



# Configuring Service Policies and Profiles

---

This section includes the following topics:

- [Configuring Service Policies, page 1](#)
- [Working with Profiles, page 36](#)
- [Configuring Security Profiles, page 44](#)
- [Configuring Security Policy Attributes, page 49](#)

## Configuring Service Policies

The following topics describe concepts and options for configuring service policies and policy sets:

- [Configuring ACL Policies and Policy Sets, on page 1](#)
- [Configuring Connection Timeout Policies, on page 8](#)
- [Configuring DHCP Policies, on page 10](#)
- [Configuring IP Audit and IP Audit Signature Policies, on page 13](#)
- [Configuring NAT/PAT Policies and Policy Sets, on page 15](#)
- [Configuring Packet Inspection Policies, on page 19](#)
- [Configuring Routing Policies, on page 21](#)
- [Configuring TCP Intercept Policies, on page 22](#)
- [Configuring Site-to-Site IPsec VPN Policies, on page 23](#)

## Configuring ACL Policies and Policy Sets

The following topics describe how to configure ACL policies and policy sets:

- [Adding an ACL Policy, on page 2](#)
- [Time Ranges in ACL Policy Rules, on page 6](#)

- [Adding an ACL Policy Set, on page 7](#)

## Adding an ACL Policy

VNMC enables you to implement access control lists based on the time of day and frequency, or inclusion in a defined group. Benefits of this feature include:

- Providing closer control of access to network resources throughout the day or week.
- Enhancing policy-based routing and queuing functions.
- Automatically rerouting traffic at specific times of the day to ensure cost-effectiveness.

### Procedure

**Step 1** Choose **Policy Management > Service Policies > root > Policies > ACL > ACL Policies**.

**Step 2** In the General tab, click **Add ACL Policy**.

**Step 3** In the Add ACL Policy dialog box, enter a name and brief description for the policy, then click **Add Rule**.

**Step 4** In the Add Rule dialog box, specify the required information as described in [Add Rule Dialog Box, on page 2](#), then click **OK**.

**Note** All Network Port conditions in a single ACL rule must have the same value selected in the Attribute Value field. For example, you would choose FTP from the Attribute Value drop-down list for all rule conditions that specify the Attribute Name of Network Port.

The Add Rule dialog box contains settings for time rules for ACL policies. For more information about using time ranges with ACL policies, see [Time Ranges in ACL Policy Rules, on page 6](#)

### Add Rule Dialog Box

Field	Description
Name	Rule name.  This name can be between 2 and 32 characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change the name after it is saved.
Description	Brief rule description.  This description can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphens, underscore, dot, and colon.

Field	Description
Action	<ol style="list-style-type: none"> <li>1 Select the action to take if the rule conditions are met: <ul style="list-style-type: none"> <li>• Drop—Drops traffic or denies access.</li> <li>• Permit—Forwards traffic or allows access.</li> <li>• Reset—Resets the connection.</li> </ul> </li> <li>2 Check the <b>Log</b> check box to enable logging.</li> </ol>
Protocol	<p>Specify the protocols to which the rule applies:</p> <ul style="list-style-type: none"> <li>• To apply the rule to any protocol, check the <b>Any</b> check box.</li> <li>• To apply the rule to specific protocols: <ol style="list-style-type: none"> <li>1 Uncheck the <b>Any</b> check box.</li> <li>2 From the Operator drop-down list, choose a qualifier: Equal, Not Equal, Member, Not Member, In range, or Not in range.</li> <li>3 In the Value fields, specify the protocol, object group, or range.</li> </ol> </li> </ul>
EtherType	<p>Specify the encapsulated protocols to be examined for this rule:</p> <ul style="list-style-type: none"> <li>• To examine all encapsulated protocols, check the <b>Any</b> check box.</li> <li>• To examine specific encapsulated protocols: <ol style="list-style-type: none"> <li>1 Uncheck the <b>Any</b> check box.</li> <li>2 From the Operator drop-down list, choose a qualifier: Equal, Not equal, Greater than, Less than, Member, Not Member, In range, or Not in range.</li> <li>3 In the Value fields, specify the hexadecimal value, object group, or hexadecimal range.</li> </ol> </li> </ul>
<b>Time Range Options</b>	
To apply the rule all the time	Check the <b>Always</b> check box.

Field	Description
To apply the rule for a specific time range	<ol style="list-style-type: none"> <li>1 Uncheck the <b>Always</b> check box.</li> <li>2 Check the <b>Range</b> check box.</li> <li>3 In the Absolute Start Time fields, provide the start date and time.</li> <li>4 In the Absolute End Time fields, provide the end date and time.</li> </ol>
To apply the rule on a periodic basis as a member of an object group	<ol style="list-style-type: none"> <li>1 Uncheck the <b>Always</b> check box.</li> <li>2 Check the <b>Pattern</b> check box.</li> <li>3 From the Operator drop-down list, choose <b>range (In range)</b>.</li> <li>4 In the Begin fields: <ol style="list-style-type: none"> <li>1 From the Begin drop-down list, choose the beginning day of the week or the frequency of the time range.</li> <li>2 Choose the beginning hour and minute, and AM or PM.</li> </ol> </li> <li>5 In the End fields: <ol style="list-style-type: none"> <li>1 From the End drop-down list, choose the ending day of the week or frequency. <p><b>Note</b> If you choose a frequency in the Begin drop-down list, choose the same frequency in the End drop-down list. For example, choose <b>Weekdays</b> from both the Begin and End drop-down lists.</p> </li> <li>2 Choose the ending hour and minute, and AM or PM.</li> </ol> </li> </ol>

Field	Description
To apply the rule on a periodic basis, with the frequency you specify	<ol style="list-style-type: none"> <li>1 Uncheck the <b>Always</b> check box.</li> <li>2 Check the <b>Pattern</b> check box.</li> <li>3 From the Operator drop-down list, choose <b>range (In range)</b>.</li> <li>4 In the Begin fields: <ol style="list-style-type: none"> <li>1 From the Begin drop-down list, choose the beginning day of the week or the frequency of the time range.</li> <li>2 Choose the beginning hour and minute, and AM or PM.</li> </ol> </li> <li>5 In the End fields: <ol style="list-style-type: none"> <li>1 From the End drop-down list, choose the ending day of the week or frequency.</li> <li>2 Choose the ending hour and minute, and AM or PM.</li> </ol> </li> </ol> <p><b>Note</b> If you choose a frequency in the Begin drop-down list, choose the same frequency in the End drop-down list. For example, choose Weekdays from both the Begin and End drop-down lists.</p>
<b>Source Conditions</b>	
Add Rule Condition	Click to add a rule condition.
Attribute Name	Name of the attribute.
Operator	Operator for the source condition.
Attribute Value	Value for the source condition.
<b>Destination Conditions</b>	
Add Rule Condition	Click to add a rule condition.
Attribute Name	Name of the attribute.
Operator	Operator for the destination condition.
Attribute Value	Value for the destination condition.

## Time Ranges in ACL Policy Rules

VNMC enables you to configure time ranges for ACL policy rules in either of the following ways:

- By specifying a time range for the ACL policy rule.
- By associating an ACL object group with the ACL policy rule.

VNMC supports the following types of time ranges:

- Periodic—Specified by day-of-week start and end times (such as Sunday to Sunday), or a frequency (such as Daily, Weekdays, or Weekends). Periodic range start and end times also include options for hours and minutes.
- Absolute—Specified by a calendar date and time for start and end times, such as 01 Sep 2012 12:00 AM to 31 Dec 2012 12:00 AM.

For each ACL policy rule, you can have:

- One absolute time range.
- Any number of periodic time ranges, or none.
  - To specify a single periodic time range, add it to an ACL policy rule.
  - To specify multiple periodic time ranges, use an ACL policy object group.

The following figure shows the Time Range fields for an ACL policy rule.

**Figure 1: Time Range Fields in an ACL Policy Rule**

## Adding an ACL Policy Set

### Procedure

- Step 1** Choose **Policy Management > Service Policies > root > Policies > ACL > ACL Policy Sets**.
- Step 2** In the General tab, click **Add ACL Policy Set**.
- Step 3** In the Add ACL Policy Set dialog box, enter the required information as described in the following table, then click **OK**:

Field	Description
Name	Policy set name.  This name can be between 2 and 32 characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is saved.

Field	Description
Description	Brief description of the policy set. This description can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphens, underscore, dot, and colon.
Admin State	Administrative state of the policy: enabled or disabled. This field is not available for all policy sets.
<b>Policies</b>	
Add Policy	Click to add a new policy.
Available	Policies that can be assigned to the policy set. Use the arrows between the columns to move policies between columns.
Assigned	Policies assigned to the policy set.
Up and down arrows	Changes the priority of the selected policies. Arrange the policies from highest to lowest priority, with the highest priority policy at the top of the list.

## Configuring Connection Timeout Policies

VNMC enables you to configure connection timeout policies so that you can establish timeout limits for different traffic types.

After you create a connection timeout policy, you can associate it with an edge profile. For more information, see [Configuring Edge Device Profiles](#), on page 39.

### Procedure

- Step 1** Choose **Policy Management > Service Policies > root > Policies > Connection Timeout**.
- Step 2** In the General tab, click **Add Connection Timeout Policy**.
- Step 3** In the Add Connection Timeout Policy dialog box:
  - a) Enter a policy name and description.



b) Choose whether the administrative status of the policy is to be enabled or disabled.

**Step 4** To add a rule to the policy, click **Add Rule**.

**Step 5** In the Add Connection Timeout Policy Rule dialog box, provide the information as described in [Add Connection Timeout Policy Rule Dialog Box](#), on page 9.

## Add Connection Timeout Policy Rule Dialog Box

**Table 1: Add Connection Timeout Policy Rule Dialog Box**

Field	Description
Name	Policy name.
Description	Brief policy description.
<b>Action</b>	
Idle TCP	Length of time (in days, hours, minutes, and seconds) a TCP connection can remain idle before it is closed.
Half-Closed	Length of time (in days, hours, minutes, and seconds) a half-closed TCP connection can remain idle before it is freed.
Send Reset To Idle Connection	Check the check box to send a reset to the TCP endpoints when a TCP connection times out.
Idle UDP	Length of time (in days, hours, minutes, and seconds) a UDP connection can remain idle before it closes. The duration must be at least one minute, and the default value is two minutes. Enter 0:0:0:0 to disable timeout.
ICMP	Length of time (in days, hours, minutes, and seconds) an ICMP state can remain idle before it is closed.
Protocol	Not available for configuration.
Source Conditions	
Destination Conditions	

## Configuring DHCP Policies

VNMC enables you to create the following DHCP policies and apply them to edge firewalls:

- DHCP relay server policy
- DHCP server policy

These policies can be authored at the organization level and can be applied only to the inside interface of an edge firewall. When they are applied, DHCP policies allow the edge firewall to act either as a DHCP server or a DHCP relay for all VMs in the inside network.

You can apply only one DHCP server or relay profile at a time to the inside interface of the edge firewall.

For more information, see the following topics:

- [Adding a DHCP Relay Server, on page 10](#)
- [Configuring a DHCP Relay Policy, on page 11](#)
- [Configuring a DHCP Server Policy, on page 11](#)

### Adding a DHCP Relay Server

DHCP relay servers are used to forward DHCP requests and replies between clients and servers when they are not on the same physical subnet. In contrast to IP router forwarding, where IP datagrams are switched between networks, DHCP relay servers receive DHCP messages and then generate a new message to send out on a different interface.

#### Procedure

- 
- Step 1** Choose **Policy Management > Service Policies > root > Policies > DHCP > DHCP Relay Server**.
- Step 2** In the General tab, click **Add DHCP Relay Server**.
- Step 3** In the New DHCP Relay Server dialog box, provide the information described in the [Add DHCP Relay Server Dialog Box, on page 10](#), then click **OK**.
- 

#### Add DHCP Relay Server Dialog Box

Field	Description
Name	Relay server name.
Description	Brief description of the relay server.
Relay Server IP	IP address of the relay server.
Interface Name	Interface to use to reach the relay server.

## Configuring a DHCP Relay Policy

VNMC enables you to associate a DHCP relay server with a DHCP relay policy, as described in this procedure.

### Procedure

- 
- Step 1** Choose **Policy Management > Service Policies > root > Policies > DHCP > DHCP Relay**.
- Step 2** In the General tab, click **Add DHCP Relay Policy**.
- Step 3** In the New DHCP Relay Policy dialog box, provide the information described in [Add DHCP Relay Policy Dialog Box, on page 11](#), then click **OK**.
- 

### Add DHCP Relay Policy Dialog Box

Name	Description
Name	Policy name.
Description	Brief policy description.
DHCP Relay Server Assignment	<p>Assign a DHCP relay server in one of the following ways:</p> <ul style="list-style-type: none"><li>• Click <b>Add DHCP Relay Server</b> to add a new DHCP relay server.</li><li>• In the Available Relay Servers list, select one of the available relay servers and move it to the Assigned Relay Servers list</li></ul> <p>You must assign at least one DHCP relay server to the policy.</p>

## Configuring a DHCP Server Policy

A DHCP server policy enables you to define the characteristics of the policy, such as ping and lease timeouts, IP address range, and DNS and WINS settings.

### Procedure

- 
- Step 1** Choose **Policy Management > Service Policies > root > Policies > DHCP > DHCP Server**.
- Step 2** In the General tab, click **Add DHCP Server Policy**.
- Step 3** In the New DHCP Server Policy dialog box, provide the information as described in [Add DHCP Server Policy Dialog Box, on page 12](#), then click **OK**.
-

**Add DHCP Server Policy Dialog Box**

Field	Description
<b>General Tab</b>	
Name	Policy name.
Description	Brief policy description.
Ping Timeout (Milliseconds)	Amount of time (in milliseconds) that the DHCP server waits for a ping reply before it stops attempting to reach a pool address for client assignment.  The valid range is 10 to 10000 milliseconds.
Lease Timeout (seconds)	Amount of time (in seconds) that the DHCP server allocates an IP address to a DHCP client before reclaiming and then reallocating it to another client.  The default value is 3600 seconds.
Edge Firewall Interface Using the DHCP Client for DHCP Server Auto Configuration	To enable DHCP server automatic configuration, enter the name of the edge firewall interface that uses the DHCP client. For ASA 1000V instances, this interface is always an outside interface.  Leaving this field empty indicates that the automatic configuration feature is disabled.
<b>Policies Tab</b>	
DNS Settings	DNS settings used by the edge firewall when configuring DHCP clients.  To add a new entry, click <b>Add DNS Setting</b> and add the required information.
WINS Servers	Windows Internet Naming Service (WINS) name servers that are available to DHCP clients.  To add a new WINS server, click <b>Add WINS Server</b> and enter the WINS server IP address.  WINS servers are listed in the order of preference, with the most preferred WINS server at the top. Select an entry in the table, and then use the arrows above the table to change server priority.

Field	Description
IP Address Range	<p>Enter the following information for the DHCP address pool:</p> <ul style="list-style-type: none"> <li>• Start IP Address—Beginning IP address of the pool.</li> <li>• End IP Address—Ending IP address of the pool.</li> <li>• Subnet Mask—Subnet mask to apply to the address pool.</li> </ul>

## Configuring IP Audit and IP Audit Signature Policies

The IP audit feature provides basic Intrusion Prevention System (IPS) support for ASA 1000V instances. VNMC supports a basic list of signatures, and enables you to configure policies that specify one or more actions to apply to traffic that matches a signature.

The following IP audit policies are available:

- Audit policies
- Signature policies

When you associate an IP audit policy with a device, the policy is applied to all traffic on the outside interface of the device.

The following topics describe how to configure these policies.

### Configuring IP Audit Policies

#### Procedure

- 
- Step 1** Choose **Policy Management > Service Policies > root > Policies > IP Audit > Audit Policies**.
- Step 2** In the General tab, click **Add IP Audit Policy**.
- Step 3** In the Add IP Audit Policy dialog box provide the following information:
- Policy name
  - Policy description
  - In the Admin State field, choose whether the administrative state of the policy is to be enabled or disabled.
- Step 4** To add a rule to the policy, click **Add Rule**.
- Step 5** In the Add IP Audit Policy Rule dialog box, provide the information as described in [Add IP Audit Policy Rule Dialog Box, on page 14](#), then click **OK**.
-

## Add IP Audit Policy Rule Dialog Box

**Table 2: IP Audit Policy Rule Dialog Box**

Field	Description
Name	Rule name.
Description	Brief rule description.
Attack-Class Action	<p>Check the check boxes of the actions to take for signature type Attack if the conditions of the rule are met:</p> <ul style="list-style-type: none"> <li>• Log--Send a message indicating that a packet matched the signature.</li> <li>• Drop--Drop the packet.</li> <li>• Reset Flow--Drop the packet and reset the connection.</li> </ul>
Information-Class Action	<p>Check the check boxes of the actions to take for signature type Informational if the conditions of the rule are met:</p> <ul style="list-style-type: none"> <li>• Log--Send a message indicating that a packet matched the signature.</li> <li>• Drop--Drop the packet.</li> <li>• Reset Flow--Drop the packet and reset the connection.</li> </ul>
Protocol	Not available for configuration.
Source Conditions	
Destination Conditions	

## Configuring IP Audit Signature Policies

An IP audit signature policy identifies the signatures that are enabled and disabled. By default, all signatures are enabled. You can disable a signature when legitimate traffic matches the signature in most situations, resulting in false alarms. However, disabling the signature is performed at a global level, meaning that no traffic will trigger the signature (even bad traffic) when it is disabled.

### Procedure

- 
- Step 1** Choose **Policy Management > Service Policies > root > Policies > IP Audit > Signature Policies**.
- Step 2** In the General tab, click **Add IP Audit Signature Policy**.
- Step 3** In the Add IP Audit Signature Policy dialog box, enter a name and description for the policy.
- Step 4** In the Signatures area, move signatures between the Enabled Signatures and Disabled Signatures lists as required.
- Note** We recommend that you do not disable signatures unless you are sure you understand the consequences of doing so.
- You can view additional information about a signature by selecting the required signature and clicking **Properties**.
- Step 5** After you have made all adjustments, click **OK**.
- 

## Configuring NAT/PAT Policies and Policy Sets

VNMC supports Network Address Translation (NAT) and Port Address Translation (PAT) policies for controlling address translation in the deployed network. These policies support both static and dynamic translation of IP addresses and ports.

VNMC enables you to configure the following policy items:

- NAT policy—Can contain multiple rules, which are evaluated sequentially until a match is found.
- NAT policy set—Group of NAT policies that can be associated with an edge security profile. When the profile is applied, the NAT policies are applied only to ingress traffic.
- PAT policy—Supports source dynamic and destination static interface PAT on edge firewalls.

The following topics describe how to configure NAT and PAT policies, and NAT policy sets.

### Configuring NAT/PAT Policies

This procedure describes how to configure NAT/PAT policies with VNMC.

#### Procedure

- 
- Step 1** Choose **Policy Management > Service Policies > root > Policies > NAT > NAT Policies**.
- Step 2** In the General tab, click **Add NAT Policy**.
- Step 3** In the Add NAT Policy dialog box, enter a name and description for the policy.
- Step 4** In the Admin State field, indicate whether the administrative state of the policy is to be enabled or disabled.
- Step 5** To add a rule to the policy, click **Add Rule**.
- Step 6** In the Add NAT Policy Rule dialog box (see [Add NAT Policy Rule Dialog Box, on page 16](#), provide the information as described in [Add NAT Policy Rule Dialog Box, on page 16](#), then click **OK**.
-

## Add NAT Policy Rule Dialog Box

**Figure 2: Add NAT Policy Rule Dialog Box**

## Add NAT Policy Rule Dialog Box

**Table 3: Add NAT Policy Rule Dialog Box**

Field	Description
Name	Rule name.
Description	Brief rule description.
<b>Original Packet Match Conditions</b>	
Source Match Conditions	<p>Source attributes that must be matched for the current policy to apply.</p> <p>To add a new condition, click <b>Add Rule Condition</b>.</p> <p>Available source attributes are IP Address and Network Port.</p>



Field	Description
Destination Match Conditions	<p>Destination attributes that must be matched for the current policy to apply.</p> <p>To add a new condition, click <b>Add Rule Condition</b>.</p> <p>Available destination attributes are IP Address and Network Port.</p>
Protocol	<p>Specify the protocols to which the rule applies:</p> <ul style="list-style-type: none"> <li>To apply the rule to any protocol, check the <b>Any</b> check box.</li> <li>To apply the rule to specific protocols: <ol style="list-style-type: none"> <li>1 Uncheck the <b>Any</b> check box.</li> <li>2 From the Operator drop-down list, choose a qualifier: Equal, Not equal, Member, Not Member, In range, or Not in range.</li> <li>3 In the Value fields, specify the protocol, object group, or range.</li> </ol> </li> </ul>
<b>NAT Action Table</b>	
NAT Action	From the drop-down list, choose the required translation option: Static or Dynamic.
Translated Address	<p>Identify a translated address pool for each original packet match condition from the following options:</p> <ul style="list-style-type: none"> <li>Source IP Pool</li> <li>Source Port Pool</li> <li>Source IP PAT Pool</li> <li>Destination IP Pool</li> <li>Destination Port Pool</li> </ul> <p>For example, if you specify a source IP address match condition, you must identify a Source IP Pool object group. Similarly, a destination network port match requires a Destination Port Pool object group.</p> <p>The Source IP PAT Pool option is available only if you choose dynamic translation.</p> <p>Click <b>Add Object Group</b> to add object groups for the translation actions.</p>

Field	Description
NAT Options	<p>Check the check box to enable the feature:</p> <ul style="list-style-type: none"> <li>• Enable Bidirectional--Whether or not connections can be initiated bidirectionally; that is, both to and from the host. Available only for static address translation.</li> <li>• Enable DNS--Whether or not DNS is enabled for NAT.</li> <li>• Enable Round Robin IP--Whether or not IP addresses are allocated on a round-robin basis. Available only for dynamic address translation.</li> </ul>

## Configuring NAT Policy Sets

Policy sets enable you to group multiple policies of the same type (such as NAT, ACL, or Interface) for inclusion in a profile. NAT policy sets are groups of NAT policies that can be associated with an edge security profile.

### Procedure

- 
- Step 1** Choose **Policy Management > Service Policies > root > Policies > NAT > NAT Policy Sets**.
- Step 2** In the General tab, click **Add NAT Policy Set**.
- Step 3** In the Add NAT Policy Set dialog box, enter a name and description for the policy set.
- Step 4** In the Admin State field, indicate whether the administrative status of the policy is to be enabled or disabled.
- Step 5** In the Policies area, select the policies to include in this policy set:
- In the Available list, select one or more policies and move them to the Assigned list.
  - Adjust the priority of the assigned policies by using the arrow keys above the list.
  - If required, click **Add NAT Policy** to add a new policy and include it in the Assigned list.
- For information on configuring a NAT policy, see [Configuring NAT/PAT Policies, on page 15](#).
- Step 6** Click **OK**.
- 

## Configuring PAT for Edge Firewalls

VNMC enables you to configure source and destination interface PAT for edge firewalls, such as the ASA 1000V. For more information, see the following topics.

### Configuring Source Dynamic Interface PAT

VNMC enables you to configure source dynamic interface PAT for edge firewalls, such as ASA 1000Vs.

### Procedure

- 
- Step 1** Choose **Policy Management > Service Policies > root > Policies > NAT > NAT Policies**.
- Step 2** In the General tab, click **Add NAT Policy**.
- Step 3** In the Add NAT Policy dialog box, enter a name and description for the policy.
- Step 4** In the Admin State field, indicate whether the administrative state of the policy is to be enabled or disabled.
- Step 5** Click **Add Rule** to add a rule to this policy.
- Step 6** In the Add NAT Policy Rule dialog box, provide the information described in [Add NAT Policy Rule Dialog Box, on page 16](#) with the following specific settings:
- a) From the NAT Action drop-down list, choose **Dynamic**.
  - b) In the Translated Address area, add a Source IP Pool object group that contains the ASA 1000V outside interface IP address.
- Step 7** Click **OK**.
- 

### Configuring Destination Static Interface PAT

VNMC enables you to configure destination static interface PAT for edge firewalls, such as ASA 1000Vs, as described in the following procedure.

### Procedure

- 
- Step 1** Choose **Policy Management > Service Policies > root > Policies > NAT > NAT Policies**.
- Step 2** In the General tab, click **Add NAT Policy**.
- Step 3** In the Add NAT Policy dialog box, enter a name and description for the policy.
- Step 4** In the Admin State field, indicate whether the administrative state of the policy is to be enabled or disabled.
- Step 5** Click **Add Rule** to add a rule to this policy.
- Step 6** In the Add NAT Policy Rule dialog box, enter the IP address of the ASA 1000V outside interface as a rule condition for Destination Match Conditions.
- Step 7** Configure other options in the Add NAT Policy Rule dialog box as described in [Add NAT Policy Rule Dialog Box, on page 16](#).
- Note** If any of the IP address fields includes a range that starts or ends with the IP address of the outside interface of the ASA 1000V, an error message will be displayed that identifies and overlap with the ASA 1000V interface IP address.
- Step 8** Click **OK**.
- 

## Configuring Packet Inspection Policies

VNMC enables you to configure policies for application-layer protocol inspection. Inspection is required for services that embed IP addressing information in the user data packet, or that open secondary channels on

dynamically assigned ports. When inspection is configured, the end device performs a deep packet inspection instead of quickly passing the packet on. As a result, inspection can affect overall device throughput.

[Protocols Supported for Packet Inspection Policies, on page 20](#) lists the application-layer protocols supported by VNMC.

## Procedure

- 
- Step 1** Choose **Policy Management > Service Policies > root > Policies > Packet Inspection**.
- Step 2** In the General tab, click **Add Packet Inspection Policy**.
- Step 3** In the Add Packet Inspection Policy dialog box, enter a name and description for the policy.
- Step 4** In the Admin State field, indicate whether the administrative status of the policy is enabled or disabled.
- Step 5** To add a rule to the policy, click **Add Rule**.
- Step 6** In the Add Packet Inspection Policy Rule Dialog box, provide the information as described in [Add Packet Inspection Policy Rule Dialog Box, on page 20](#), then click **OK**.
- 

## Protocols Supported for Packet Inspection Policies

### Protocols Supported for Packet Inspection Policies

CTIQBE	ICMP	PPTP	SQLNet
DCE/RPC	ICMP Error	RSH	SunRPC
DNS	ILS	RSTP	TFTP
FTP	IP Options	SIP	WAAS
H323 H225	IPsec Pass-Through	Skinny	XDMCP
H323 RAS	MGCP	SMTP	
HTTP	NetBIOS	SNMP	

## Add Packet Inspection Policy Rule Dialog Box

*Table 4: Add Packet Inspection Policy Rule Dialog Box*

Field	Description
Name	Rule name.
Description	Brief rule description.

Field	Description
Action	In the Enable Inspection fields, check the check boxes of protocols to be inspected if the rule conditions are met.
Protocol	Not available for configuration.
Source Conditions	
Destination Conditions	

## Configuring Routing Policies

VNMC enables you to use routing policies to configure static routes for managed endpoints on an edge firewall.



### Note

You can configure only inside and outside interfaces on edge firewalls by using VNMC. Use the CLI to configure routes on the edge firewall management interface.

After you configure a static route routing policy, you can implement the policy by:

- Including the routing policy in an edge device profile.
- Applying the edge device profile to an edge firewall that has managed endpoints.

### Procedure

- Step 1** Choose **Policy Management > Service Policies > root > Policies > Routing**.
- Step 2** In the General tab, click **Add Routing Policy**.
- Step 3** In the Add Routing Policy dialog box, enter a name and brief description for the routing policy.
- Step 4** To add a new static route, click **Add Static Route**.
- Step 5** In the Add Static Route dialog box, enter the following information:
  - a) In the Destination Network fields, enter the IP route prefix and prefix mask for the destination.
  - b) In the Forwarding (Next Hop) fields, enter the IP address of the next hop that can be used to reach the destination network.
 

**Note** The Forwarding Interface field applies only to ASA 1000V data interfaces. Use the CLI to configure routes on the ASA 1000V management interface.
  - c) (Optional) In the Distance Metric field, enter the distance metric.
- Step 6** Click **OK**.

## Configuring TCP Intercept Policies

VNMC enables you to configure TCP intercept policies that you can then associate with an edge security profile. TCP intercept policies that you associate with a device via an edge security profile are applied to all traffic on the outside interface of the device.

### Procedure

- 
- Step 1** Choose **Policy Management > Service Policies > root > Policies > TCP Intercept**.
  - Step 2** In the General tab, click **Add TCP Intercept Policy**.
  - Step 3** In the Add TCP Intercept Policy dialog box, enter a name and brief description for the policy.
  - Step 4** In the Admin State field, indicate whether the administrative status of the policy is to be enabled or disabled.
  - Step 5** To add a rule to the policy, click **Add Rule**.
  - Step 6** In the Add TCP Intercept Policy Rule dialog box, provide the information as described in [Add TCP Intercept Policy Rule Dialog Box](#), on page 22.
- 

### Add TCP Intercept Policy Rule Dialog Box

Field	Description
Name	Rule name.
Description	Brief rule description.
Maximum Number of Embryonic TCP Connections (0-65535)	<p>Number of embryonic TCP connections allowed overall and per client:</p> <ol style="list-style-type: none"> <li>1 In the Total field, enter the maximum number of embryonic TCP connections allowed.</li> <li>2 In the client field, enter the maximum number of embryonic TCP connections allowed per client.</li> </ol> <p>The default value 0 (zero) indicates unlimited connections.</p>
Protocol	Not available for configuration.
Source Conditions	
Destination Conditions	

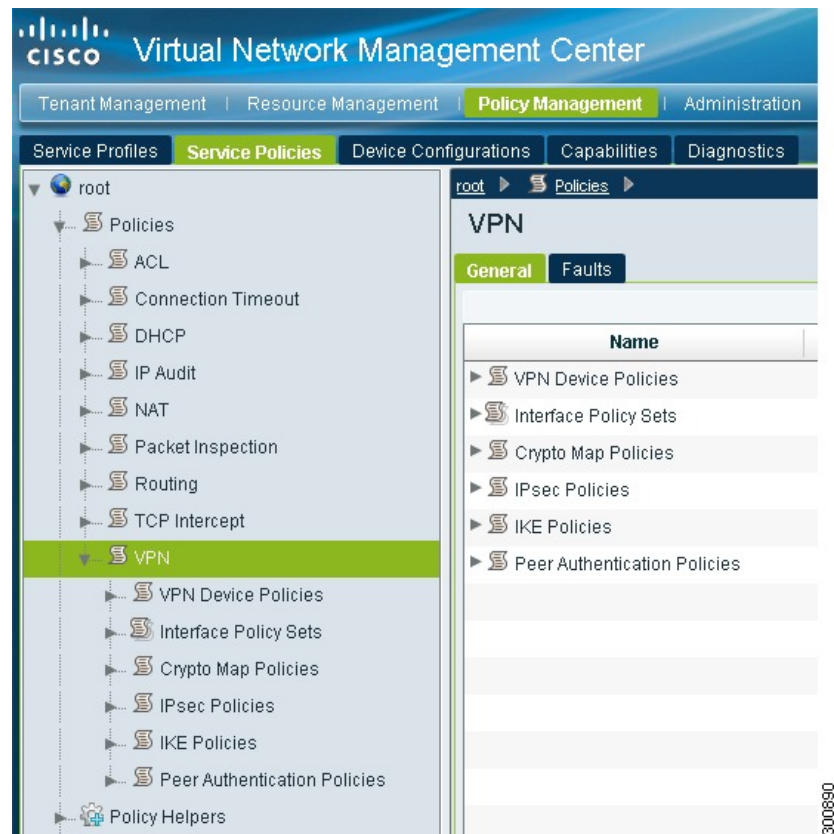
## Configuring Site-to-Site IPsec VPN Policies

VNMC enables you to configure site-to-site IPsec VPNs. In addition, you can configure a crypto map policy and attach it to an edge profile. For ease of configuration and to keep logical IPsec entities separate, configuration is divided into the following sections:

- Configuring Crypto Map Policies
- Configuring IKE Policies
- Configuring Interface Policy Sets
- Configuring IPsec Policies
- Configuring Peer Authentication Policies
- Configuring VPN Device Policies

To access VPN policies, choose **Policy Management > Service Policies > root > Policies > VPN** as shown in the following figure.

**Figure 3: VPN Policies in VNMC**



## Configuring Crypto Map Policies

VNMC enables you to create crypto map policies that include:

- Rules for source and destination conditions.
- IP Security (IPsec) options, including an IPsec policy.
- Internet Key Exchange (IKE) options, including a peer device.

Crypto map policies are applied to interfaces by means of their inclusion in interface policy sets and edge security policies.

### Procedure

- 
- Step 1** Choose **Policy Management > Service Policies > root > Policies > VPN > Crypto Map Policies**.
- Step 2** In the General tab, click **Add Crypto Map Policy**.
- Step 3** In the Add Crypto Map Policy dialog box, provide the information as described in [Add Crypto Map Policy Dialog Box](#), on page 24, then click **OK**.
- Step 4** To add a policy rule, click **Add Rule** in the General tab and provide the required information as described in [Add Crypto Map Policy Rule Dialog Box](#), on page 26.
- 

### Add Crypto Map Policy Dialog Box

Field	Description
<b>General Tab</b>	
Name	Policy name.
Description	Brief policy description.
Admin State	Whether the administrative status of the policy is enabled or disabled.
<b>Rule Table</b>	
Add Rule	Click <b>Add Rule</b> to add a new rule to the current policy.
<b>IPsec Settings Tab</b>	
SA Lifetime	Length of time (in days, hours, minutes, and seconds) that a security association (SA) lives before expiring.



Field	Description
SA Lifetime Traffic (KB)	Volume of traffic, in kilobytes, that can pass between IPsec peers using a given SA before that association expires.
Enable Perfect Forwarding Secrecy	<p>Whether or not Perfect Forward Secrecy (PFS) is enabled.</p> <p>PFS is a cryptographic characteristic associated with a derived shared secret value. With PFS, if one key is compromised, previous and subsequent keys are not compromised, because subsequent keys are not derived from previous keys.</p>
Diffie-Hellman Group	<p>Available if PFS is enabled.</p> <p>Choose the Diffie-Hellman (DH) group for this policy:</p> <ul style="list-style-type: none"> <li>• Group 1--The 768-bit DH group.</li> <li>• Group 2--The 1024-bit DH group.</li> <li>• Group 5--The 1536-bit DH group.</li> </ul>
IPsec Policies	<p>The IPsec policy that applies to the current policy.</p> <p>Select an existing IPsec policy or click <b>Add IPsec Policy</b> to create a new policy.</p>
Peer Device	<p>Peer device.</p> <p>Choose an existing peer or click <b>Add Peer Device</b> to add a new peer.</p> <p>In the Add Peer Device dialog box, enter the peer device IP address or hostname.</p>
<b>Other Settings Tab</b>	
Enable NAT Traversal	Whether or not IPsec peers can establish a connection through a NAT device.
Enable Reverse Route Injection	Whether or not static routes are automatically added to the routing table and then announced to neighbors on the private network.

Field	Description
Connection Type	<p>Connection type for this policy:</p> <ul style="list-style-type: none"> <li>• Answer-Only--Responds only to inbound IKE connections during the initial proprietary exchange to determine the appropriate peer to which to connect.</li> <li>• Bidirectional--Accepts and originates connections based on this policy.</li> <li>• Originate-Only--Initiates the first proprietary exchange to determine the appropriate peer to which to connect.</li> </ul>
Negotiation Mode	<p>Mode to use for exchanging key information and setting up SAs:</p> <ul style="list-style-type: none"> <li>• Aggressive Mode--Faster mode, using fewer packets and exchanges, but does not protect the identity of the communicating parties.</li> <li>• Main Mode--Slower mode, using more packets and exchanges, but protects the identities of the communicating parties.</li> </ul>
DH Group for Aggressive Mode	DH group to use when in aggressive mode: Group 1, Group 2, or Group 5.

### Add Crypto Map Policy Rule Dialog Box

Field	Description
Name	Rule name.
Description	Brief rule description.
VPN Action	Action to take based on this rule: Permit or Deny.

Field	Description
Protocol	<p>Protocols to examine for this rule:</p> <ul style="list-style-type: none"> <li>To examine all protocols, check the <b>Any</b> check box.</li> <li>To examine specific protocols: <ol style="list-style-type: none"> <li>1 Uncheck the <b>Any</b> check box.</li> <li>2 From the Operator drop-down list, choose a qualifier: Equal, Not equal, Member, Not Member, In range, or Not in range.</li> <li>3 In the Value fields, specify the protocol, object group, or range.</li> </ol> </li> </ul>
Source Conditions	<p>Source attributes that must be matched for the rule to apply.</p> <p>To add a new condition, click <b>Add Rule Condition</b>.</p> <p>Available source attributes are IP Address and Network Port.</p>
Destination Conditions	<p>Destination attributes that must be matched for the rule to apply.</p> <p>To add a new condition, click <b>Add Rule Condition</b>.</p> <p>Available destination attributes are IP Address and Network Port.</p>

## Configuring IKE Policies

The Internet Key Exchange (IKE) protocol is a hybrid protocol that implements Oakley and SKEME key exchanges inside the Internet Security Association and Key Management Protocol (ISAKMP) framework. The initial IKE implementation used the IPsec protocol, but IKE can be used with other protocols. IKE provides authentication of the IPsec peers, negotiates IPsec keys, and negotiates the IPsec Security Associations (SAs).

### Procedure

- 
- Step 1** Choose **Policy Management > Service Policies > root > Policies > VPN > IKE Policies**.
- Step 2** In the General tab, click **Add IKE Policy**.
- Step 3** In the Add IKE Policy dialog box, enter a name and description for the policy.
- Step 4** Configure either an IKE V1 or IKE V2 policy:
- IKE V1 Policy
    - 1 Click **Add IKE V1 Policy**.

- 2 In the Add IKE V1 Policy dialog box, provide the information described in [IKE V1 Policy Dialog Box](#), on page 28, then click **OK**.
- IKE V2 Policy
    - 1 Click **Add IKE V2 Policy**.
    - 2 In the Add IKE V2 Policy dialog box, provide the information described in [IKE V2 Policy Dialog Box](#), on page 28, then click **OK**.

**Step 5** Click **OK**.

---

### IKE V1 Policy Dialog Box

Field	Description
DH Group	Diffie-Hellman group: Group 1, Group 2, or Group 5.
Encryption	Encryption method: 3DES, AES, AES-192, AES-256, or DES.
Hash	Hash algorithm: MD5 or SHA.
Authentication	Authentication method is Preshared key.
SA Lifetime	Length of time (in days, hours, minutes, and seconds) that an SA lives before expiring.

### IKE V2 Policy Dialog Box

Field	Description
DH Group	Diffie-Hellman group: Group 1, Group 2, Group 5, or Group 14.
Encryption	Encryption method: 3DES, AES, AES-192, AES-256, or DES.
Hash	Hash integrity algorithm: MD5, SHA, SHA256, SHA384, or SHA512.
Pseudo Random Function Hash	Pseudo-random function (PRF) has algorithm: MD5, SHA, SHA256, SHA384, or SHA512.

Field	Description
SA Lifetime	Length of time (in days, hours, minutes, and seconds) that an SA lives before expiring.

## Configuring Interface Policy Sets

Interface policy sets enable you to group multiple policies for inclusion in an edge security profile.

### Procedure

- 
- Step 1** Choose **Policy Management > Service Policies > root > Policies > VPN > Interface Policy Sets**.
- Step 2** In the General tab, click **Add Interface Policy Set**.
- Step 3** In the Add Interface Policy Set dialog box, provide the information as described in [Add Interface Policy Set Dialog Box](#), on page 29, then click **OK**.
- 

### Add Interface Policy Set Dialog Box

#### General Tab

Field	Description
Name	Policy set name.
Description	Brief description of the policy set.
Admin State	Administrative state of the policy set: enabled or disabled.
<b>Policies Area</b>	
Add Crypto Map Policy	Click to add a new policy.
Available	Policies that can be assigned to the policy set. Use the arrows between the columns to move policies between columns.
Assigned	Policies assigned to the policy set.
Up and down arrows	Changes the priority of the selected policies. Arrange the policies from highest to lowest priority, with the highest priority policy at the top of the list.

**Domain Settings Tab**

Field	Description
Enable IKE (Must check at least one)	Check the appropriate check box to specify IKE V1 or IKE V2.
Enable IPsec Pre-fragmentation	Check the check box to fragment packets before encryption. Pre-fragmentation minimizes post-fragmentation (fragmentation after encryption) and the resulting reassembly before decryption, thereby improving performance.
Do Not Fragment	<p>Available only if the Enable IPsec Pre-fragmentation check box is checked.</p> <p>From the drop-down list, choose the action to take with the Don't Fragment (DF) bit in the encapsulated header:</p> <ul style="list-style-type: none"> <li>• Clear</li> <li>• Copy</li> <li>• Set</li> </ul>

**Configuring IPsec Policies**

IPsec policies define the IPsec policy objects used to create a secure IPsec tunnel for a VPN.

**Procedure**

- 
- Step 1** Choose **Policy Management > Service Policies > root > Policies > VPN > IPsec Policies**.
- Step 2** In the General tab, click **Add IPsec Policy**.
- Step 3** In the Add IPsec Policy dialog box, enter a name and description for the policy. You must configure either an IKE V1 or IKE V2 proposal for an IPsec policy.
- Step 4** To configure an IKE V1 proposal:
- In the IKE v1 Proposal Table area, click **Add IPsec IKEv1 Proposal**.
  - In the IPsec IKEv1 Proposal dialog box, provide the information described in [IPsec IKEv1 Proposal Dialog Box, on page 31](#), then click **OK**.
- Step 5** To configure an IKE V2 proposal:
- In the IKE v2 Proposal Table area, click **Add IPsec IKE v2 Proposal**.
  - In the IPsec IKEv2 Proposal dialog box, provide the information described in [IPsec IKEv2 Proposal Dialog Box, on page 32](#), then click **OK**.
- Step 6** Click **OK** to save the policy.
-

**IPsec IKEv1 Proposal Dialog Box**

Field	Description
Mode	<p>Mode in which the IPsec tunnel operates.</p> <p>In Tunnel mode, the IPsec tunnel encapsulates the entire IP packet.</p>
ESP Encryption	<p>Encapsulating Security Protocol (ESP) encryption method:</p> <ul style="list-style-type: none"> <li>• 3DES—Encrypts three times according to the Data Encryption Standard (DES) using 56-bit keys.</li> <li>• AES—Encrypts according to the Advanced Encryption Standard (AES) using 128-bit keys.</li> <li>• AES-192—Encrypts according to the AES using 192-bit keys.</li> <li>• AES-256—Encrypts according to the AES using 256-bit keys.</li> <li>• DES—Encrypts according to the DES using 56-bit keys.</li> <li>• Null—Null encryption algorithm. Transform sets defined with ESP-Null provide authentication without encryption; this method is typically used for testing purposes only.</li> </ul>
ESP Authentication	<p>Hash authentication algorithm:</p> <ul style="list-style-type: none"> <li>• MD5—Produces a 128-bit digest.</li> <li>• Null—Does not perform authentication.</li> <li>• SHA—Produces a 160-bit digest.</li> </ul>

**IPsec IKEv2 Proposal Dialog Box**

Field	Description
ESP Encryption Algorithm Table	<p>To add an ESP encryption method:</p> <ol style="list-style-type: none"> <li>1 Click <b>Add ESP Encryption Algorithm</b>.</li> <li>2 From the ESP Encryption drop-down list, choose the encryption method: <ul style="list-style-type: none"> <li>• 3DES—Encrypts three times according to the Data Encryption Standard (DES) using 56-bit keys.</li> <li>• AES—Encrypts according to the Advanced Encryption Standard (AES) using 128-bit keys.</li> <li>• AES-192—Encrypts according to the AES using 192-bit keys.</li> <li>• AES-256—Encrypts according to the AES using 256-bit keys.</li> <li>• DES—Encrypts according to the DES using 56-bit keys.</li> <li>• Null—Null encryption algorithm. Transform sets defined with ESP-Null provide authentication without encryption; this method is typically used for testing purposes only.</li> </ul> </li> </ol>
Integrity Algorithm Table	<p>To add an integrity algorithm:</p> <ol style="list-style-type: none"> <li>1 Click <b>Add Integrity Algorithm</b>.</li> <li>2 From the Integrity Algorithm drop-down list, choose the authentication algorithm: <ul style="list-style-type: none"> <li>• MD5—Produces a 128-bit digest.</li> <li>• Null—Does not perform authentication.</li> <li>• SHA—Produces a 160-bit digest.</li> </ul> </li> </ol>

**Configuring Peer Authentication Policies**

Use a peer authentication policy to define the method used to authenticate a peer.



## Procedure

- 
- Step 1** Choose **Policy Management > Service Policies > root > Policies > VPN > Peer Authentication**.
- Step 2** In the General tab, click **Add Peer Authentication Policy**.
- Step 3** In the Add Peer Authentication Policy dialog box, enter a name and description for the policy.
- Step 4** Click **Add Policy to Authenticate Peer**.
- Step 5** In the Add Policy to Authenticate Peer dialog box, provide the information described in [Add Policy to Authenticate Peer Dialog Box](#), on page 33, then click **OK**.
- Step 6** Click **OK** to save the policy.
- 

### Add Policy to Authenticate Peer Dialog Box

Field	Description
Peer Device (Unique)	Unique IP address or hostname of the peer.
<b>IKEv1 Area</b>	
Local	Preshared key.
Confirm	Preshared key for confirmation.
Set	Whether or not the preshared key has been set and is properly configured (read-only).
<b>IKEv2 Area</b>	
Local	Local preshared key.
Confirm	Local preshared key for confirmation.
Set	Whether or not the local preshared key has been set and is properly configured (read-only).
Remote	Remote preshared key.
Confirm	Remote preshared key for confirmation.
Set	Whether or not the remote preshared key has been set and is properly configured (read-only).

## Configuring VPN Device Policies

A VPN device policy enables you to specify VPN global settings, such as:

- IKE policy
- IKE global settings
- IPsec global settings
- Peer authentication policy

### Procedure

- 
- Step 1** Choose **Policy Management > Service Policies > root > Policies > VPN > VPN Device Policies**.
- Step 2** In the General tab, click **Add VPN Device Policy**.
- Step 3** In the Add VPN Device Policy dialog box, provide the information as described in [Add VPN Device Policy Dialog Box](#), on page 34.
- Step 4** As needed, provide the information described in the following tables:
- [Configuring IKE Policies](#), on page 27
  - [Configuring Peer Authentication Policies](#), on page 32
- Step 5** Click **OK** to create the policy.
- 

### Add VPN Device Policy Dialog Box

#### General Tab



**Note** A VPN device policy requires both an IKE policy and a peer authentication policy.

Field	Description
Name	Policy name.
Description	Brief policy description.
IKE Policy	Choose an existing policy from the drop-down list, or click <b>Add IKE Policy</b> to add a new policy.
Peer Authentication Policy	Choose an existing policy from the drop-down list, or click <b>Add Peer Authentication Policy</b> to add a new policy.

**IKE Settings Tab**

Field	Description
Enable IPsec over TCP	Whether or not IPsec traffic is allowed over TCP. If IPsec over TCP is enabled, this method takes precedence over all other connection methods.
Send Disconnect Notification	Whether or not clients are notified that sessions will be disconnected.
Allow Inbound Aggressive Mode	Whether or not inbound aggressive mode is permitted.
Wait for Termination before Rebooting	Whether or not a reboot can occur only when all active sessions have terminated voluntarily.
Threshold for Cookie Challenge (0-100 Percent)	Percentage of the maximum number of allowed Security Associations (SAs) that can be in-negotiation (open) before cookie challenges are issued for future SA negotiations.
Negotiation Threshold for Maximum SAs (0-100 Percent)	Percentage of the maximum number of allowed SAs that can be in-negotiation before additional connections are denied.  The default value is 100 percent.
IKE Identity	Phase 2 identification method: <ul style="list-style-type: none"> <li>• Automatic--Determines ISAKMP negotiation by connection type: <ul style="list-style-type: none"> <li>◦ IP address for a preshared key.</li> <li>◦ Cert DN for certificate authentication.</li> </ul> </li> <li>• IP Address--IP address of the host exchanging ISAKMP identity information.</li> <li>• Hostname--Fully qualified domain name of the host exchanging ISAKMP identity information.</li> <li>• Key ID--String used by the remote peer to look up the preshared key.</li> </ul>
Key for IKE Identity	The key to use for IKE identify if the IKE identification method is Key ID.
NAT Traversal	Whether or not IPsec peers can establish a connection through a NAT device.

Field	Description
Keep-Alive Time for NAT Traversal	Length of time (in hours, minutes, and seconds) that a tunnel can exist with no activity before the device sends keepalive messages to the peer.  Values range from 10 to 3600 seconds, with a default of 20 seconds.
IKE Version 2 Maximum Security Associations	Whether or not the total number of IKE V2 SAs on the node can be set.
Maximum number of SA	Maximum number of SA connections allowed.
IKE V1 over TCP Port Table	<ol style="list-style-type: none"> <li>1 Click <b>Add IKE V1 Over TCP Port</b> to add a new port.</li> <li>2 In the Port field, enter the TCP port to use for IKE V1.</li> </ol>

#### IPsec Settings Tab

Field	Description
Anti Replay	Whether or not SA anti-replay is enabled.
Anti Replay Window Size	Window size to use to track and prevent duplication of packets. Using a larger window size allows the decryptor to track more packets.
SA Lifetime	Length of time (in days, hours, minutes, and seconds) that an SA can live before expiring.
SA Lifetime Volume (KB)	Volume of traffic, in kilobytes, that can pass between IPsec peers using a given SA before the association expires.

## Working with Profiles

A profile is a collection of policies. By creating a profile with policies that you select, and then applying that profile to multiple objects, such as edge firewalls, you can ensure that those objects have consistent policies.

A device must be registered to VNMC before you can apply a profile to it.

VNMC enables you to create and apply the following types of profiles:

- Compute security profiles—Compute firewall profiles that include ACL policies and user-defined attributes.

- Edge device profiles—Edge firewall profiles that include routing, VPN, DHCP, and IP Audit policies.
- Edge security profiles—Edge firewall profiles that include access and threat mitigation policies.

The following topics describe how to configure and apply profiles.

## Configuring Compute Security Profiles

VNMC enables you to create compute security profiles at the root or tenant level. Creating a compute security profile at the root level enables you to apply the same profile to multiple tenants.

### Procedure

- 
- Step 1** Choose **Policy Management > Service Profiles > root > Compute Firewall > Compute Security Profiles**.
- Step 2** In the General tab, click **Add Compute Security Profile**.
- Step 3** In the Add Compute Security Profile dialog box, provide the information as described in [Add Compute Security Profile Dialog Box, on page 37](#), then click **OK**.
- 

### Add Compute Security Profile Dialog Box

#### General Tab

Field	Description
Name	Profile name.  This name can be between 2 and 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is saved.
Description	Brief profile description.  This description can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphens, underscore, dot, and colon.
Policy Set	Drop-down list of policy sets.
Add ACL Policy Set	Click the link to add an ACL policy set.
Resolved Policy Set	Click the link to edit the resolved policy set.
<b>Resolved Policies Area</b>	
(Un)assign Policy	Click the link to assign or unassign a policy.

Field	Description
Name	Rule name.
Source Condition	Source condition for the rule.
Destination Condition	Destination condition for the rule.
Protocol	Protocol to which the rule applies.
EtherType	Encapsulated protocol to which the rule applies.
Action	Action to take if the rule conditions are met.
Description	Rule description.

**Attributes Tab**

Field	Description
Add User Defined Attribute	Opens a dialog box for adding an attribute.
Name	Attribute name.
Value	Attribute value.

## Verifying Compute Firewall Policies

Use this procedure to verify active policies and optionally modify policy objects for compute firewalls.

**Procedure**

- 
- Step 1** Choose **Resource Management > Managed Resources > root > tenant > Compute Firewalls > compute-firewall**.
  - Step 2** In the Compute Security Profiles tab, select the required policy, then click **Show Resolved Policies**.
  - Step 3** In the Edit dialog box, click the required policy in the Resolved Policies table to view the policy details, such as source and destination conditions.
  - Step 4** To modify a policy, in the Policy Set area, either choose a different policy from the drop-down list, or click **Add ACL Policy Set** to configure a new policy.
  - Step 5** Click **Apply** to accept any changes or **OK** when you have finished reviewing the policies.
-

## Configuring Edge Device Profiles

Edge device profiles contain the following policies in addition to a timeout value for address translation:

- DHCP
- IP audit signature
- Routing
- VPN device

You can create an edge device profile at any level of the organization hierarchy (root, tenant, virtual data center (VDC), app, or tier). Creating an edge device profile at the root level enables you to apply it to multiple edge firewalls for different tenants.

### Procedure

- 
- Step 1** Choose **Policy Management > Service Profiles > root > Edge Firewall > Edge Device Profiles**.
- Step 2** In the General tab, click **Add Edge Device Profile**.
- Step 3** In the Add Edge Device Profile dialog box, enter the information as described in [Edge Device Profile Dialog Box](#), on page 39, then click **OK**.
- 

### Edge Device Profile Dialog Box

Field	Description
<b>General Tab</b>	
Name	Profile name.
Description	Brief profile description.
<b>Policies Tab</b>	
Routing Policy	Choose an existing policy or click <b>Add Routing Policy</b> to add a new policy.  Click the Resolved Policy link to review or modify the assigned policy.
IP Audit Signature Policy	Choose an existing policy or click <b>Add IP Audit Signature Policy</b> to add a new policy.  Click the Resolved Policy link to review or modify the assigned policy.

Field	Description
VPN Device Policy	Choose an existing policy or click <b>Add VPN Device Policy</b> to add a new policy.  Click the Resolved Policy link to review or modify the assigned policy.
Address Translations Timeout	Length of time (in days, hours, minutes, and seconds) that a translation can remain unused before it expires.
<b>DHCP Policy</b>	
Edge DHCP Policy	Click to add a new DHCP policy.
Type	Type of DHCP service: relay or server.
Interface Name	Interface to which the DHCP policy is applied.
Server/Relay Policy	DHCP policy name.

**Events Tab**

Field	Description
ID	Unique event identifier.
User	One of the following user types: <ul style="list-style-type: none"> <li>• admin</li> <li>• internal</li> <li>• blank</li> </ul>
Created at	Date and time at which the fault occurred.
Cause	Unique identifier associated with the event cause.
Description	Event description.

## Configuring Edge Security Profiles

Edge security profiles can include any of the following:

- ACL policy sets (ingress and egress)
- Connection timeout policies
- IP audit policies



- NAT policy sets
- Packet inspection policies
- TCP intercept policies
- VPN interface policy sets

You can create an edge security profile at any level of the organizational hierarchy (root, tenant, VDC, app, or tier). Creating an edge security profile at the root level enables you to apply it to multiple edge firewalls for different tenants.

### Procedure

- 
- Step 1** Choose **Policy Management > Service Profiles > Edge Firewall > Edge Security Profiles**.
- Step 2** In the General tab, click **Add Edge Security Profile**.
- Step 3** In the Add Edge Security Profile dialog box provide the information as described in [Add Edge Security Profile Dialog Box](#), on page 41.
- 

## Add Edge Security Profile Dialog Box

Field	Description
<b>General Tab</b>	
Name	Profile name.
Description	Brief profile description.
<b>Ingress Tab</b>	
Policy Set	Choose an existing policy set or click <b>Add ACL Policy Set</b> to add a new policy set.  Click the <b>Resolved Ingress Policy Set</b> link to modify the assigned policy set.
Resolved Policies	Click <b>(Un)assign Policy</b> to assign or remove a policy for the current policy set.
<b>Egress Tab</b>	
Policy Set	Choose an existing policy set or click <b>Add ACL Policy Set</b> to add a new policy set.  Click the <b>Resolved Egress Policy Set</b> link to modify the assigned policy set.

Field	Description
Resolved Policies	Click <b>(Un)assign Policy</b> to assign or remove a policy for the current policy set.
<b>NAT Tab</b>	
Policy Set	Choose an existing policy set or click <b>Add NAT Policy Set</b> to add a new policy set. Click the <b>Resolved NAT Policy Set</b> link to modify the assigned policy set.
Resolved Policies	Click <b>(Un)assign Policy</b> to assign or remove a policy for the current policy set.
<b>VPN Tab</b>	
Policy Set	Choose an existing policy set or click <b>Add Interface Policy Set</b> to add a new policy set. Click the <b>Resolved VPN Interface Policy Set</b> link to modify the assigned policy set.
<b>Advanced Tab</b>	
Packet Inspection Policy	Choose an existing policy or click <b>Add Packet Inspection Policy</b> to add a new policy. Click the <b>Resolved Policy</b> link to modify the assigned policy.
Connection Timeout Policy	Choose an existing policy or click <b>Add Connection Timeout Policy</b> to add a new policy. Click the <b>Resolved Policy</b> link to modify the assigned policy.
TCP Intercept Policy	Choose an existing policy or click <b>Add TCP Intercept Policy</b> to add a new policy. Click the <b>Resolved Policy</b> link to modify the assigned policy.
IP Audit Policy	Choose an existing policy or click <b>Add IP Audit Policy</b> to add a new policy. Click the <b>Resolved Policy</b> link to modify the assigned policy.

## Applying an Edge Device Profile

After you have created an edge device profile, you can apply the profile to multiple edge firewalls to ensure consistent policies across the firewalls.

### Procedure

- 
- Step 1** Choose **Resource Management > Managed Resources > root > tenant > Edge Firewalls > edge-firewall**.
  - Step 2** In the General tab, click **Select** in the Edge Device Profile field.
  - Step 3** In the Select Edge Device Profile dialog box, select the required profile, then click **OK**.
  - Step 4** Click **Save**.
- 

## Applying an Edge Security Profile

After you have created an edge security profile, you can apply it to edge firewall instances to ensure consistent policies on the interfaces.

**Note**

Edge security profiles can be applied only on outside interfaces of edge firewalls.

---

### Procedure

- 
- Step 1** Choose **Resource Management > Managed Resources > root > tenant > Edge Firewalls > edge-firewall**.
  - Step 2** In the Interfaces table, select the required outside interface, then click **Edit**.
  - Step 3** In the Edit dialog box, click **Select** in the Edge Security Profile field.
  - Step 4** In the Select Edge Security Profile dialog box, select the required profile, then click **OK**.
  - Step 5** Click **OK** in the open dialog boxes, then click **Save**.
- 

## Verifying Edge Firewall Policies

Use this procedure to verify active policies and optionally modify policy objects for edge firewalls.

### Procedure

- 
- Step 1** Choose **Resource Management > Managed Resources > root > tenant > Edge Firewalls > edge-firewall**.
- Step 2** In the Edge Security Profiles tab, select the required policy, then click **Show Resolved Policies**.
- Step 3** To view policy or policy set details, use the tabs in the Edit dialog box to navigate to the required policy or policy set, then click the required policy or policy set in Resolved field
- Step 4** To use a different policy or policy set, navigate to the required policy or policy set, then either choose a different policy or policy set from the drop-down list, or add a new policy or policy set.
- Step 5** Click **Apply** to accept any changes or **OK** when you have finished reviewing the policies.
- 

## Configuring Security Profiles

### Editing a Security Profile for a Compute Firewall

#### Procedure

- 
- Step 1** Choose **Policy Management > Service Profiles > root > Compute Firewalls > Compute Security Profiles**.
- Step 2** In the General tab, select the profile you want to edit, then click **Edit**.
- Step 3** In the Edit Compute Security Profile dialog box, edit the fields as required by using the information in the following tables, then click **OK**.

**Table 5: General Tab**

Field	Description
Name	Profile name.
Description	Brief policy description.
Policy Set	List of available policy sets.
Add ACL Policy Set	Click to add a new ACL policy set.
Resolved Policy Set	Click the link to view and optionally edit the resolved policy set.
<b>Resolved Policies</b>	
(Un)assigned Policy	Click to assign or unassign policies.
Source Condition	Source condition for the policy.

Field	Description
Destination Condition	Destination condition for the policy.
Protocol	Protocol specify by the policy.
Ethertype	EtherType specified by the policy.
Action	Action to take if the specified condition is met.
Description	Brief policy description.

**Table 6: Attributes Tab**

Field	Description
Add User Defined Attribute	Click to add a custom attribute.
Name	Attribute name.
Value	Attribute value.

## Editing a Security Profile for an Edge Firewall

This procedure enables you to edit a security profile associated with an edge firewall.

### Procedure

- Step 1** Choose **Policy Management > Service Profiles > root > Edge Firewall > Edge Security Profiles**.
- Step 2** In the General tab, select the edge security profile that you want to edit, then click **Edit**.
- Step 3** In the Edit Edge Security Profile dialog box, edit the entries as required by using the information in the following table, then click **OK**.

Field	Description
<b>General Tab</b>	
Name	Profile name.
Description	Brief profile description.
ID	Unique profile identifier.

Field	Description
<b>Ingress Tab</b>	
Policy Set	Choose an existing policy set or click <b>Add ACL Policy Set</b> to add a new policy set. Click the <b>Resolved Ingress Policy Set link</b> to modify the assigned policy set.
Resolved Policies	Click <b>(Un)assign Policy</b> to assign or remove a policy for the current policy set.
<b>Egress Tab</b>	
Policy Set	Choose an existing policy set or click <b>Add ACL Policy Set</b> to add a new policy set. Click the <b>Resolved Egress Policy Set link</b> to modify the assigned policy set.
Resolved Policies	Click <b>(Un)assign Policy</b> to assign or remove a policy for the current policy set.
<b>NAT Tab</b>	
Policy Set	Choose an existing policy set or click <b>Add NAT Policy Set</b> to add a new policy set. Click the <b>Resolved NAT Policy Set link</b> to modify the assigned policy set.
Resolved Policies	Click <b>(Un)assign Policy</b> to assign or remove a policy for the current policy set.
<b>VPN Tab</b>	
Policy Set	Choose an existing policy set or click <b>Add Interface Policy Set</b> to add a new policy set. Click the <b>Resolved VPN Interface Policy Set link</b> to modify the assigned policy set.
<b>Advanced Tab</b>	
Packet Inspection Policy	Choose an existing policy or click <b>Add Packet Inspection Policy</b> to add a new policy. Click the <b>Resolved Policy link</b> to modify the assigned policy.

Field	Description
Connection Timeout Policy	Choose an existing policy or click <b>Add Connection Timeout Policy</b> to add a new policy. Click the <b>Resolved Policy link</b> to modify the assigned policy.
Threat Migration	Choose an existing policy or click <b>Add TCP Intercept Policy</b> to add a new policy. Click the <b>Resolved Policy link</b> to modify the assigned policy.
IP Audit Policy	Choose an existing policy or click <b>Add IP Audit Policy</b> to add a new policy. Click the <b>Resolved Policy link</b> to modify the assigned policy.

## Deleting a Security Profile

### Procedure

- Step 1** In the Navigation pane, click the **Policy Management** tab.
- Step 2** In the Navigation pane, click the **Security Policies** subtab.
- Step 3** In the **Navigation** pane, expand **root > Security Profiles**.
- Step 4** In the **Work** pane, click the security profile you want to delete.
- Step 5** Click **Delete**.
- Step 6** In the Confirm dialog box, click **OK**.

## Deleting a Security Profile Attribute

### Procedure

---

- Step 1** In the Navigation pane, click the **Policy Management** tab.
  - Step 2** In the Navigation pane, click the **Security Policies** subtab.
  - Step 3** In the **Navigation** pane, expand **root > Security Profiles**.
  - Step 4** In the **Navigation** pane, click the security profile that contains the attribute you want to delete.
  - Step 5** In the **Work** pane, click the **Attributes** tab.
  - Step 6** Click the attribute you want to delete.
  - Step 7** Click **Delete**.
  - Step 8** In the Confirm dialog box, click **OK**.
- 

## Assigning a Policy

### Procedure

---

- Step 1** In the Navigation pane, click the **Policy Management** tab.
  - Step 2** In the Navigation pane, click the **Security Policies** subtab.
  - Step 3** In the **Navigation** pane, expand **root > Security Profiles**.
  - Step 4** In the **Navigation** pane, click the profile where you want to assign the policy.
  - Step 5** In the **Work** pane, click the **(Un)assign Policy** link.
  - Step 6** In the **(Un)assign Policy** dialog box, move the policy you want assigned to the **Assigned** list.
  - Step 7** Click **OK**.
-



## Unassigning a Policy

### Procedure

- Step 1** In the Navigation pane, click the **Policy Management** tab.
- Step 2** In the Navigation pane, click the **Security Policies** subtab.
- Step 3** In the **Navigation** pane, expand **root > Security Profiles**.
- Step 4** In the **Navigation** pane, click the profile where you want to unassign the policy.
- Step 5** In the **Work** pane, click the **(Un)assign Policy** link.
- Step 6** In the **(Un)assign Policy** dialog box, move the policy you want unassigned to the **Available** list.
- Step 7** Click **OK**.

## Configuring Security Policy Attributes

### Configuring Object Groups

#### Adding an Object Group

### Procedure

- Step 1** Choose **Policy Management > Service Policies > root > tenant > Policy Helpers > Object Groups**.
- Step 2** In the General tab, click **Add Object Group**.
- Step 3** In the Add Object Group dialog box, complete the following fields, then click **OK**:  
**Note** You must specify an attribute type and name before adding an object group expression.

Field	Description
Name	Object group name.  This name can be between 2 and 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is saved.
Description	Brief description of the object group.  This description can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphens, underscore, dot, and colon.

Field	Description
Attribute Type	Available attribute types. You must configure an attribute type and name to add an object group expression.
Attribute Name	Available attribute names.
<b>Expression Table</b>	
Add Object Group Expression	Click to add an object group expression.
Operator	Operator for the selected expression.
Value	Value for the selected expression.

## Adding an Object Group Expression

### Procedure

- Step 1** Choose **Policy Management > Service Policies > root > Policy Helpers > Object Groups**.
- Step 2** In the General tab, select the object group you want to add an object group expression to, then click **Edit**.  
**Note** For new object groups, you must specify the attribute type and name before adding an object group expression.
- Step 3** In the Edit Object Group dialog box, click **Add Object Group Expression**.
- Step 4** In the Add Object Group Expression dialog box, specify the object group expression by using the information in the following table, then click **OK** in the open dialog boxes.

Field	Description
Attribute Name	Attribute (read-only).
Operator	Available operators for this attribute.
Attribute Value	Attribute value for this expression.

## Editing an Object Group

### Procedure

- Step 1** Choose **Policy Management > Service Policies > root > tenant > Policy Helpers > Object Groups**.
- Step 2** In the General tab, select the object group you want to edit, then click **Edit**.
- Step 3** In the Edit Object Group dialog box, update the fields as follows, then click **OK**:

Field	Description
Name	Object group name (read-only).
Description	Object group description. This description can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphens, underscore, dot, and colon.
Attribute Type	Specified attribute type (read-only).
Attribute Name	Specified attribute name (read-only).
<b>Expression Table</b>	
Add Object Group Expression	Click to add a new object group expression.
Operator	Expression operator.
Value	Expression attribute value.

## Editing an Object Group Expression

### Procedure

- Step 1** Choose **Policy Management > Service Policies > root > Policy Helpers > Object Groups**.
- Step 2** In the General tab, select the object group with the expression you want to edit, then click **Edit**.
- Step 3** In the Expression table in the Edit Object Group dialog box, select the expression you want to edit, then click **Edit**.
- Step 4** In the Edit Object Group Expression dialog box, edit the fields as required, then click **OK** in the open dialog boxes.

Field	Description
Attribute Name	Attribute name (read-only).
Operator	Available operators for this expression.
Attribute Value	Attribute value for this expression.

## Deleting an Object Group

### Procedure

- Step 1** Choose **Policy Management > Service Policies > root > Policy Helpers > Object Groups**.
- Step 2** In the General tab, select the Object Group you want to delete, then click **Delete**.
- Step 3** When prompted, confirm the deletion.

## Deleting an Object Group Expression

### Procedure

- Step 1** Choose **Policy Management > Service Policies > root > Policy Helpers > Object Groups**.
- Step 2** In the General tab, select the object group that contains the expression you want to delete, then click **Edit**.
- Step 3** In the Edit Object Group dialog box, select the expression that you want to delete In the Expression table, then click **Delete**.
- Step 4** When prompted confirm the deletion.
- Step 5** Click **OK** in the open dialog box to save the change.

# Configuring Security Profile Dictionary

## Adding a Security Profile Dictionary

### Procedure

- Step 1** Choose **Policy Management > Service Policies > root > tenant > Policy Helpers > Security Profile Dictionary**.
- Note** You can create one security profile dictionary at the root level and one for each tenant.
- Step 2** In the General tab, click **Add Security Profile Dictionary**.
- Step 3** In the Add Security Profile Dictionary dialog box, complete the following fields as appropriate, then click **OK**:

Field	Description
Name	<p>Name of the security profile dictionary.</p> <p>This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.</p> <p><b>Note</b> You can create one security profile dictionary at the root level and one at the tenant level.</p>
Description	<p>A description of the security profile dictionary.</p> <p>This description can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphens, underscore, dot, and colon.</p>
<b>Attributes Table</b>	
Add Security Profile Custom Attribute	Click to add a new attribute.
Name	Custom attribute name.
Description	Custom attribute description.

## Adding a Security Profile Dictionary Attribute

### Procedure

- Step 1** Choose **Policy Management > Service Policies > root > tenant > Policy Helpers > Security Profile Dictionary**.
- Step 2** In the General tab, select the security profile dictionary that you want to add an attribute to, then click **Edit**.
- Step 3** In the Edit Security Profile Dictionary dialog box, click **Add Security Profile Custom Attribute**.
- Step 4** In the Add Security Profile Custom Attribute dialog box, complete the following fields, then click **OK**:

Field	Description
Name	Attribute name.  This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Description	Attribute description.  This description can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphens, underscore, dot, and colon.

## Editing a Security Profile Dictionary

### Procedure

- Step 1** Choose **Policy Management > Service Policies > root > Policy Helpers > Security Profile Dictionary**.
- Step 2** In the General tab, select the security profile dictionary you want to edit, then click **Edit**.
- Step 3** In the Edit Security Profile Dictionary dialog box, modify the fields as appropriate, then click **OK**:

Field	Description
Name	Name of the security profile dictionary (read-only).
Description	Description of the security profile dictionary.
<b>Attributes</b>	
Add Security Profile Custom Attribute	Click to add a custom attribute.
Name	Attribute name.

Field	Description
Description	Attribute description.

## Editing a Security Profile Dictionary Attribute

### Procedure

- Step 1** Choose **Policy Management > Service Policies > root > Policy Helpers > Security Profile Dictionary**.
- Step 2** In the General tab, select the security profile dictionary that contains the attribute you want to edit, then click **Edit**.
- Step 3** In the Edit Security Profile Dictionary dialog box, select the attribute you want to edit, then click **Edit**.
- Step 4** In the Edit Security Custom Attribute dialog box, edit the Description field as required, then click **OK** in the open dialog boxes to save the change.

## Deleting a Security Profile Dictionary

### Procedure

- Step 1** Choose **Policy Management > Service Policies > root > Policy Helpers > Security Profile Dictionary**.
- Step 2** In the General tab, select the security profile dictionary you want to delete, then click **Delete**.
- Step 3** When prompted, confirm the deletion.

## Deleting a Security Profile Dictionary Attribute

### Procedure

- Step 1** Choose **Policy Management > Service Policies > root > Policy Helpers > Security Profile Dictionary**. In the General tab, select the dictionary that contains the attribute you want to delete, then click **Edit**.
- Step 2** In the Edit Security Profile Dictionary dialog box, in Attributes table, select the attribute you want to delete, then click **Delete**.
- Step 3** When prompted, confirm the deletion.

## Working with vZones

A virtual zone (vZone) is a logical grouping of VMs or hosts. vZones facilitate working with policies and profiles because vZones enable you to write policies based on vZone attributes by using vZone names.

The high level flow for working with vZones in VNMC is as follows:

1. Define a vZone, each with one or more condition for inclusion in the vZone.
2. Define a service policy with the rules based on zone or network conditions.
3. Create a policy set that includes the service policy defined in Step 2.
4. Create a security profile that includes the policy set created in Step 3.
5. Bind the security profile to the ASA 1000V or VSG port profile.
6. Assign the security profile to the ASA 1000V or VSG in VNMC.

See the following topics for more information about working with vZones.

## Adding a vZone

### Procedure

**Step 1** Choose **Policy Management > Service Policies > root > Policy Helpers > vZones**.

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

**Step 3** In the Add vZone dialog box, provide the required information as described in the following table, then click **OK**:

Field	Description
Name	vZone name.  This name can be between 2 and 32 characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change the name after it is saved.
Description	Brief vZone description.  This description can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphens, underscore, dot, and colon.
<b>vZone Condition</b>	
Add Zone Condition	Click to add a zone condition.
Attribute Name	Condition attribute name.
Operator	Condition operator.
Attribute Value	Condition attribute value.



## Editing a vZone

### Procedure

- Step 1** Choose **Policy Management > Service Policies > root > Policy Helpers > vZones**.
- Step 2** In the General tab, select the vZone that you want to edit, then click **Edit**.
- Step 3** In the Edit vZone dialog box in the General tab, edit the fields as required, then click **OK**.

Field	Description
Name	vZone name (read-only).
Description	Brief vZone description.
<b>vZone Condition</b>	
Add vZone	Click to add a vZone condition.
Up and down arrows	Change the priority of the selected policies.
Attribute Name	Attribute name for the selected vZone condition.
Operator	Operator for the selected vZone condition.
Attribute Value	Attribute value for the selected vZone condition.

- Step 4** To change a vZone condition:
- In the vZone Condition table, select the attribute you want to edit, then click **Edit**.
  - In the Edit Zone Condition dialog box, make the required changes using the following information:

Field	Description
Attribute Type	Attribute type for the condition (read-only).
Attribute Name	Attribute name for the condition (read-only).
Operator	Operator to apply for the condition.
Attribute Value	Attribute value for the condition.

**Step 5** Click **OK** in the open dialog boxes, then click **Save**.

---

## Deleting a vZone Condition

### Procedure

---

- Step 1** Choose **Policy Management > Service Policies > root > Policy Helpers > vZones**.
- Step 2** In the General tab, select the vZone with the condition that you want to delete, then click **Edit**.
- Step 3** In the Edit vZone dialog box, select the condition in the vZone Condition table that you want to delete, then click **Delete**.
- Step 4** Confirm the deletion.
- Step 5** In the Edit vZone dialog box, click **OK** or **Apply**.
- 

## Deleting a vZone

### Procedure

---

- Step 1** Choose **Policy Management > Service Policies > root > Policy Helpers > vZones**.
- Step 2** In the General tab, select the vZones that you want to delete, then click **Delete**.
- Step 3** Confirm the deletion.
-