Configuring Managed Resources

This section includes the following topics:

- Resource Management, page 1
- Resource Manager, page 2
- Virtual Machines, page 2
- Virtual Security Gateways, page 2
- ASA 1000V Cloud Firewalls, page 3
- Importing Service Images, page 3
- Managing Compute Firewalls, page 4
- Managing Edge Firewalls, page 9
- Verifying VM Registration, page 12
- Examining Fault Details, page 13
- Launching ASDM, page 14
- Managing Pools, page 15

Resource Management

The Resource Management tab displays the following resources that are managed by Prime Network Services Controller:

- Virtual Machines (VMs)
- ASA 1000V edge firewalls
- VSG compute firewalls
- Virtual Supervisor Modules (Nexus 1000V VSM)

You manage ASA 1000Vs and VSGs by placing them in service:

- You place an ASA 1000V in service by creating an edge firewall in an organization and assigning the ASA 1000V to that edge firewall.
- You place a VSG in service by creating a compute firewall in an organization and assigning the VSG to that compute firewall.

You manage VMs by discovering those VMs that have at least one network interface configured with a Nexus 1000V port profile.

Resource Manager

Resource Manager manages logical edge and compute firewalls and their association with ASA 1000Vs and VSGs, respectively. When an edge firewall is associated with an ASA 1000V, the device configuration profile information (defined by the edge firewall) is pushed to the ASA 1000V which, in turn, triggers the ASA 1000V to download the security profiles and policies from Policy Manager.

Resource Manager is responsible for the following services:

- Maintaining an inventory of ASA 1000Vs, VSGs, and VSMs.
- With user input, defining compute firewalls and associating them with VSGs for provisioning.
- With user input, defining edge firewalls and associating them with ASA 1000Vs for provisioning.
- Integrating with hypervisor instances to retrieve VM attributes.

Virtual Machines

Virtualization allows you to create multiple VMs that run in isolation, side by side on the same physical machine. Each VM has virtual RAM, a virtual CPU and NIC, and an operating system and applications. Because of virtualization, the operating system sees a consistent set of hardware regardless of the actual physical hardware components.

VMs are encapsulated in files for rapid saving, copying, and provisioning, which means that you can move full systems, configured applications, operating systems, BIOS, and virtual hardware within seconds, from one physical server to another. Encapsulated files allow for zero-downtime maintenance and continuous workload consolidation.

Instances of Prime Network Services Controller are installed on VMs.

Virtual Security Gateways

VSGs evaluate Prime Network Services Controller 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 VSM 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.

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

ASA 1000V Cloud Firewalls

The Cisco Adaptive Security Appliance 1000V Cloud Firewall (ASA 1000V) is a virtual appliance that was developed using the ASA infrastructure to secure the tenant edge in multi-tenant environments with Cisco Nexus 1000V Series switch deployments. ASA 1000V firewalls perform the following functions:

- Support site-to-site VPN, NAT, and DHCP.
- Act as a default gateway.
- Secure the VMs within a tenant against any network-based attacks.

In Prime Network Services Controller, an edge firewall is associated with an ASA 1000V instance. After association, all applicable profile types for the ASA 1000V device type are pushed to the ASA 1000V instance. All edge profile objects that are created at the same organization level as the edge firewall object are pushed to the device.

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 4
- Adding an Edge Firewall, on page 10

Note For HA-specific configurations, please refer to the appropriate Cisco Virtual Security Gateway (VSG) or Cisco Adaptive Security Appliance 1000V (ASA 1000V) configuration guides for additional information.

Procedure

Step 1 Choose **Resource Management > Resources > Service Devices > 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, select the type of image to import: ASA1000V or VSG.
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, then click **OK**:

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

Managing Compute Firewalls

You can add, edit, and delete compute firewalls. In addition, you can assign a VSG to compute firewall, thereby placing the VSG in service. The following topics describe these activities in more detail.

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.

Users with infrastructure-admin and tenant-admin roles can work with service VMs as follows:

- Users with the infrastructure-admin role can instantiate and delete service VMs.
- Users with the tenant-admin role can view service VM details, but cannot instantiate or delete service VMs.

Note

- We recommend that you add the compute firewall at the tenant level or below, and not at the root level.
- Users with the tenant-admin role cannot add or delete firewalls under a tenant.

Before You Begin

To place a VSG in service, at least one of the following must exist:

- To assign a VSG, an available VSG that is registered in Prime Network Services Controller. For more information, see Verifying VM Registration, on page 12.
- To assign a VSG pool, a VSG pool with at least one available VSG.

- To instantiate a VSG service device from an image, an imported service device image and VM Manager must be configured in Prime Network Services Controller.

Procedure

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

Step 2 In the General tab, click **Add Compute Firewall**.
The Add Compute Firewall Wizard opens.

Step 3 In the Properties screen, provide the information as described in Properties Screen, on page 5, then click **Next**.

Step 4 In the Service Device screen, select the required VSG service device as described in Service Device Screen, on page 6, 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, 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, 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, then click **Finish**.

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.

Field	Description
Host Name	Management hostname of the firewall.
Device Configuration 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. In 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.
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** In the VM Access password fields, enter the password for the admin user account.

Editing a Compute Firewall

You can edit existing compute firewalls as needed.

Procedure

Step 1 In the Resource Management tab, choose **Managed Resources > root >** *tenant* **> Compute Firewalls** where *tenant* is the required tenant.

Step 2 In the Compute Firewalls table, select the compute firewall you want to edit, then click **Edit**.

Step 3 In the Edit dialog box, modify the fields as appropriate, using the information in the following tables, then click **OK**.

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.
Pool Name	Pool to which the compute firewall is assigned.
Device Profile	Device profile associated with the compute firewall.
Status	
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	Indicates 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.

Field	Description
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.
Data Center	IP address of the VM data center.
Host	IP address of the VM host.
VM Name	VM 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.

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.

Field	Description
Port Group	Port group associated with the interface.

Deleting a Compute Firewall

Prime Network Services Controller enables you to delete firewalls that are not needed.

Note Users with the tenant-admin role cannot add or delete firewalls under a tenant.

Procedure

Step 1 Choose **Resource Management > Managed Resources > root >** *tenant* **> Compute Firewalls**.
Step 2 In the General tab, select the compute firewall you want to delete, then click **Delete**.
Step 3 When prompted, confirm the deletion.

Unassigning a VSG

Procedure

Step 1 Choose **Resource Management > Managed Resources > root >** *tenant* **> Compute Firewalls**.
Step 2 In the Compute Firewalls table, select the firewall with the VSG you want to unassign.
Step 3 In the toolbar, choose **Actions > Unassign VSG/Pool**.
Step 4 When prompted, confirm the action.

Managing Edge Firewalls

You can add an edge firewall, associate it with either an existing ASA 1000V instance or instantiate a new ASA 1000V from a service device image. The following topics describe these activities in more detail.

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.

Users with infrastructure-admin and tenant-admin roles can work with service VMs as follows:

- Users with the infrastructure-admin role can instantiate and delete service VMs.
- Users with the tenant-admin role can view service VM details, but cannot instantiate or delete service VMs.

Before You Begin

At least one of the following must exist:

- To assign an ASA 1000V to the edge firewall, an ASA 1000V must be registered in Prime Network Services Controller and must be available for assignment. For more information about VM registration, see the Cisco Prime Network Services Controller 3.0.2 Quick Start Guide.
- To instantiate an ASA 1000V service device from an image, an imported service device image and a VM Manager must be configured in Prime Network Services Controller.

Procedure

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

Step 2 In the General tab, click **Add Edge Firewall**.
The Add Edge Firewall Wizard opens.

Step 3 In the Properties screen, provide the information described in Properties Screen, on page 11, then click **Next**.

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

- To assign an existing ASA 1000V service device:
  1. Click **Assign ASA 1000V**.
  2. In the **ASA 1000V Device** drop-down list, choose the required ASA 1000V.
- To instantiate a new ASA 1000V:
  1. Click **Instantiate**.
  2. In the list of available VMs, select the VM 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, 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, 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, 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 vCenter console.

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 vCenter.

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* **> Edge Firewalls** .
Step 2 In the Edge Firewalls table, select the required edge firewall.
Step 3 In the toolbar, choose **Actions > Unassign ASA 1000V**.
Step 4 When prompted, confirm the action.

Verifying VM Registration

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

- ASA 1000V
- InterCloud
- VSG
- VSM

Procedure

Step 1 Choose **Administration > Service Registry > Clients >** *client*.

Step 2 In the table, confirm that the Oper State column contains *registered* for the selected client.

Examining Fault Details

Prime Network Services Controller enables you to examine the faults associated with successfully applied policies and configurations.

To examine faults for compute and edge firewalls, see the following topics:

- Examining Faults for Compute Firewalls, on page 13
- Examining Faults for Edge Firewalls, on page 13

Examining Faults for Compute Firewalls

Prime Network Services Controller enables you to examine faults and configuration errors for compute firewalls.

Before You Begin

Assign the compute firewall to a VSG instance.

Procedure

Step 1 Choose **Resource Management > Managed Resources > root >** *tenant* **> Compute Firewalls**.
The Edit Compute Firewall dialog box is displayed.

Step 2 In the Compute Firewalls table, select the required firewall, then click **Edit**.

Step 3 In the General tab, in the Status area, check the configuration, association, and reachability status.

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

Examining Faults for Edge Firewalls

Prime Network Services Controller enables you to view faults for edge firewalls.

Before You Begin

Assign the edge firewall to an ASA 1000V instance or instantiate an ASA 1000V service VM.

Procedure

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

Step 2 In the Edge Firewalls table, choose the required edge firewall, then click **Edit**.

Step 3 In the General tab, in the Status area, check the configuration, association, and reachability status.

Step 4 In the Faults tab, review the displayed faults. To view additional information about an entry, double-click the entry or select 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 now; 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 > Resources > Services Devices > All ASA 1000Vs**.

Step 2 In the All ASA 1000Vs table, choose the required ASA 1000V, then click **Launch ASDM**.
The ASDM Launch screen opens.

Step 3 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 Pools

Adding a Pool

Procedure

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

Step 2 In the General tab, click **Add Pool**.

Step 3 In the Add Pool dialog box, enter the information as described in the following table, then click **OK**:

Field	Description
Name	Pool 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	Brief pool description. This description can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphens, underscore, dot, and colon.
Pool Members Area	
(Un)Assign	Click to add pool members to or remove pool members from the pool.
Management IP Address	Management IP address of the pool member.
Firewall	Associated compute or edge firewall.
Association State	Association state of the pool member: unassociated, associating, associated, disassociating, or failed.
Service ID	Unique identifier for the pool member.
Operational State	Pool member operational state.

Step 4 (Optional) Assign pool members to the pool by performing the following tasks:

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

b) In the (Un)Assign Pool Member(s) dialog box, select the firewall that you want to assign, and then click the arrow to move it to the Assigned Firewalls list.

c) Click **OK**.

Step 5 Click **OK**.

Assigning a Pool

After you have created a pool, you can assign it to a compute or edge firewall.

Procedure

Step 1 Choose **Resource Management > Managed Resources > root > Compute Firewalls** or **Edge Firewalls**.

Step 2 In the list of firewalls, select the required firewall, then click **Assign Pool**.

Step 3 In the Assign Pool dialog box, either choose a pool from the Name drop-down list or click **Add Pool** to add a new pool.

Step 4 Click **OK**.

Editing a Pool

Procedure

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

Step 2 In the General tab, select the pool that you want to edit, then click **Edit**.

Step 3 In the Edit Pool dialog box, edit the information as required by using the information in the following table, then click **OK**.

Field	Description
Name	Pool name (read-only).
Description	Brief pool description.
Pool Members	
Toolbar	
(Un)Assign	Assigns or unassigns pool members.
Delete	Deletes the selected pool member.
Filter	Filters entries by the string or value that you enter.
Table	
Management IP Address	Management IP address of the pool member.
Firewall	Firewall associated with the pool member.
Association State	Association state of the pool member.
Service ID	Unique identification number for the pool member.
Operational State	Pool member operational state.

Unassigning a Pool

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

Procedure

Step 1 Choose **Resource Management > Managed Resources > root > Compute Firewalls** or **Edge Firewalls**.

Step 2 In the list of firewalls, select the required firewall, then click **Unassign** *object*/**Pool** where *object* is either ASA 1000V or VSG, depending on whether you selected an edge or compute firewall.

Step 3 When prompted, confirm the deletion.

Deleting a Pool

Procedure

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

Step 2 In the General tab, select the pool you want to delete, then click **Delete**.

Step 3 When prompted, confirm the deletion.