

StarWind iSCSI SAN Software: IP Security Policy Configuration

www.starwindsoftware.com

Copyright © StarWind Software 2008-2011. All rights reserved.

COPYRIGHT

Copyright © StarWind Software 2008-2011. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior written consent of StarWind Software.

TRADEMARKS

“StarWind”, “StarWind Software” and the StarWind and the StarWind Software logos are trademarks of StarWind Software which may be registered in some jurisdictions. All other trademarks are owned by their respective owners.

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.

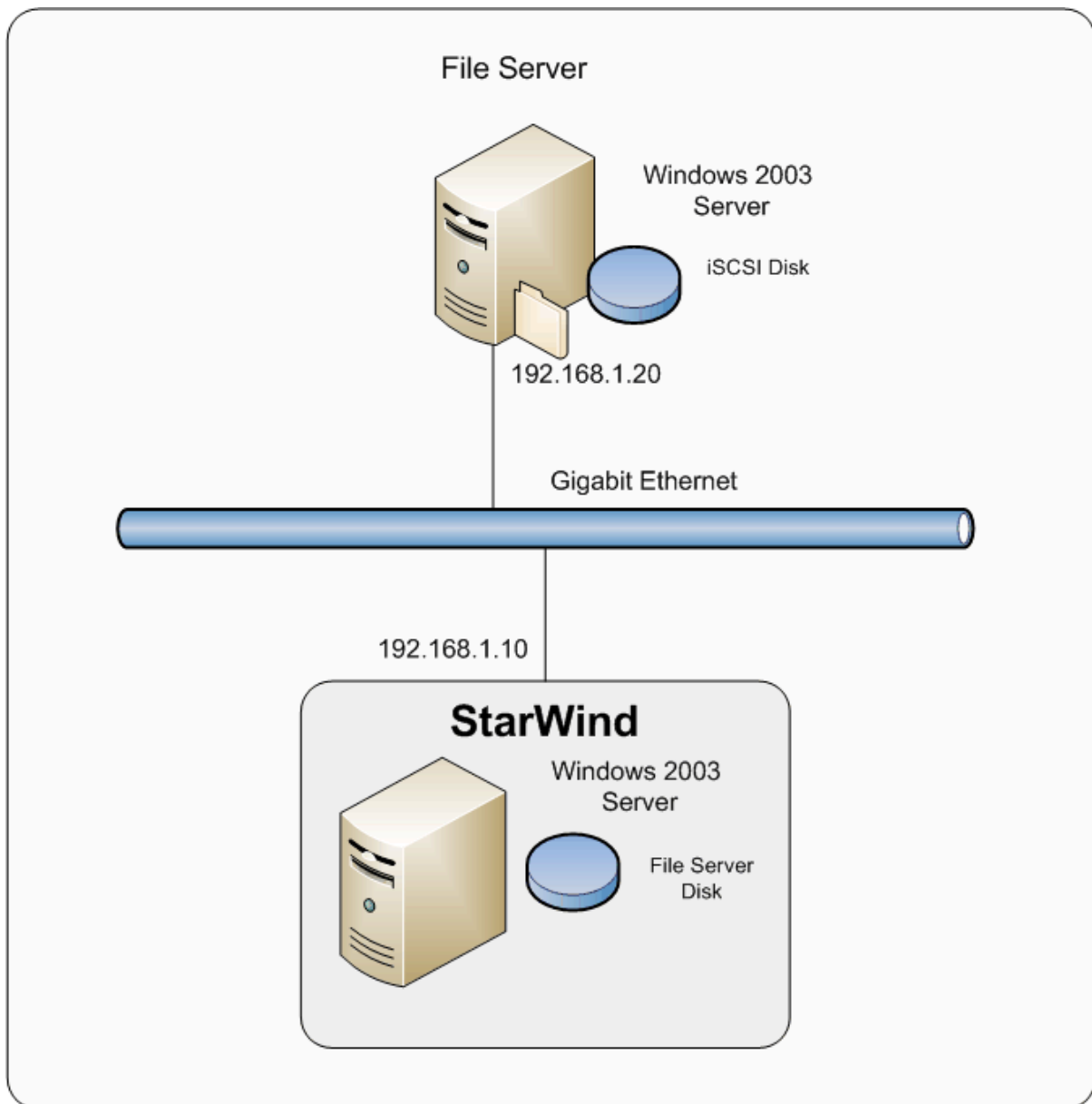
Table of Contents

Introduction.....	4
Configuring iSCSI Storage	5
Server-Side Configuration, Creating New Ip Security Policy	12
Client-Side Configuration, Creatng New Ip Security Policy	36
Connecting to the Target Using MS iSCSI Initiator	57

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.

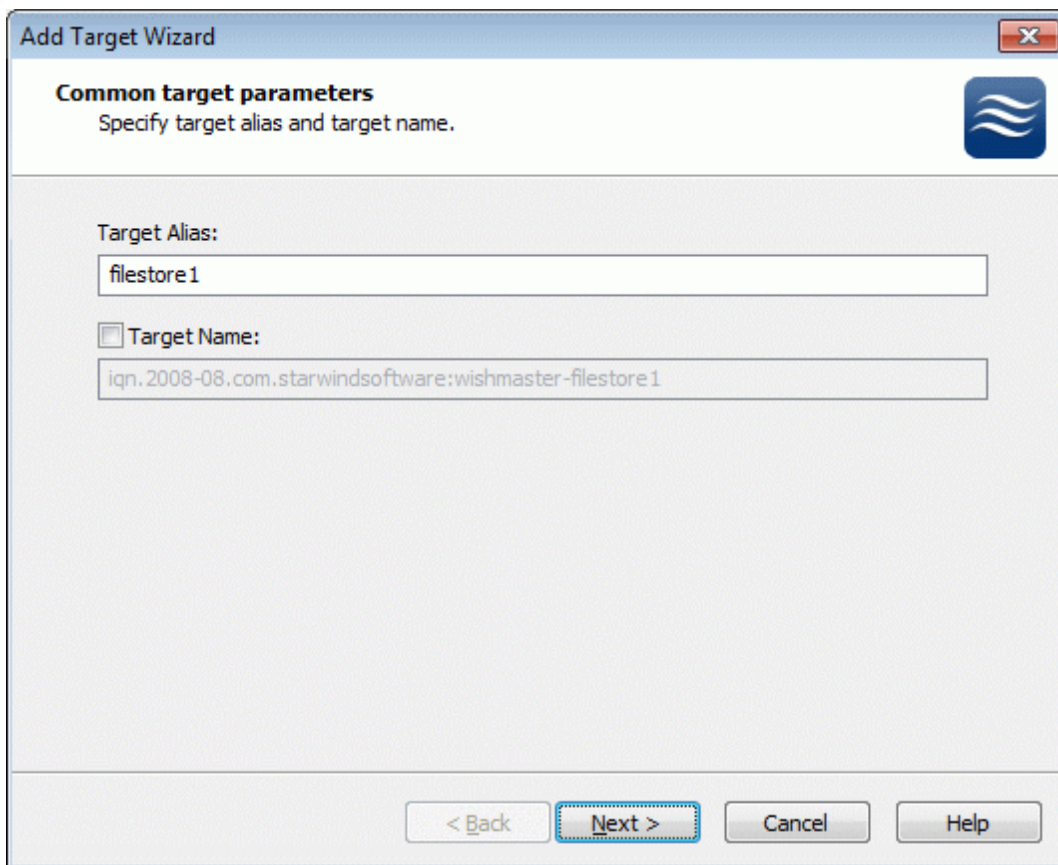


Configuring iSCSI Storage

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.

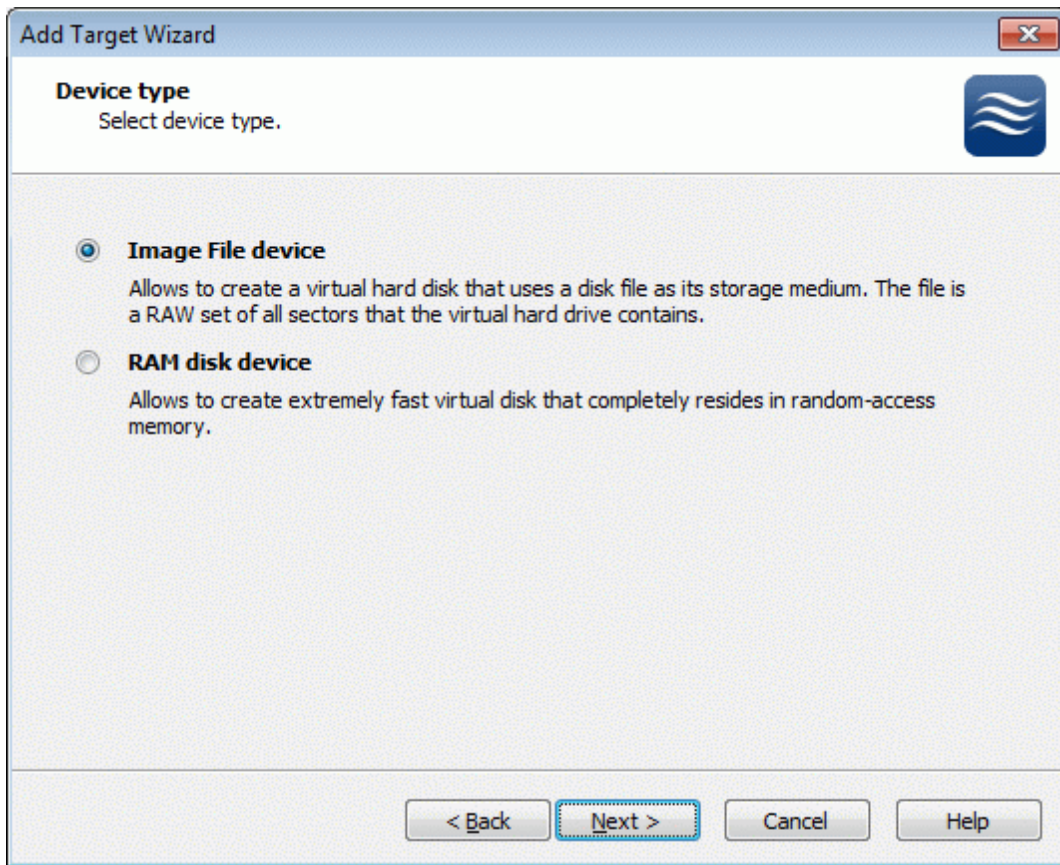
After you have successfully connected to the **StarWind** service press the **Add Target** button to continue.

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.



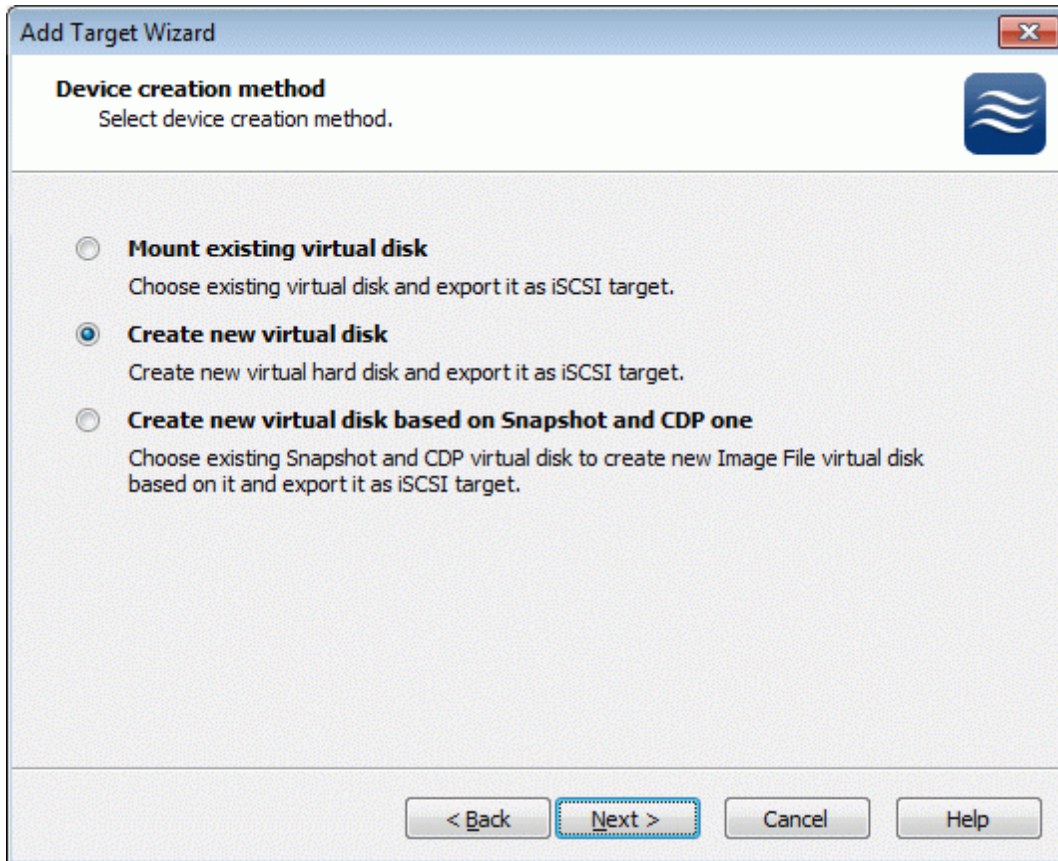
Press the **Next** button to continue.

Select **Image File device**.



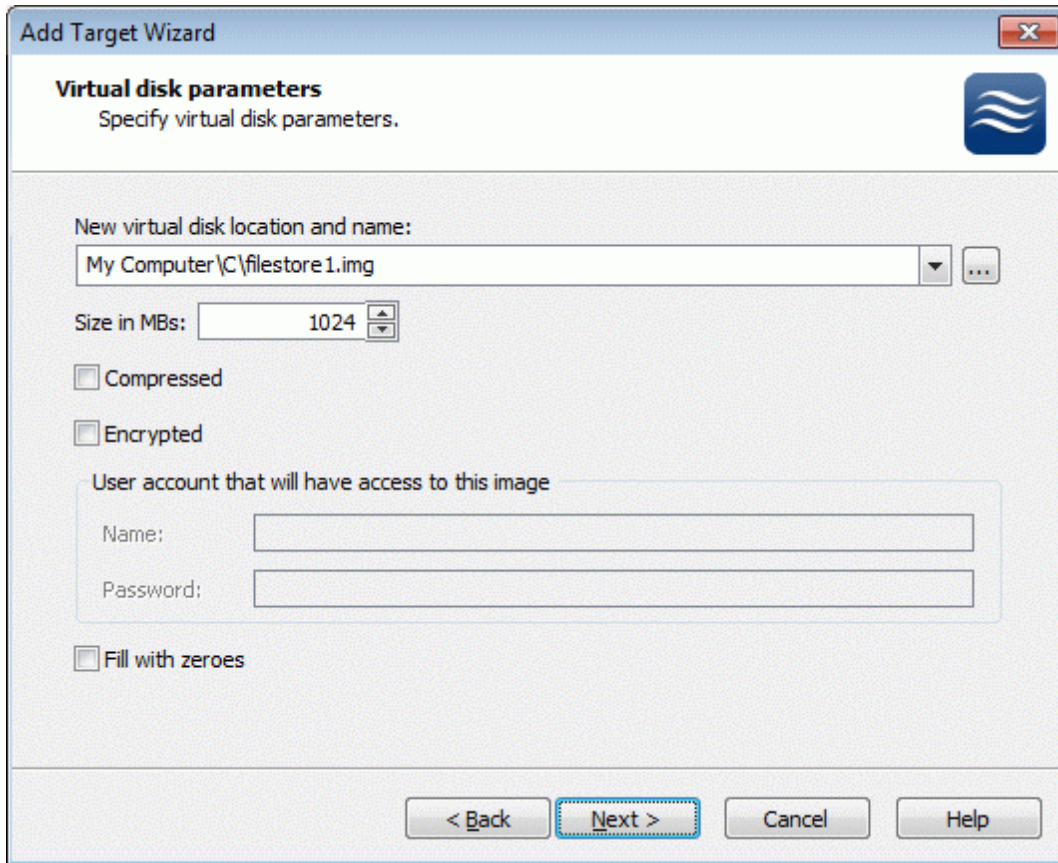
Press the **Next** button to continue.

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.



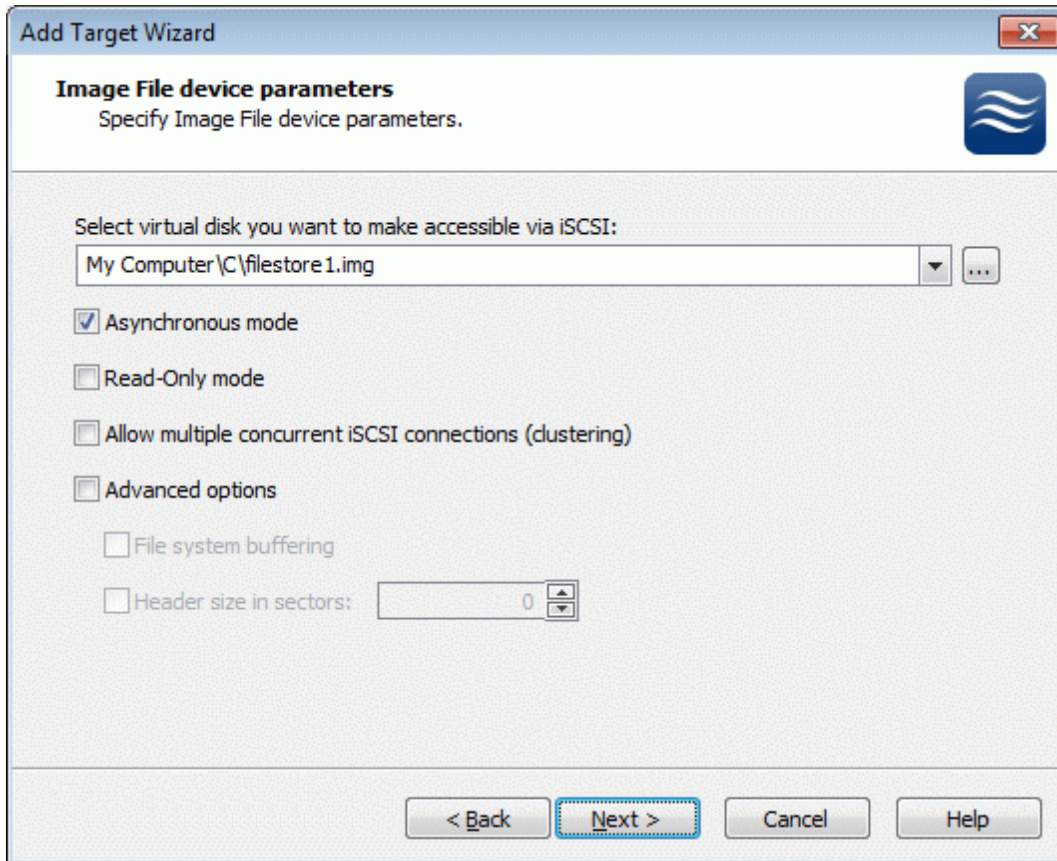
Press the **Next** button to continue.

If you have decided to create a new virtual disk, specify the location and the name of the virtual disk 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**).



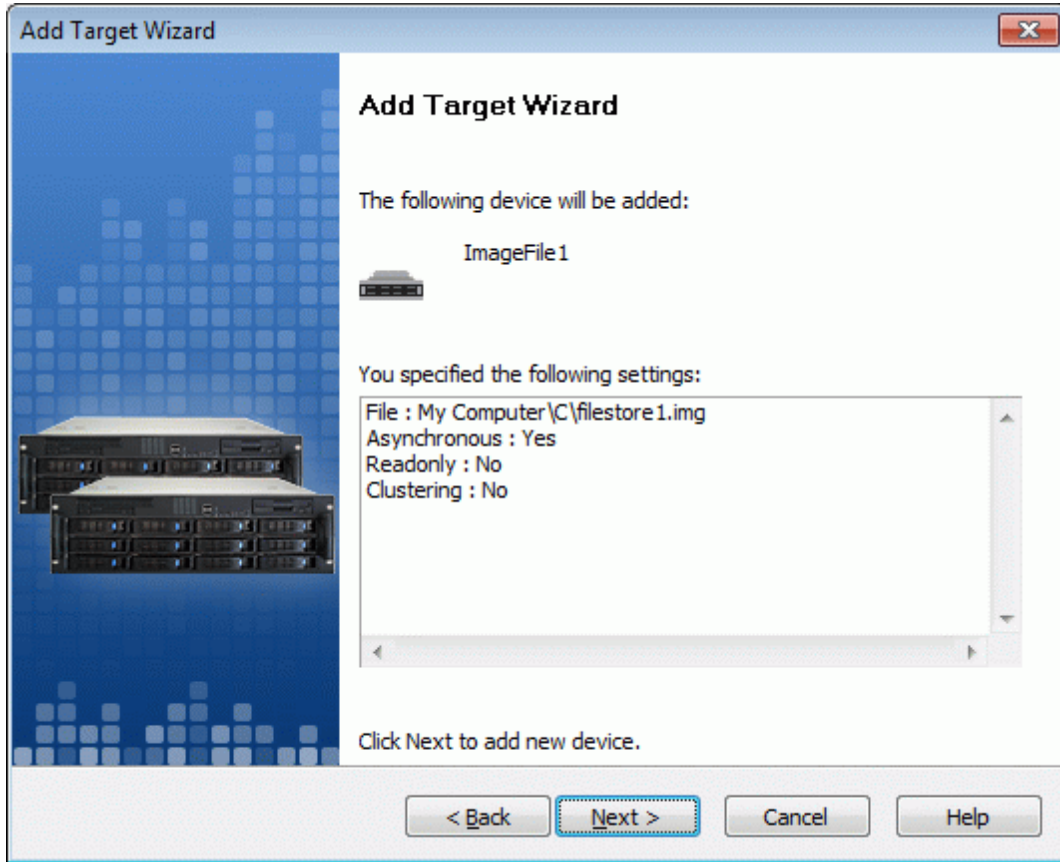
Press the **Next** button to continue.

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**).



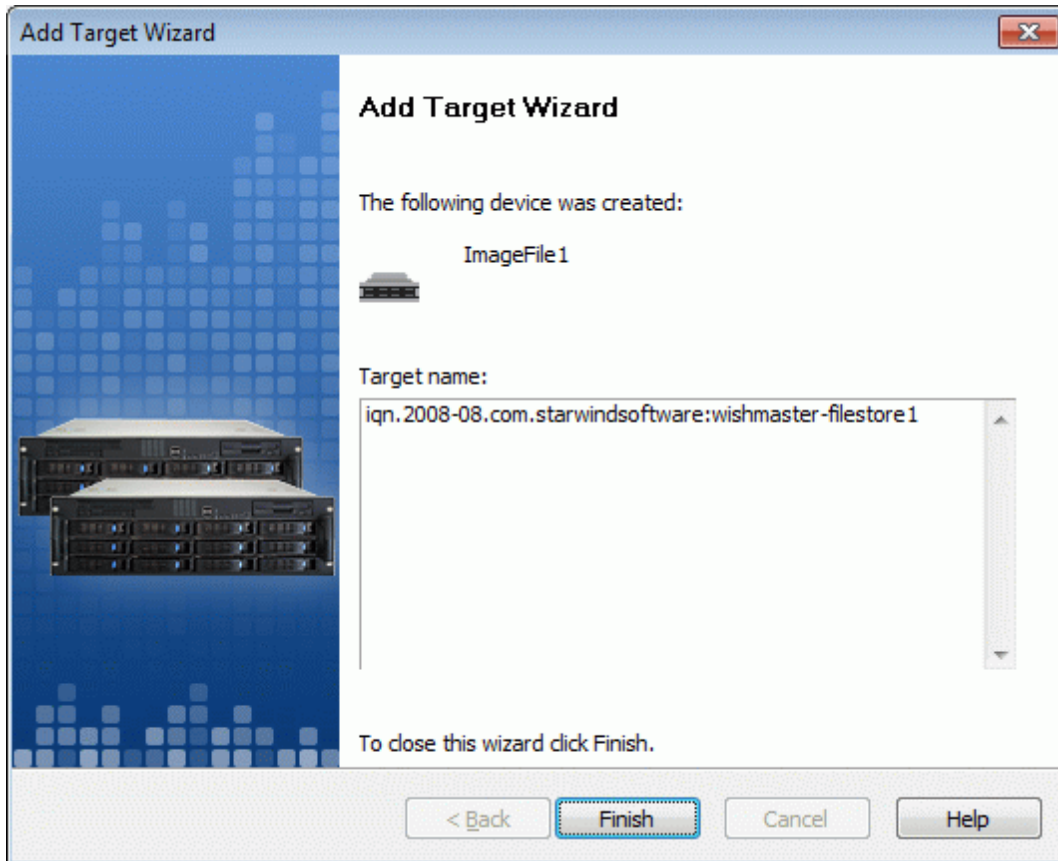
Press the **Next** button to continue.

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



Press the **Next** button to continue.

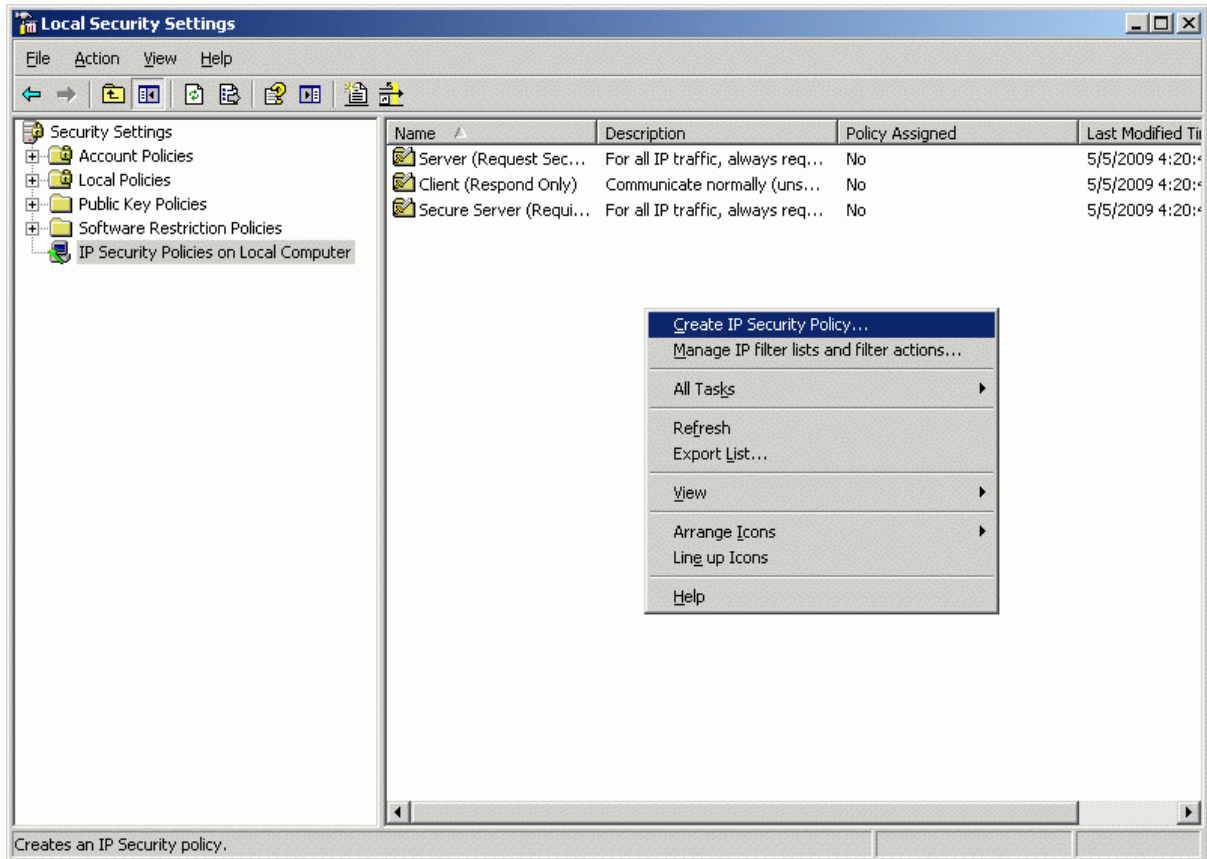
The information about the recently created device is displayed on the last wizard page (see image below).



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.



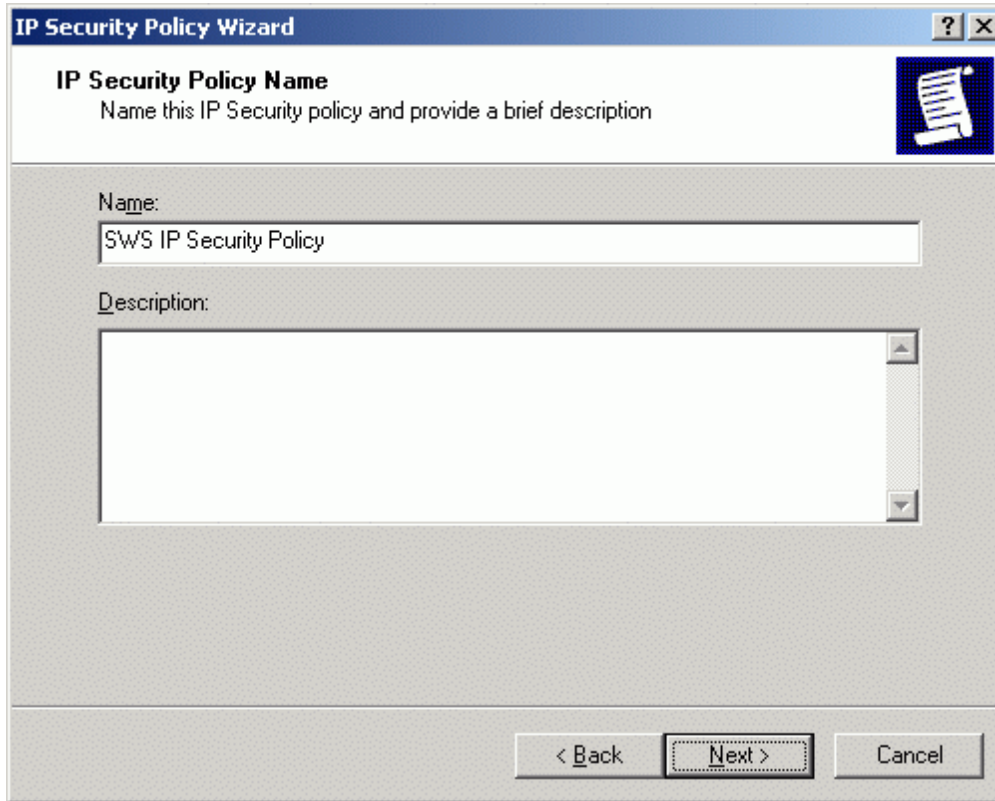
Click the right mouse button and select **Create IP Security Policy** option.

IP Security Policy Wizard appears.



Press the **Next** button to continue.

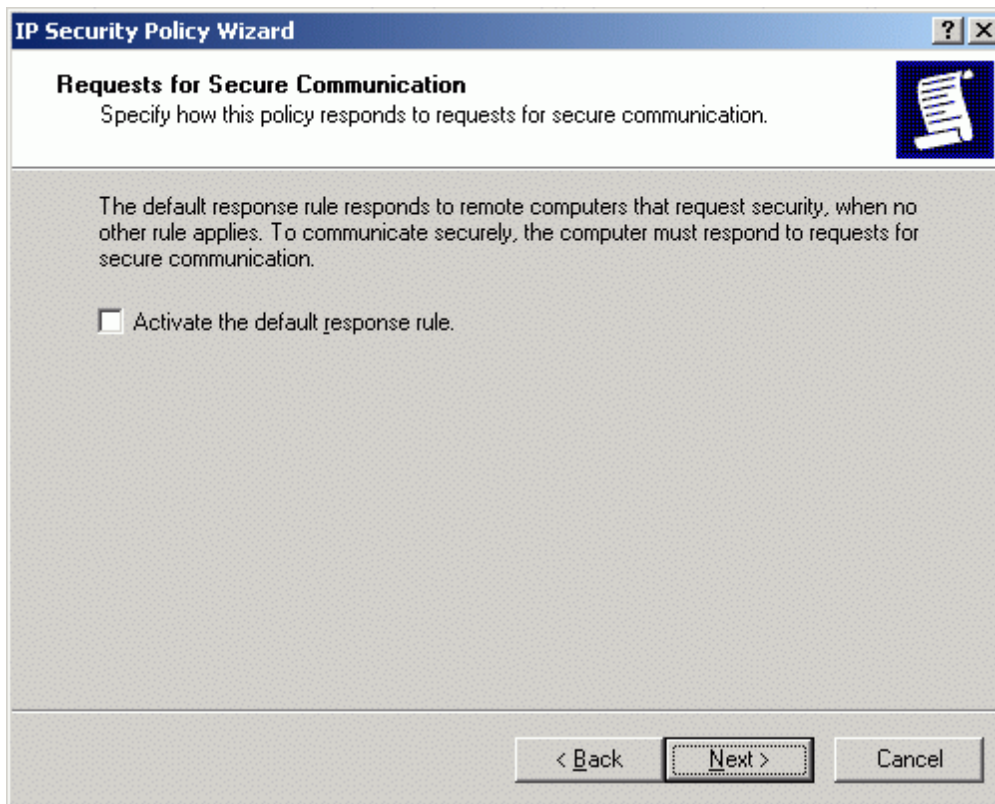
Specify the **Name** of the new **IP Security Policy** and optionally provide a brief description of it.



The image shows a Windows-style dialog box titled "IP Security Policy Wizard". The dialog has a title bar with a question mark and a close button. The main content area is divided into two sections. The first section is titled "IP Security Policy Name" and contains the instruction "Name this IP Security policy and provide a brief description" next to a document icon. Below this is a text input field labeled "Name:" containing the text "SWS IP Security Policy". The second section is labeled "Description:" and contains a large, empty text area with a vertical scrollbar. At the bottom of the dialog, there are three buttons: "< Back", "Next >" (which is highlighted with a dashed border), and "Cancel".

Press the **Next** button to continue.

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



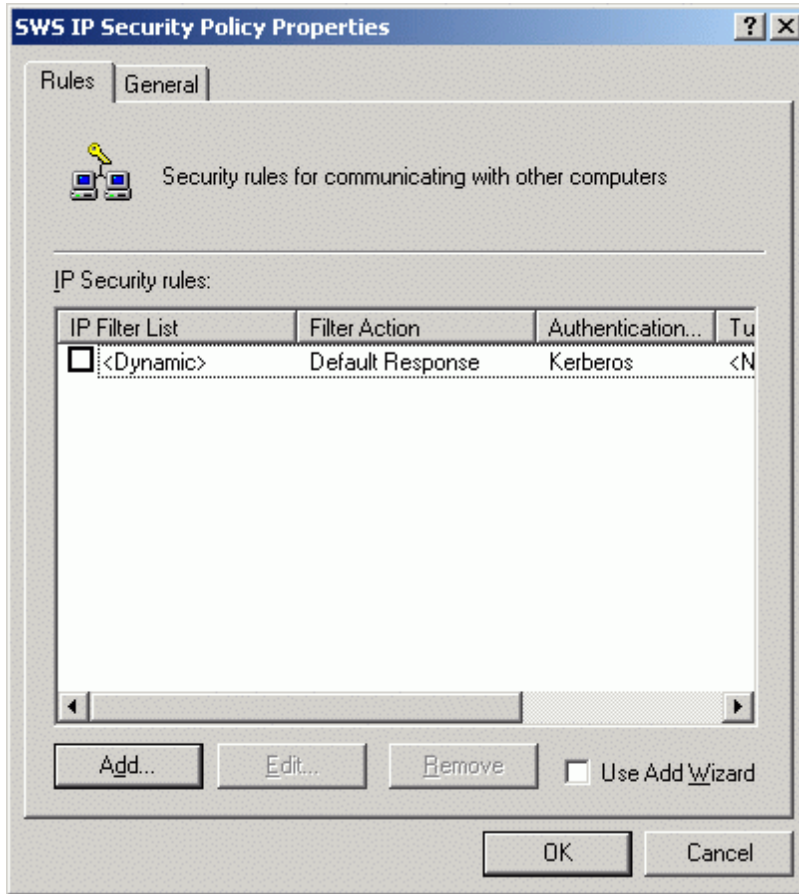
Press the **Next** button to continue.

Set the **Edit properties** option.



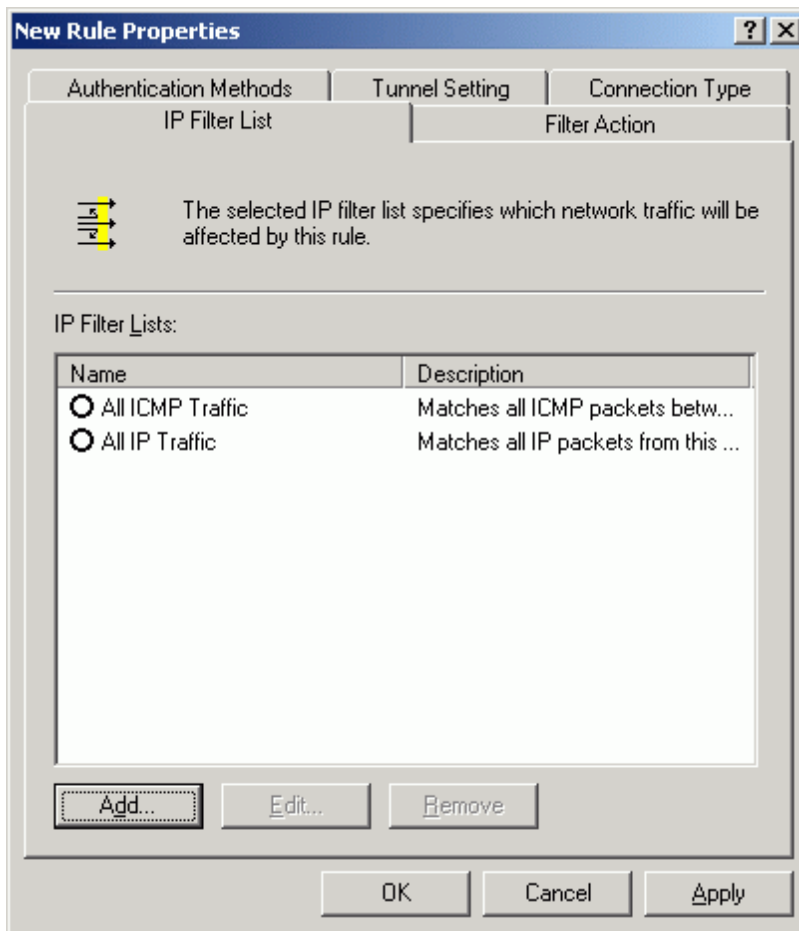
Press the **Finish** button.

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



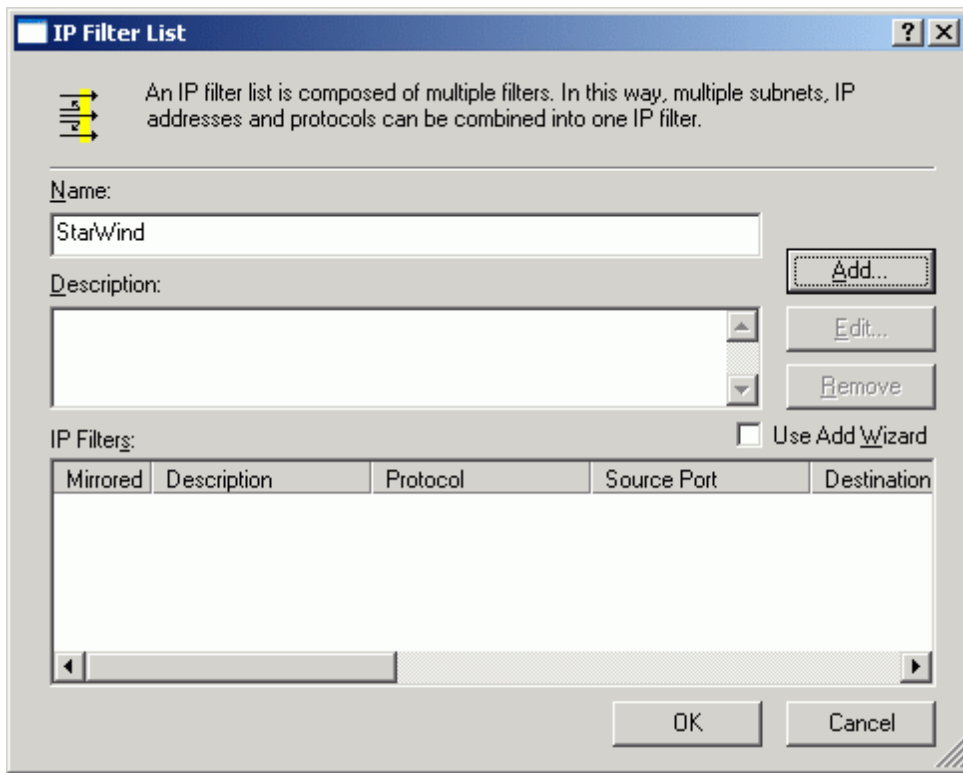
Press the **Add** button on the Rules tab.

New Rules Properties window appears.



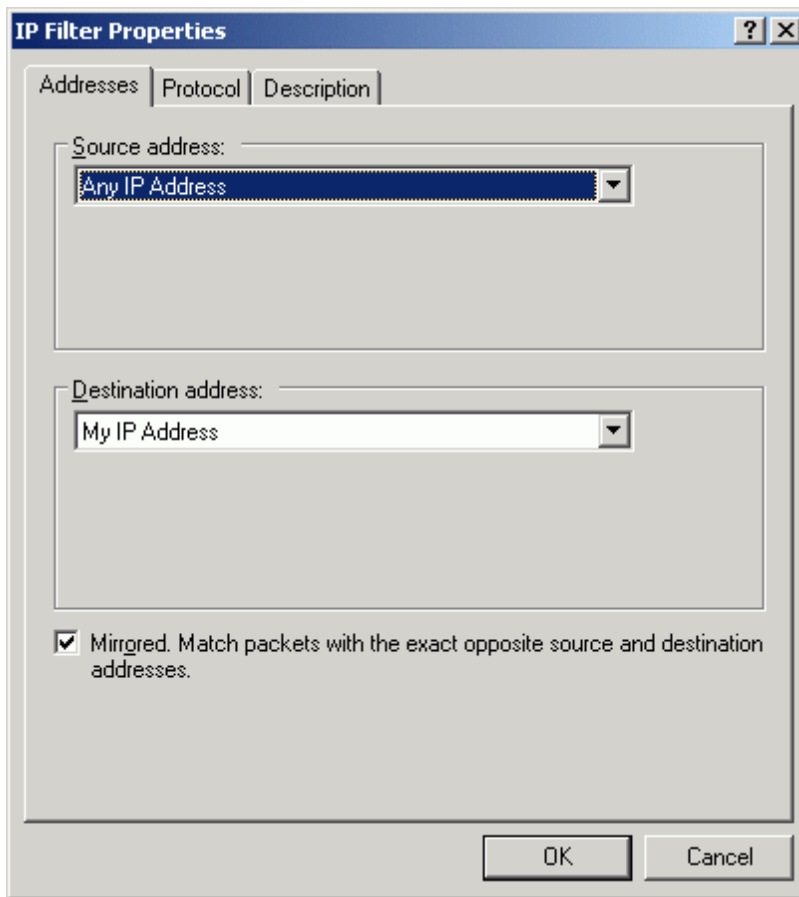
Press the **Add** button on the **IP Filter List** tab.

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



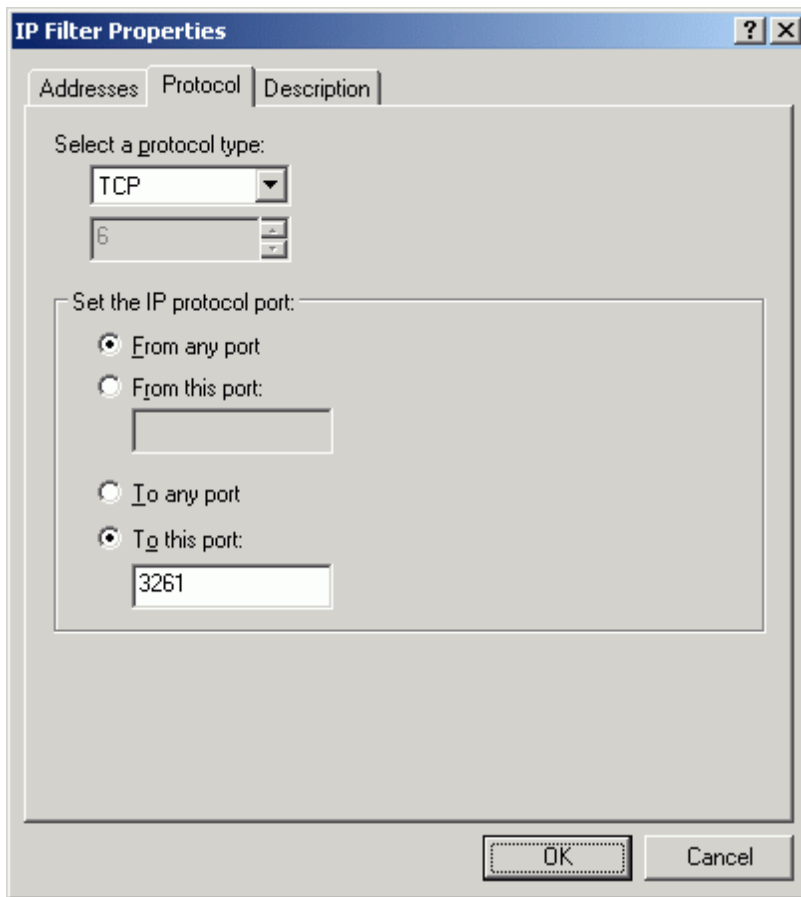
Specify the **Name** of IP Filter and optionally a brief description and press **Add** button.

Filter Properties window appears.



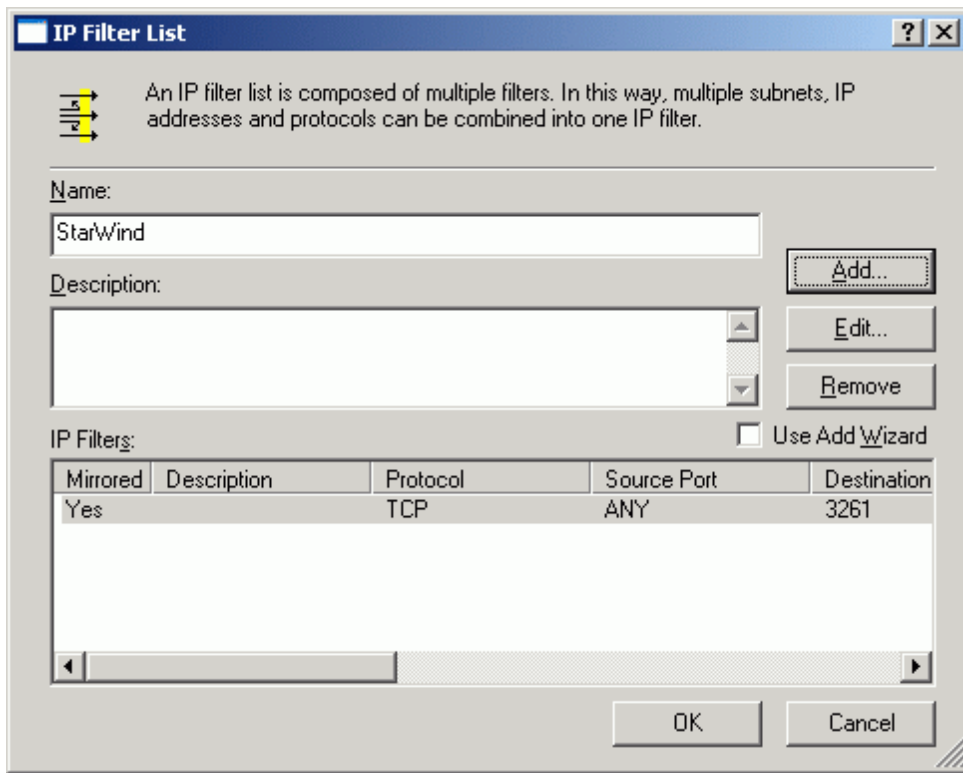
Specify **Source address** and **Destination address**. To delimit allow connections more strictly in the **Source address** field you can specify IP address of the separate host or subnet.

Switch to the **Protocol** tab.



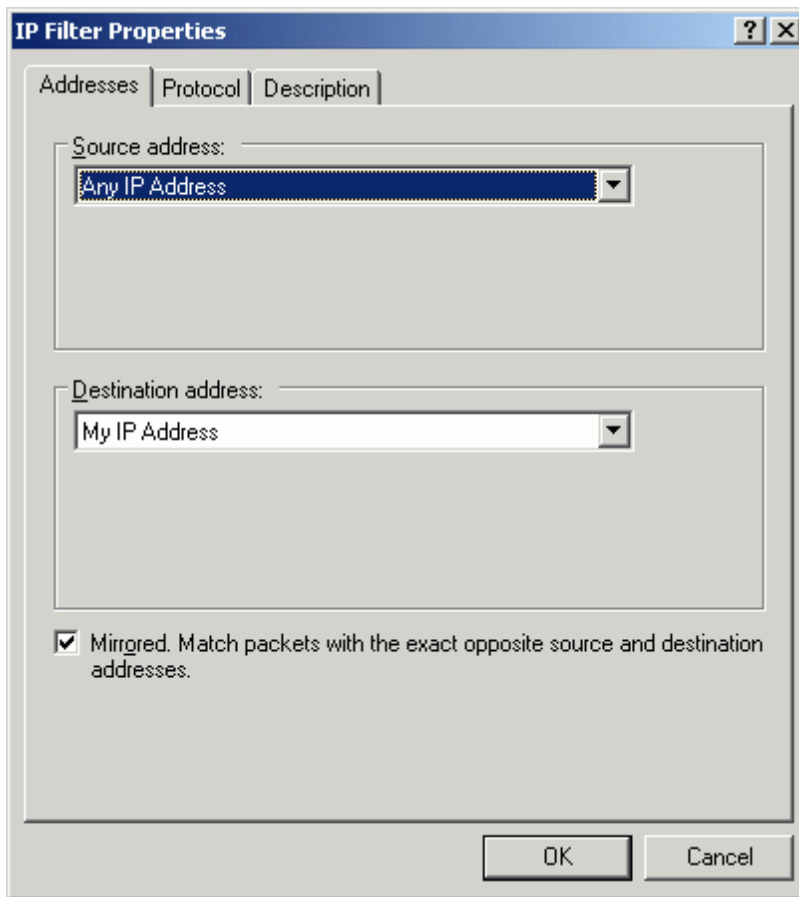
Specify protocol (**TCP** in our case) and port number (**3261**) and press **OK**. This filter is for **StarWind** management console connections.

New rule appears in the list.



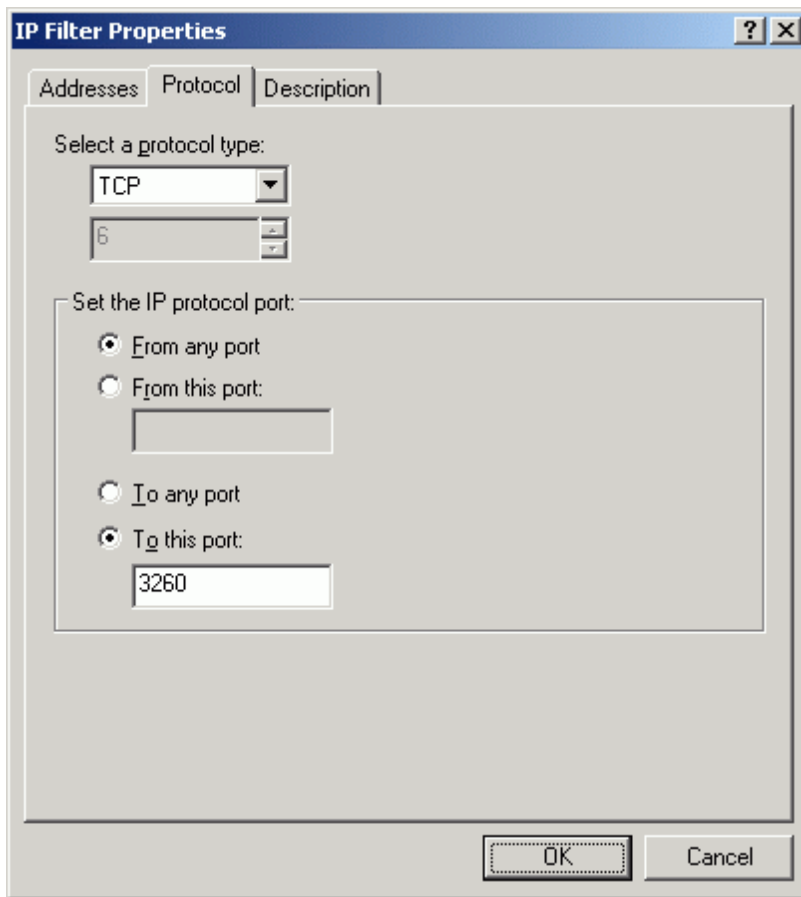
Click the **Add** button again.

Filter Properties window appears.



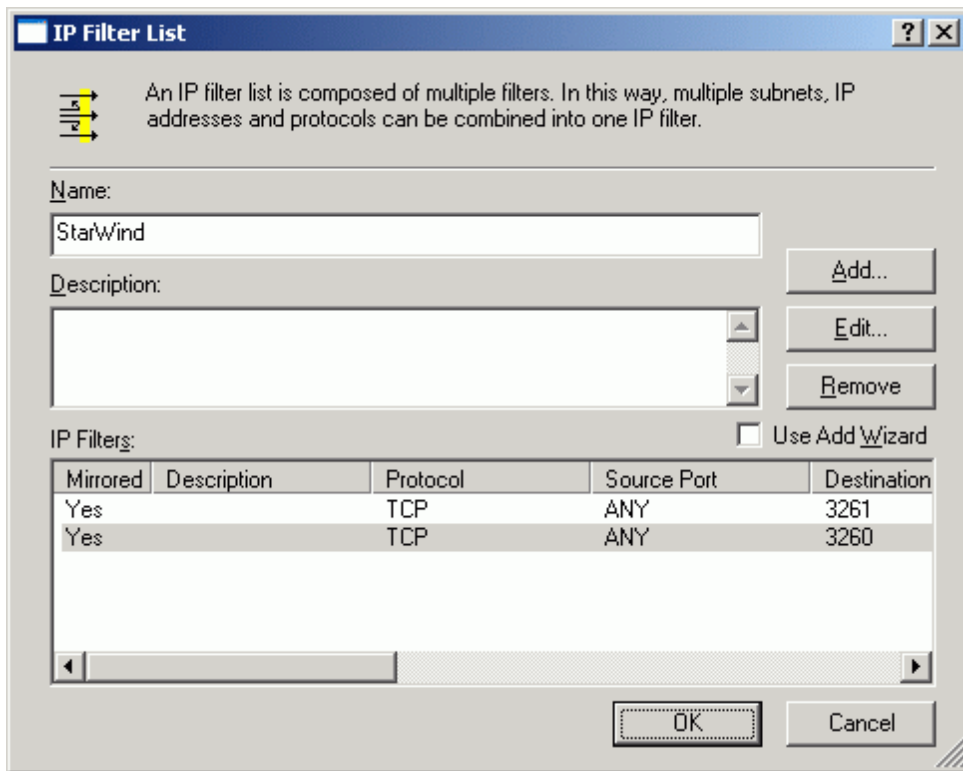
Specify **Source address** and **Destination address**.

Switch to the **Protocol** tab.



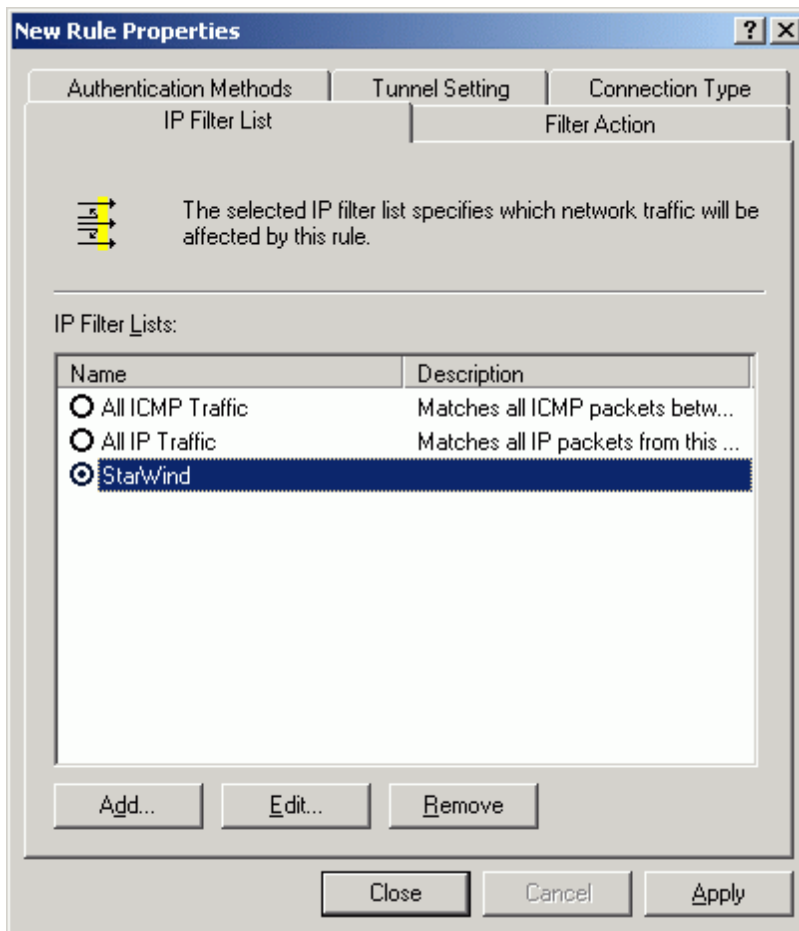
Specify protocol (**TCP** in our case) and port number (**3260**) and press **OK**. This filter is for **StarWind** service connections (iSCSI traffic itself).

One more new rule appears in the list.



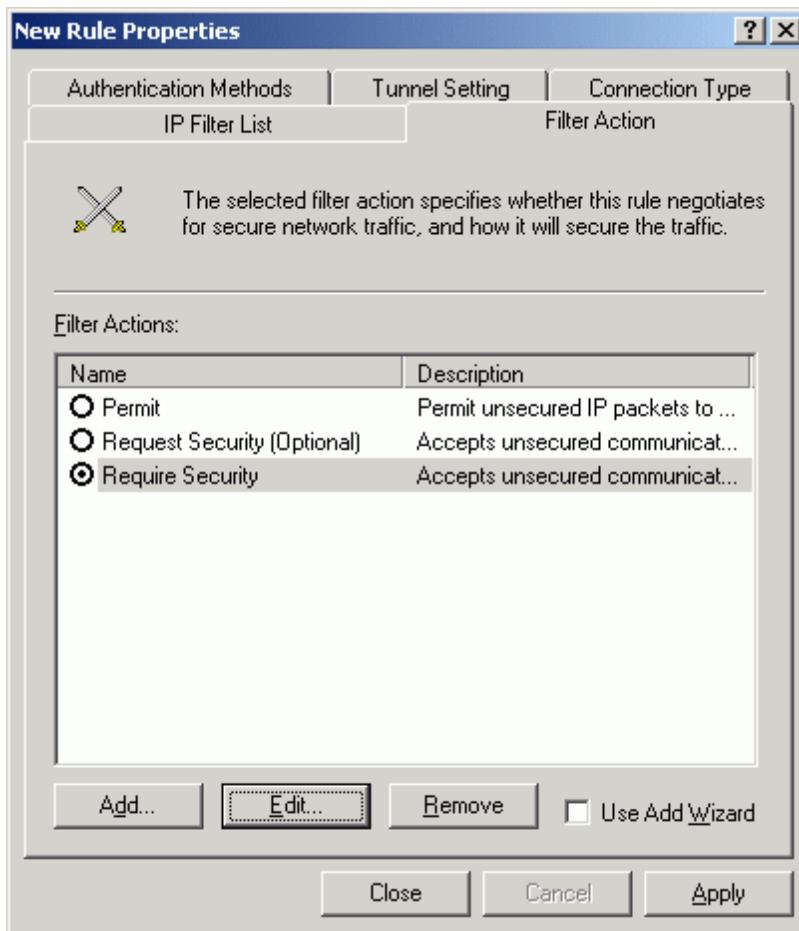
Press the **OK** button to continue.

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



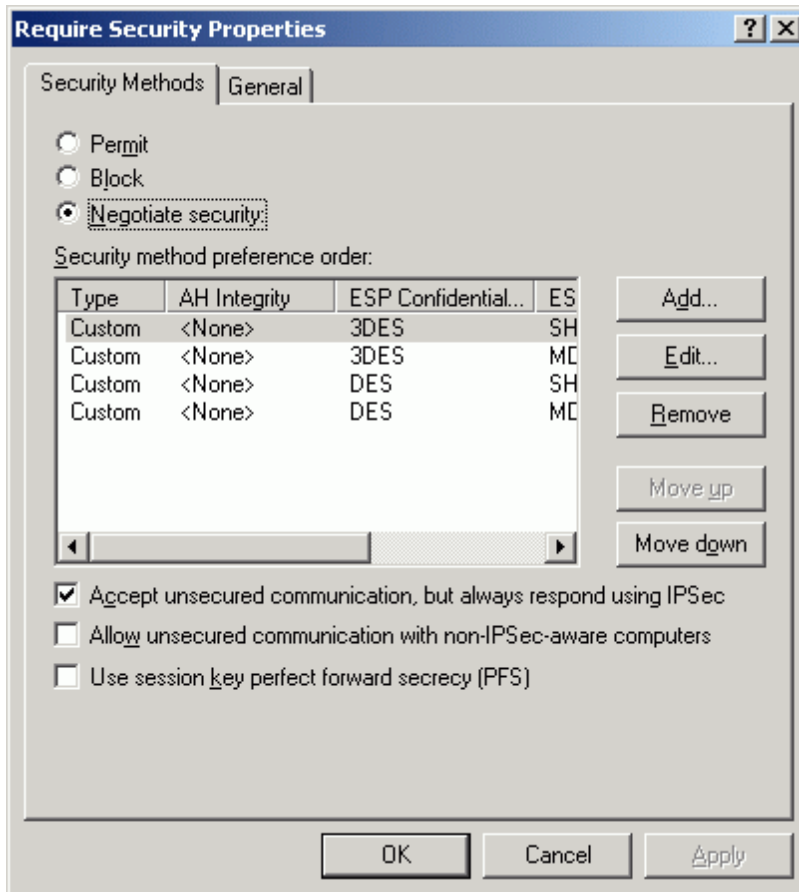
Select newly created filter **StarWind** from the list and switch to the **Filter Action** tab.

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



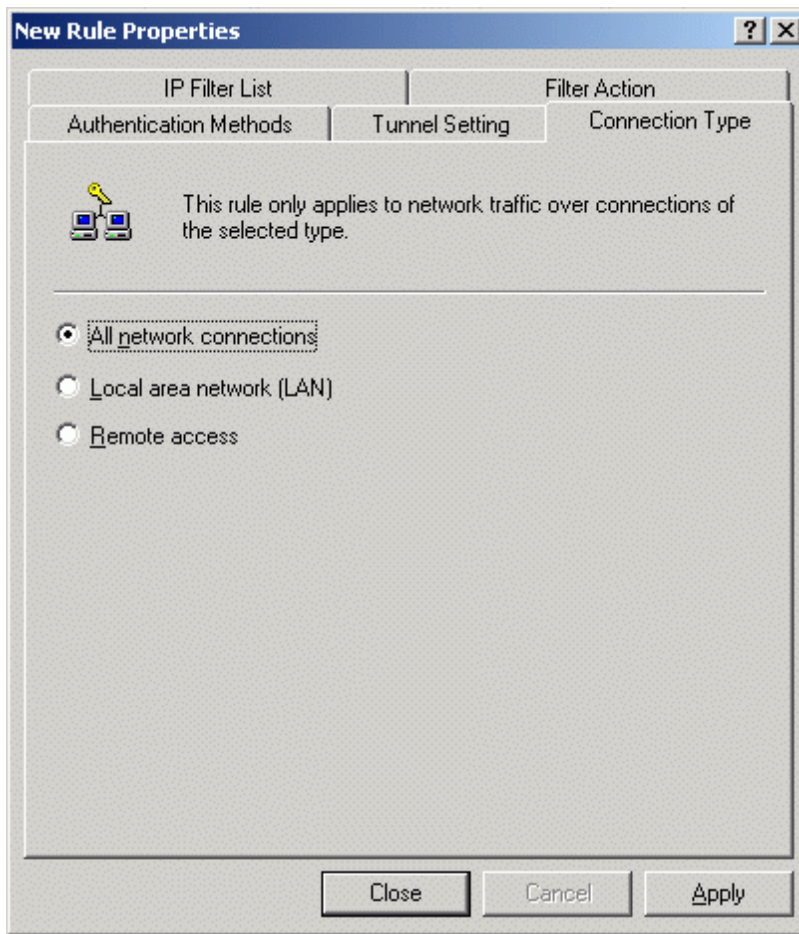
Press the **Edit** button to continue.

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



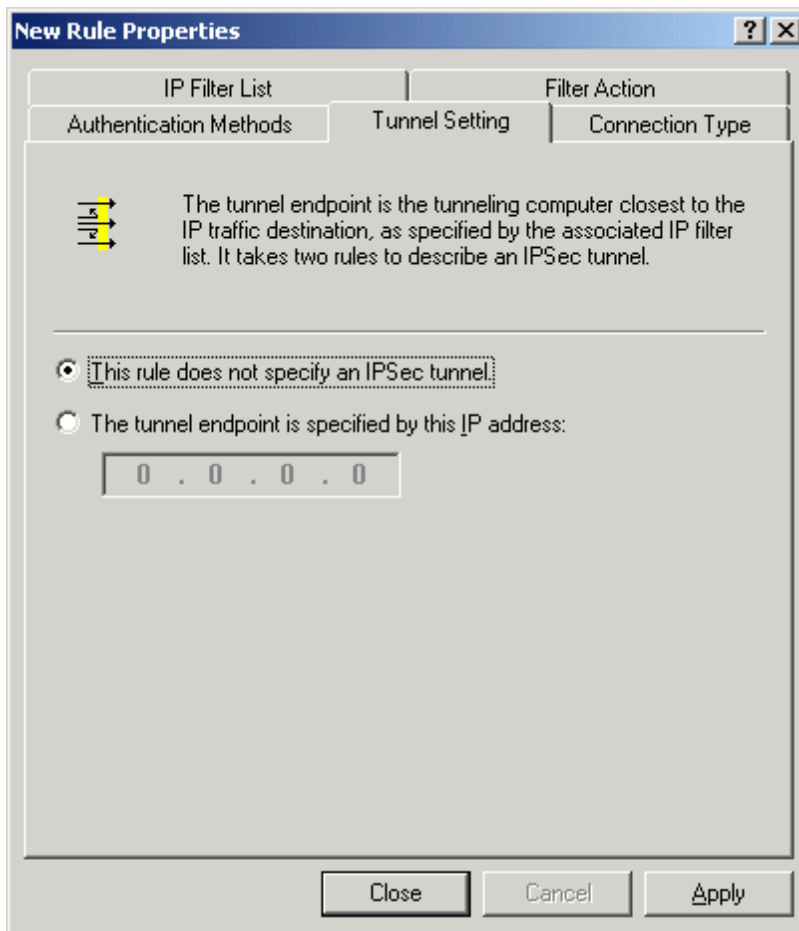
Press the **OK** button to continue.

Switch to the **Connection Type** tab.



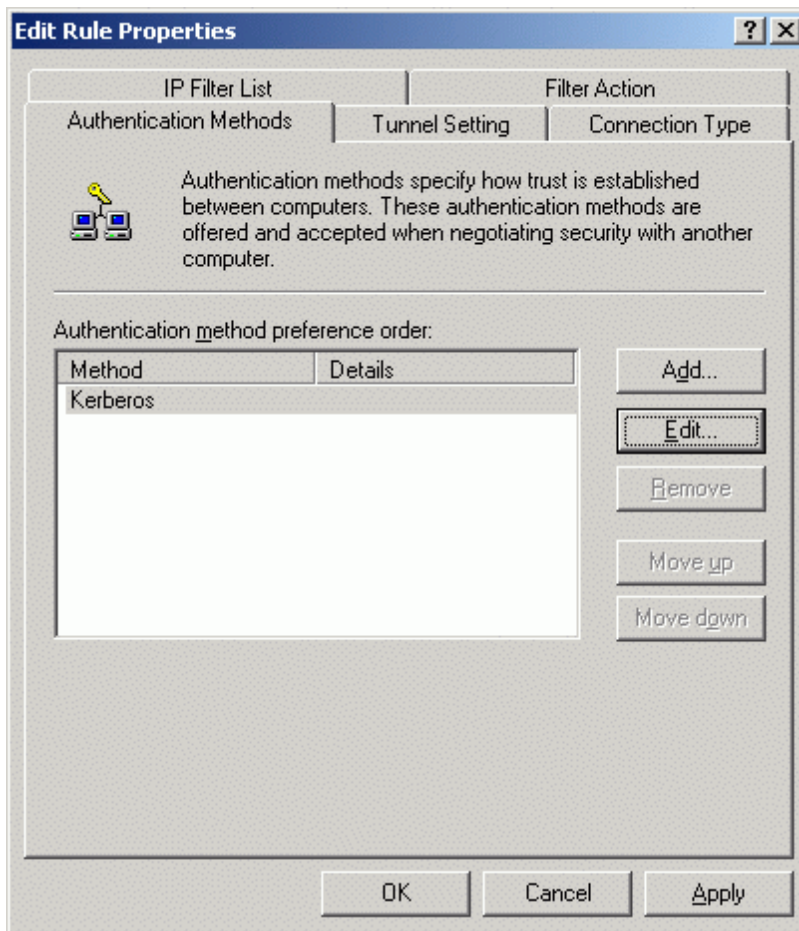
Select **All network connections**.

Switch to the **Tunnel Setting** tab.



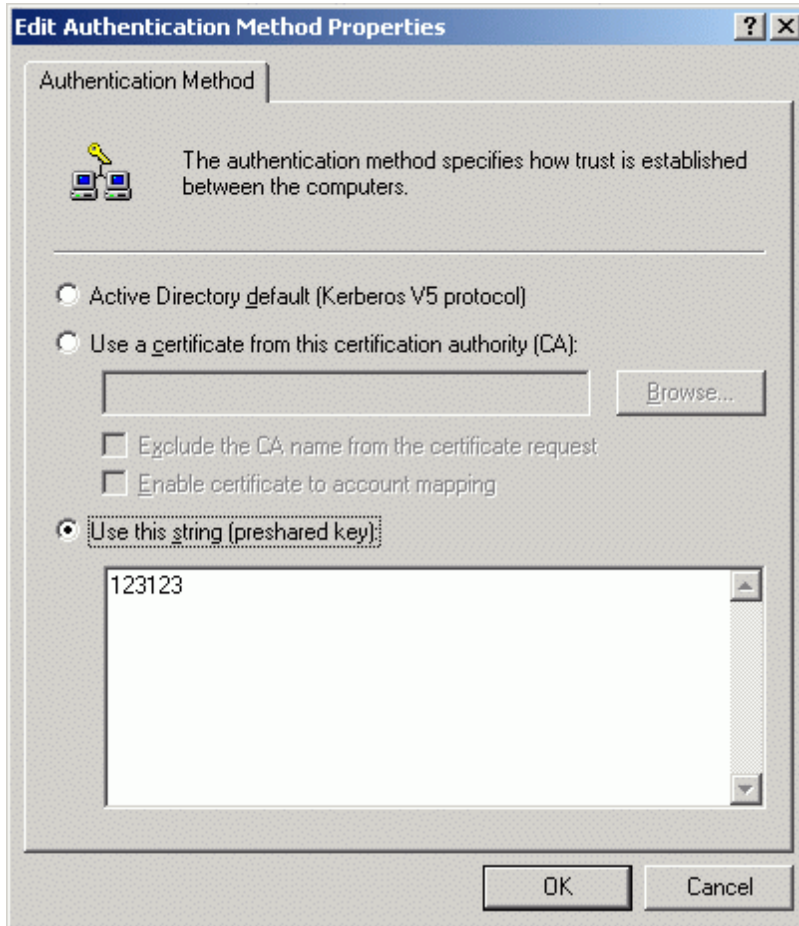
Select **This rule does not specify an IPsec tunnel.**

Switch to the **Authentication Methods** tab.



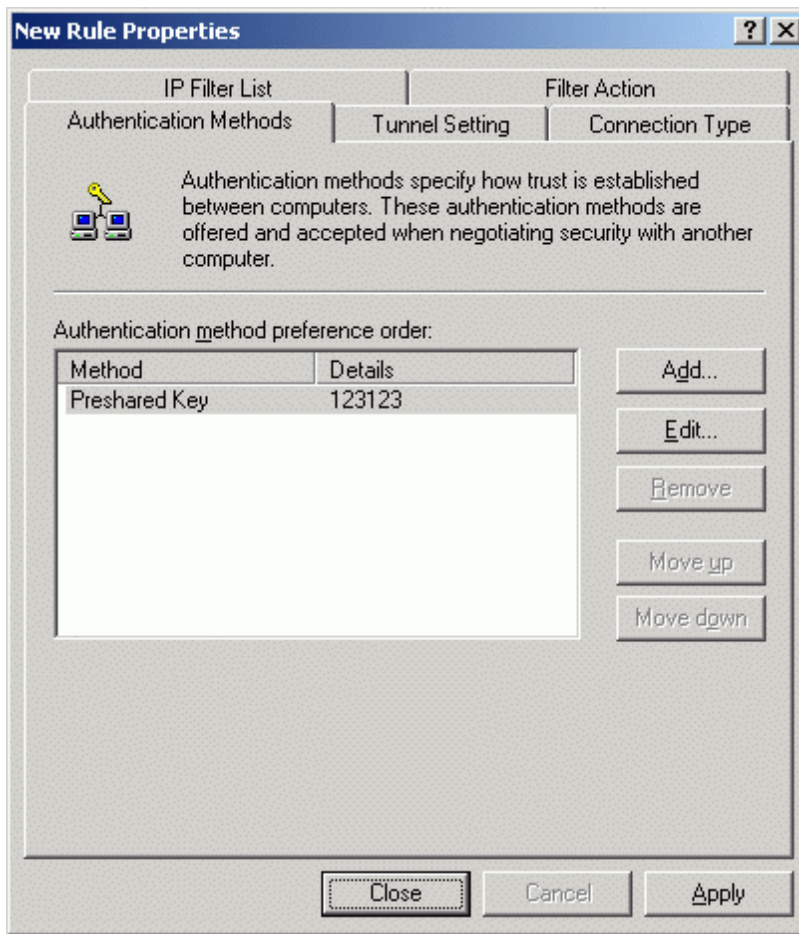
Press the **Edit** button to continue.

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



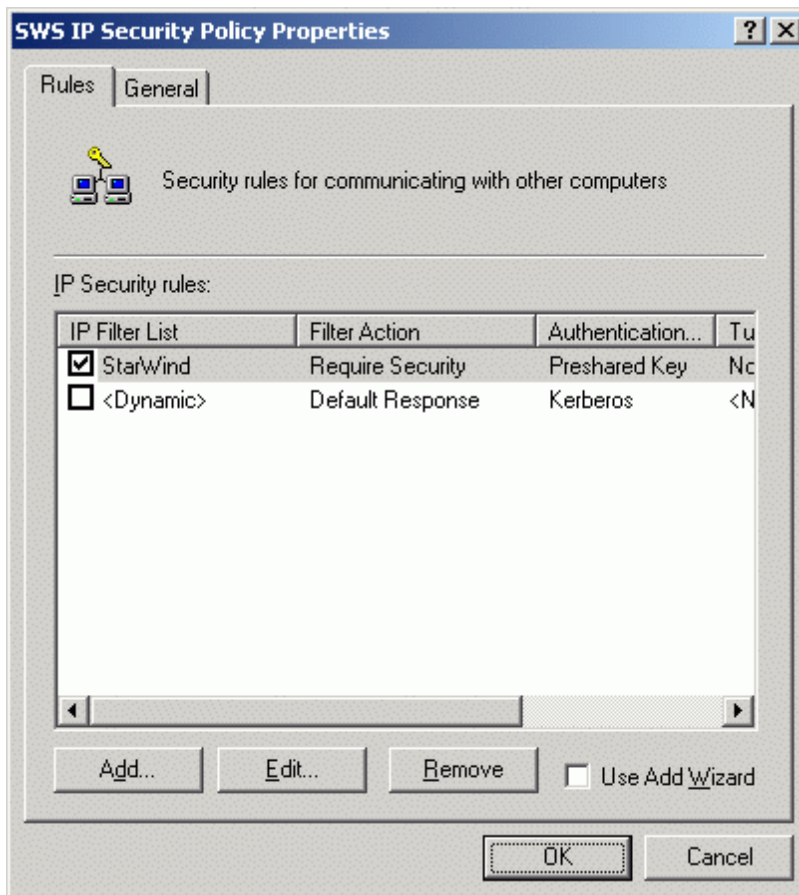
Press the **OK** button to continue.

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



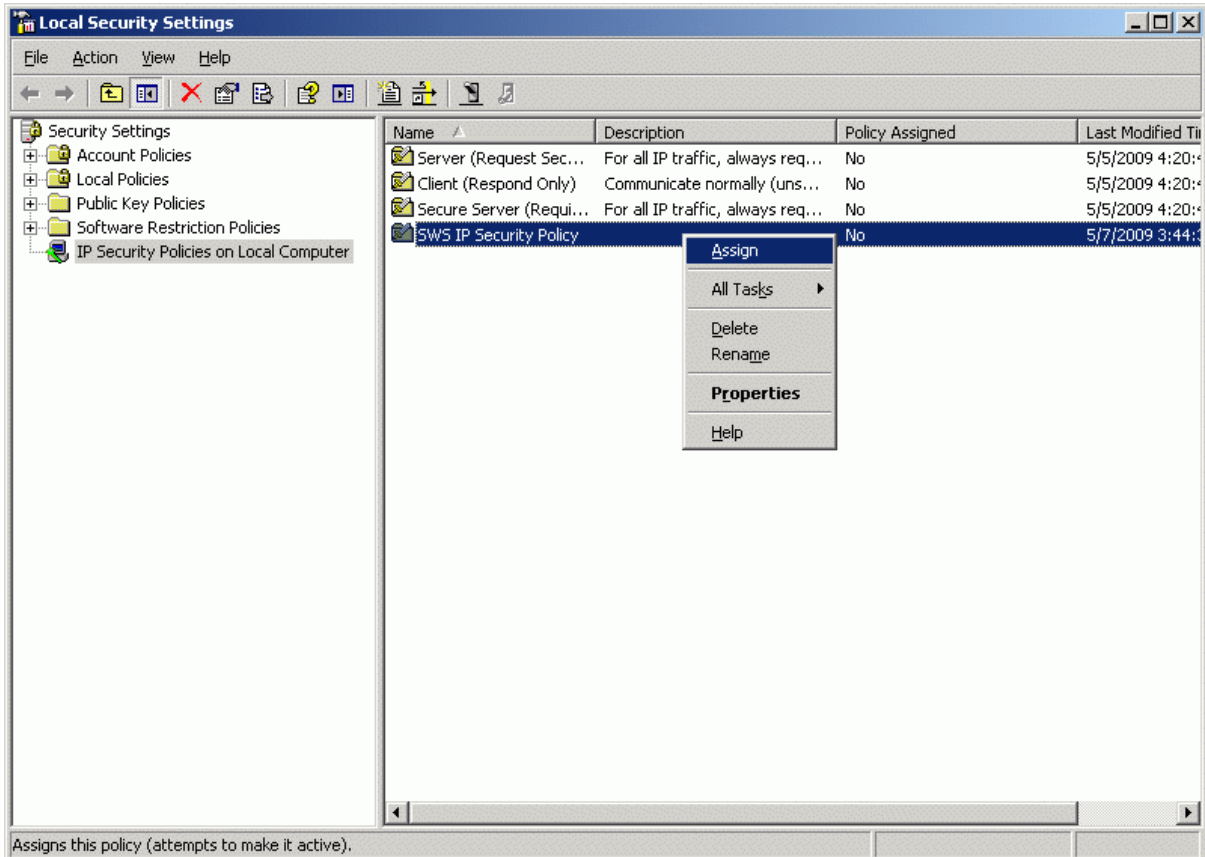
Press the **Close** button to continue.

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



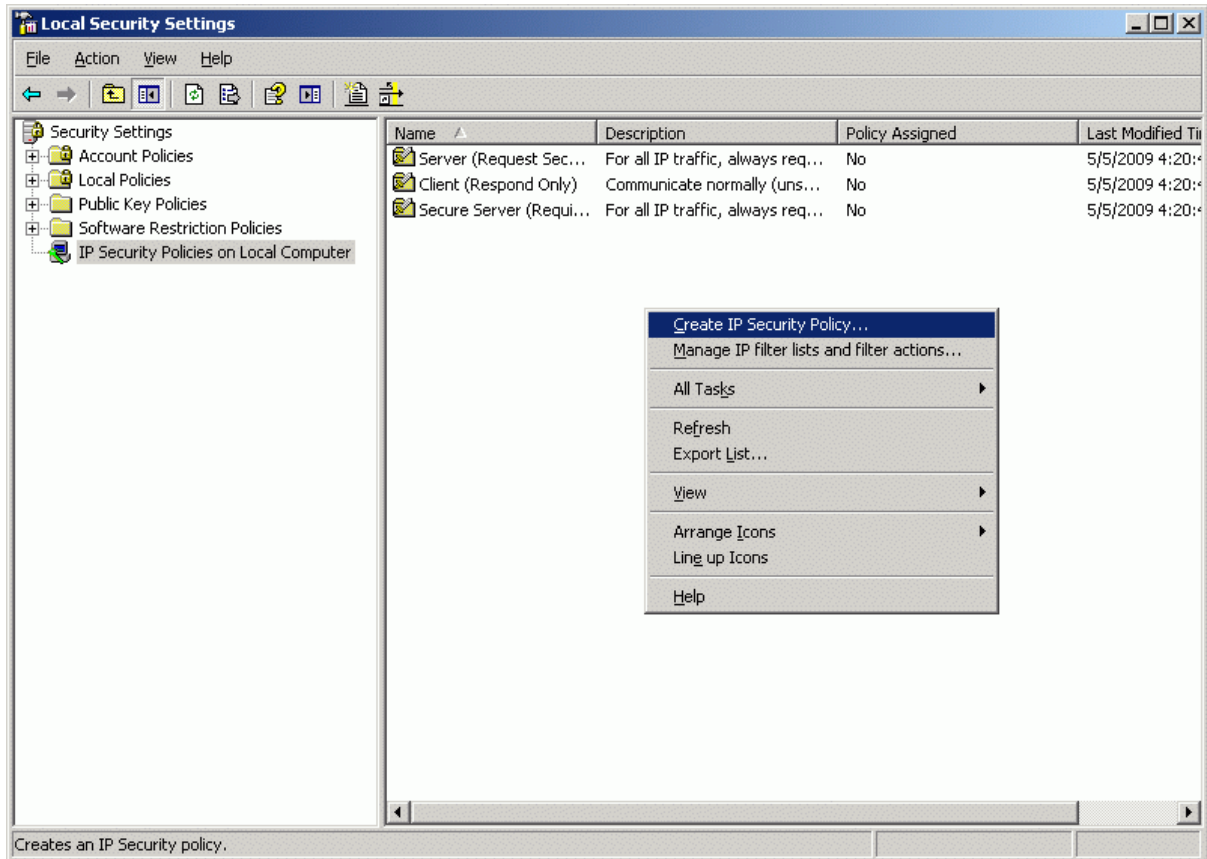
Press the **Close** button.

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



Client-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**.



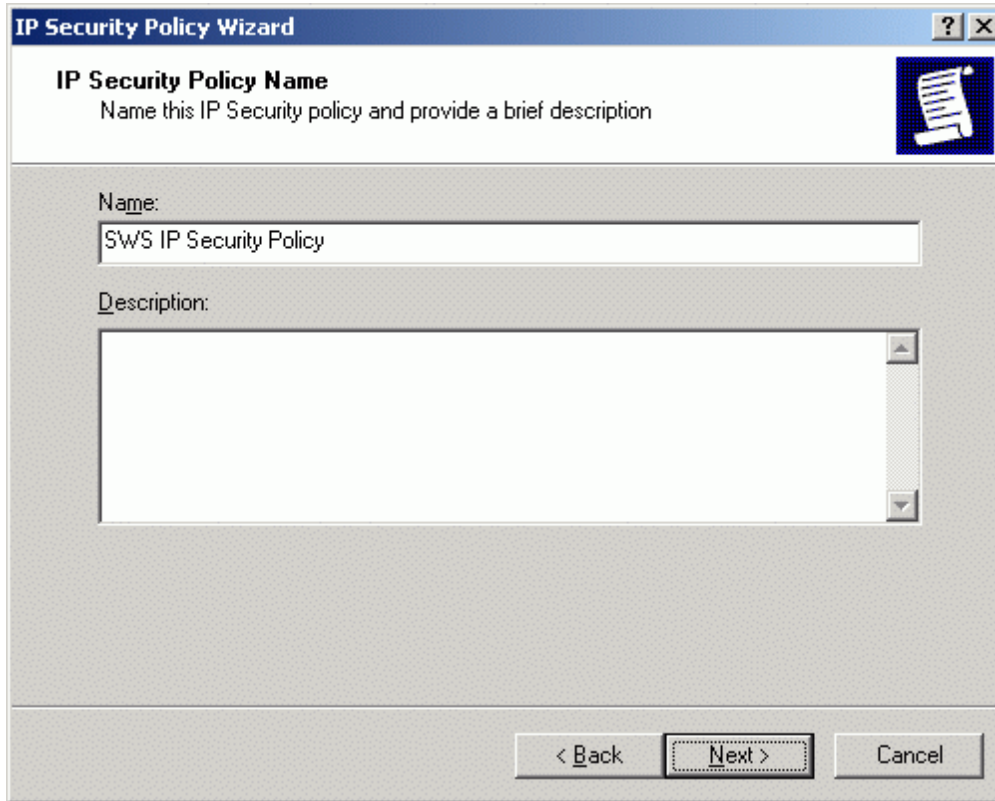
Click the right mouse button and select **Create IP Security Policy** option.

IP Security Policy Wizard appears.



Press the **Next** button to continue.

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

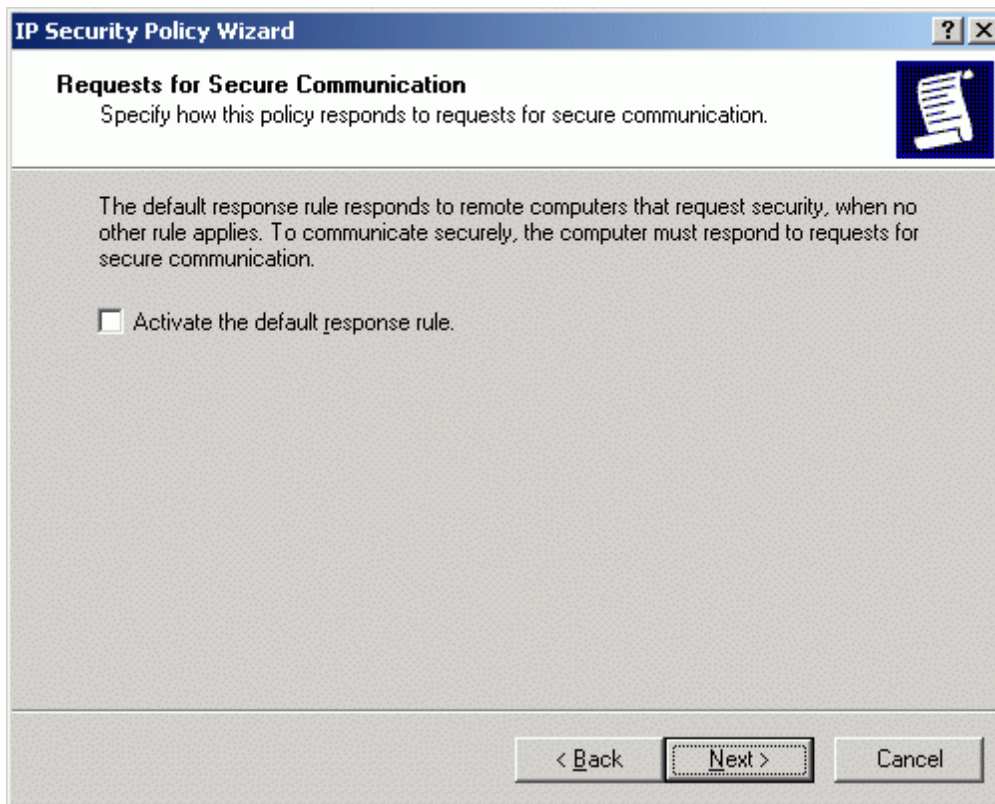


The image shows a Windows-style dialog box titled "IP Security Policy Wizard". The window has a blue title bar with a question mark and a close button. The main content area is white and contains the following elements:

- IP Security Policy Name**: A bold heading followed by the instruction "Name this IP Security policy and provide a brief description". To the right of this text is a small icon of a document with a pencil.
- Name:**: A text label followed by a single-line text input field containing the text "SWS IP Security Policy".
- Description:**: A text label followed by a multi-line text input field that is currently empty.
- Buttons:** At the bottom right of the dialog, there are three buttons: "< Back", "Next >" (which is highlighted with a dashed border), and "Cancel".

Press the **Next** button to continue.

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



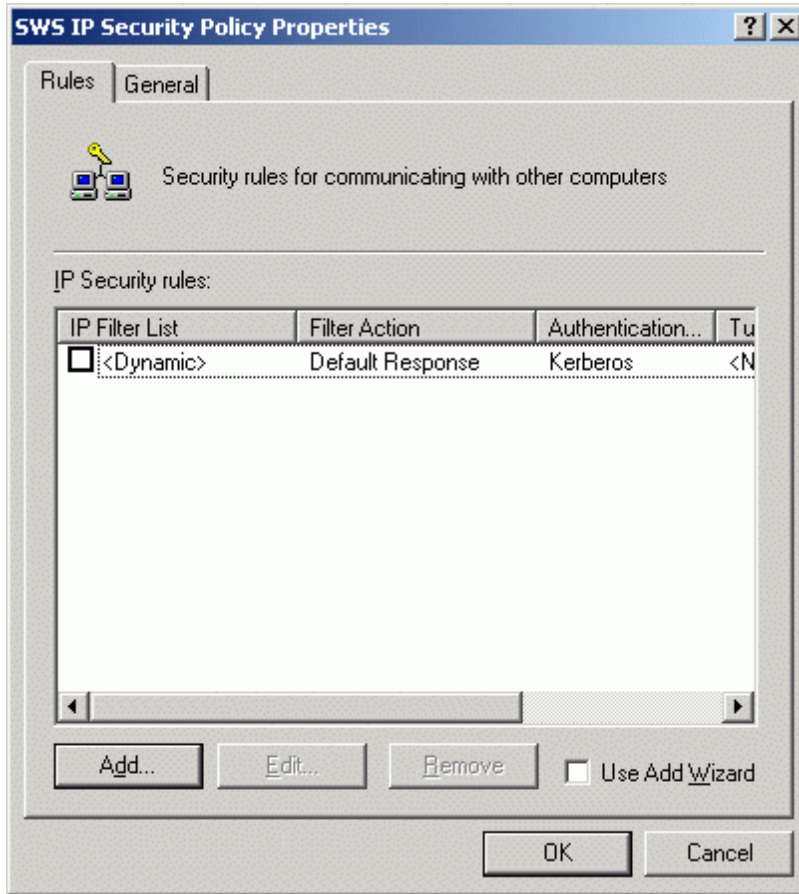
Press the **Next** button to continue.

Set the **Edit properties** option.



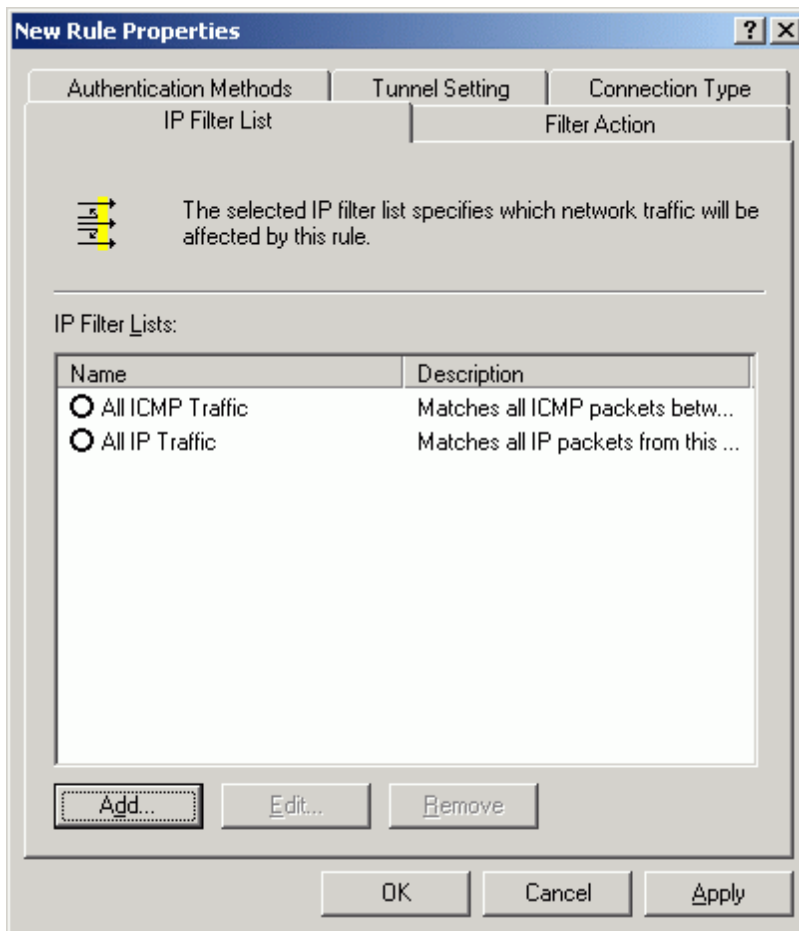
Press the **Finish** button.

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



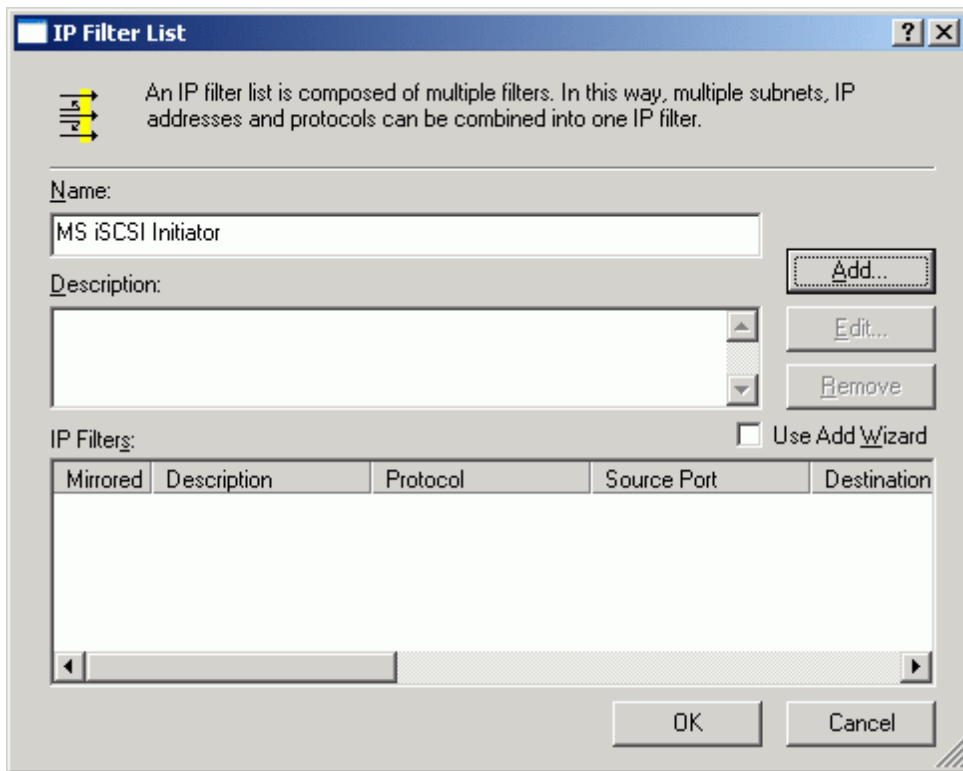
Press the **Add** button on the Rules tab.

New Rules Properties window appears.



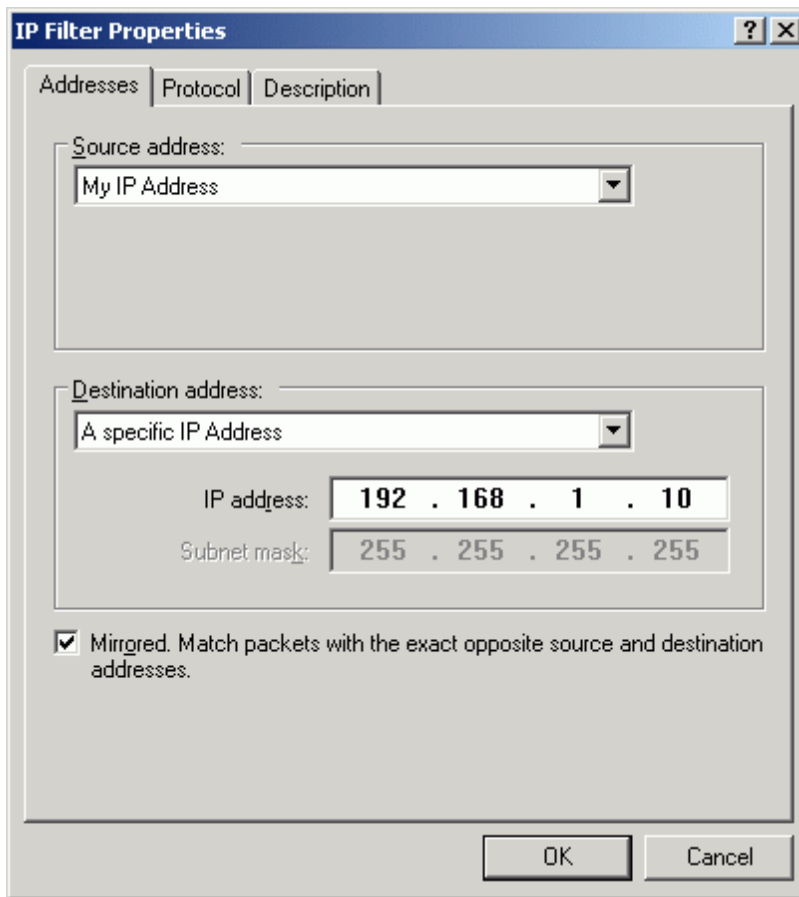
Press the **Add** button on the **IP Filter List** tab.

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



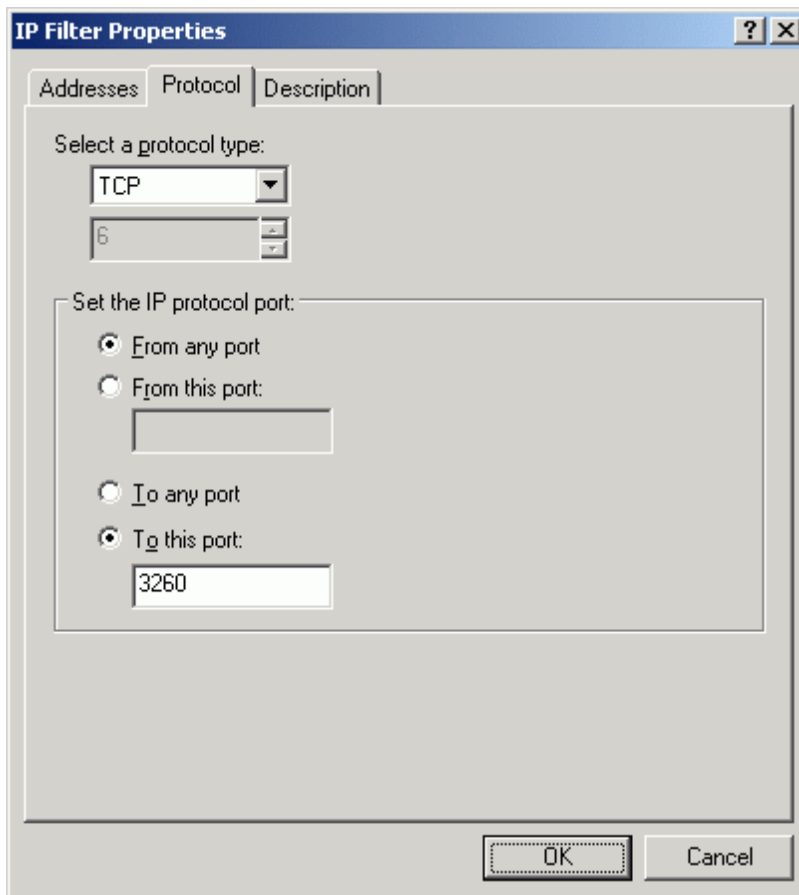
Specify the **Name** of **IP Filter** and optionally a brief description and press **Add** button.

IP Filter Properties window appears.



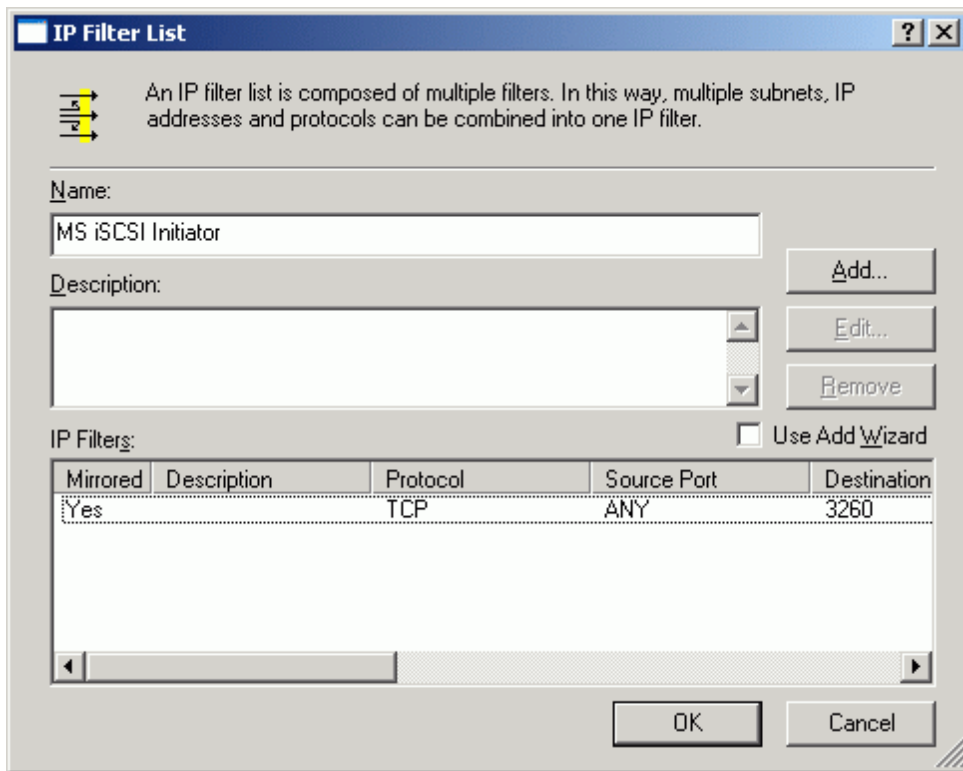
Specify **Source address** and **Destination address**. **Destination address** is the IP address of the **StarWind** server you wish to connect to.

Switch to the **Protocol** tab.



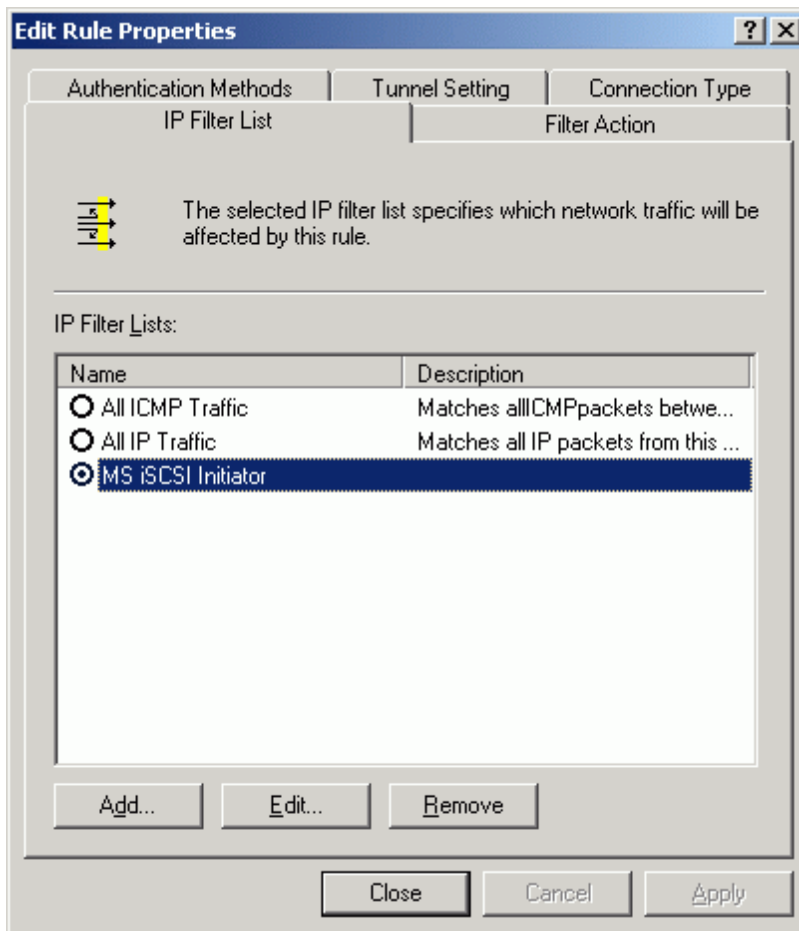
Specify protocol (**TCP** in our case) and port number (**3260**) and press **OK**. This filter is for **StarWind** service connections (iSCSI traffic itself).

New rule appears in the list.



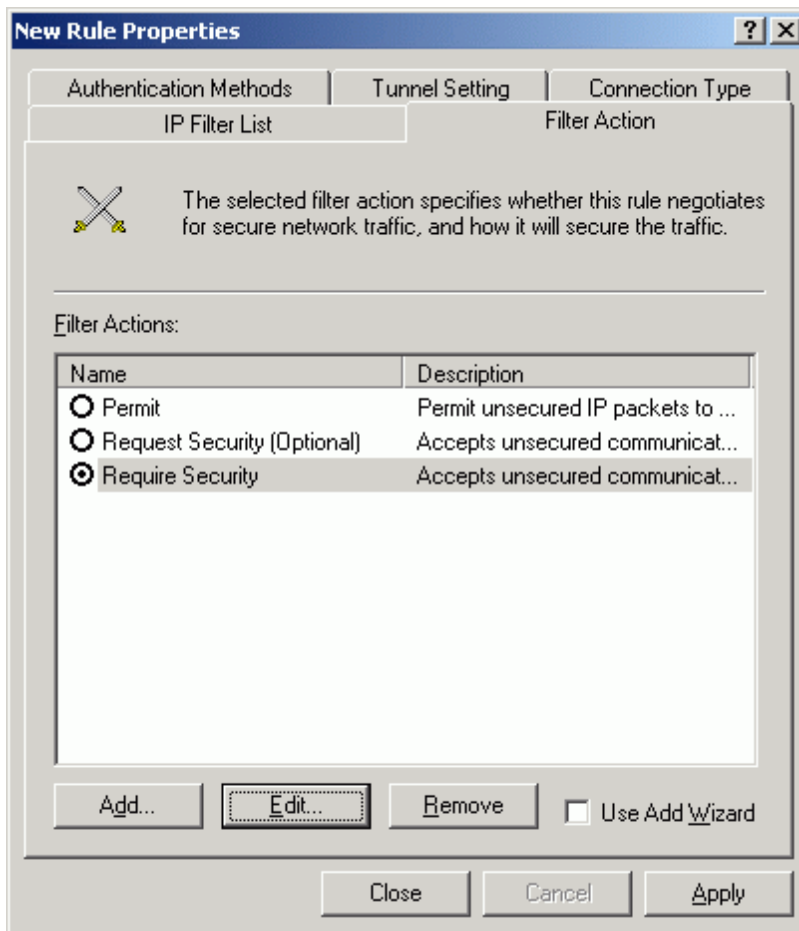
Press the **OK** button.

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



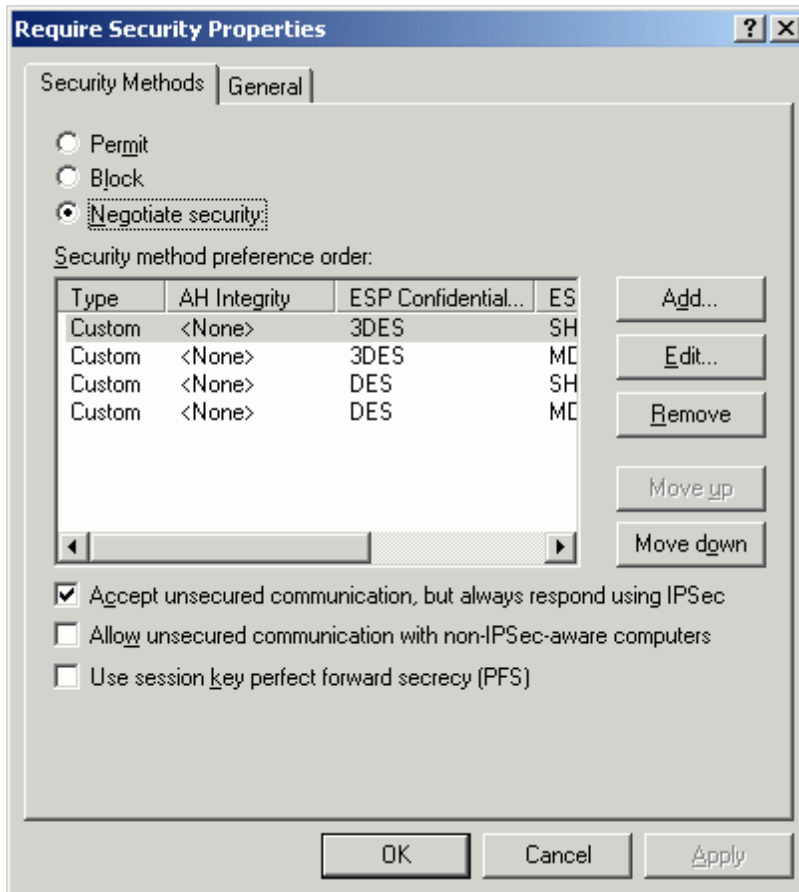
Select newly created filter **MS iSCSI Initiator** from the list and switch to the **Filter Action** tab.

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



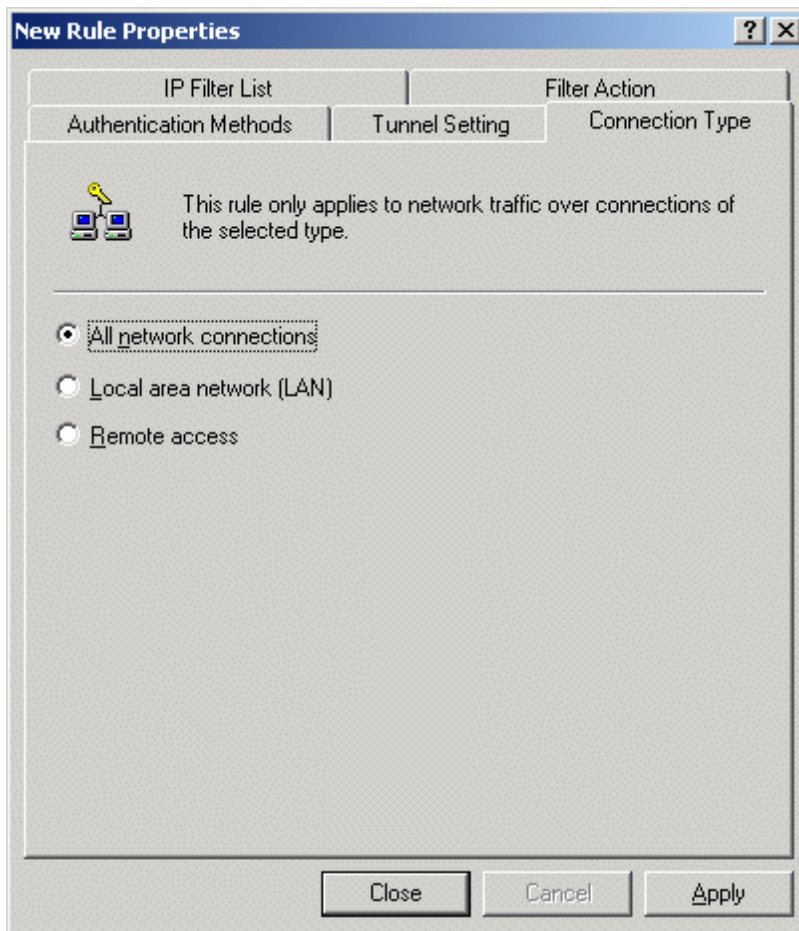
Press the **Edit** button to continue.

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



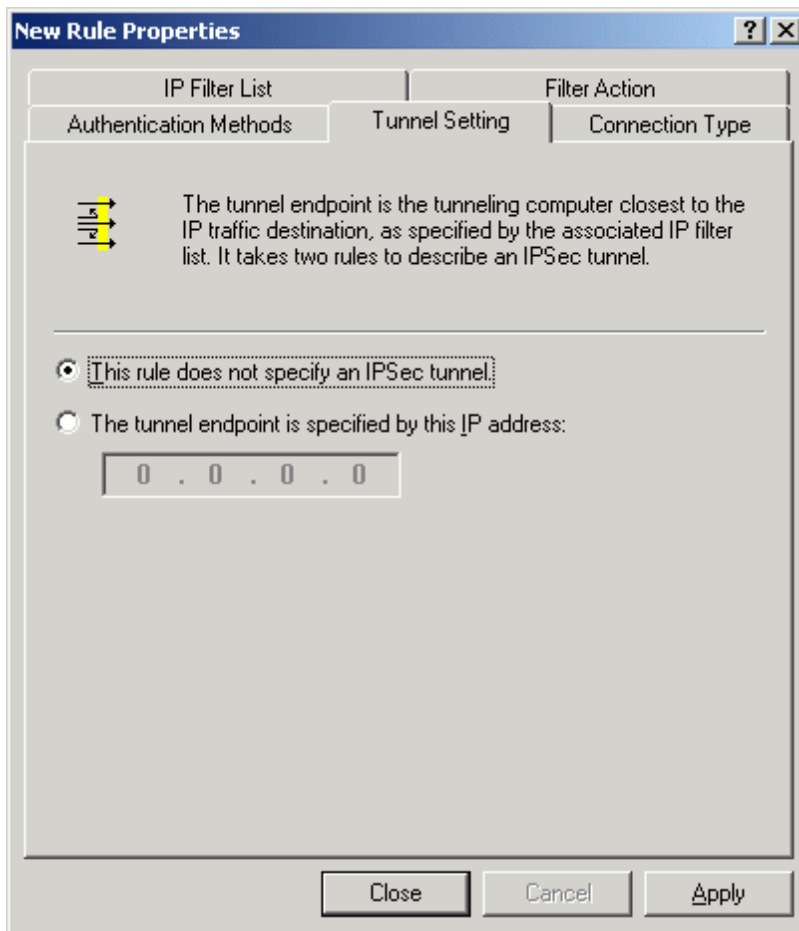
Press the **OK** button to continue.

Switch to the **Connection Type** tab.



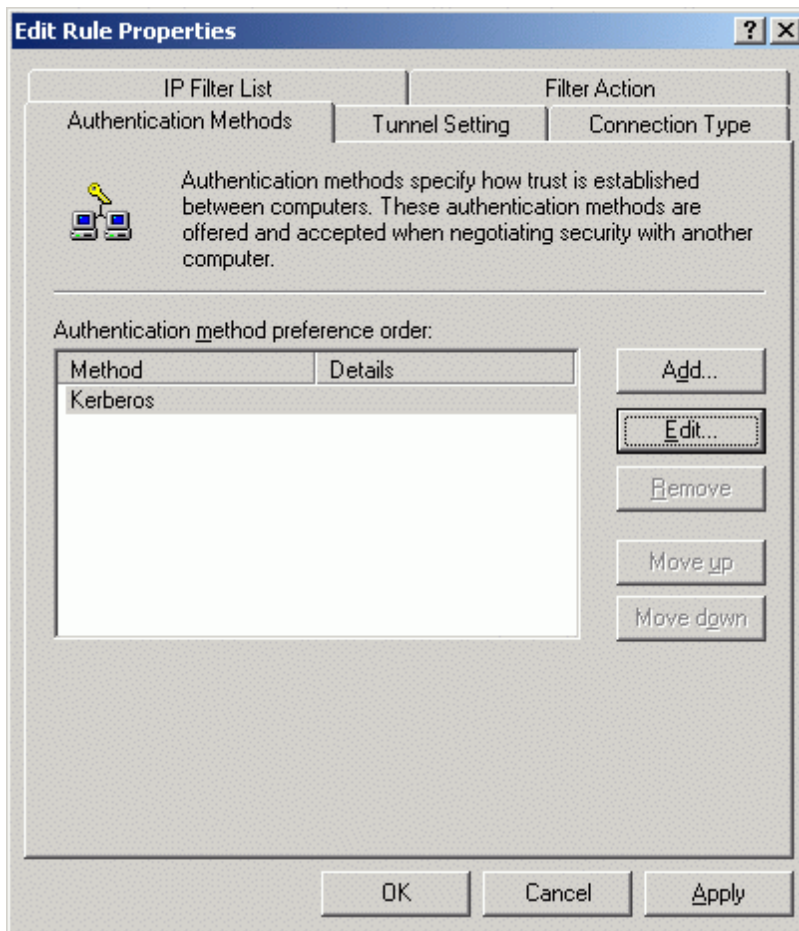
Select **All network connections**.

Switch to the **Tunnel Setting** tab.



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

Switch to the **Authentication Methods** tab.



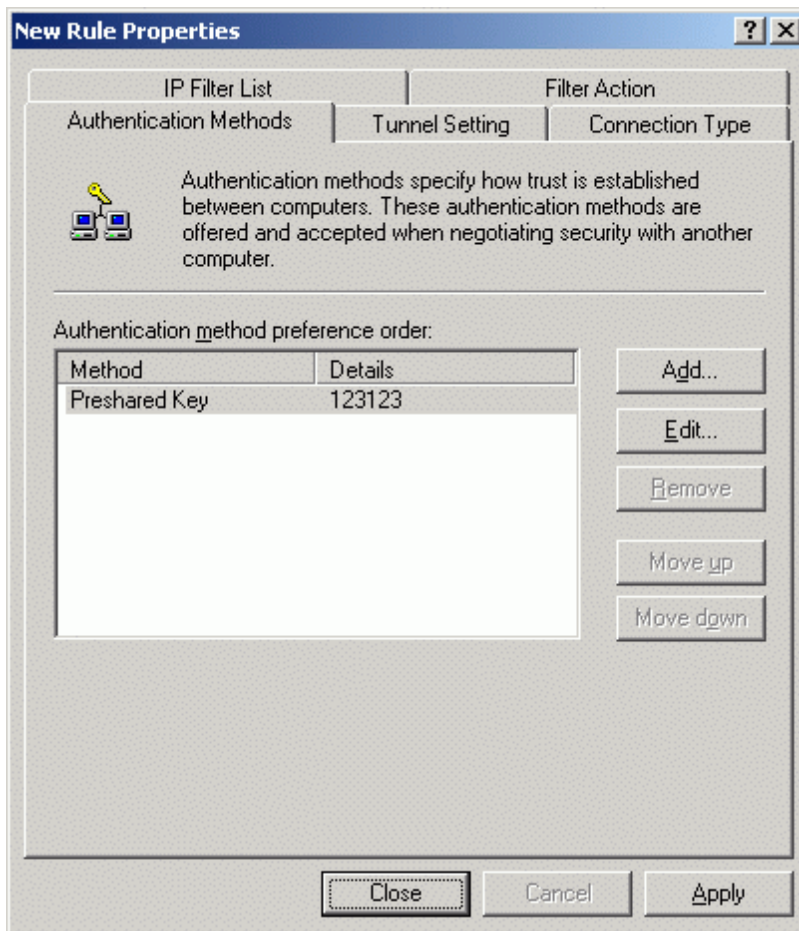
Press the **Edit** button to continue.

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).



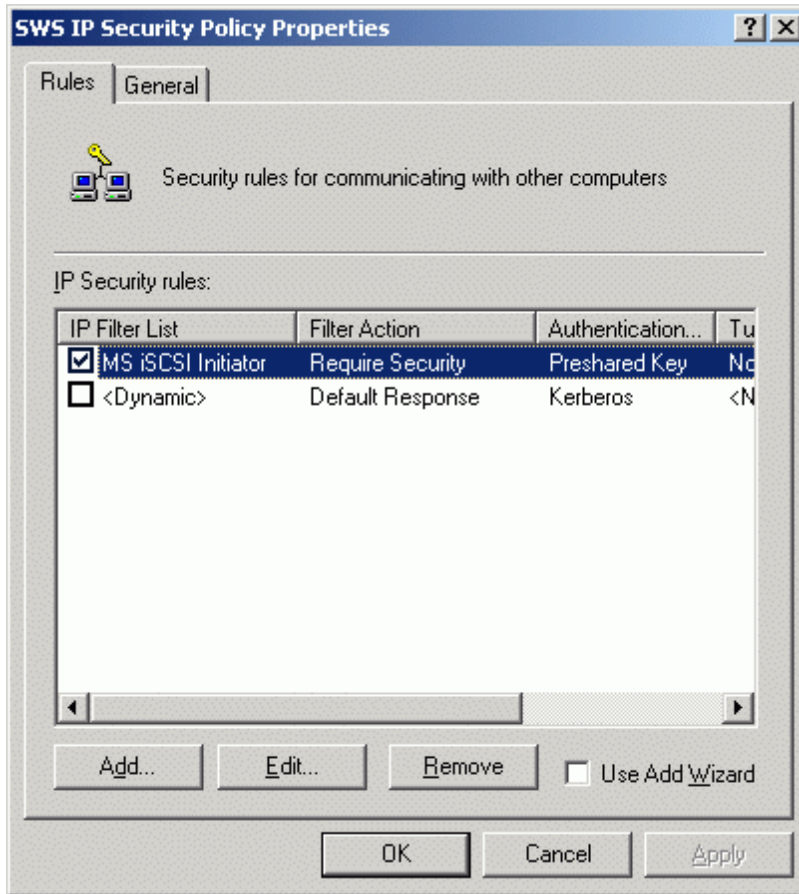
Press the **OK** button to continue.

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



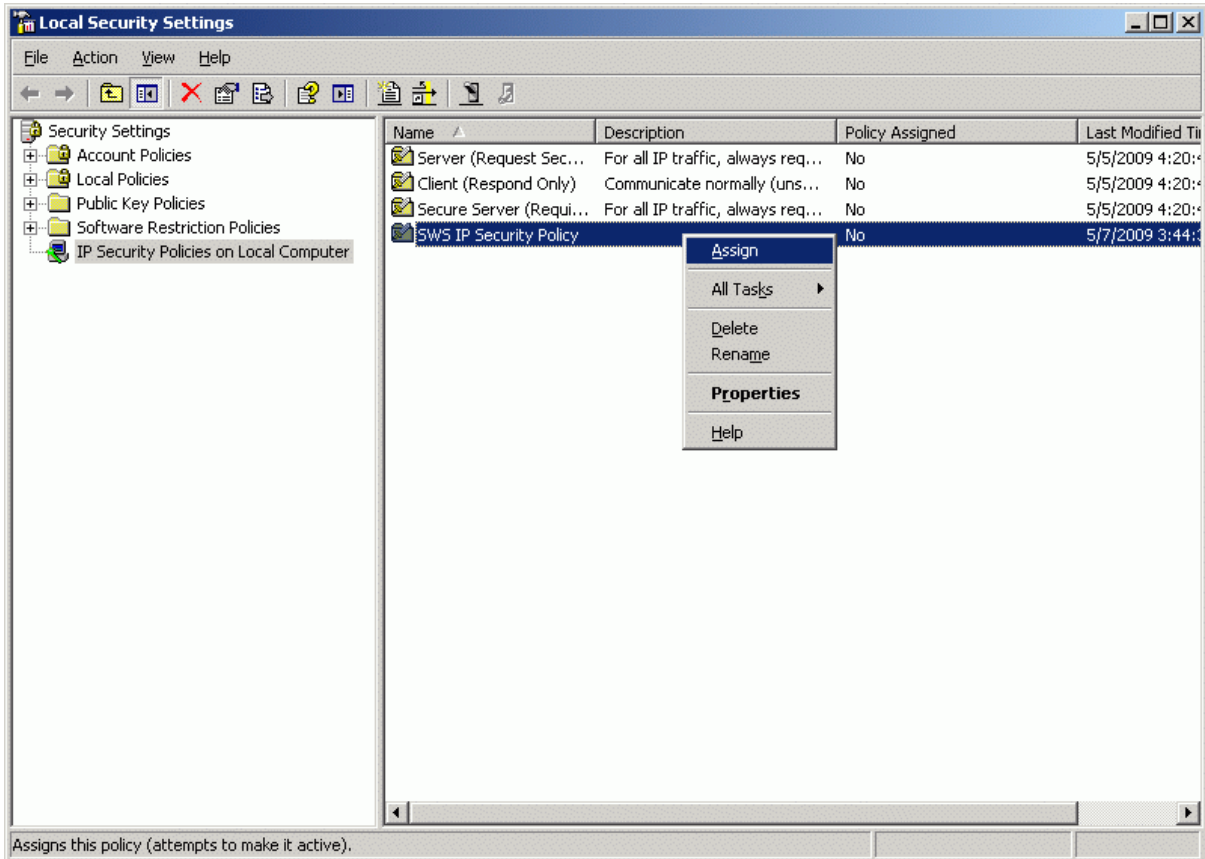
Press the **Close** button to continue.

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



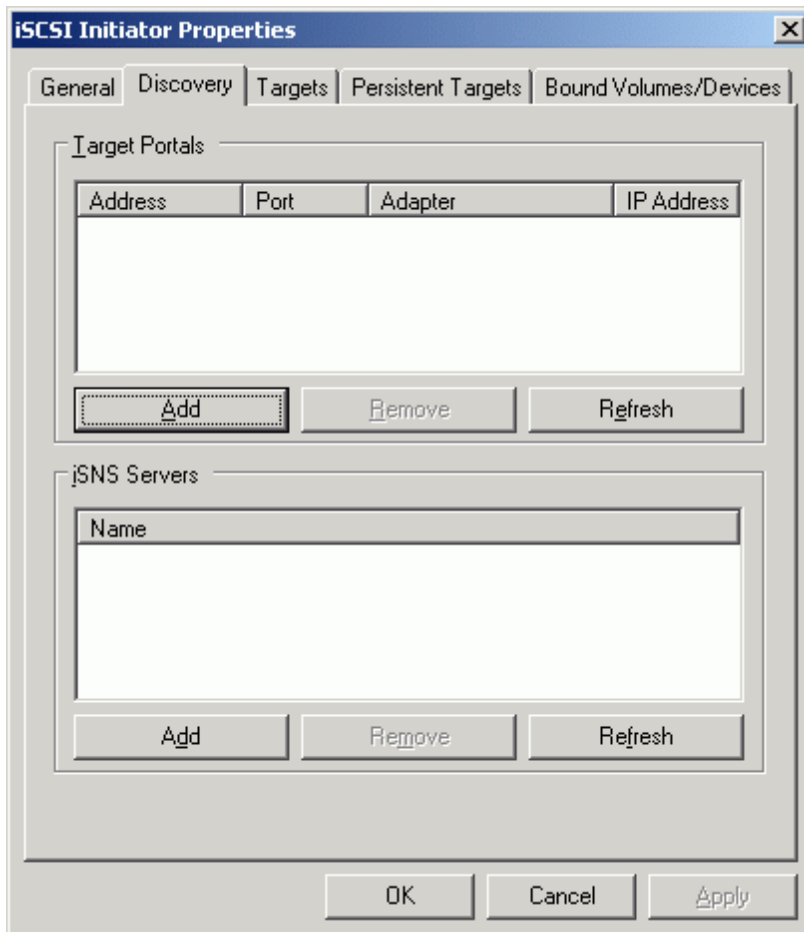
Press the **OK** button.

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



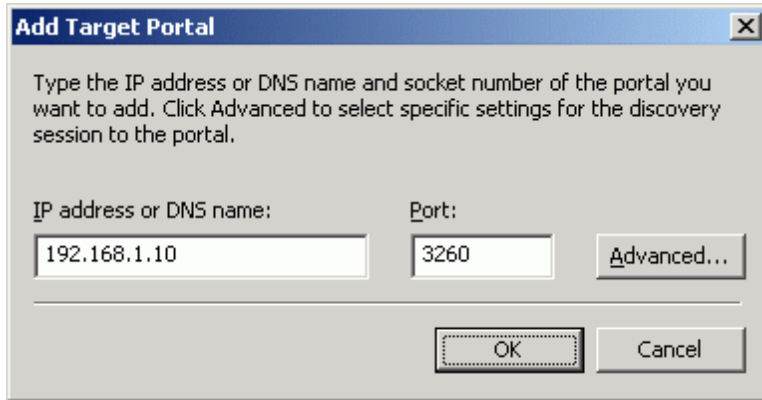
Connecting to the Target Using MS iSCSI Initiator

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.



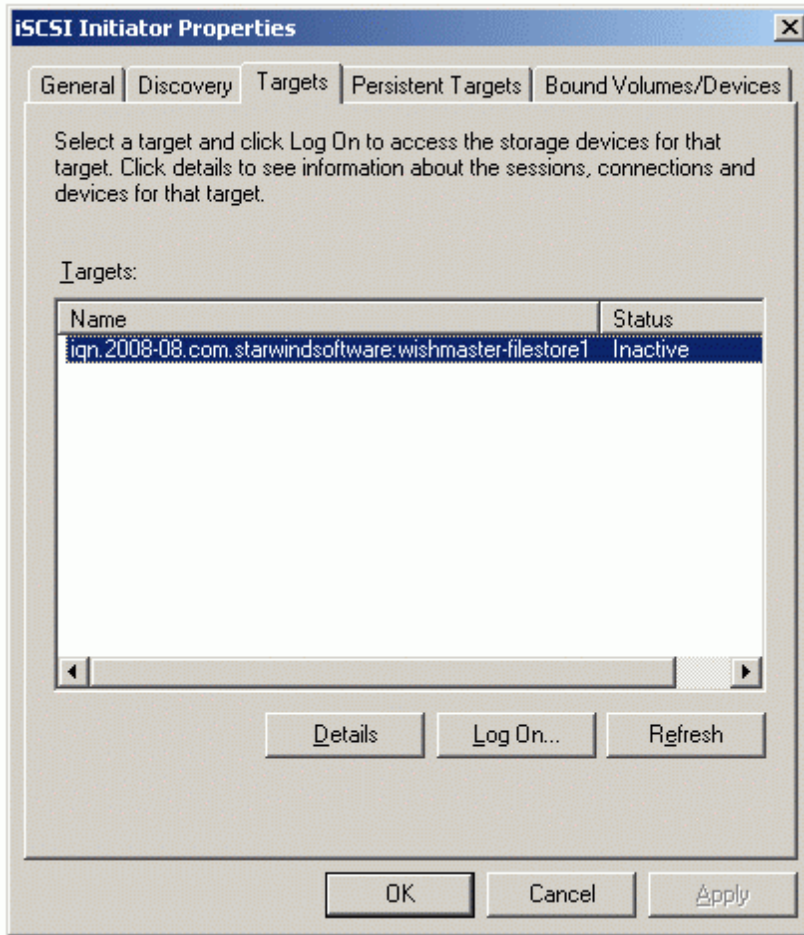
Press the **Add** button to continue.

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



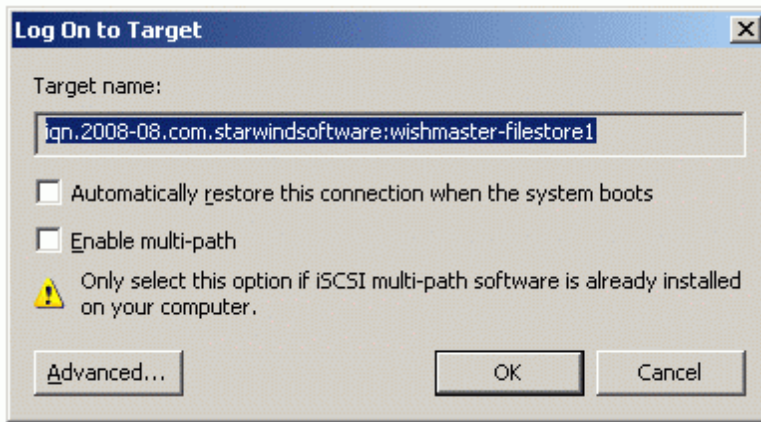
Press the **OK** button to continue.

Switch to the **Targets** tab.



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

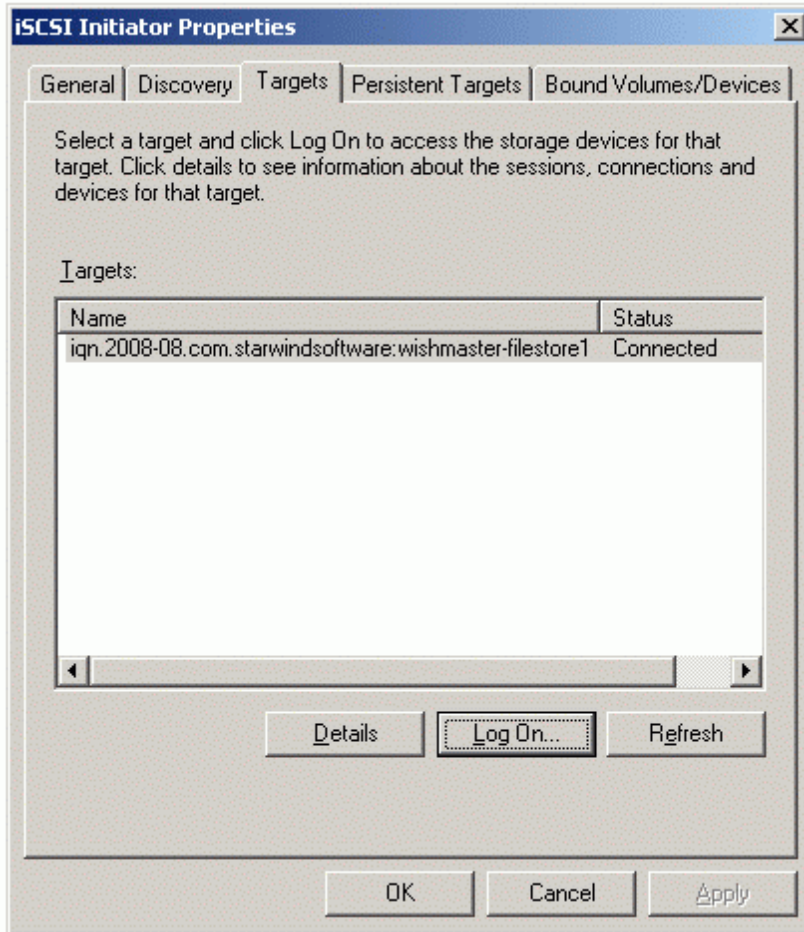
Log On to Target dialog appears.



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.



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

Contacts

Support: www.starwindsoftware.com/support

Support Forum: www.starwindsoftware.com/forums

Sales E-mail: sales@starwindsoftware.com

US Headquarters

Direct phone number: 1-617-449-7717

Fax: 1-617-507-5845

EMEA, APAC

Direct phone numbers: +44-0-2071936727

+44-0-2071936350

Voice Mail: 1-866-790-2646

StarWind Software Inc.

40 Mall Rd., Burlington

MA 01803, USA

www.starwindsoftware.com