

## Defining Network Connect Split Tunneling Policies (NSM Procedure)

Network Connect (NC) split tunneling policies specify one or more network IP address/netmask combinations for which the device handles traffic passed between the remote client and the corporate intranet. You can also specify traffic that should not pass through the NC tunnel.

When split-tunneling is used, NC modifies routes on clients so that traffic meant for the corporate intranet networks to NC and all other traffic goes through the local physical adapter. The IVE tries to resolve all DNS requests through the physical adapter first and then routes those that fail to the NC adapter.

For example,

- If split tunneling is disabled and the exclude route contains 10.204.50.0/24, then all traffic except 10.204.50.0 networks will go through NC.
- If split tunneling is enabled and the included route contains 10.204.64.0/18 and the exclude traffic contains 10.204.68.0/24, networks from 10.204.64.0/18 to 10.204.127.0/18 will pass through the NC tunnel. The 10.204.68.0/24 network will not pass through the NC tunnel.
- If split tunneling is enabled and the include route contains 10.204.64.0/24 (subnet of the excluded route), and the exclude route contains 10.204.64.0/18 (super set of the included route), then the included network's traffic will still be routed through the NC tunnel.

To write an NC split-tunneling networks resource policy:

1. In the navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to write an NC split-tunneling networks resource policy.
2. Click the **Configuration** tab. Select **Users > Resource Policies > Network Connect > Split-tunneling Networks**.
3. Click **New Profile**, and then enter the name and the description for the policy.
4. Add or modify more settings as specified in Table 1.
5. Click one:
  - **OK**—Saves the changes.
  - **Cancel**—Cancels the modifications.

**Table 1: Configuring Network Connect Split Tunneling Policy Details**

Options	Your Action
Resources	Enter the new resource name for the split tunnel resource policy.

**Table 1: Configuring Network Connect Split Tunneling Policy Details** (continued)

Options	Your Action
Applies to Roles	Select one of the following options from the drop-down list: <ul style="list-style-type: none"> <li>■ <b>ALL</b> —To apply this policy to all users.</li> <li>■ <b>Selected</b>—To apply this policy only to users who are mapped to roles in the Selected roles list. Upon selecting this option, the Role Selections tab is enabled.</li> <li>■ <b>Except those selected</b>—To apply this policy to all users except for those who map to the roles in the Selected roles list.</li> </ul>
Action	Select one of the following options from the drop-down list: <ul style="list-style-type: none"> <li>■ <b>Allow</b>—This option allows the Network IP address/netmask combinations specified in the Resources field to pass through the NC tunnel.</li> <li>■ <b>Detailed Rules</b> —This option defines resource policy rules that put additional restrictions on the specified resources. Upon selecting this option, the Detailed Rules tab is enabled.</li> <li>■ <b>Deny</b>—This option denies the Network IP address/netmask combinations specified in the Resources field not to pass through the NC tunnel.</li> </ul>
<b>Roles Selection tab</b>	
Roles Selections	Select the members from the <b>Members</b> list. You can add or remove the members to the Non-members list by selecting <b>Add</b> , <b>Remove</b> , <b>Add All</b> , or <b>Remove All</b> .
<b>Detailed Rules tab</b>	
Name	Enter the name for the rule.
Action	Select <b>Allow</b> or <b>deny</b> from the drop-down list.  Enter the new resource name for the rule.



**NOTE:** On the Network Connect Split Tunneling Policies page, prioritize the policies according to how you want the device to evaluate them. Once the device matches the resource requested by the user to a resource that belongs to a Resource list of a policy (or a detailed rule's), it performs the specified action and stops processing policies.

- Related Topics**
- Configuring a Network Connect Connection Profile Resource Policy (NSM Procedure)
  - Configuring Web Rewriting Resource Policies (NSM Procedure)

Published: 2009-08-20