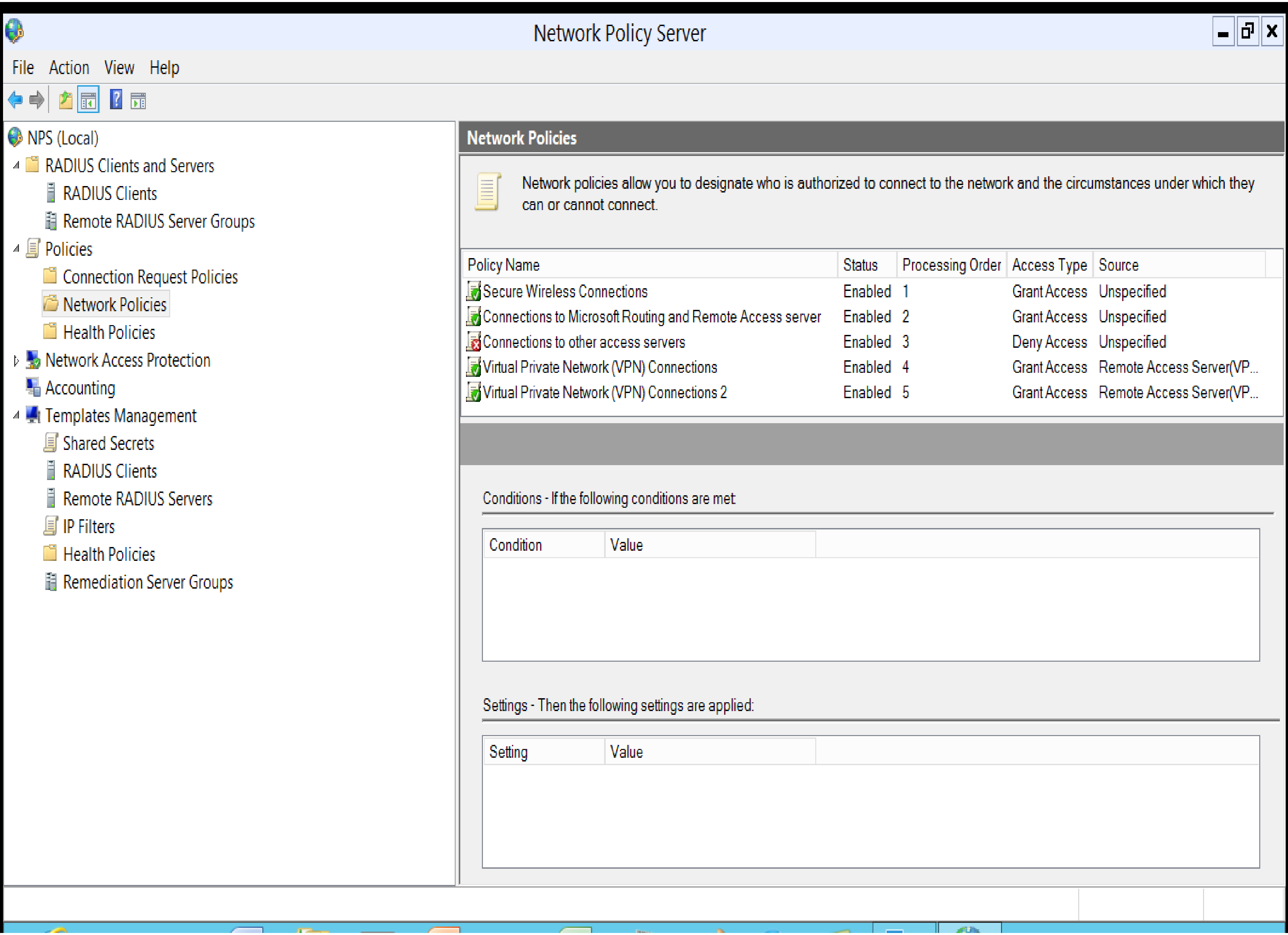
Configure network policies



Network Policies

Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

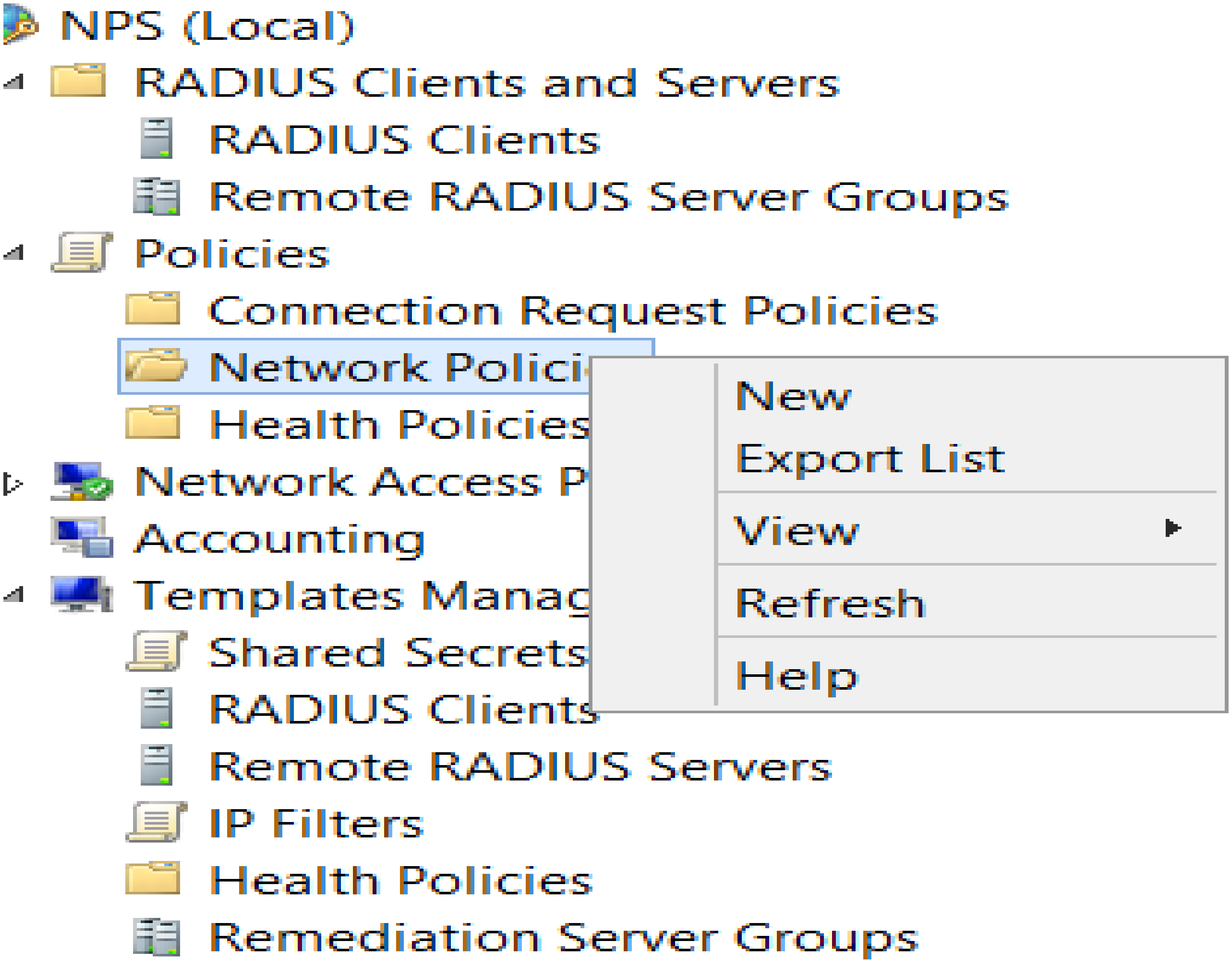
Policy Name	Status	Processing Order	Access Type	Source
Secure Wireless Connections	Enabled	1	Grant Access	Unspecified
Connections to Microsoft Routing and Remote Access server	Enabled	2	Grant Access	Unspecified
Connections to other access servers	Enabled	3	Deny Access	Unspecified
Virtual Private Network (VPN) Connections	Enabled	4	Grant Access	Remote Access Server(VP...
Virtual Private Network (VPN) Connections 2	Enabled	5	Grant Access	Remote Access Server(VP...

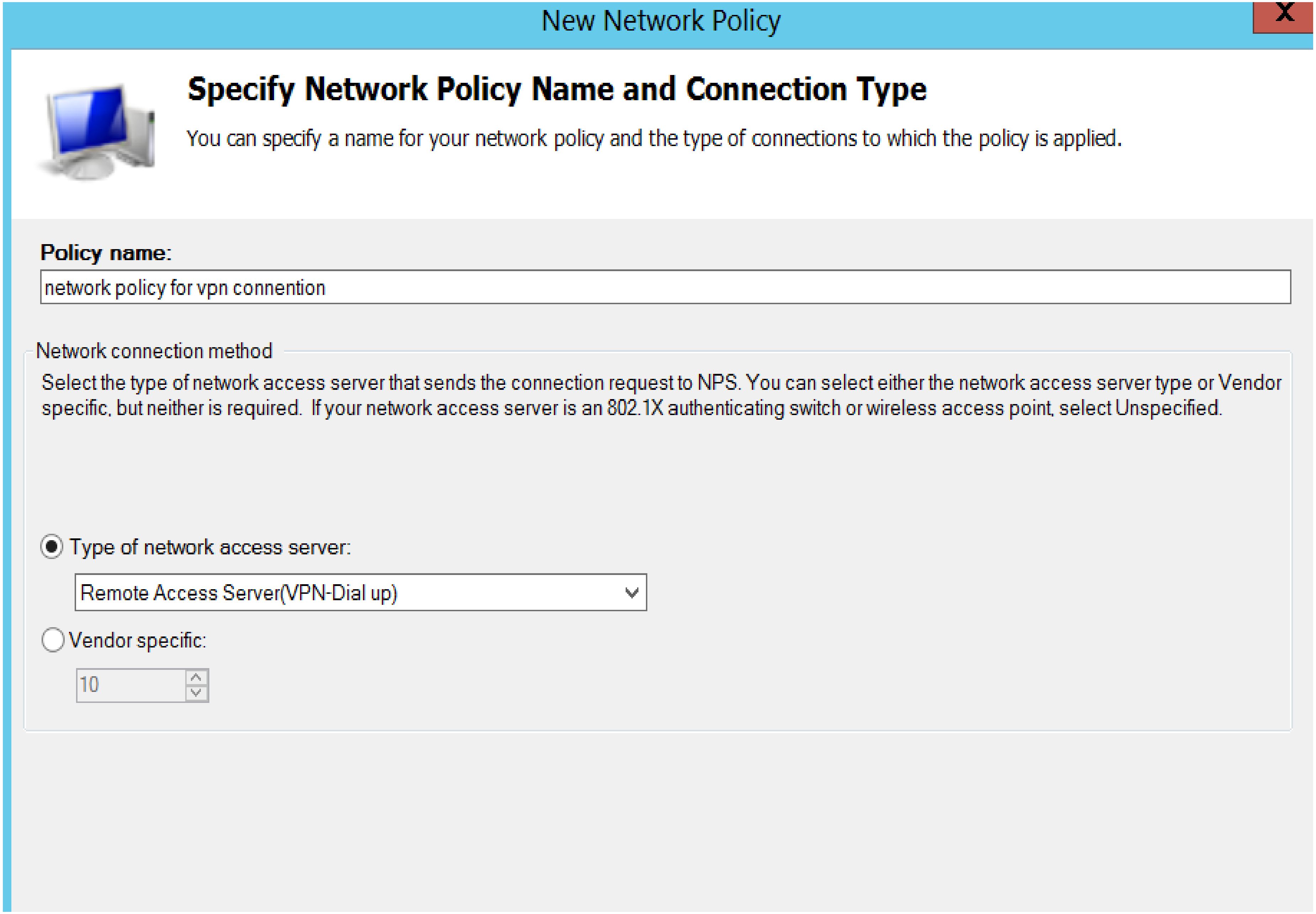
Conditions - If the following conditions are met:

Condition	Value

Settings - Then the following settings are applied:

Setting	Value


NPS (Local)
RADIUS Clients and Servers
RADIUS Clients
Remote RADIUS Server Groups
Policies
Connection Request Policies
Network Polici
Health Policies
Network Access P
Accounting
Templates Manag
Shared Secrets
RADIUS Clients
Remote RADIUS Servers
IP Filters
Health Policies
Remediation Server Groups
New
Export List
View
Refresh
Help



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 policy for vpn connention

Network connection method

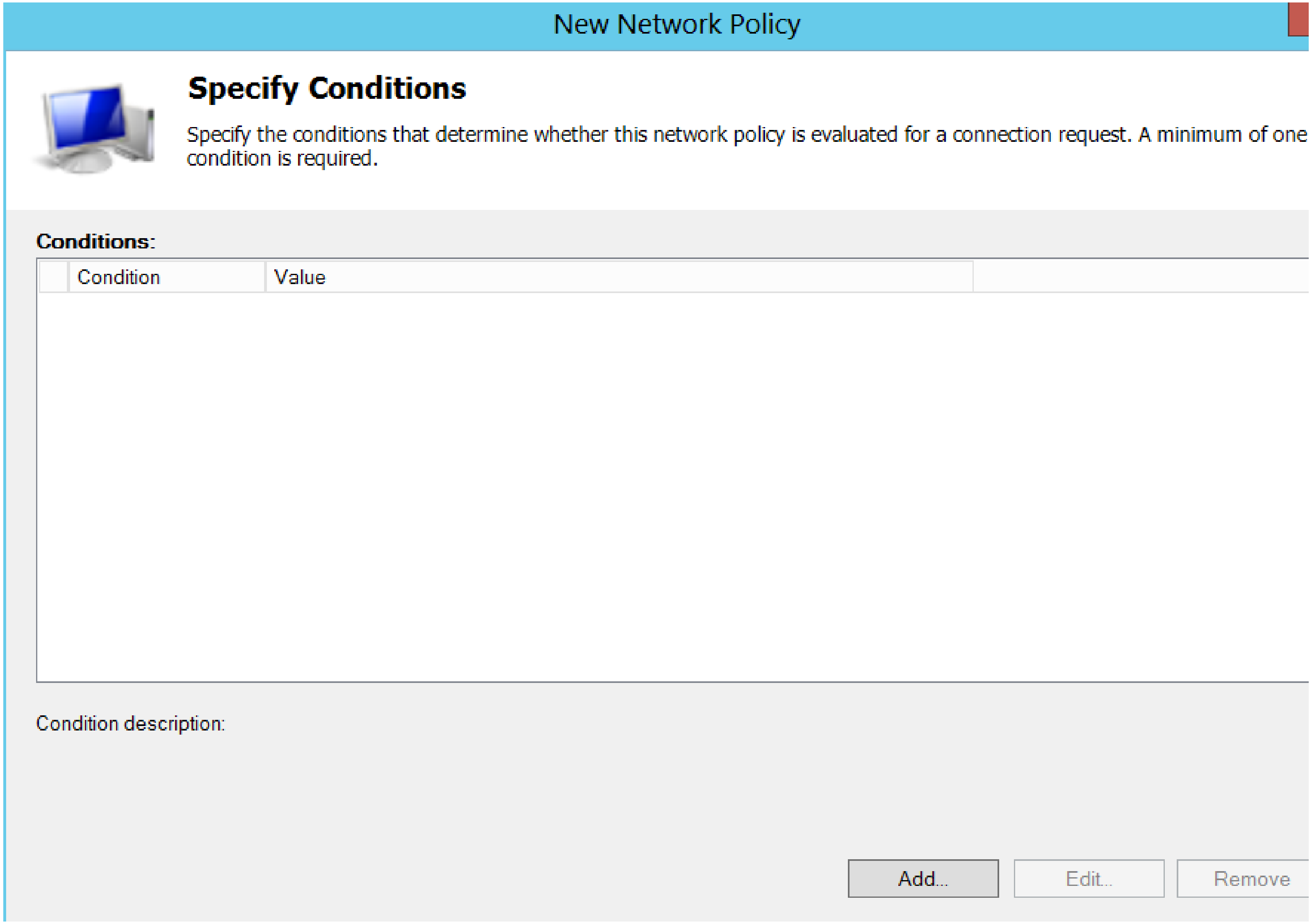
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.

● Type of network access server:

Remote Access Server(VPN-Dial up)

○ Vendor specific:

10



New Network Policy

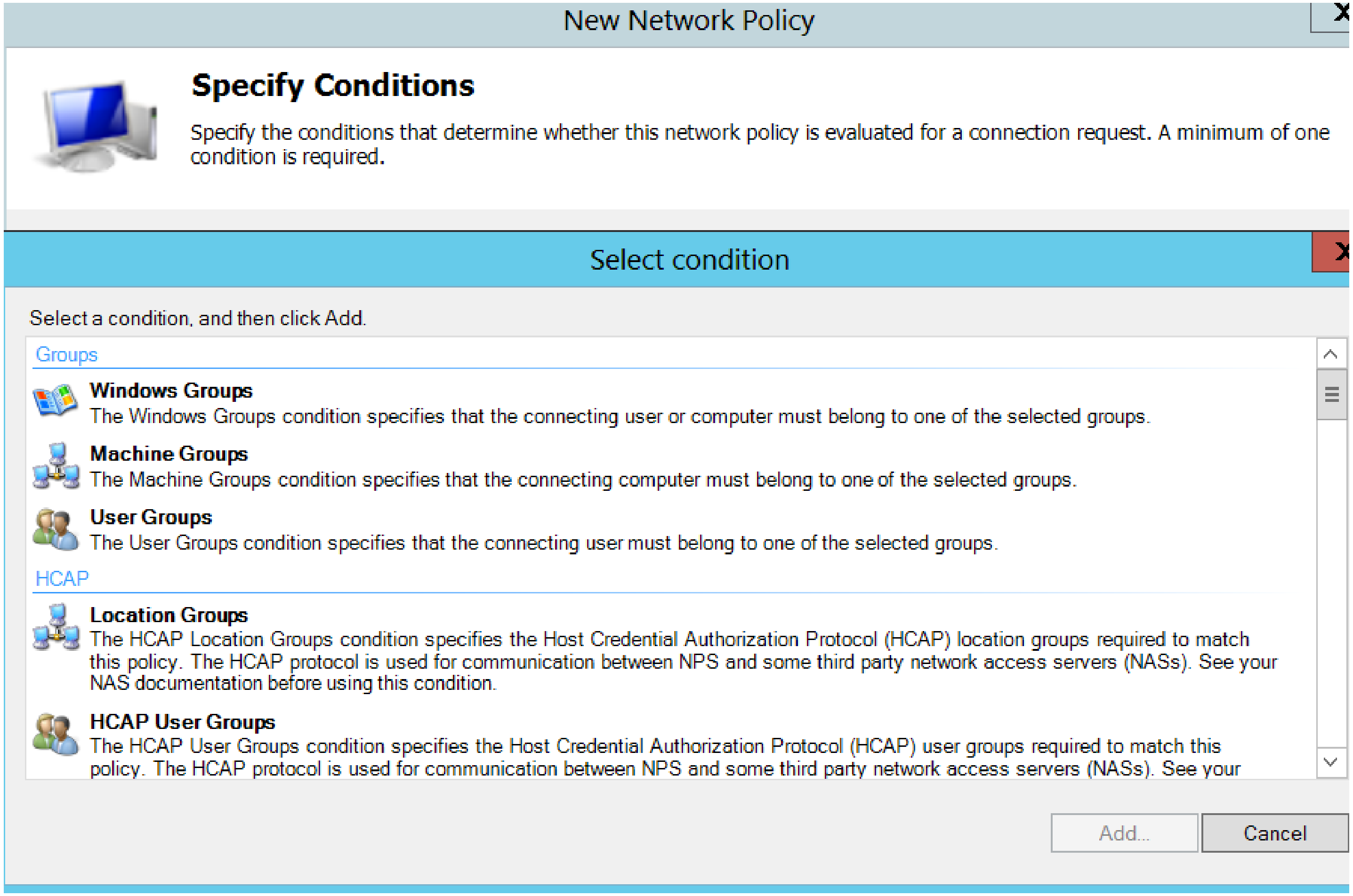
Specify Conditions

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:



Specify Conditions

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

Select a condition, and then click Add.

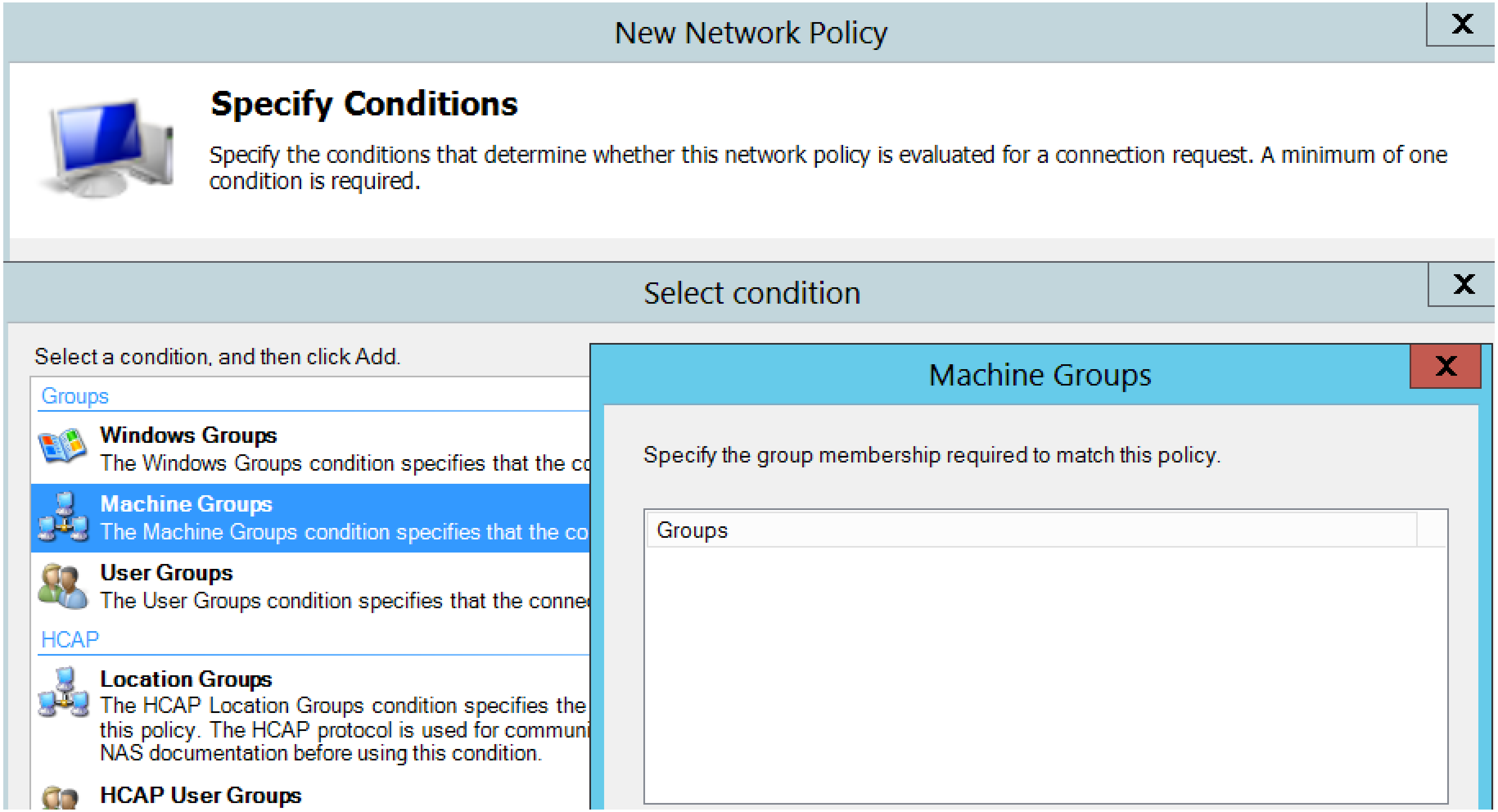
Windows Groups
The Windows Groups condition specifies that the connecting user or computer must belong to one of the selected groups.

Machine Groups
The Machine Groups condition specifies that the connecting computer must belong to one of the selected groups.

User Groups
The User Groups condition specifies that the connecting user must belong to one of the selected groups.

Location Groups
The HCAP Location Groups condition specifies the Host Credential Authorization Protocol (HCAP) location groups required to match this policy. The HCAP protocol is used for communication between NPS and some third party network access servers (NASs). See your NAS documentation before using this condition.

HCAP User Groups
The HCAP User Groups condition specifies the Host Credential Authorization Protocol (HCAP) user groups required to match this policy. The HCAP protocol is used for communication between NPS and some third party network access servers (NASs). See your



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.

Select condition

Select a condition, and then click Add.

Groups

Windows Groups
The Windows Groups condition specifies that the co

Machine Groups
The Machine Groups condition specifies that the co

User Groups
The User Groups condition specifies that the conne

HCAP

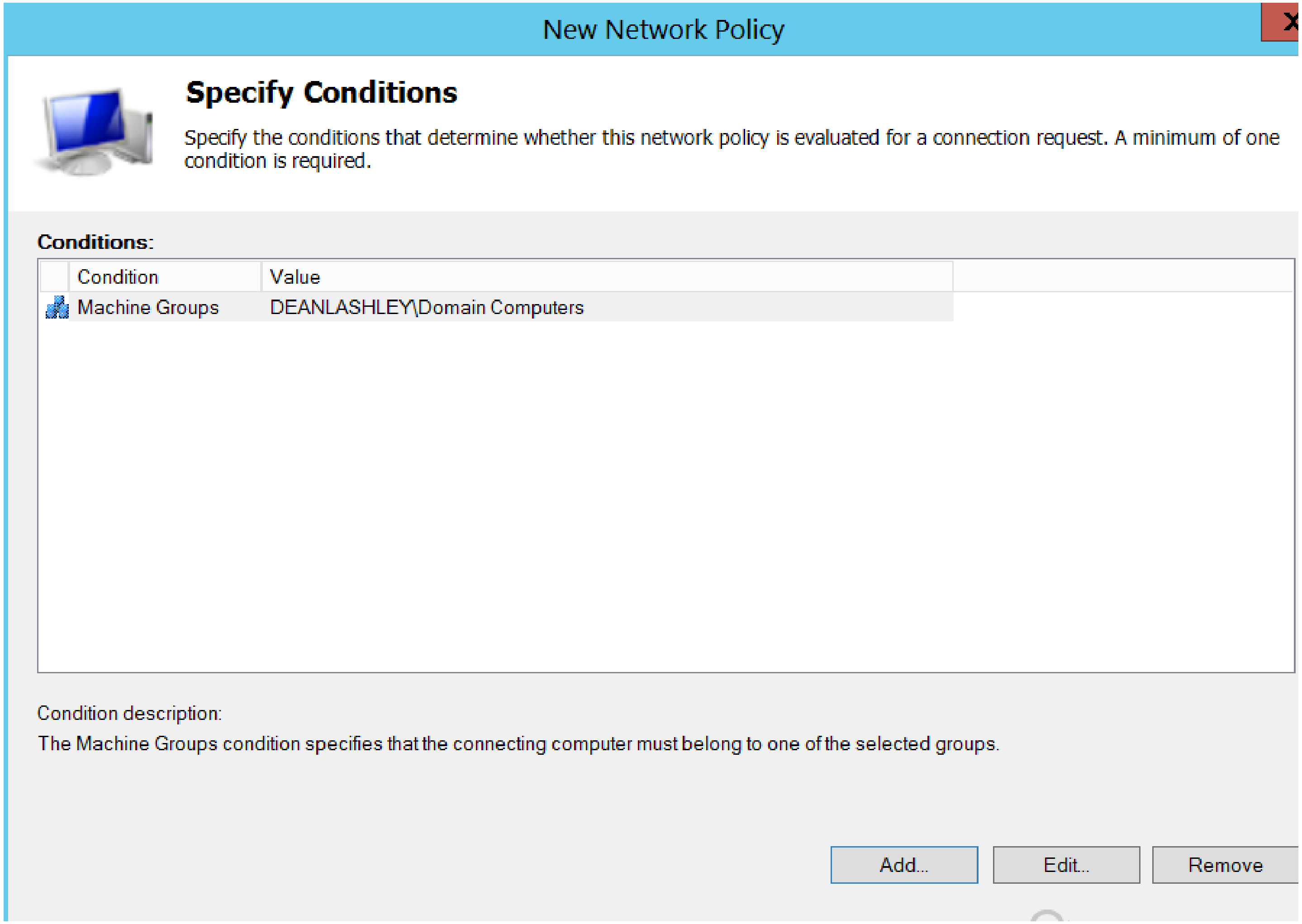
Location Groups
The HCAP Location Groups condition specifies the
this policy. The HCAP protocol is used for communi
NAS documentation before using this condition.

HCAP User Groups

Machine Groups

Specify the group membership required to match this policy.

Groups



Specify Conditions

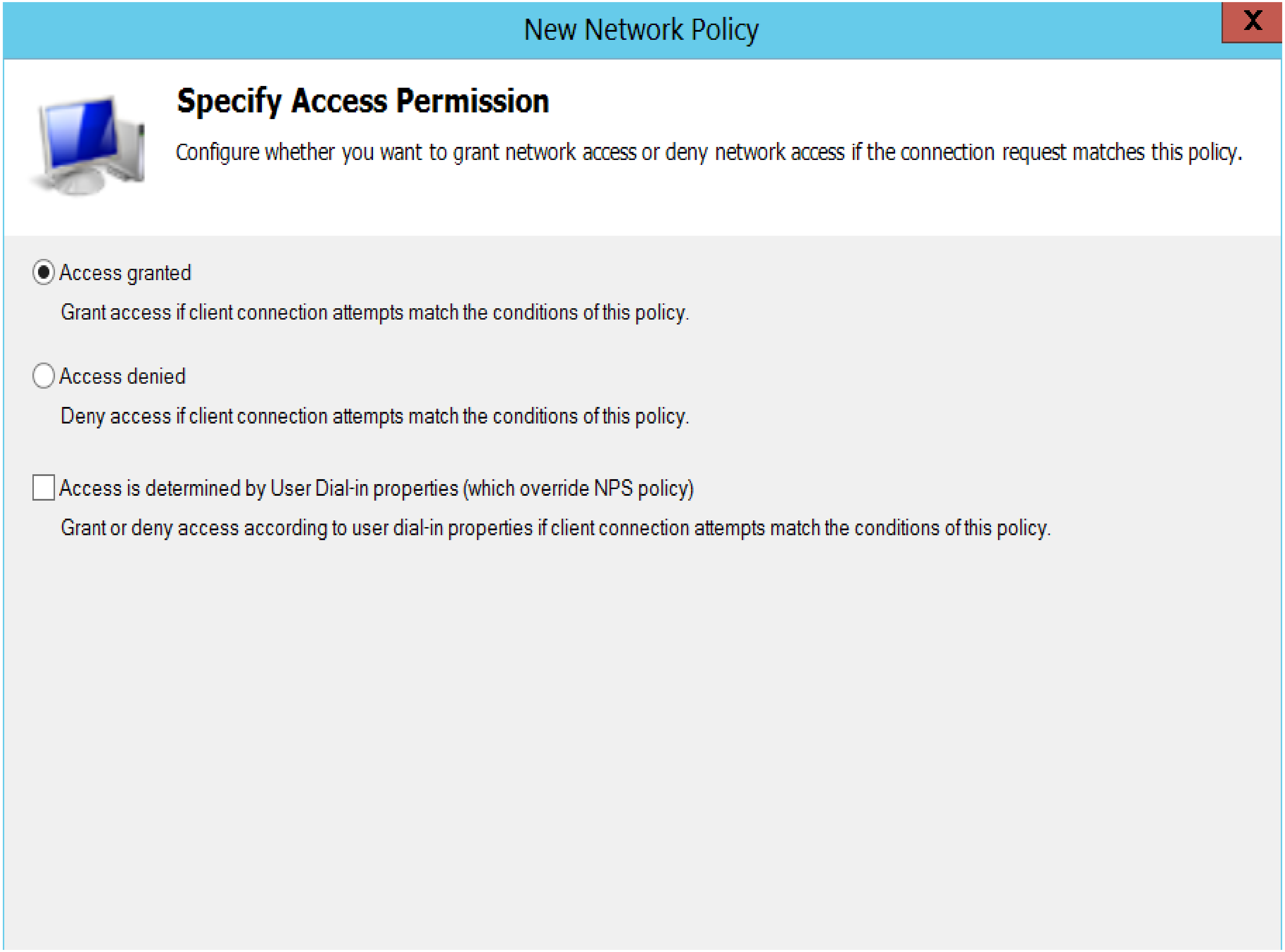
Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required.

Conditions:

Condition	Value
Machine Groups	DEANLASHLEY\Domain Computers

Condition description:

The Machine Groups condition specifies that the connecting computer must belong to one of the selected groups.



New Network Policy

Specify Access Permission

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

● Access granted

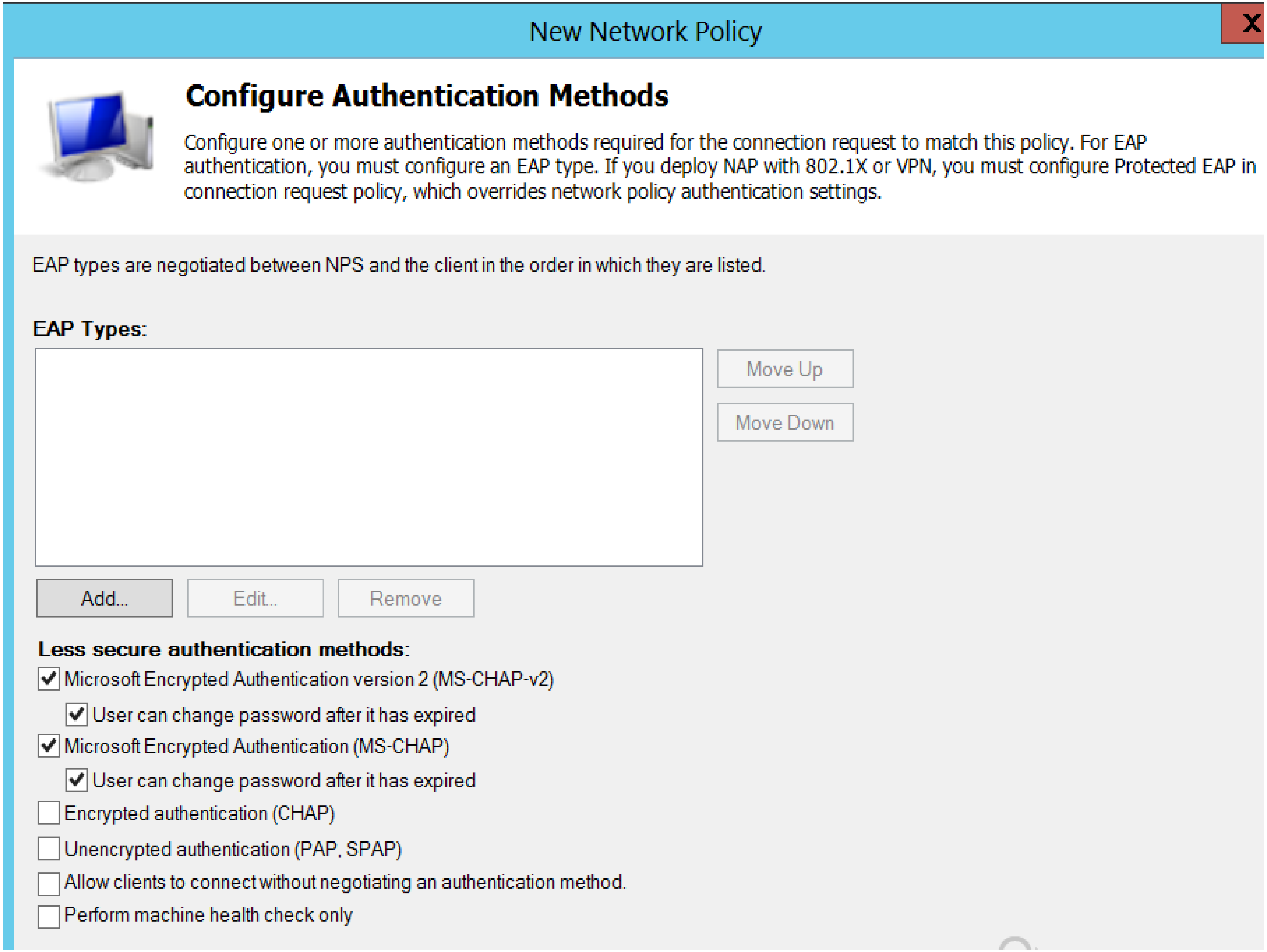
Grant access if client connection attempts match the conditions of this policy.

○ 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.



New Network Policy

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)

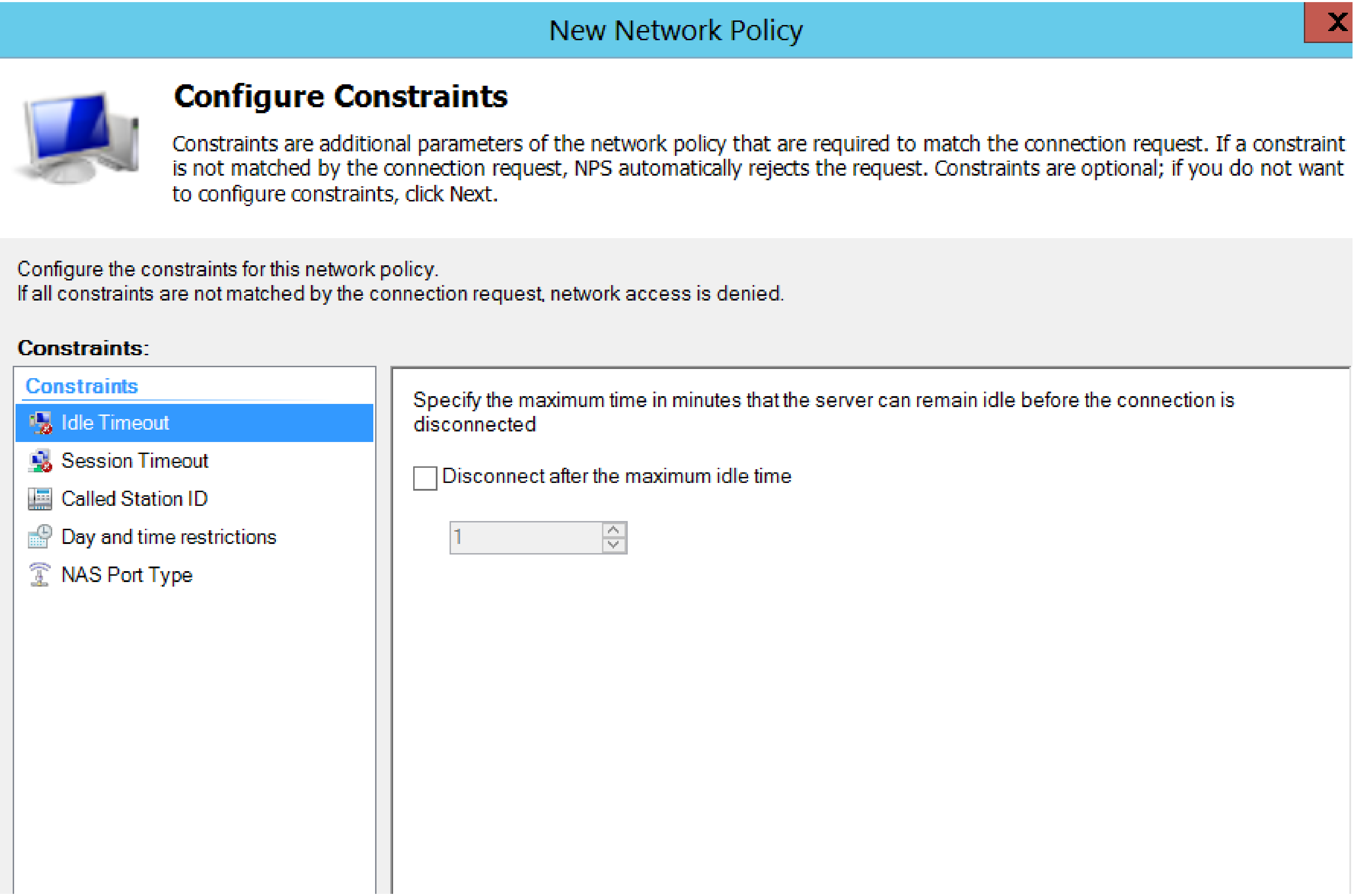
☑ User can change password after it has expired

□ Encrypted authentication (CHAP)

□ Unencrypted authentication (PAP, SPAP)

□ Allow clients to connect without negotiating an authentication method.

□ Perform machine health check only



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.

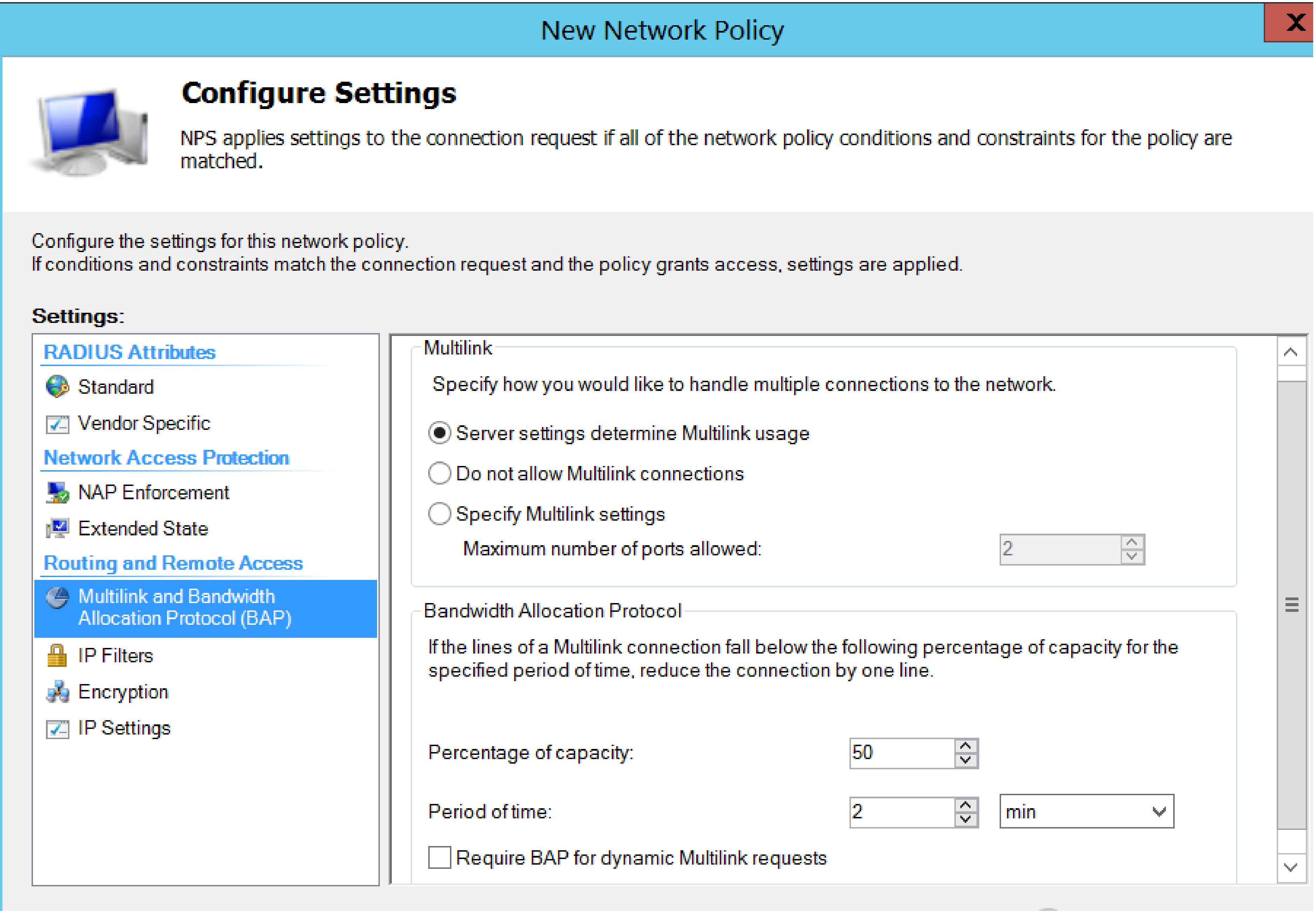
Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.

Constraints:

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

☐ Disconnect after the maximum idle time

1



New Network Policy

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:

Multilink

Specify how you would like to handle multiple connections to the network.

● Server settings determine Multilink usage

○ Do not allow Multilink connections

○ Specify Multilink settings

Maximum number of ports allowed: 2

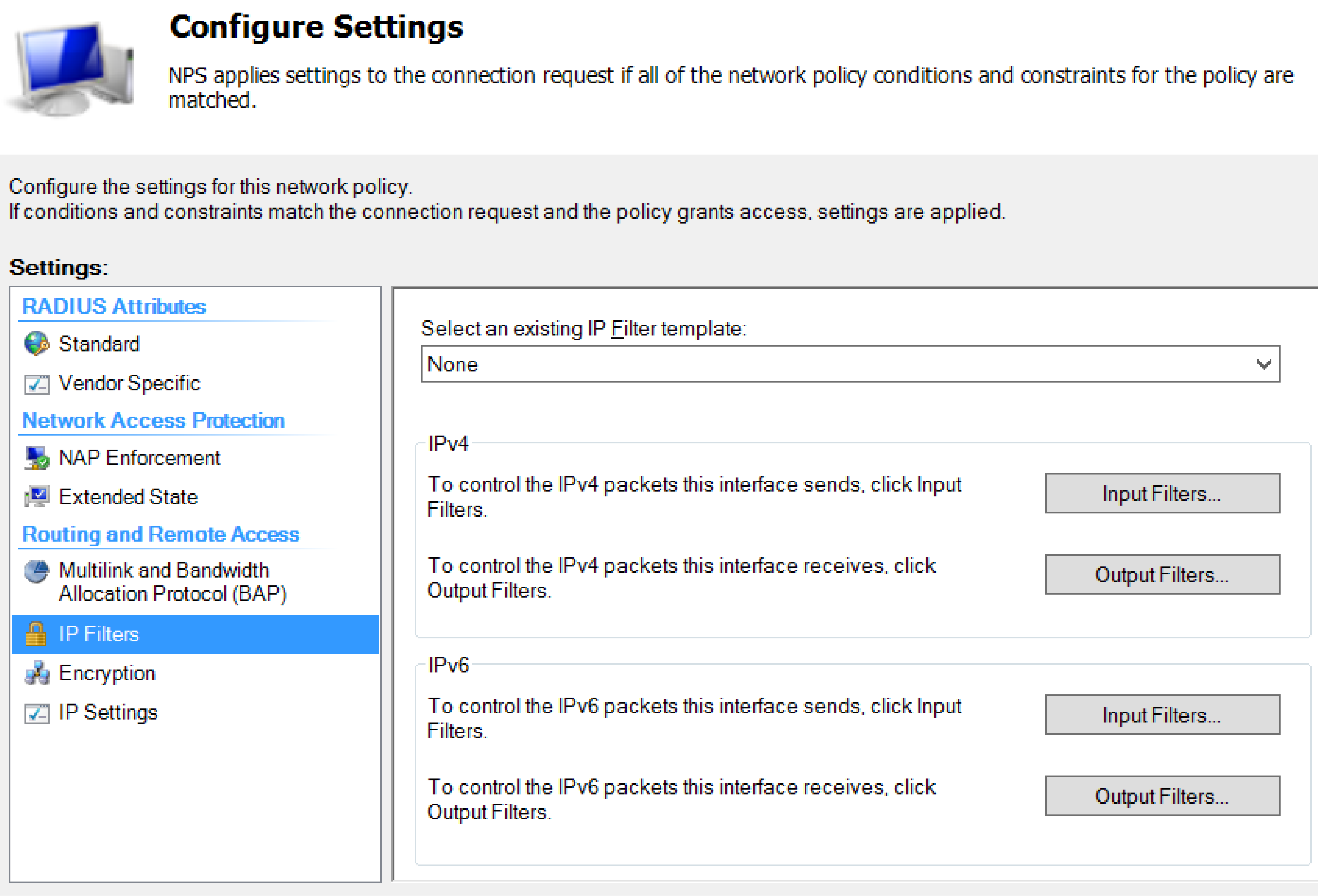
Bandwidth Allocation Protocol

If the lines of a Multilink connection fall below the following percentage of capacity for the specified period of time, reduce the connection by one line.

Percentage of capacity: 50

Period of time: 2 min

□ Require BAP for dynamic Multilink requests



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:

Select an existing IP Filter template:

None

IPv4

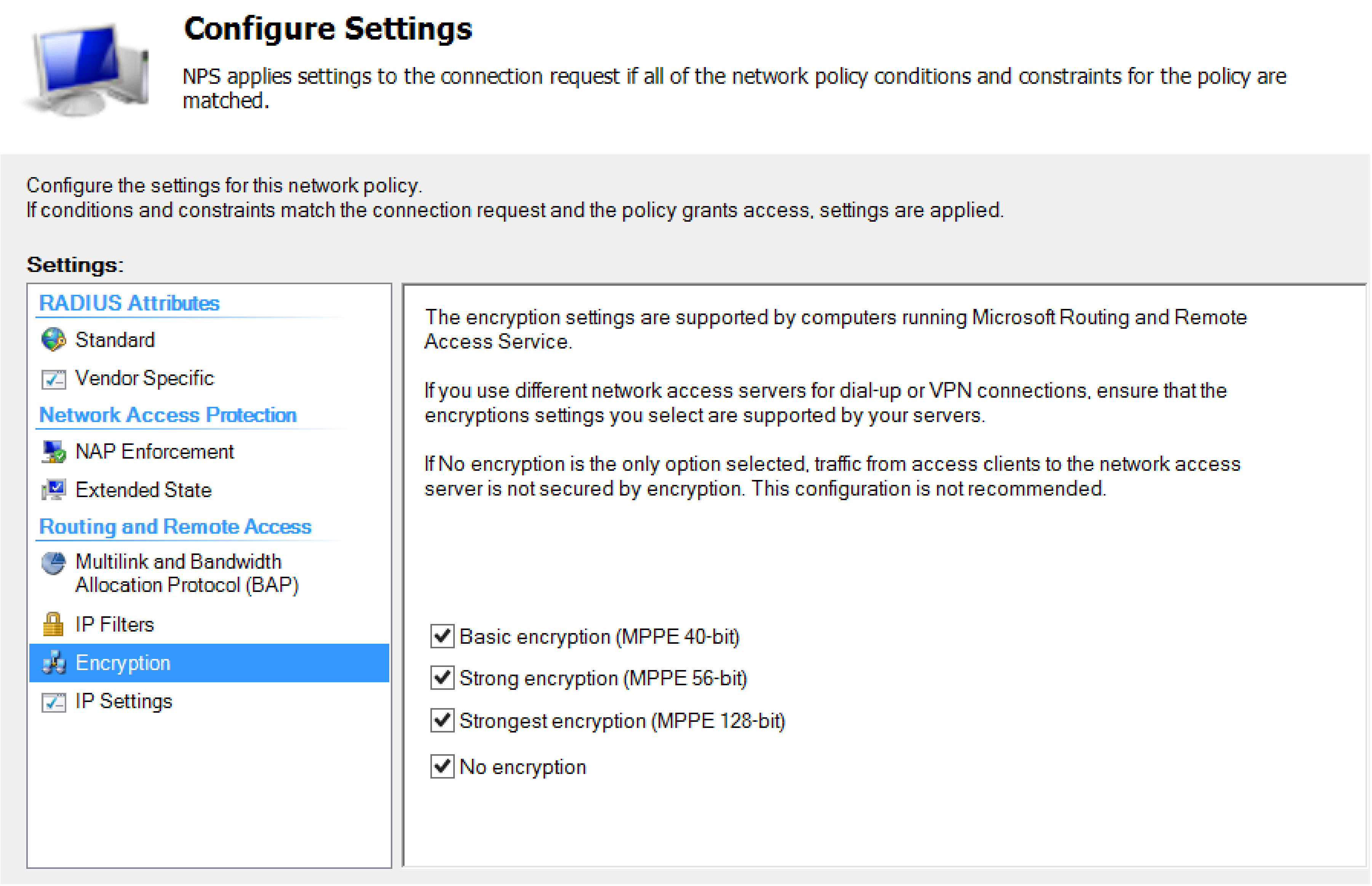
To control the IPv4 packets this interface sends, click Input Filters.

To control the IPv4 packets this interface receives, click Output Filters.

IPv6

To control the IPv6 packets this interface sends, click Input Filters.

To control the IPv6 packets this interface receives, click Output Filters.



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:

The encryption settings are supported by computers running Microsoft Routing and Remote Access Service.

If you use different network access servers for dial-up or VPN connections, ensure that the encryptions settings you select are supported by your servers.

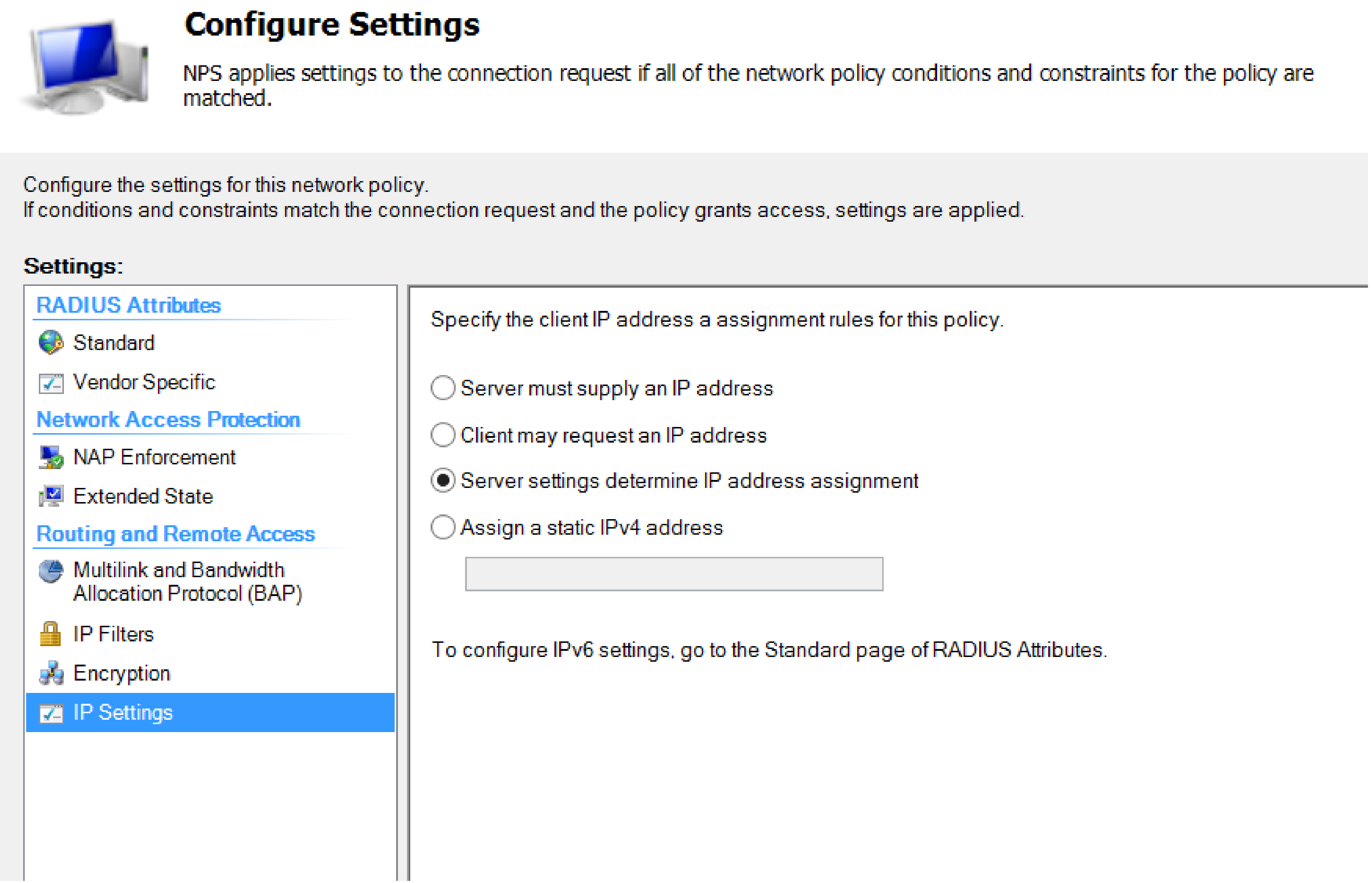
If No encryption is the only option selected, traffic from access clients to the network access server is not secured by encryption. This configuration is not recommended.

☑ Basic encryption (MPPE 40-bit)

☑ Strong encryption (MPPE 56-bit)

☑ Strongest encryption (MPPE 128-bit)

☑ No encryption



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:

Specify the client IP address a assignment rules for this policy.

○ Server must supply an IP address

○ Client may request an IP address

● Server settings determine IP address assignment

○ Assign a static IPv4 address

To configure IPv6 settings, go to the Standard page of RADIUS Attributes.