

Lesson 13: Configuring NPS Policies

MOAC 70-411: Administering
Windows Server 2012

Overview

- Exam Objective 4.2: Configure NPS Policies
- Managing NPS Policies

Managing NPS Policies

Lesson 13: Configuring NPS Policies

Network Policy Server (NPS) Policies

Connection Request

- Specifies which RADIUS servers perform authentication, authorization, and accounting

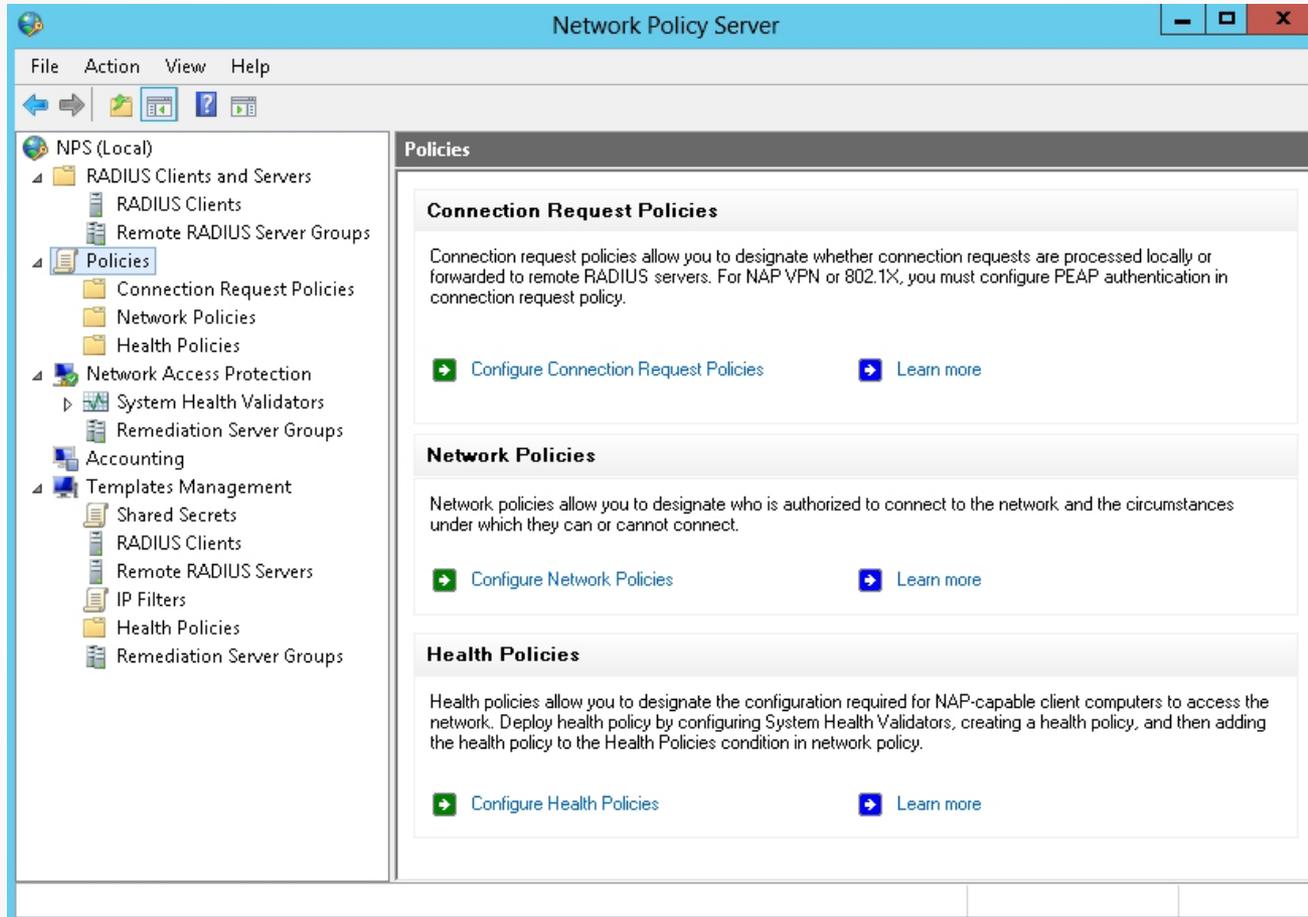
Network

- Specifies who is authorized to connect to the network and circumstances under which they can or cannot connect

Health

- Establishes system health validators (SHVs) and other settings that define client computer configuration requirements for NAP-capable computers

NPS Policies



Configuring Connection Request Policies

Connection request policies are based on a range of factors such as:

- The time of day and day of the week
- The realm name in the connection request
- The type of connection requested
- The IP address of the RADIUS client

Configuring Connection Request Policies

When you create a connection request policy, you define these parameters:

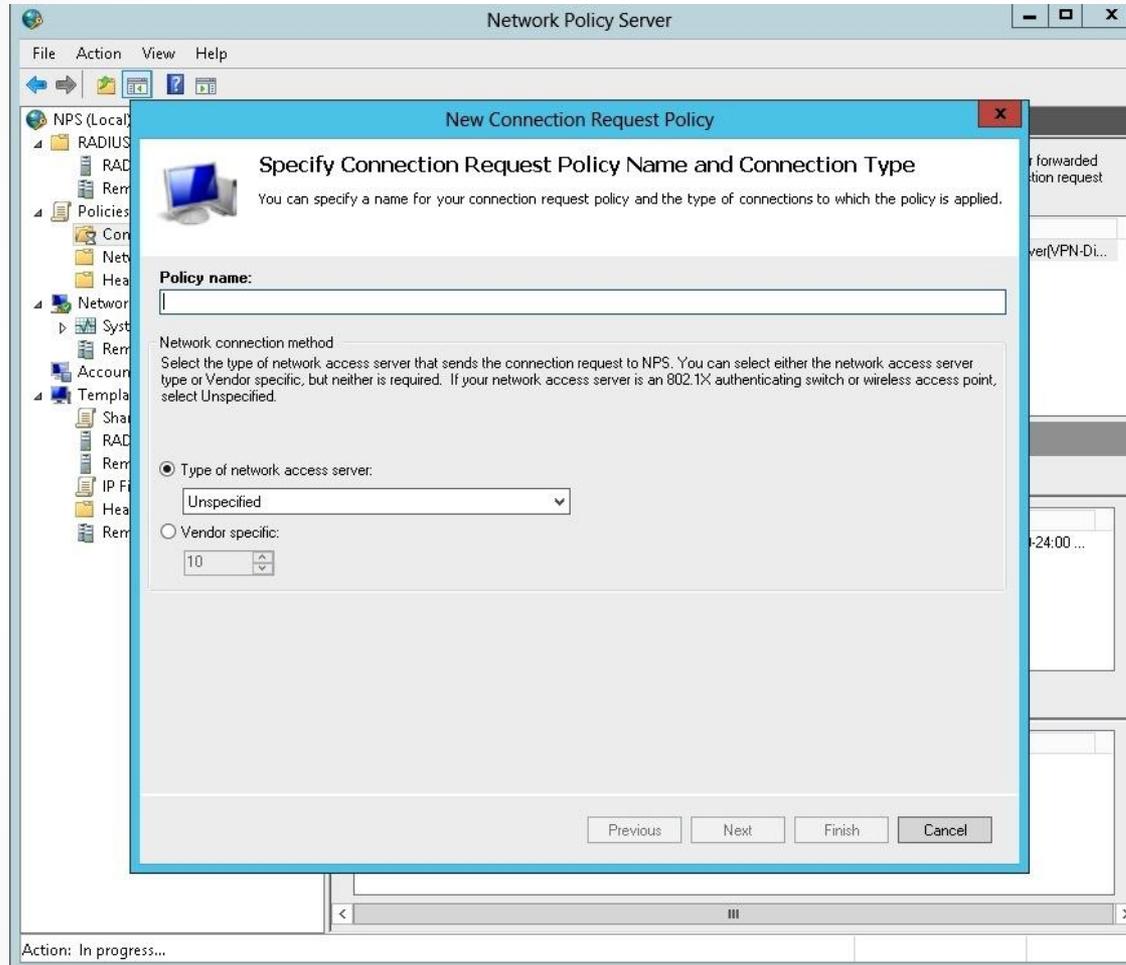
- Type of network access server such as remote access server (VPN dial-up)
- Condition that specifies who or what can connect to the network based on one or more RADIUS attributes
- Settings that are applied to an incoming RADIUS message such as authentication, accounting, and attribute manipulation

Configuring Connection Request Policies

Connection request policy conditions:

- Are one or more RADIUS attributes that are compared to the attributes of the incoming RADIUS Access-Request message.
- If there are multiple conditions, all of the conditions in the connection request message and in the connection request policy must match in order for the policy to be enforced by NPS.

Create a Connection Request Policy



Defining the policy name

Create a Connection Request Policy

New Connection Request Policy ✕

 **Specify Conditions**

Specify the conditions that determine whether this connection request policy is evaluated for a connection request. A minimum of one condition is required.

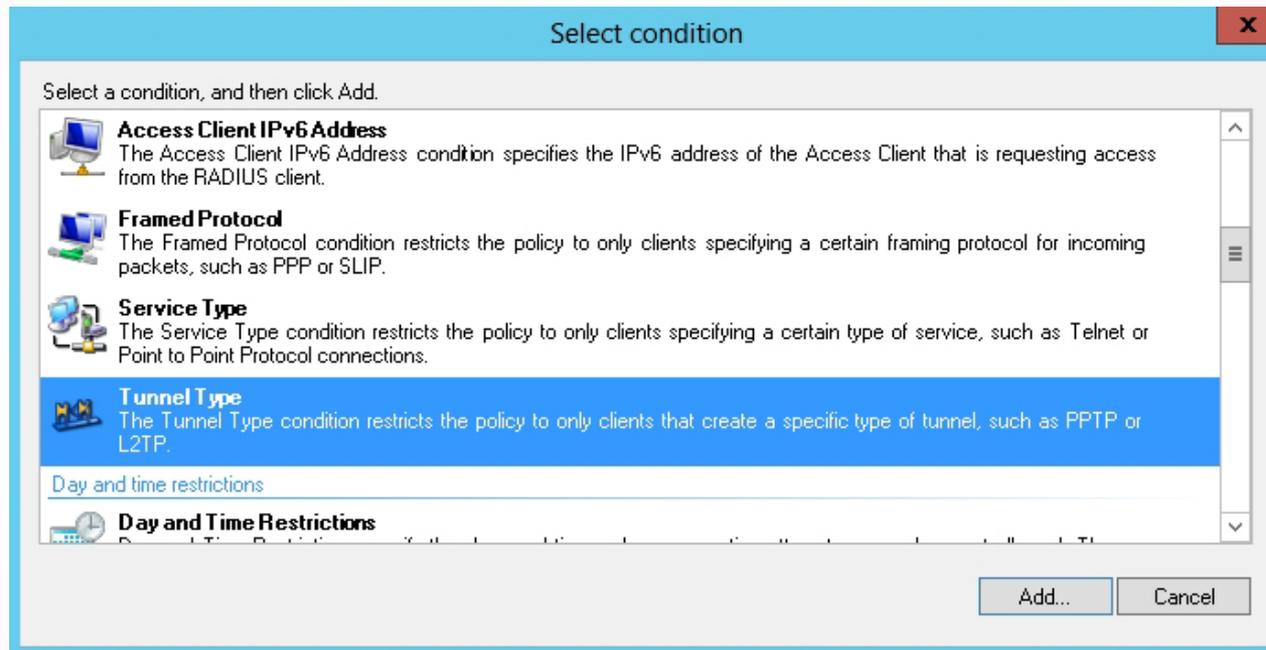
Conditions:

Condition	Value
-----------	-------

Condition description:

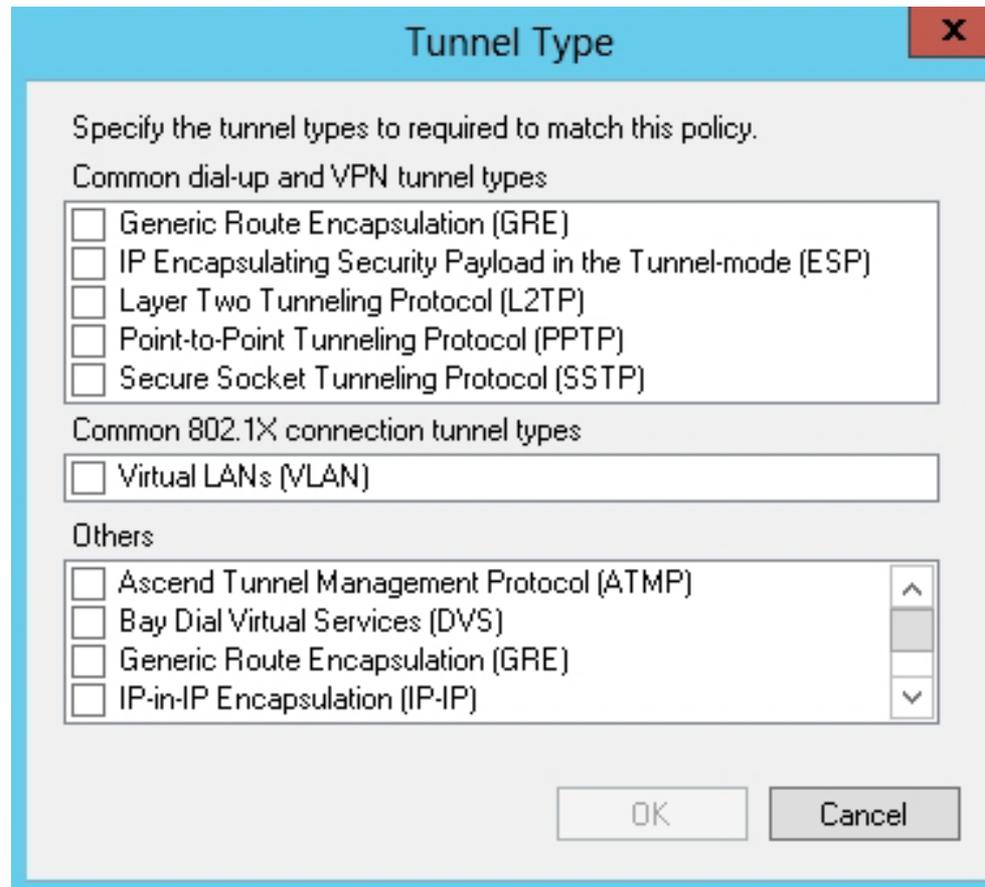
Specifying conditions

Create a Connection Request Policy



Selecting a condition

Create a Connection Request Policy



Selecting a tunnel type

Create a Connection Request Policy

The screenshot shows a window titled "New Connection Request Policy" with a close button in the top right corner. The main heading is "Specify Connection Request Forwarding". Below the heading is a small icon of a computer monitor and a text box explaining that the connection request can be authenticated by the local server or forwarded to RADIUS servers in a remote RADIUS server group. A note states: "If the policy conditions match the connection request, these settings are applied." Under the "Settings:" section, there is a tree view on the left with "Forwarding Connection Request" expanded, showing "Authentication" (selected with a green arrow) and "Accounting". The main area contains instructions: "Specify whether connection requests are processed locally, are forwarded to remote RADIUS servers for authentication, or are accepted without authentication." There are three radio button options: "Authenticate requests on this server" (selected), "Forward requests to the following remote RADIUS server group for authentication:" (with a dropdown menu showing "<not configured>" and a "New..." button), and "Accept users without validating credentials". At the bottom, there are four buttons: "Previous", "Next", "Finish", and "Cancel".

Specifying Connection Request Forwarding page

Create a Connection Request Policy

The screenshot shows a Windows-style dialog box titled "New Connection Request Policy" with a close button (X) in the top right corner. The main heading is "Specify Authentication Methods". Below the heading is a small icon of a computer monitor and a mouse, followed by a paragraph of text: "Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type. If you deploy NAP with 802.1X or VPN, you must configure Protected EAP." Below this is a checkbox labeled "Override network policy authentication settings". Underneath is a paragraph: "These authentication settings are used rather than the constraints and authentication settings in network policy. For VPN and 802.1X connections with NAP, you must configure PEAP authentication here." This is followed by another paragraph: "EAP types are negotiated between NPS and the client in the order in which they are listed." Below this is a section titled "EAP Types:" with an empty list box. To the right of the list box are "Move Up" and "Move Down" buttons. Below the list box are "Add...", "Edit...", and "Remove" buttons. Below these is a section titled "Less secure authentication methods:" with a list of checkboxes: "Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)", "Microsoft Encrypted Authentication (MS-CHAP)", "Encrypted authentication (CHAP)", "Unencrypted authentication (PAP, SPAP)", and "Allow clients to connect without negotiating an authentication method." At the bottom of the dialog are "Previous", "Next", "Finish", and "Cancel" buttons.

New Connection Request Policy

Specify Authentication Methods

Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type. If you deploy NAP with 802.1X or VPN, you must configure Protected EAP.

Override network policy authentication settings

These authentication settings are used rather than the constraints and authentication settings in network policy. For VPN and 802.1X connections with NAP, you must configure PEAP authentication here.

EAP types are negotiated between NPS and the client in the order in which they are listed.

EAP Types:

Move Up
Move Down

Add... Edit... Remove

Less secure authentication methods:

- Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
 - User can change password after it has expired
- Microsoft Encrypted Authentication (MS-CHAP)
 - User can change password after it has expired
- Encrypted authentication (CHAP)
- Unencrypted authentication (PAP, SPAP)
- Allow clients to connect without negotiating an authentication method.

Previous Next Finish Cancel

Specifying Authentication Methods page

Create a Connection Request Policy

The screenshot shows a window titled "New Connection Request Policy" with a close button (X) in the top right corner. The main heading is "Configure Settings". Below the heading is a small computer icon and a paragraph: "NPS applies settings to the connection request if all of the connection request policy conditions for the policy are matched." Below this is another paragraph: "Configure the settings for this network policy. If conditions match the connection request and the policy grants access, settings are applied." Under the heading "Settings:", there are two main sections. The first is "Specify a Realm Name" with a sub-section "Attribute" containing "RADIUS Attributes". Under "RADIUS Attributes", there are two options: "Standard" (with a globe icon) and "Vendor Specific" (with a checkmark icon). The second section is "Select the attributes to which the following rules will be applied. Rules are processed in the order they appear in the list." It features a dropdown menu for "Attribute:" set to "Called-Station-Id". Below this is a "Rules:" table with two columns: "Find" and "Replace With". The table is currently empty. To the right of the table are five buttons: "Add", "Edit", "Remove", "Move Up", and "Move Down". At the bottom of the window are four buttons: "Previous", "Next", "Finish", and "Cancel".

New Connection Request Policy

Configure Settings

NPS applies settings to the connection request if all of the connection request policy conditions for the policy are matched.

Configure the settings for this network policy. If conditions match the connection request and the policy grants access, settings are applied.

Settings:

Specify a Realm Name

Attribute

RADIUS Attributes

- Standard
- Vendor Specific

Select the attributes to which the following rules will be applied. Rules are processed in the order they appear in the list.

Attribute:

Rules:

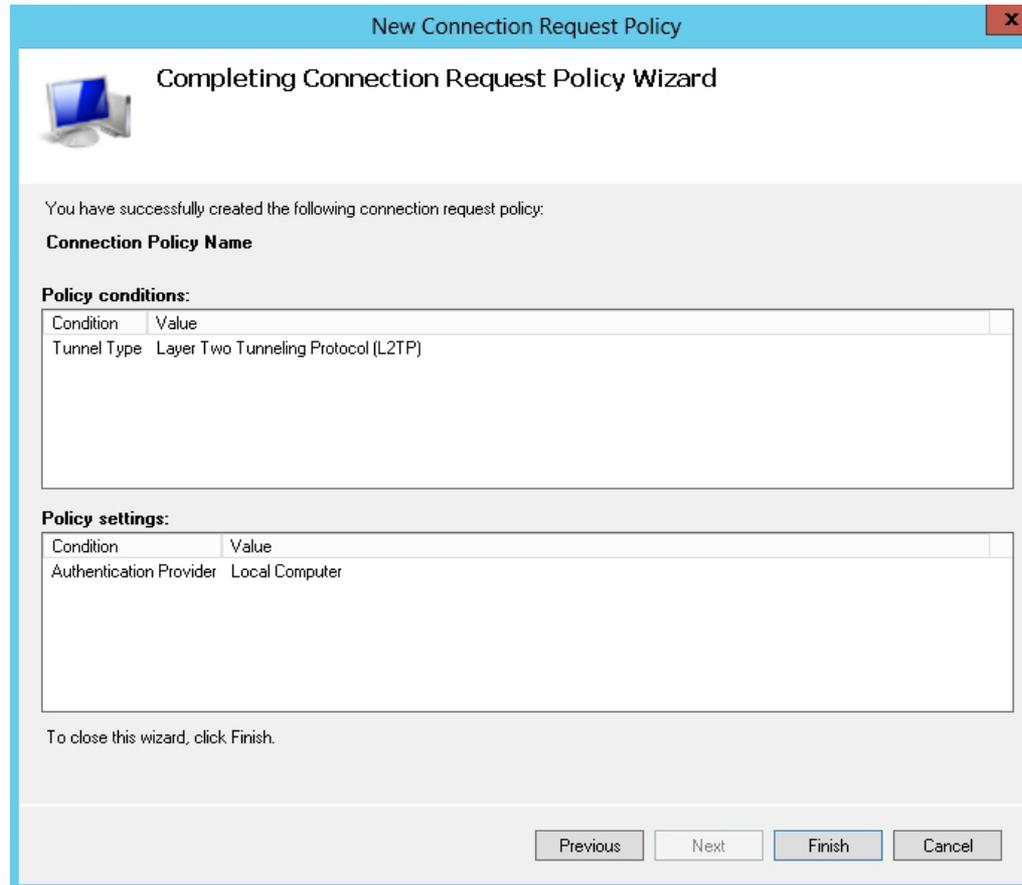
Find	Replace With
------	--------------

Add
Edit
Remove
Move Up
Move Down

Previous Next Finish Cancel

Configuring Settings page

Create a Connection Request Policy



Completing Connection Request Policy Wizard

Create a Connection Request Policy

Connection Policy Name Properties

Overview Conditions Settings

Policy name:

Policy State
If enabled, NPS evaluates this policy while processing connection requests. If disabled, NPS does not evaluate this policy.

Policy enabled

Network connection method
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.

Type of network access server:

Vendor specific:

OK Cancel Apply

Configuring Connection Request Policy properties

Configuring Network Policies

An NPS network policy evaluates remote connections based on these three components:

- Conditions
- Constraints
- Settings

Configuring Network Policies

When a user attempts to connect to a remote access server, this process occurs:

1. User attempts to initiate a remote access connection.
2. Remote access server checks the conditions in the first configured NPS network policy.
3. If the conditions of this NPS network policy do not match, the remote access server checks the next configured NPS network policies. It keeps checking each policy until it finds a match or reaches the last policy.
4. When the remote access server finds an NPS network policy with conditions that match the incoming connection attempt, the remote access server checks any constraints that have been configured for the policy.

Configuring Network Policies

When a user attempts to connect to a remote access server, this process occurs (continued):

5. Once the remote access server finds an NPS network policy with conditions that match the incoming connection attempt, the remote access server checks any constraints (such as time of day or minimum encryption level) that have been configured for the policy.
6. If the connection attempt does not match any configured constraints, the remote access server denies the connection.
7. If the connection attempt matches both the conditions and the constraints of a particular NPS network policy, the remote access server will allow or deny the connection, based on the Access Permissions configured for that policy.

Create a Network Policy

New Network Policy

Specify Network Policy Name and Connection Type

You can specify a name for your network policy and the type of connections to which the policy is applied.

Policy name:

Network connection method

Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.

Type of network access server:

Unspecified

Vendor specific:

10

Previous Next Finish Cancel

Starting the New Network Policy Wizard

Create a Network Policy

New Network Policy ✕

 **Specify Conditions**
Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required.

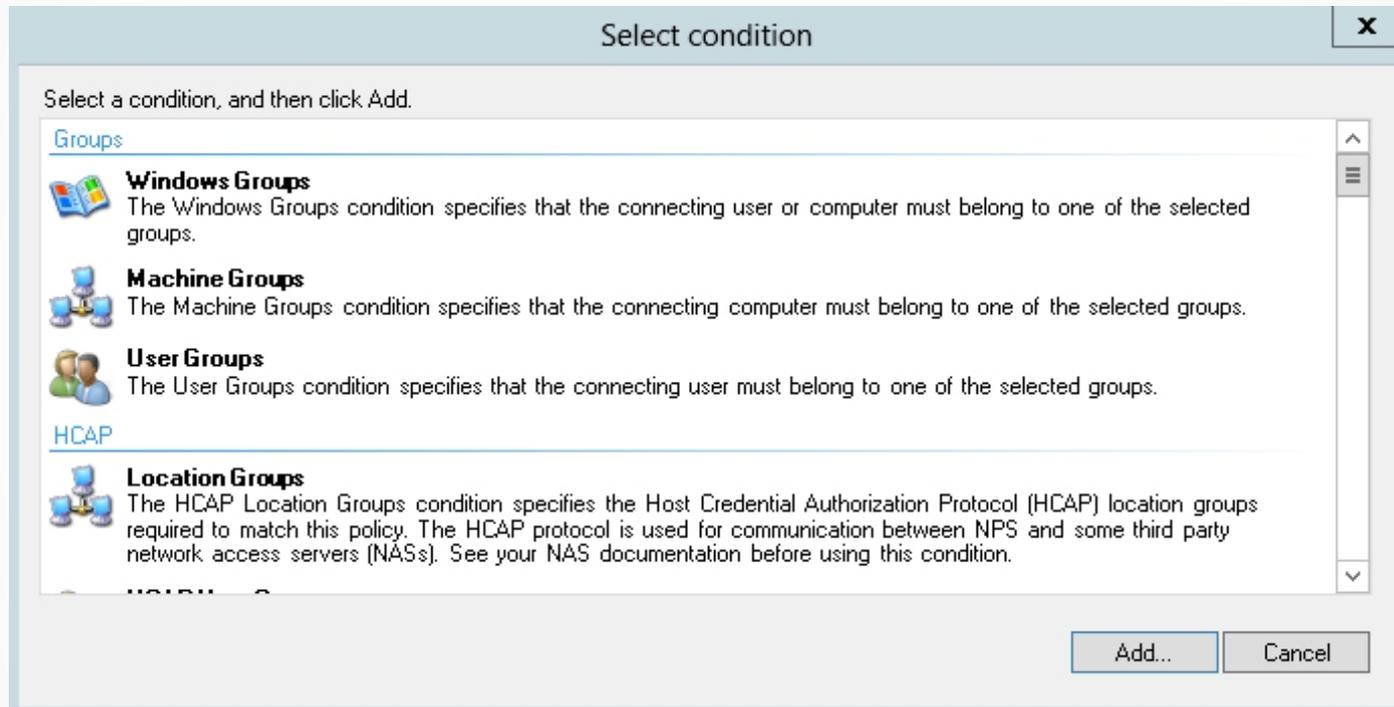
Conditions:

Condition	Value
-----------	-------

Condition description:

Specifying conditions

Create a Network Policy



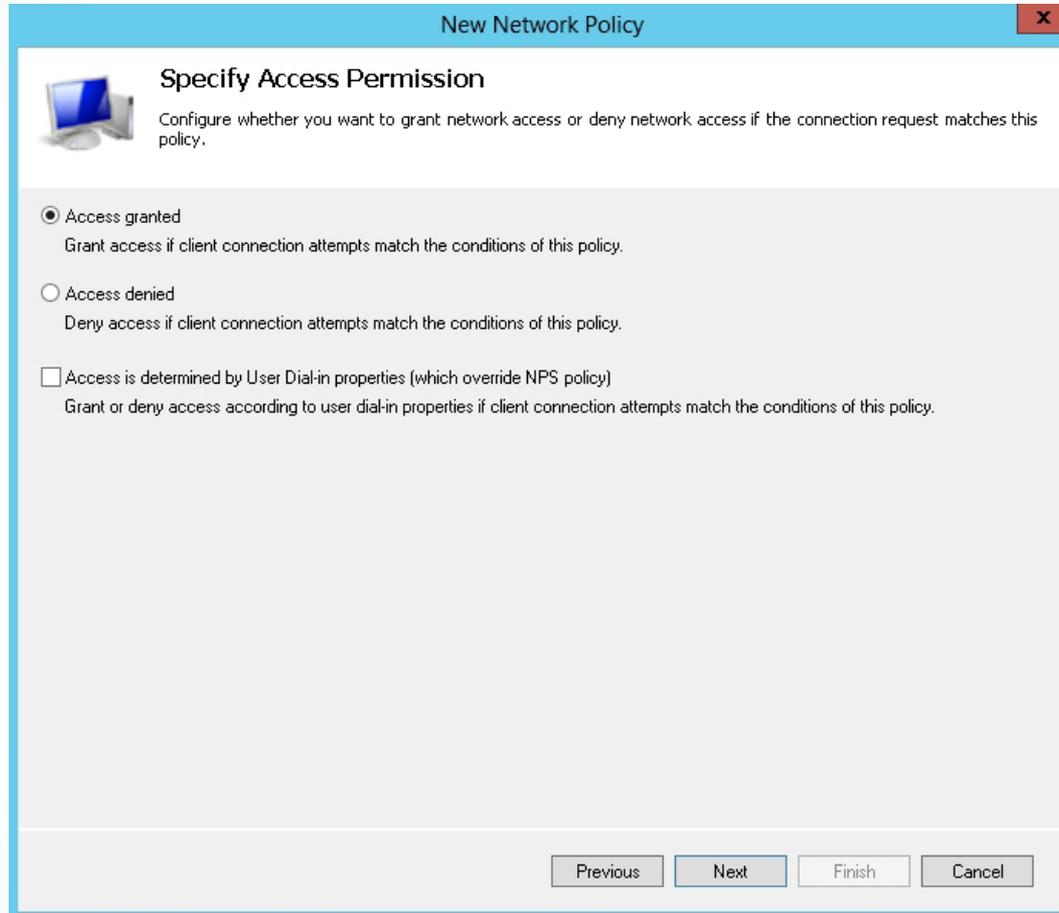
Selecting conditions

Create a Network Policy



Adding Windows groups

Create a Network Policy



The screenshot shows a Windows-style dialog box titled "New Network Policy" with a close button (X) in the top right corner. The main heading is "Specify Access Permission". Below the heading is a small icon of a computer monitor and a mouse. The text below the icon reads: "Configure whether you want to grant network access or deny network access if the connection request matches this policy." There are three radio button options: "Access granted" (selected), "Access denied", and "Access is determined by User Dial-in properties (which override NPS policy)". Each option has a descriptive sub-text. At the bottom of the dialog are four buttons: "Previous", "Next", "Finish", and "Cancel".

New Network Policy [X]

Specify Access Permission

Configure whether you want to grant network access or deny network access if the connection request matches this policy.

Access granted
Grant access if client connection attempts match the conditions of this policy.

Access denied
Deny access if client connection attempts match the conditions of this policy.

Access is determined by User Dial-in properties (which override NPS policy)
Grant or deny access according to user dial-in properties if client connection attempts match the conditions of this policy.

Previous Next Finish Cancel

Specifying access permissions

Create a Network Policy

New Network Policy [X]

Configure Authentication Methods

Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type. If you deploy NAP with 802.1X or VPN, you must configure Protected EAP in connection request policy, which overrides network policy authentication settings.

EAP types are negotiated between NPS and the client in the order in which they are listed.

EAP Types:

Less secure authentication methods:

- Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
 - User can change password after it has expired
- Microsoft Encrypted Authentication (MS-CHAP)
 - User can change password after it has expired
- Encrypted authentication (CHAP)
- Unencrypted authentication (PAP, SPAP)
- Allow clients to connect without negotiating an authentication method.
- Perform machine health check only

Configuring authentication methods

Create a Network Policy

New Network Policy ✕

Configure Constraints

 Constraints are additional parameters of the network policy that are required to match the connection request. If a constraint is not matched by the connection request, NPS automatically rejects the request. Constraints are optional; if you do not want to configure constraints, click Next.

Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.

Constraints:

- Constraints**
-  Idle Timeout
-  Session Timeout
-  Called Station ID
-  Day and time restrictions
-  NAS Port Type

Specify the maximum time in minutes that the server can remain idle before the connection is disconnected

Disconnect after the maximum idle time

1

Previous Next Finish Cancel

Configuring constraints

Create a Network Policy

New Network Policy [X]

Configure Settings

NPS applies settings to the connection request if all of the network policy conditions and constraints for the policy are matched.

Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

- RADIUS Attributes**
 - Standard
 - Vendor Specific
- Network Access Protection**
 - NAP Enforcement
 - Extended State
- Routing and Remote Access**
 - Multilink and Bandwidth Allocation Protocol (BAP)
 - IP Filters
 - Encryption
 - IP Settings

To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Attributes:

Name	Value
Framed-Protocol	PPP
Service-Type	Framed

Configuring settings

Create a Network Policy

New Network Policy x

 **Completing New Network Policy**

You have successfully created the following network policy:

Policy Name

Policy conditions:

Condition	Value
Windows Groups	CONTOSO\Domain Users

Policy settings:

Condition	Value
Authentication Method	MS-CHAP v1 OR MS-CHAP v1 (User can change password after it has expired) OR MS-CHAP v2 ...
Access Permission	Grant Access
Update Noncompliant Clients	True
NAP Enforcement	Allow full network access
Framed-Protocol	PPP
Service-Type	Framed

To close this wizard, click Finish.

Completing new network policies

Create a Network Policy

Policy Name Properties

Overview | Conditions | Constraints | Settings

Policy name:

Policy State
If enabled, NPS evaluates this policy while performing authorization. If disabled, NPS does not evaluate this policy.

Policy enabled

Access Permission
If conditions and constraints of the network policy match the connection request, the policy can either grant access or deny access. [What is access permission?](#)

Grant access. Grant access if the connection request matches this policy.

Deny access. Deny access if the connection request matches this policy.

Ignore user account dial-in properties.
If the connection request matches the conditions and constraints of this network policy and the policy grants access, perform authorization with network policy only; do not evaluate the dial-in properties of user accounts.

Network connection method
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.

Type of network access server:

Vendor specific:

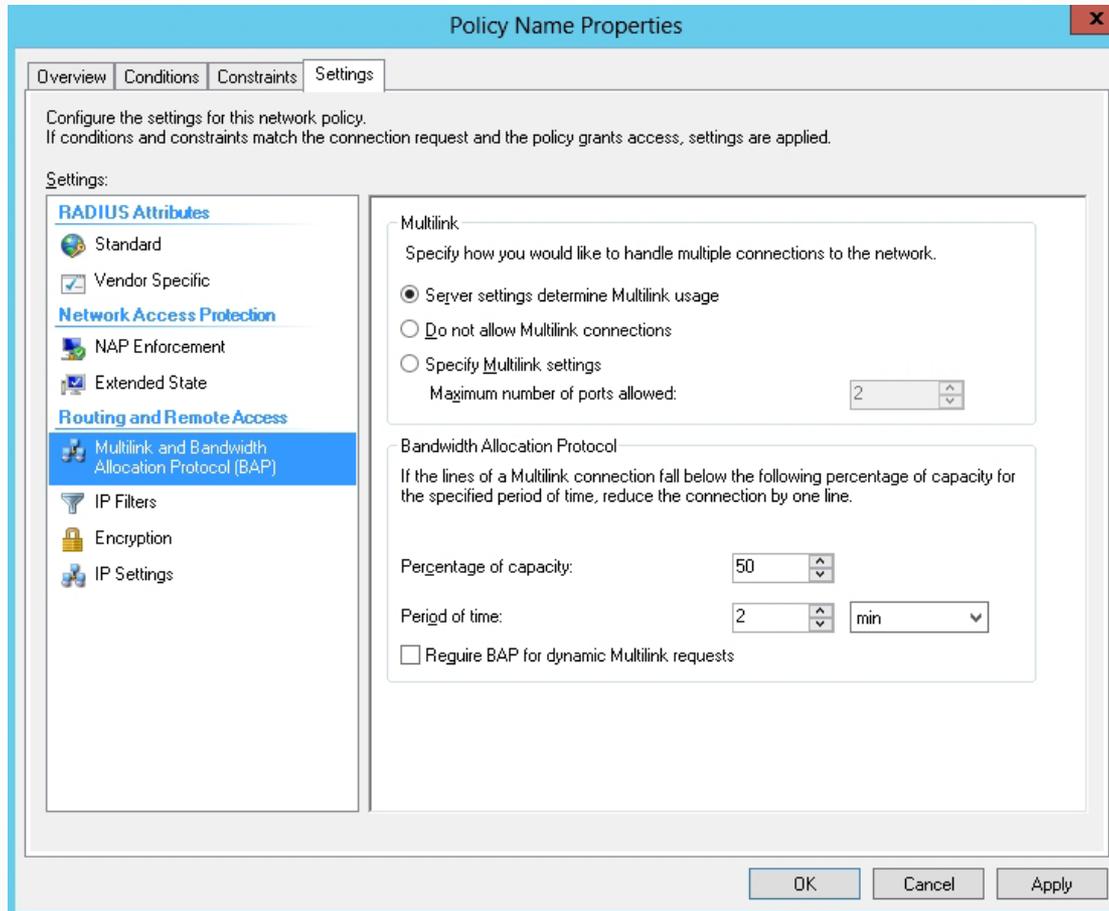
OK Cancel Apply

Configuring Network Policy properties

Multilink and Bandwidth Allocation

- ISDN includes multiple channels, which allow simultaneous voice and data communications.
- With multilink and Bandwidth Allocation Protocol (BAP) settings, you can specify:
 - Whether multiple connections form a single connection to increase bandwidth
 - How BAP determines when these extra lines are dropped

Multilink and Bandwidth Allocation



Configuring Multilink and BAP settings

IP Filters

Allow you to control which packets are allowed through the network connection based on IP address.

To configuration:

1. Click the *Input Filters* or *Output Filters* for IPv4 or IPv6.
2. Specify to permit or not permit packets.
3. Click the *New* button to specify the source network or destination network.

IP Filters

Inbound Filters [?] [X]

These filters control which packets are forwarded or processed by this network.

Filter action:

Do not permit packets listed below

Permit only the packets listed below

Filters:

Source Address	Source Network Mask	Destination Address	Destination Mask	P

< [] >

[New...] [Edit...] [Delete]

[OK] [Cancel]

Add IP Filter [?] [X]

Source network

IP address: [. . .]

Subnet mask: [. . .]

Destination network

IP address: [. . .]

Subnet mask: [. . .]

Protocol: [Any v]

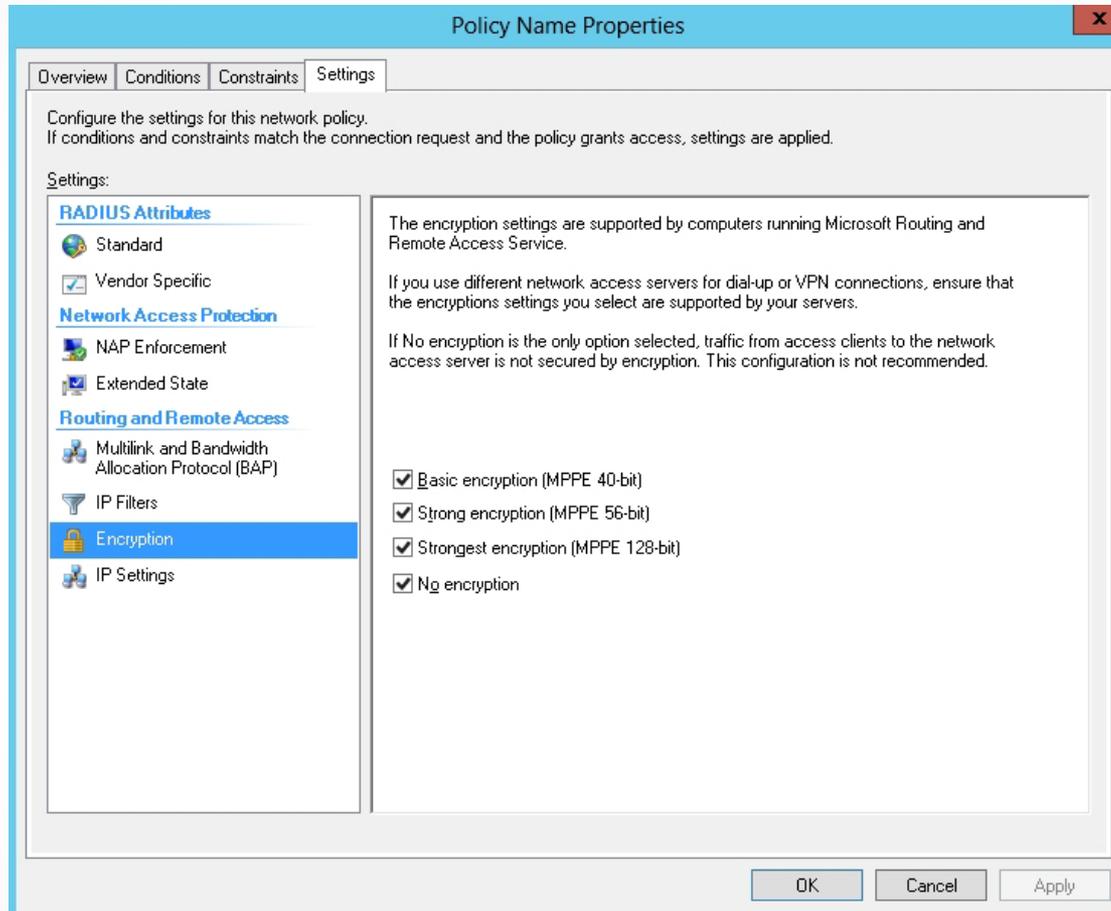
[OK] [Cancel]

Configuring an IPv4 Inbound filter

Encryption Options

- **Basic Encryption (MPPE 40-Bit):** For dial-up and PPTP-based VPN connections, MPPE is used with a 40-bit key. For L2TP/IPsec VPN connections, 56-bit DES encryption is used.
- **Strong Encryption (MPPE 56-Bit):** For dial-up and PPTP VPN connections, MPPE is used with a 56-bit key. For L2TP/IPsec VPN connections, 56-bit DES encryption is used.
- **Strongest Encryption (MPPE 128-Bit):** For dial-up and PPTP VPN connections, MPPE is used with a 128-bit key. For L2TP/IPsec VPN connections, 168-bit Triple DES encryption is used.
- **No Encryption:** This option allows unencrypted connections that match the remote access policy conditions. Clear this option to require encryption.

Encryption Settings



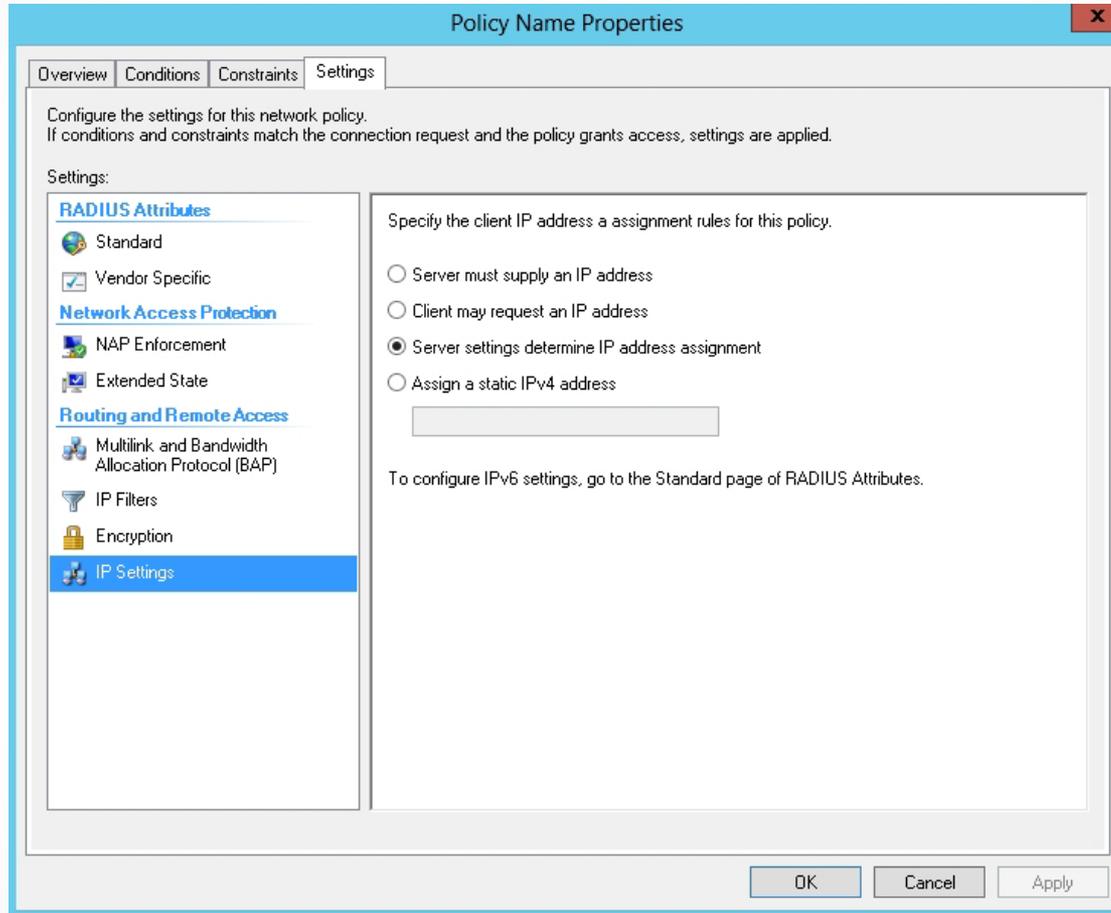
Configuring encryption settings

IP Addressing

IP settings include these options:

- Server Must Supply An IP Address
- Client May Request An IP Address
- Server Settings Determine IP Address Assignment (the default setting)
- Assign A Static IP Address

IP Addressing



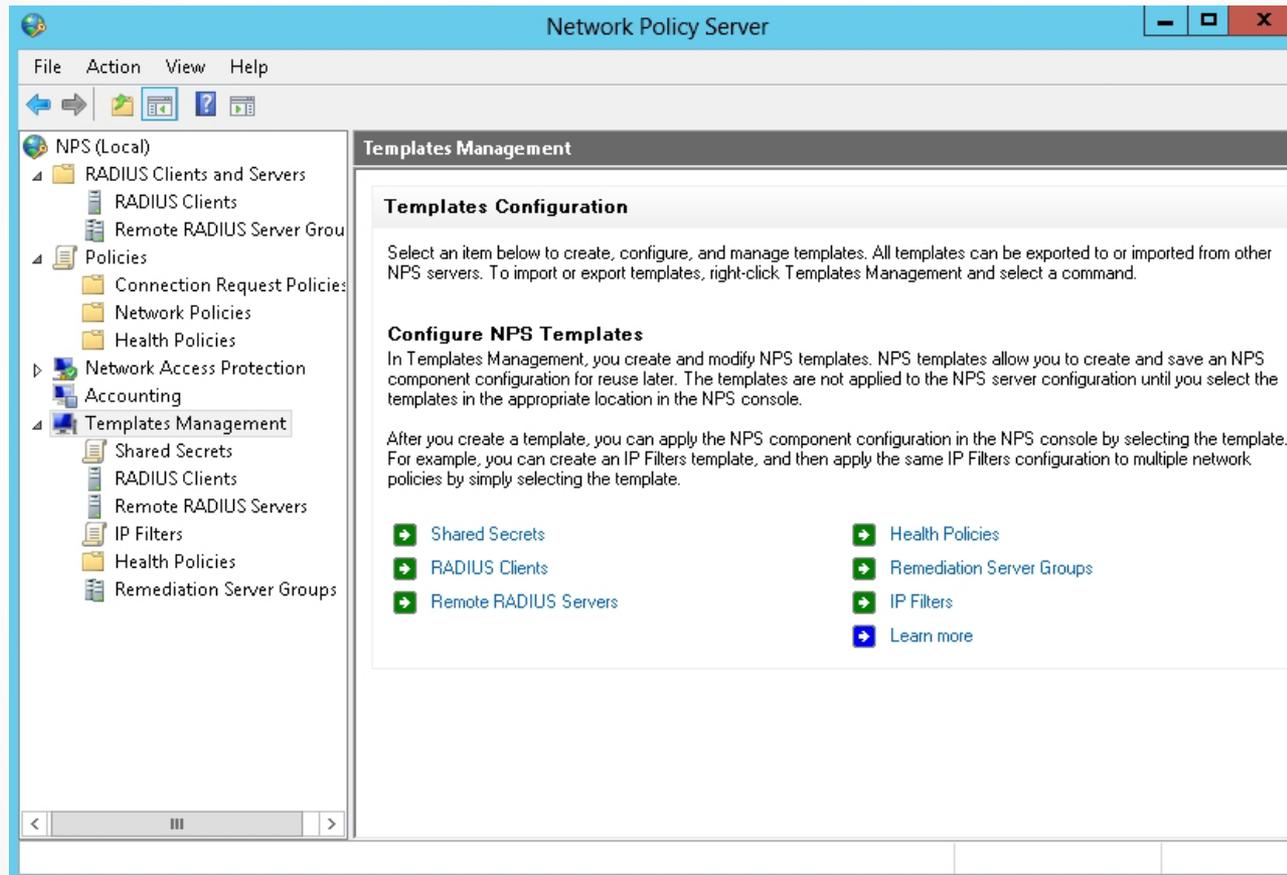
Configuring IP assignment settings

Managing NPS Templates

NPS template types available in Templates Management:

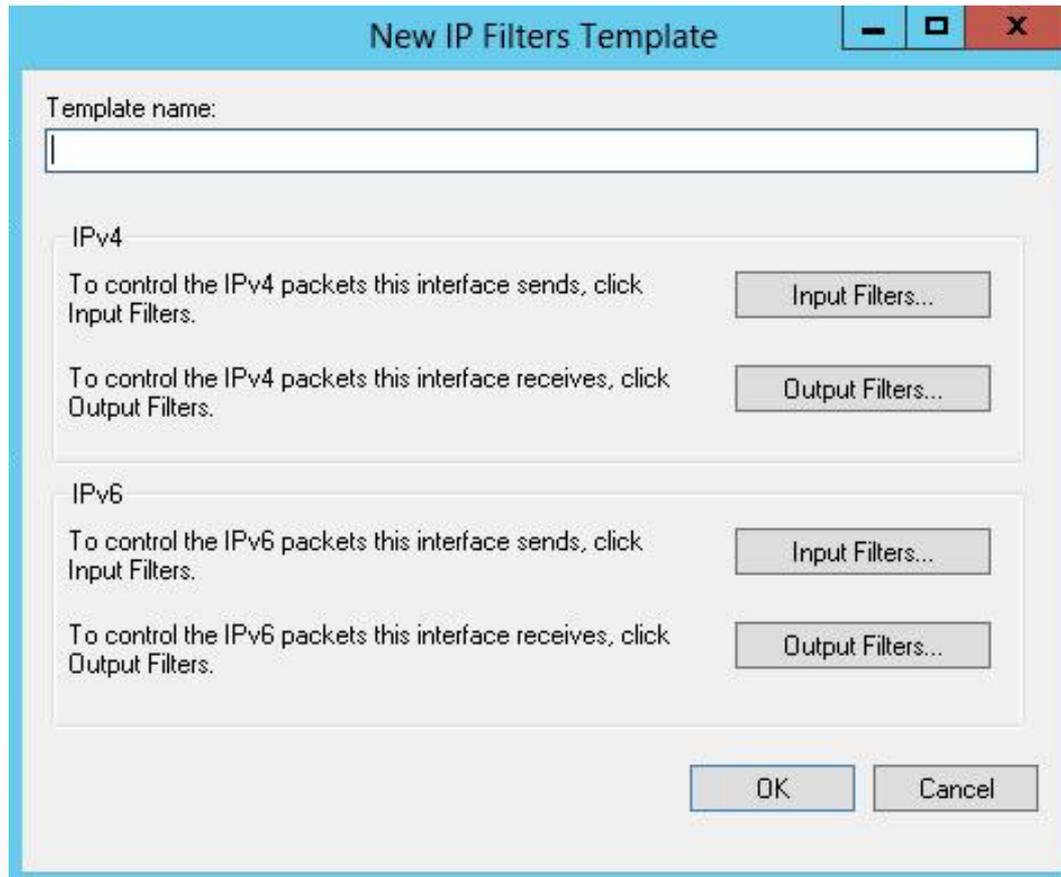
- Shared Secrets
- RADIUS Clients
- Remote RADIUS Servers
- IP Filters
- Health Policies
- Remediation Server Groups

Managing NPS Templates



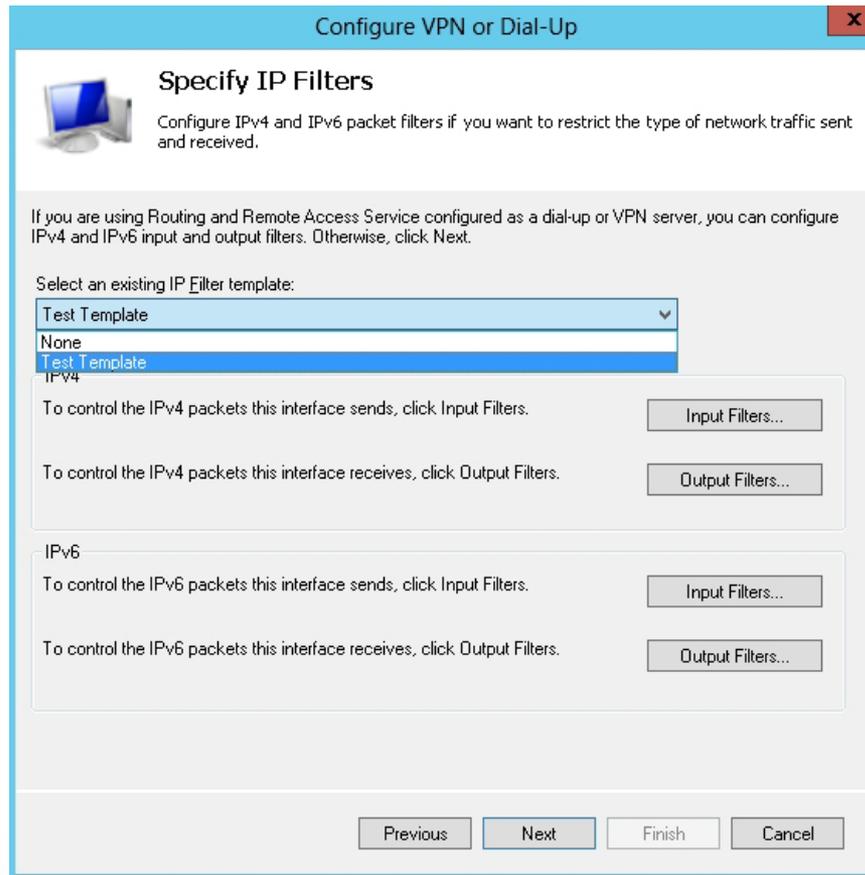
Configuring templates in NPS

Managing NPS Templates



Creating a new IP filter template

Managing NPS Templates



The screenshot shows a dialog box titled "Configure VPN or Dial-Up" with a close button (X) in the top right corner. The main heading is "Specify IP Filters" with a computer icon. Below the heading is the instruction: "Configure IPv4 and IPv6 packet filters if you want to restrict the type of network traffic sent and received." A paragraph explains that if using Routing and Remote Access Service as a dial-up or VPN server, IPv4 and IPv6 input and output filters can be configured; otherwise, the user should click "Next". A dropdown menu labeled "Select an existing IP Filter template:" shows "Test Template" selected, with "None" and "Test Template" as other options. Below this, there are two sections: "IPv4" and "IPv6". Each section contains two instructions: "To control the [IPv4/IPv6] packets this interface sends, click Input Filters." and "To control the [IPv4/IPv6] packets this interface receives, click Output Filters." Each instruction is followed by an "Input Filters..." or "Output Filters..." button. At the bottom of the dialog are four buttons: "Previous", "Next", "Finish", and "Cancel".

Applying the template

Exporting and Importing the NPS Configuration Including NPS Policies

Use the `netsh` command to export the entire NPS configuration from one NPS server for import on another NPS server.

NPS configuration includes:

- RADIUS clients and servers
- Network policy
- Connection request policy
- Registry
- Logging configuration

Lesson Summary

- An NPS policy is a set of permissions or restrictions that are used by remote access authenticating servers that determine who, when, and how a client can connect to a network.
- With remote access policies, connections can be authorized or denied based on user attributes, group membership, and so on.
- Connection request policies are policies that establish sets of conditions and settings that specify which RADIUS servers perform the authentication, authorization, and accounting of connection requests received by the NPS server from RADIUS clients.
- Network policies establish sets of conditions, constraints, and settings that specify who is authorized to connect to the network and the circumstances under which they can or cannot connect.
- With multilink and Bandwidth Allocation Protocol (BAP) settings, you can specify whether multiple connections form a single connection to increase bandwidth. In addition, you can specify how BAP determines when these extra lines are dropped.

Lesson Summary

- The IP filters allow you to control which packets are allowed through the network connection based on IP address.
- The Encryption settings enable you to specify the supported encryption used with network connections.
- The last setting in the Routing and Remote Access is IP settings, which specify how IP addresses are assigned.
- Network Policy Server templates enable you to create configuration elements that can be reused on the local NPS server and can be exported to other NPS servers.
- You can export the entire NPS configuration, including RADIUS clients and servers, network policy, connection request policy, registry, and logging configuration from one NPS server for import on another NPS server by using the `netsh` command.

Copyright 2013 John Wiley & Sons, Inc.

All rights reserved. Reproduction or translation of this work beyond that named in Section 117 of the 1976 United States Copyright Act without the express written consent of the copyright owner is unlawful. Requests for further information should be addressed to the Permissions Department, John Wiley & Sons, Inc. The purchaser may make back-up copies for his/her own use only and not for distribution or resale. The Publisher assumes no responsibility for errors, omissions, or damages, caused by the use of these programs or from the use of the information contained herein.