Radius Server for Dial up or VPN Clients

Radius Server Infrastructure

Network Policy Server

File Action View Help

- NPS (Local)
  - RADIUS Clients and Servers
    - RADIUS Clients
    - Remote RADIUS Server Groups
  - Policies
    - Connection Request Policies
    - Network Policies
    - Health Policies
  - Network Access Protection
  - Accounting
  - Templates Management
    - Shared Secrets
    - RADIUS Clients
    - Remote RADIUS Servers
    - IP Filters
    - Health Policies
    - Remediation Server Groups

NPS (Local)

Getting Started

Network Policy Server (NPS) allows you to create and enforce organization-wide network access policies for client health, connection request authentication, and connection request authorization.

Standard Configuration

Select a configuration scenario from the list and then click the link below to open the scenario wizard.

RADIUS server for Dial-Up or VPN Connections

RADIUS server for Dial-Up or VPN Connections

When you configure NPS as a RADIUS server for Dial-Up or VPN connections, you create network policies that allow NPS to authenticate and authorize connections from Dial-Up or VPN network access servers (also called RADIUS clients).

Configure VPN or Dial-Up

Learn more

Advanced Configuration

Templates Configuration

Configure VPN or Dial-Up

Select Dial-up or Virtual Private Network Connections Type

Type of connections:

- ○ Dial-up Connections

  When you deploy Dial-up servers on your network, NPS can authenticate and authorize connection requests made by dial-up clients connecting through the servers.

- ◉ Virtual Private Network (VPN) Connections

  When you deploy VPN servers on your network, NPS can authenticate and authorize connection requests made by VPN clients connecting through the servers.

Name:

This default text is used as part of the name for each of the policies created with this wizard. You can use the default text or modify it .

Virtual Private Network (VPN) Connections 2

Previous | Next | Finish | Cancel

Configure VPN or Dial-Up

Specify Dial-Up or VPN Server

RADIUS clients are network access servers, not client computers. If the local computer is running Routing and Remote Access as a VPN server, it is automatically added to the list of RADIUS clients below.

If you want to add remote VPN servers as RADIUS clients, click Add.

RADIUS clients:

Radius client No1
myradiusclient

Add...
Edit...
Remove

Previous | Next | Finish | Cancel

New RADIUS Client

Settings

☑ Select an existing template:

Template1

Name and Address

Friendly name:

Template1

Address (IP or DNS):

192.168.254.202 Verify...

Shared Secret

Select an existing Shared Secrets template:

None

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

◉ Manual ○ Generate

Shared secret:

••••••••

Confirm shared secret:

••••••••

OK Cancel

Configure VPN or Dial-Up

Specify Dial-Up or VPN Server

RADIUS clients are network access servers, not client computers. If the local computer is running Routing and Remote Access as a VPN server, it is automatically added to the list of RADIUS clients below.

If you want to add remote VPN servers as RADIUS clients, click Add.

RADIUS clients:

Radius client No1
myradiusclient
Template1

Add...
Edit...
Remove

Previous | Next | Finish | Cancel

Configure VPN or Dial-Up

Configure Authentication Methods

The following protocols are supported by servers running Microsoft Routing and Remote Access. If you use a different remote access server, make sure the protocols you select are supported by that software.

☐ Extensible Authentication Protocol

Type (based on method of access and network configuration):

Microsoft: Smart Card or other certificate | Configure...

☑ Microsoft Encyrpted Authentication version 2 (MS-CHAPv2)

Select this option to allow your users to specify a password for authentication.

☐ Microsoft Encyrpted Authentication (MS-CHAP)

Select this option only if your network runs operating systems that do not support MS-CHAPv2.

Previous | Next | Finish | Cancel

Configure VPN or Dial-Up

Specify User Groups

Users that are members of the selected group or groups will be allowed or denied access based on the network policy Access Permission setting.

To select User Groups, click Add. If no groups are selected, this policy applies to all users.

Groups

Add...

Remove

Previous | Next | Finish | Cancel

Configure VPN or Dial-Up

Specify IP Filters

Configure IPv4 and IPv6 packet filters if you want to restrict the type of network traffic sent and received.

If you are using Routing and Remote Access Service configured as a dial-up or VPN server, you can configure IPv4 and IPv6 input and output filters. Otherwise, click Next.

Select an existing IP Filter template:

None

IPv4

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

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

IPv6

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

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

Previous | Next | Finish | Cancel

Inbound Filters

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

Filter action:

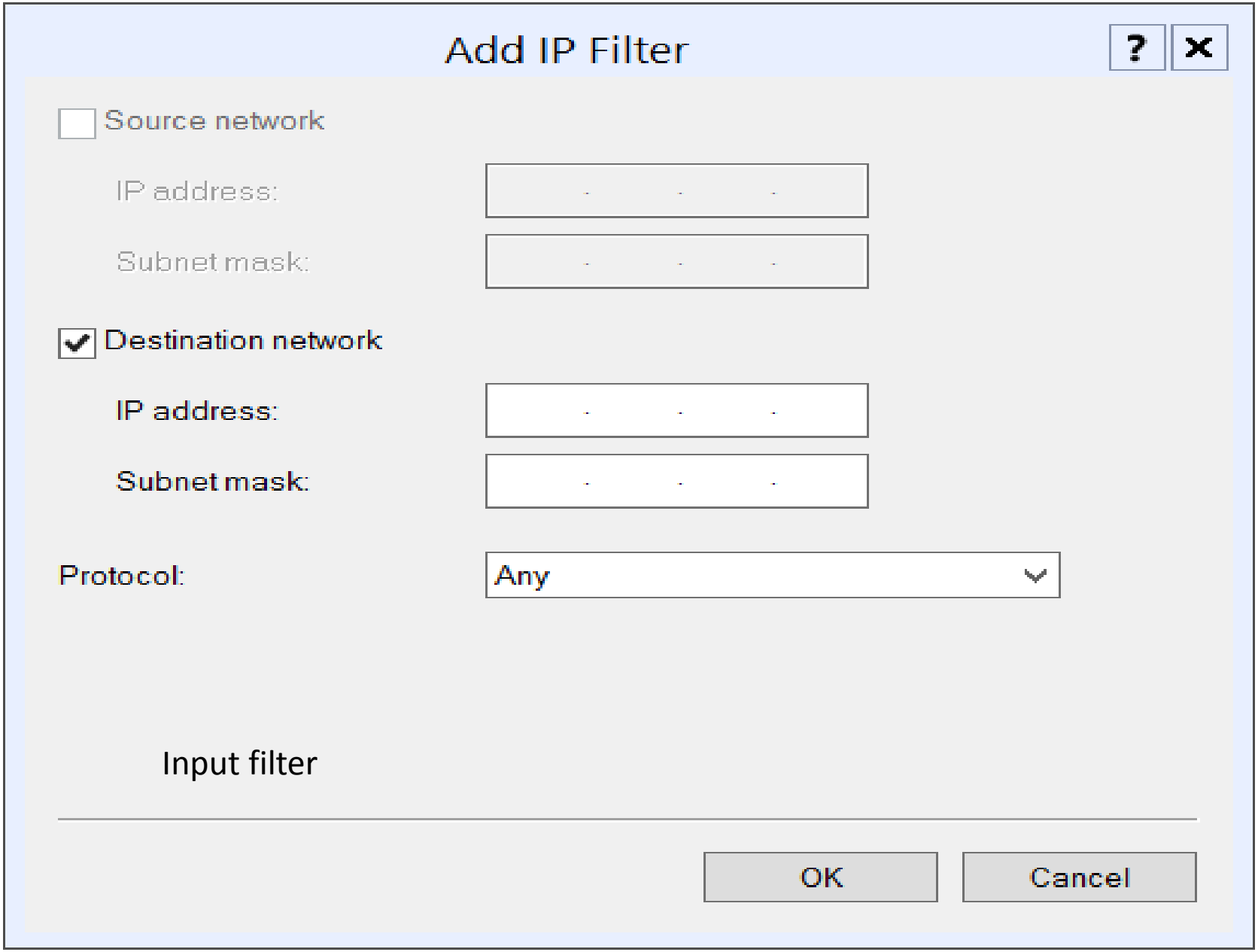
- (●) Do not permit packets listed below
- ( ) Permit only the packets listed below

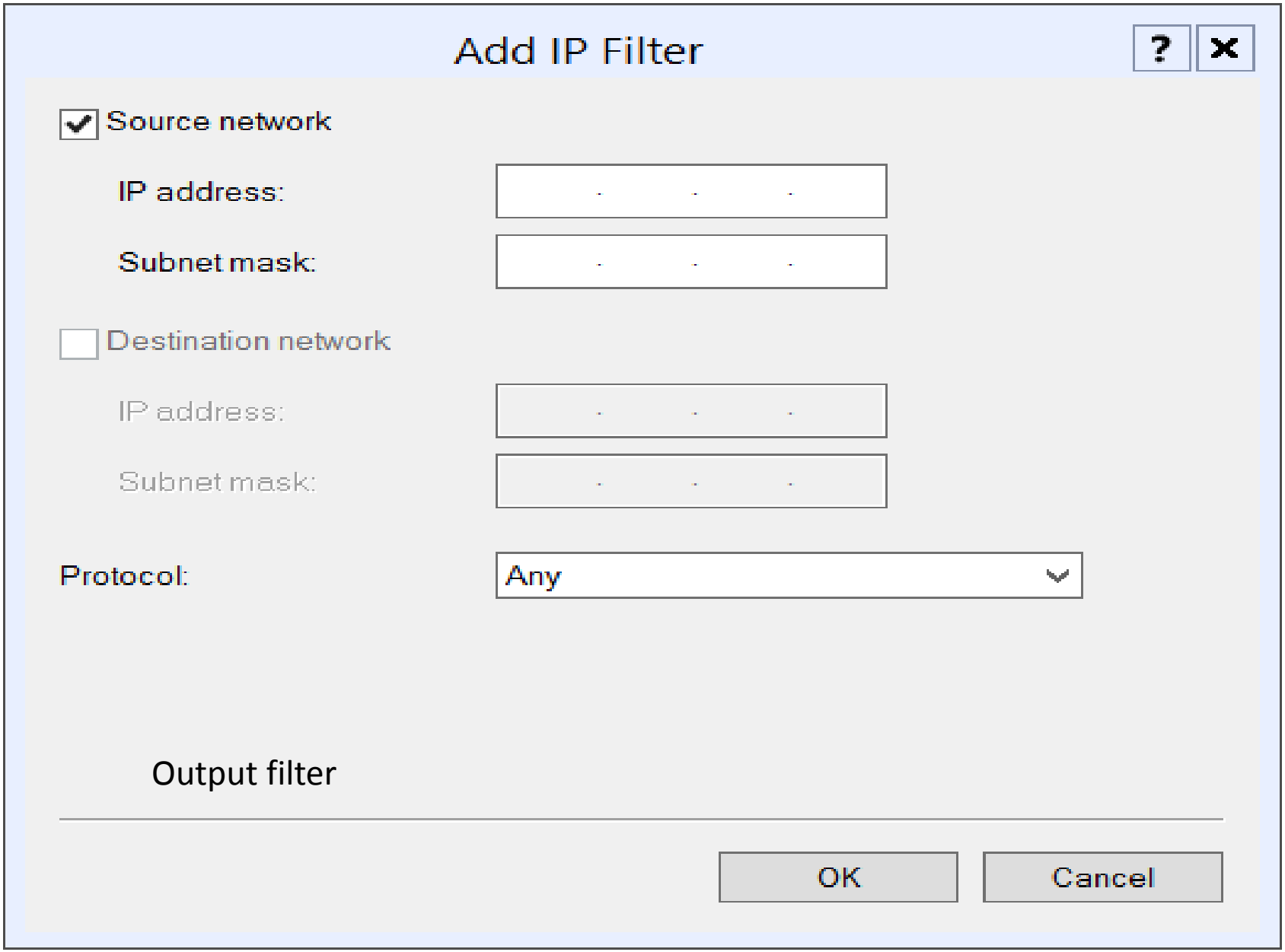
Filters:

Source Address	Source Network Mask	Destination Address	Destination Mask	Protoco

New... | Edit... | Delete

OK | Cancel


Add IP Filter
Source network
IP address:
Subnet mask:
Destination network
IP address:
Subnet mask:
Protocol:
Any
Input filter
OK
Cancel


Add IP Filter
Source network
IP address:
Subnet mask:
Destination network
IP address:
Subnet mask:
Protocol:
Any
Output filter
OK
Cancel

Configure VPN or Dial-Up

Specify Encryption Settings

Specify the allowed encryption strengths used for traffic between access clients and the network access server.

If you are using Routing and Remote Access Service configured as a dial-up or VPN server, you can configure encryption strength.

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.

- [x] Basic encryption (MPPE 40-bit)
- [x] Strong encryption (MPPE 56-bit)
- [x] Strongest encryption (MPPE 128-bit)

Previous | Next | Finish | Cancel

Configure VPN or Dial-Up

Specify a Realm Name

If you specify a realm name, the user account location supplied by users in log on credentials, such as a domain name, is replaced by the value you choose.

Your ISP uses a portion of the user name to identify which connection requests to route to this server. This part of the user name is the realm name.

If you do not know your realm name, contact your ISP. If you do not care about realm name, please click next.

Type the realm name, including the separator character (the period or the forward slash), that your ISP uses to forward requests.

Realm name:

Example: ISP.

☑ Before authentication, remove the realm name from the user name

If the realm name is an identifier added to the existing Windows user name, it must be removed before Windows can authenticate the connection request.

Previous | Next | Finish | Cancel

Configure VPN or Dial-Up

Completing New Dial-up or Virtual Private Network Connections and RADIUS clients

You have successfully created the following policies and configured the following RADIUS clients.

- To view the configuration details in your default browser, click Configuration Details.
- To change the configuration, click Previous.
- To save the configuration and close this wizard, click Finish.

RADIUS clients:
Template1 (192.168.254.202)

Connection Request Policy:
Virtual Private Network (VPN) Connections 2

Network Policies:
Virtual Private Network (VPN) Connections 2

Configuration Details

Previous | Next | Finish | Cancel