_number
```

Where *vlan_number* is the VLAN of the ASA 1000V inside interface.

Because the ASA 1000V is the default gateway for the inside VMs, it is connected to the same VLAN as the VMs.

Note For VXLAN, provide VXLAN information instead of VLAN information. See the following guide:
Cisco Nexus 1000V VXLAN Configuration Guide

Step 5 Create a port profile for the VMs and attach the vservice to the port profile by entering the following commands:

```
switch(config)# port-profile type vethernet port_profile_name
switch(config-port-prof)# vservice node vservice_name profile edge_profile_name
switch(config-port-prof)# org org_path
```

Where *edge_profile_name* is the name of the edge security profile created in the Cisco VNMC and *org_path* is the organization hierarchy in the Cisco VNMC in which ASA 1000V is created; for example, root/tenant1/datacenter1.

Note When installing the Nexus 1000V, you created port profiles for the four ASA 1000V interfaces: inside, outside, management, and high availability (failover). For detailed information, see the "Predeployment Task Flow" section on page 1-11 in Step 5.

For more information about configuring port profiles, see the Cisco Nexus 1000V documentation:

Cisco Nexus 1000V Port Profiles Configuration Guide

For more information about the organization in the Cisco VNMC, see the Cisco VNMC documentation:

- Cisco VNMC CLI Configuration Guide
- Cisco VNMC GUI Configuration Guide

Launching ASDM from Cisco VNMC to Monitor the ASA 1000V

VNMC 2.0 enables you to launch ASDM as a Web Start application on your desktop.

Note Complete this task only when you have configured the ASA 1000V to use the VNMC management mode. When you launch ASDM from Cisco VNMC, you can only use ASDM to monitor the ASA 1000V. You cannot use ASDM launched from Cisco VNMC to configure policies. Only monitoring is supported in VNMC management mode.

Prerequisites

Before completing this task, you must have configured VNMC management mode for ASA 1000V and enabled ASDM to be launched from VNMC.

Note If you configured the ASA 1000V to run in VNMC management mode, you can launch ASDM from VNMC for monitoring only.
See the "Information About the ASA 1000V Deployment" section on page 2-1.

For more information, see the "Setting Up ASDM to Be Used by the ASA 1000V" section on page 2-12.

Detailed Steps

Step 1 Log into the VNMC.

Step 2 Choose **Resource Management > Resources > Firewalls > All ASA 1000Vs >** *virtual-asa* where *virtual-asa* is the edge firewall for which you want to launch ASDM.

Step 3 Click **Launch ASDM** in the upper-right corner of the screen.

Step 4 In the ASDM Launch screen, click **Run ASDM**.

ASDM opens in a new browser window on your desktop.