StarWind iSCSI SAN Software: IP Security policy configuration

www.starwindsoftware.com

COPYRIGHT

TRADEMARKS

CHANGES

The material in this document is for information only and is subject to change without notice. While reasonable efforts have been made in the preparation of this document to assure its accuracy, StarWind Software assumes no liability resulting from errors or omissions in this document, or from the use of the information contained herein. StarWind Software reserves the right to make changes in the product design without reservation and without notification to its users.

TECHNICAL SUPPORT AND SERVICES

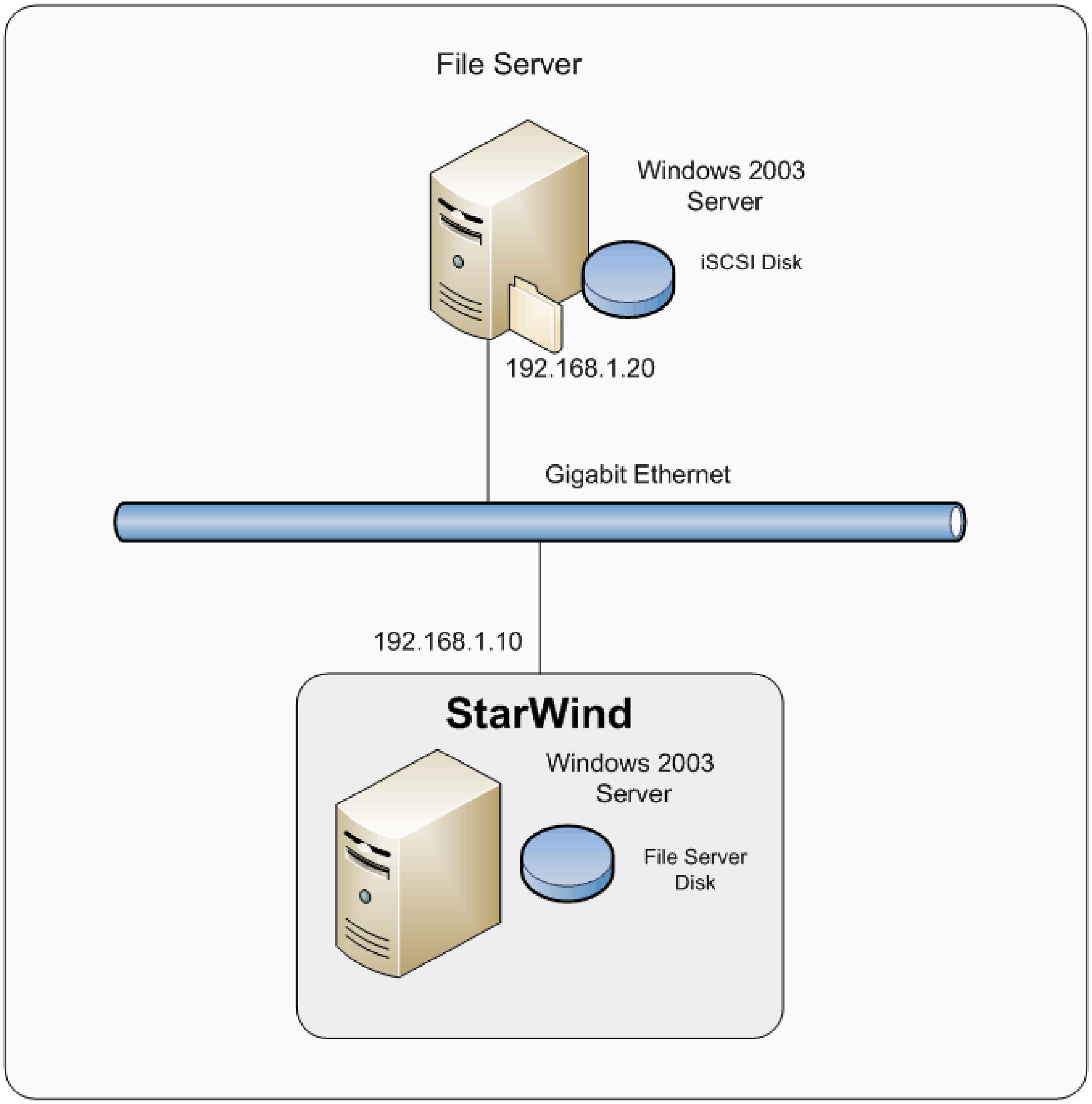
If you have questions about installing or using this software, check this and other documents first - you will find answers to most of your questions here or there. If you need further assistance, please contact us.

Table of Contents

Guide

Introduction

This document will help you to configure the IP security policy on Windows 2003 Server for achieving secure connection between Target and Initiator sides. The diagram below illustrates the reference configuration used throughout this document.



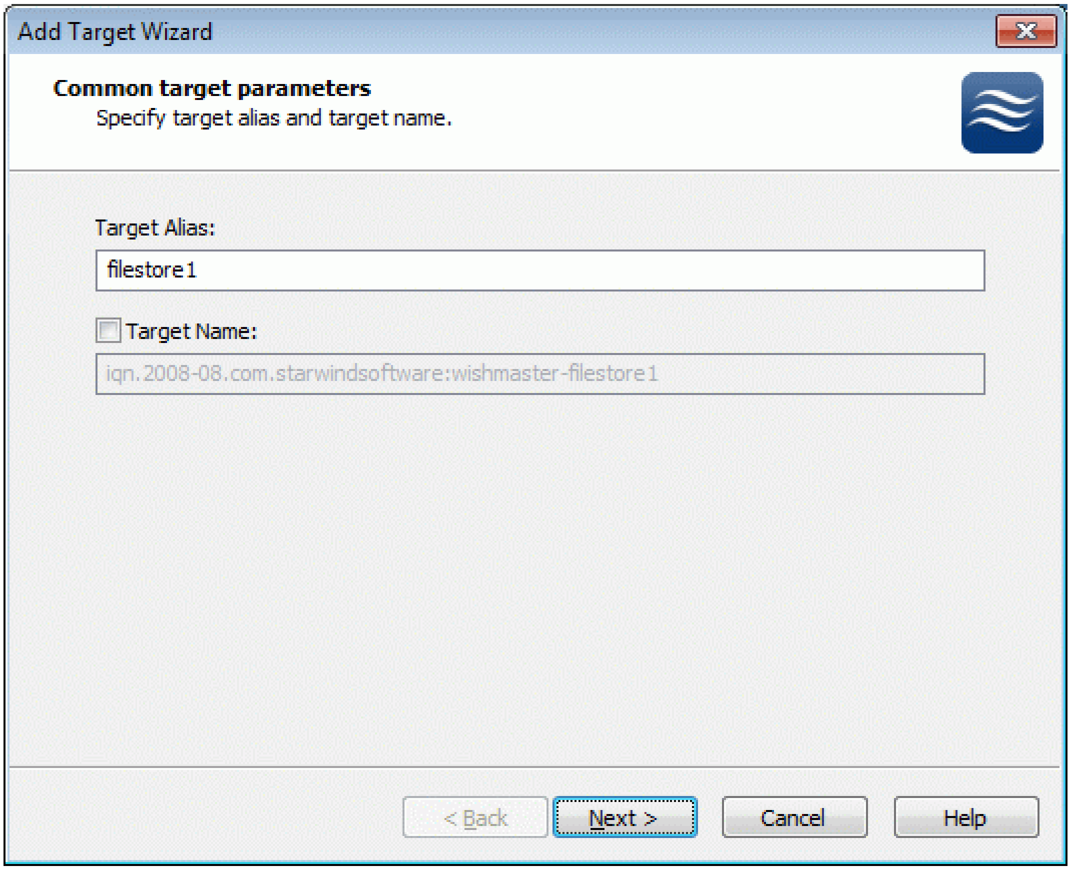
Configuring iSCSI Storage

Launch the **StarWind** console selecting **Start -> All Programs -> StarWind Software -> Starwind**. After the console is launched its icon appears in the system tray. Double click the icon with the left mouse button or single click it with the right mouse button and select **Start Management** menu item from the pop-up menu.

From the **StarWind Servers** tree please select the server you want to connect to. Press **Connect** button to continue. You will be prompted to enter the login and password. Default ones are: **root, starwind**. You can always change them later.

After you have successfully connected to the **StarWind** service press the **Add Target** button to continue.

In the wizard that appears please specify **target name**. Under this **target name**, the device will be declared to the iSCSI initiators connecting to the **StarWind** over an IP network.



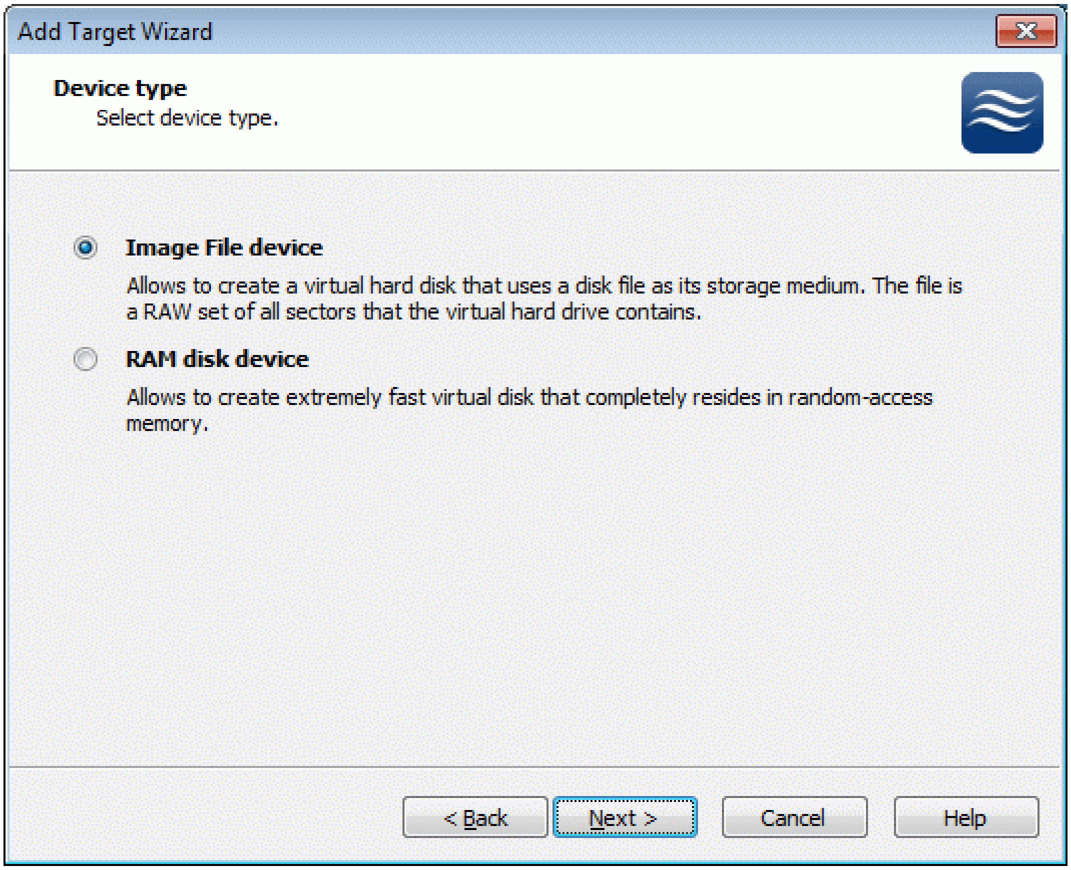
Common target parameters
Specify target alias and target name.

Target Alias:
filestore1

□ Target Name:
iqn.2008-08.com.starwindsoftware:wishmaster-filestore1

Press the **Next** button to continue.

Select **Image File device**.



Add Target Wizard

Device type

Select device type.

● **Image File device**

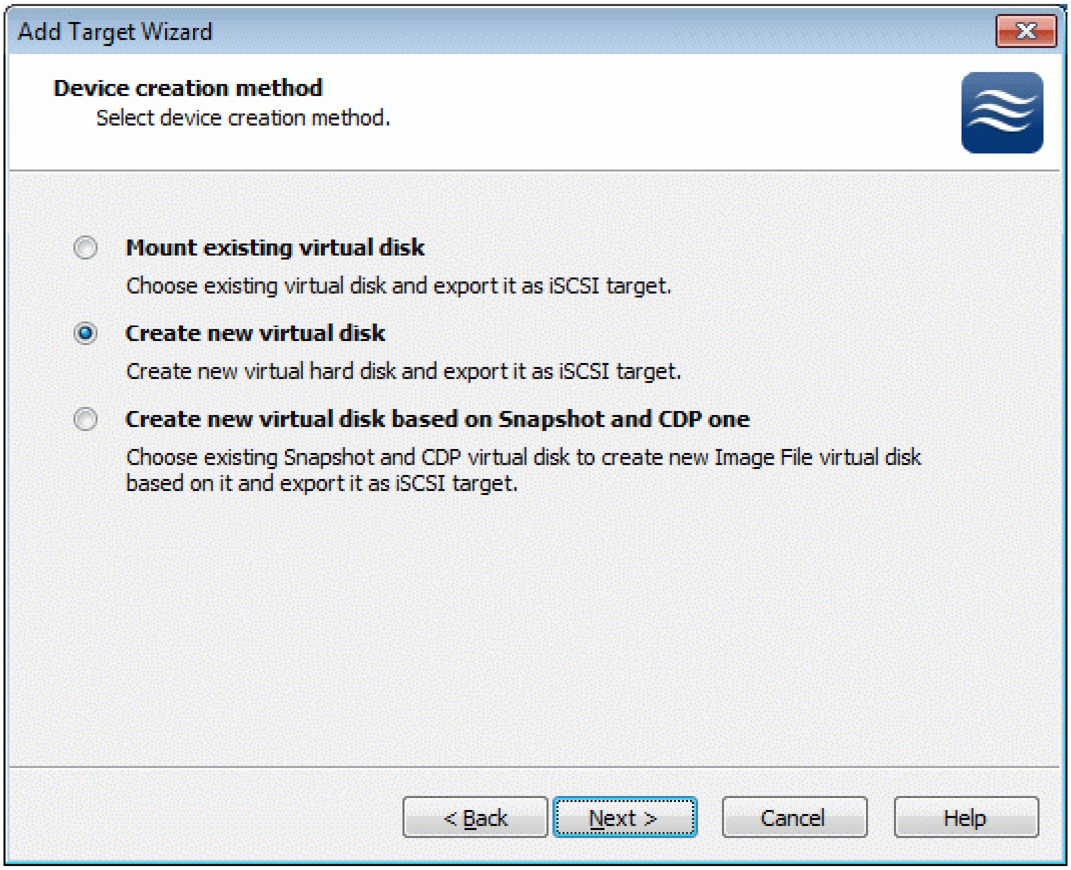
Allows to create a virtual hard disk that uses a disk file as its storage medium. The file is a RAW set of all sectors that the virtual hard drive contains.

○ **RAM disk device**

Allows to create extremely fast virtual disk that completely resides in random-access memory.

Press the **Next** button to continue.

Select **Create new virtual disk** to create a new hard disk image or **Mount existing virtual disk** to mount an existing image that you've prepared before.



Add Target Wizard

Device creation method

Select device creation method.

○ **Mount existing virtual disk**

Choose existing virtual disk and export it as iSCSI target.

● **Create new virtual disk**

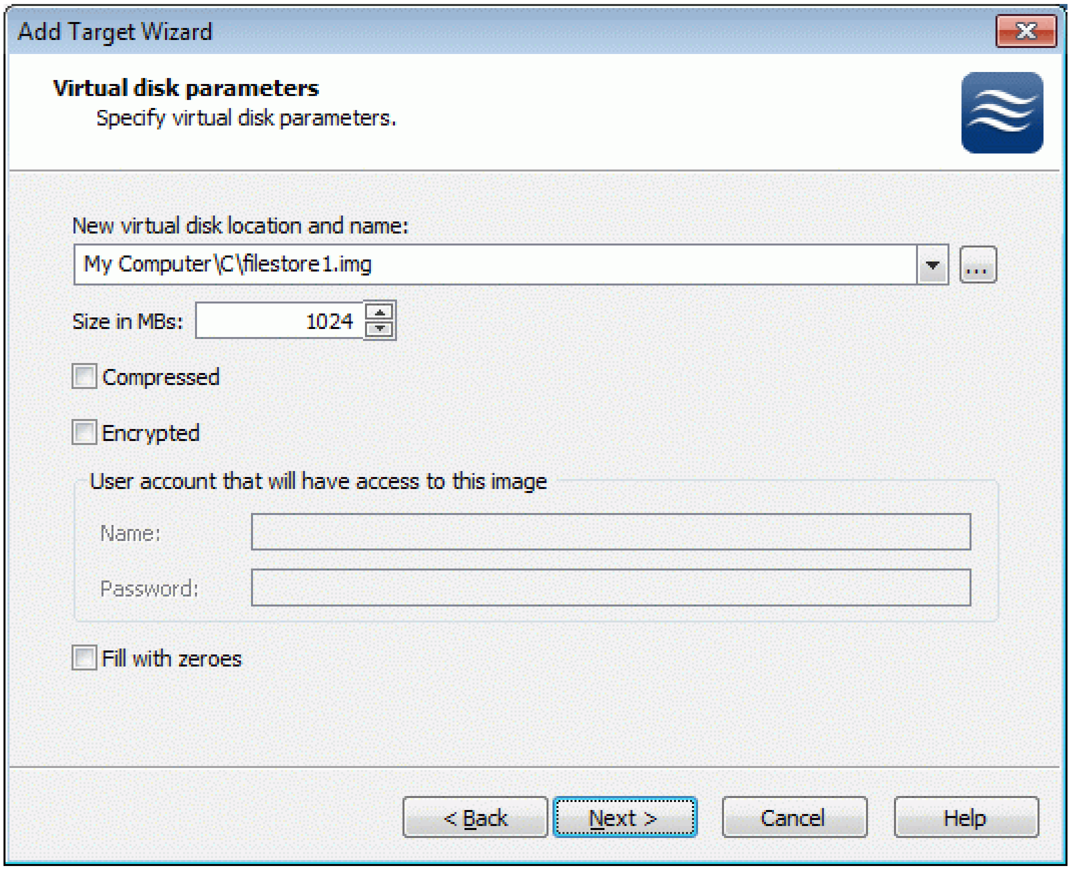
Create new virtual hard disk and export it as iSCSI target.

○ **Create new virtual disk based on Snapshot and CDP one**

Choose existing Snapshot and CDP virtual disk to create new Image File virtual disk based on it and export it as iSCSI target.

Press the **Next** button to continue.

If you have decided to create a new virtual disk, specify the location and the name of the virtual disj you wish to be created. The virtual disk size is specified in megabytes. Refer to the online help for details regarding additional parameters (**Fill with zeroes, Compressed** and **Encrypted**).



Add Target Wizard

Virtual disk parameters

Specify virtual disk parameters.

New virtual disk location and name: My Computer\C\filestore1.img

Size in MBs: 1024

□ Compressed

□ Encrypted

User account that will have access to this image

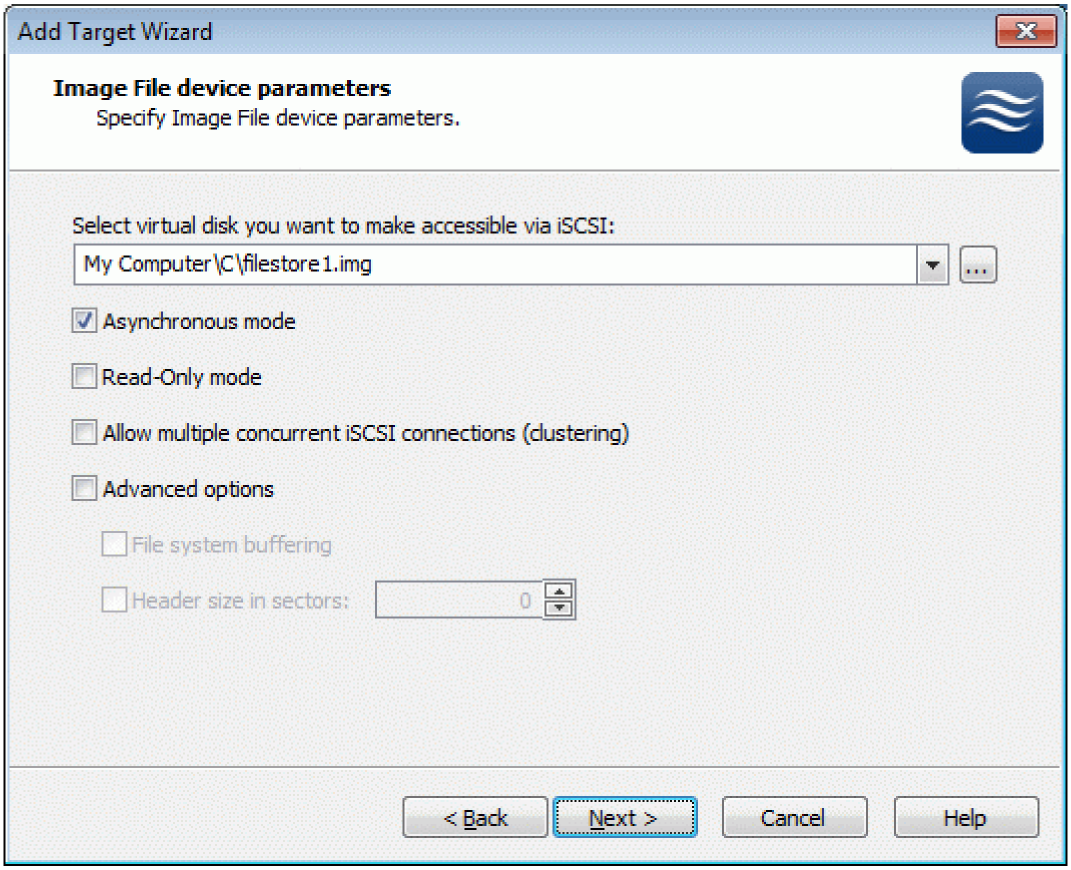
Name:

Password:

□ Fill with zeroes

Press the **Next** button to continue.

An Image File device can have additional parameters. Refer to the online help for details regarding the additional parameters (**Asynchronous mode, Allow multiple connections (clustering), Read-Only mode** and **Advanced options**).



Add Target Wizard

Image File device parameters

Specify Image File device parameters.

Select virtual disk you want to make accessible via iSCSI: My Computer\C\filestore1.img

☑ Asynchronous mode

□ Read-Only mode

□ Allow multiple concurrent iSCSI connections (clustering)

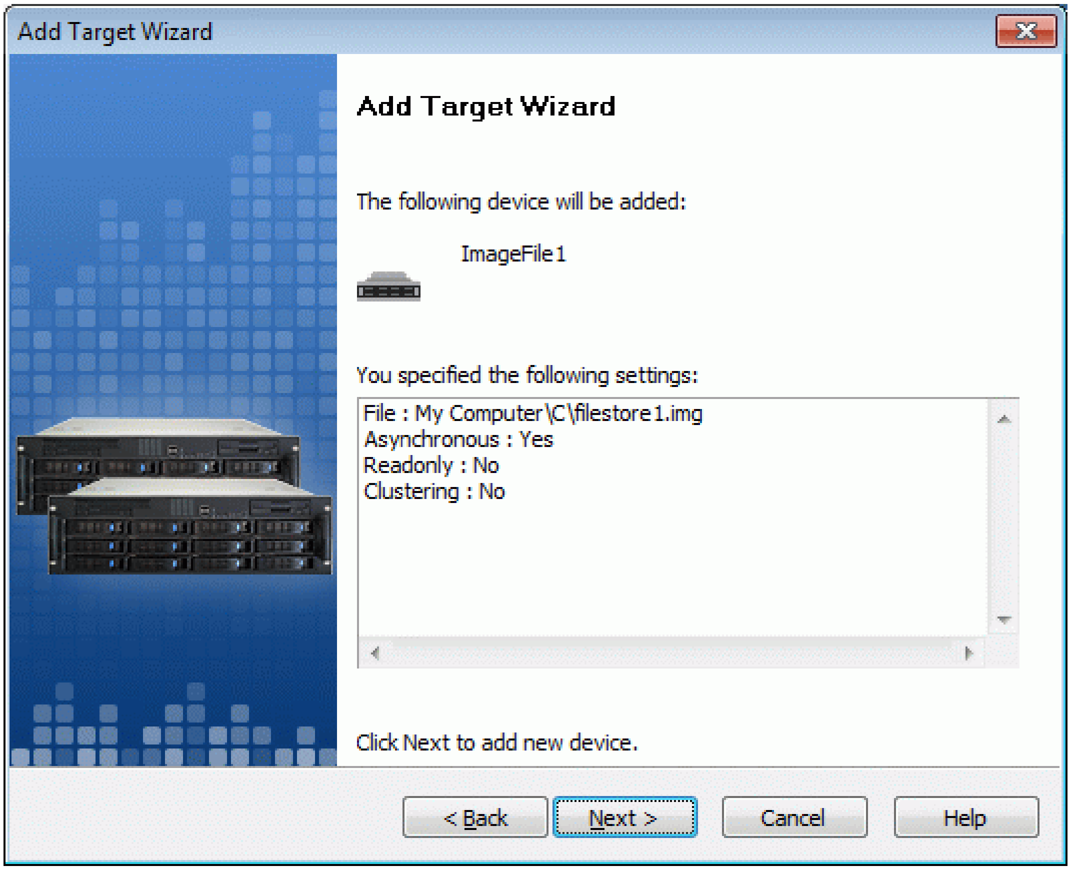
□ Advanced options

□ File system buffering

□ Header size in sectors: 0

Press the **Next** button to continue.

Check if all of the device parameters are correct. Press the **Back** button if any changes are required.



Add Target Wizard

The following device will be added:

ImageFile1

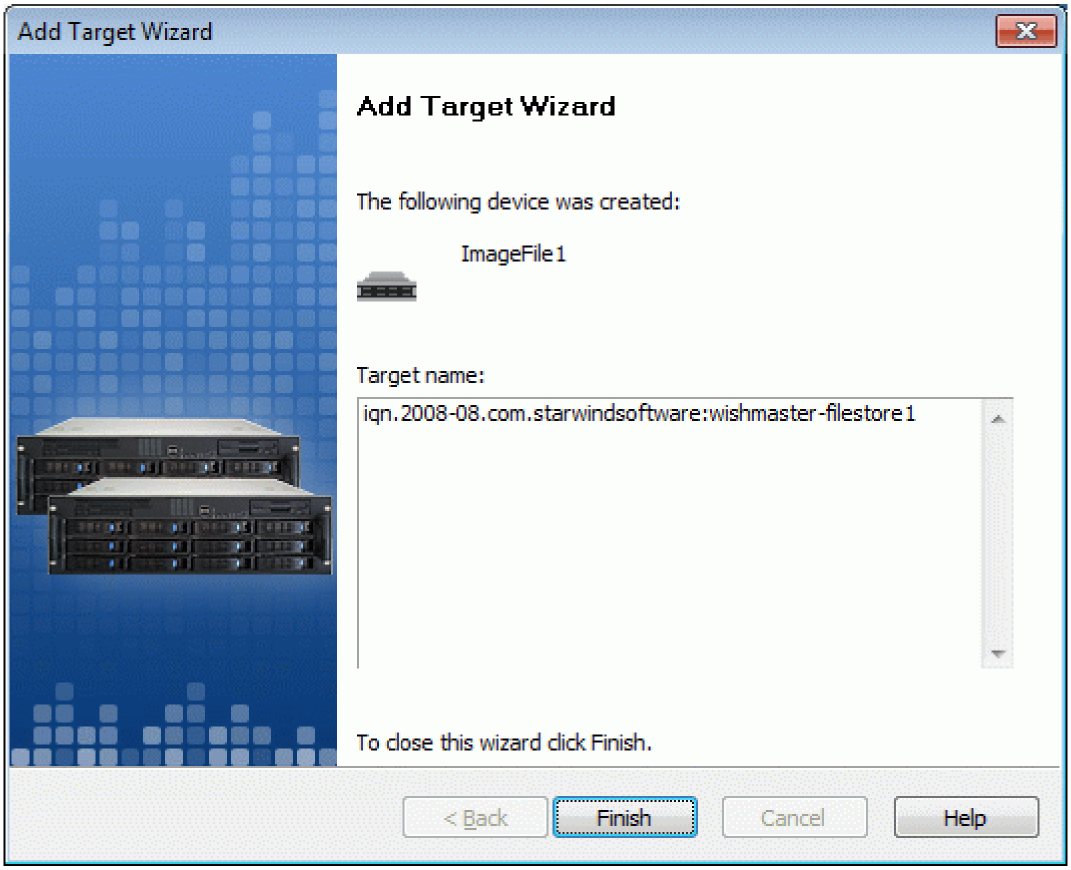
You specified the following settings:

File : My Computer\C\filestore1.img
Asynchronous : Yes
Readonly : No
Clustering : No

Click Next to add new device.

Press the **Next** button to continue.

The information about the recently created device is displayed on the last wizard page (see image below).



Add Target Wizard

The following device was created:

ImageFile1

Target name:

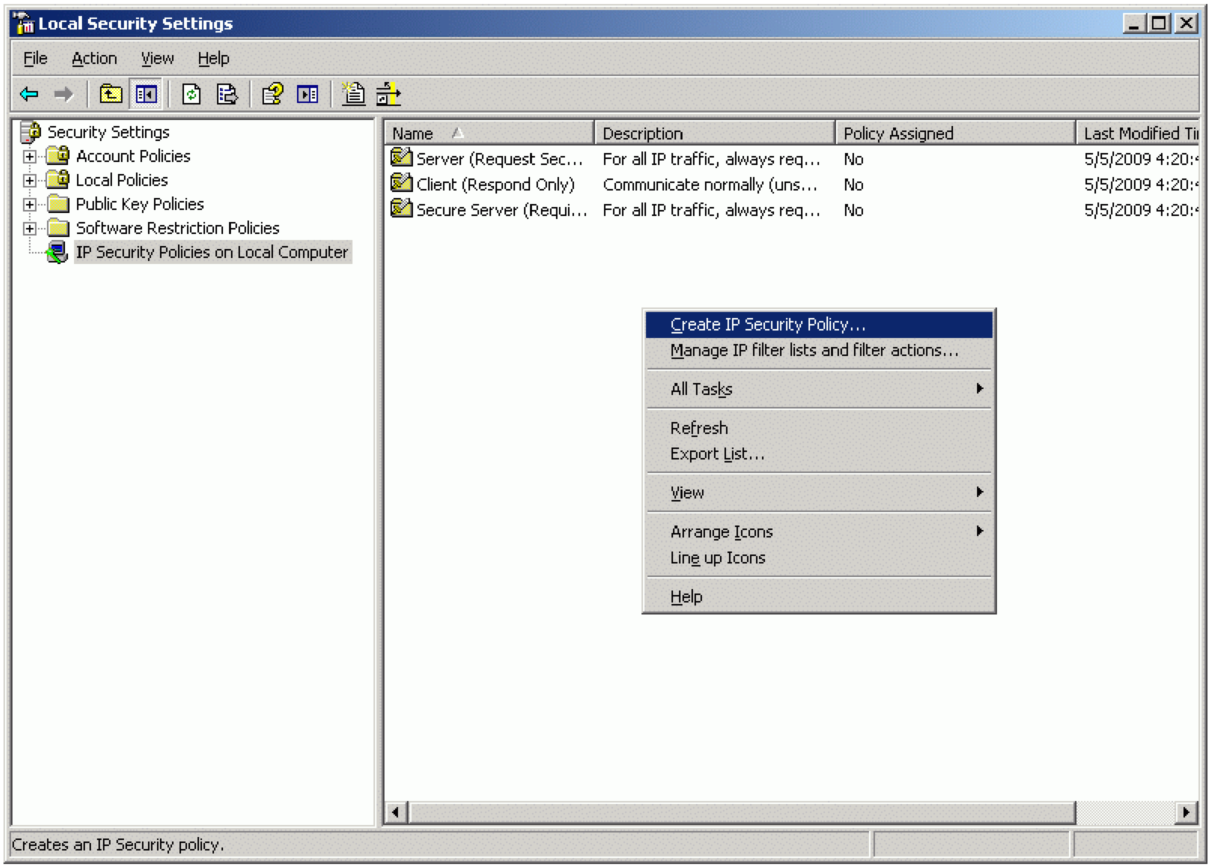
iqn.2008-08.com.starwindsoftware:wishmaster-filestore1

To close this wizard click Finish.

Press the **Finish** button to close the wizard.

Server-Side Configuration, Creating New Ip Security Policy

Launch the **Local Security Settings** management console selecting **Start -> Control Panel -> Administrative tools -> Local Security Policy**. **Local Security Settings** management console appears. Switch to the **IP Security Policies on Local Computer** tree item.

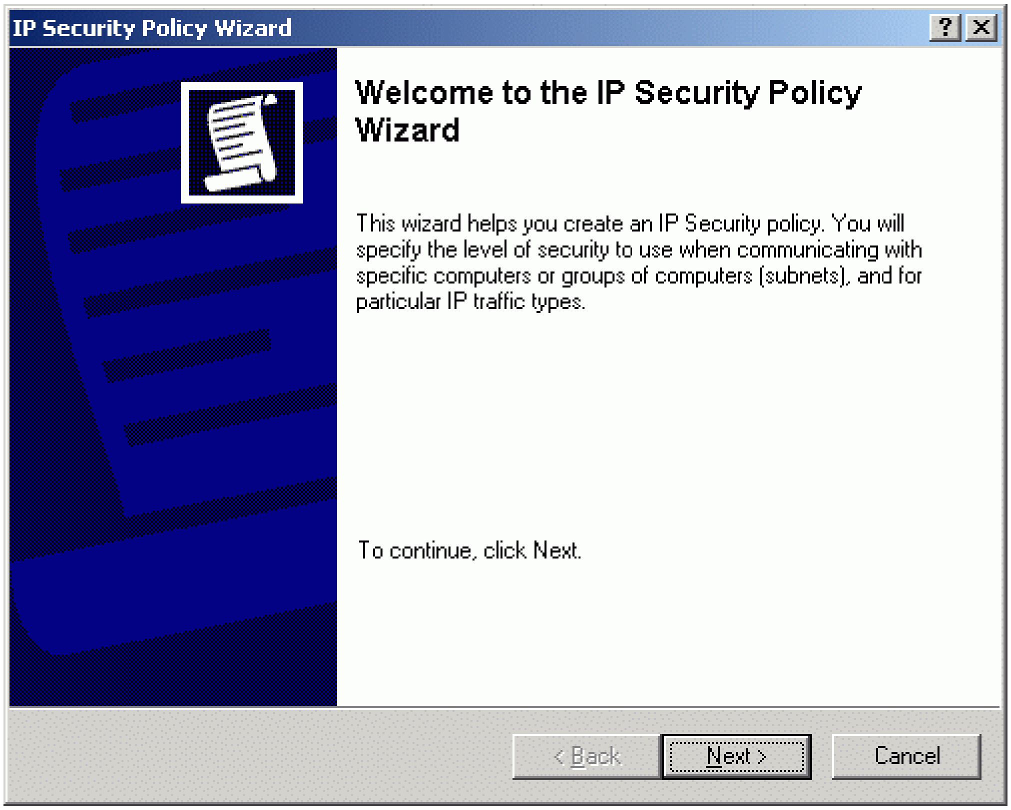


Name	Description	Policy Assigned	Last Modified Ti
Server (Request Sec...	For all IP traffic, always req...	No	5/5/2009 4:20:
Client (Respond Only)	Communicate normally (uns...	No	5/5/2009 4:20:
Secure Server (Requi...	For all IP traffic, always req...	No	5/5/2009 4:20:

Creates an IP Security policy.

Click the right mouse button and select **Create IP Security Policy** option.

IP Security Policy Wizard appears.



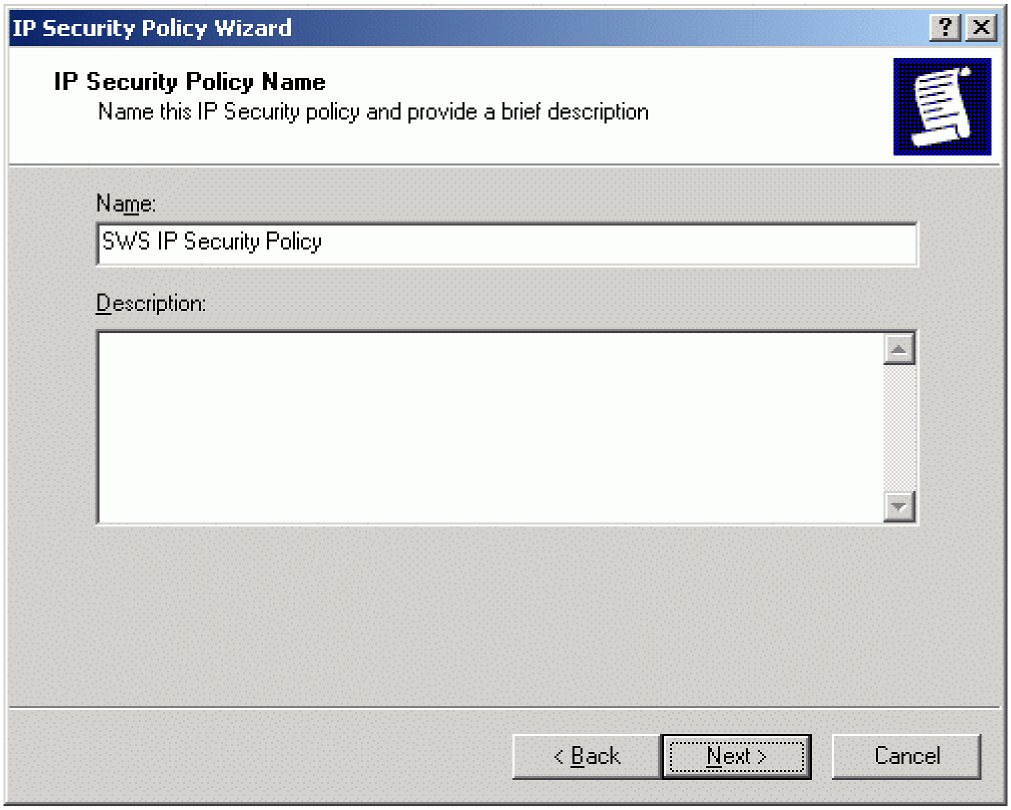
Welcome to the IP Security Policy Wizard

This wizard helps you create an IP Security policy. You will specify the level of security to use when communicating with specific computers or groups of computers (subnets), and for particular IP traffic types.

To continue, click Next.

Press the **Next** button to continue.

Specify the **Name** of the new **IP Security Policy** and optionally provide a brief description of it.



IP Security Policy Wizard

IP Security Policy Name

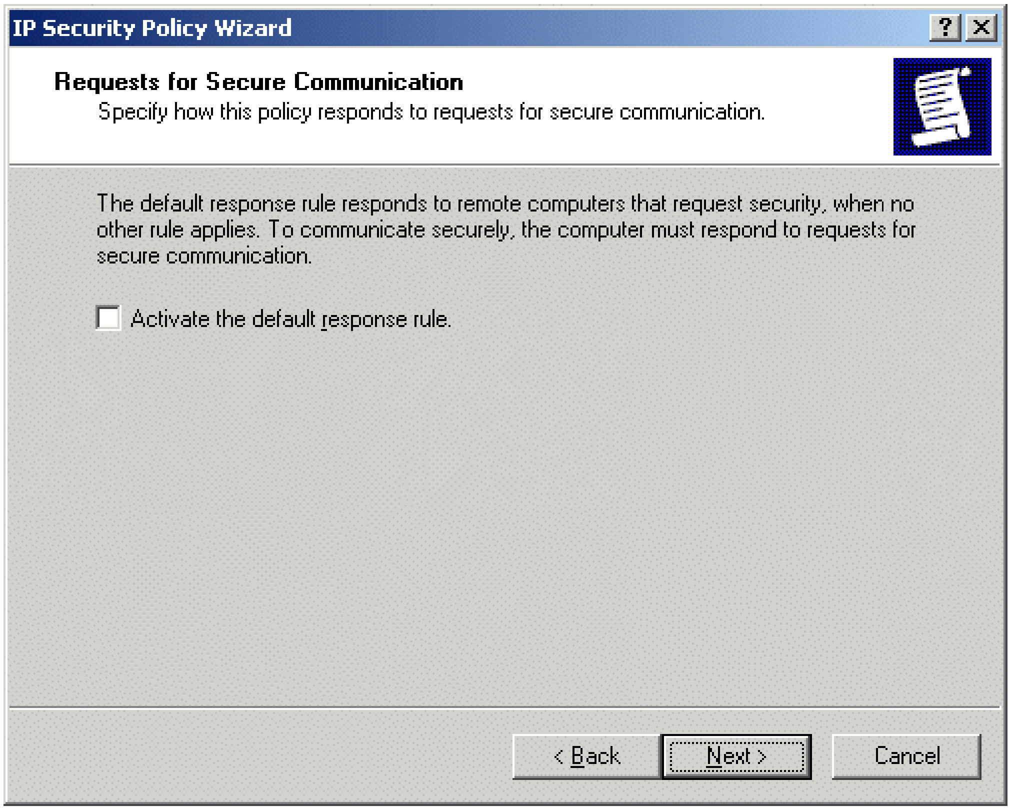
Name this IP Security policy and provide a brief description

Name: SWS IP Security Policy

Description:

Press the **Next** button to continue.

Uncheck the **Activate the default response rule** option.



IP Security Policy Wizard

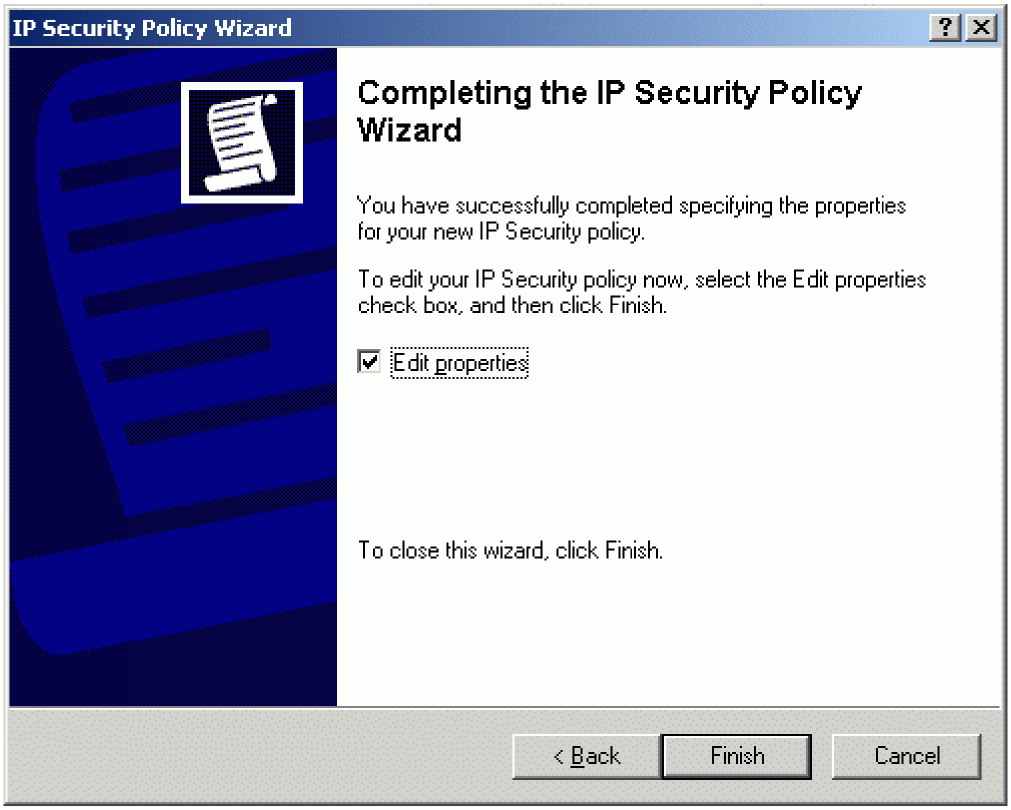
Requests for Secure Communication
Specify how this policy responds to requests for secure communication.

The default response rule responds to remote computers that request security, when no other rule applies. To communicate securely, the computer must respond to requests for secure communication.

□ Activate the default response rule.

Press the **Next** button to continue.

Set the **Edit properties** option.



Completing the IP Security Policy Wizard

You have successfully completed specifying the properties for your new IP Security policy.

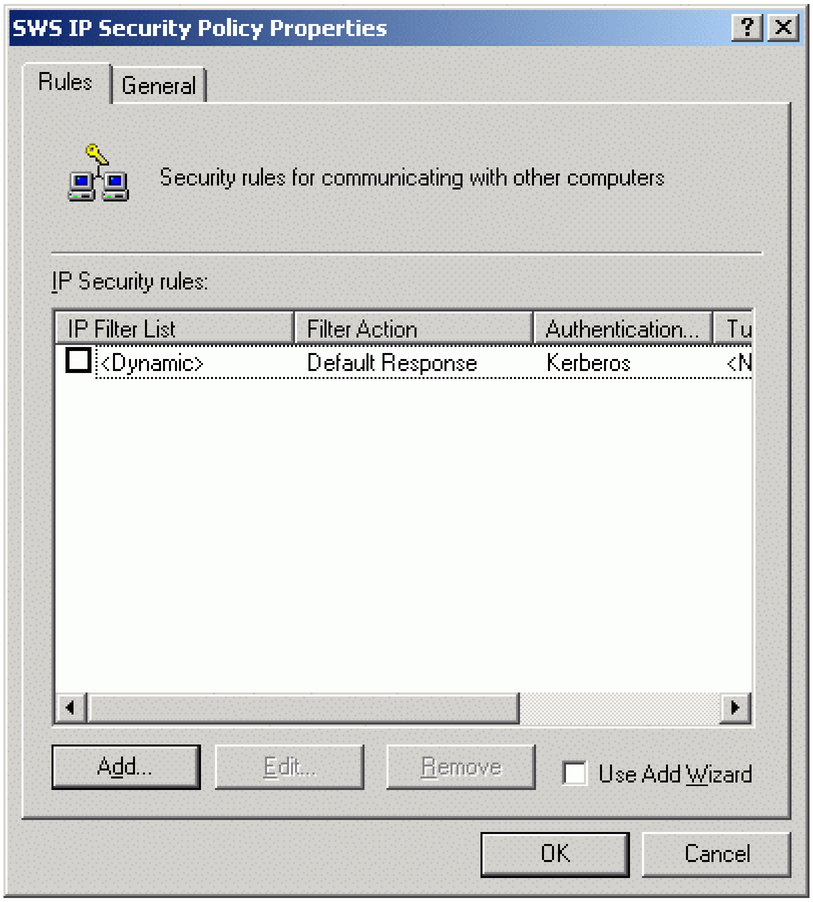
To edit your IP Security policy now, select the Edit properties check box, and then click Finish.

☑ Edit properties

To close this wizard, click Finish.

Press the **Finish** button.

On the **SWS IP Security Policy Properties** window that appears uncheck the **Use Add Wizard** option.



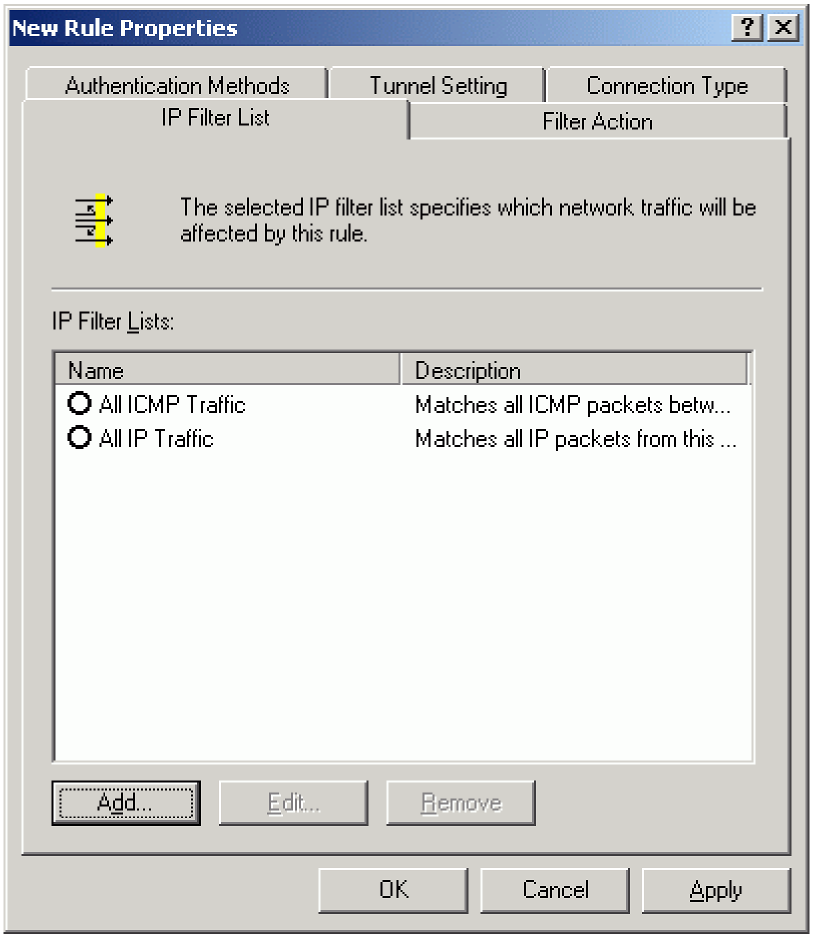
Security rules for communicating with other computers

IP Security rules:

IP Filter List	Filter Action	Authentication...	Tu
☐ <Dynamic>	Default Response	Kerberos	<N

Press the **Add** button on the Rules tab.

New Rules Properties window appears.

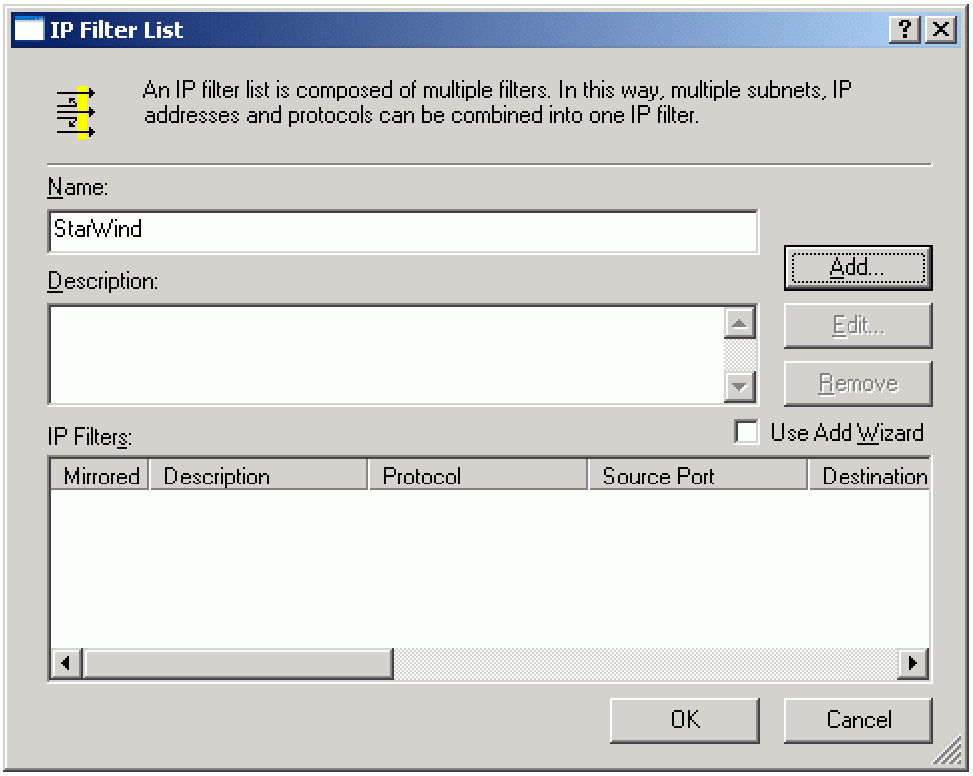


The selected IP filter list specifies which network traffic will be affected by this rule.

Name	Description
○ All ICMP Traffic	Matches all ICMP packets betw...
○ All IP Traffic	Matches all IP packets from this ...

Press the **Add** button on the **IP Filter List** tab.

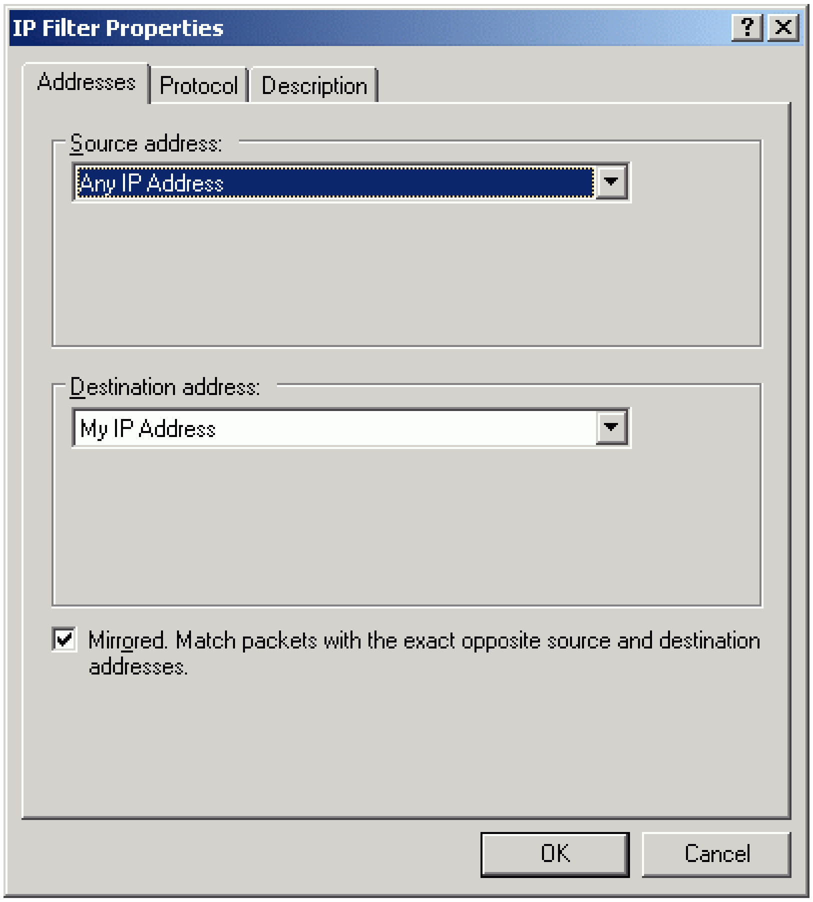
IP Filter List window appears. Uncheck the **Use Add Wizard** option.



IP Filter List
An IP filter list is composed of multiple filters. In this way, multiple subnets, IP addresses and protocols can be combined into one IP filter.
Name:
StarWind
Description:
Add...
Edit...
Remove
IP Filters:
□ Use Add Wizard
Mirrored
Description
Protocol
Source Port
Destination
OK
Cancel

Specify the **Name** of IP Filter and optionally a brief description and press **Add** button.

Filter Properties window appears.



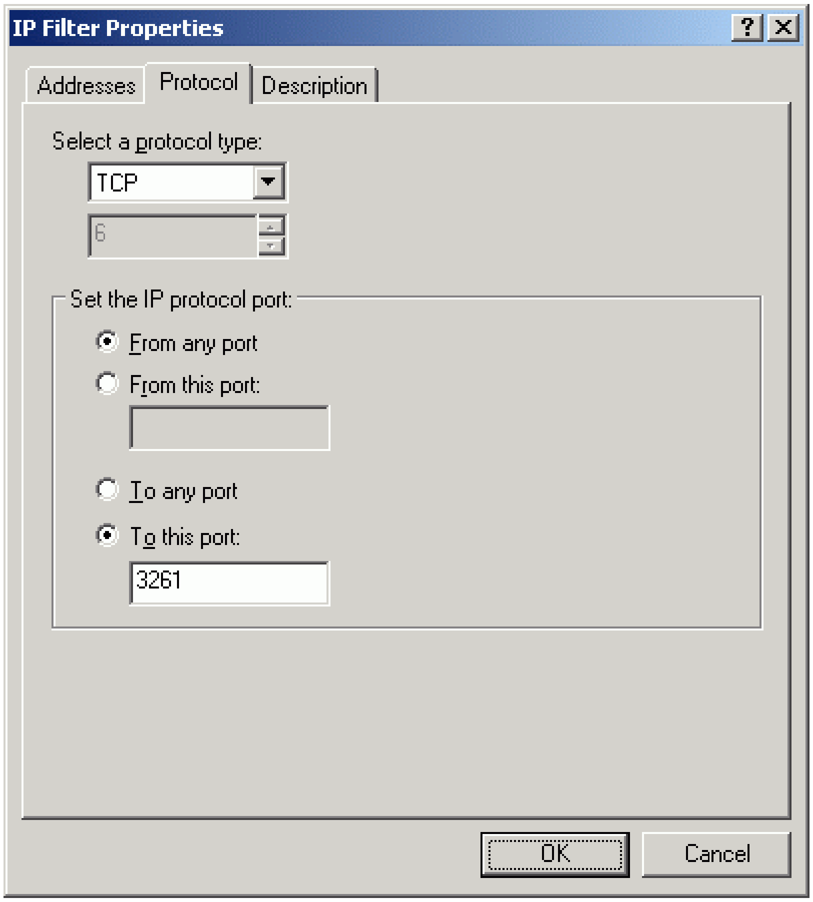
Source address: Any IP Address

Destination address: My IP Address

☑ Mirrored. Match packets with the exact opposite source and destination addresses.

Specify **Source address** and **Destination address**. To delimit allow connections more strictly in the **Source address** field you can specify IP address of the separate host or subnet.

Switch to the **Protocol** tab.



IP Filter Properties

Select a protocol type: TCP

6

Set the IP protocol port:

● From any port

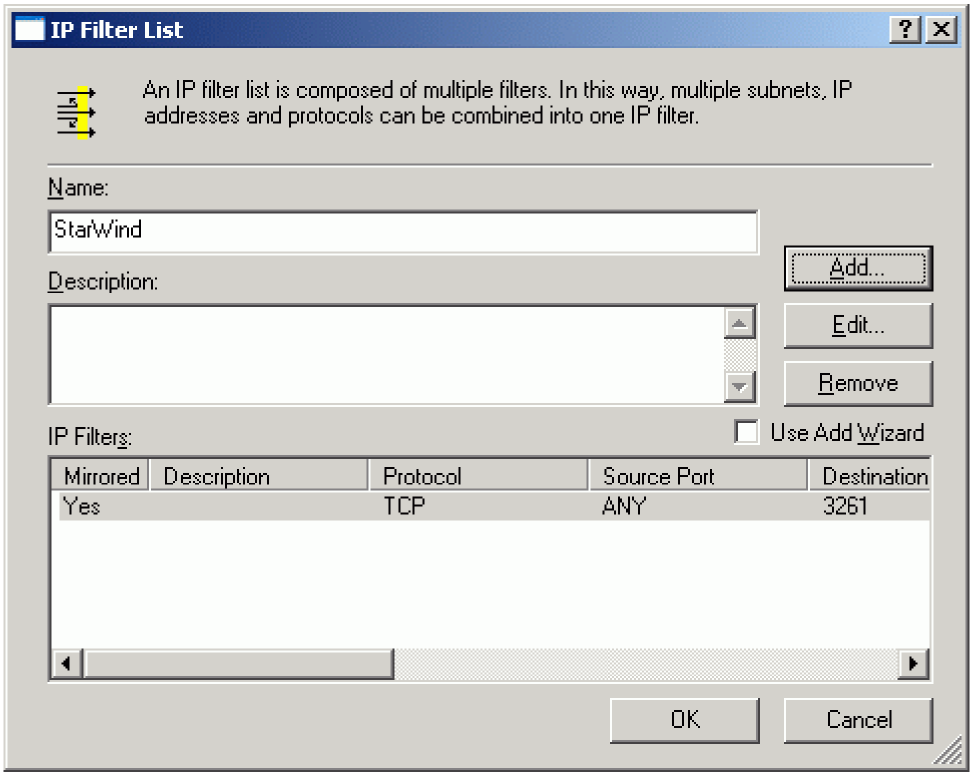
○ From this port:

○ To any port

● To this port: 3261

Specify protocol (**TCP** in our case) and port number (**3261**) and press **OK**. This filter is for **StarWind** management console connections.

New rule appears in the list.



IP Filter List

An IP filter list is composed of multiple filters. In this way, multiple subnets, IP addresses and protocols can be combined into one IP filter.

Name: StarWind

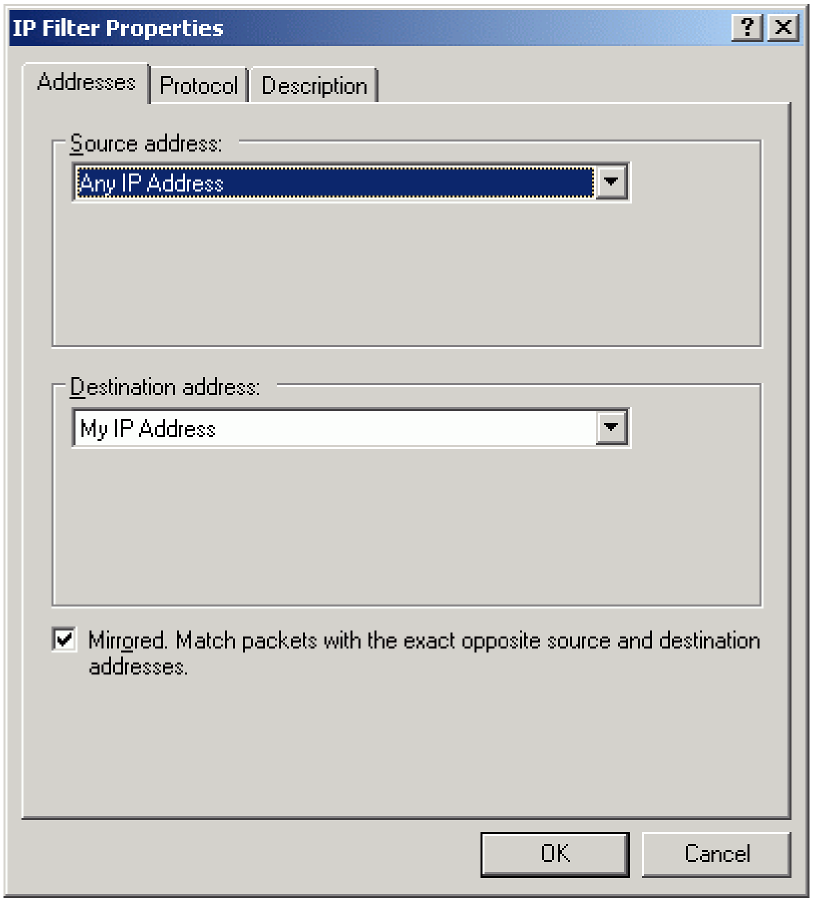
Description:

IP Filters:

Mirrored	Description	Protocol	Source Port	Destination
Yes		TCP	ANY	3261

Click the **Add** button again.

Filter Properties window appears.



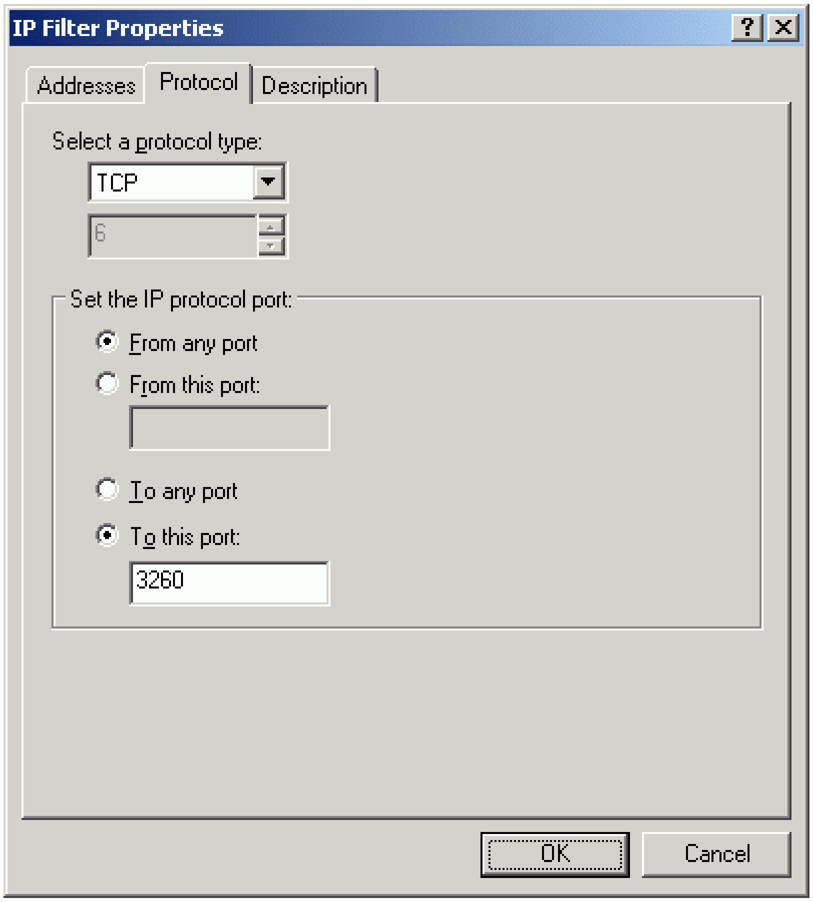
Source address: Any IP Address

Destination address: My IP Address

☑ Mirrored. Match packets with the exact opposite source and destination addresses.

Specify **Source address** and **Destination address**.

Switch to the **Protocol** tab.



Select a protocol type: TCP

6

Set the IP protocol port:

● From any port

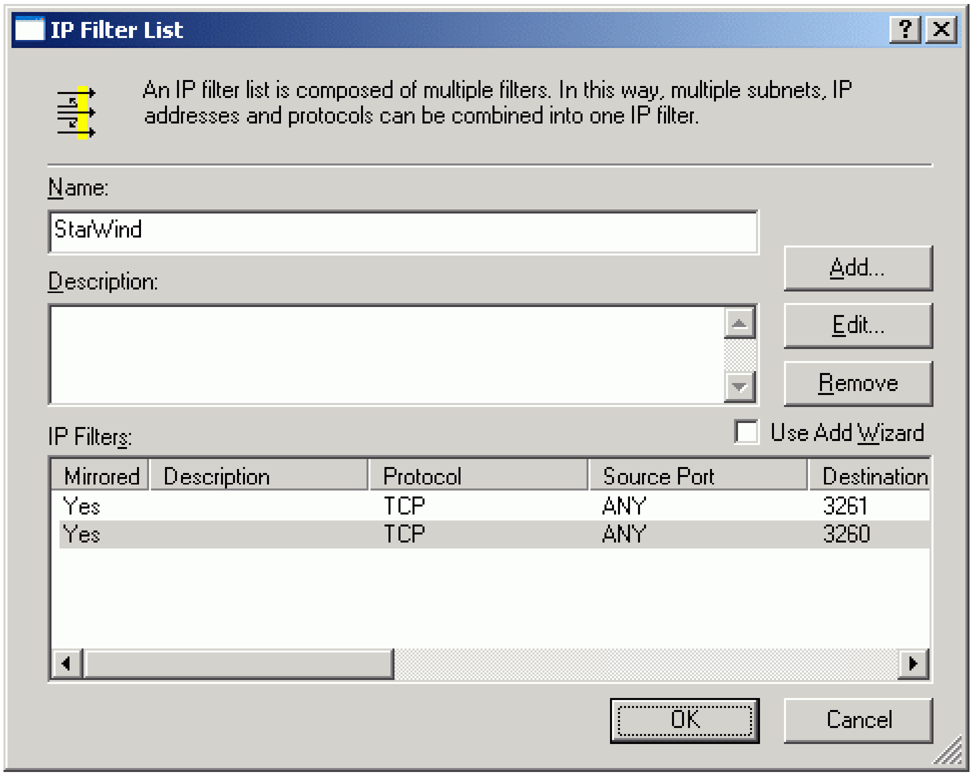
○ From this port:

○ To any port

● To this port: 3260

Specify protocol (**TCP** in our case) and port number (**3260**) and press **OK**. This filter is for **StarWind** service connections (iSCSI traffic itself).

One more new rule appears in the list.



An IP filter list is composed of multiple filters. In this way, multiple subnets, IP addresses and protocols can be combined into one IP filter.

Name: StarWind

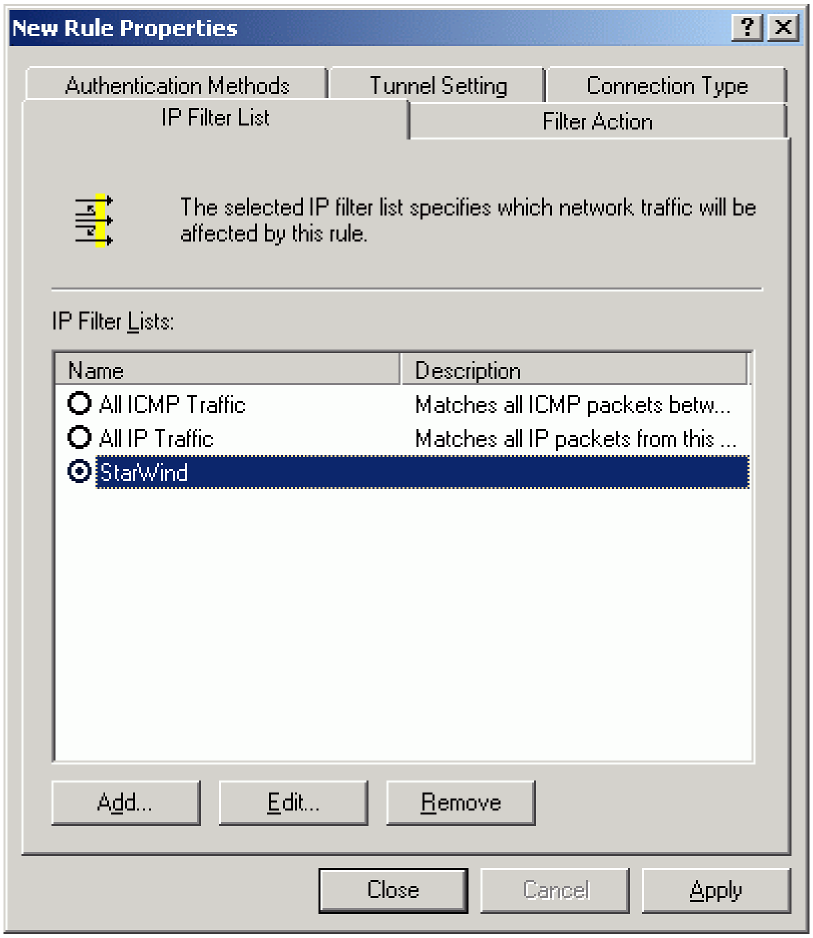
Description:

IP Filters:

Mirrored	Description	Protocol	Source Port	Destination
Yes		TCP	ANY	3261
Yes		TCP	ANY	3260

Press the **OK** button to continue.

We return to the **IP Filter List** tab again.



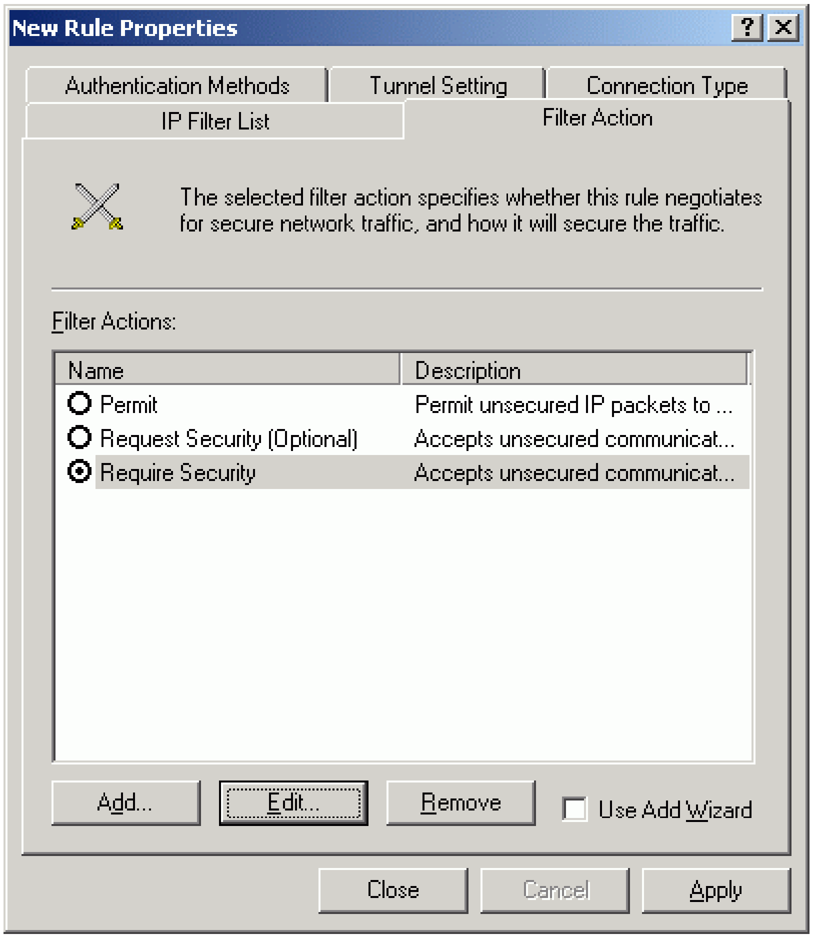
The selected IP filter list specifies which network traffic will be affected by this rule.

IP Filter Lists:

	Name	Description
○	All ICMP Traffic	Matches all ICMP packets betw...
○	All IP Traffic	Matches all IP packets from this ...
●	StarWind	

Select newly created filter **StarWind** from the list and switch to the **Filter Action** tab.

On the **Filter Action** tab select **Require Security** option from the list.



The selected filter action specifies whether this rule negotiates for secure network traffic, and how it will secure the traffic.

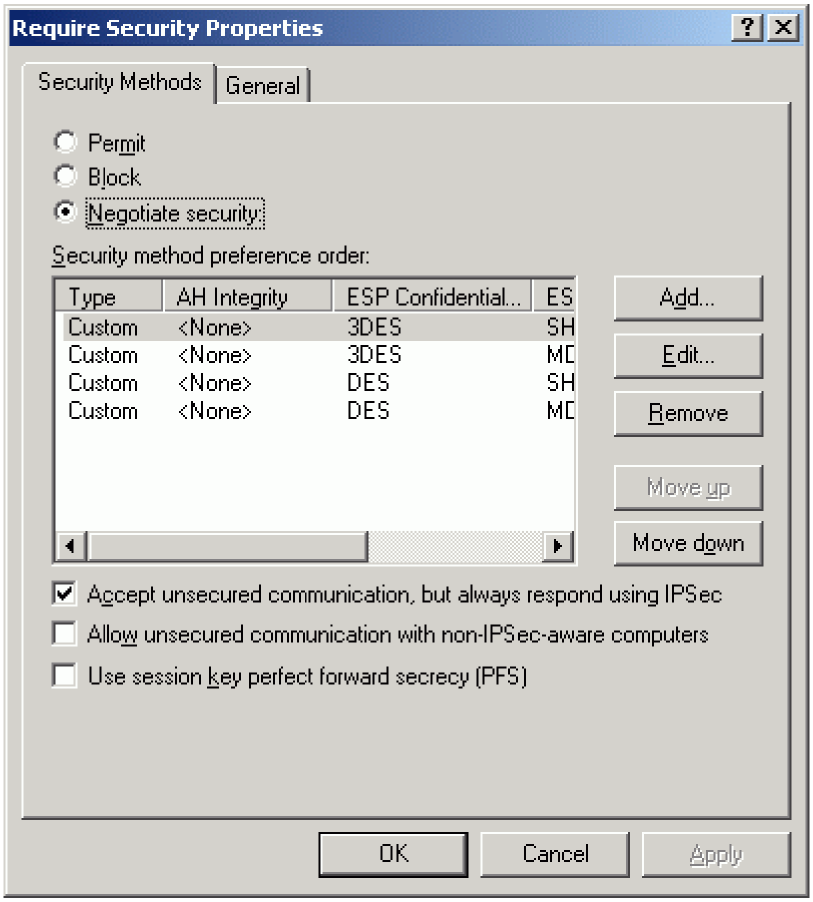
Filter Actions:

Name	Description
○ Permit	Permit unsecured IP packets to ...
○ Request Security (Optional)	Accepts unsecured communicat...
● Require Security	Accepts unsecured communicat...

□ Use Add Wizard

Press the **Edit** button to continue.

Require Security Properties window appears. Select **Negotiate security**, specify **Security method preference** order and set **Accept unsecured communication, but always respond using IPSec** option.



Require Security Properties

Security Methods | General

○ Permit
○ Block
● Negotiate security:

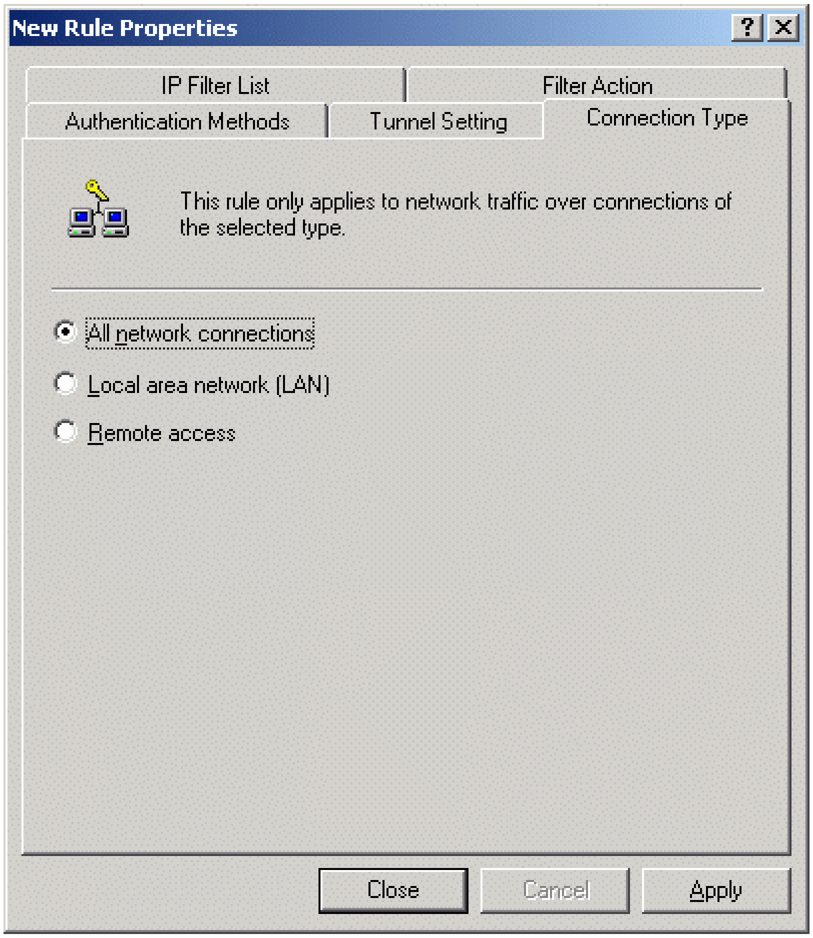
Security method preference order:

Type	AH Integrity	ESP Confidential...	ES
Custom	<None>	3DES	SH
Custom	<None>	3DES	MD
Custom	<None>	DES	SH
Custom	<None>	DES	MD

☑ Accept unsecured communication, but always respond using IPSec
☐ Allow unsecured communication with non-IPSec-aware computers
☐ Use session key perfect forward secrecy (PFS)

Press the **OK** button to continue.

Switch to the **Connection Type** tab.



This rule only applies to network traffic over connections of the selected type.

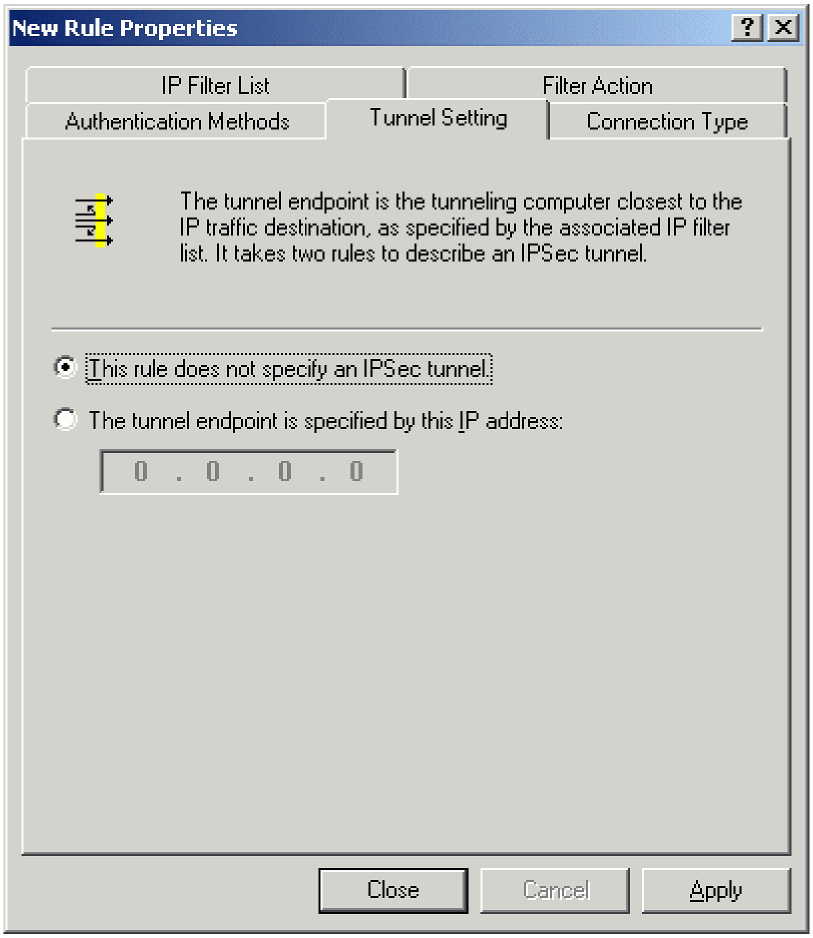
● All network connections

○ Local area network (LAN)

○ Remote access

Select **All network connections**.

Switch to the **Tunnel Setting** tab.



New Rule Properties

The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the associated IP filter list. It takes two rules to describe an IPSec tunnel.

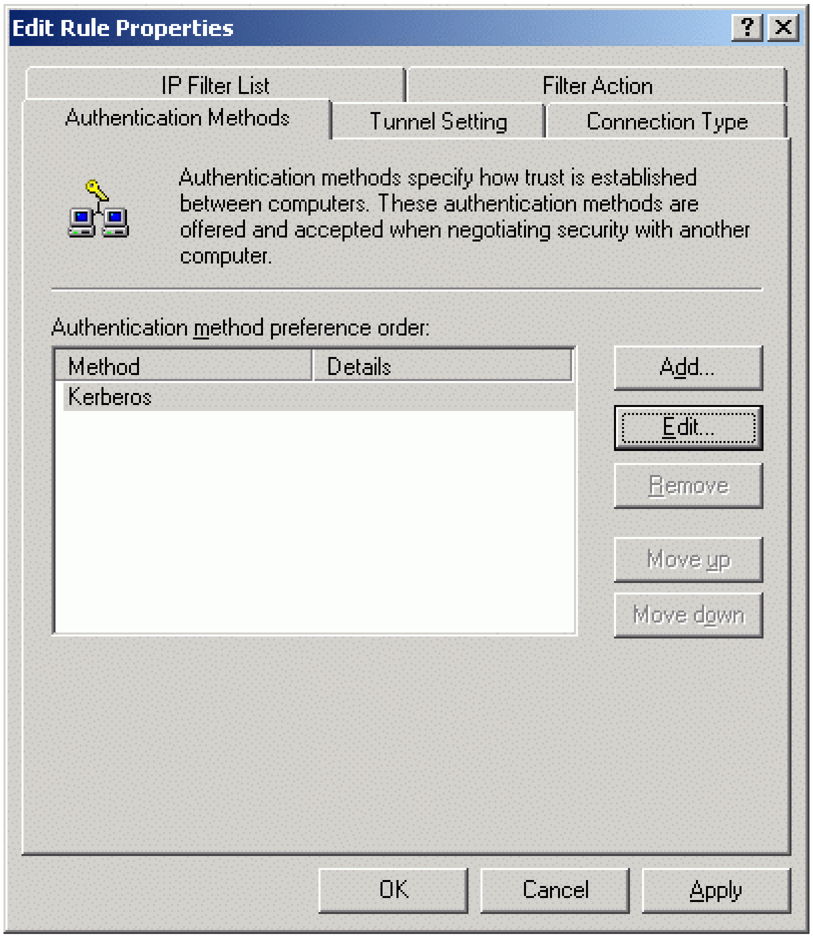
● This rule does not specify an IPSec tunnel.

○ The tunnel endpoint is specified by this IP address:

0 . 0 . 0 . 0

Select **This rule does not specify an IPSec tunnel**.

Switch to the **Authentication Methods** tab.



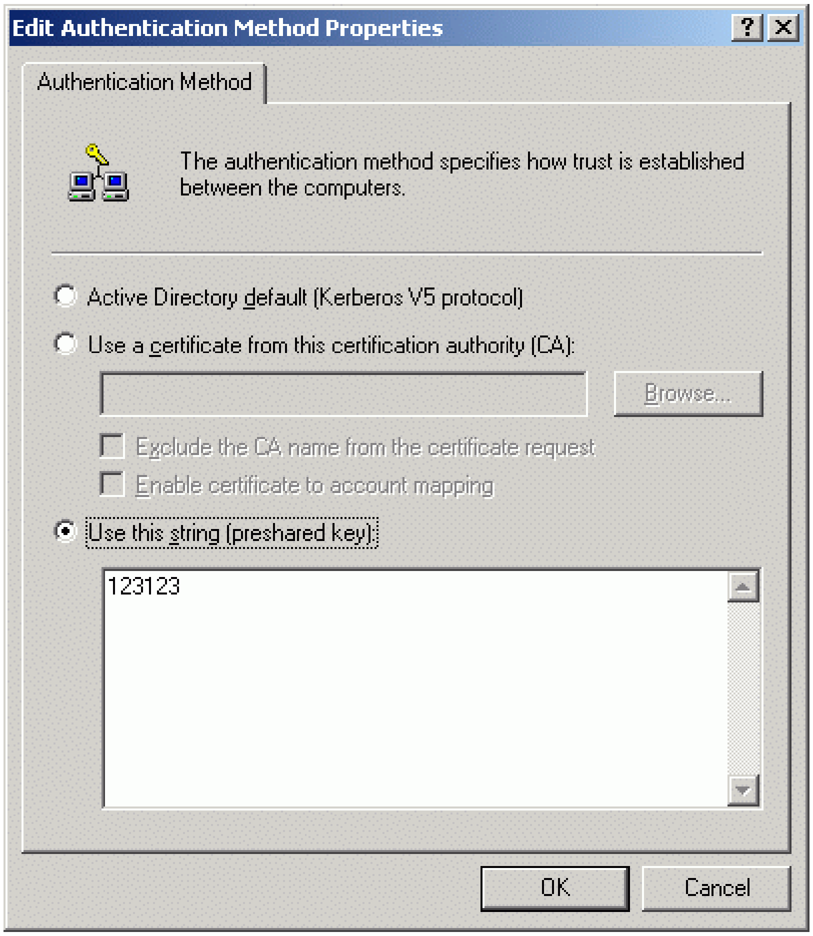
Authentication methods specify how trust is established between computers. These authentication methods are offered and accepted when negotiating security with another computer.

Authentication method preference order:

Method	Details
Kerberos	

Press the **Edit** button to continue.

Edit **Authentication Method Properties** window appears. Select **Use this string (preshared key)** option and type in the preshared key in the field.



Edit Authentication Method Properties

Authentication Method

The authentication method specifies how trust is established between the computers.

○ Active Directory default (Kerberos V5 protocol)

○ Use a certificate from this certification authority (CA):

□ Exclude the CA name from the certificate request

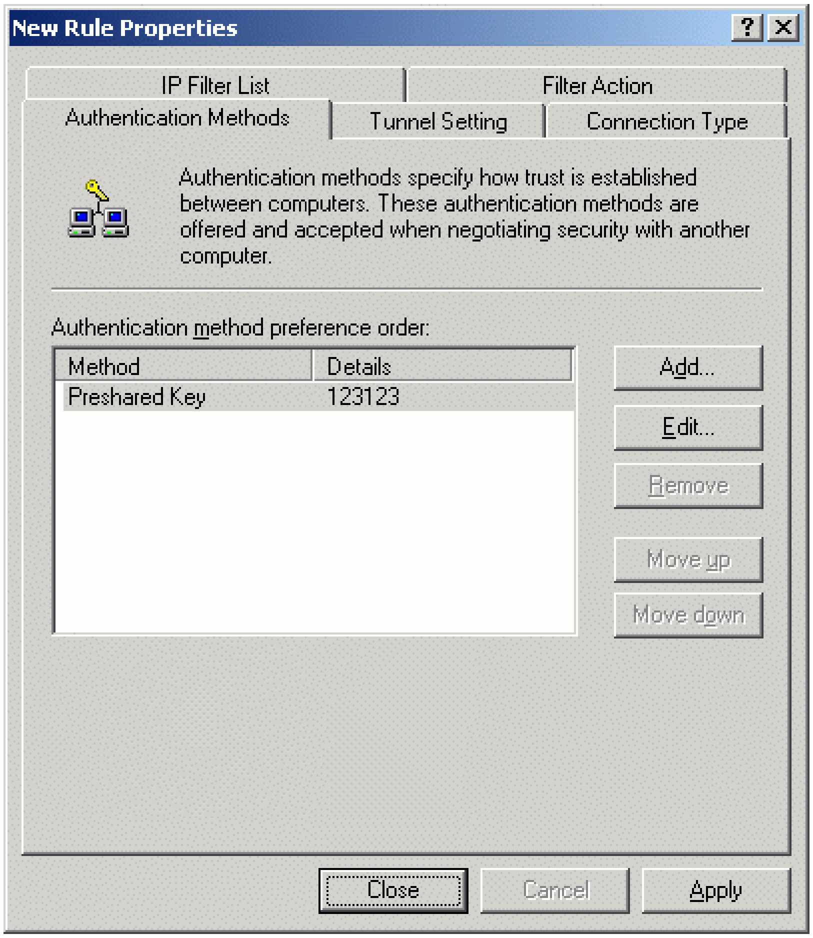
□ Enable certificate to account mapping

● Use this string (preshared key):

123123

Press the **OK** button to continue.

We return to the **Authentication Methods** tab.



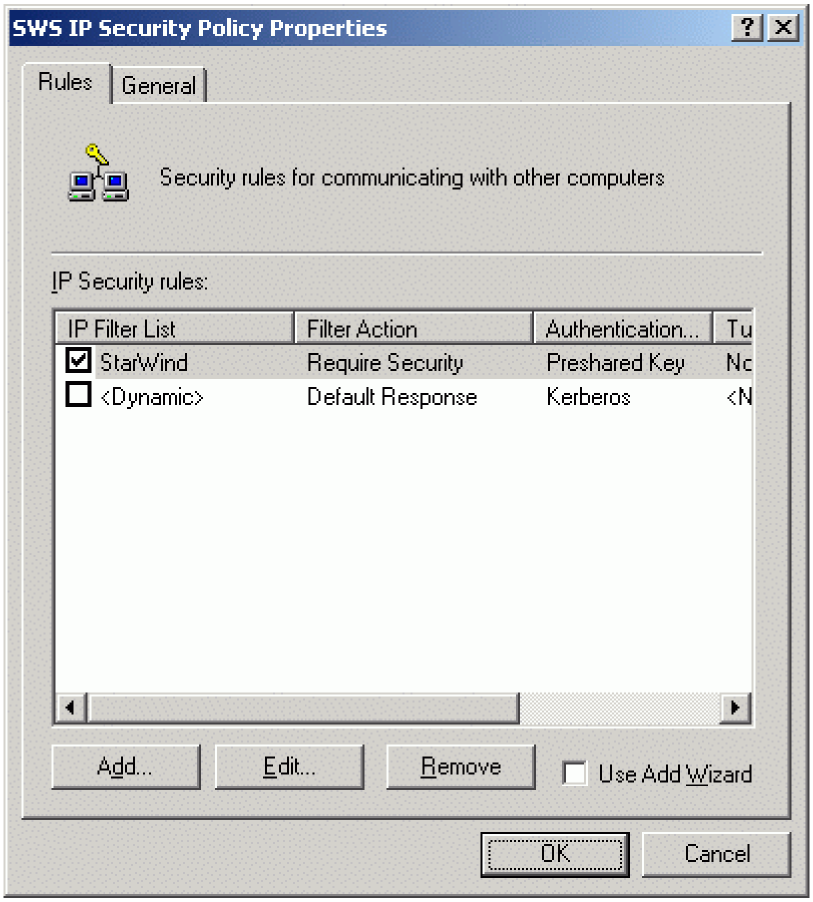
Authentication methods specify how trust is established between computers. These authentication methods are offered and accepted when negotiating security with another computer.

Authentication method preference order:

Method	Details
Preshared Key	123123

Press the **Close** button to continue.

Select **StarWind** from the list of available IP Security rules.

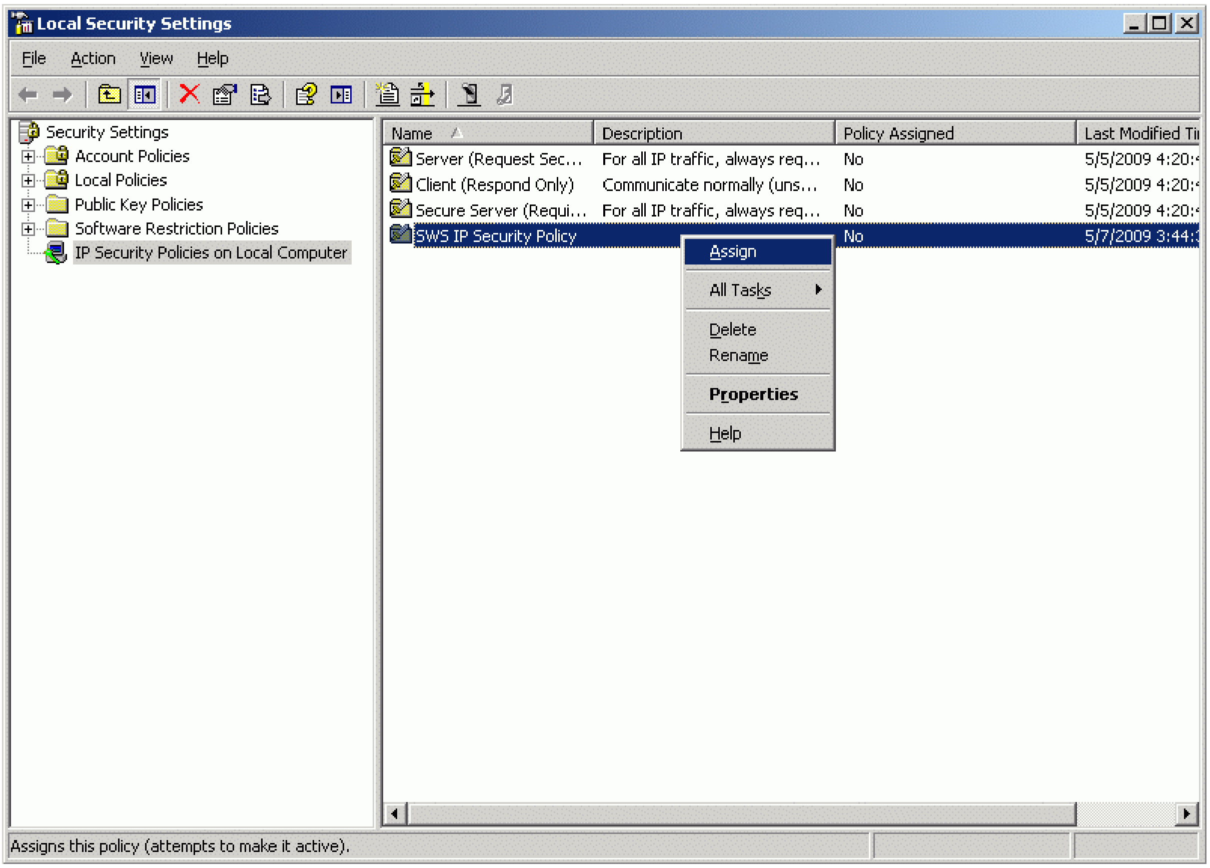

SWS IP Security Policy Properties
?
×
Rules
General
Security rules for communicating with other computers
IP Security rules:
Add...
Edit...
Remove
Use Add Wizard
OK
Cancel

IP Filter List	Filter Action	Authentication...	Tu
☑ StarWind	Require Security	Preshared Key	Nc
□ <Dynamic>	Default Response	Kerberos	<N

□ Use Add Wizard

Press the **Close** button.

Assign recently created policy by pressing right mouse button and selecting **Assign** option.

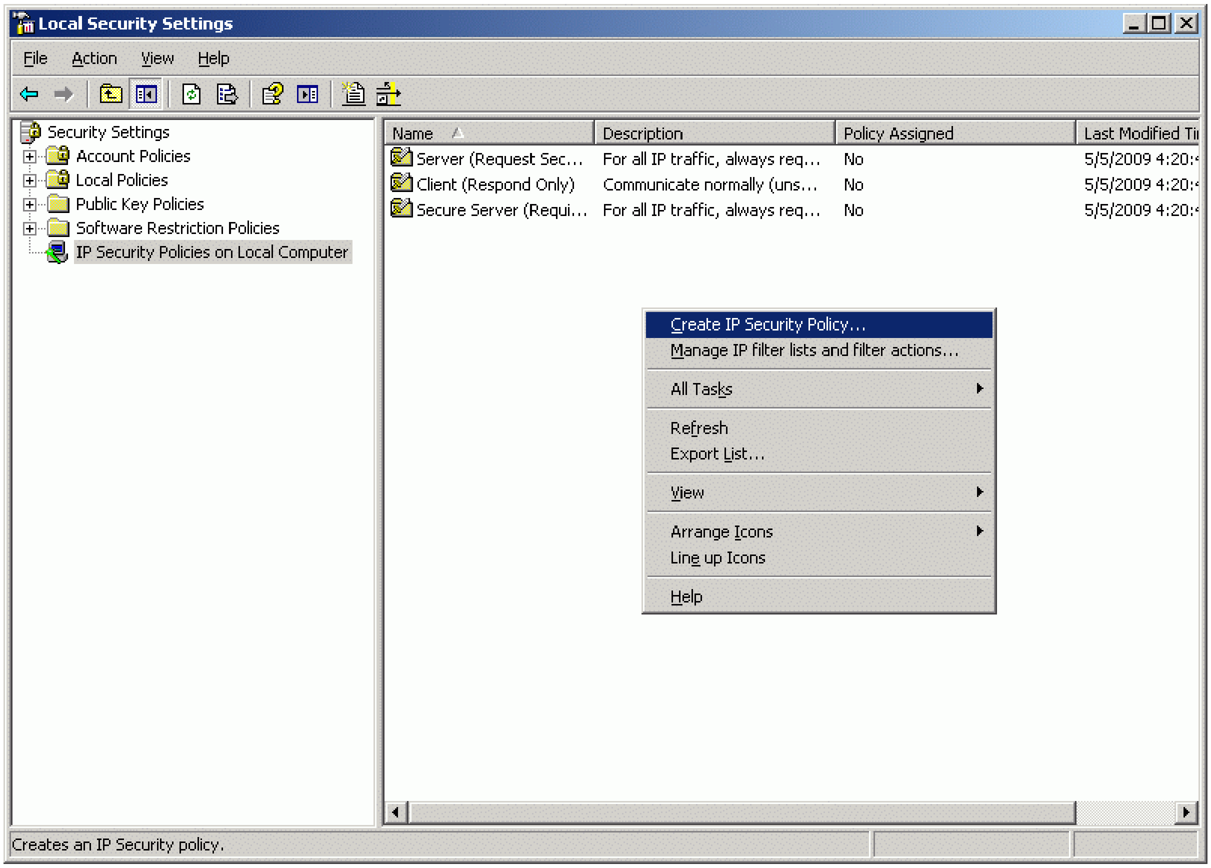


Name	Description	Policy Assigned	Last Modified Ti
Server (Request Sec...	For all IP traffic, always req...	No	5/5/2009 4:20:
Client (Respond Only)	Communicate normally (uns...	No	5/5/2009 4:20:
Secure Server (Requi...	For all IP traffic, always req...	No	5/5/2009 4:20:
SWS IP Security Policy		No	5/7/2009 3:44:

Assigns this policy (attempts to make it active).

Client-Side Configuration, Creatng New Ip Security Policy

Launch the **Local Security Settings** management console selecting **Start -> Control Panel -> Administrative tools -> Local Security Policy**. **Local Security Settings** management console appears. Switch to the **IP Security Policies on Local Computer**.

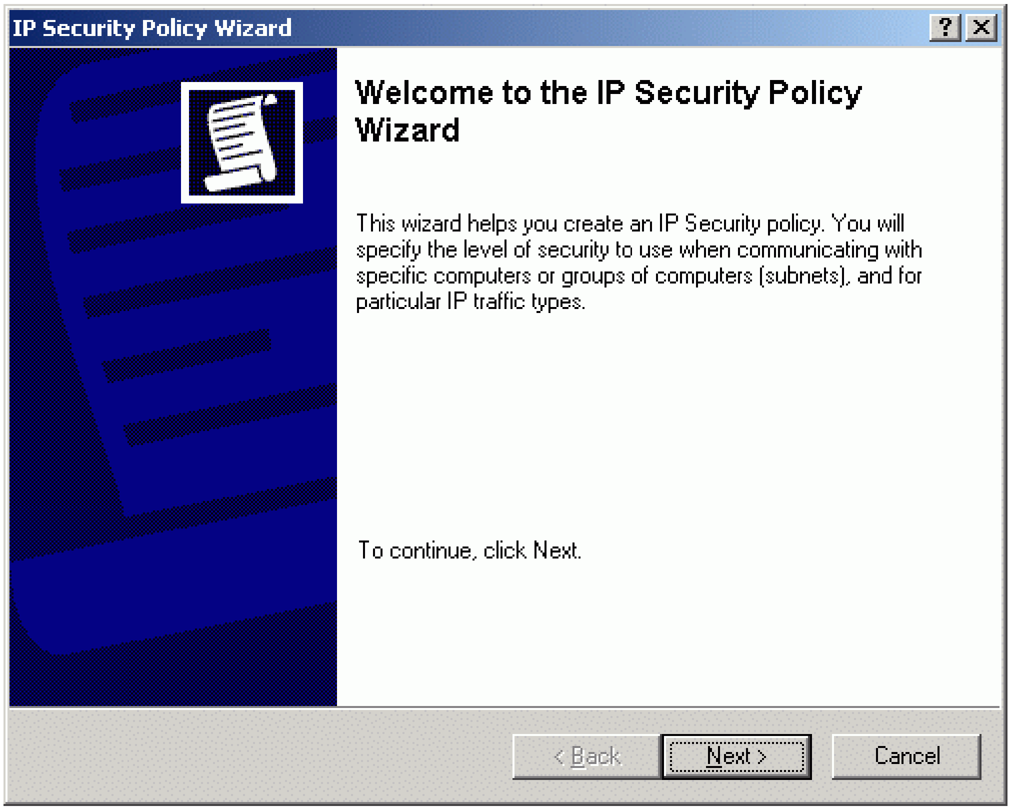


Name	Description	Policy Assigned	Last Modified Ti
Server (Request Sec...	For all IP traffic, always req...	No	5/5/2009 4:20:
Client (Respond Only)	Communicate normally (uns...	No	5/5/2009 4:20:
Secure Server (Requi...	For all IP traffic, always req...	No	5/5/2009 4:20:

Creates an IP Security policy.

Click the right mouse button and select **Create IP Security Policy** option.

IP Security Policy Wizard appears.



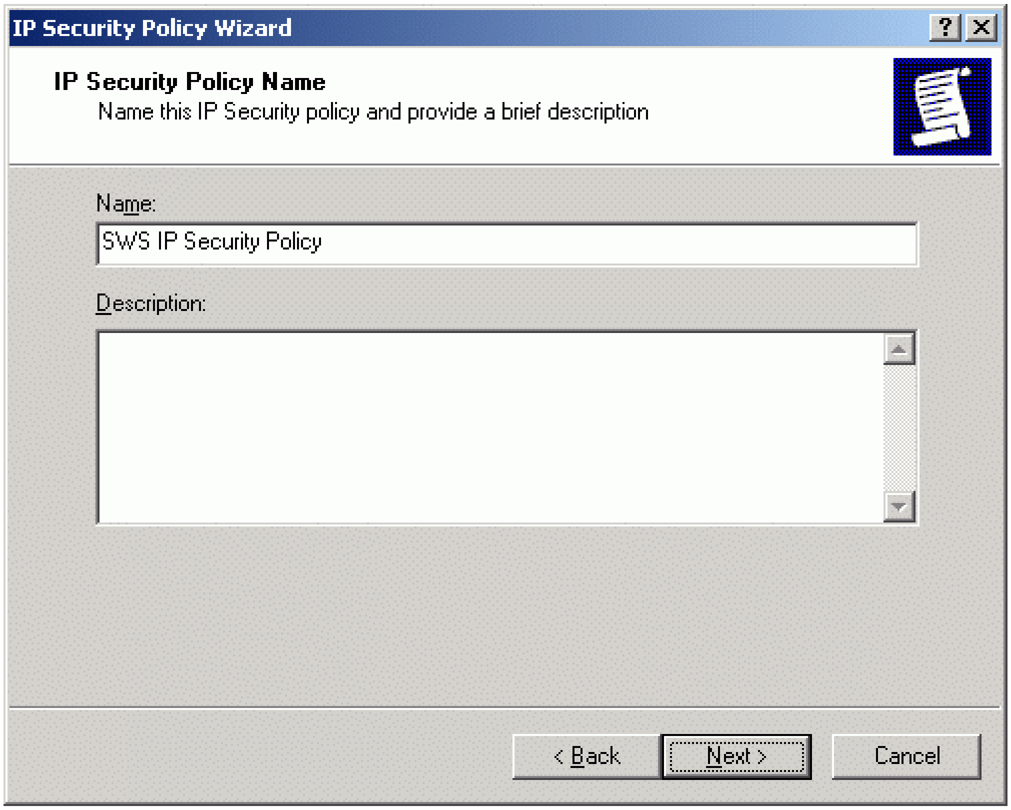
Welcome to the IP Security Policy Wizard

This wizard helps you create an IP Security policy. You will specify the level of security to use when communicating with specific computers or groups of computers (subnets), and for particular IP traffic types.

To continue, click Next.

Press the **Next** button to continue.

Specify the **Name** of the **new IP Security policy** and optionally provide a brief description.



IP Security Policy Wizard

IP Security Policy Name

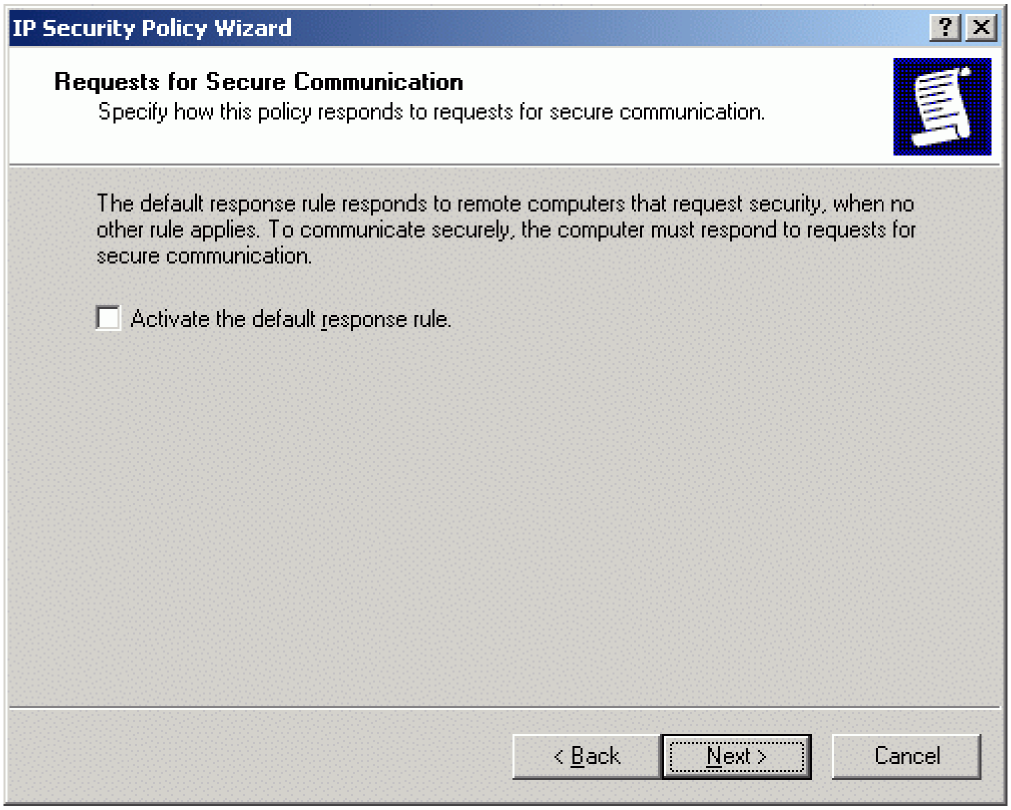
Name this IP Security policy and provide a brief description

Name: SWS IP Security Policy

Description:

Press the **Next** button to continue.

Uncheck the **Activate the default response rule** option.



Requests for Secure Communication

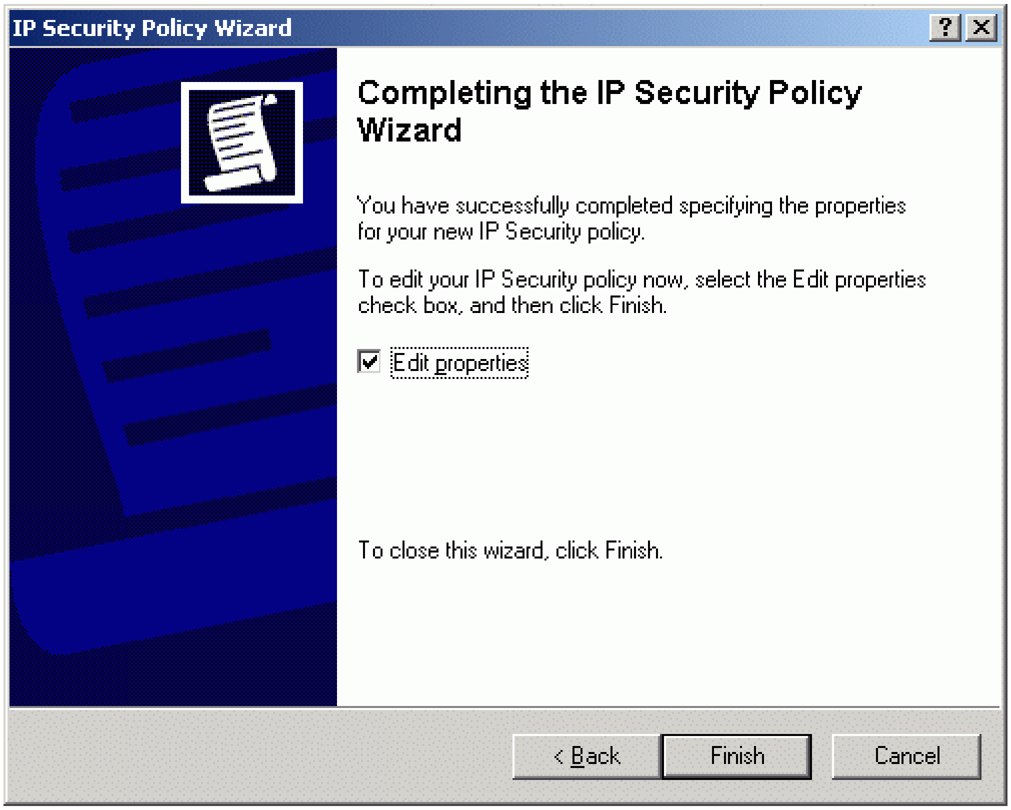
Specify how this policy responds to requests for secure communication.

The default response rule responds to remote computers that request security, when no other rule applies. To communicate securely, the computer must respond to requests for secure communication.

□ Activate the default response rule.

Press the **Next** button to continue.

Set the **Edit properties** option.



Completing the IP Security Policy Wizard

You have successfully completed specifying the properties for your new IP Security policy.

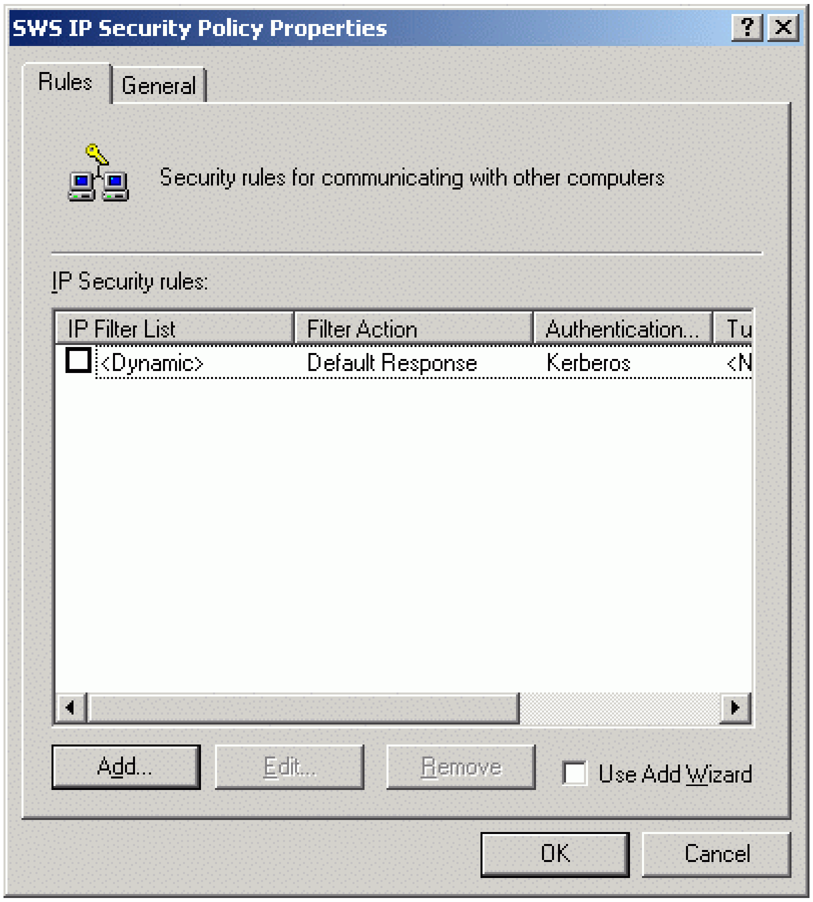
To edit your IP Security policy now, select the Edit properties check box, and then click Finish.

☑ Edit properties

To close this wizard, click Finish.

Press the **Finish** button.

On the **SWS IP Security Policy Properties** window that appears uncheck the **Use Add Wizard** option.



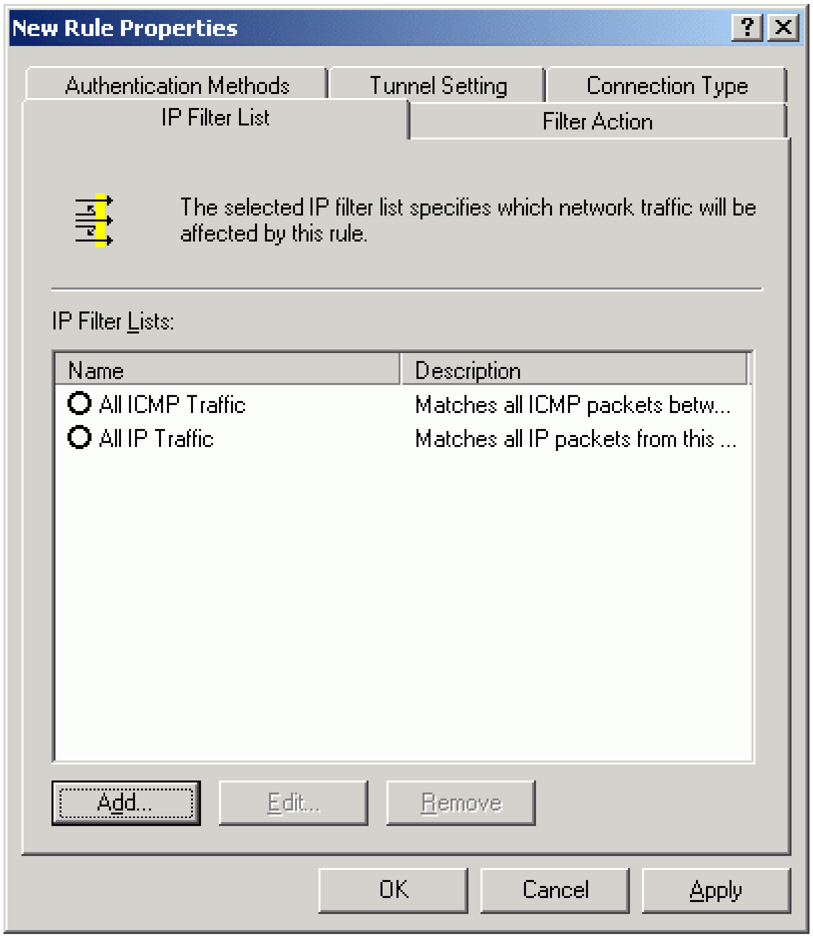
Security rules for communicating with other computers

IP Security rules:

IP Filter List	Filter Action	Authentication...	Tu
☐ <Dynamic>	Default Response	Kerberos	<N

Press the **Add** button on the Rules tab.

New Rules Properties window appears.



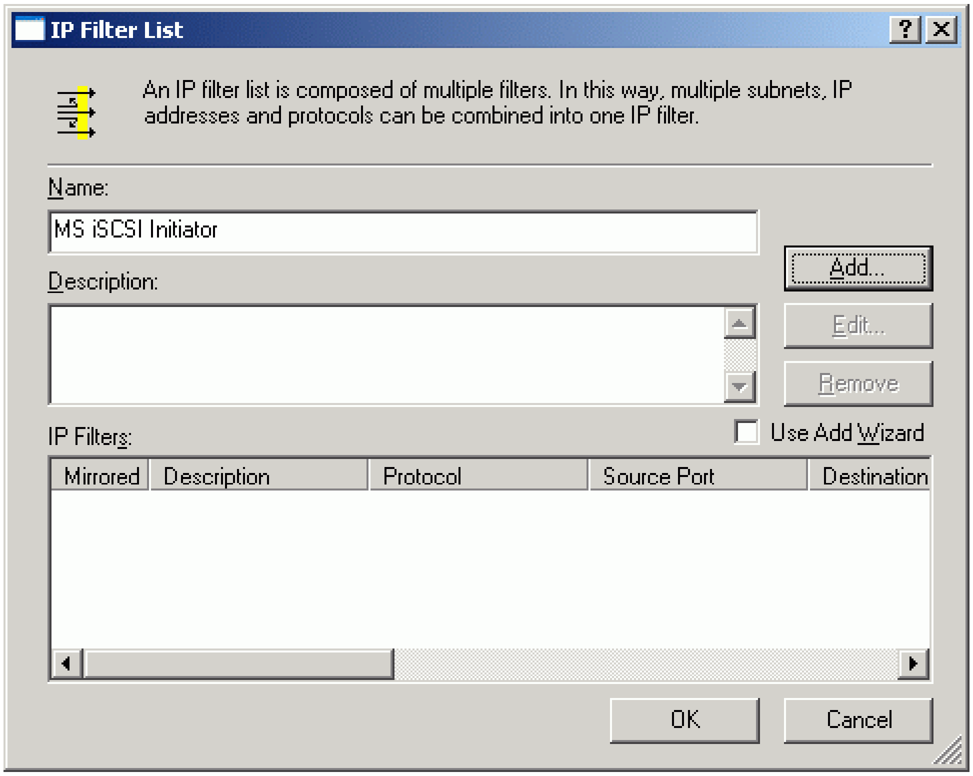
The selected IP filter list specifies which network traffic will be affected by this rule.

IP Filter Lists:

Name	Description
○ All ICMP Traffic	Matches all ICMP packets betw...
○ All IP Traffic	Matches all IP packets from this ...

Press the **Add** button on the **IP Filter List** tab.

IP Filter List window appears. Uncheck the **Use Add Wizard** option.



An IP filter list is composed of multiple filters. In this way, multiple subnets, IP addresses and protocols can be combined into one IP filter.

Name: MS iSCSI Initiator

Description:

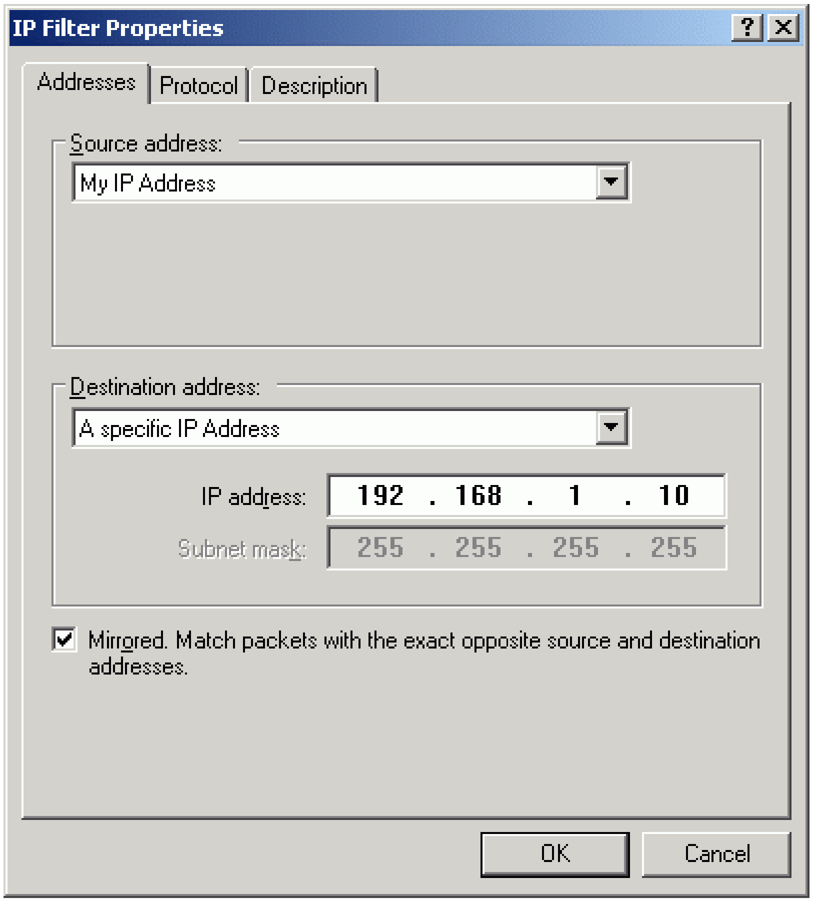
IP Filters:

□ Use Add Wizard

Mirrored	Description	Protocol	Source Port	Destination

Specify the **Name** of **IP Filter** and optionally a brief description and press **Add** button.

IP Filter Properties window appears.



IP Filter Properties

Source address: My IP Address

Destination address: A specific IP Address

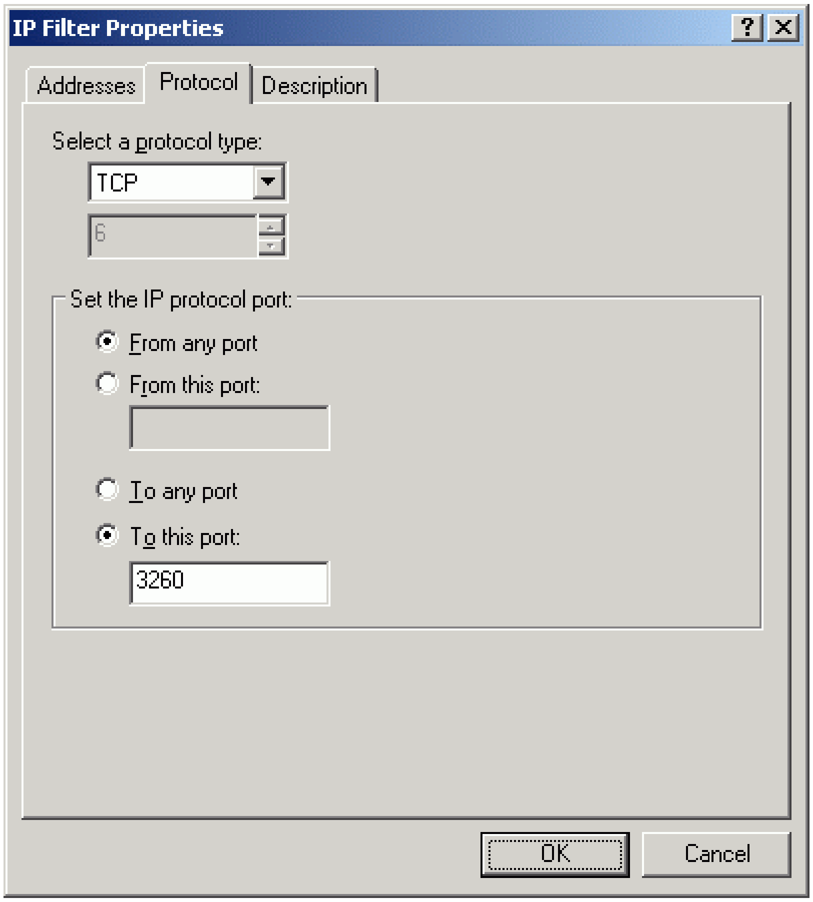
IP address: 192 . 168 . 1 . 10

Subnet mask: 255 . 255 . 255 . 255

☑ Mirrored. Match packets with the exact opposite source and destination addresses.

Specify **Source address** and **Destination address**. **Destination address** is the IP address of the **StarWind** server you wish to connect to.

Switch to the **Protocol** tab.



IP Filter Properties

Select a protocol type: TCP

6

Set the IP protocol port:

● From any port

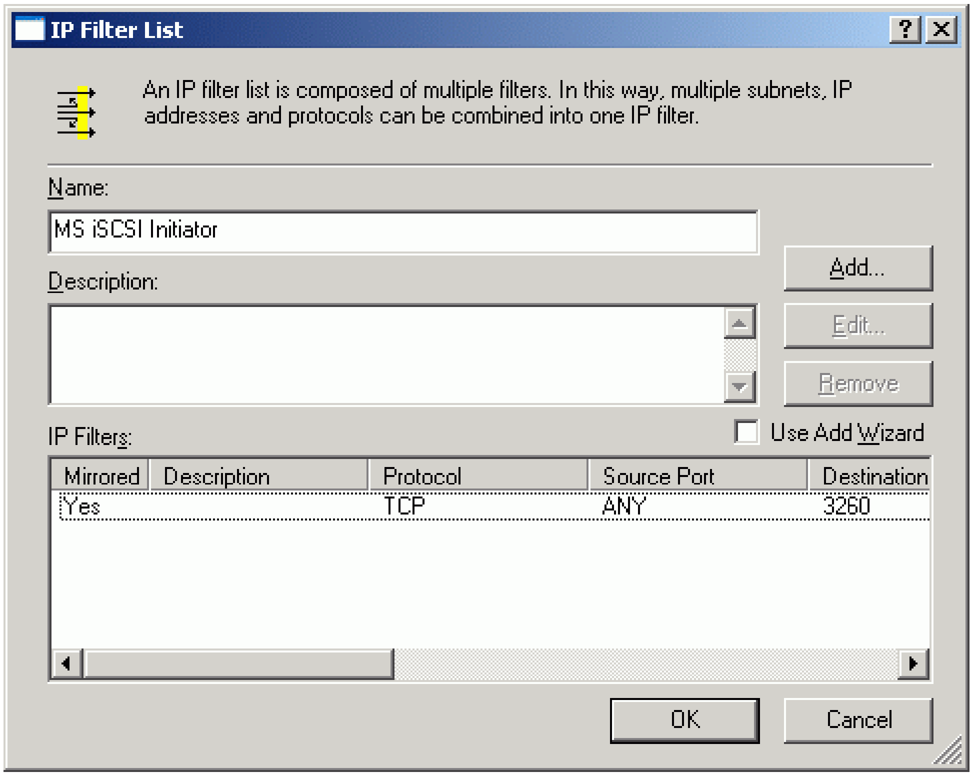
○ From this port:

○ To any port

● To this port: 3260

Specify protocol (**TCP** in our case) and port number (**3260**) and press **OK.** This filter is for **StarWind** service connections (iSCSI traffic itself).

New rule appears in the list.



IP Filter List

An IP filter list is composed of multiple filters. In this way, multiple subnets, IP addresses and protocols can be combined into one IP filter.

Name: MS iSCSI Initiator

Description:

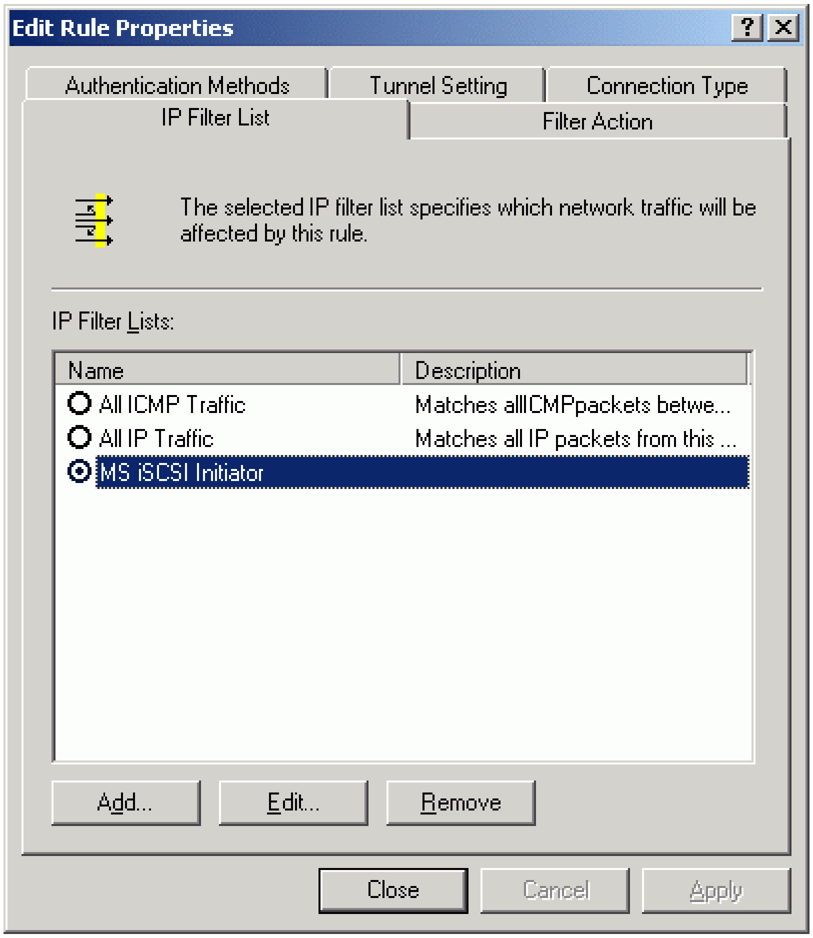
IP Filters:

☐ Use Add Wizard

Mirrored	Description	Protocol	Source Port	Destination
Yes		TCP	ANY	3260

Press the **OK** button.

We return to the **IP Filter List** tab again.



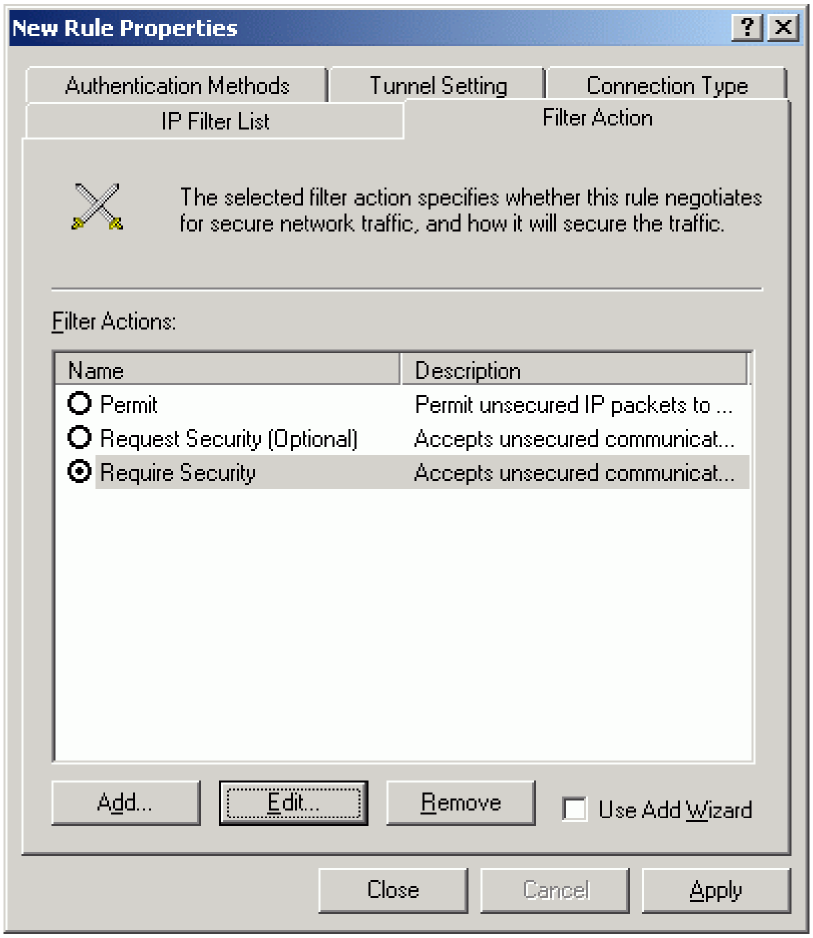
The selected IP filter list specifies which network traffic will be affected by this rule.

IP Filter Lists:

Name	Description
○ All ICMP Traffic	Matches allICMPpackets betwe...
○ All IP Traffic	Matches all IP packets from this ...
● MS iSCSI Initiator	

Select newly created filter **MS iSCSI Initiator** from the list and switch to the **Filter Action** tab.

On the **Filter Action** tab select **Require Security** option from the list.



New Rule Properties

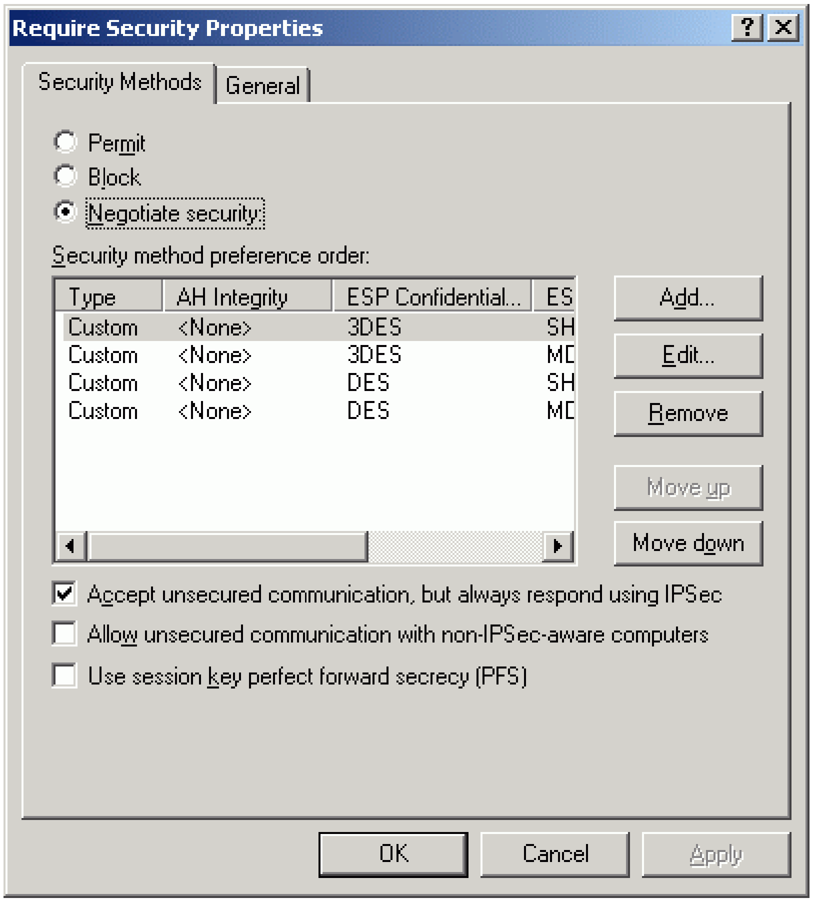
The selected filter action specifies whether this rule negotiates for secure network traffic, and how it will secure the traffic.

Filter Actions:

Name	Description
○ Permit	Permit unsecured IP packets to ...
○ Request Security (Optional)	Accepts unsecured communicat...
● Require Security	Accepts unsecured communicat...

Press the **Edit** button to continue.

Require Security Properties window appears. Select **Negotiate security**, specify **Security method preference** order and set **Accept unsecured communication, but always respond using IPSec** option.



○ Permit
○ Block
● Negotiate security:

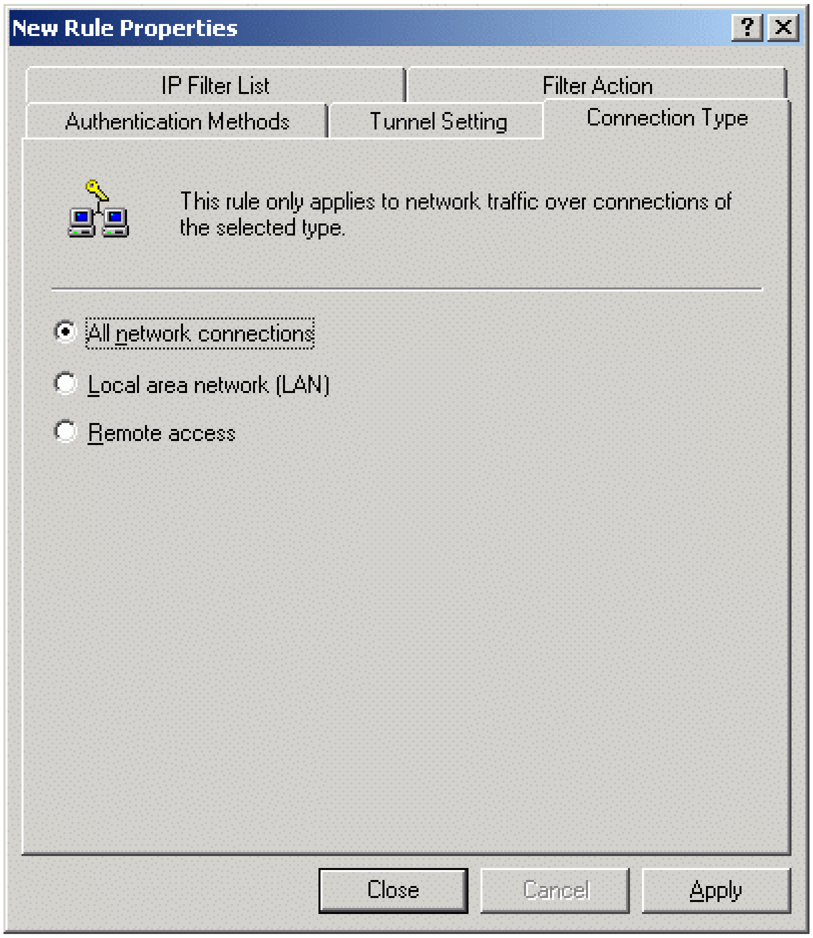
Security method preference order:

Type	AH Integrity	ESP Confidential...	ES
Custom	<None>	3DES	SH
Custom	<None>	3DES	MD
Custom	<None>	DES	SH
Custom	<None>	DES	MD

☑ Accept unsecured communication, but always respond using IPSec
☐ Allow unsecured communication with non-IPSec-aware computers
☐ Use session key perfect forward secrecy (PFS)

Press the **OK** button to continue.

Switch to the **Connection Type** tab.



New Rule Properties

This rule only applies to network traffic over connections of the selected type.

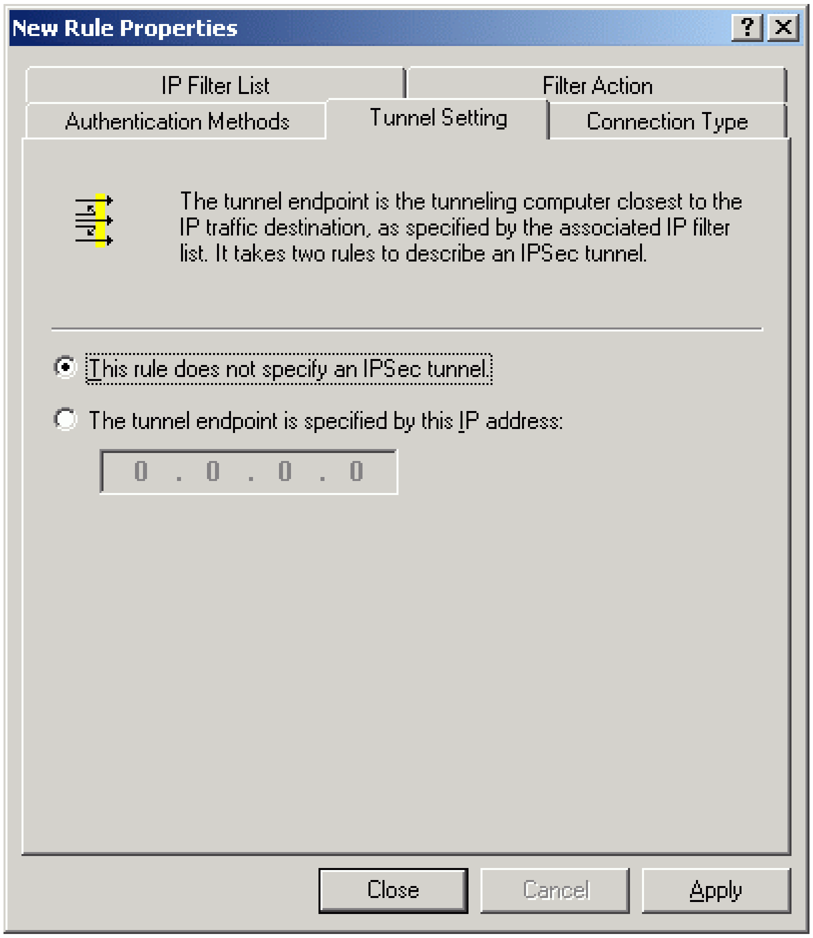
● All network connections

○ Local area network (LAN)

○ Remote access

Select **All network connections**.

Switch to the **Tunnel Setting** tab.



The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the associated IP filter list. It takes two rules to describe an IPSec tunnel.

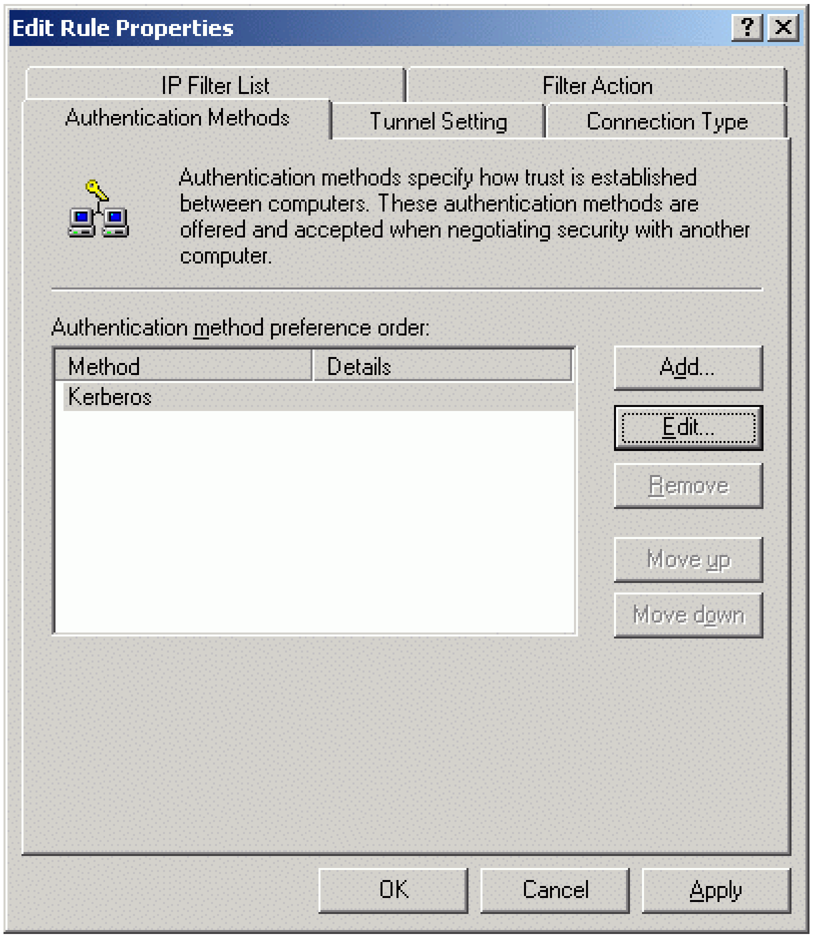
● This rule does not specify an IPSec tunnel.

○ The tunnel endpoint is specified by this IP address:

0 . 0 . 0 . 0

Select **This rule does not specify an IPSec tunnel**.

Switch to the **Authentication Methods** tab.



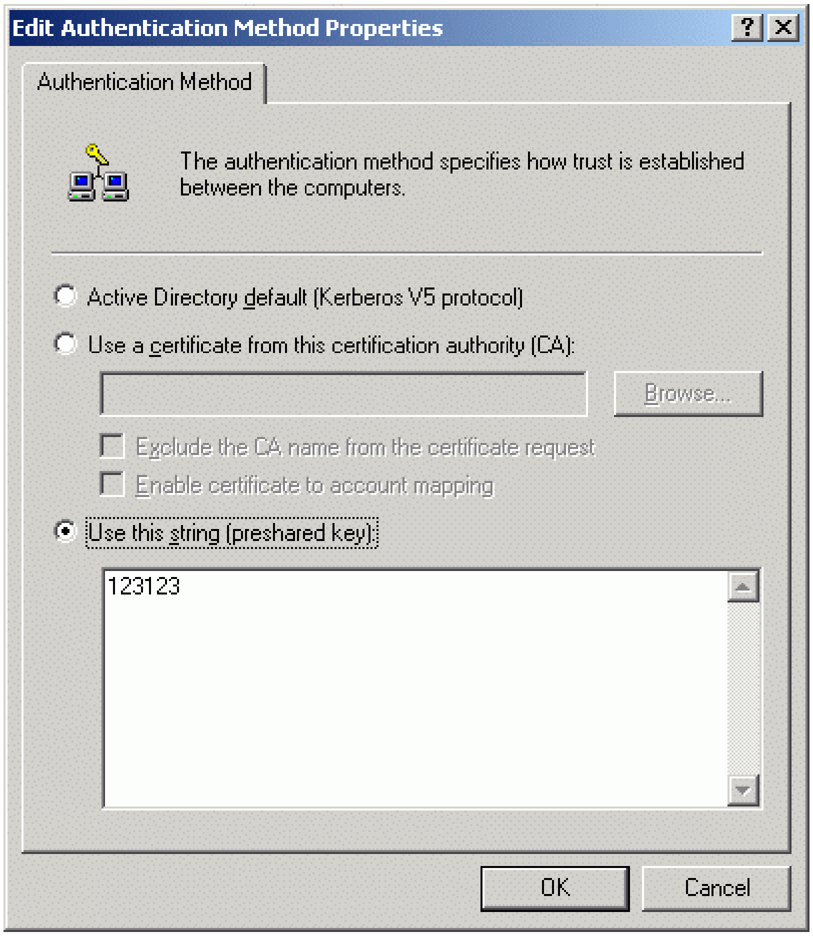
Authentication methods specify how trust is established between computers. These authentication methods are offered and accepted when negotiating security with another computer.

Authentication method preference order:

Method	Details
Kerberos	

Press the **Edit** button to continue.

Edit **Authentication Method Properties** window appears. Select **Use this string (preshared key)** option and type in the preshared key in the field (the same one as in StarWind IPSec policy).



Edit Authentication Method Properties

Authentication Method

The authentication method specifies how trust is established between the computers.

○ Active Directory default (Kerberos V5 protocol)

○ Use a certificate from this certification authority (CA):

□ Exclude the CA name from the certificate request

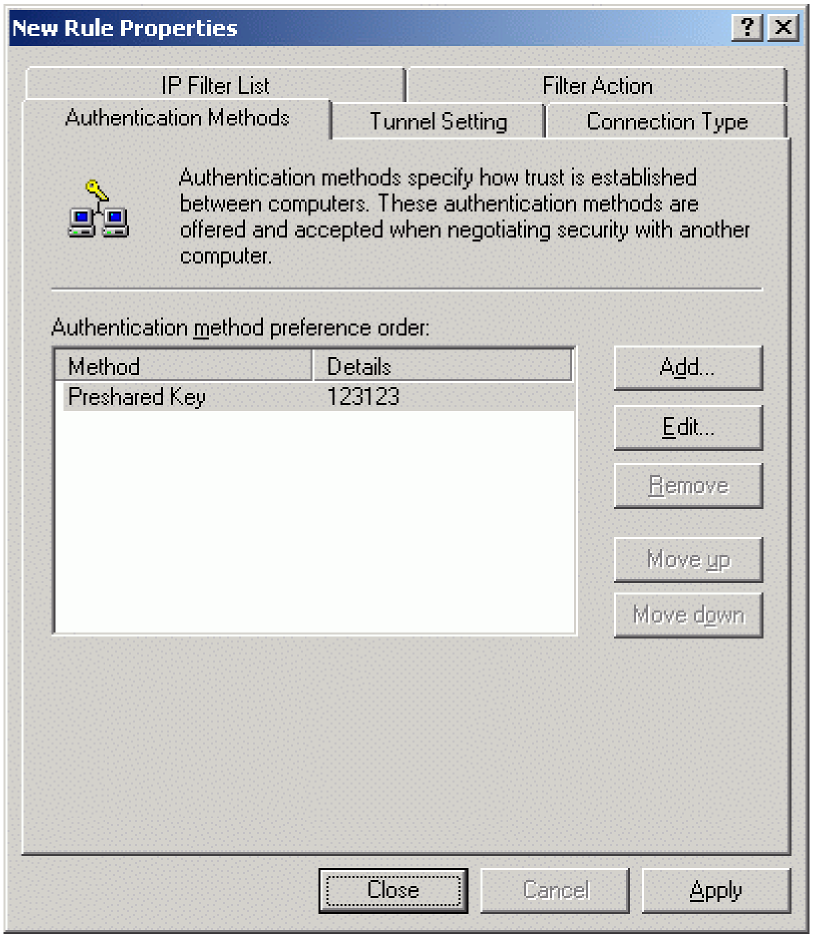
□ Enable certificate to account mapping

● Use this string (preshared key):

123123

Press the **OK** button to continue.

We return to the **Authentication Methods** tab.



New Rule Properties

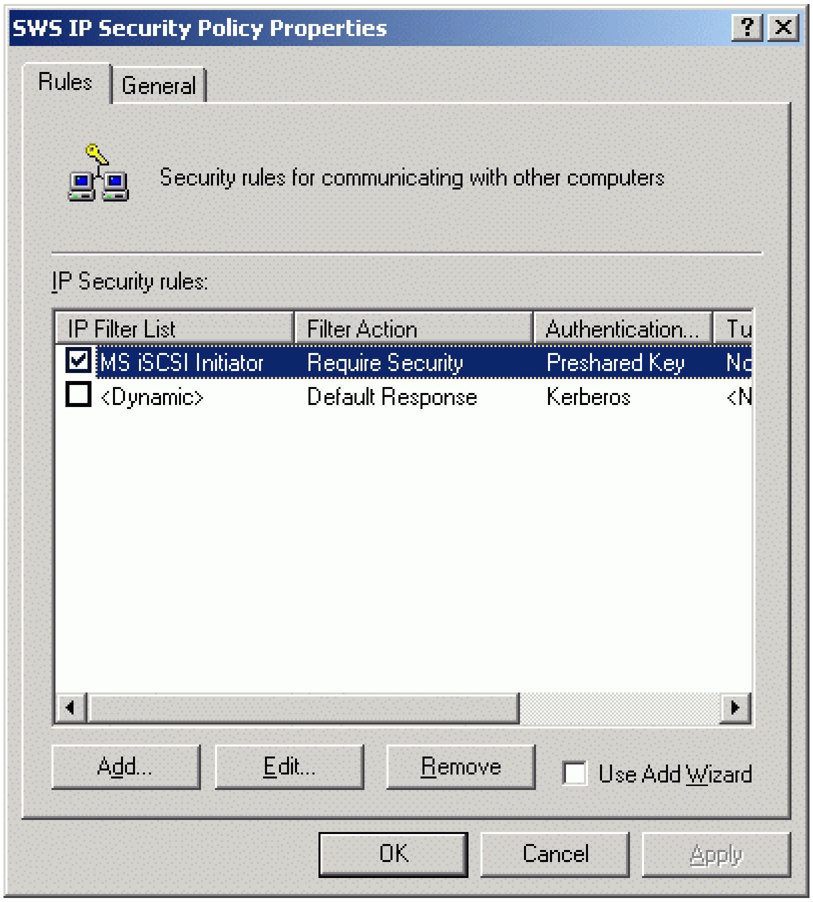
Authentication methods specify how trust is established between computers. These authentication methods are offered and accepted when negotiating security with another computer.

Authentication method preference order:

Method	Details
Preshared Key	123123

Press the **Close** button to continue.

Select **MS iSCSI Initiator** from the list of available **IP Security rules**.



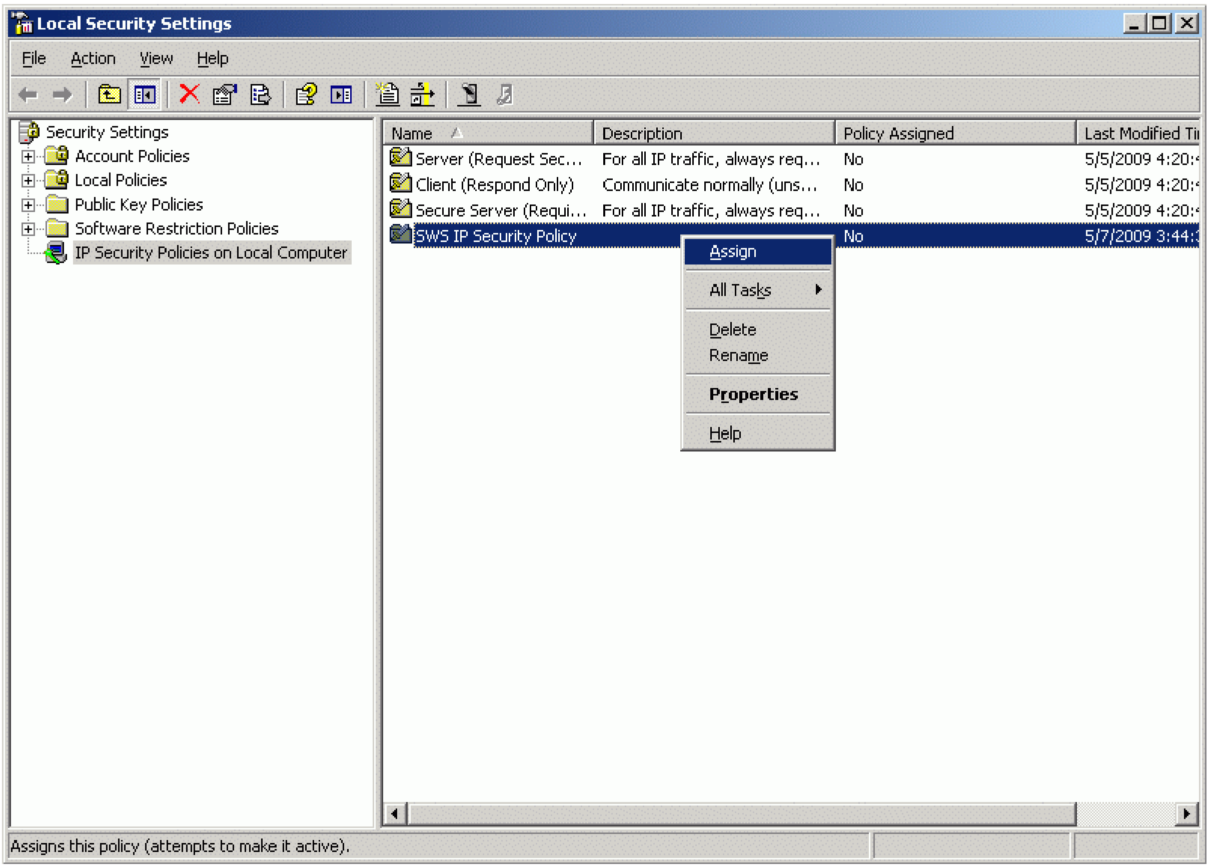
SWS IP Security Policy Properties
Rules
General
Security rules for communicating with other computers
IP Security rules:

IP Filter List	Filter Action	Authentication...	Tu
☑ MS iSCSI Initiator	Require Security	Preshared Key	Nc
□ <Dynamic>	Default Response	Kerberos	<N

Add...
Edit...
Remove
□ Use Add Wizard
OK
Cancel
Apply

Press the **OK** button.

Assign recently created policy by pressing right mouse button and selecting **Assign** option.

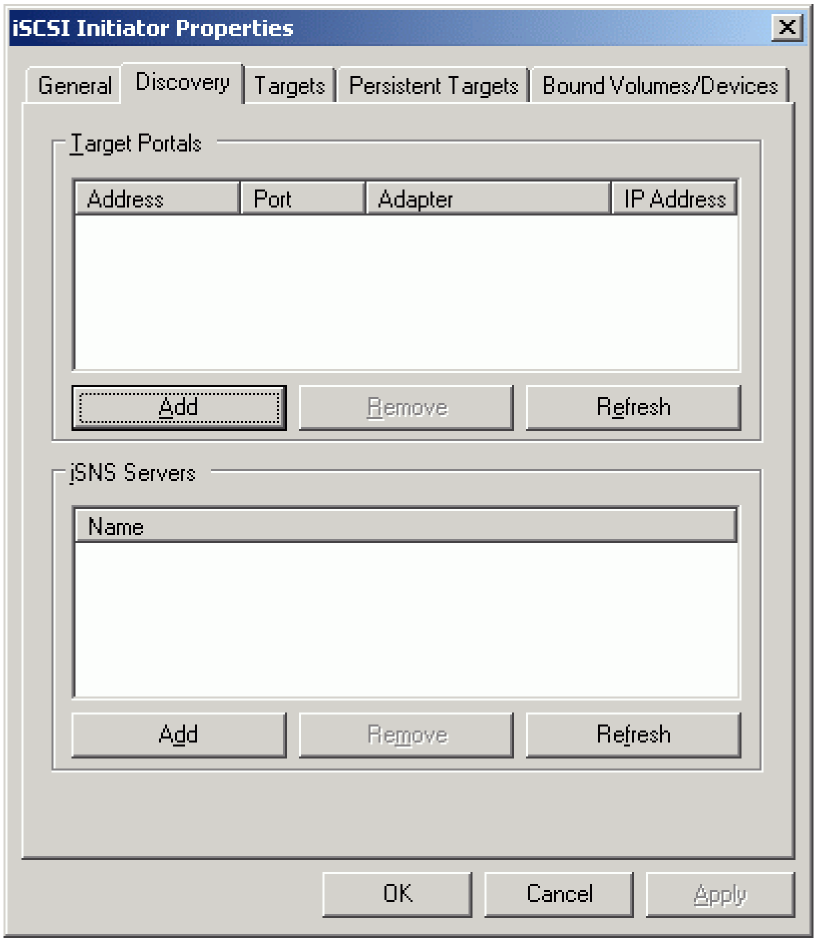


Name	Description	Policy Assigned	Last Modified Ti
Server (Request Sec...	For all IP traffic, always req...	No	5/5/2009 4:20:
Client (Respond Only)	Communicate normally (uns...	No	5/5/2009 4:20:
Secure Server (Requi...	For all IP traffic, always req...	No	5/5/2009 4:20:
SWS IP Security Policy		No	5/7/2009 3:44:

Assigns this policy (attempts to make it active).

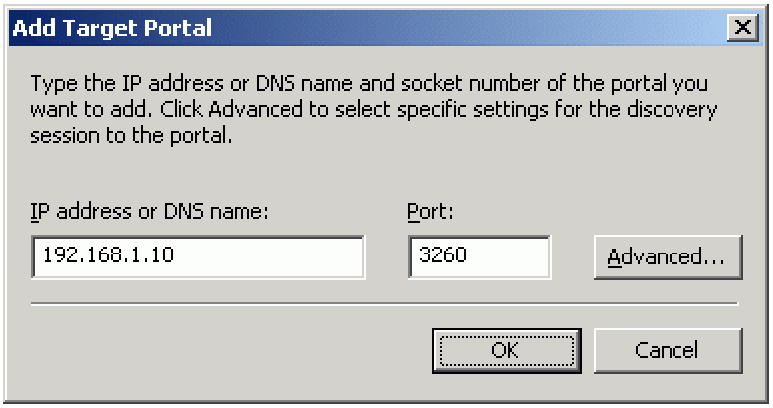
Connecting to the Target Using MS iSCSI Initiator

Launch the **MS iSCSI Initiator** by selecting **Start -> All Programs -> Microsoft iSCSI Initiator -> Microsoft iSCSI Initiator**. Switch to the **Discovery** tab. Here you can specify the computer with the **StarWind** installed or **iSNS** server.



Press the **Add** button to continue.

In the appearing dialog type in the **IP address** of the computer with **StarWind** installed and port of that machine



Add Target Portal

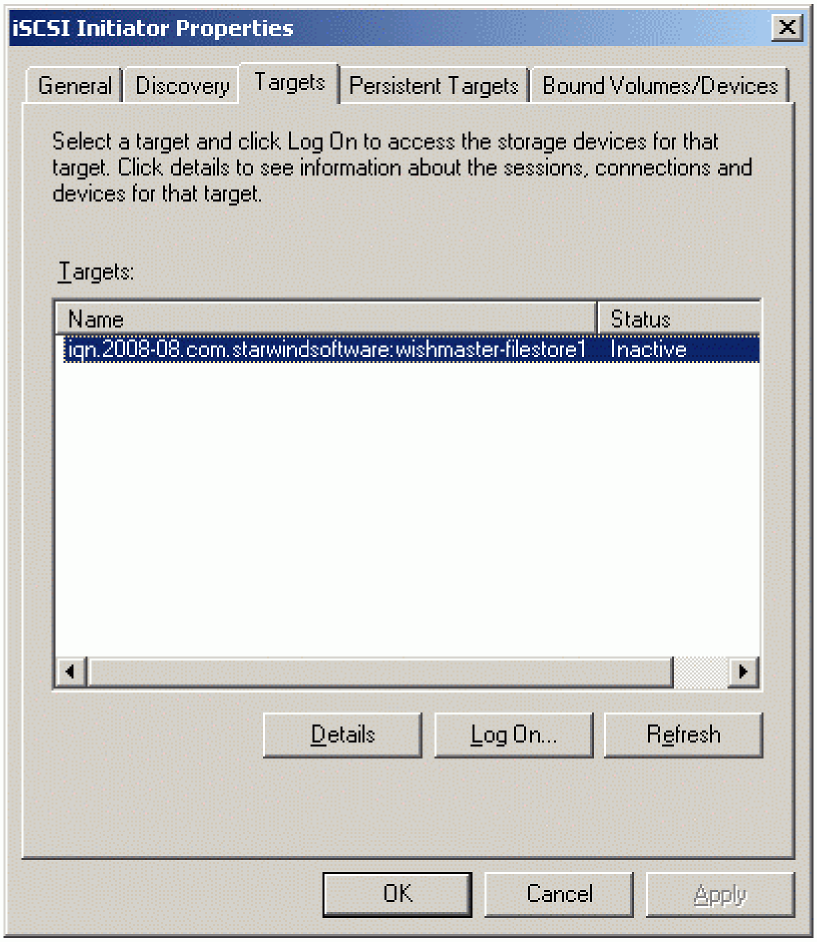
Type the IP address or DNS name and socket number of the portal you want to add. Click Advanced to select specific settings for the discovery session to the portal.

IP address or DNS name: 192.168.1.10

Port: 3260

Press the **OK** button to continue.

Switch to the **Targets** tab.



iSCSI Initiator Properties

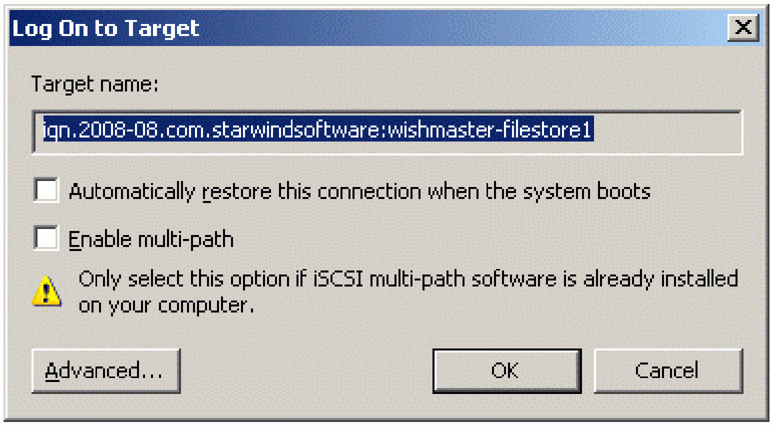
Select a target and click Log On to access the storage devices for that target. Click details to see information about the sessions, connections and devices for that target.

Targets:

Name	Status
iqn.2008-08.com.starwindsoftware:wishmaster-filestore1	Inactive

Select the device you have recently shared and press **Log On** to continue.

Log On to Target dialog appears.



Log On to Target

Target name:

iqn.2008-08.com.starwindsoftware:wishmaster-filestore1

□ Automatically restore this connection when the system boots

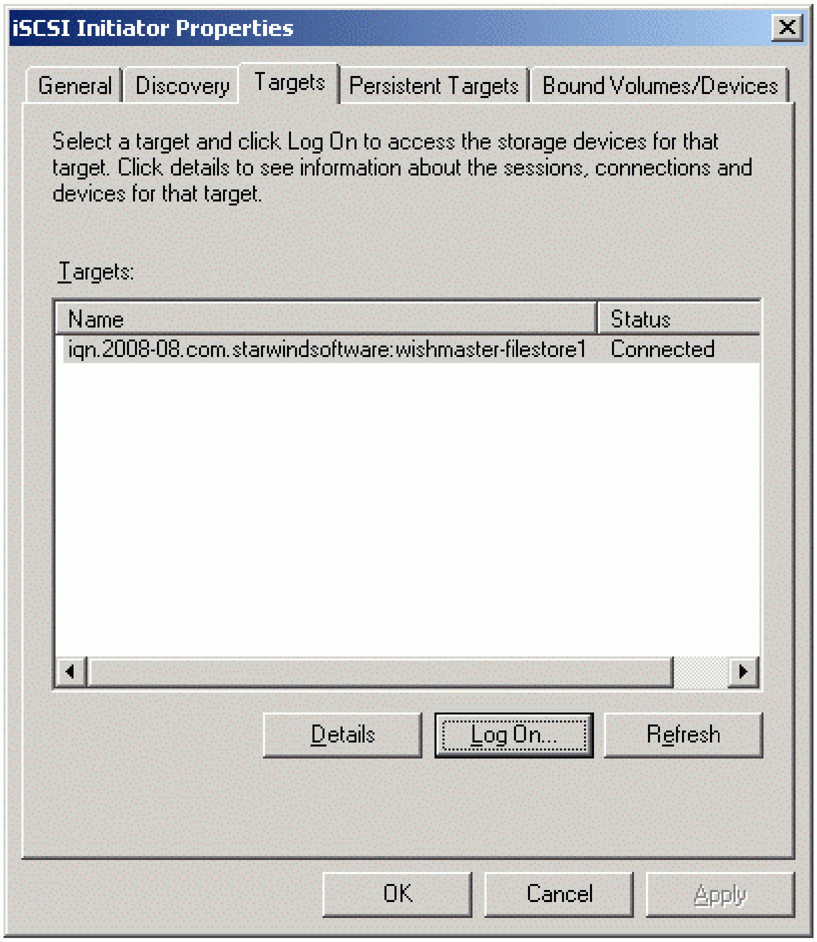
□ Enable multi-path

Only select this option if iSCSI multi-path software is already installed on your computer.

Check any additional parameters of the target you wish to connect. For example **Automatically restore this connection when the system boots** checkbox.

Press the **OK** button to logon to the **StarWind**.

The information about the connection status is displayed on the **Targets** tab (see the image below). If the logon is successful the new iSCSI device will appear in the system after a few seconds.



Select a target and click Log On to access the storage devices for that target. Click details to see information about the sessions, connections and devices for that target.

Targets:

Name	Status
iqn.2008-08.com.starwindsoftware:wishmaster-filestore1	Connected

Press the **OK** button to exit initiator management console.

Conclusion

Contacts

Support:	www.starwindsoftware.com/support
Support Forum:	www.starwindsoftware.com/forums
Sales E-mail:	sales@starwindsoftware.com
US Headquarters	
Phone:	617-449-7717
Fax:	617-505-5845
EMEA:	1-888-532-2203

StarWind Software Inc.
40 Mall Rd., Burlington
MA 01803, USA
www.starwindsoftware.com