Configuring Managed Resources

This section contains the following topics:

Resource Management

Prime Network Services Controller enables you to manage the following resources:

- Compute firewalls—A virtual firewall that delivers security and compliance for a virtual computing environment at the VM level. Context-based and VLAN-independent policies can be applied to VM zones, thereby providing topology-invariant, policy-based security controls. In addition, traffic from external sources to VMs, and from VM to VM can be protected.
- Edge firewalls—A virtual appliance that secures the tenant edge in a multitenant environment. An example of an edge firewall is a Cisco Adaptive Security Appliance 1000V (ASA 1000V). An edge firewall:
  - Supports site-to-site VPN, NAT, and DHCP.

- Acts as a default gateway.
- Secures the VMs within a tenant against network-based attacks.

- Edge routers—A virtual edge router that serves as a single-tenant WAN gateway in a multitenant cloud. It allows enterprises to extend their WANs into external provider-hosted clouds.
- Load balancers—A virtual appliance that distributes network and application traffic across multiple servers. It improves application performance and prevents server failures by alleviating loads on servers.
- Virtual Security Gateways (VSGs)—VSGs evaluate policies based on network traffic. The main functions of a VSG are as follows:
  - Receive traffic from Virtual Network Service Data Path (vPath).
    For every new flow, the vPath component encapsulates the first packet and sends it to a VSG as specified in the Nexus 1000V port profiles. It assumes that the VSG is Layer 2 adjacent to vPath. The mechanism used for communication between vPath and the VSG is similar to VEM and Nexus 1000V communication on a packet VLAN.
  - Perform application fix-up processing such as FTP, TFTP, and RSH.
  - Evaluate policies by inspecting the packets sent by vPath using network, VM, and custom attributes.
  - Transmit the policy evaluation results to vPath.

Note Each vPath component maintains a flow table for caching VSG policy evaluation results.

- Virtual Supervisor Modules (VSMs)—A virtual appliance that runs on a Nexus 1000V switch and that manages, monitors, and configures multiple Virtual Ethernet Modules (VEMs). VEMs run as part of a hypervisor where they act as virtual switches. VSMs are tightly integrated with hypervisors, so that configurations made on a VSM are automatically propagated to the VEMs. As a result, instead of configuring soft switches inside the hypervisor on a host-by-host basis, you can define configurations for immediate use on all VEMs that are managed by the VSM from a single interface.

You manage resources by placing them in service. The general workflow for placing devices in service is as follows:

1. Create tenants and subordinate organizations.
2. Configure device policies.
3. Register or instantiate service devices from service images.

Registering Third-Party VMs

Registering third-party VMs in Prime Network Services Controller is a two-step process, as described in the following topics:

1. Installing the Prime Network Services Controller Device Adapter, on page 4
2. Deploying and Registering Third-Party VMs, on page 3

Deploying and Registering Third-Party VMs

This procedure describes how to deploy third-party VMs (such as Citrix NetScaler 1000V and Citrix NetScaler VPX) and register them with Prime Network Services Controller.

Before You Begin

Confirm the following:

- Prime Network Services Controller Device Adapter is successfully registered with Prime Network Services Controller by choosing **Administration > Service Registry > Providers**. The Providers table should include managed-endpoint and mgmt-controller entries for the Prime Network Services Controller Device Adapter VM.
- The third-party OVA is available from the VMware vSphere Client.

Note If you are prompted with a third-party login screen requesting information (for example, management IP information or upload feature licenses), you can do either of the following:

- Use the existing configuration and ignore this screen.
- Refer to the following URL for additional Citrix licensing features: http://support.citrix.com/proddocs/topic/netscaler-getting-started-map-10-1/ns-initial-config-using-ftu-wizard-tsk.html

Procedure

Step 1 In VMware, choose the host on which to deploy the third-party VM.

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

Step 3 In the wizard, provide the information as described in the following table.

Note The same information is required for both Citrix NetScaler 1000V and Citrix NetScaler VPX VMs.

Screen	Action
Source	Choose the OVA that you want to deploy.
OVF Template Details	Review the details.
Name and Location	Enter a name and choose a location for the VM.
Storage	Choose the location for the VM files.
Disk Format	Choose the format in which to store the virtual disks.
Network Mapping	Choose the destination networks for the VM.

Step 4 In the Ready to Complete screen, review the deployment settings for accuracy, and then click **Finish**.

Step 5 Open the VM console so that you can monitor the deployment status.

Step 6 When prompted in the console, enter the following information for the VM:

- IP address
- Subnet mask
- Gateway IP address

Step 7 When the information is correct, enter **4** and press **Return**.
You can continue to monitor the progress in the console.

Step 8 Confirm that the VM is registered in Prime Network Services Controller by choosing **Resource Management > Resources >** *resource*. For example, for Citrix NetScaler load balancer VMs, you would choose **Resource Management > Resources > VPX**.

Installing the Prime Network Services Controller Device Adapter

The Prime Network Services Controller Device Adapter enables third-party VMs (such as Citrix NetScaler load balancers) to register with Prime Network Services Controller.

Note

- Prime Network Services Controller Device Adapter is required and must be installed before you deploy and register third-party service nodes, such as Citrix NetScaler 1000V and Citrix NetScaler VPX service nodes.
- Adding or editing policies from the Prime Network Services Controller Device Adapter is not supported. All configuration must be performed using the Prime Network Services Controller GUI.
- You need to install the Prime Network Services Controller Device Adapter only once for each Prime Network Services Controller instance.

Before You Begin

Make sure that a network path exists between the Prime Network Services Controller Device Adapter IP address and the Prime Network Services Controller management IP address.

Procedure

Step 1 Use the VMware vSphere Client to log in to the vCenter server.

Step 2 Choose the host on which to deploy the Prime Network Services Controller Device Adapter.

Step 3 Choose **File > Deploy OVF Template**.

Step 4 In the wizard, provide the required information as described in the following table:

Screen	Action
Source	Navigate to and choose the nsc-device-adapter.3.2.*nx*.ova file.
OVF Template Details	Review the details of the Prime Network Services Controller Device Adapter template.
End User License Agreement	Review the agreement and click **Accept**.
Name and Location	Specify a name and location for the VM. The name must begin with a letter.
Deployment Configuration	Choose **Installer**.
Storage	Choose the data store for the VM.
Disk Format	Choose the required format.
Network Mapping	Choose the management network port group for the VM.
Properties	Provide the required information with particular attention to the following fields: • NTP—Enter the IP address for an NTP server. • Prime Network Services Controller Device Adapter IP Address RegIP—Enter the IP address for the Prime Network Services Controller server.
Ready to Complete	Review the deployment settings for accuracy.

Step 5 Click **Finish**.

Step 6 After the deployment is complete, power up the VM.
You can monitor the progress of the deployment by opening the VM console.

Step 7 Confirm that the Prime Network Services Controller Device Adapter VM is successfully registered with Prime Network Services Controller by logging in to the Prime Network Services Controller server and choosing **Administration > Service Registry > Providers**.
The Providers table should include managed-endpoint and mgmt-controller entries for the Prime Network Services Controller Device Adapter VM that you deployed.

Verifying VM Registration

Use this procedure to verify that the following VMs are successfully registered in Prime Network Services Controller:

- ASA 1000V
- CSR 1000V
- InterCloud
- Citrix NetScaler load balancer
- VSG
- VSM

To confirm registration with Prime Network Services Controller, choose **Resource Management > Resources > *resource***. In the content pane, the consolidated status for each resource is displayed in the Status column. This consolidated status is determined by assessing the following attributes in sequence:

1. Reachability
2. Association
3. Config State
4. Running

If any of these attributes fail, the failure of that attribute is displayed. For example, if the device cannot be reached, the status *unreachable* is displayed. Similarly, if the device is reachable and associated, but the configuration fails, the status *config failed* is displayed.

Importing Service Images

Prime Network Services Controller enables you to import service images that you can then use to instantiate a service device.

After you import an image, Prime Network Services Controller automatically places the file in the correct location and populates the Images table.

For information on instantiating a service VM from a service image, see the following topics:

- Adding a Compute Firewall, on page 7
- Adding an Edge Firewall, on page 13
- Adding Edge Routers, on page 18
- Adding Load Balancers, on page 22

Before You Begin

Confirm that the service images are available for importing into Prime Network Services Controller.

Procedure

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

Step 2 Click **Import Service Image**.

Step 3 In the Importing Service Image Dialog box:

a) Enter a name and description for the image you are importing.

b) In the Type field, choose the type of image to import.

c) In the Version field, enter a version number that you want to assign to the image.

d) In the Import area, provide the following information, and then click **OK**:

- Protocol to use for the import operations: FTP, SCP, or SFTP.
- Hostname or IP address of the remote host with the images.
- Account username and password for the remote host.
- Absolute image path and filename, starting with a slash (/).

Compute Firewalls

Adding a Compute Firewall

You can add a compute firewall and assign it to a VSG, thereby placing the VSG in service. A wizard walks you through the configuration process, which includes assigning profiles, assigning a VSG or instantiating a VSG service image, and configuring interfaces.

When you add a new compute firewall, the firewall data IP address can be the same as the data IP address of an existing compute firewall in Prime Network Services Controller as long as the firewalls have different organizational paths. That is, as long as the firewalls do not reside in the same organization, including parent and child organizations.

Note We recommend that you add the compute firewall at the tenant level or below, and not at the root level.

Before You Begin

- You must have at least one of the following:
  - An available VSG that is registered in Prime Network Services Controller. For more information, see Verifying VM Registration, on page 6.
  - A VSG pool with at least one available VSG.
  - An imported VSG service image.
- A VM Manager must be configured in Prime Network Services Controller.

Note For HA-specific configurations, refer to the appropriate Cisco Adaptive Security Appliance 1000V (ASA 1000V) configuration guide for additional information.

Procedure

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

Step 2 In the Network Services tab, choose **Add Compute Firewall**.

Step 3 In the Properties screen, provide the information as described in Properties Screen, on page 9, and then click **Next**.

Step 4 In the Service Device screen, select the required VSG service device, provide any required information as described in Service Device Screen, on page 9, and then click **Next**.

Step 5 (Instantiate option only) If you instantiate a VSG service device from an image, do one or both of the following in the Placement screen, and then click **Next**:

- Navigate to and choose the host or resource pool to use for the VSG instance.
- If you enabled high availability, either check the **Same as Primary** check box, or navigate to and choose the host or resource pool to use for the secondary VSG instance.

Step 6 In the Interfaces screen, configure interfaces as follows, and then click **Next**:

- If you assigned a VSG, enter the data IP address and subnet mask.
- If you assigned a VSG pool, enter the data IP address and subnet mask.
- If you instantiated a VSG service device without high availability, add management and data interfaces.
- If you instantiated a VSG service device with high availability, add management, data, and HA interfaces.

For field-level help when configuring the interfaces, see the online help.

Step 7 In the Summary screen, confirm that the information is correct, and then click **Finish**.

Compute Firewall Deployment Options

VSG compute firewalls are available in the following deployment models based on the memory, CPU speed, and number of virtual CPUs. Choose the deployment size that is appropriate for your environment.

Deployment Size	Memory	CPU Speed	Number of Virtual CPUs
Small	2 GB	1.0 GHz	1
Medium	2 GB	1.5 GHz	1
Large	2 GB	1.5 GHz	2

Field Descriptions

Properties Screen

Field	Description
Name	Compute firewall name. This name can contain 1 to 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is created.
Description	Compute firewall description.
Host Name	Management hostname of the firewall.
Device Profile	Do either of the following: • Click the profile name to view or optionally modify the currently assigned device configuration profile. • Click **Select** to choose a different device configuration profile.

Service Device Screen

Field	Description
Assign VSG	Assign a VSG to the compute firewall. From the **VSG Device** drop-down list, choose the required service device.
Assign VSG Pool	Assign a VSG pool to the compute firewall. In the **VSG Pool** field, either choose the required pool from the drop-down list or click **Add Pool** to add a new pool.

Field	Description
Instantiate	Instantiate a VSG service device from an available image. 1 In the list of available images, select the image to use to instantiate a new VSG service device. 2 In the High Availability field, check the **Enable HA** check box to enable high availability. 3 From the Deployment Size drop-down list, choose the size of the deployment. For more information, see Compute Firewall Deployment Options, on page 8. 4 In the VM Access password fields, enter the password for the admin user account.

Managing Compute Firewalls

You can edit and view fault information on existing compute firewalls as needed.

Procedure

Step 1 In the Resource Management tab, choose **Managed Resources > root >** *tenant*.

Step 2 In the Network Services tab, select the required compute firewall, and then click **Edit** or **Delete**.

Step 3 If you chose **Edit**, modify the fields as appropriate, using the information in the following tables, and then click **OK**.

Note To view additional information about an entry in the Faults tab, double-click the entry, or select the entry and then click **Properties**.

General Tab

Field	Description
Name	Compute firewall name.
Description	Compute firewall description.
Management IP Address	Management IP address for the compute firewall.
HA Role	High availability role of the compute firewall: standalone or active standby.
Deployment Size	Size of the deployment: Small, Medium, or Large.
Device Profile	Device profile associated with the compute firewall.
Status	

Field	Description
Deploy State	Deployment state of the firewall.
Power State	Whether the firewall is powered off or on.
Config Status	Configuration status of the compute firewall: applied, applying, failed-to-apply, or not-applied.
Association Status	Association state of the firewall: associated, associating, disassociating, failed, or unassociated.
Reachable	Whether or not the compute firewall is reachable.

Placement Tab

This tab is displayed only if the compute firewall is instantiated from a service image.

Field	Description
Image Table (read-only)	
Select	Radio-button indicating image selection.
Name	Service image name.
Version	Service image version.
VM Manager Details If high availability is enabled, the following fields are displayed for both the primary and secondary service devices.	
VM Manager	VM Manager for the service device.
Host	IP address of the VM host.
Instance Name	VM instance name.

Network Interfaces Tab—VSG Assigned

This tab is displayed only if a VSG was assigned to the compute firewall.

Field	Description
Management Hostname	Management hostname for the compute firewall.
Data IP Address	Compute firewall data IP address.
Data IP Subnet	Netmask for the data IP address.

Field	Description
VLAN	VLAN to use for service path configuration if the device is running in Layer 2 mode.

Network Interfaces Tab—VSG Instantiated

This tab is displayed only if the compute firewall was instantiated from a service image.

Field	Description
Toolbar	
Add Interface	Adds an interface.
Edit	Enables you to edit the selected interface.
Delete	Deletes the selected interface.
Filter	Filters the table contents by the string or value that you enter.
Table	
Type	Interface type: Data, HA, or Management.
IP Address	Interface IP address.
Port Group / Sub Network	Port group or subnetwork associated with the interface.

Unassigning a VSG

Use this procedure to remove a VSG from a compute firewall.

Procedure

Step 1 Choose **Resource Management > Managed Resources > root >** *tenant*.
Step 2 In the Network Services tab, choose the compute firewall with the VSG that you want to unassign.
Step 3 In the toolbar, choose **Actions > Unassign VSG**.
Step 4 When prompted, confirm the action.

Edge Firewalls

Adding an Edge Firewall

You can add an edge firewall and assign it to an ASA 1000V, thereby placing the ASA 1000V in service. A wizard walks you through the configuration process, which includes assigning configuration and service profiles, assigning an ASA 1000V or instantiating an ASA 1000V service image, and configuring interfaces.

Before You Begin

- At least one of the following must exist:
  - An ASA 1000V must be registered in Prime Network Services Controller and must be available for assignment.
  - An imported ASA 1000V service image.
- A VM Manager must be configured in Prime Network Services Controller. For more information about VM registration, see the Cisco Prime Network Services Controller 3.2 Quick Start Guide.

Note For HA-specific configurations, refer to the appropriate Cisco Adaptive Security Appliance 1000V (ASA 1000V) configuration guide for additional information.

Procedure

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

Step 2 In the Network Services tab, choose **Add Edge Firewall**.

Step 3 In the Properties screen, provide the information described in Properties Screen, on page 14, and then click **Next**.

Step 4 In the Service Device screen, do one of the following, and then click **Next**:

- To assign an existing ASA 1000V service device:
  1. Click **Assign ASA 1000V**.
  2. From the **ASA 1000V Device** drop-down list, choose the required ASA 1000V.
- To instantiate a new ASA 1000V:
  1. Click **Instantiate**.
  2. Choose the image to use to instantiate a new ASA 1000V service device.
  3. In the VM Access password fields, enter the password for the admin user account.

Step 5 (Instantiate option only) If you instantiate a ASA 1000V service device from an image, do one or both of the following in the Placement screen, and then click **Next**:

- Navigate to and choose the host or resource pool to use for the ASA 1000V instance.
- If you enabled high availability, either check the **Same as Primary** check box, or navigate to and choose the host or resource pool to use for the secondary ASA 1000V instance.

Step 6 In the Interfaces screen, add the required interfaces as follows, and then click **Next**:

- If you assigned an ASA 1000V without high availability, configure one inside and one outside interface.
- If you assigned an ASA 1000V with high availability, configure one inside and one outside interface, each with a secondary IP address.
- If you instantiated an ASA 1000V without high availability, configure management, inside, and outside interfaces.
- If you instantiated an ASA 1000V with high availability, configure management, inside, outside, and HA interfaces.

  Note The management and HA interfaces must use different port profiles.

Step 7 In the Summary screen, confirm that the information is accurate, and then click **Finish**.

Step 8 If you instantiated the ASA 1000V from a service image, you must do the following to ensure registration with Prime Network Services Controller:

a) **Within 15 minutes of instantiation**, manually register the ASA 1000V to Prime Network Services Controller by using the ASA 1000V CLI.

b) If you do not register the ASA 1000V within 15 minutes of instantiation, the instantiated ASA 1000V will enter a failed state, and you must delete it manually from Prime Network Services Controller and the hypervisor.

Field Descriptions

Properties Screen

Field	Description
Name	Edge firewall name. This name can contain 1 to 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is created.
Description	Edge firewall description.
Host Name	Management hostname of the firewall.
High Availability	Check the **Enable HA** check box to enable high availability.

Field	Description
Device Configuration Profile	Do either of the following: • Click the profile name to view and optionally modify the currently assigned device configuration profile. • Click **Select** to choose a different device configuration profile.
Device Service Profile	Do either of the following: • Click the profile name to view and optionally modify the currently assigned device service profile. • Click **Select** to choose a different device service profile.

Unassigning an ASA 1000V

If required, you can unassign an ASA 1000V from an edge firewall.

Procedure

Step 1 Choose **Resource Management > Managed Resources > root >** *tenant*.
Step 2 In the Network Services tab, choose the required edge firewall.
Step 3 In the toolbar, choose **Actions > Unassign ASA 1000V**.
Step 4 When prompted, confirm the action.

Edge Routers

Edge Router Configuration Workflow

This workflow describes how to create an edge router under a tenant.

Steps	Notes
1. Confirm that prerequisites are met.	See Prerequisites for Configuring Edge Routers, on page 16.

Steps	Notes
2. (Optional) Configure Edge Router configuration and service profiles and policies. If needed, you can use the default profiles.	• Choose **Policy Management > Service Profiles > *tenant* > Edge Router** and select **Device Service Profiles** or **Interface Service Profiles** • Choose **Policy Management > Service Policies > *tenant*** and select **Policies** or **Policy Helpers**
3. Add an edge router under a tenant.	Choose **Resource Management > Managed Resources > *tenant*** and select **Add Edge Router** from the Network Services Actions drop-down list.
4. Enter the appropriate information in the Add Edge Router Wizard.	See Adding Edge Routers, on page 18.
5. Verify that the edge router has been created.	Choose **Resource Management > Resources** and select the edge router device and view the device status in the table. **Note** It takes some time for the logical device to associate with the physical device.

Prerequisites for Configuring Edge Routers

The following table lists the information you should have on hand and any prerequisites for configuring edge routers. For information on adding and configuring edge routers, see Edge Router Configuration Workflow, on page 15 and Adding Edge Routers, on page 18.

Note By default, CSR 1000V OVA images contain three vNICs and Prime Network Services Controller will instantiate CSR 1000V service images with only three interfaces. If you need more than three edge router interfaces, see http://www.cisco.com/en/US/docs/routers/csr1000/software/configuration/vminterface.html for information on how to configure additional interfaces.

Item	Notes
Decide whether you are assigning or instantiating an edge router.	Note all the necessary edge router information needed for configuration. • To assign an edge router to Prime Network Services Controller, an edge router VM must be installed. Use VM management software (such as VMware) to deploy a device image from an OVA template and register the device with Prime Network Services Controller. For Cisco Cloud Services Router 1000V, see the Cisco CSR 1000V Configuration Guide. • To instantiate an edge router, an edge router service image must be available. For more information, see Importing Service Images, on page 6.
At least one tenant is configured	See Creating a Tenant.
Determine the number of loopback interfaces required on the edge router.	Loopback interfaces cannot be added or deleted after an edge router is instantiated. Therefore, all required loopback interfaces must be configured before assignment or during instantiation.
Determine the number of data (Gigabit Ethernet) interfaces required on the edge router.	Data interfaces cannot be added or deleted after an edge router is instantiated. Therefore, all required data interfaces must be configured before assignment or during instantiation.
Decide whether to create a new edge router device profile	Prime Network Services Controller offers a default configuration profile that contains common policies for all devices managed in Prime Network Services Controller. You can use or edit the default profile, or customize a new profile. To create a new device configuration profile, choose **Policy Management > Device Configurations > *root* (or *tenant*) > Device Profiles** and click **Add Device Profile**.

Item	Notes
Decide whether to configure or use the default device service profiles.	To create or edit a device service profile, note the following applicable router policy and interface information you need for configuration: **Device Service Profile (Policies)** • Routing Policy ◦ Static ◦ BGP ◦ OSPF • NAT **Note** Edge routers support a limited set of NAT policy options. • Zone-Based Firewall **Note** For more information on zone-based firewall configuration, see Configuring Zone-Based Firewall Policies. **Note** A zone policy defines the traffic that you want to allow or deny between zones. A zone-pair policy allows you to specify a unidirectional firewall policy between two zones. The direction is defined by specifying a source and destination zone. **Interface Service Profiles** • Ingress • Egress • NAT Membership • Firewall Zone Membership **Note** A firewall zone is a group of interfaces to which a policy can be applied. By default, traffic can flow freely within that zone but all traffic to and from that zone is dropped. To allow traffic to pass between zones, you must explicitly declare it by creating a zone-pair and a policy for that zone.

Adding Edge Routers

This procedure describes the steps in the Add Edge Router wizard. The Add Edge Router wizard is part of the Edge Router Configuration Workflow, on page 15. Before using the Add Edge Router wizard, see Prerequisites for Configuring Edge Routers, on page 16.

Procedure

Step 1 Choose **Resource Management > Managed Resources >** *tenant*, and then choose **Add Edge Router**.

Step 2 Enter edge router device information in the Properties window and click **Next**.

Step 3 If you are instantiating an edge router, do the following, and then click **Next**:

a) Select the image to use to instantiate the edge router.

b) In the Compute area, enter the number of virtual CPUs and amount of memory you need to meet the required throughput. For more information, see Edge Router Deployment Options, on page 19.

c) In the VM Access area, enter the access credentials.

Step 4 In the Service Device screen, if you are assigning an edge router, choose the deployed edge router, configure the applicable interfaces and IP addresses, and then click **OK**.

Note
- You must configure at least two Gigabit interfaces.
- The primary IP address and the sub management IP address must be in the same subnet.

Step 5 In the Placement screen, choose the location for the edge router.

Step 6 In the Interface screen, assign the IP address. Keep in mind that the the primary IP address and the sub management IP address must be in the same subnet.

Step 7 Click **Finish** if the summary details are correct.

Edge Router Deployment Options

Edge routers can support different amounts of throughput based on the number of virtual CPUs and amount of memory. Choose the number of virtual CPUs and amount of memory that are appropriate for your environment and for the desired throughput.

Throughput	Technology Package		
Speed	**Standard**	**Advanced**	**Premium**
10 Mbps	1 vCPU, 2.5 GB RAM	1 vCPU, 2.5 GB RAM	1 vCPU, 2.5 GB RAM
50 Mbps	1 vCPU, 2.5 GB RAM	1 vCPU, 2.5 GB RAM	1 vCPU, 2.5 GB RAM
100 Mbps	1 vCPU, 2.5 GB RAM	1 vCPU, 2.5 GB RAM	1 vCPU, 2.5 GB RAM
250 Mbps	4 vCPU, 4 GB RAM	4 vCPU, 4 GB RAM	4 vCPU, 4 GB RAM
500 Mbps	4 vCPU, 4 GB RAM	—	—
1 Gbps	4 vCPU, 4 GB RAM	—	—

Managing Edge Routers

You can do the following edge router management tasks:

- Edit information and network interfaces.
- Modify the device profile, device service profile, and the interface service profile.
- Delete an edge router.
- Monitor status and view fault information.
- You can start, stop, and reboot edge routers that have been instantiated.
- You can perform assign and unassign operations for edge routers that have been registered.

For information on initial edge router configuration, see Edge Router Configuration Workflow, on page 15 and Prerequisites for Configuring Edge Routers, on page 16.

Procedure

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

Step 2 In the Network Services tab, choose the required edge router and then click **Edit** or **Delete**.

Step 3 If you chose **Edit**, modify or view the appropriate tab information in the Edit dialog box, and then click **OK**.

Note To view additional information about an entry in the Faults tab, double-click the entry, or select the entry and then click **Properties**.

Load Balancers

Load Balancer Configuration Workflow

This workflow describes how to create a load balancer under a tenant. The workflow includes creating a virtual server profile and an associated service if one does not exist.

Steps	Notes
1. Confirm that the prerequisites are met.	See Prerequisites for Configuring Load Balancers, on page 21. This topic also includes the following information: • Importing load balancer licenses. • Installing the device adapter.
2. Add a virtual server profile to a tenant.	Add a service and enter general and server farm information. See Load Balancing Service Dialog Boxes, on page 23 for server farm information.

Steps	Notes
3. Verify that the virtual server profile has been created.	Choose **Policy Management > Service Profiles >** ***tenant*** **> Load Balancer** and confirm that the virtual server has been created in the Virtual Server Profiles table.
4. Add a load balancer device under a tenant.	Choose **Resource Management > Managed Resources >** ***tenant*** and then choose **Add Load Balancer** from the Network Services Actions drop-down list.
5. Enter the appropriate information in the Add Load Balancer Wizard.	The wizard maps a logical load balancer and configures the virtual IP addresses to the selected virtual servers. For more information, see Adding Load Balancers, on page 22.
6. Verify that the load balancer has been created.	Choose **Resource Management > Resources > VPX >** *load-balancer* and then view the device status in the table. It takes some time for the logical device to associate with the physical device.

After a load balancer is added and configured, you can view faults, edit, and monitor the load balancer. For more information, see Managing Load Balancers, on page 26. Also, if you would like to edit services on a server profile (for example, add ping monitors), choose **Policy Management > Service Profiles >** ***tenant*** **> Load Balancer > Virtual Server Profiles >** ***service*** and click **Edit**.

Prerequisites for Configuring Load Balancers

The following table lists the information you should have on hand and any prerequisites for configuring load balancers:

Note For load balancer configuration, see Load Balancer Configuration Workflow, on page 20 and Adding Load Balancers, on page 22.

Item	Notes
Tenant	At least one existing tenant configured.
Load Balancer Information	
For Citrix NetScaler load balancers, the Prime Network Services Controller Device Adapter must be deployed	See Registering Third-Party VMs.

Item	Notes
Decide whether you are assigning or instantiating a load balancer	Note all the necessary load balancer information needed before configuration. To assign a load balancer, the load balancer OVA must first be deployed. For Citrix NetScaler load balancers, see Citrix Netscaler documentation and also Registering Third-Party VMs. To instantiate a load balancer, a load balancer service image must be available. See Importing Service Images for information on how to import a service image.
Virtual Server Profile Information	
Determine the number of virtual servers required on the load balancer	Virtual servers cannot be added or deleted after a load balancer is instantiated. All required virtual servers must be configured before registration or during instantiation.
Service and server farm information	• Protocol • Port • Algorithm • Persistence • Real server • Host name or IP address For more information, see Load Balancing Service Dialog Boxes, on page 23.
Monitor information	• TCP • HTTP • Ping

Adding Load Balancers

This procedure describes the steps in the Add Load Balancer wizard. Before using the Add Load Balancer wizard, confirm that the prerequisites are met in Prerequisites for Configuring Load Balancers, and see Load Balancer Configuration Workflow.

Procedure

Step 1 Enter load balancer device information in the Properties window and click **Next**.

Note If you choose to enable vPath, only vPath-enabled devices (like Citrix Netscaler 1000V) will be available for selection in the instantiation image list.

Step 2 Choose whether you want to register or instantiate a load balancer in the Service Device window.

Step 3 Do one of the following:

1 If you are registering a load balancer:

- Enter all required information (device IP address, subnet mask and gateway information).
- Select the device type and version from the drop-down lists.
- Enter the device access credentials.
- Configure one data interface and one virtual IP interface in the Configure Interface window, then click **Next**. All interfaces must be in different subnetworks. The management interface is automatically taken from the device IP address that you entered above.

2 If you are instantiating a load balancer:

- Select the instantiation image and locate where the VM will be hosted.
- Enter the virtual machine access credentials and click **Next**.
- Navigate to VM placement.
- Configure one data interface and one management interface in the Configure Interface window, then click **Next**.

Step 4 Configure a virtual server by selecting an existing virtual server profile and assigning virtual IP addresses (VIPs) in the Configure Virtual Server window, then click **Next**.

Note
- VIPS are public IP addresses that clients connect to and where all traffic is directed to. Behind VIPs are real servers where load balancing occurs. Limit the number of VIPs to 64 VIPs per load balancer.
- The VIP IP address cannot be on the management network.

Step 5 Click **Finish** if the summary details are correct.

For troubleshooting information, view errors in the Faults tab (see Managing Load Balancers). If you would like to modify the virtual server profile services (for example, add monitors to your server farm) choose **Policy Management > Service Profiles > *tenant* > Load Balancer > Virtual Server Profiles > *service*** and click **Edit**. Navigate to the Server Farm tab to modify any information.

Load Balancing Service Dialog Boxes

Various Service dialog boxes appear when configuring a virtual server service for a load balancer profile. For more information on how to configure a load balancer profile, see the Load Balancer Configuration Workflow topic.

Server Farm Information

Note

- If you need to add a new server farm, you must enter information in the Real Server and Monitor tabs.
- To confirm that your configurations were applied, you can view the device's UI.

Field	Notes
Protocol	If you select SSL or SSL_TCP, a security policy must be configured. See the Security Policy Dialog Boxes topic which describes.
Algorithm	Select the scheduling algorithm for the server farm. • Least Connection—New connections are sent to the server with the fewest connections. • Destination IP Hash—Selects a server based on a hash of the source IP address of each packet. • Least Bandwidth—New connections are sent to the server with the least bandwidth. • Least Packets—New connections are sent to the server with the least packets. • Least Response Time—New connections are sent to the server with the least response time. • Round Robin—Each server is used in turn according to the weight assigned to it. • URL Hash—The left part of the URL (before the question mark) is hashed and divided by the total weight of the running servers. The result designates which server will receive the request. Applicable to only HTTP service load balancing.
Increment Interval	Interval at which the server is pinged.

Field	Notes
Persistence	Select the persistence method that will define how the load balance service handles information. The following persistence restrictions exist: • SSL—Applies only to SSL-based services. • Cookie Insert—Applies only to HTTP-based services. **Note** If the service protocol and persistence is an invalid combination, a "failed-to-apply" status appears in the Network Services tab.
Monitors	
HTTP	Monitors HTTP traffic.
Ping	Pings real servers to see if they are up and running.
TCP	Monitors TCP traffic.

Limitations

- 64 real servers per server farm
- 64 monitors per server farm
- 16 services per virtual server

Security Policy Dialog Boxes

Load Balancing Security Policy Information

For load balancing, if SSL and SSL-TCP protocols are selected, security policies must be configured. You can configure security policies so that cryptographic authentication is enabled using the SSL Params, Cipher Groups, Certificate, and Certificate Key File dialog boxes.

Note SSL offload configuration requires a valid certificate and key file.

Dialog Box	Description
SSL Params	Allows you to customize the SSL configuration. From this dialog box you may choose to enable and configure the following: • Ephemeral RSA • Session reuse • Cipher redirect • SSL and SSLv2 redirect • Selection of TLSv1, SSLv3, and SSLv2 protocols • Close notifications • SSL redirect port rewrite
Cipher Group	Allows you to select or add cipher groups. A cipher group is a set of cipher suites that you attach to an SSL service.
Certificate and Certificate Key File	Allows you to configure or add certificates and certificate key files.

Managing Load Balancers

You can do the following load balancer management tasks:

- Edit information and network interfaces.

Note Management and data IP interfaces cannot be modified after creation.

- Delete a load balancer.
- Monitor status and view fault information.

Procedure

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

Step 2 In the Network Services tab, choose the required load balancer, and then click **Edit** or **Delete**.

Step 3 If you chose **Edit**, modify or view the appropriate tab information in the Edit dialog box, and then click **OK**.

Note To view additional information about an entry in the Faults tab, double-click the entry, or select the entry and then click **Properties**.

If you would like to modify the virtual server profile services (for example, add monitors to your server farm) choose **Policy Management > Service Profiles >** ***tenant*** **> Load Balancer > Virtual Server Profiles >** ***service*** and click **Edit**. Navigate to the Server Farm tab to modify any information.

Adding a Port Profile to a VSM

Prime Network Services Controller enables you to add a port profile to an enterprise VSM. You cannot add a port profile to a cloud VSM.

If an enterprise VSM has preconfigured port profiles or virtual service configurations that were created outside of Prime Network Services Controller, these configurations will not be displayed in the Prime Network Services Controller GUI.

If you create a port profile in Prime Network Services Controller and specify a VLAN, you must create the VLAN itself on the VSM and then add it to the necessary system and uplink port profiles. The same steps apply for VLANs that you specify while creating service devices, such as edge or compute firewalls: you must create the VLANs on the devices, and then add them to the appropriate system and uplink port profiles.

Before You Begin

Confirm the following:

- An enterprise VSM is registered and in the *applied* state in Prime Network Services Controller by choosing **Resource Management > Resources > VSMs**.
- You have admin privileges.

Procedure

Step 1 Choose **Resource Management > Resources > VSMs >** *vsm*, then click **Edit**.

Step 2 Above the Port Profile table, click **Add**.

Step 3 In the Add Port Profile dialog box, enter the required information as follows, then click **OK**:

1. In the General tab, provide the following information:
   - Name
   - Description
   - State: Enabled or Disabled.
   - Type of Binding: Dynamic, Ephemeral, or Static.
   - Binding Option: Auto, AutoExpand, or None.
   - Maximum and minimum number of ports.
   - Tenant or subordinate organization in which to create the port profile.
2. In the L2 Network Membership tab, provide the following information:
   - Capability: Bridge Domain or VLAN.

- Mode: Access or Trunk
- VLAN number (Access mode) or VLAN range (Trunk mode).

The NICs table is populated automatically after you bind a service path to the port profile and the service path is used the first time. For more information about configuring a service path and binding it to a port profile, see Service Path Configuration Workflow.

Updating Discovered VSM Port Profiles

When Prime Network Services Controller discovers a VSM port profile that was configured directly on the Nexus 1000V, only some of the configuration information is available to Prime Network Services Controller. As a result, you need to provide the missing information in Prime Network Services Controller.

This situation usually occurs under the following circumstances:

- A VSM port profile with an organization and virtual service have been configured on a Nexus 1000V.
- VMs with vNICs that use the port profile have also been configured on the device.

Procedure

Step 1 Log in to the Prime Network Services Controller GUI and choose **Resource Management > Resources > VSM**.

Step 2 Choose the VSM with the port profile that was configured using the CLI, and then click **Edit**.

Step 3 In the Port Profiles table, choose the required port profile, and then click **Edit**.

Step 4 Update the port profile properties so that they are consistent with the configured port profile, and save your changes. You can then use the port profile as needed.

Step 5 If any port profile properties are modified via the CLI, update them in Prime Network Services Controller so that the configurations remain synchronized.

Troubleshooting Devices and Services

You can use Prime Network Services Controller to troubleshoot faults associated with managed devices and services.

Procedure

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

Step 2 In the Network Services tab, choose the required service or device, and then click **Edit**.

Step 3 In the General tab, review the Status area for any issues or states affecting reachability, configuration, or association.

Step 4 In the Faults tab, review the displayed faults. To view additional information about a fault, double-click the entry, or choose the entry and then click **Properties**.

Launching ASDM

Prime Network Services Controller enables you to launch Cisco Adaptive Security Device Manager (ASDM) as a Web Start application on your desktop.

You can set up ASDM to be used by the ASA 1000V when it is configured for either Prime Network Services Controller management mode or ASDM management mode. When the ASA 1000V is configured to use Prime Network Services Controller management mode, you can use ASDM to monitor the status of the ASA 1000V, but you cannot use it to manage configurations.

Before You Begin

You must complete the following tasks before launching ASDM from Prime Network Services Controller:

1 Do one of the following:

- If you have not already deployed the ASA 1000V OVA, do so; during the deployment, provide the ASDM client IP address.
- If you have already deployed the ASA 1000V OVA, apply the following configuration by using the VM console in the vSphere client:
  - Add a route on the management interface to the ASDM client subnet by issuing the following command:
    ```
    ASA1000V(config)# route interface ip subnet next-hop-ip
    ```
    where *interface* is the management interface to the ASDM client subnet, *ip* is the IP address of the host that accesses ASDM, *subnet* is the ASDM client subnet, and *next-hop-ip* is the IP address of the gateway.

    Note Perform this step only if the next hop gateway IP address was not specified when deploying the ASA 1000V.

  - Allow HTTP access via the management interface for the ASDM client subnet by entering the following command:
    ```
    ASA1000V(config)# http ip subnet interface
    ```
    where *ip* is the IP address of the host that accesses ASDM, and *interface* is the ASDM client interface.

Note Perform this step only if the ASDM client IP address was not specified when deploying the ASA 1000V.

2 Confirm the following:

- The ASA 1000V is registered to Prime Network Services Controller.
- A valid username and password exist for the ASA 1000V VM console.

3 Assign the edge firewall to an ASA 1000V instance. If the edge firewall is not assigned to an ASA 1000V instance, the ASDM options are not displayed in the UI.

4 Confirm that your system is configured to run downloaded Java Web Start applications.

For more information about configuring ASDM, see the *Cisco ASA 1000V Cloud Firewall Getting Started Guide*.

Procedure

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

Step 2 In the Network Services tab, choose the required edge firewall, and then click **Edit**.

Step 3 In the Edit dialog box, click **Launch ASDM**.
The ASDM Launch screen opens.

Step 4 In the ASDM Launch screen, click **Run ASDM**.
The ASDM Web Start application is automatically downloaded and runs. If prompted, accept the certificates.
Note If an ASDM login dialog box is displayed, you can click **OK** without entering login credentials.

Managing VSG Pools

Adding a VSG Pool

Procedure

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

Step 2 In the VSG Pools tab, click **Add Pool**.

Step 3 In the Add Pool dialog box, enter a name and description for the pool.

Step 4 To assign members to the pool:

a) Click **(Un)Assign**.

b) In the Available list, choose the VSGs that you want to add to the pool, and then click the arrow to move them to the Assigned list.
c) Click **OK**.

Step 5 Click **OK**.

Assigning a VSG Pool

You can assign a VSG pool to a compute firewall when you add a compute firewall to a tenant or other organization. For information on assigning a VSG to a compute firewall, see Adding a Compute Firewall, on page 7.

Editing a VSG Pool

After you create a VSG pool, you can change its description and add or remove VSGs from the pool as required.

Procedure

Step 1 Choose **Resource Management > Managed Resources > root >** *tenant*.
Step 2 In the VSG Pools tab, choose the pool that you want to edit, and then click **Edit**.
Step 3 In the Edit Pool dialog box, modify the following information as required, and then click **OK**:
a) Edit the description.
b) To add or remove VSGs from the pool, click **(Un)Assign**.
c) To delete a VSG from the pool, choose the required VSG from the list of pool members, and then click **Delete**.

Unassigning a VSG Pool

If required, you can unassign a pool from a compute firewall.

Procedure

Step 1 Choose **Resource Management > Managed Resources > root >** *tenant*.
Step 2 In the Network Services tab, select the required firewall, and then choose **Actions > Unassign VSG/Pool**.
Step 3 When prompted, confirm the action.

Deleting a VSG Pool

Procedure

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

Step 2 In the VSG Pools tab, choose the pool that you want to delete, and then click **Delete**.

Step 3 When prompted, confirm the deletion.