

Configuring Infranet Controller IPsec Routing Policies (NSM Procedure)

An IPsec routing policy specifies the Infranet Enforcer device that endpoints must use to access resources when using IPsec. The IPsec routing policy also specifies that endpoints must use an IPsec tunnel to the Infranet Enforcer to access resources.

To configure an IPsec routing policy:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller for which you want to configure IPsec routing policies.
3. Click the **Configuration** tab. In the configuration tree, select **UAC > Infranet Enforcer > IPsec Routing**.
4. Add or modify IPsec routing policy settings as specified in Table 1 on page 1.
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 1: IPsec Routing Policies Configuration Details

Option	Function	Your Action
Name	Specifies the IPsec routing policy name.	Enter a name for the IPsec routing policy.
Description	Describes the IPsec routing policy.	Enter a brief description for the IPsec routing policy.
Resource Type	Specifies whether the Infranet Controller dynamically provisions or manually provisions the IPsec routing policy.	<ul style="list-style-type: none"> ■ Select Manual— if you are using ScreenOS version 6.1 or earlier. ■ Select Dynamic—if you are using ScreenOS version 6.1 or later.
Set Resources	Specifies the IP address and netmask of each resource that requires endpoints to use IPsec.	<ul style="list-style-type: none"> ■ Click Set Resources. The Set Resources dialog box appears. Select Resources and enter new resources one per line in the following format: < ip address > [/netmask] ■ Click Set Resources > Exceptions and enter new exceptions one per line in the following format: < ip address > [/netmask]
Enforcer	Specifies the Infranet Enforcer to which endpoints connect to access the resources specified in this IPsec routing policy.	Select the Infranet Enforcer.

Table 1: IPsec Routing Policies Configuration Details (continued)

Option	Function	Your Action
Destination Zone	<p>Specifies the destination zone where the protected resources specified in this IPsec routing policy are located.</p> <p>This destination zone is configured on the Infranet Controller.</p>	Enter the destination zone that is configured on the Infranet Enforcer. For example: enter trust .
Always use UDP Encapsulation	Allows the Odyssey Access Client and the Infranet Enforcer to create an IPsec tunnel inside a third-party IPsec tunnel by using UDP encapsulation even if a NAT device is not present.	Select this check box.
Always use a virtual adapter	Forces the use of a virtual adapter on the endpoint. If you select this option, you must also set up IP address pools even if a NAT device is not present.	Select this check box.
Persistent Tunnel Mode	Allows you to determine whether or not a tunnel is established when a user first connects to the Infranet Controller. If the check box is selected, an IPsec tunnel is established, and users can access protected resources behind the Infranet Enforcer. If the check box is not selected, the tunnel is not automatically set up: a tunnel will not be initiated until there is a request for traffic.	Select this check box.

Table 1: IPsec Routing Policies Configuration Details (continued)

Option	Function	Your Action
Applies to roles	Specifies the policies that apply to the roles.	<ul style="list-style-type: none"> <li data-bbox="1052 369 1422 474">■ Select Policy applies to ALL roles to apply this Infranet Controller IPsec routing policy to all users. <li data-bbox="1052 485 1422 642">■ Select Policy applies to SELECTED roles to apply this Infranet Controller IPsec routing policy only to users who are mapped to roles in the Selected roles list. <li data-bbox="1052 653 1422 810">■ Select Policy applies to roles OTHER THAN those selected to apply this Infranet Controller IPsec routing policy to all users except those who map to the roles in the Selected roles list. <p data-bbox="1052 842 1422 947">NOTE: Select the policies from the Non-members list and click Add to move it to the Members list before applying the policies to the roles.</p>

- Related Topics**
- Configuring Infranet Controller IP Address Pool Policies (NSM Procedure)
 - Configuring Infranet Enforcer Resource Access Policies (NSM Procedure)

