Lesson 13: Configuring NPS Policies

MOAC 70-411: Administering Windows Server 2012

Microsoft Official Academic Course

WILEY

Overview

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

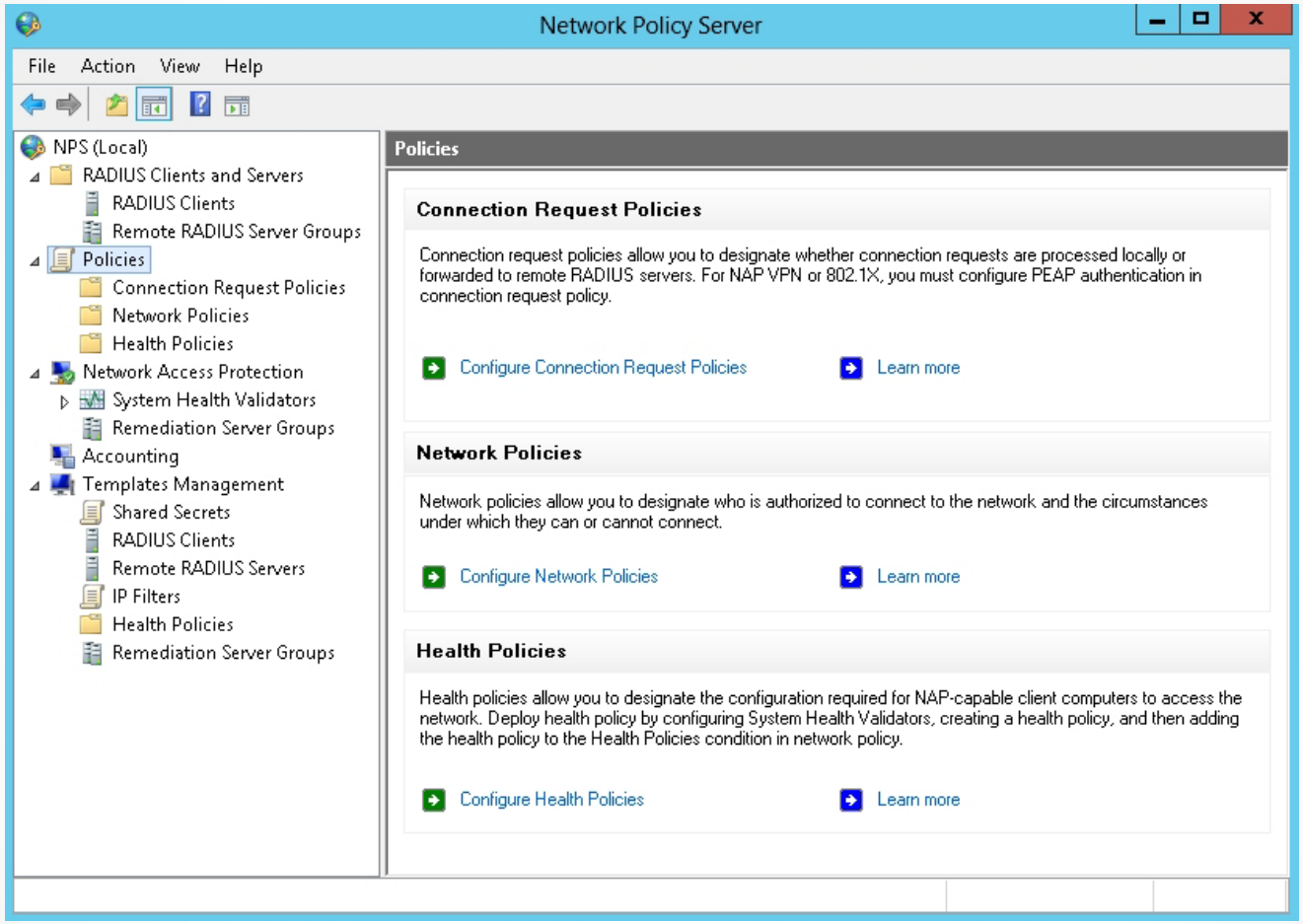
Managing NPS Policies

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 polices 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:

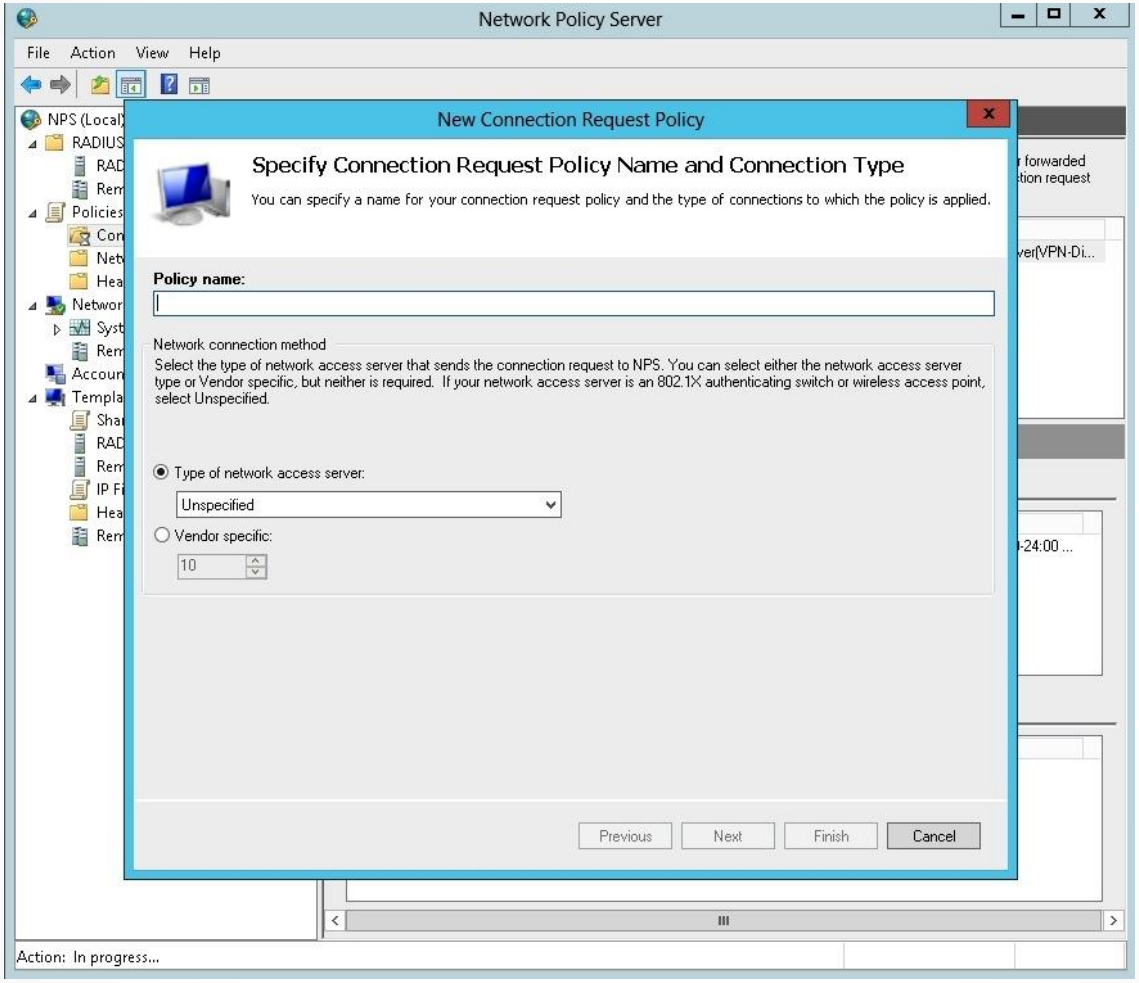
- Type of network access server such as remote access server (VPN dial-up)
- Condition that species who or what can connect to the network based on one or more RADIUS attributes
- Settings that are applied to an incoming RADIUS message such as authentication, accounting, and attribute manipulation

Configuring Connection Request Policies

Connection request policy conditions:

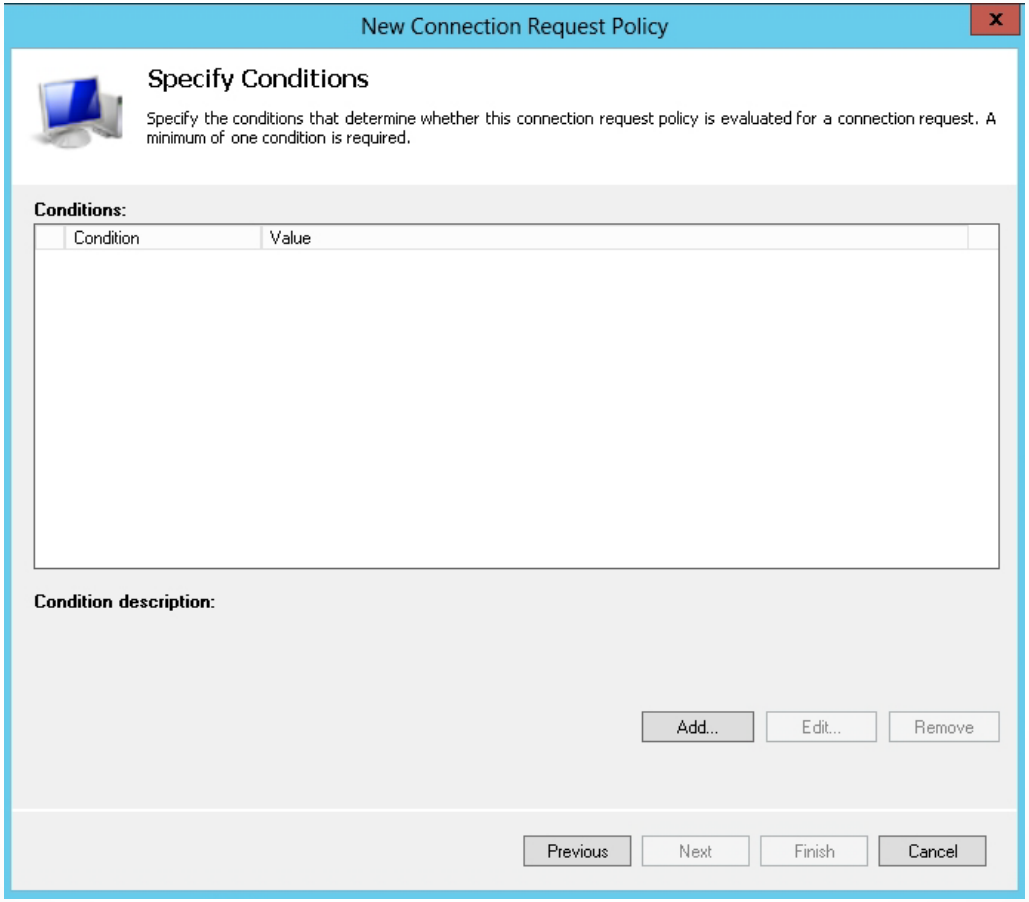
- Are one or more RADIUS attributes that are compared to the attributes of the incoming RADIUS Access-Request message.
- If there are multiple conditions, all of the conditions in the connection request message and in the connection request policy must match in order for the policy to be enforced by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

Create a Connection Request Policy



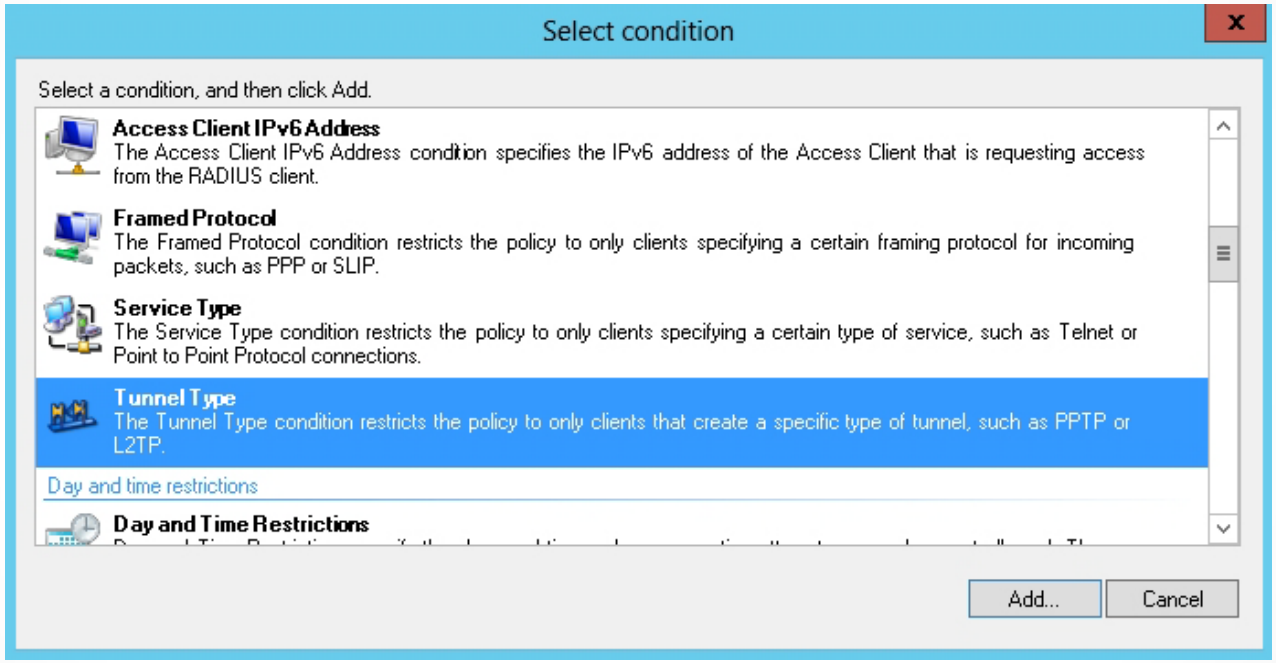
Defining the policy name

Create a Connection Request Policy



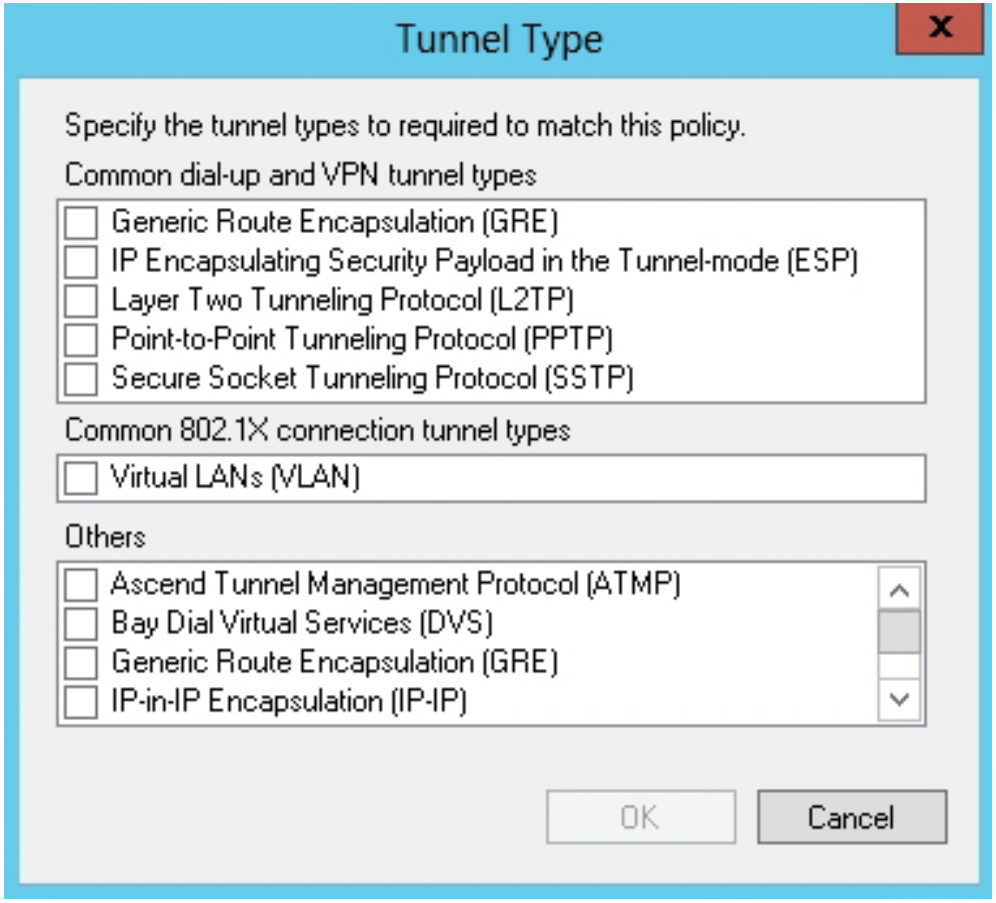
Specifying conditions

Create a Connection Request Policy



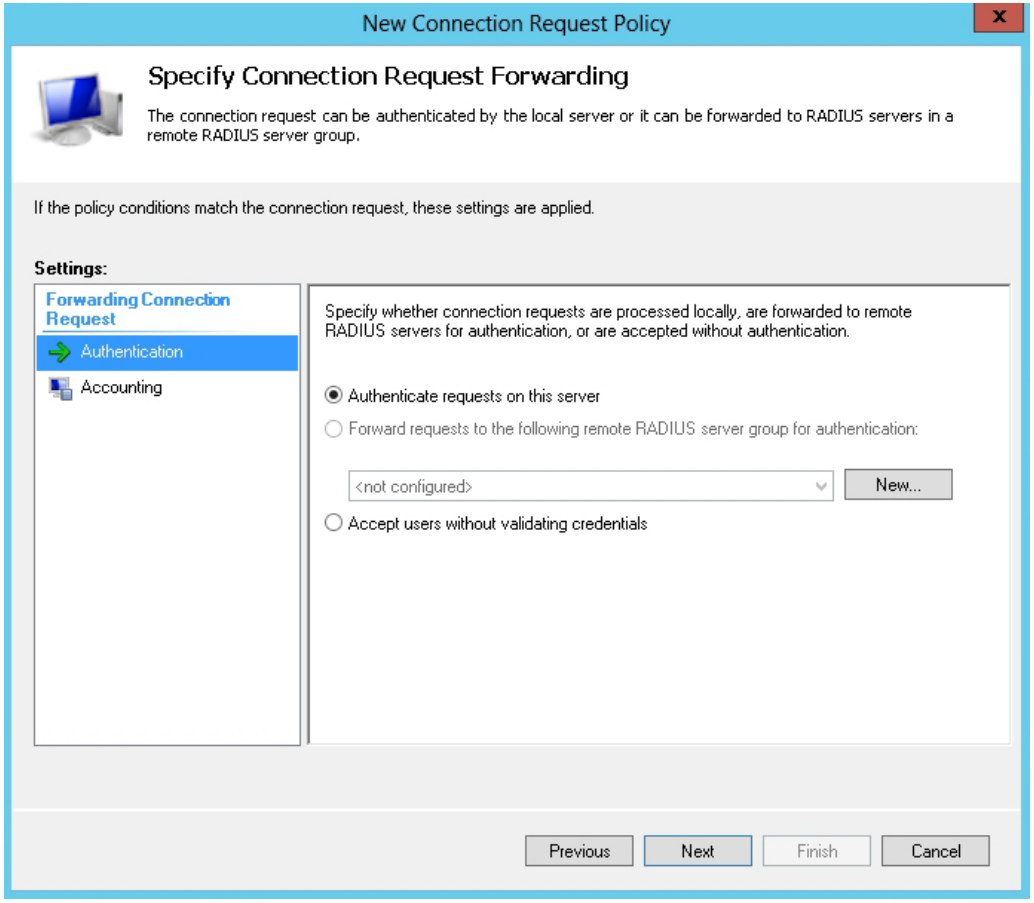
Selecting a condition

Create a Connection Request Policy



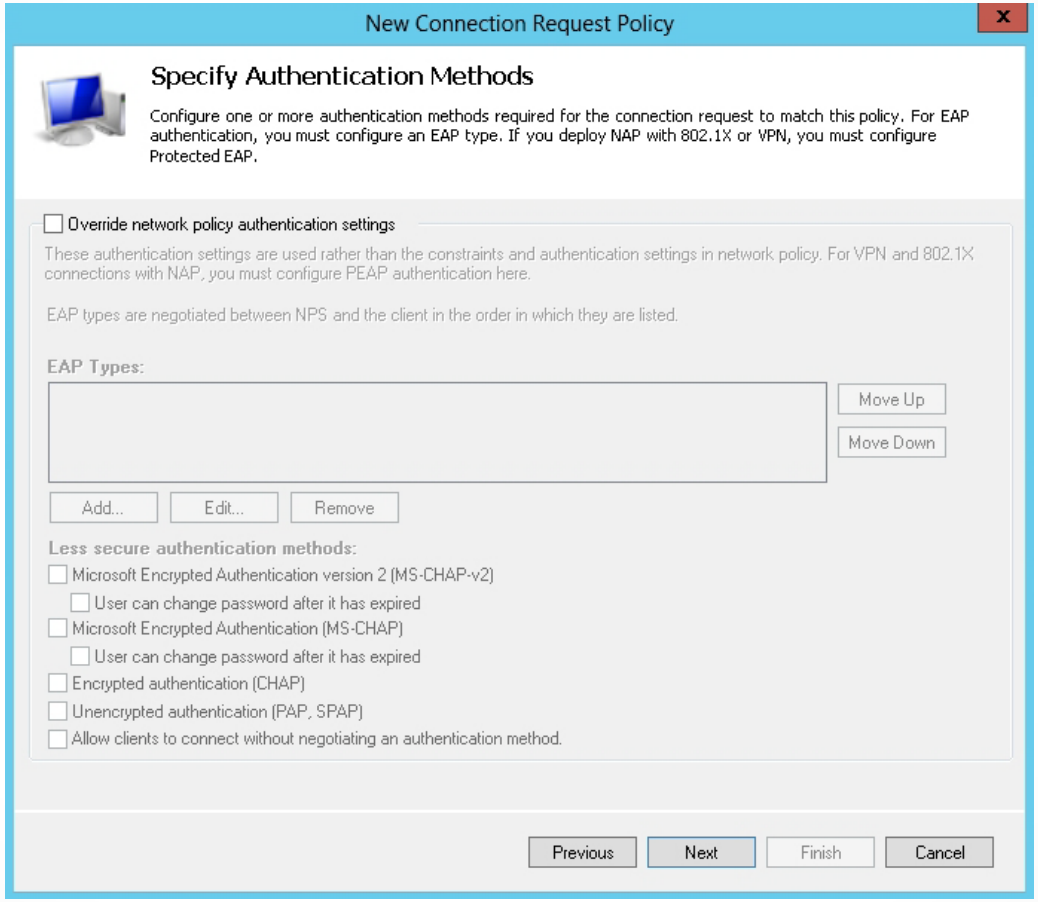
Selecting a tunnel type

Create a Connection Request Policy



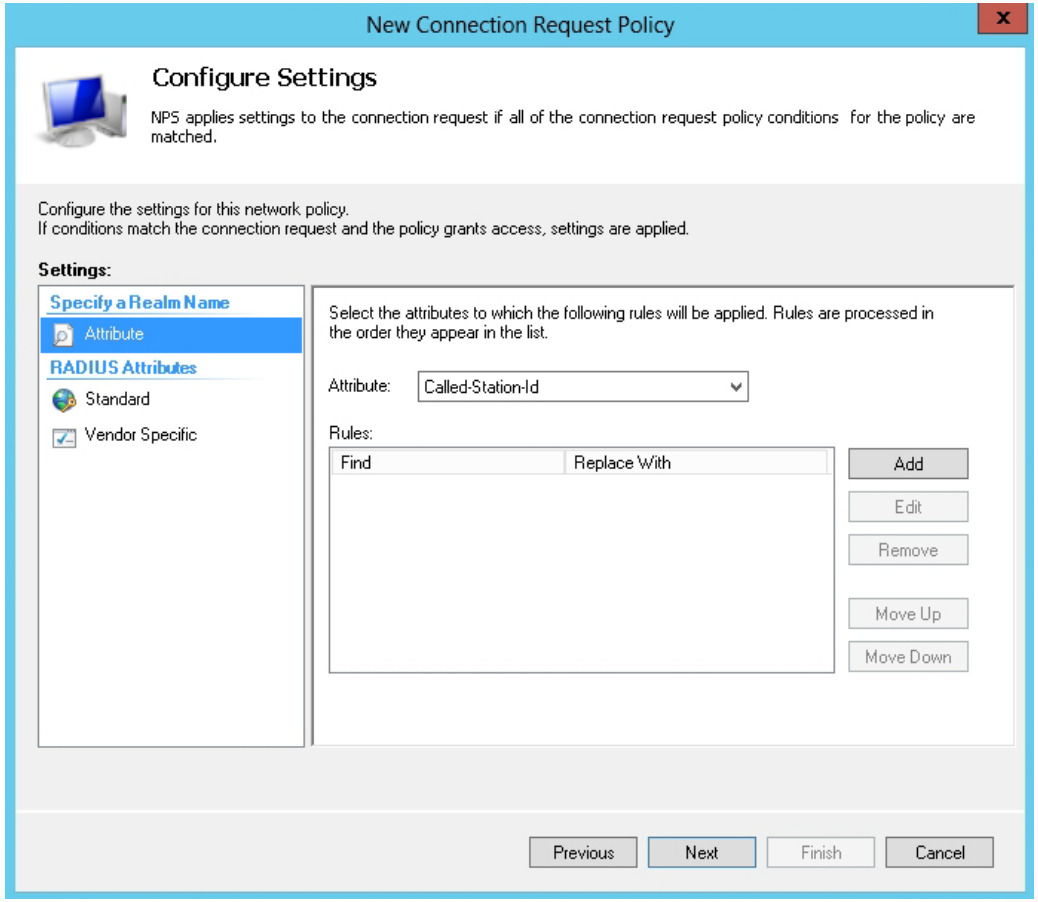
Specifying Connection Request Forwarding page

Create a Connection Request Policy



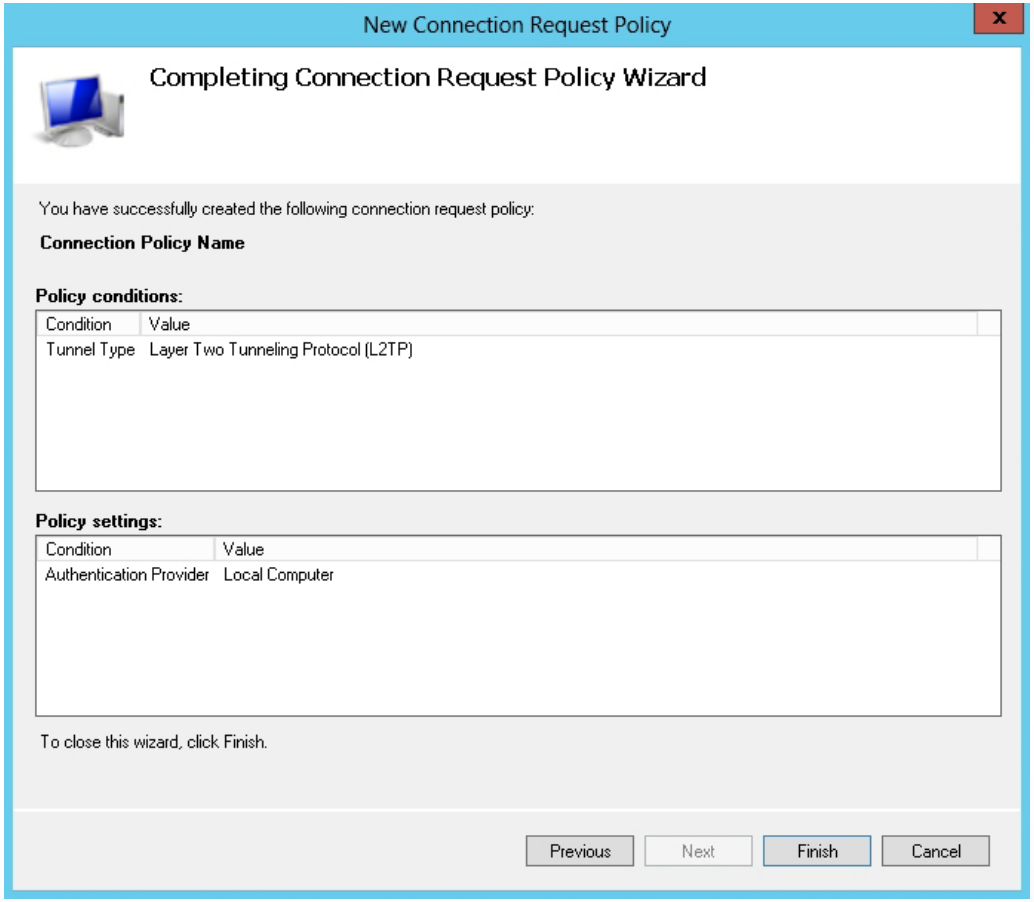
Specifying Authentication Methods page

Create a Connection Request Policy



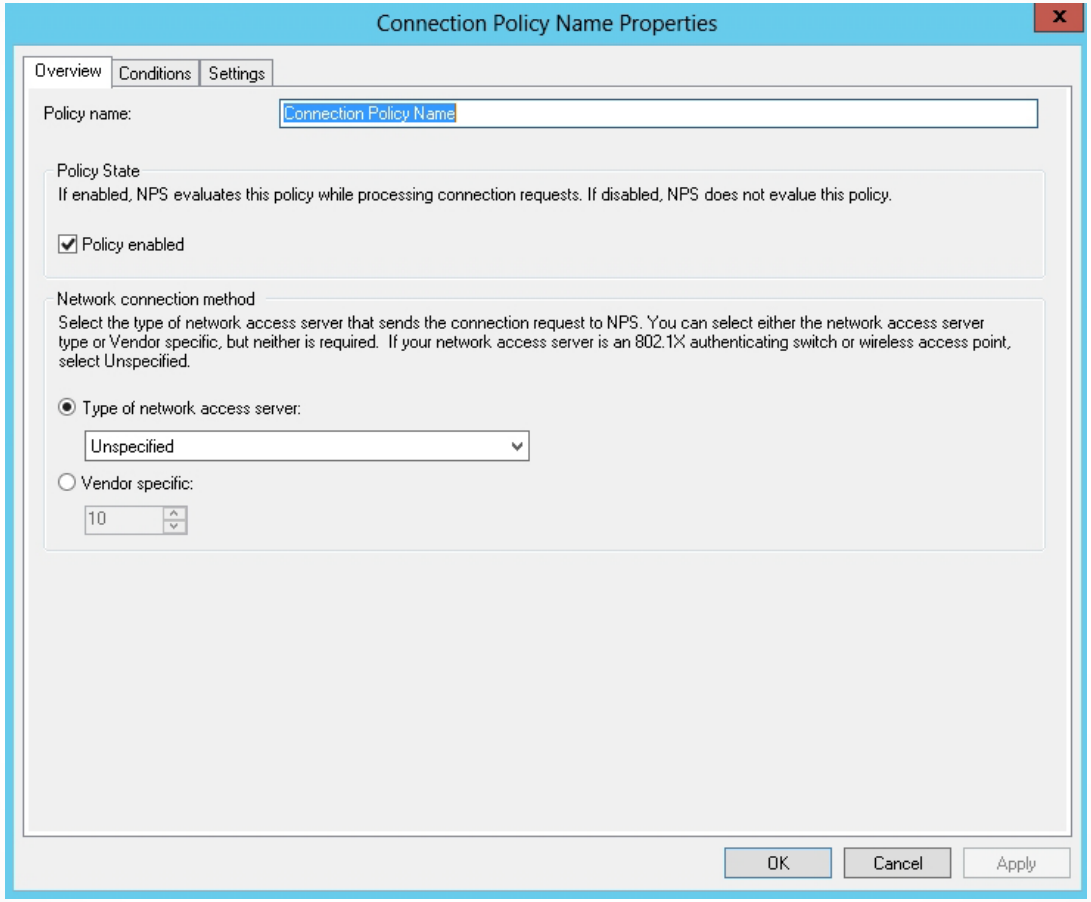
Configuring Settings page

Create a Connection Request Policy



Completing Connection Request Policy Wizard

Create a Connection Request Policy



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:

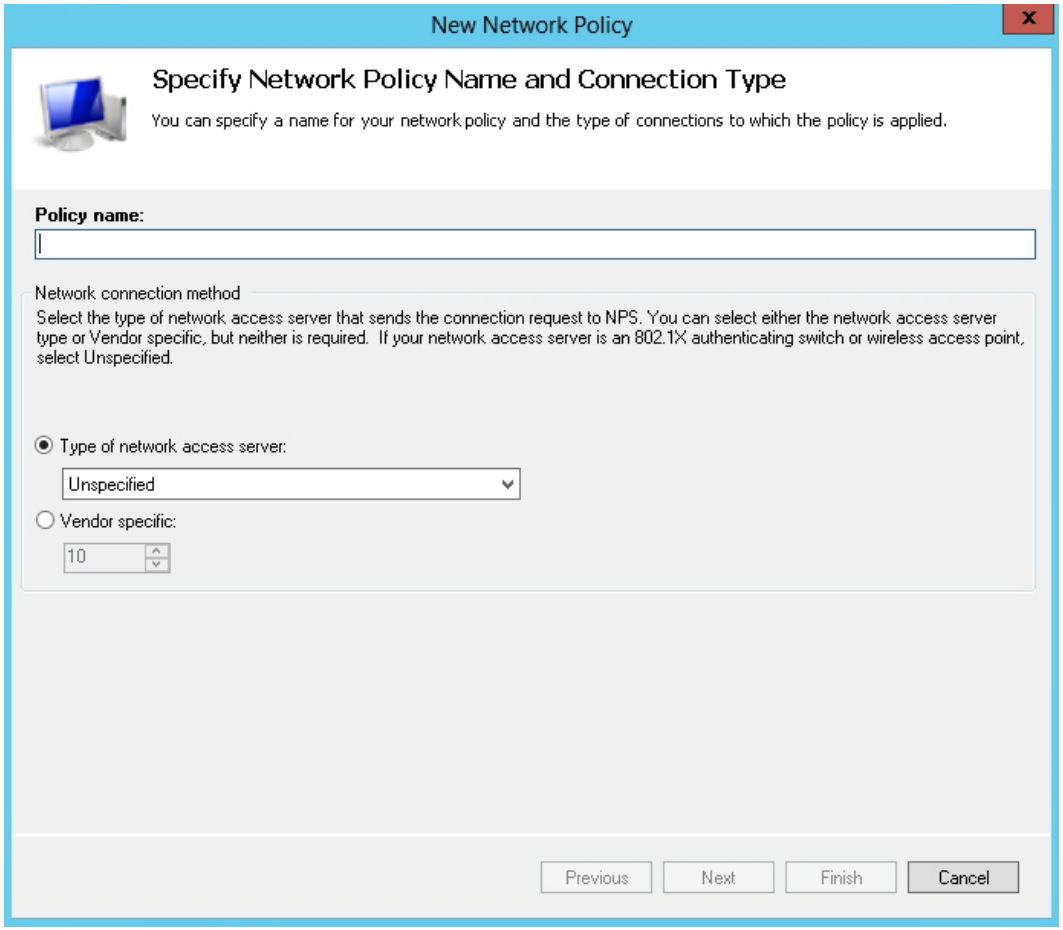
1. User attempts to initiate a remote access connection.
2. Remote access server checks the conditions in the first configured NPS network policy.
3. If the conditions of this NPS network policy do not match, the remote access server checks the next configured NPS network policies. It keeps checking 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):

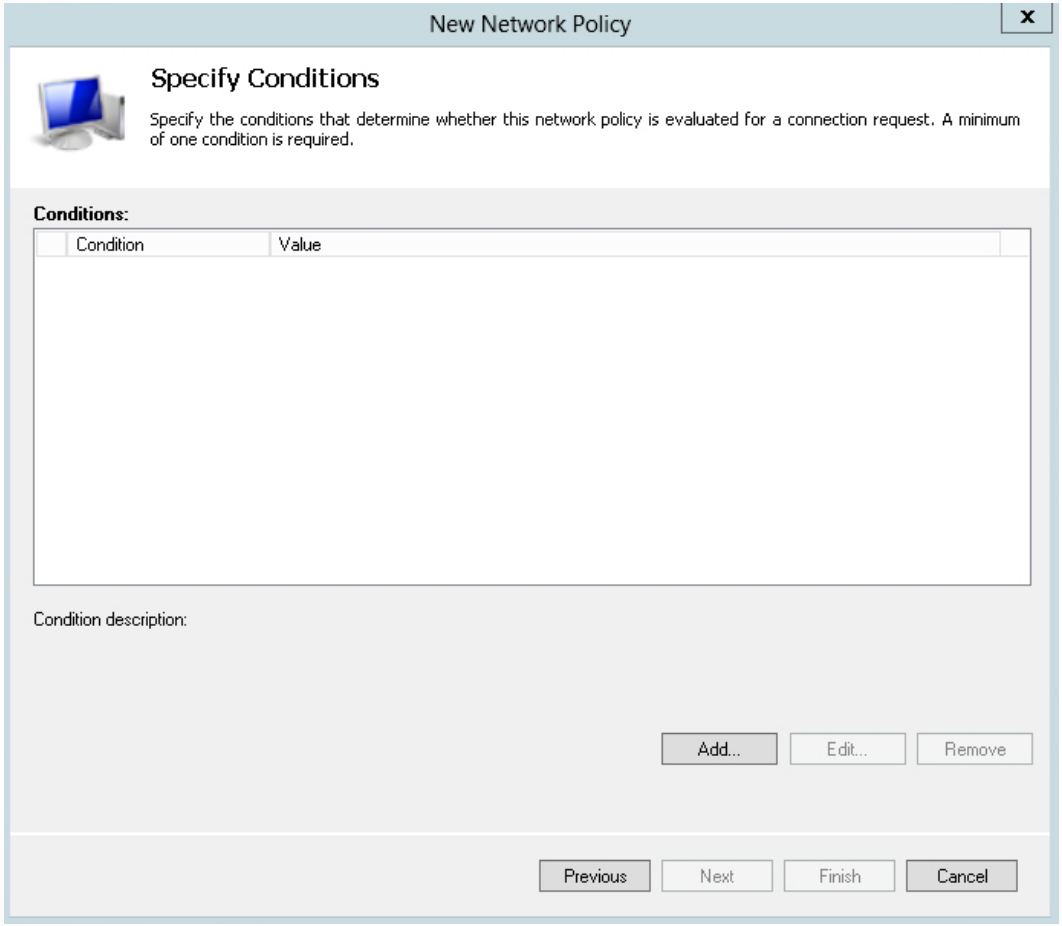
5. Once the remote access server finds an NPS network policy with conditions that match the incoming connection attempt, the remote access server checks any constraints (such as time of day or minimum encryption level) that have been configured for the policy.
6. If the connection attempt does not match 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



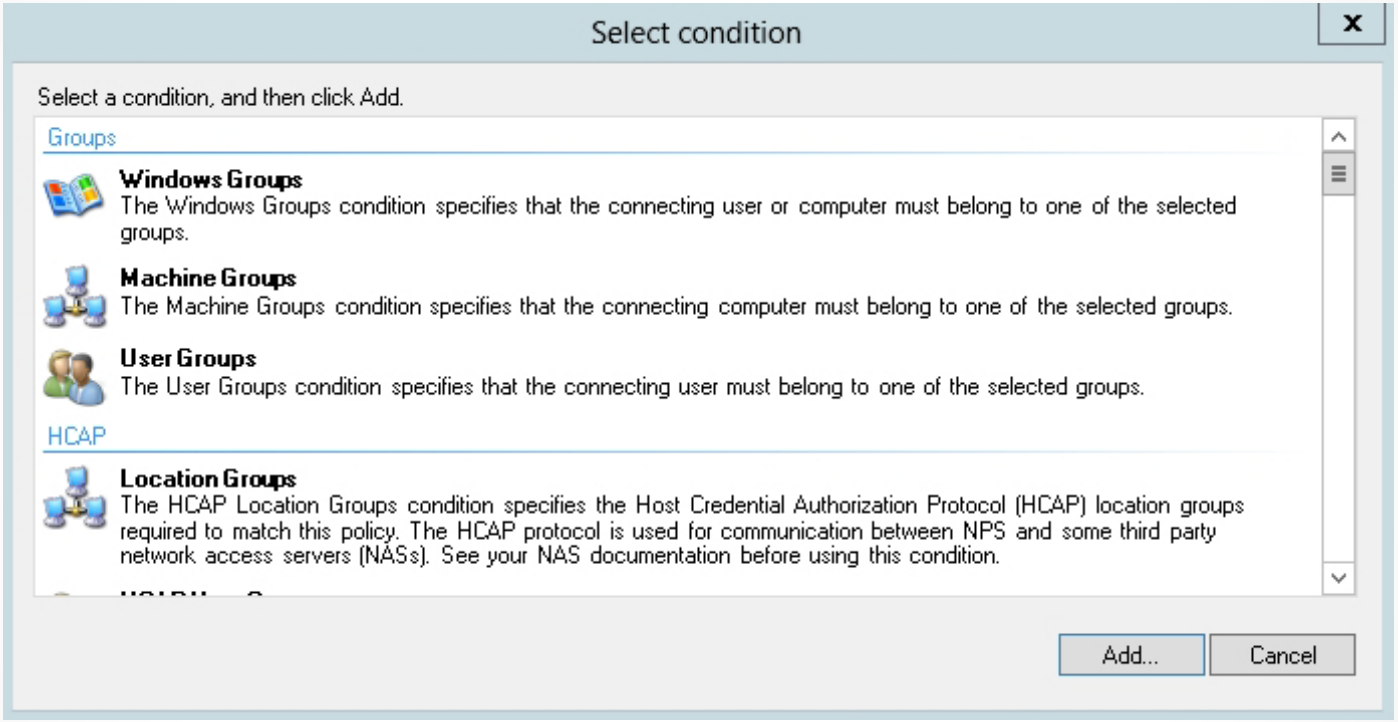
Starting the New Network Policy Wizard

Create a Network Policy



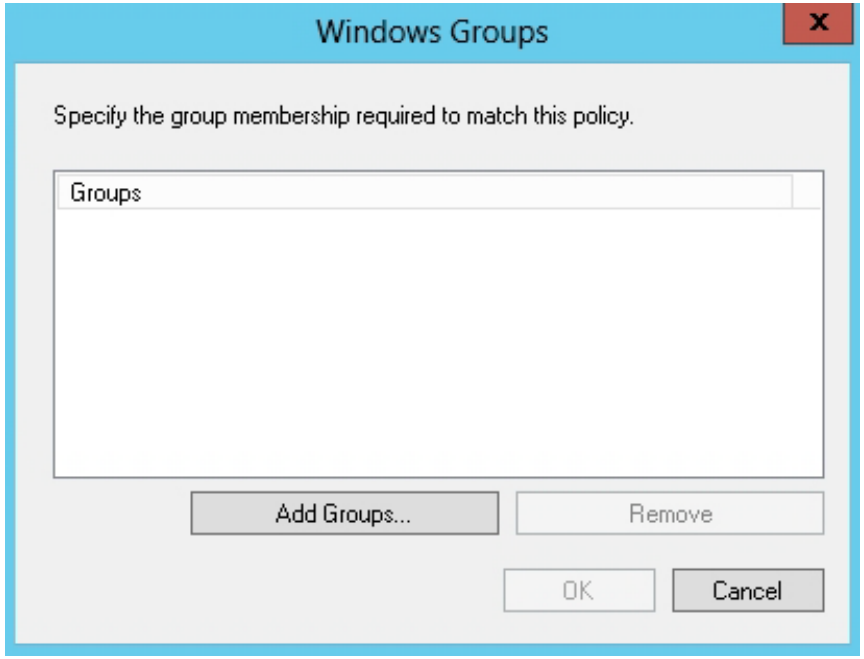
Specifying conditions

Create a Network Policy



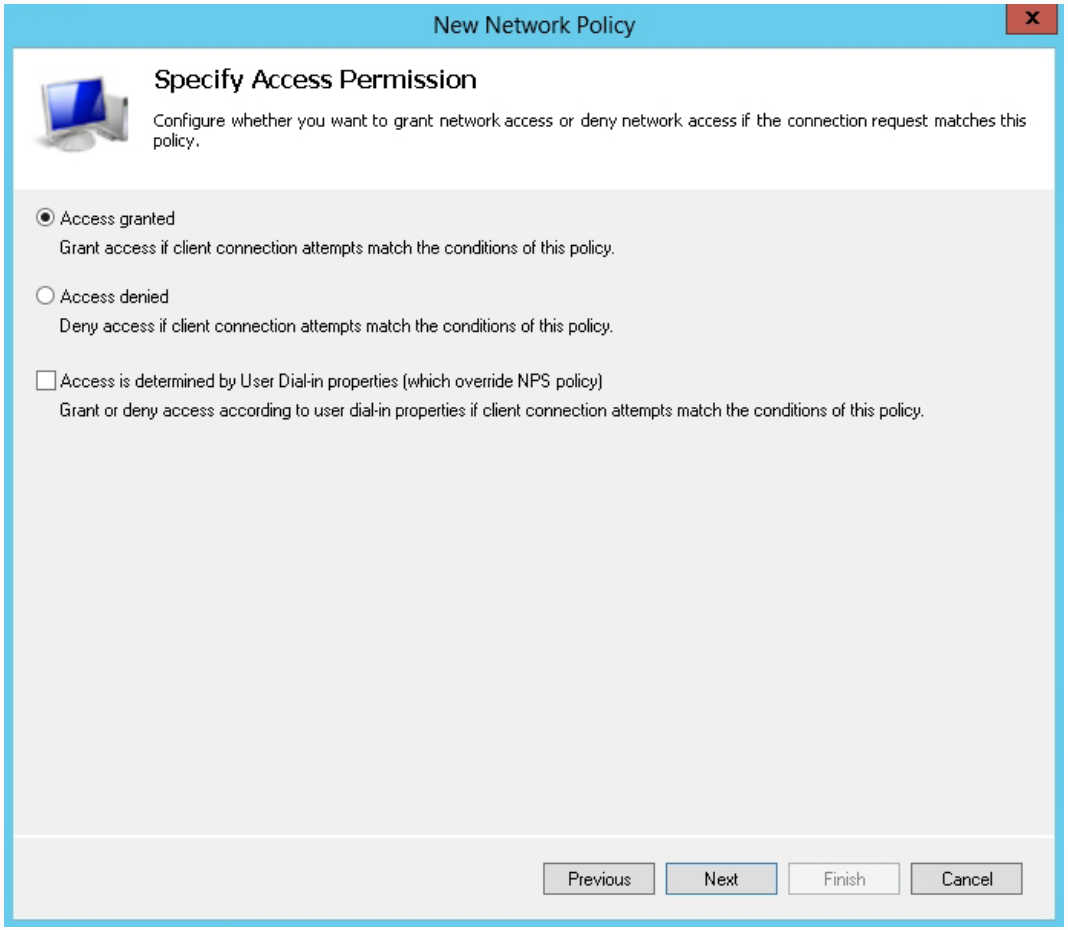
Selecting conditions

Create a Network Policy



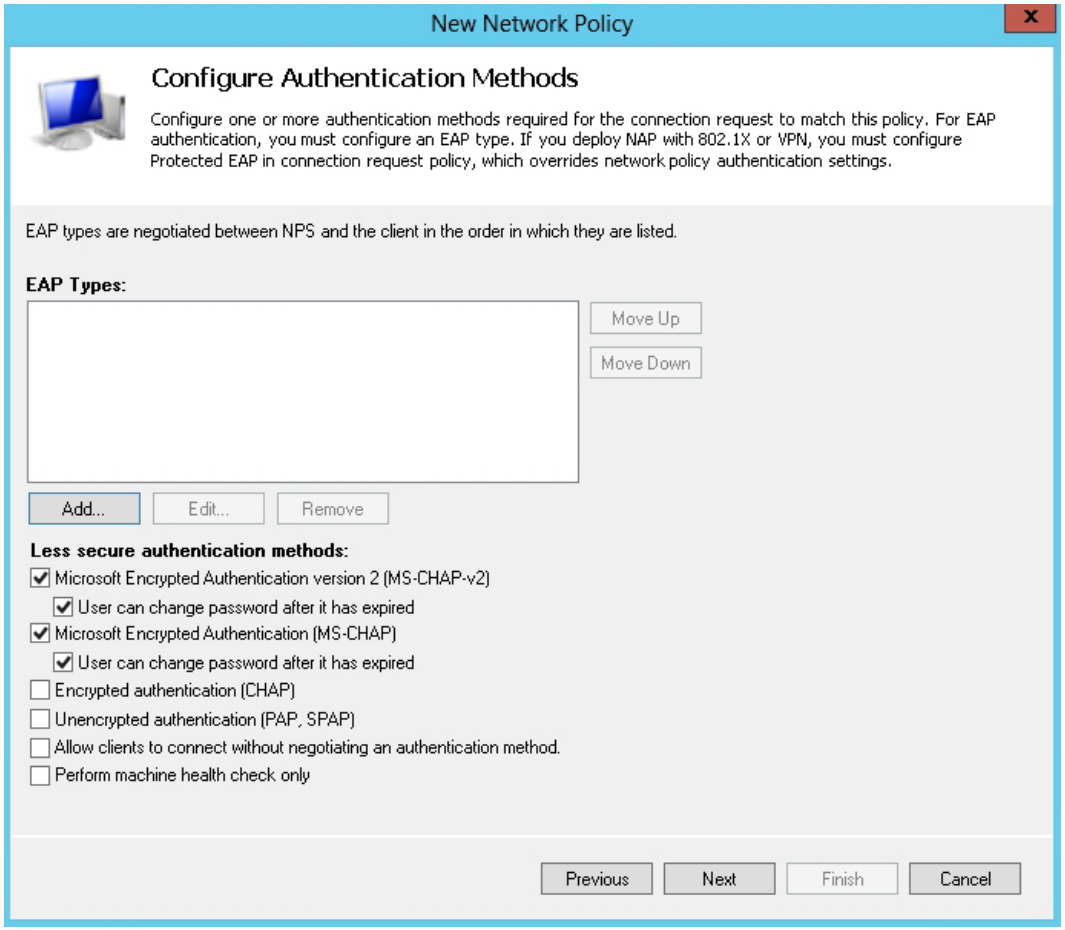
Adding Windows groups

Create a Network Policy



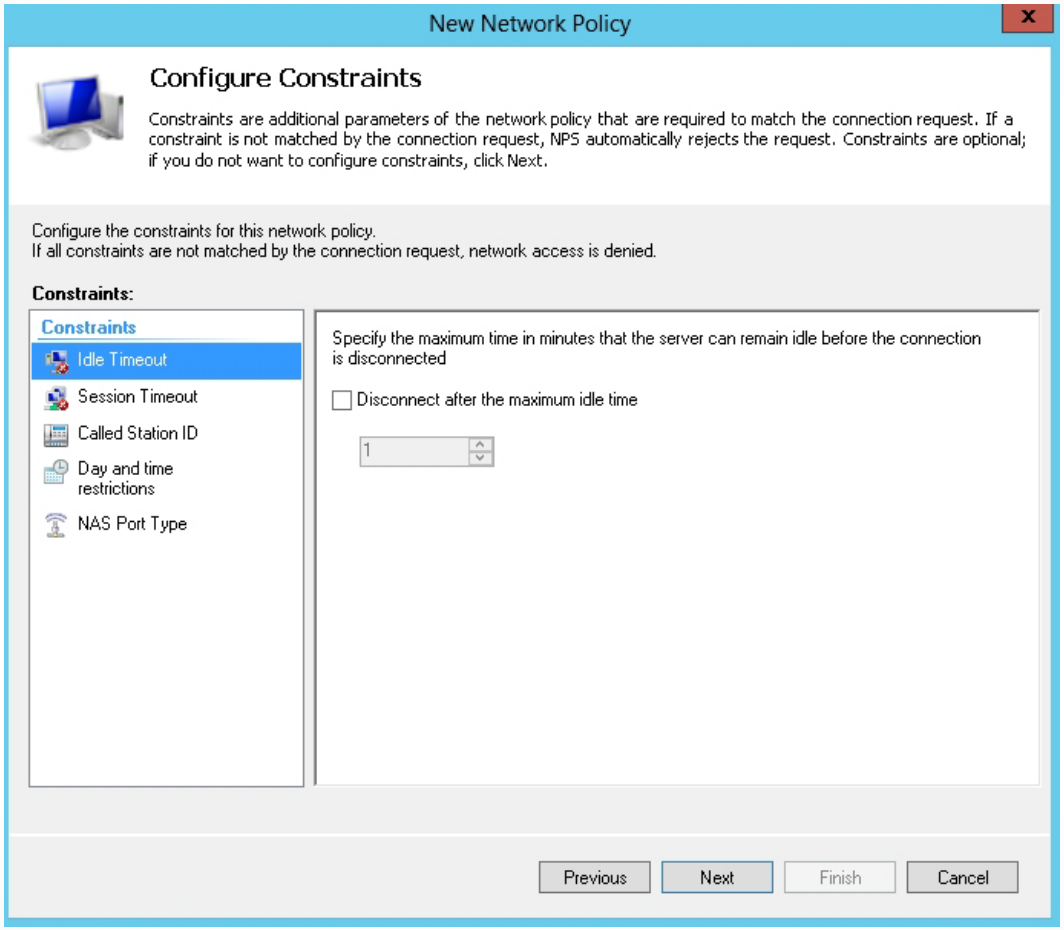
Specifying access permissions

Create a Network Policy



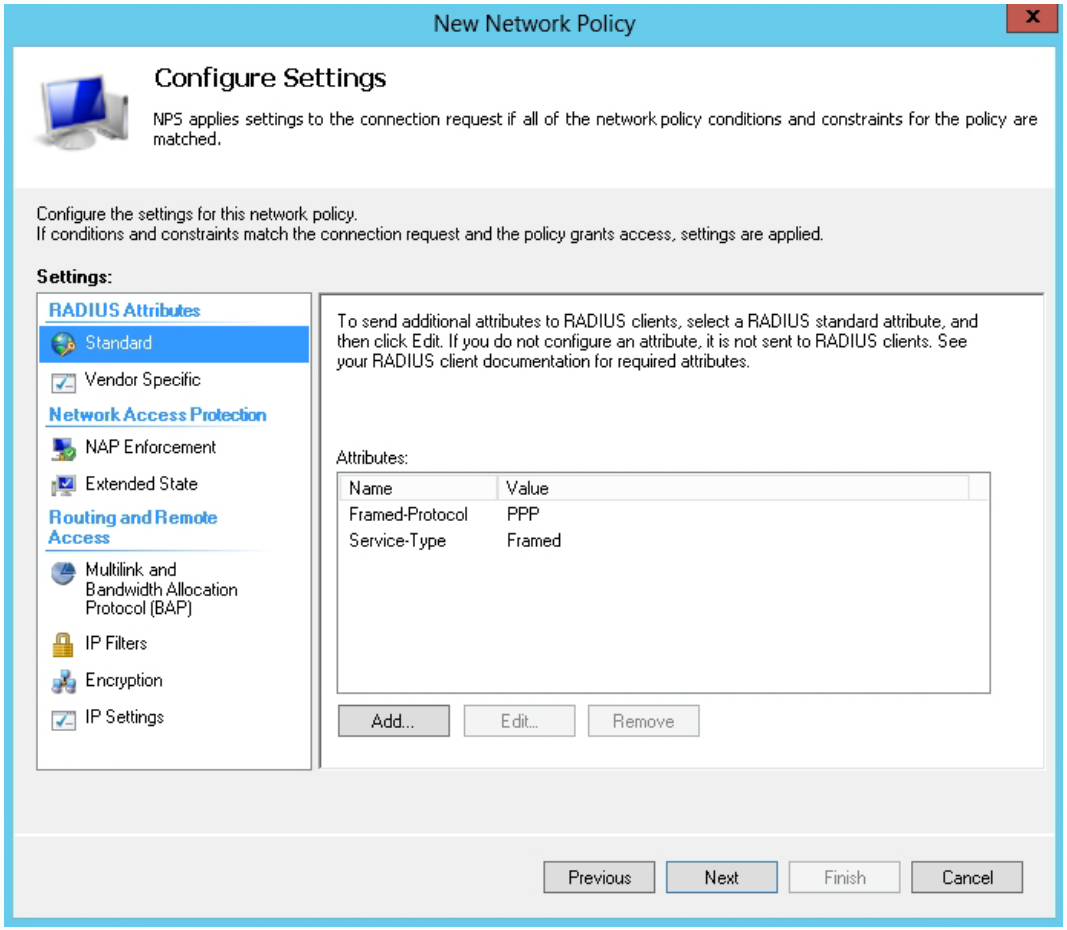
Configuring authentication methods

Create a Network Policy



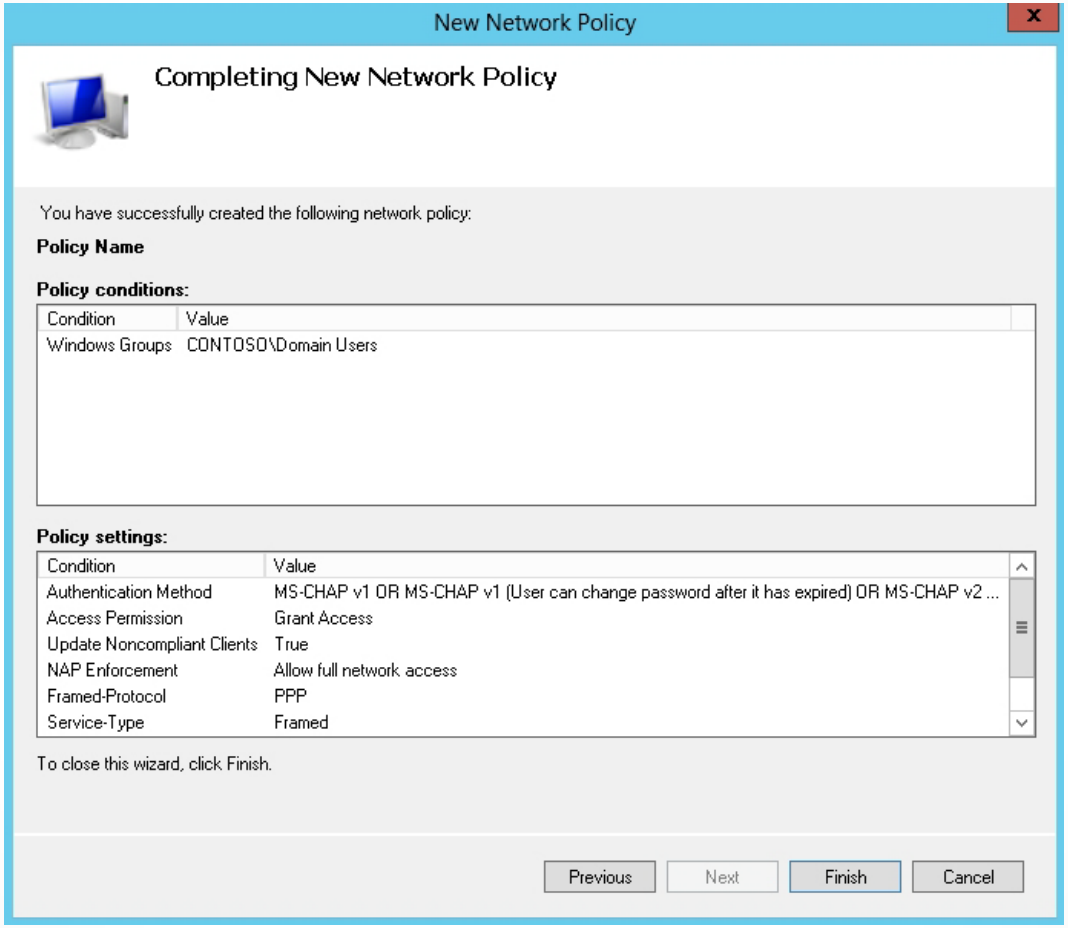
Configuring constraints

Create a Network Policy



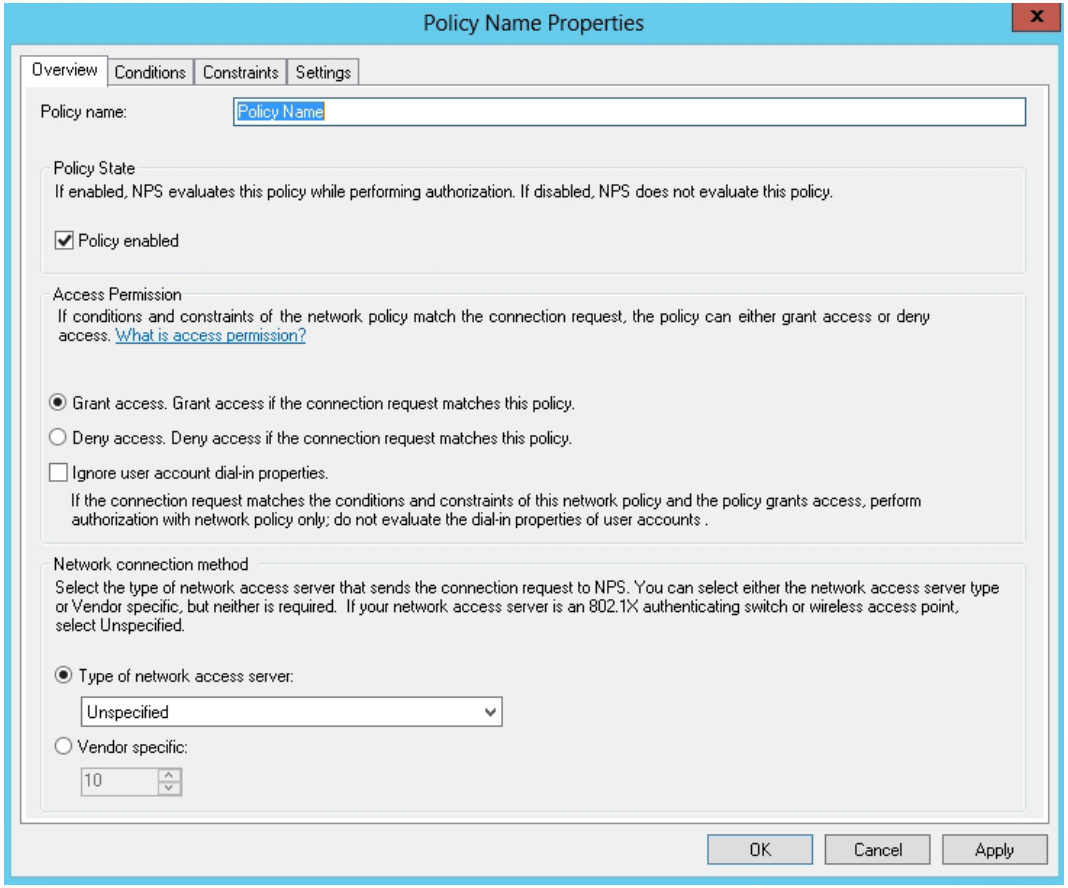
Configuring settings

Create a Network Policy



Completing new network policies

Create a Network Policy

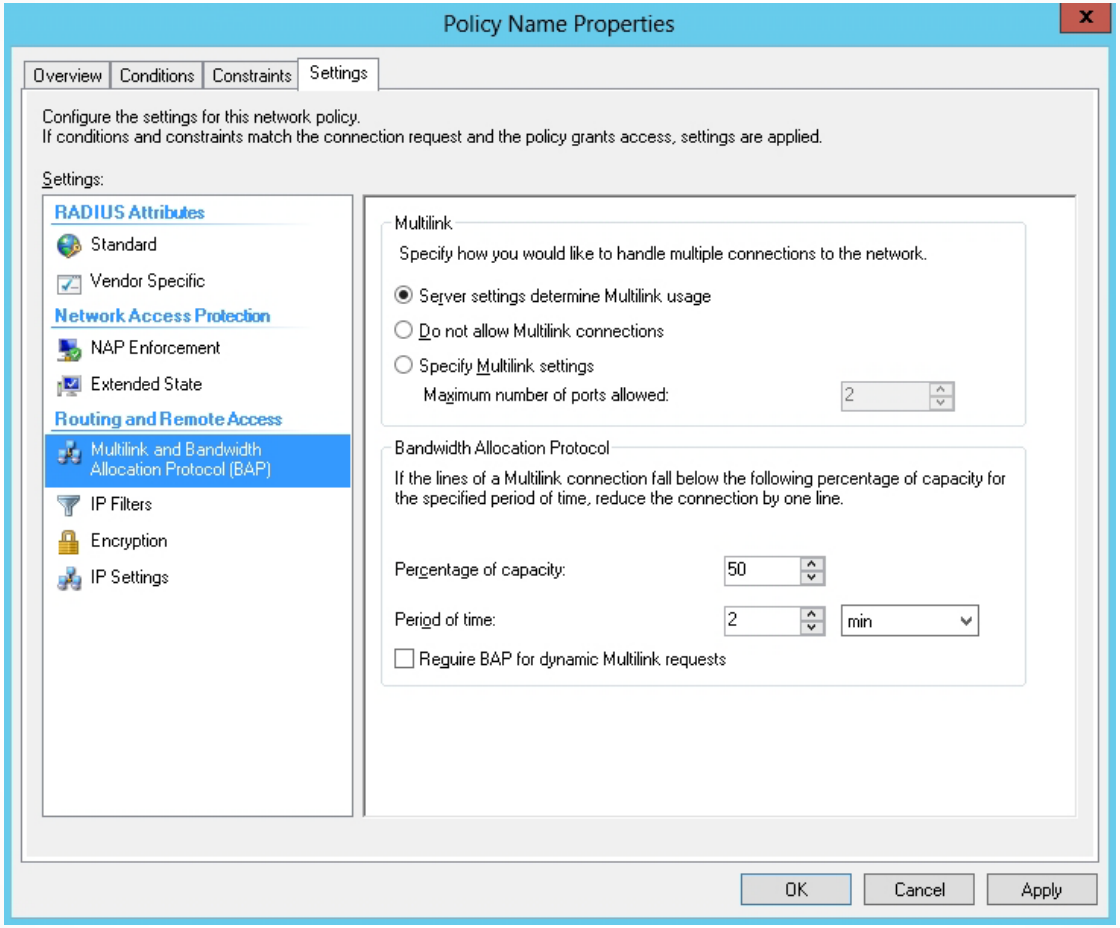


Configuring Network Policy properties

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

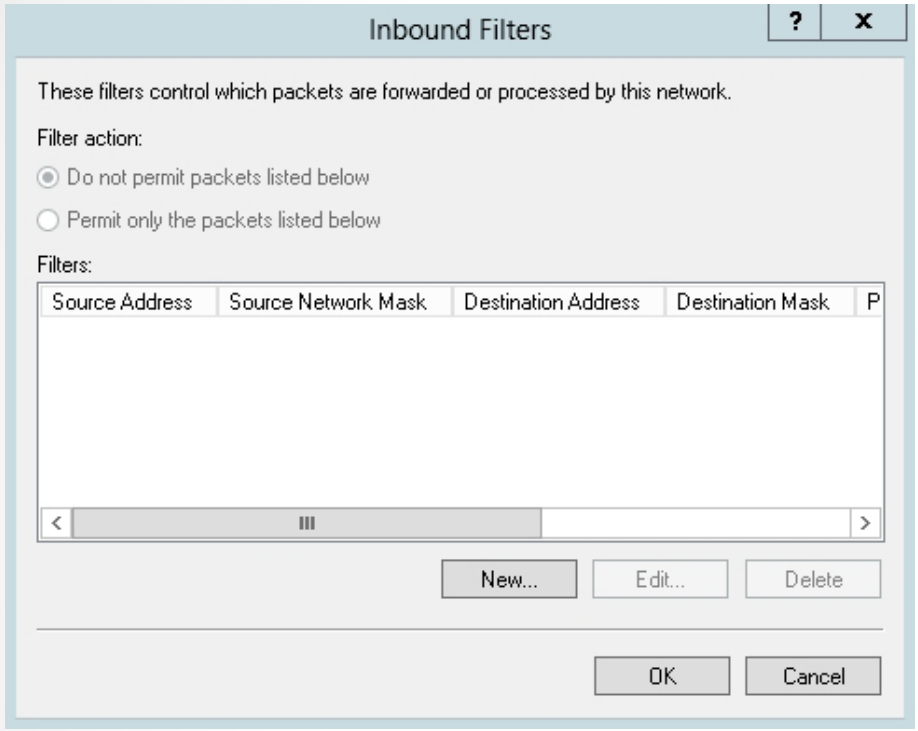
IP Filters

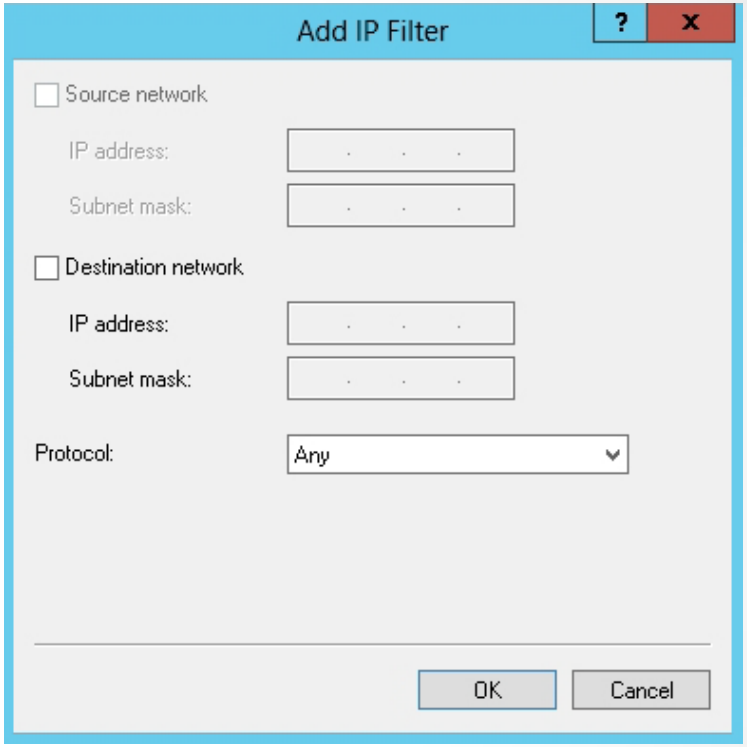
Allow you to control which packets are allowed through the network connection based on IP address.

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



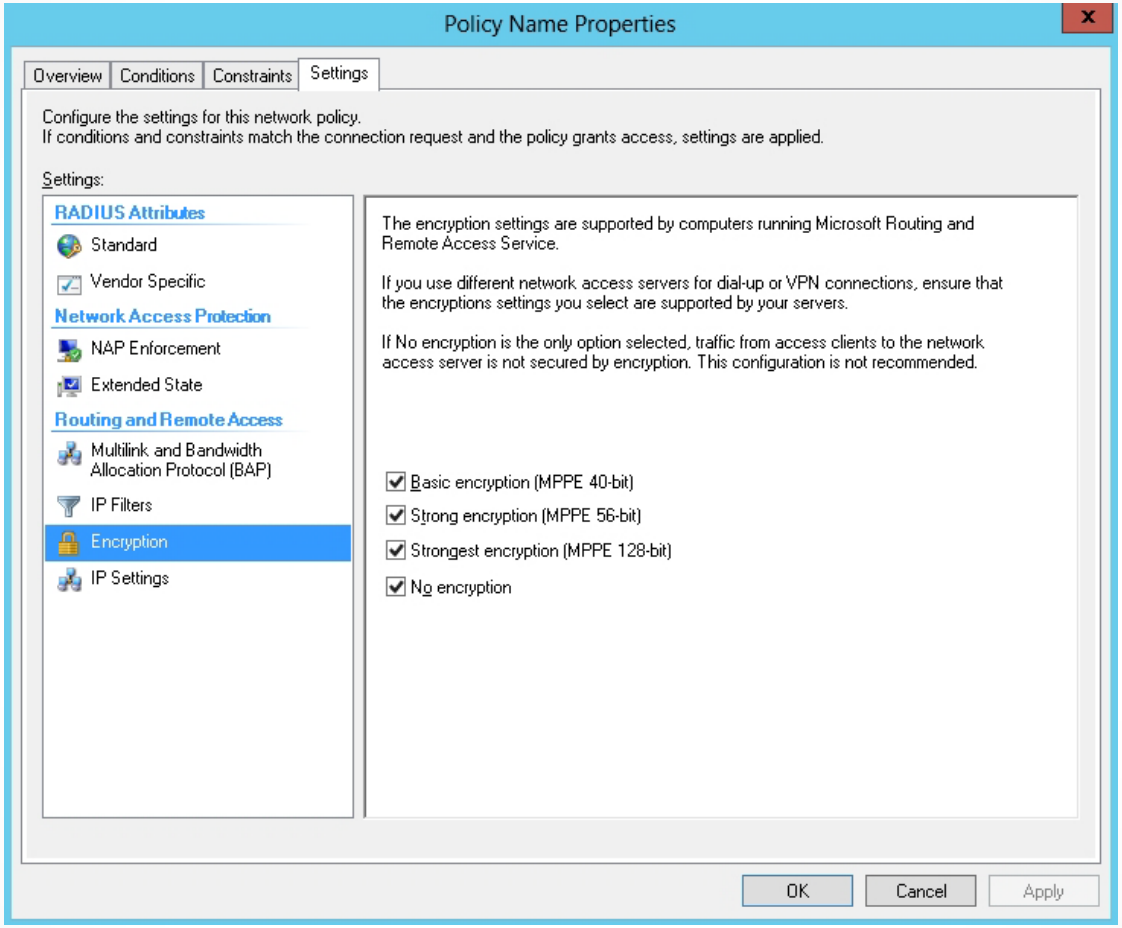


Configuring an IPv4 Inbound filter

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



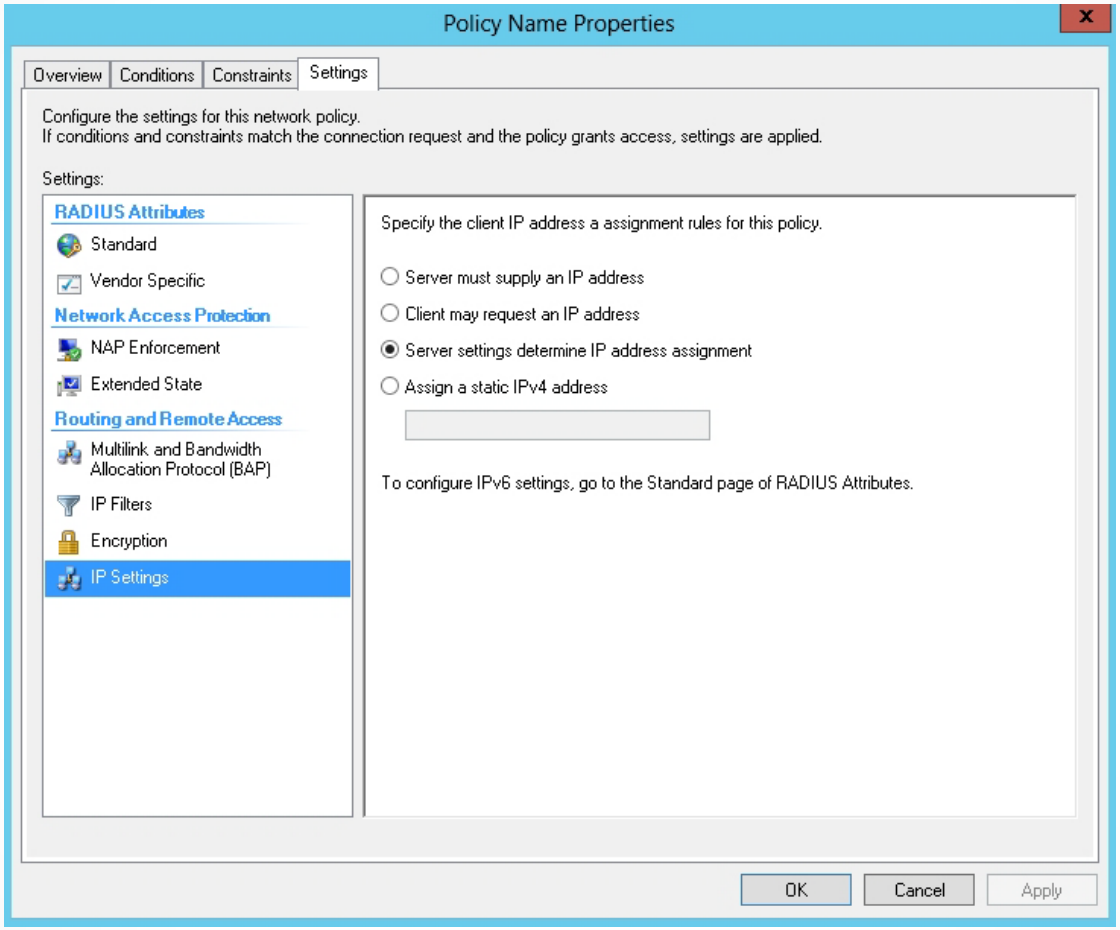
Configuring encryption settings

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



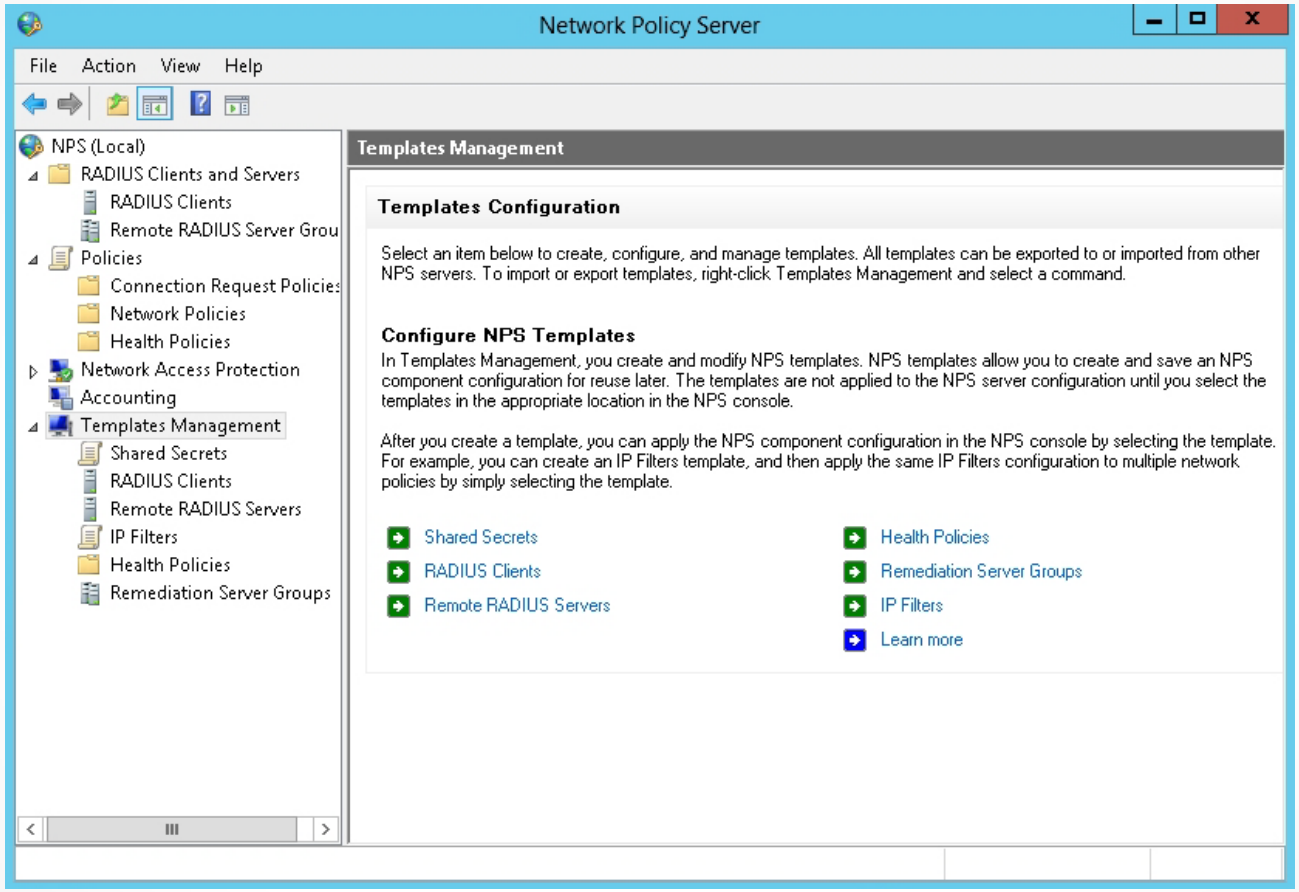
Configuring IP assignment settings

Managing NPS Templates

NPS template types available in Templates Management:

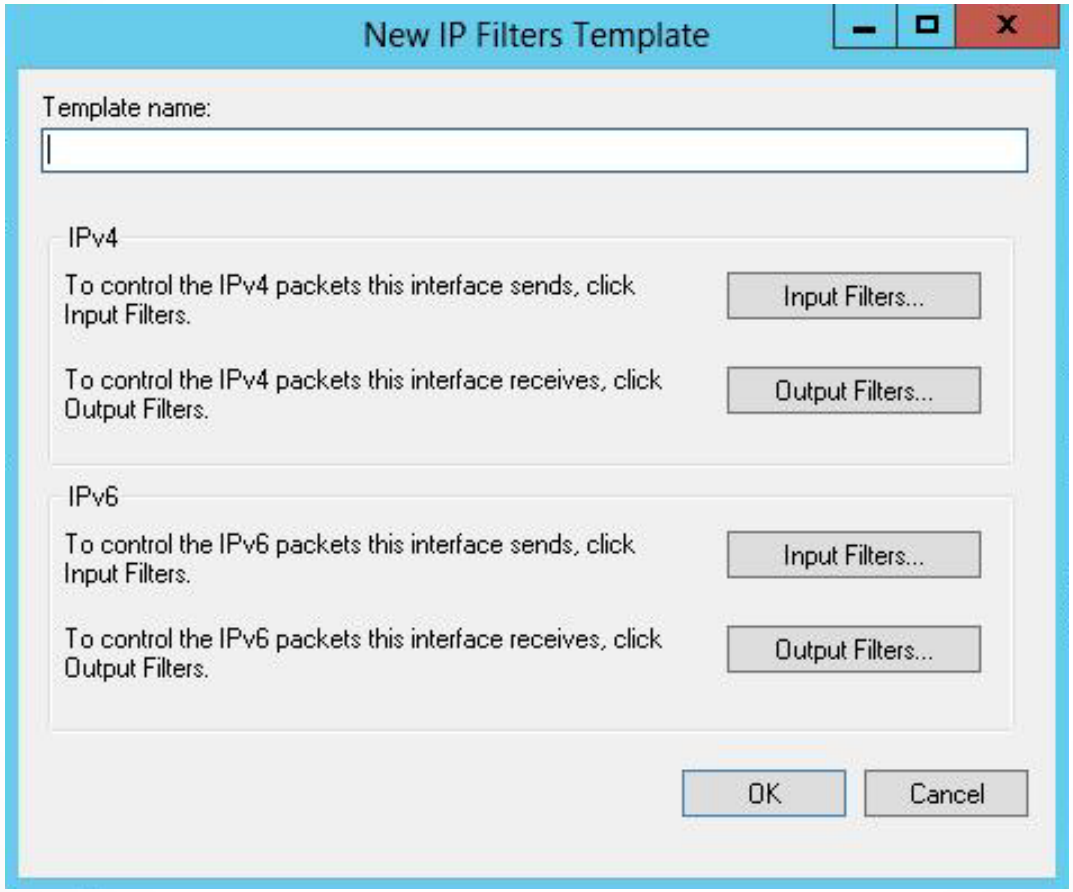
- Shared Secrets
- RADIUS Clients
- Remote RADIUS Servers
- IP Filters
- Health Policies
- Remediation Server Groups

Managing NPS Templates



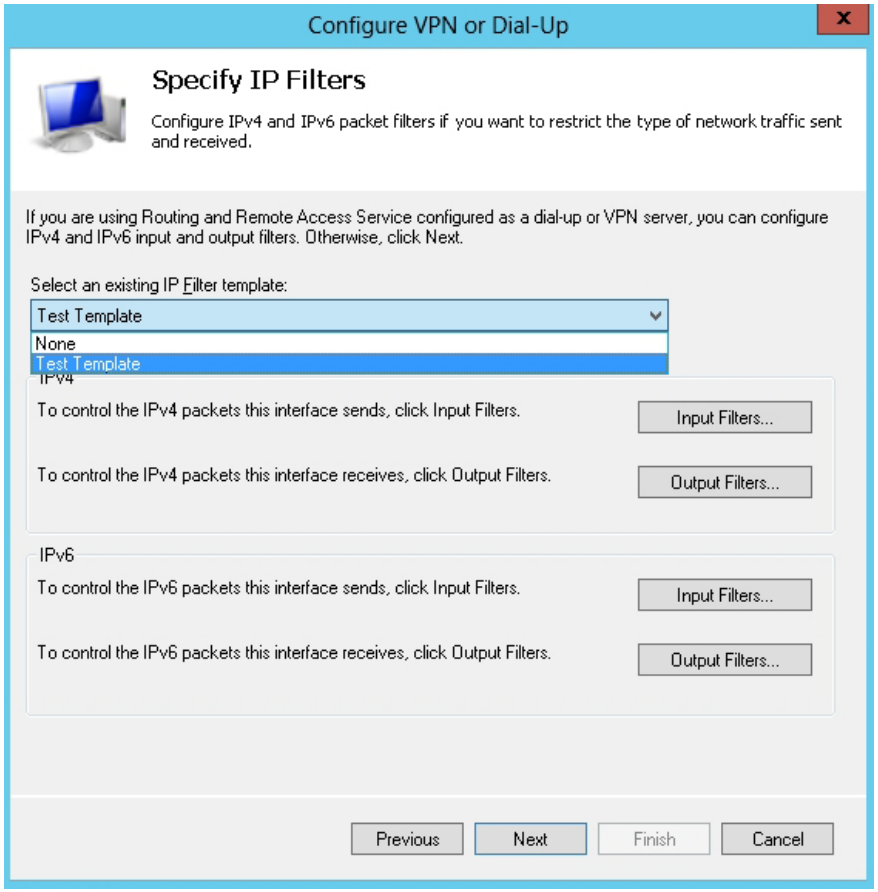
Configuring templates in NPS

Managing NPS Templates



Creating a new IP filter template

Managing NPS Templates



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.