iStorage Server: IP SEC under Windows Server 2008 R2

Monday, July 4, 2011

KernSafe Technologies, Inc.

www.kernsafe.com

Table of Contents

KernSafe iStorage Server is an advanced and powerful, full-featured software-only iSCSI Target that fully conforms to the latest iSCSI Standard 1.0 (former Draft 20). It is an IP SAN solution allowing you to quickly export existing storages such as disk images, VHD files, physical disks, partitions, CD/DVD-ROMs, tapes or any other type of SCSI based devices and even a variety of popular CD/DVD images to the client machines. The software thus delivers immediate benefits, as it allows storage to be consolidated, virtualized and centrally managed. iStorage Server also provides RAID-1 (mirror) feature enabling you to create two iSCSI devices for mirror backup. Furthermore, iStorage Server also supports a lot of features such as: VHD (Virtual Hard Disk) target, snapshots, STPI, RAID-1 and failover, these features are very important and poplar in storage industry world and make iStorage Server is suitable for any size of business.

After iStorage Server 2.0, it supports server side mirroring, synchronous replication and failover which allows user to create a high-availability iSCSI SAN.

Internet Protocol Security (IPSec) is an architecture defined by the Internet Engineering Task Force (IETF) RFC 2401. This architecture involves several protocols that perform various functions in the architecture.

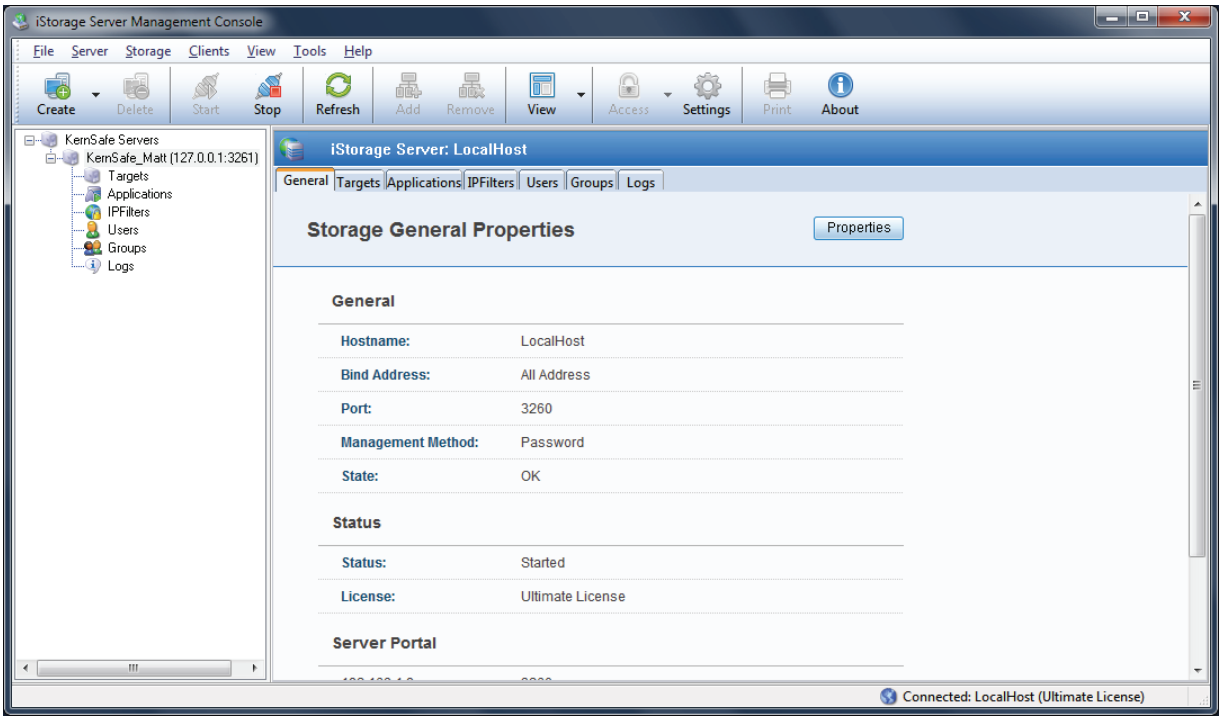
A network is not secure until servers can identify the computers communicating with them. IPSec enables secure, trusted communications between IP addresses. The system behind the IP address has an identity that is verified by using an authentication process. The only computers that must be aware of IPSec are the sending and receiving computers. Each computer handles security at its respective end, and assumes that the medium over which the communication takes place is not secure. Any computers that route data between the source and destination computer are not required supporting IPSec.

This article demonstrates how to make a Security iSCSI Target under the Windows IP Security Policies (IP Sec) environment by using KernSafe iStorage Server. It is shown how to do it under Windows Server 2008 R2. At the time this article also demonstrates how to use the two method of security policy in the iStorage Server, CHAP and IP Address authentication mechanism and how to configurate Local Security Policy in the both client and server side.

Configuring iStorage Server

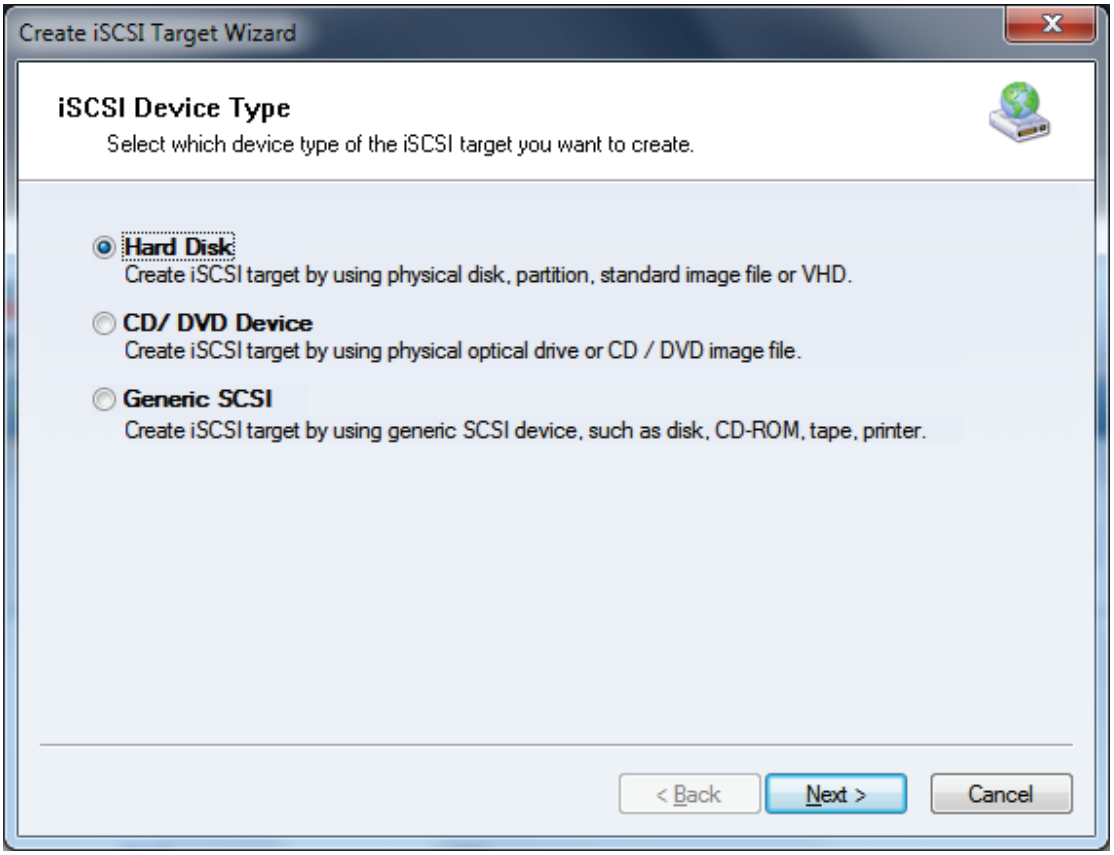
Creating Target

Open **iStorage Server Management Console**.



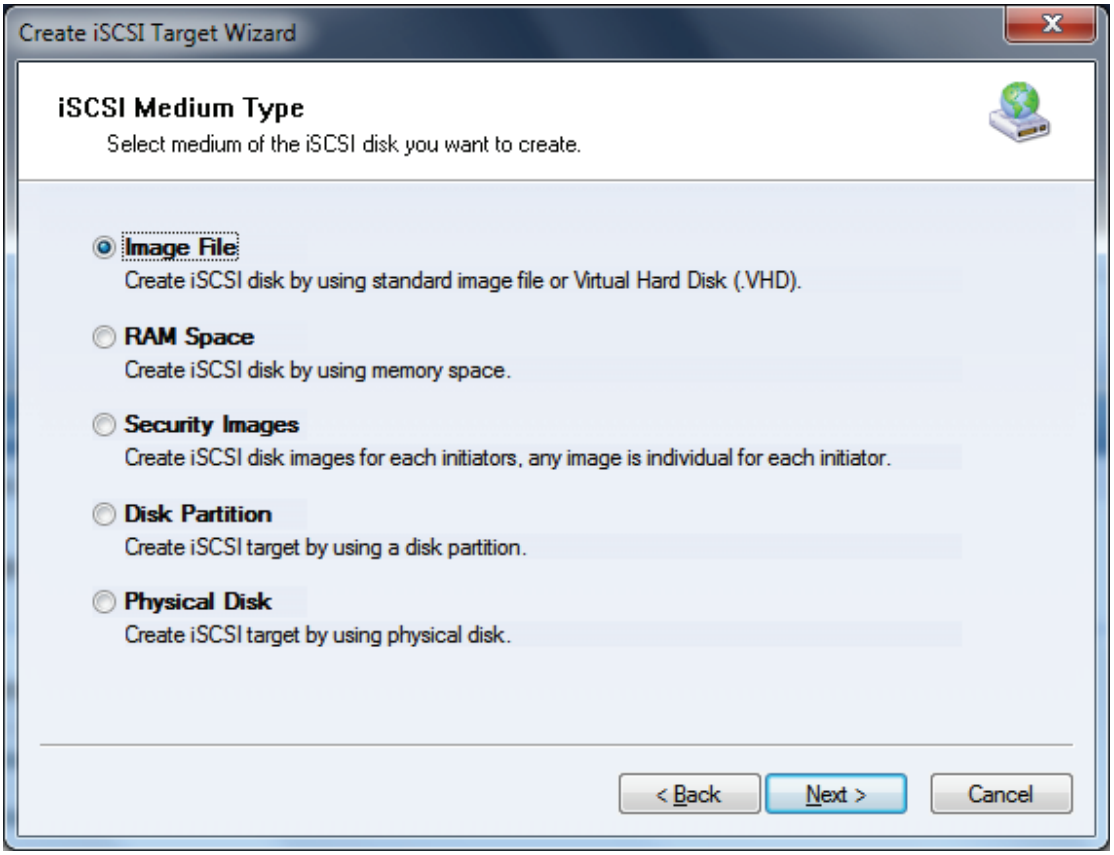
Launch the **iStorage Server Management Consolle**, press the **Create** button on the toolbar, the **Create iSCSI Target Wizard** will appear.

Select device type.



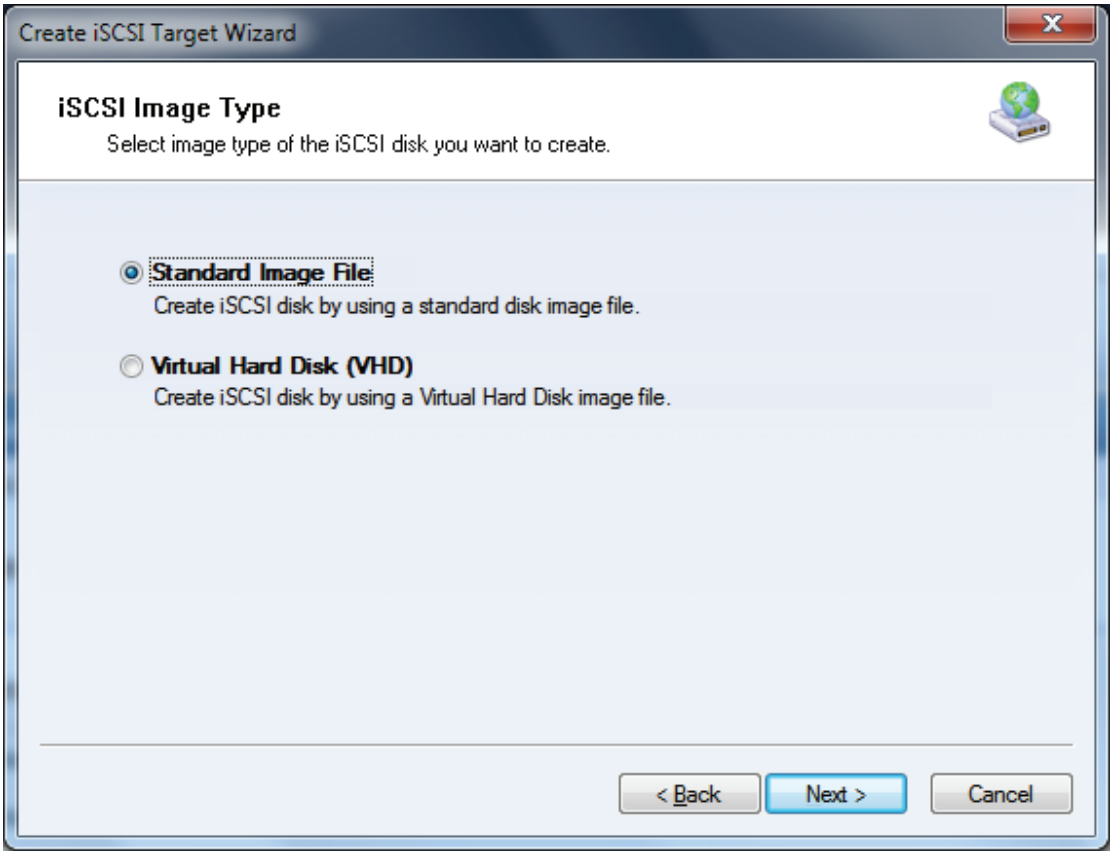
Chose **Hard Disk**.

Press the **Next** button to continue.



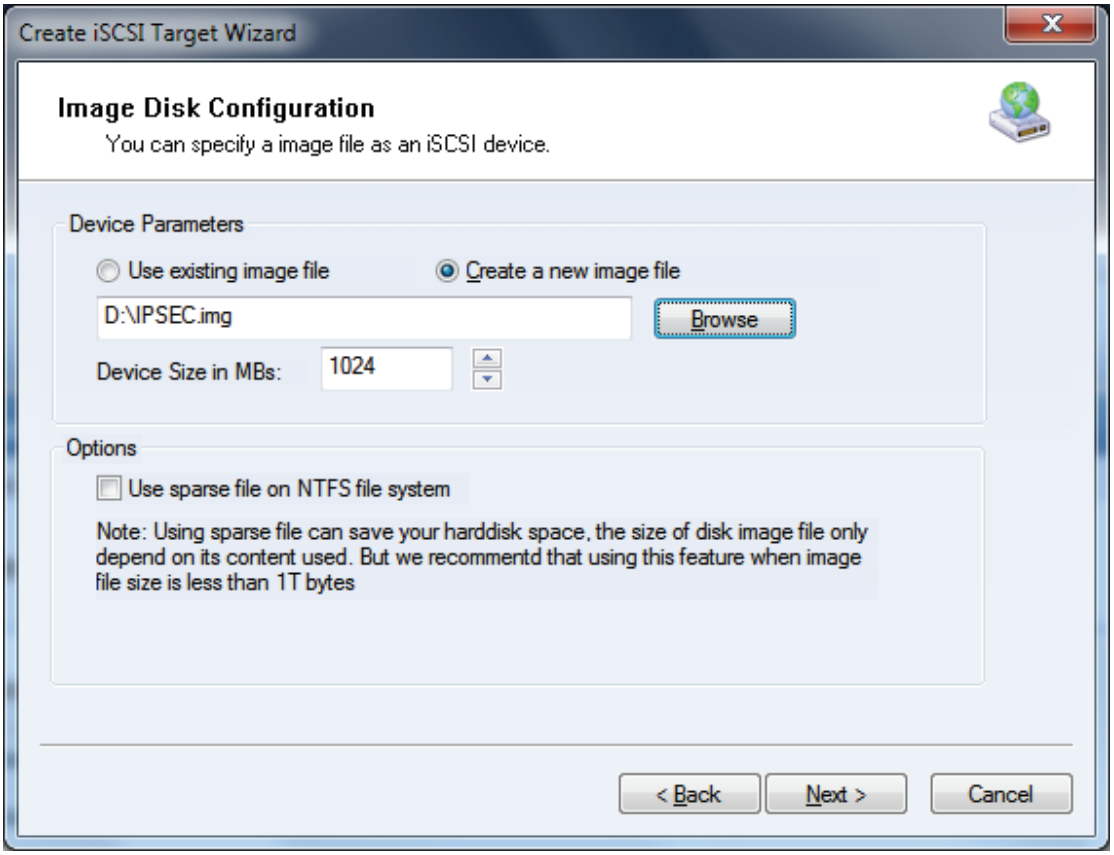
Choose **Image File** in **iSCSI Medium Type** page.

Press the **Next** button to continue.



Chose **Standard Image File** in **iSCSI Image Type**.

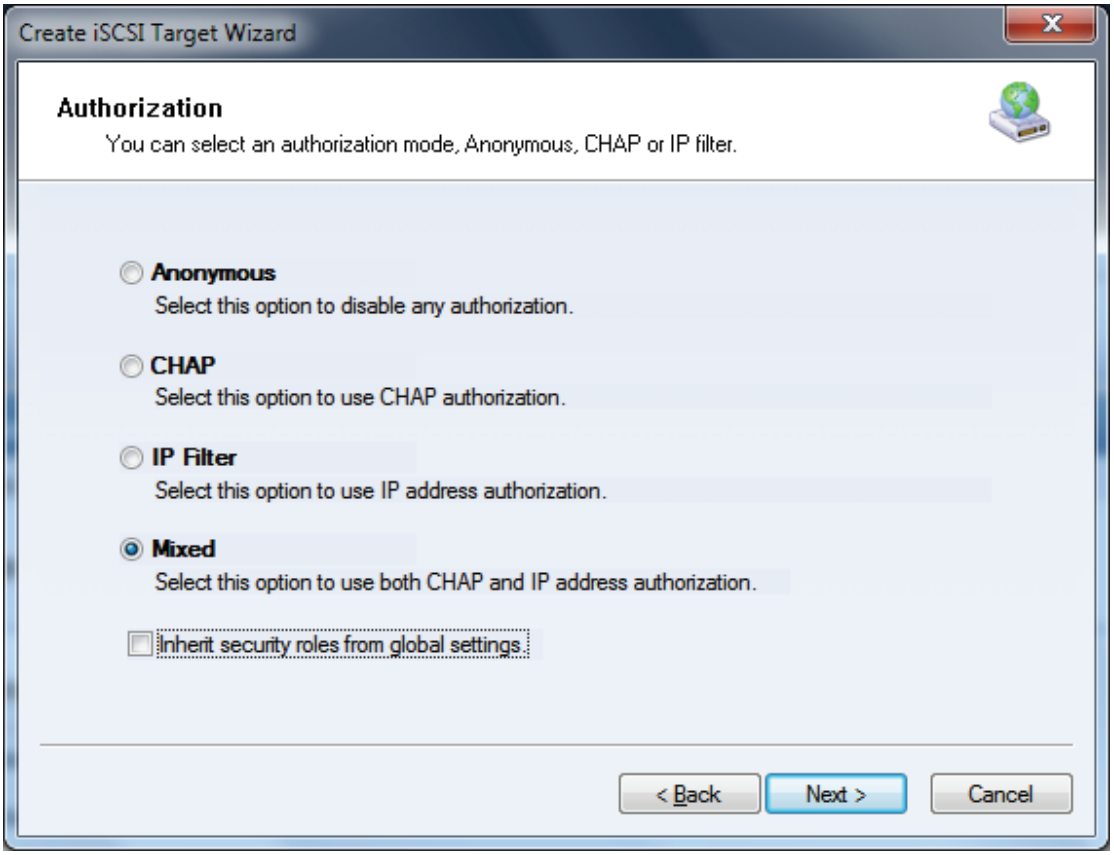
Press the **Next** button to continue.



Select **Create a new image file** or **Use existing image file** if you already have one. Then specify the device size.

Checking **Use sparse file on NTFS file system** will save your hard disk space by expanding image file depending on its content used.

Press the **Next** button to continue.



Decide which authentication mechanisms you would want to use: **Anonymous**, **CHAP**, **IP Filter** or **Mixed** authentication.

1) Anonymous

All initiators will get full access permission without any authorization required.

2) CHAP (Challenge-handshake authentication protocol)

All initiators need to specify a CHAP user and secret to connect to the target. iStorage Server has a built-in user called “Guest”, which is used for initiators without CHAP secret specified.

3) IP Filters

All initiators will be authorized by the incoming IP address defined by IP Filter roles.

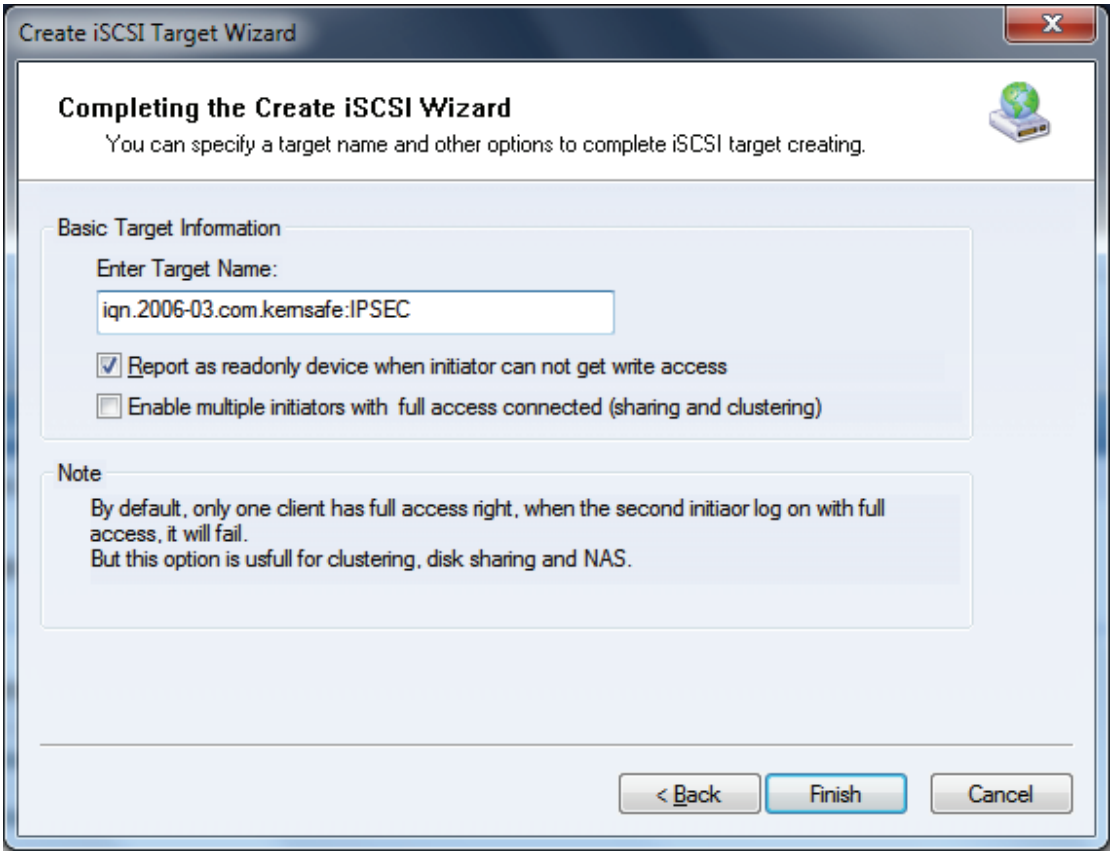
4) Mixed

Security policy is determined by both CHAP and IP Filters.

If you check **Inherit security roles from global settings**, all client security roles are form global settings, otherwise, each client will have its own permission.

For this purpose I will choose **Mixed** and I will uncheck **Inherit security roles from global settings** since I will set it up manually for this target.

Press the **Next** button to continue.



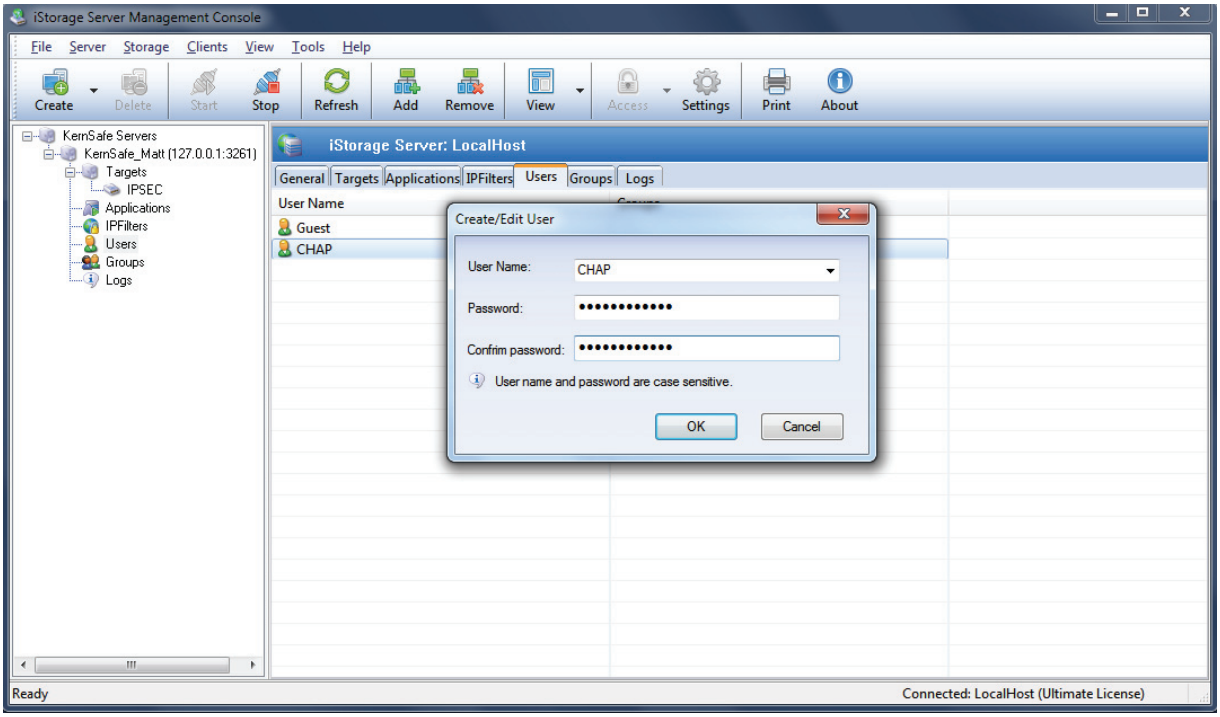
Enter the name for your target device.

If you check **Report as readonly device when initiator cannot get write access**, the system will give you a report when you load the target without write access.

Press the **Finish** button to continue.

Now we need to set up **CHAP** and **IP filter.**

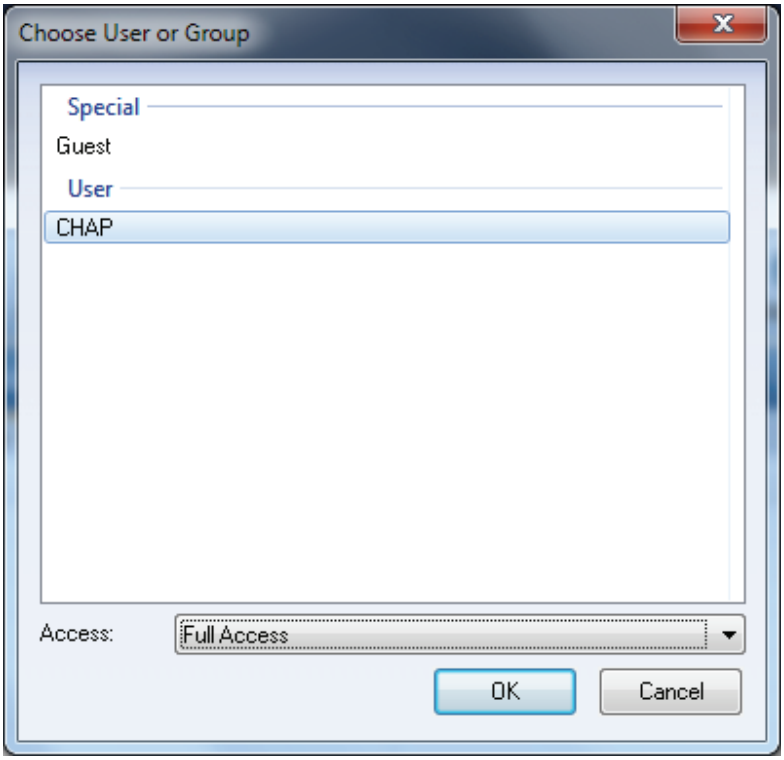
To set up **CHAP** for this target please switch to the **Users** group in the left side panel. **Right click** on empty space and choose **New User …**.



Type desired **User Name** and **Password** but keep in mind that perfect password should be from 12 to 16 characters long and it is case sensitive.

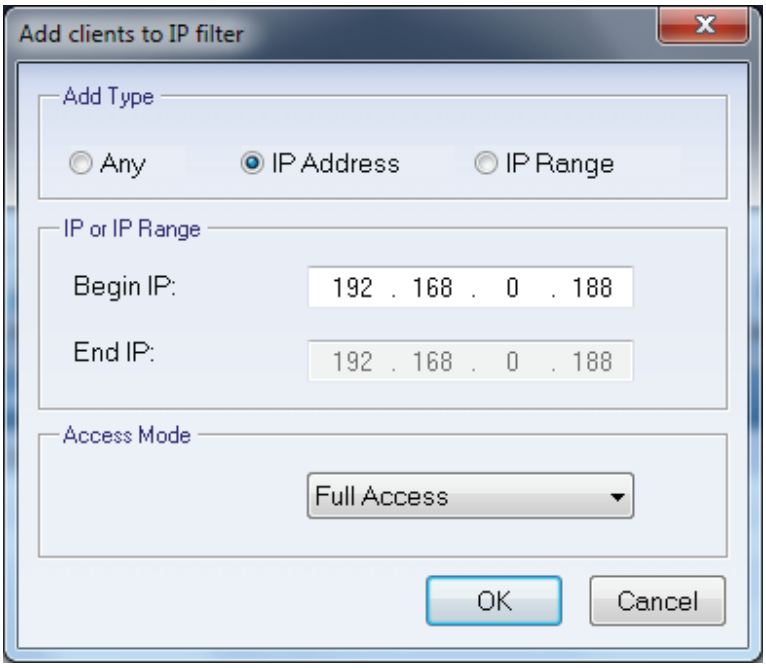
Click **OK** to continue.

After finishing, please click on name of your target in left side panel and switch to **CHAP** tab.
Right click on empty space and choose **Add Item…**



Choose your chap user and specify access rights. Click **OK** button to continue.

Now please switch to **IPFilters** tab.
Right Click on empty space and choose **Add Item…**, the **Add clients to IP filter** dialog is shown.



Set up your IP filter.

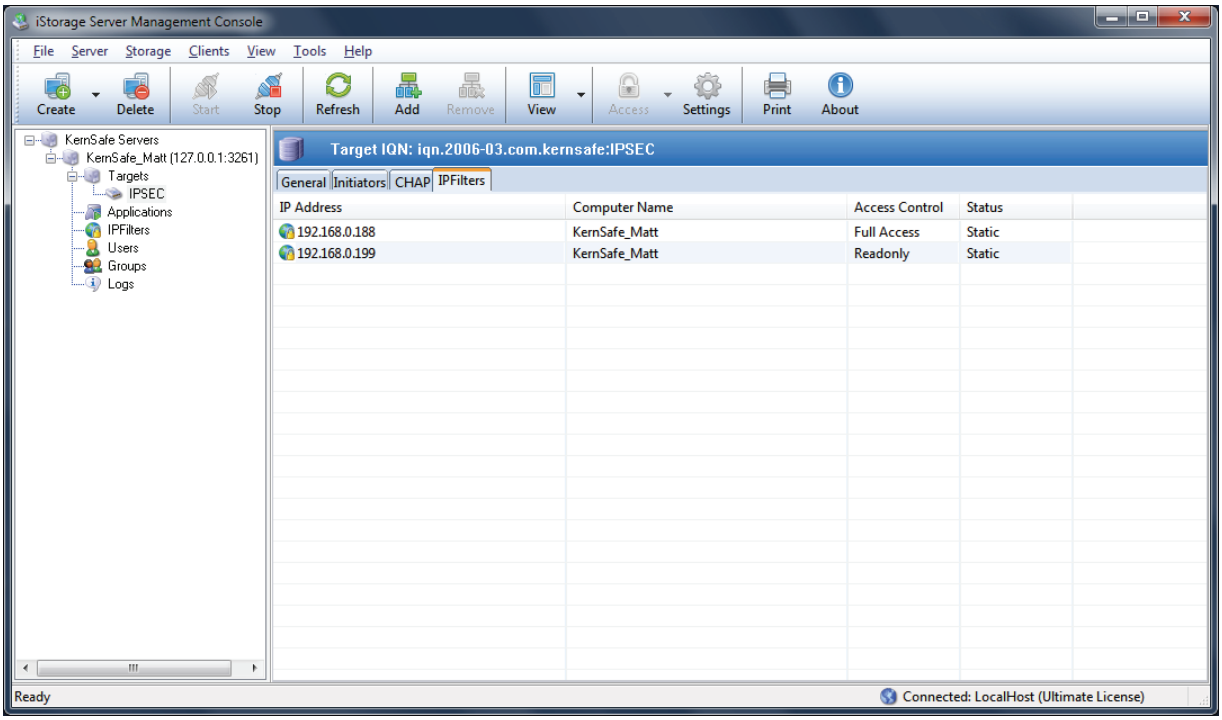
Any: Indicate all of the clients connected to the target have the same access right.

IP Address: Indicate the IP address has the given access right.

IP Range: Indicate the clients specified by the range has the given access right.

Here, for example, I chose **IP Adress**.

Press the **OK** button to add an IP filter item.



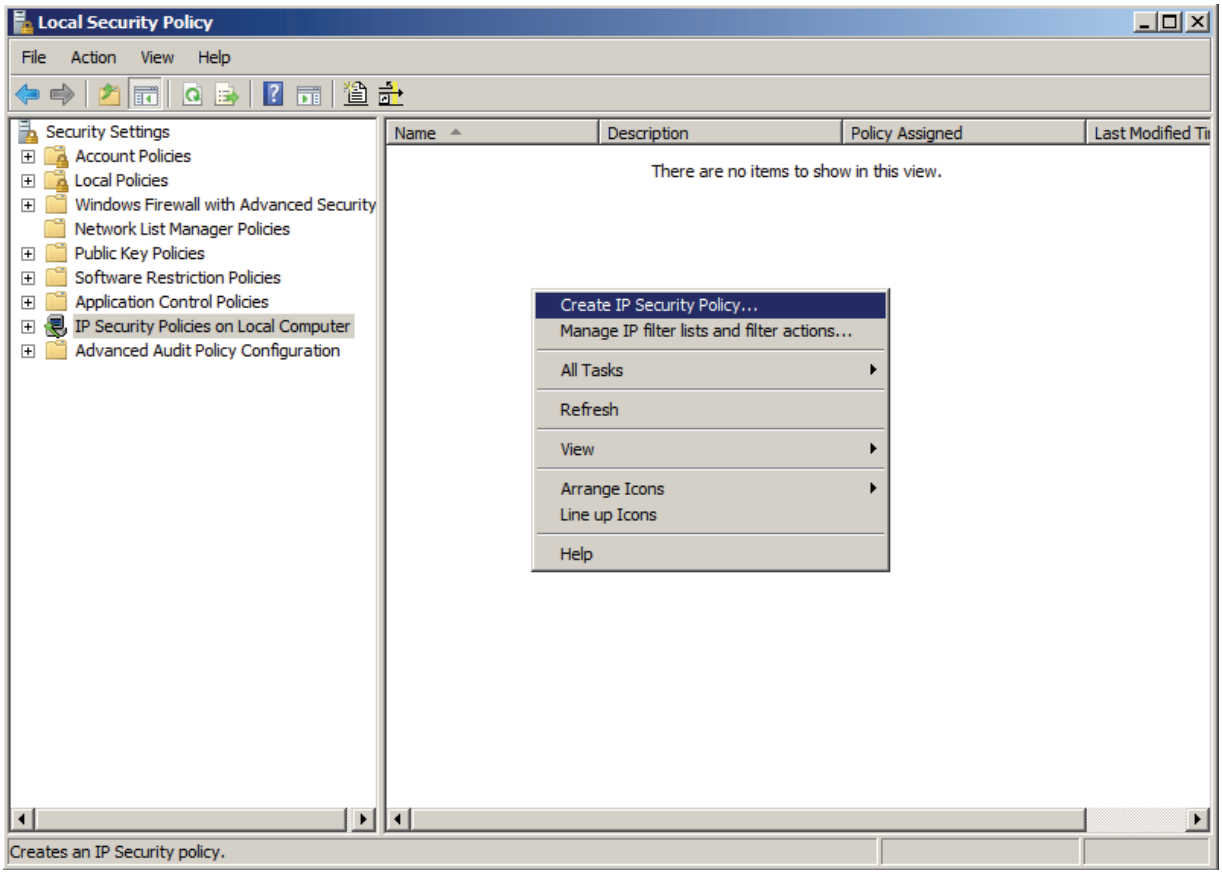
Here you can modify **IP filter** item's access right - Read Only, Refuse, Virtual Write and Full Access.

Now we successfully finished configuration of our iSCSI Target in iStorage Server.

Server Side Local Security Policy Setting

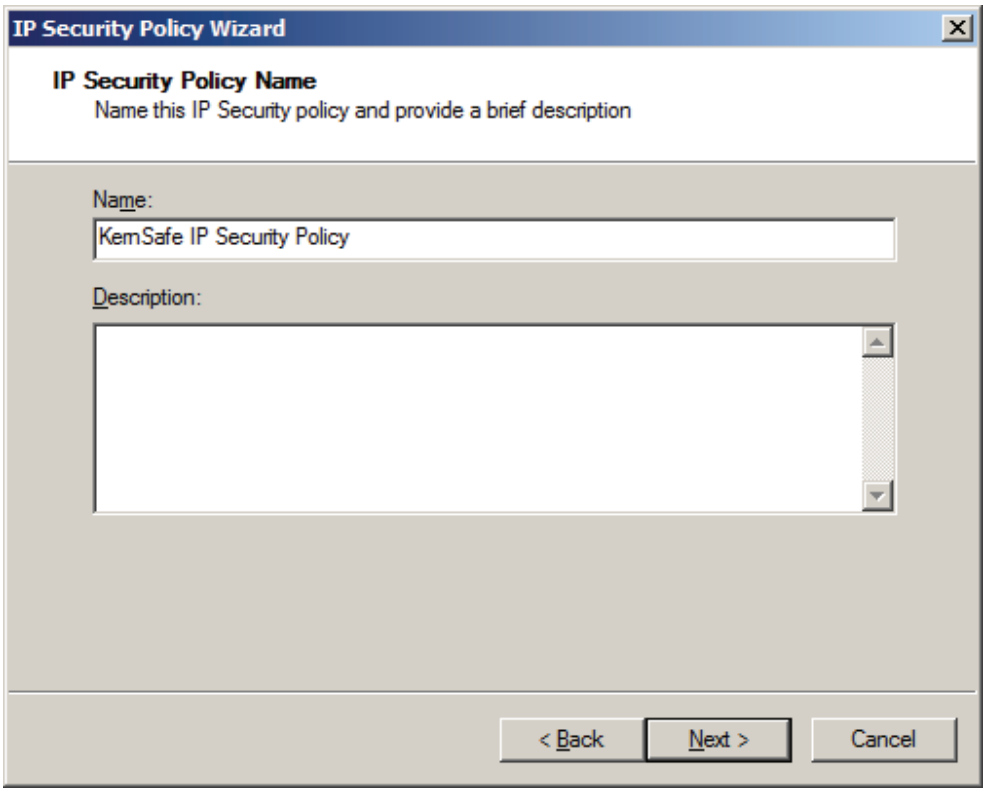
To access **Local Security Policy** under Windows Server 2008 R2, you can either type **Local Security Policy** in **Start search box** or you can navigate there by going:

Start --> **Control Panel** --> **Administrative Tools** --> **Local Security Policy**



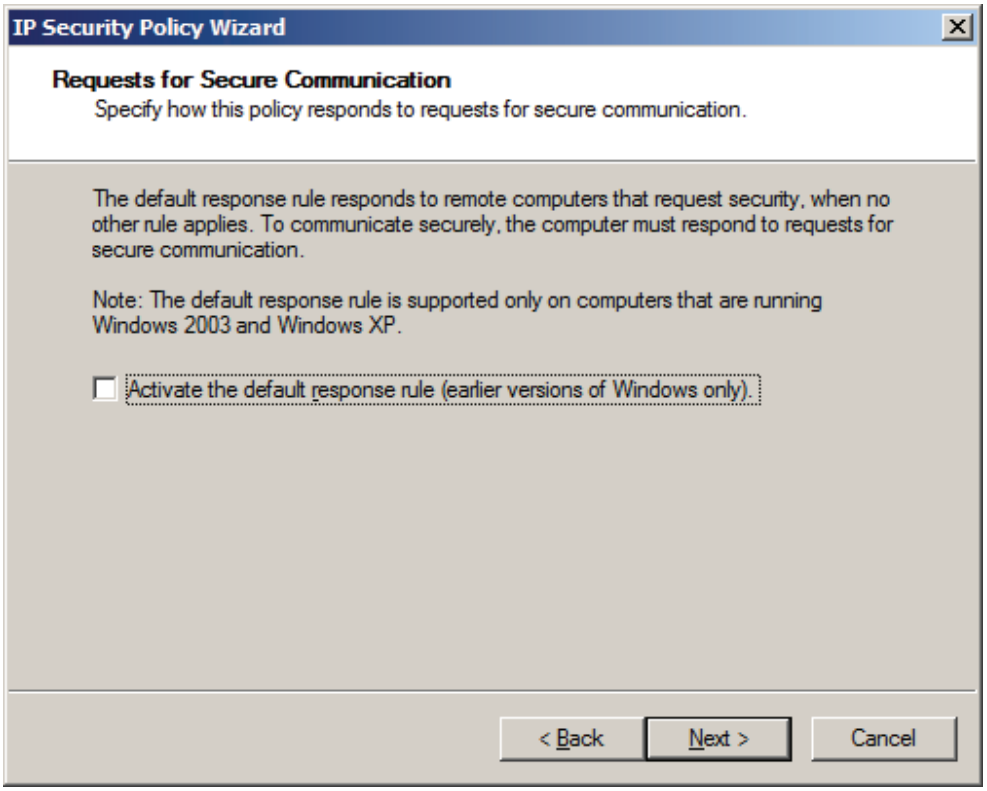
Select **IP Security Policies on Local** Computer in the left side panel, then select **Create IP Security Policy...** from the content menu, the **IP Security Policy Wizard** is shown.

Press **Next** button to continue.



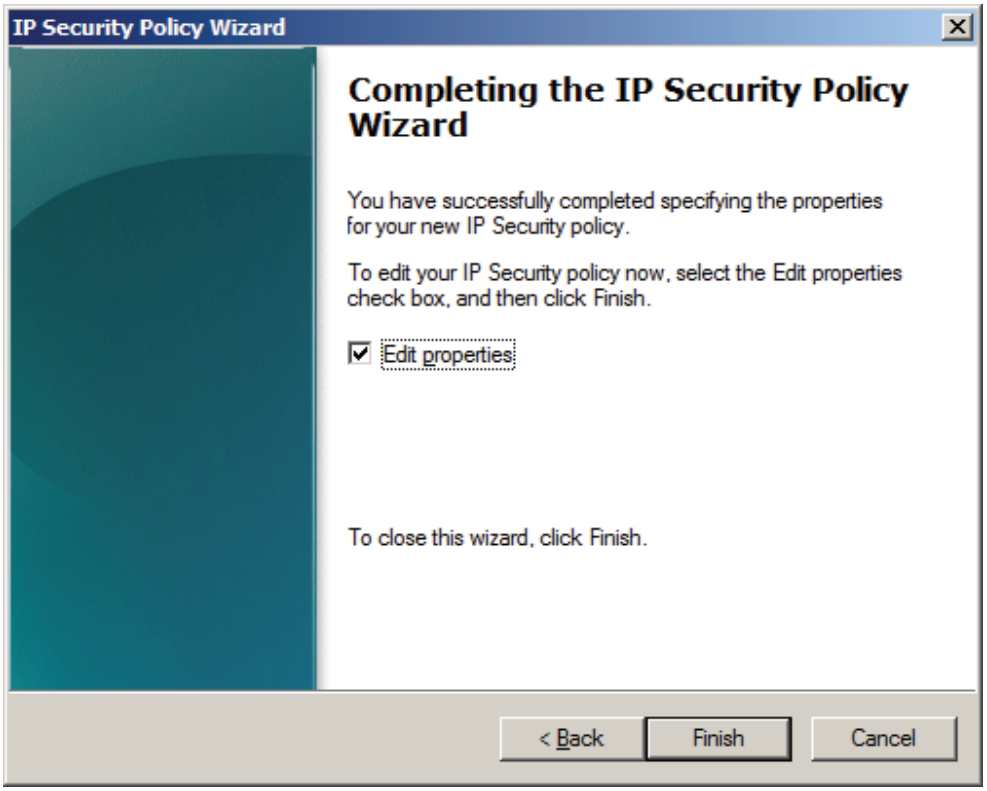
Type **KernSafe IP Security Policy**.
Press **Next** button to continue.

Specify how this policy responds to requests for secure communication.



Do not select Activate the default response rule.

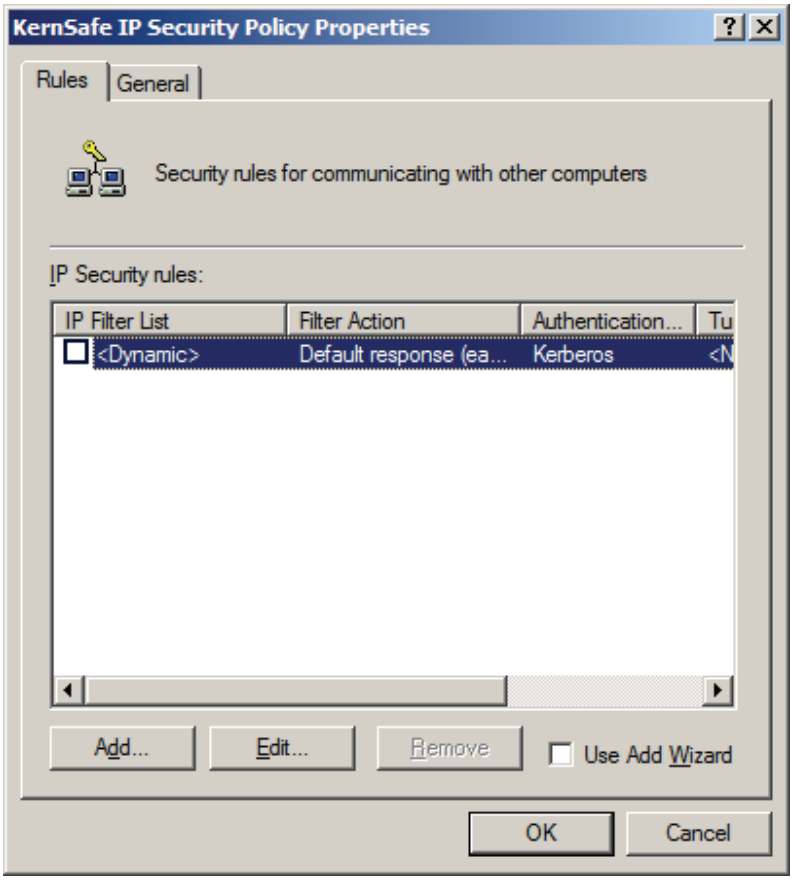
Press the **Next** button to continue.



Select the **Edit properties**.

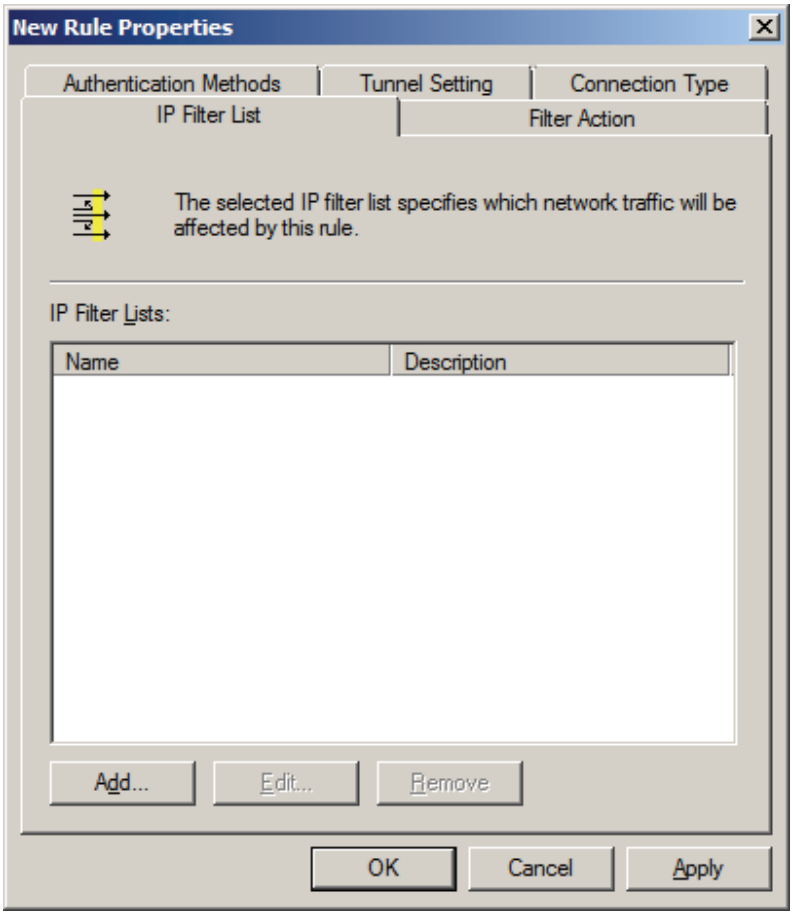
Press the **Finish** to continue.

Then the **KernSafe IP Security Policy Properties** dialog is shown.



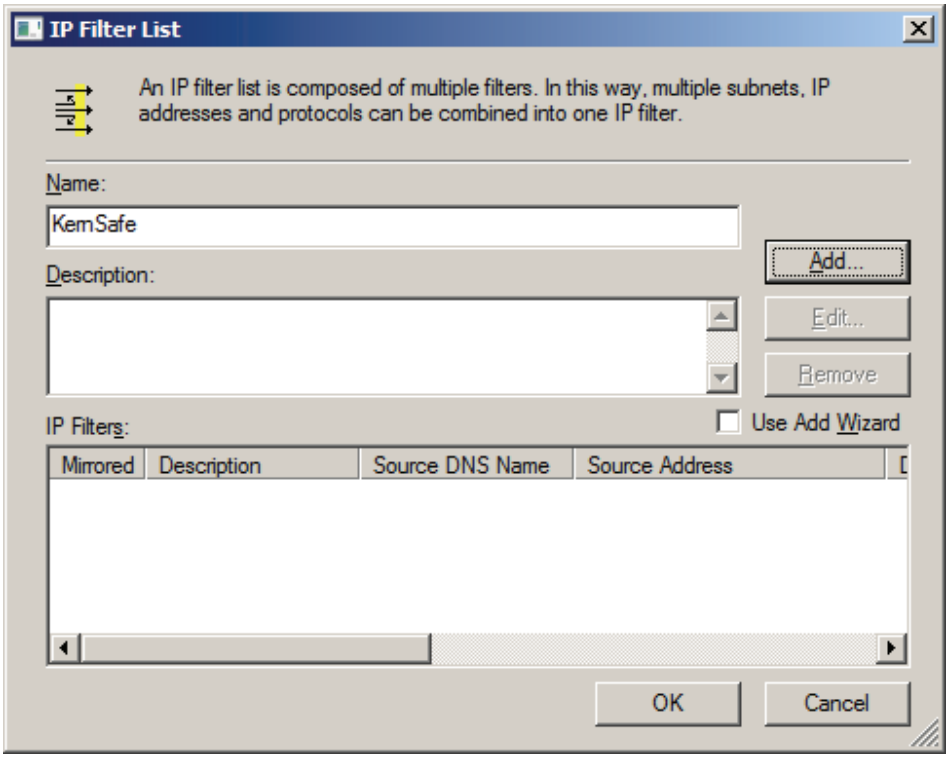
Do not select **Use Add Wizard**.

Press the **Add** button, the **New Role Properties** dialog is shown.



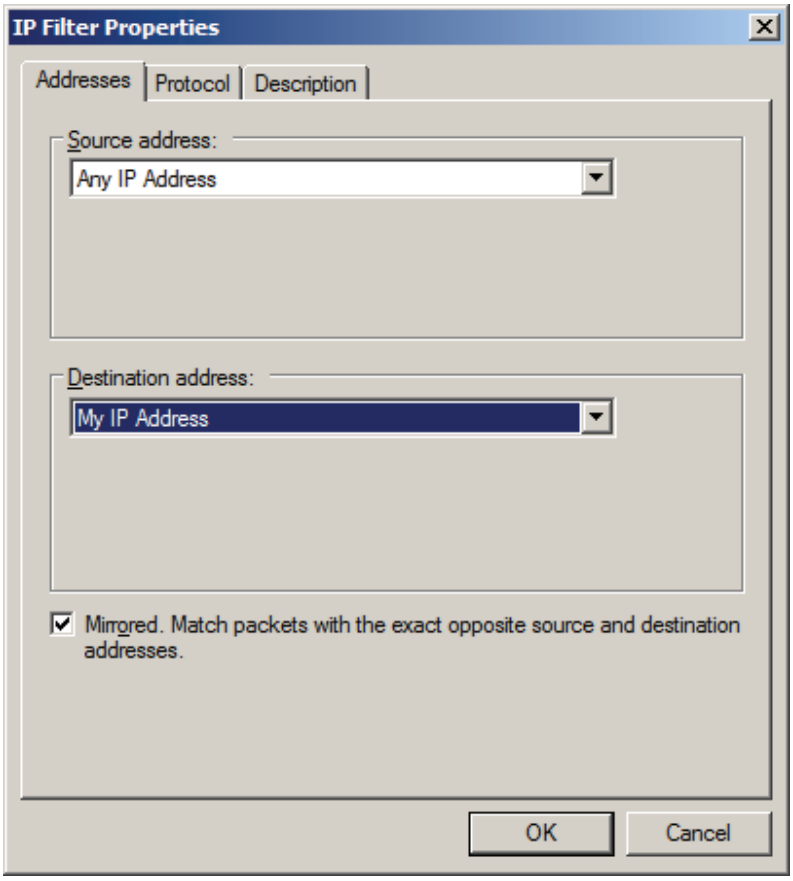
Press the **Add** button, the **IP Filter List dialog** is shown.

Input IP Filter name.



Type KernSafe in the **Name** and do not select **Use Add Wizard**.

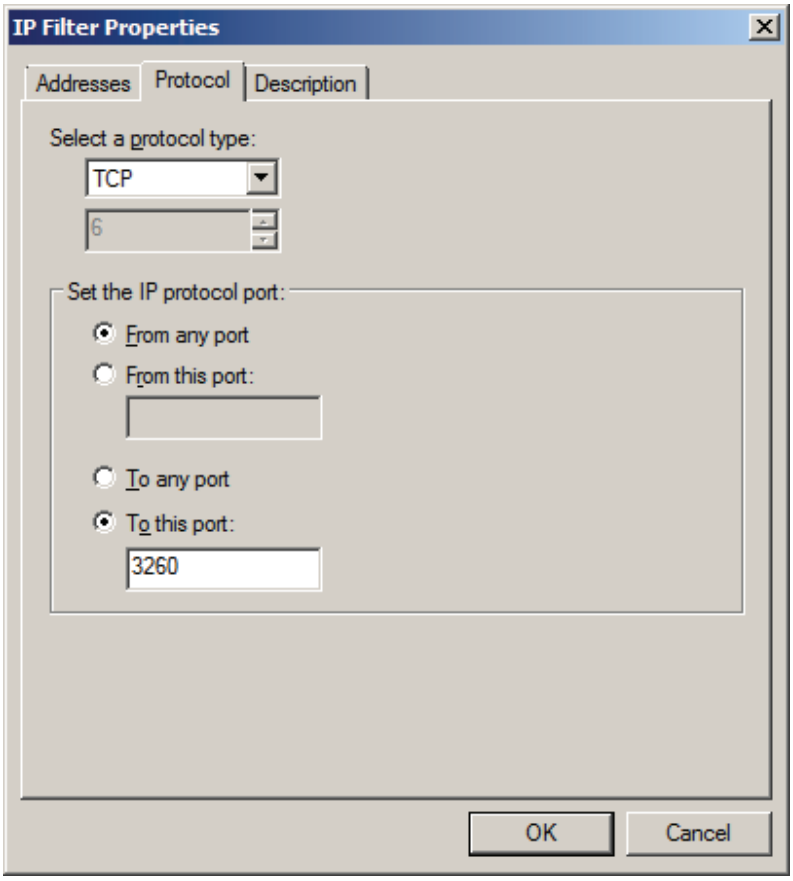
Press the **Add** button to continue.



Select **Any IP Address** in the **Source address**.

Select **My IP Address** in the **Destination address**.

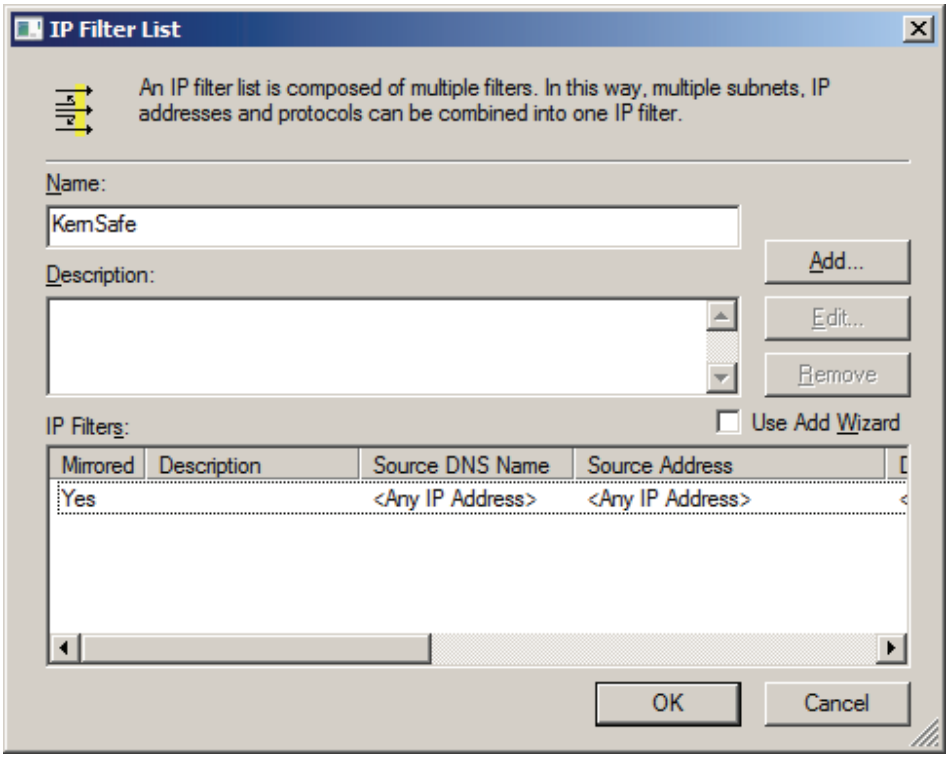
Then change to the **Protocol** tab.



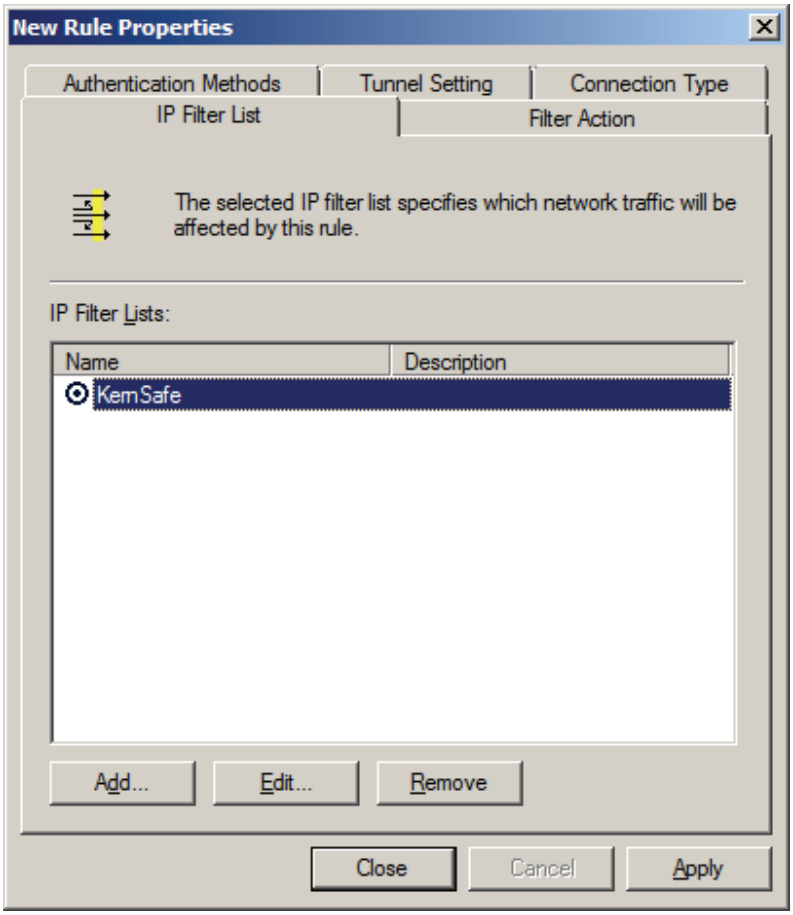
Select **TCP** in Select a protocol type field.

Type **3260** in the **To this port**.

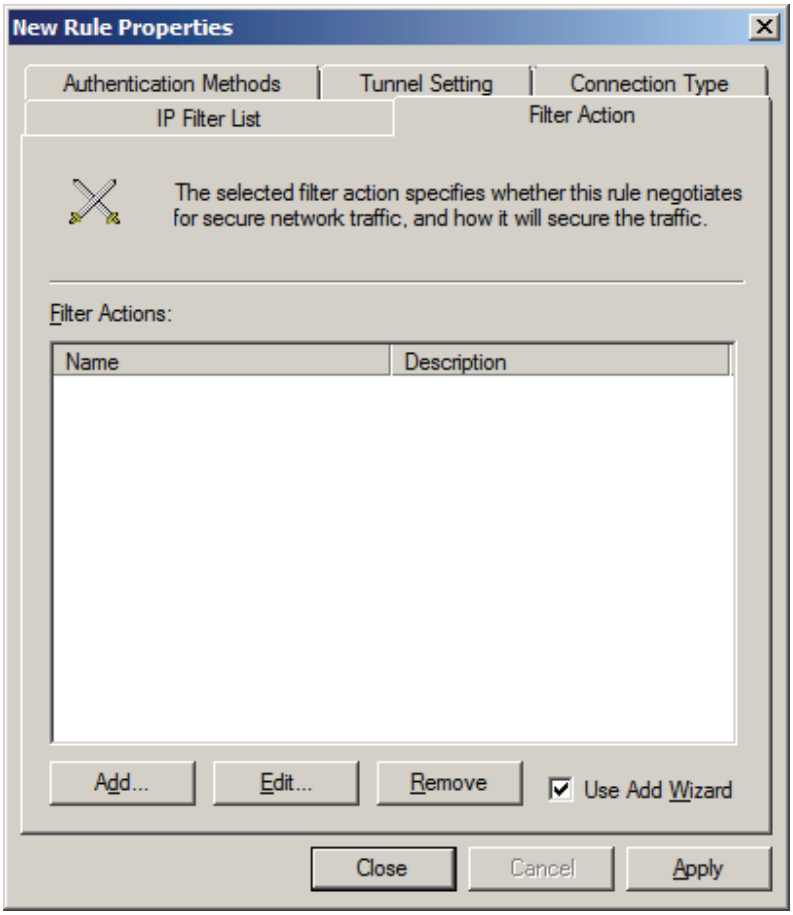
Press the **OK** button to continue.



Press the **OK** button to continue.



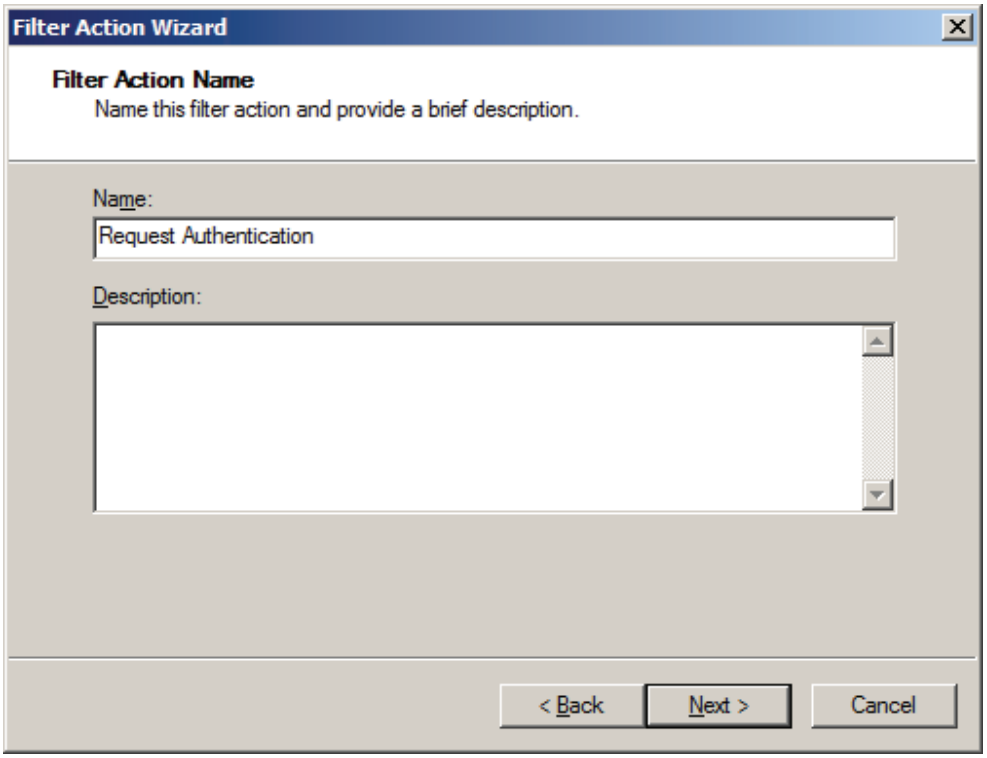
Select the **KernSafe** IP Filter item which we just created and change to **Filter Action** tab.



Leave **Use Add Wizard** checked and click on **Add…** button.

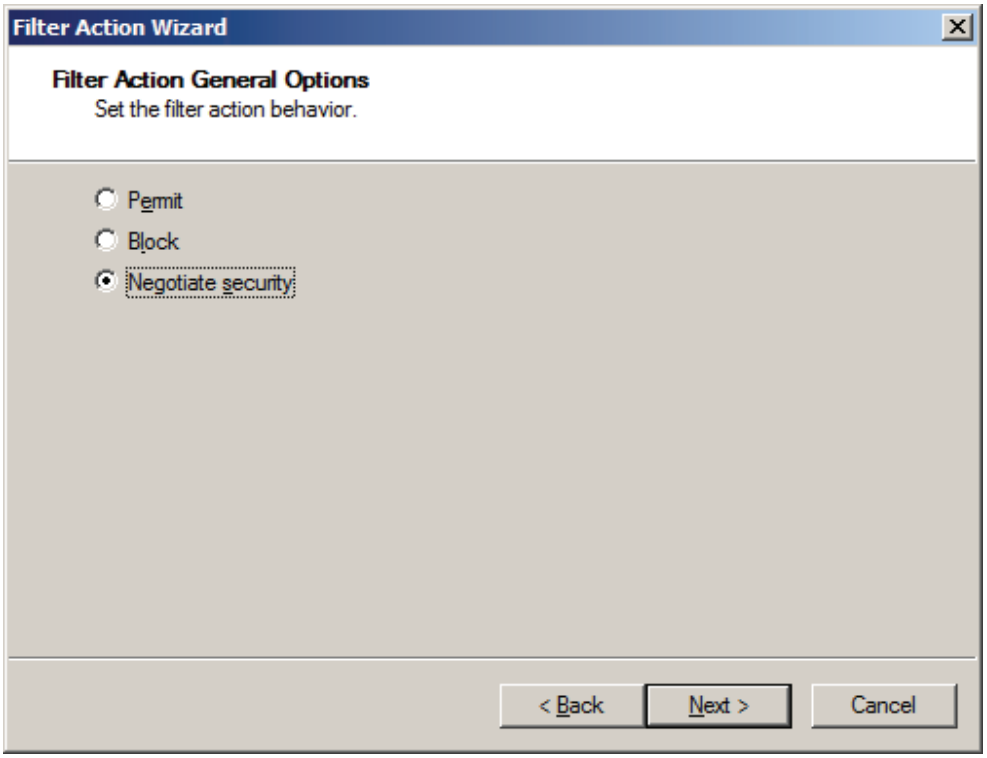
Filter Action Wizard is shown.

Press **Next** to continue.

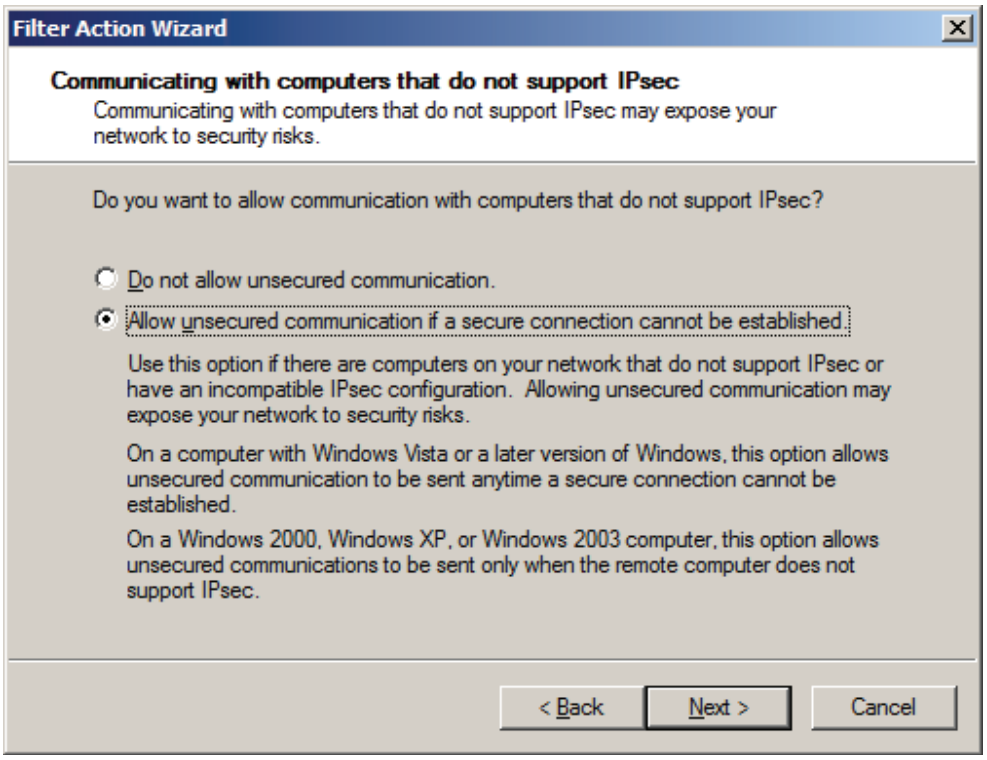


In **Name** field type **Request Authentication**.

Press **Next** button to continue.

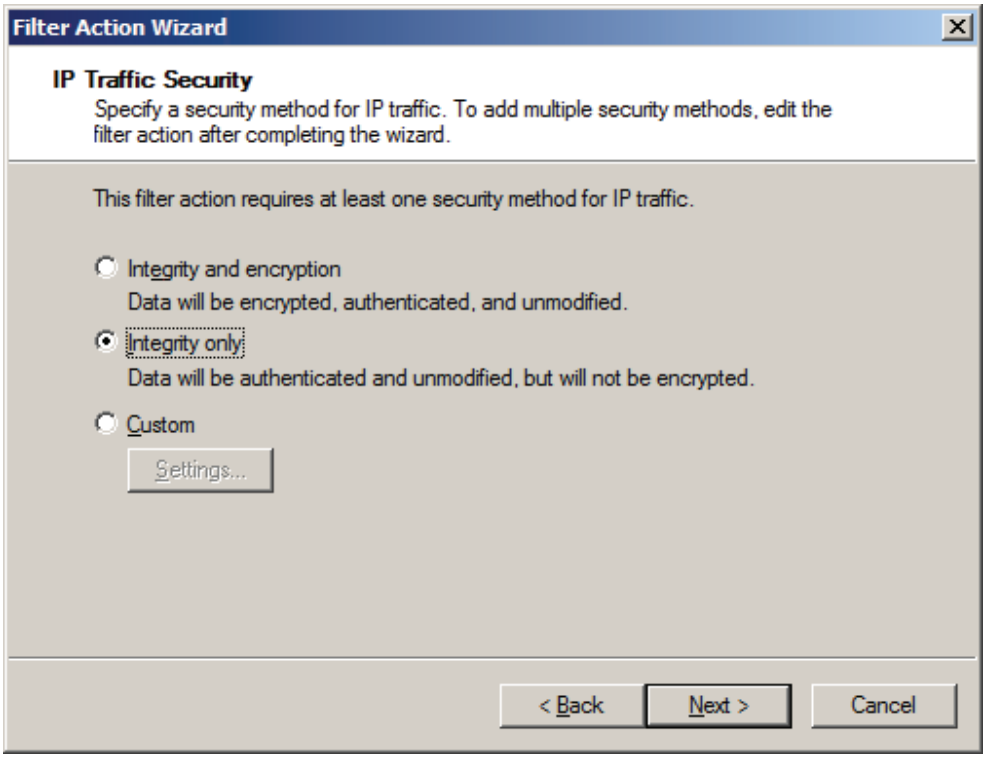


On the **Filter Action General Options page**, click **Negotiate security**, and then click **Next**.



On the **Communicating with computers that do not support IPsec page**, click **Allow unsecured communication if a secure connection cannot be established**.

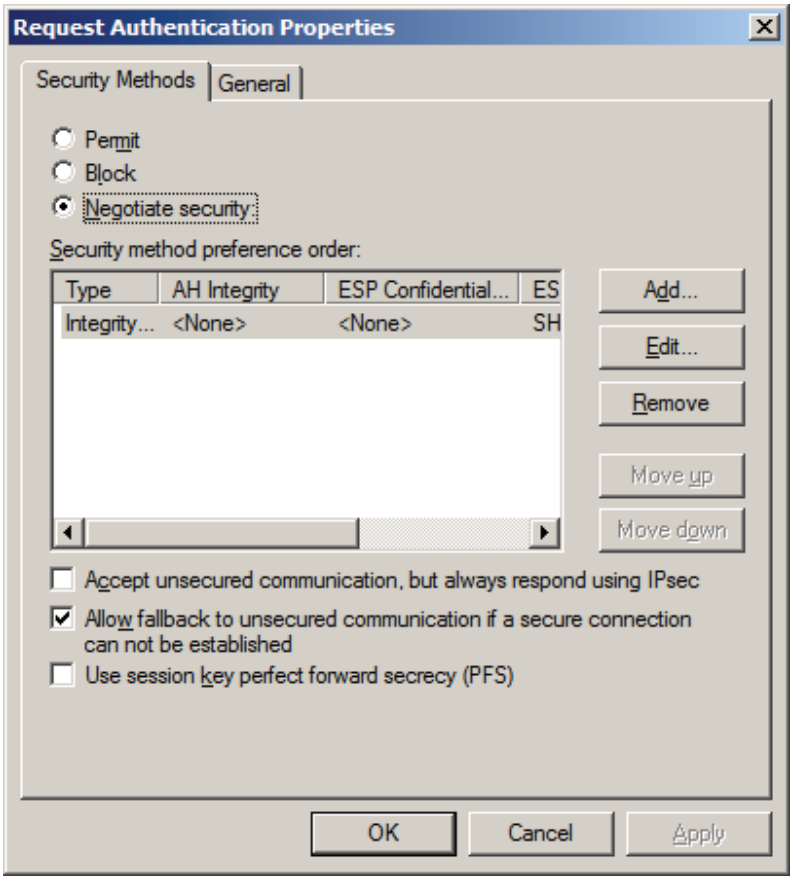
Press **Next** to continue.



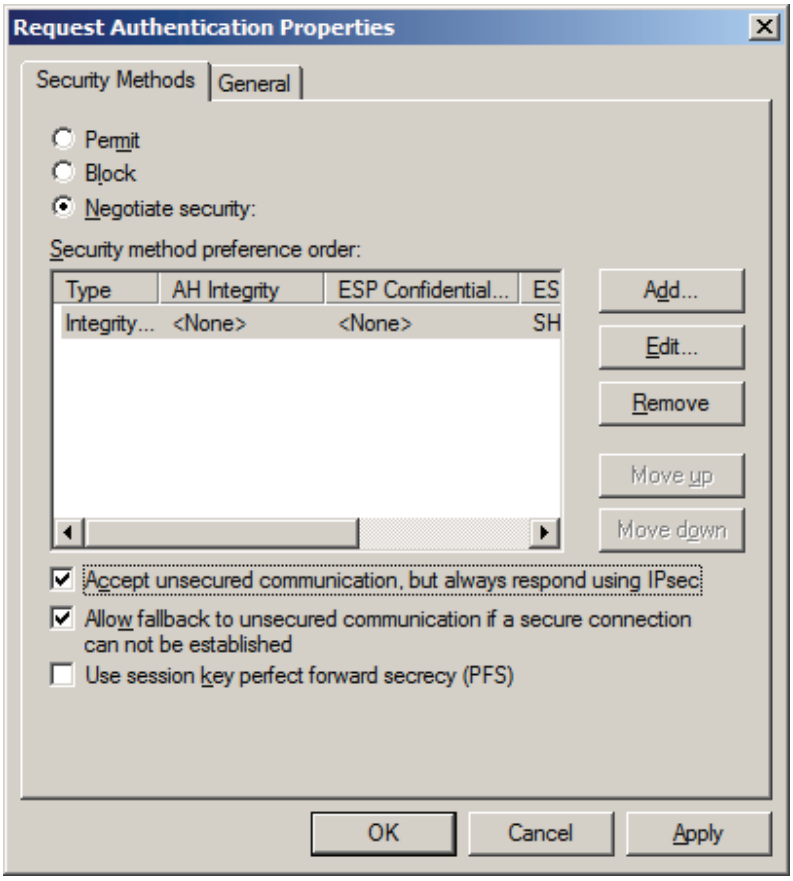
On the **IP Traffic Security** page, click **Integrity only**, and then click **Next**.

On the last page, select **Edit properties**, and then click **Finish**.

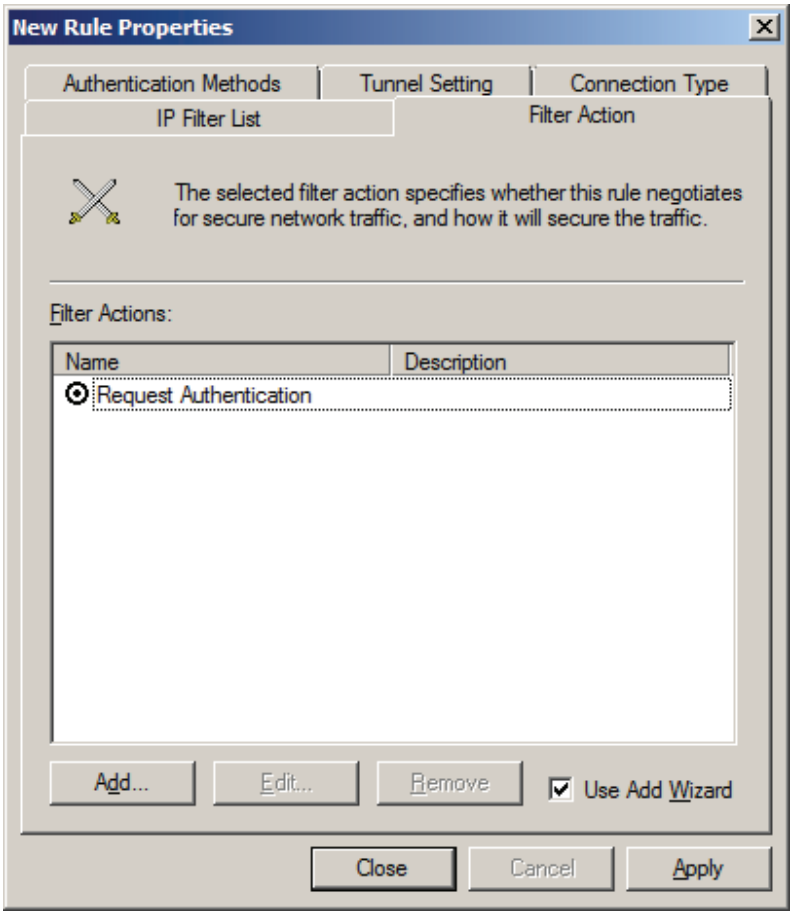
The **Properties** page for the filter action appears.



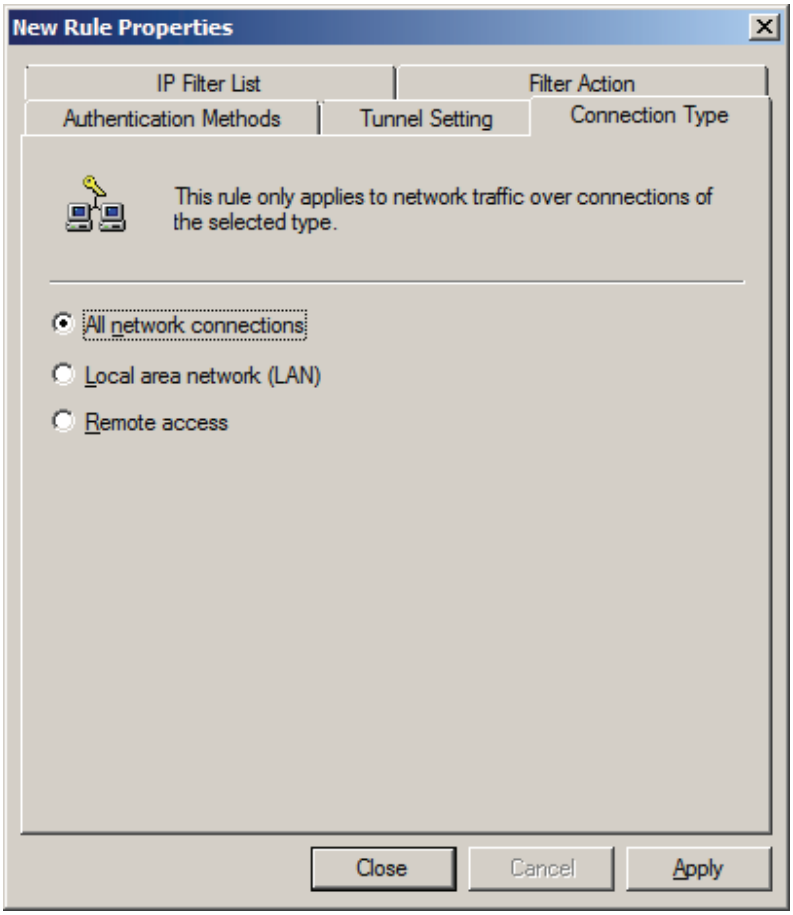
Select **Accept unsecured communication, but always respond using IPsec** to enable inbound fallback-to-clear behavior.



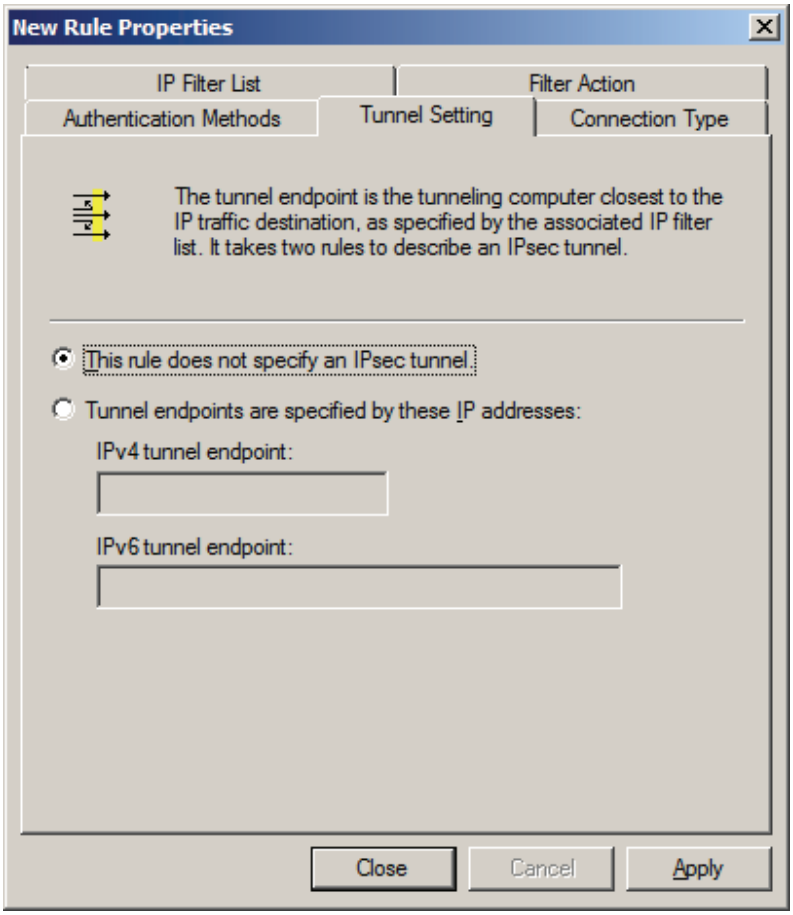
Press **Apply** button and then hit **OK.**



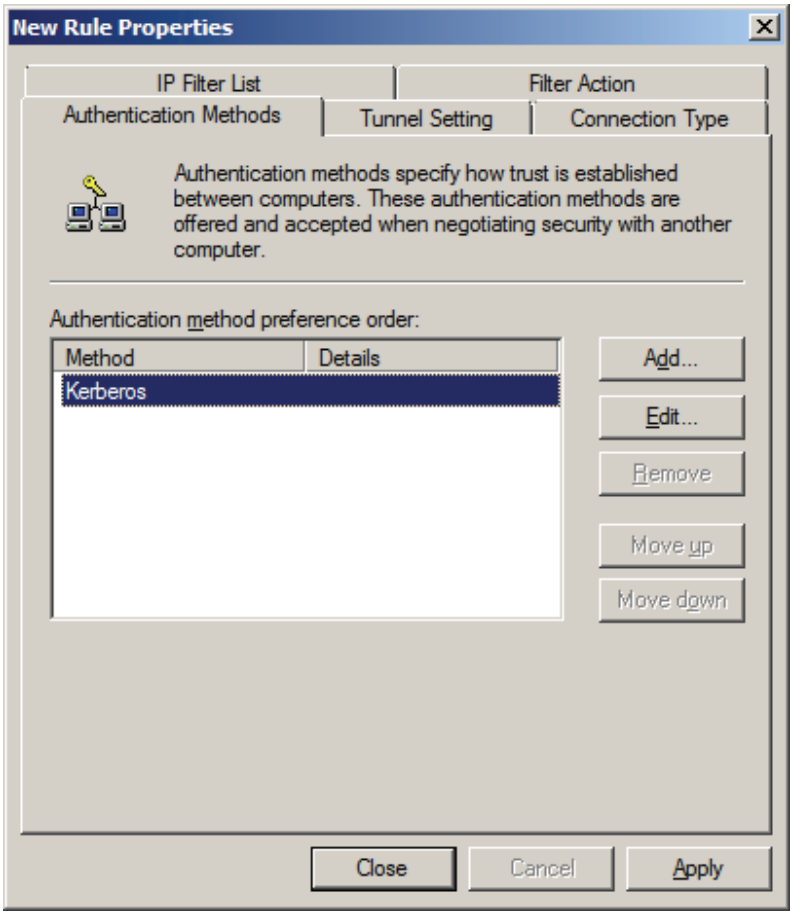
Switch to **Connection Type** tab.



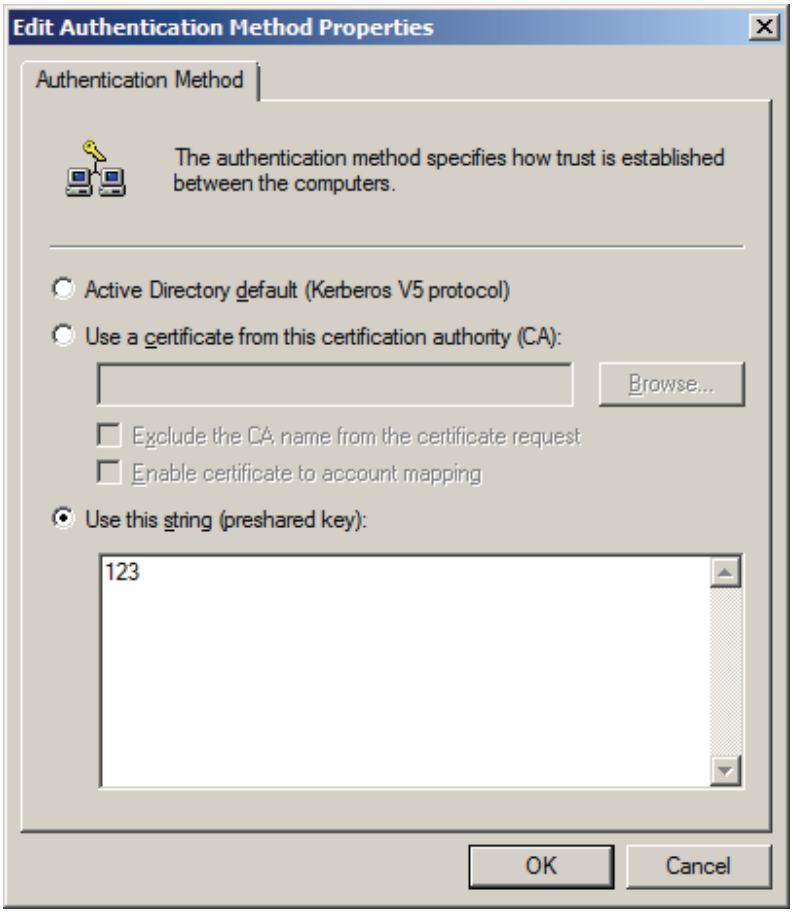
Select the **All network connections**, and then change to **Tunnel Setting** page.



Select **This rule does not specify an IPSec tunnel**, and then change to **Authentication Methods** tab.

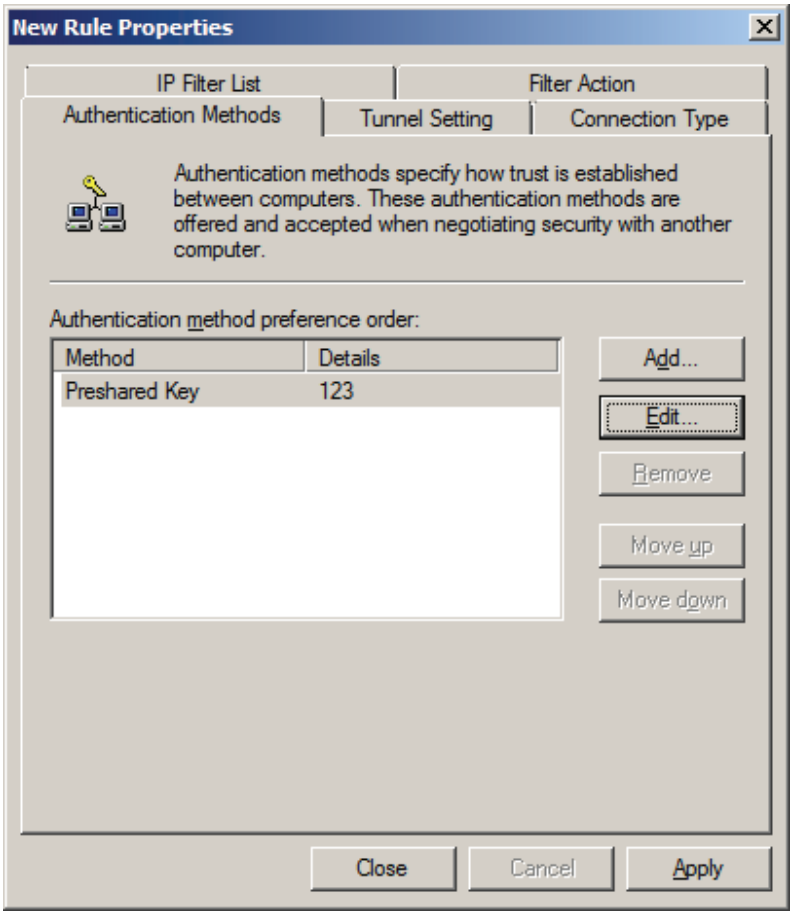


Select **Kerberos**, press the **Edit** button, the **Edit Authentication Method Properties** dialog is shown.

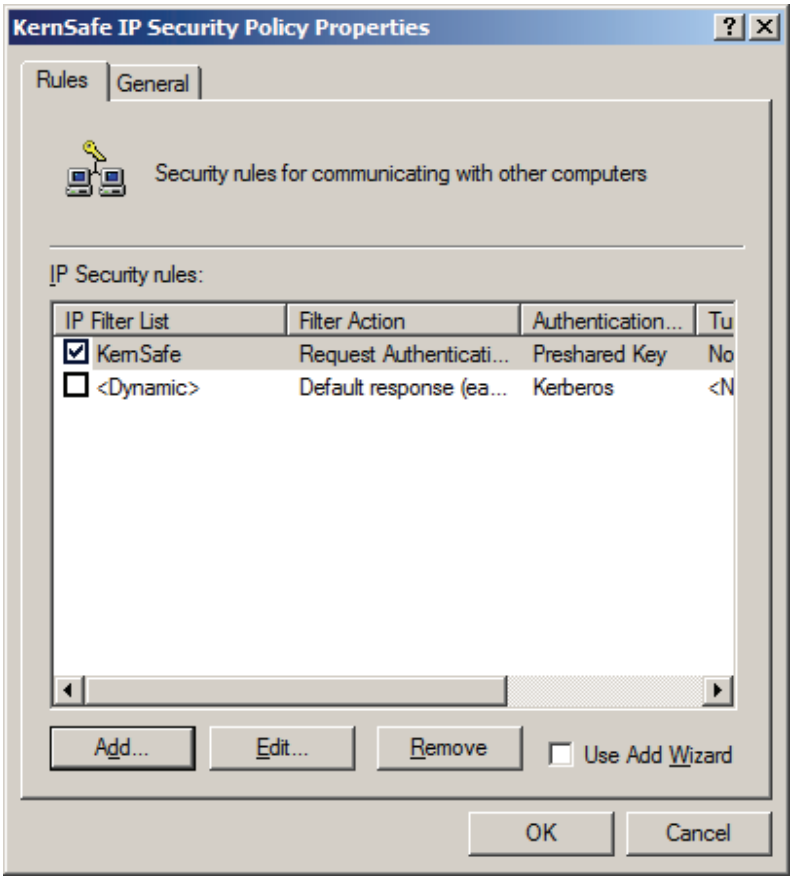


Select **Use this string (preshared key)**, type the preshared key, I take **123** as an example.

Click **OK** button to continue.

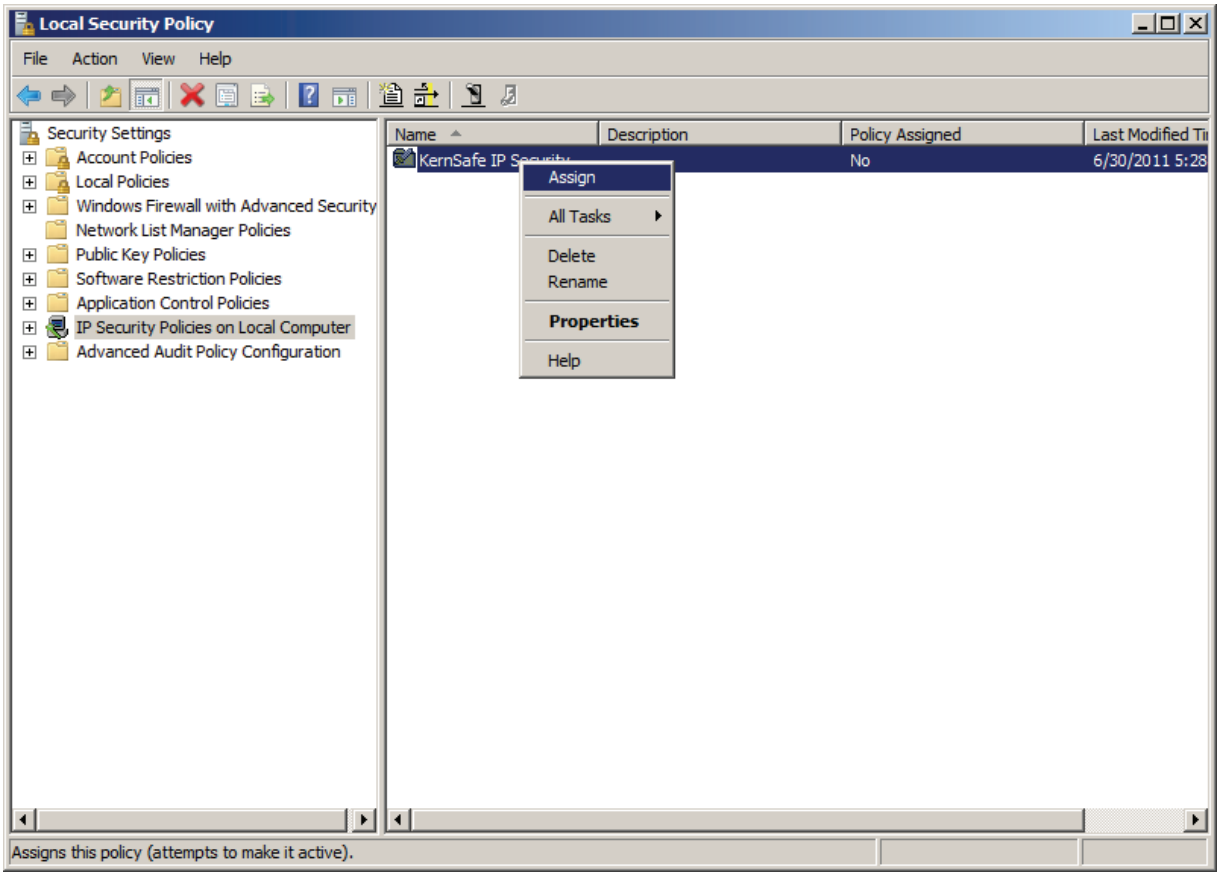


Press the **Apply** button to save settings and press the **OK** button to close this dialog.



Check **KernSafe** in the **IP Filter List** and then press the **OK** button to continue.

Back to **Local Security Settings** main interface.

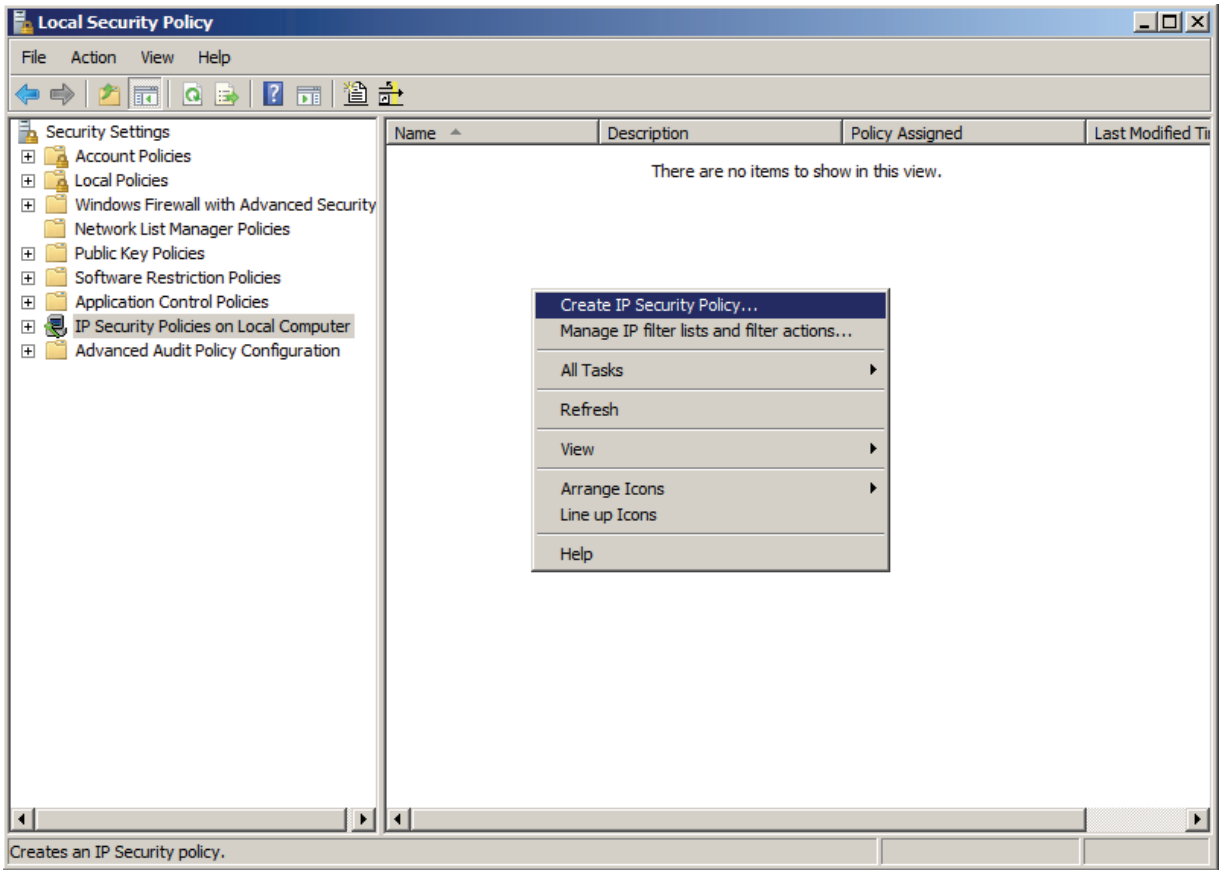


Right click on the **KernSafe IP Security Policy** item and then select **Assign** to make this item enabled.

Client Side Local Security Policy Setting

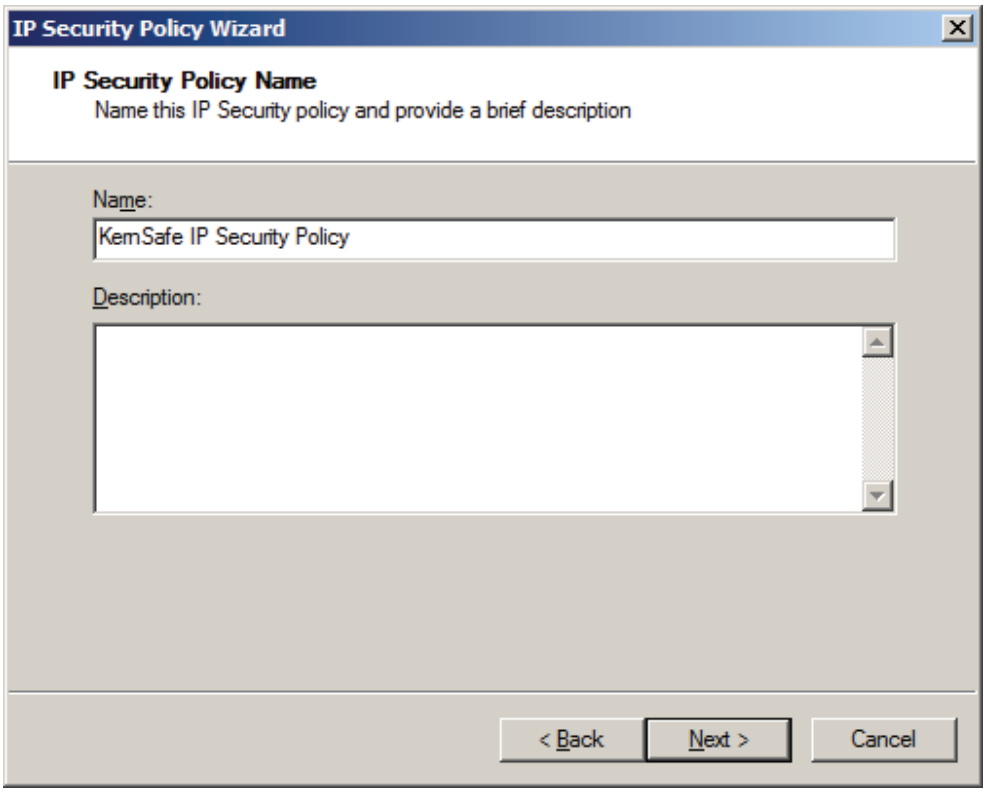
To access **Local Security Policy** under Windows Server 2008 R2, you can either type **Local Security Policy** in **Start search box** or you can navigate there by going:

Start --> **Control Panel** --> **Administrative Tools** --> **Local Security Policy**



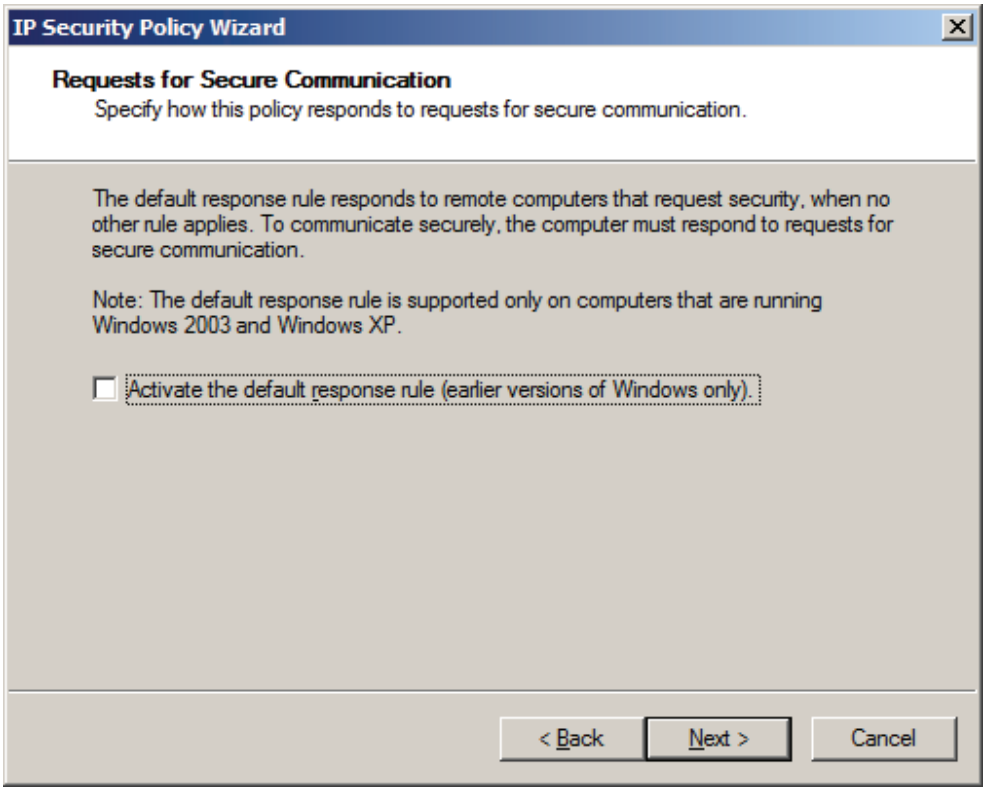
Select **IP Security Policies on Local** Computer in the left side panel, then select **Create IP Security Policy...** from the content menu, the **IP Security Policy Wizard** is shown.

Press **Next** button to continue.



Type **KernSafe IP Security Policy**.
Press **Next** button to continue.

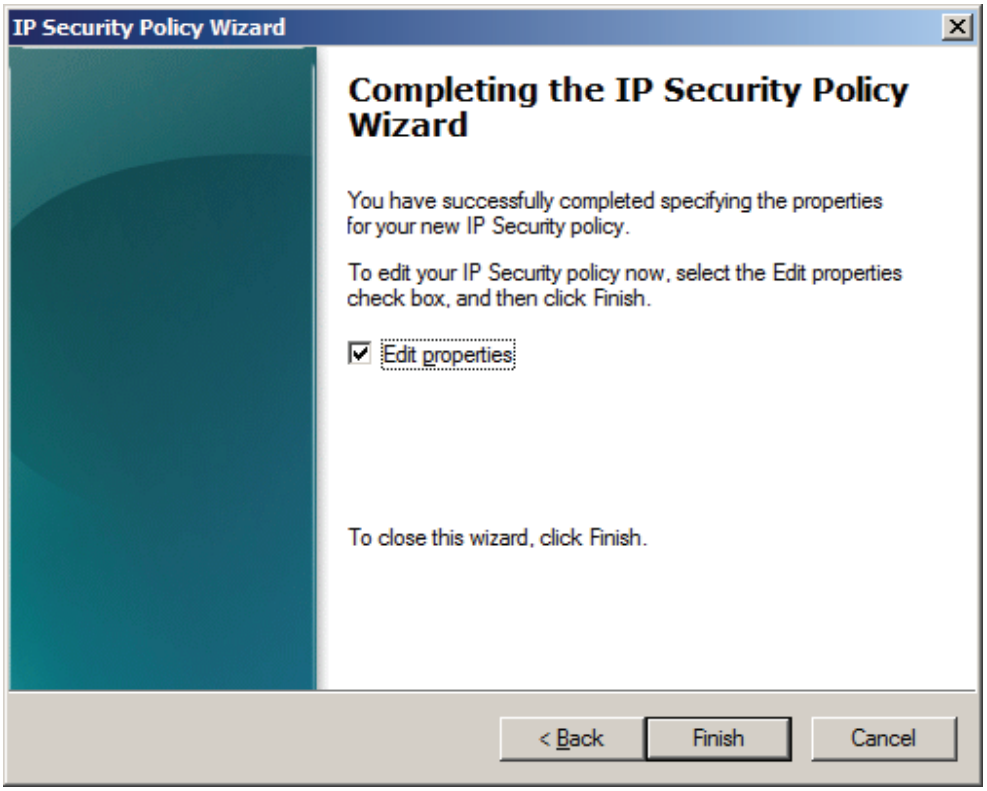
Specify how this policy responds to requests for secure communication.



Do not select Activate the default response rule.

Press the **Next** button to continue.

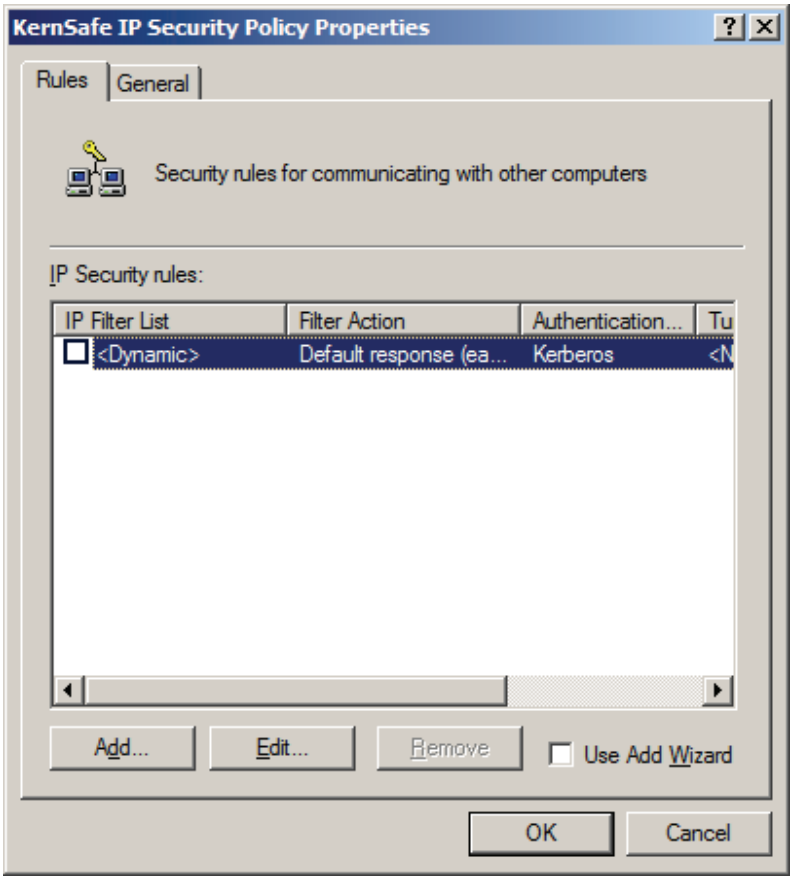
Completing the IP Security Policy Wizard.



Select the **Edit properties** by default.

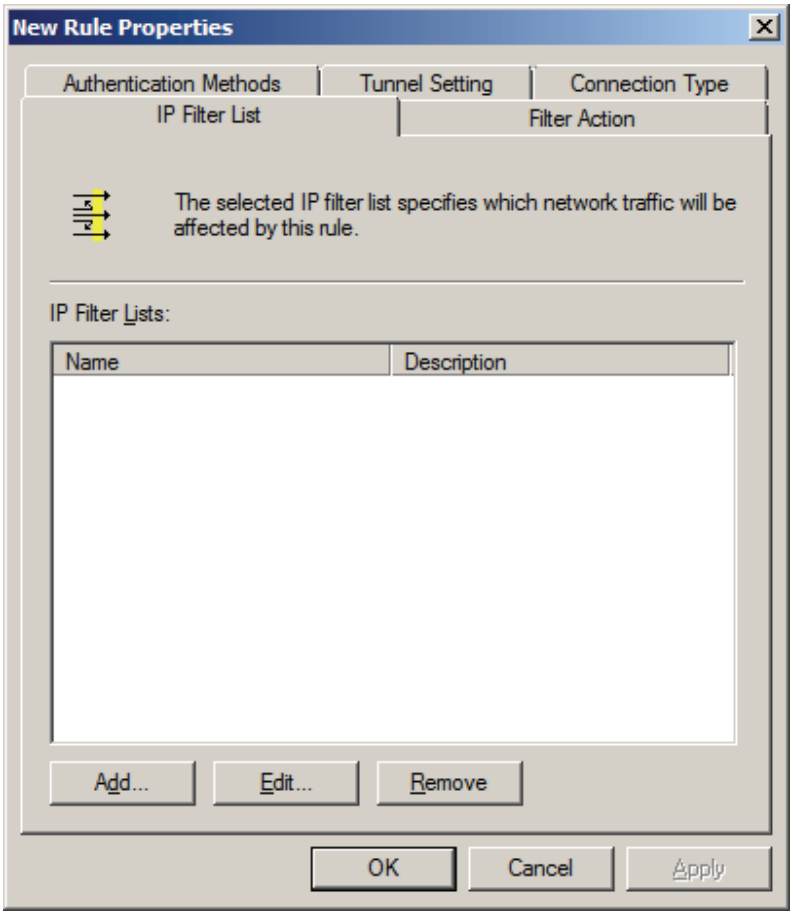
Press the **Finish** to continue.

Then the **KernSafe IP Security Policy Properties** dialog is shown.



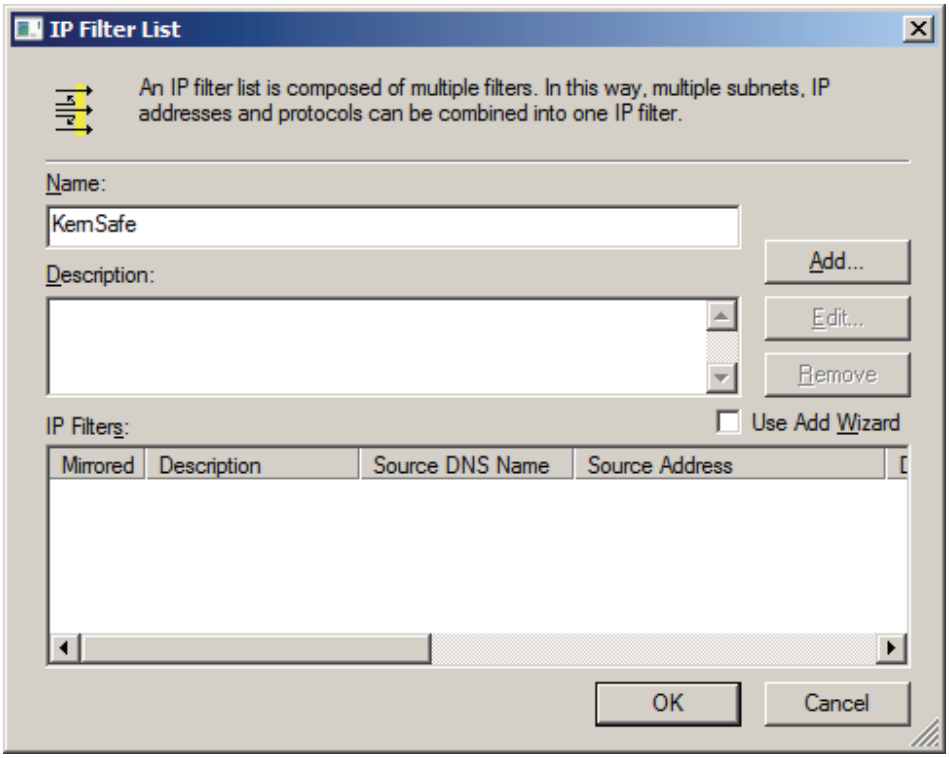
Don’t select the **Use Add Wizard** option.

Press the **Add** button, the **New Rule Properties** dialog is shown.



Press the **Add** button to continue.

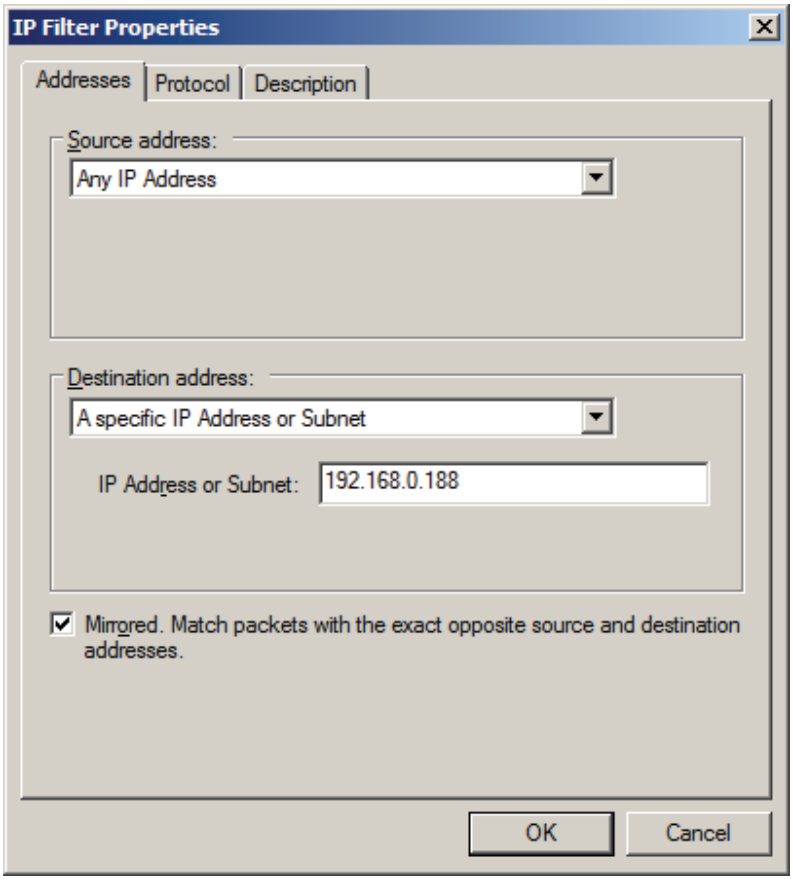
Setting **IP Filter List**.



Type the name of IP filter.

Don’t select the **Use Add Wizard** option.

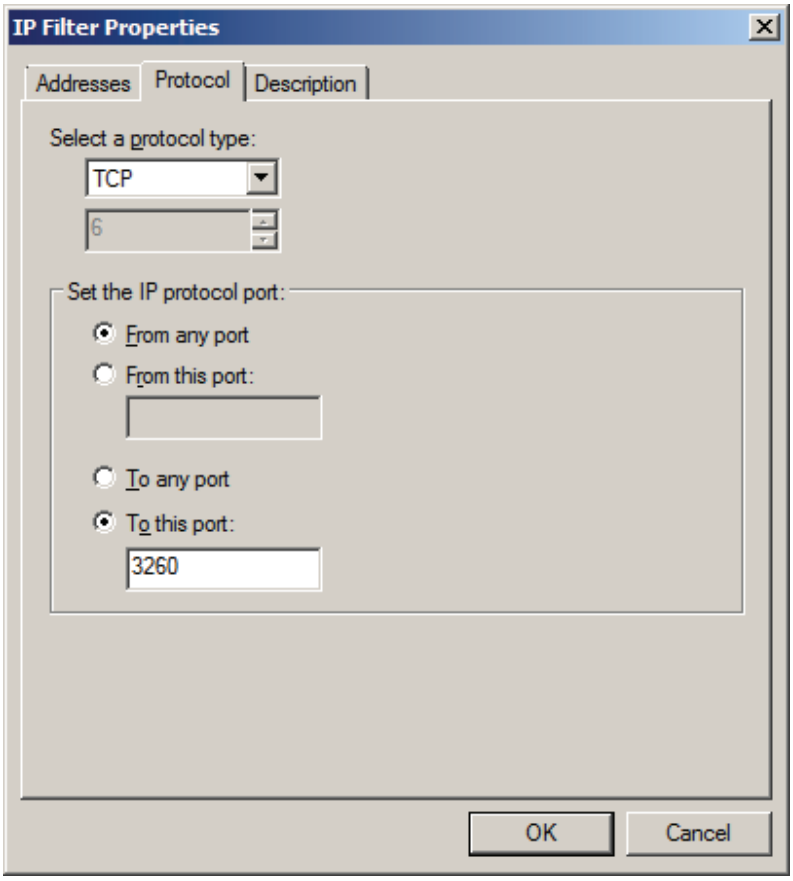
Press the **Add** button, the **IP Filter Properties** dialog is shown.



Select **My IP Address** in **Source address** category.
Select **A specific IP Address or Subnet** in **Destination address** category, and then type the **IP address** of your server machine.

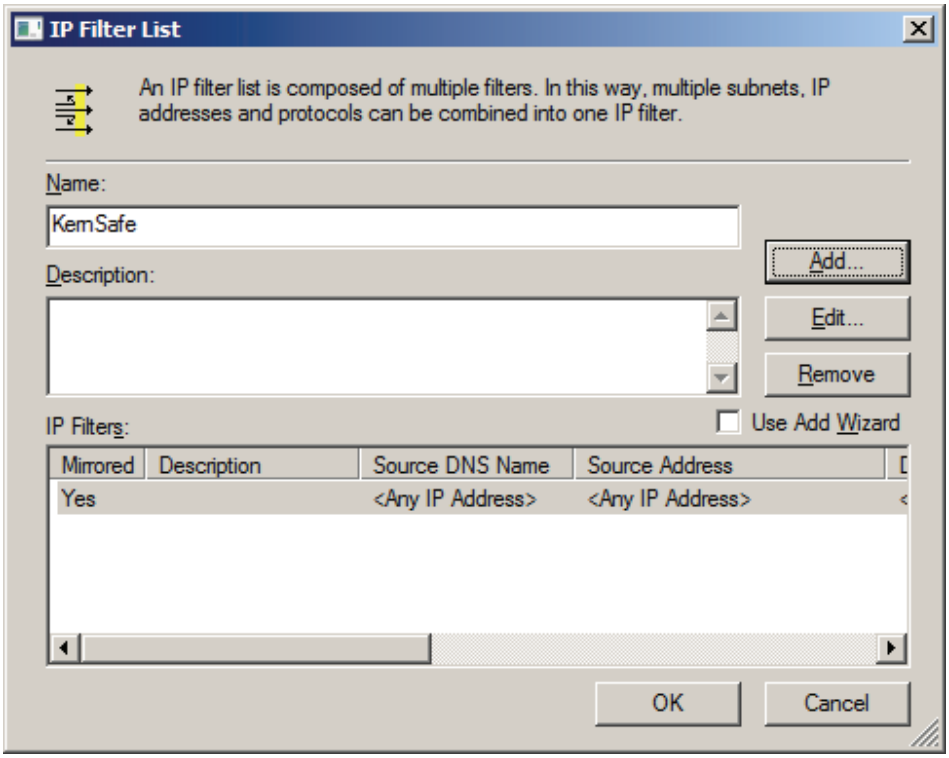
Switch to the **Protocol** tab to continue.

Set protocol properties.

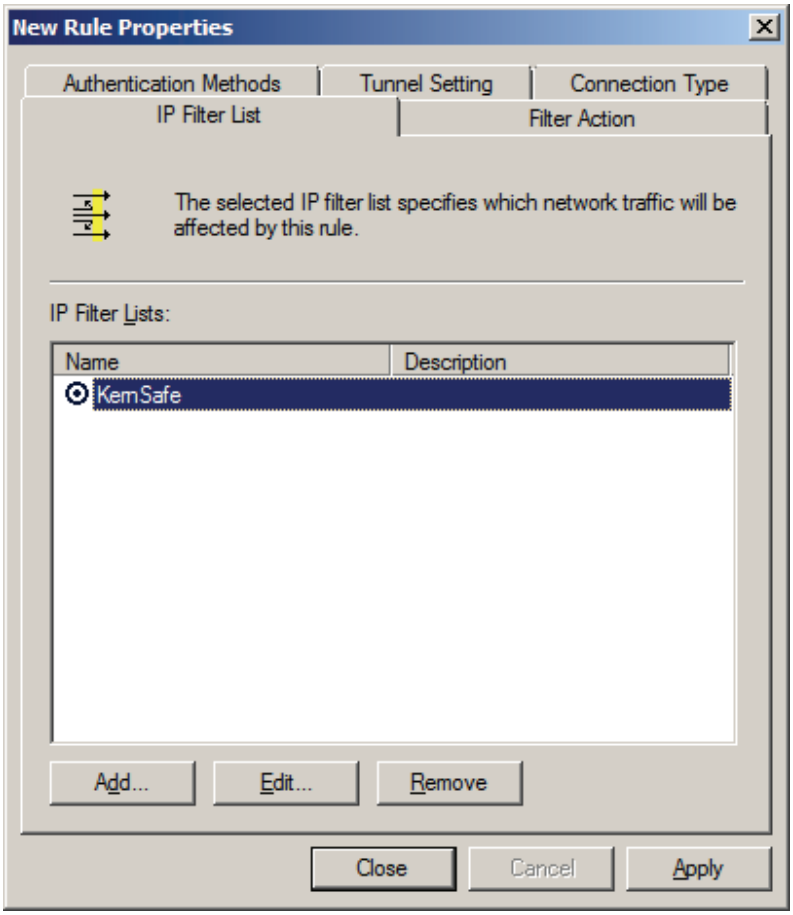


Select **TCP** in the **Select a protocol type** categories, and then type **3260** in the **To this port**.
Press the **OK** button to continue.

Now we come back to the **IP Filter List** interface.

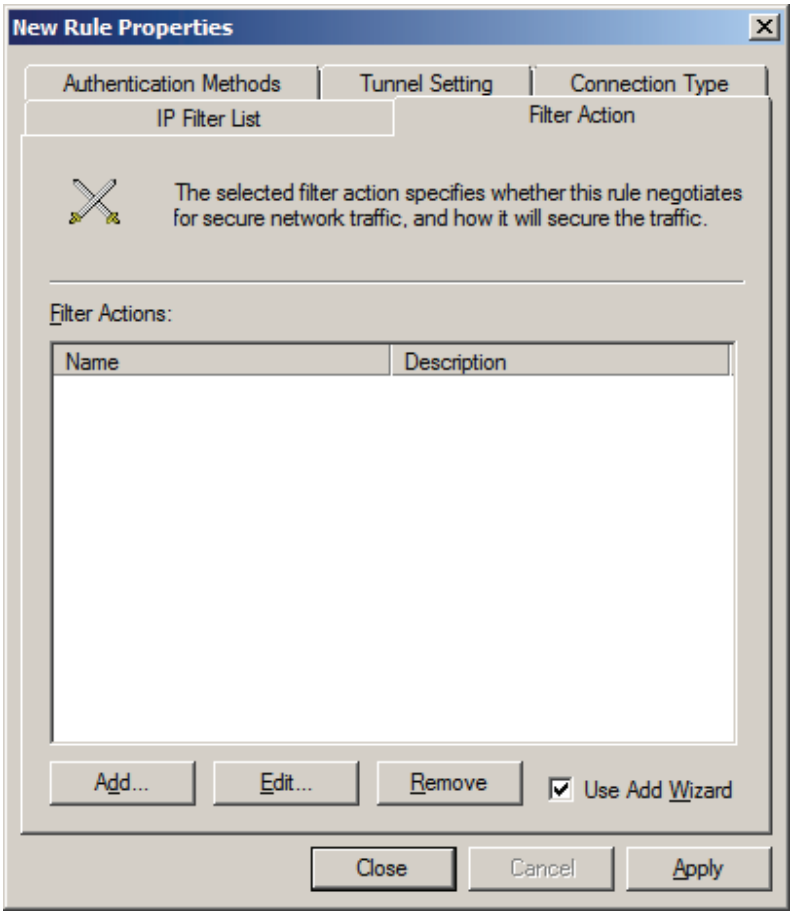


Press the **OK** button to complete the IP Filter Item creation.



Select the KernSafe IP Filter item we just create. Change to **Filter Action** tab.

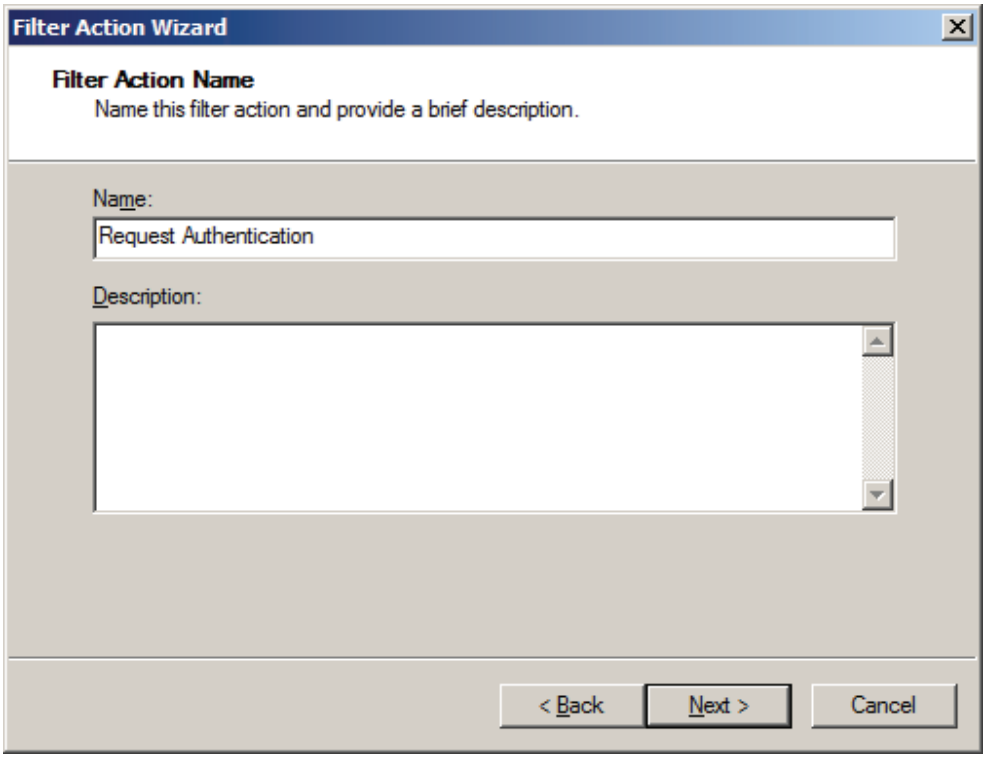
Select the **KernSafe** IP Filter item which we just created and change to **Filter Action** tab.



Leave **Use Add Wizard** checked and click on **Add…** button.

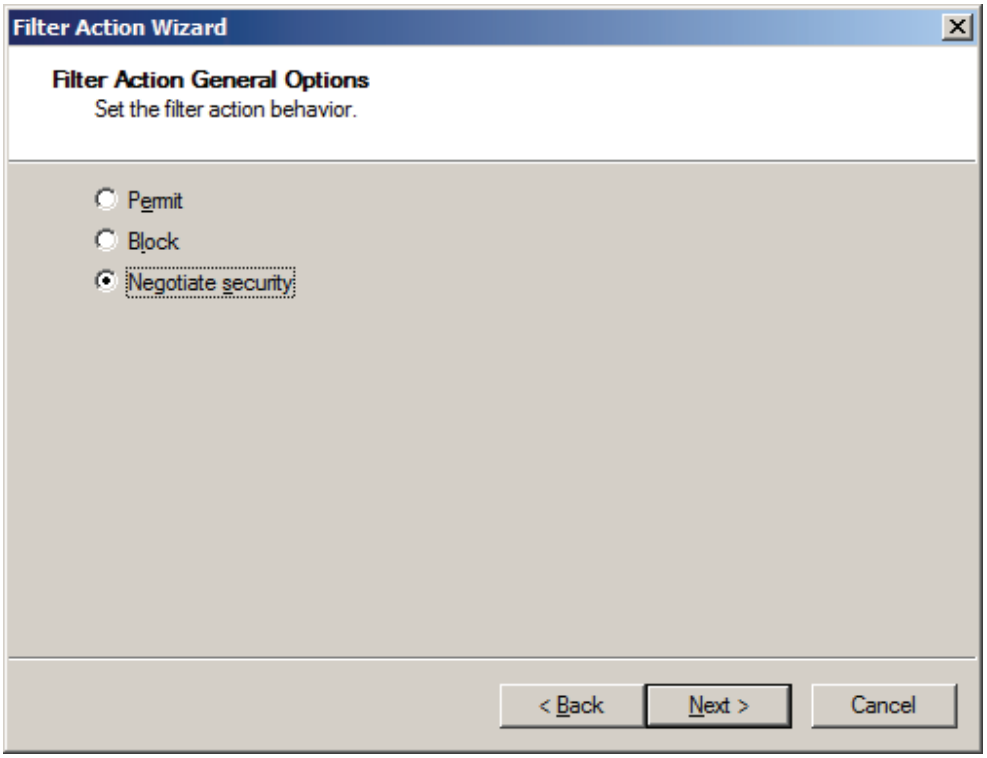
Filter Action Wizard is shown.

Press **Next** to continue.

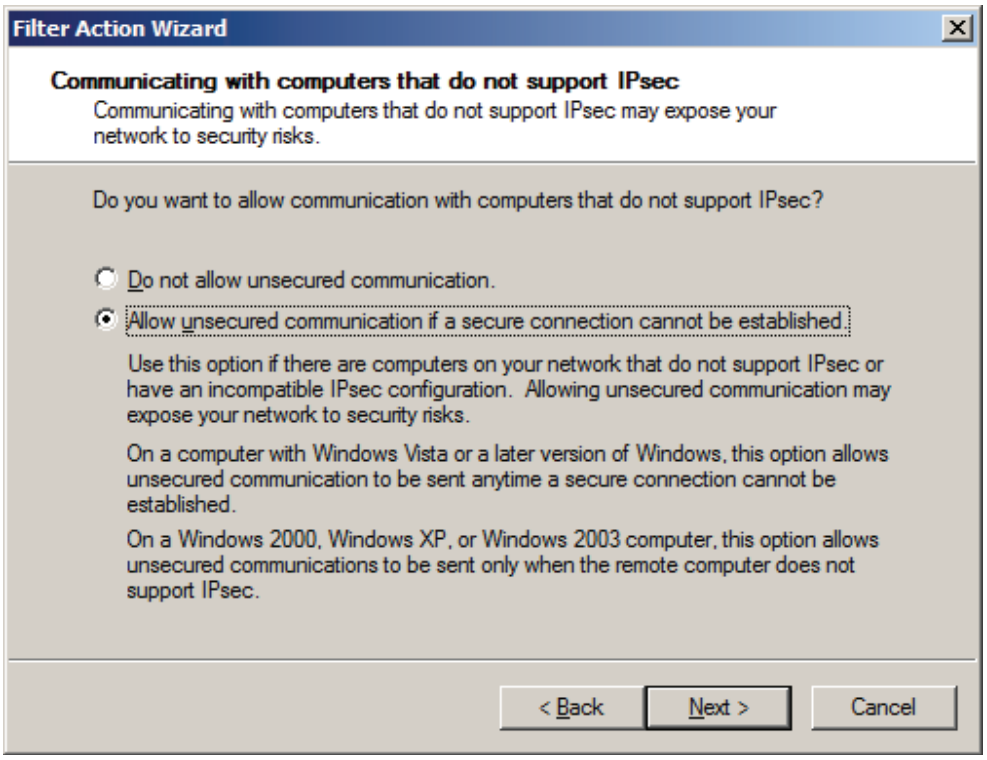


In **Name** field type **Request Authentication**.

Press **Next** button to continue.

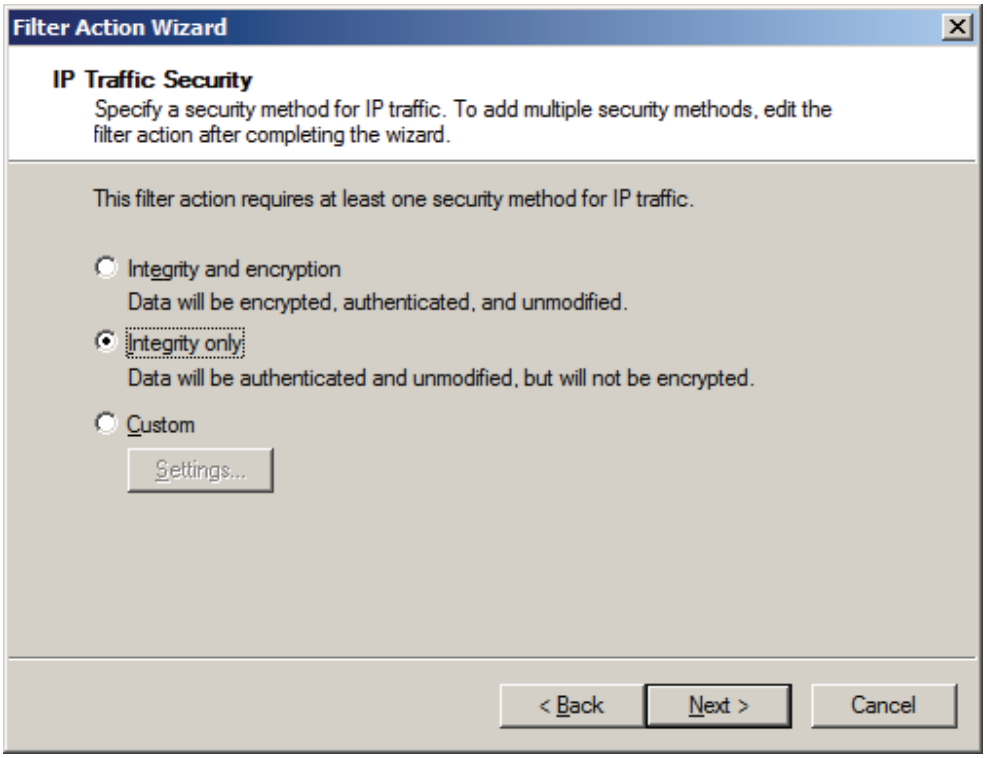


On the **Filter Action General Options page**, click **Negotiate security**, and then click **Next**.



On the **Communicating with computers that do not support IPsec page**, click **Allow unsecured communication if a secure connection cannot be established**.

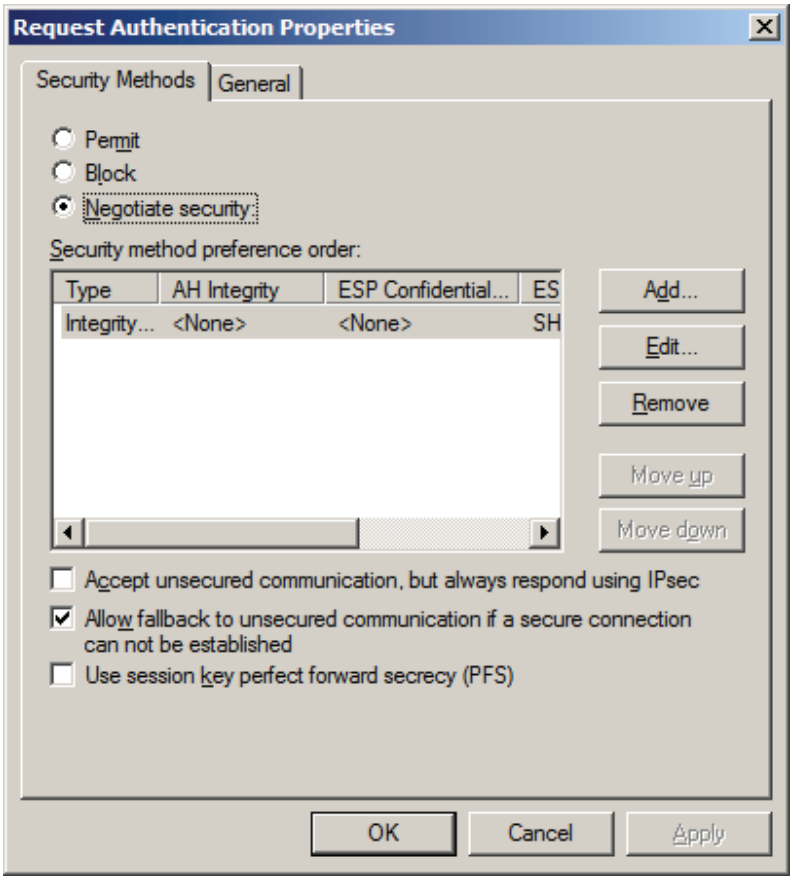
Press **Next** to continue.



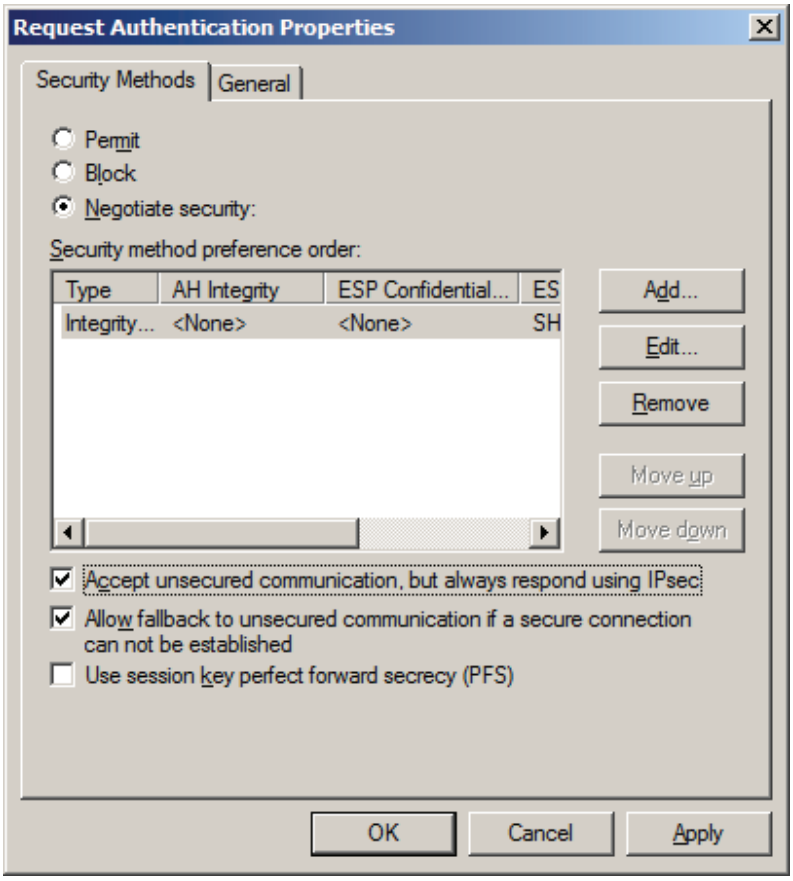
On the **IP Traffic Security** page, click **Integrity only**, and then click **Next**.

On the last page, select **Edit properties**, and then click **Finish**.

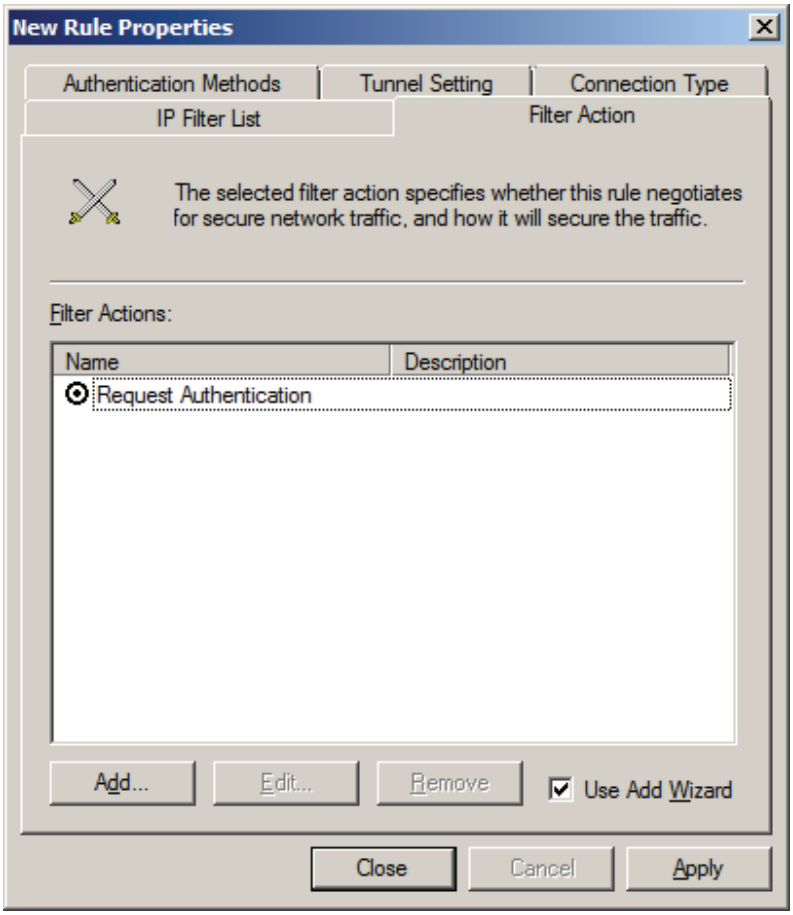
The **Properties** page for the filter action appears.



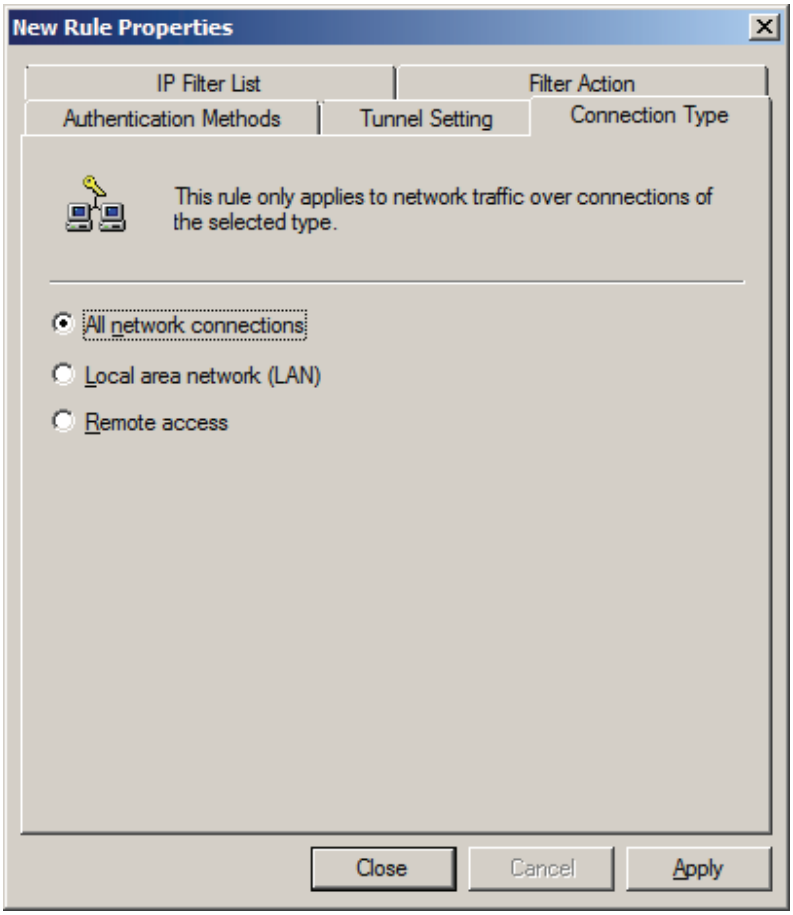
Select **Accept unsecured communication, but always respond using IPsec** to enable inbound fallback-to-clear behavior.



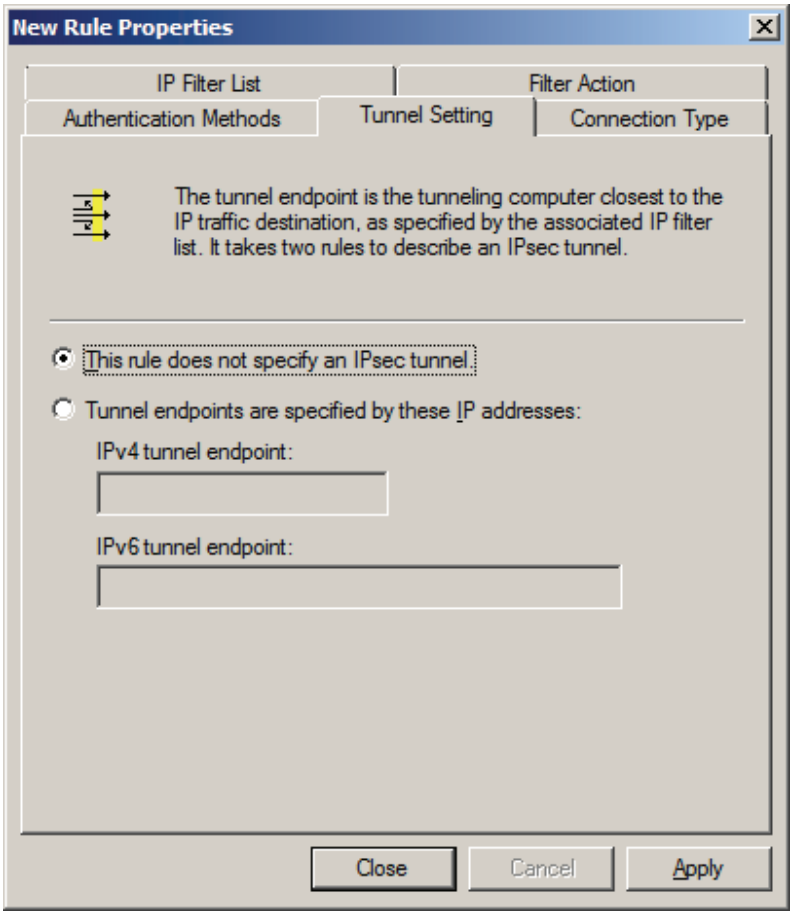
Press **Apply** button and then hit **OK.**



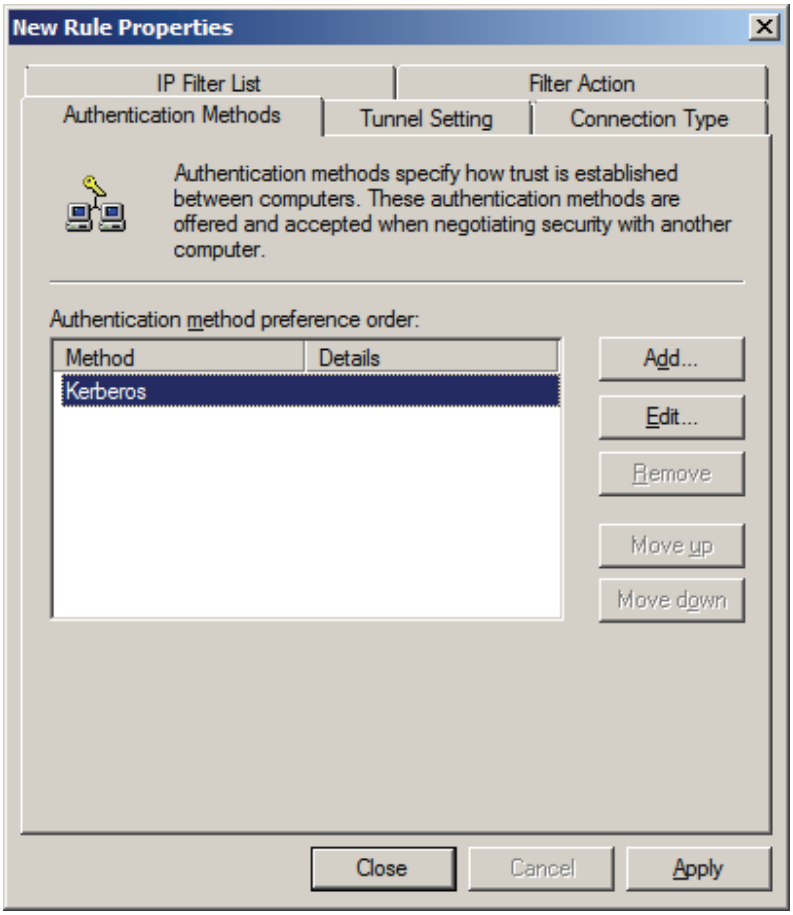
Switch to **Connection Type** tab.



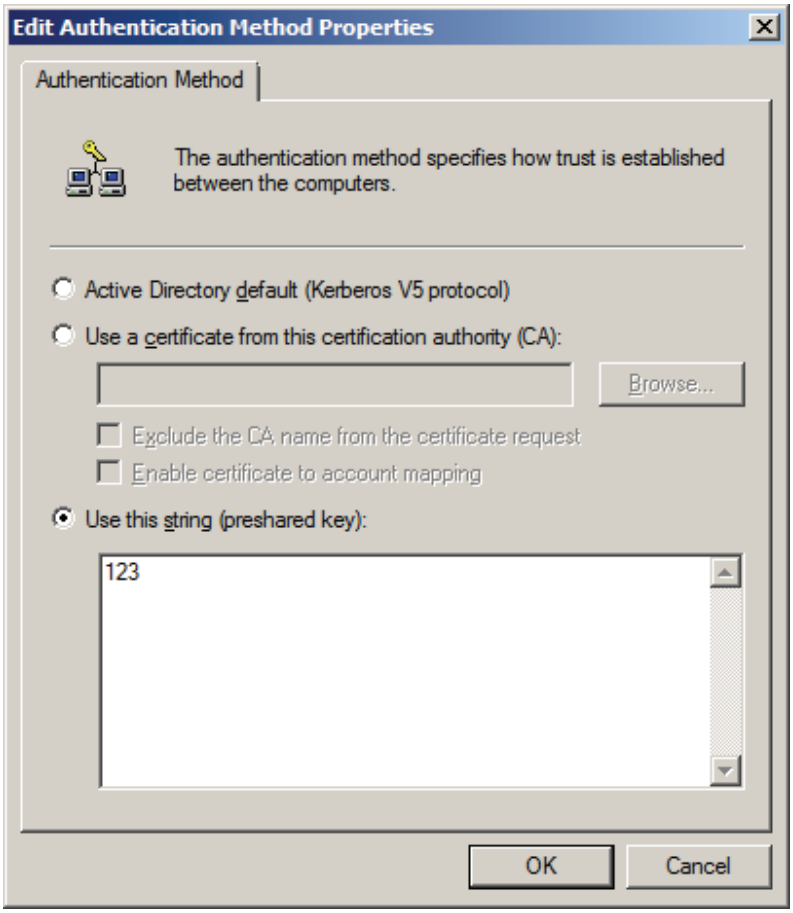
Select the **All network connections**, and then change to **Tunnel Setting** page.



Select **This rule does not specify an IPSec tunnel**, and then change to **Authentication Methods** tab.

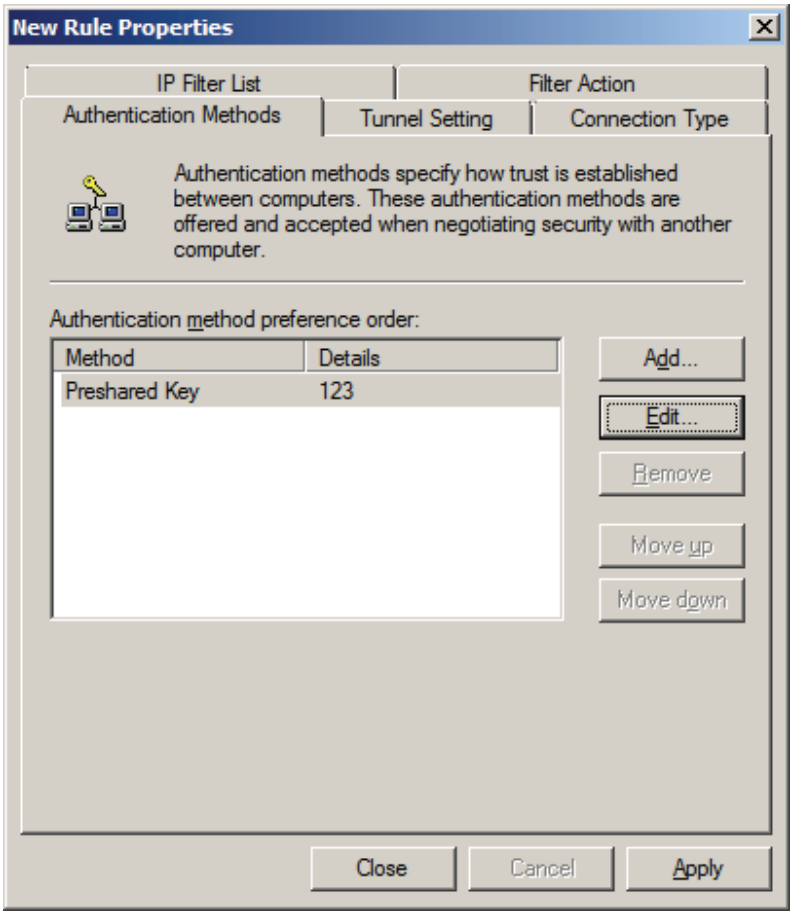


Select **Kerberos**, press the **Edit** button, the **Edit Authentication Method Properties** dialog is shown.

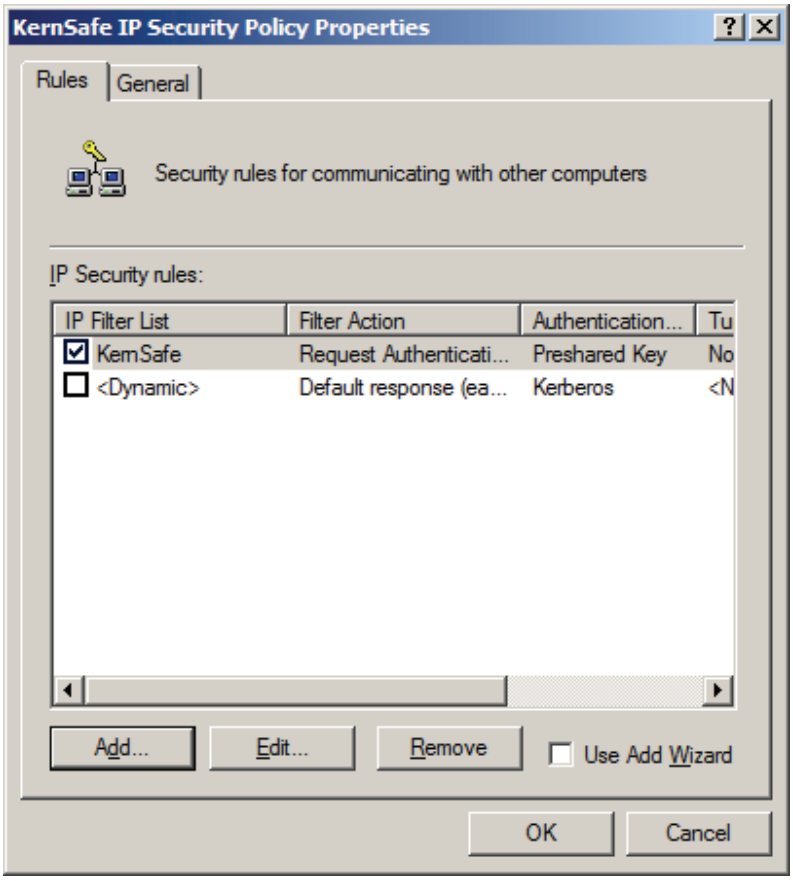


Select **Use this string (preshared key)**, type the preshared key, I take **123** as an example.

Click **OK** button to continue.

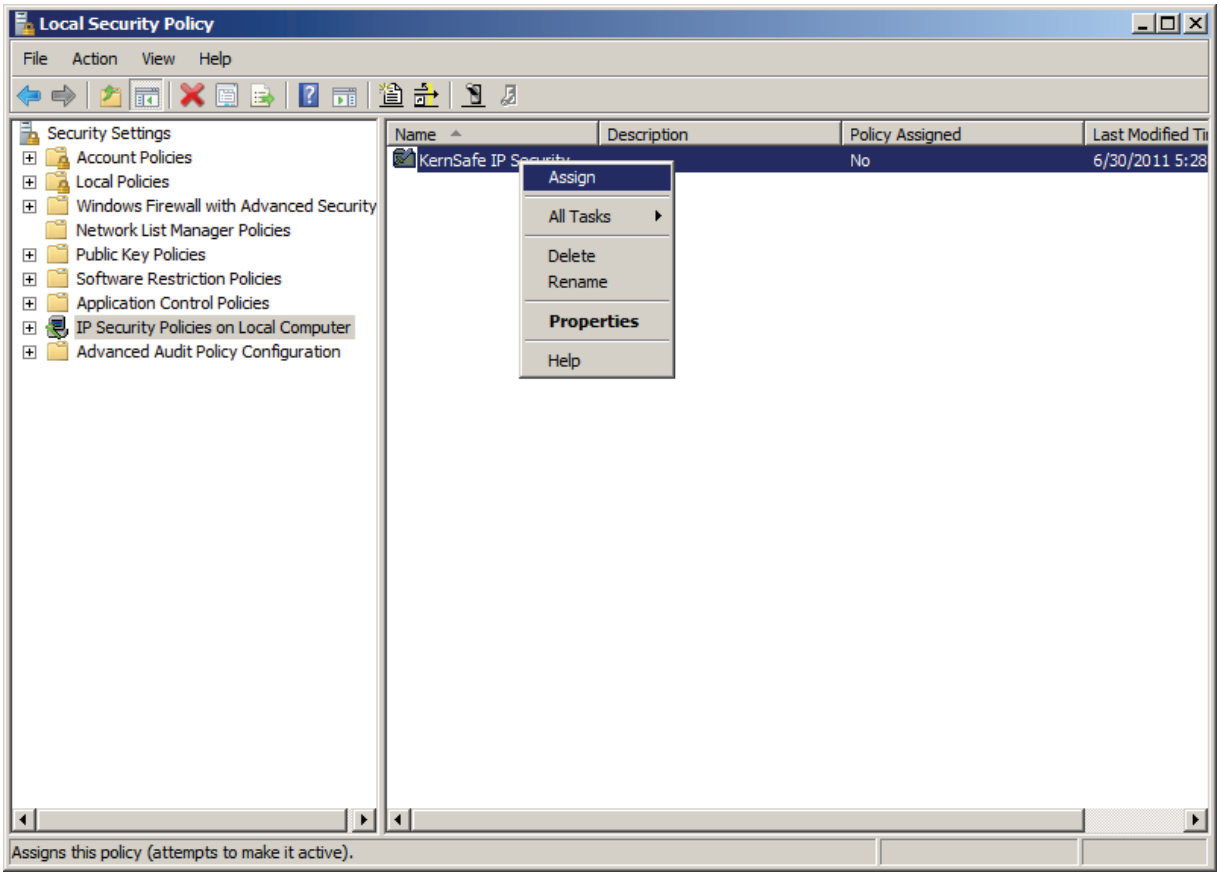


Press the **Apply** button to save settings and press the **OK** button to close this dialog.



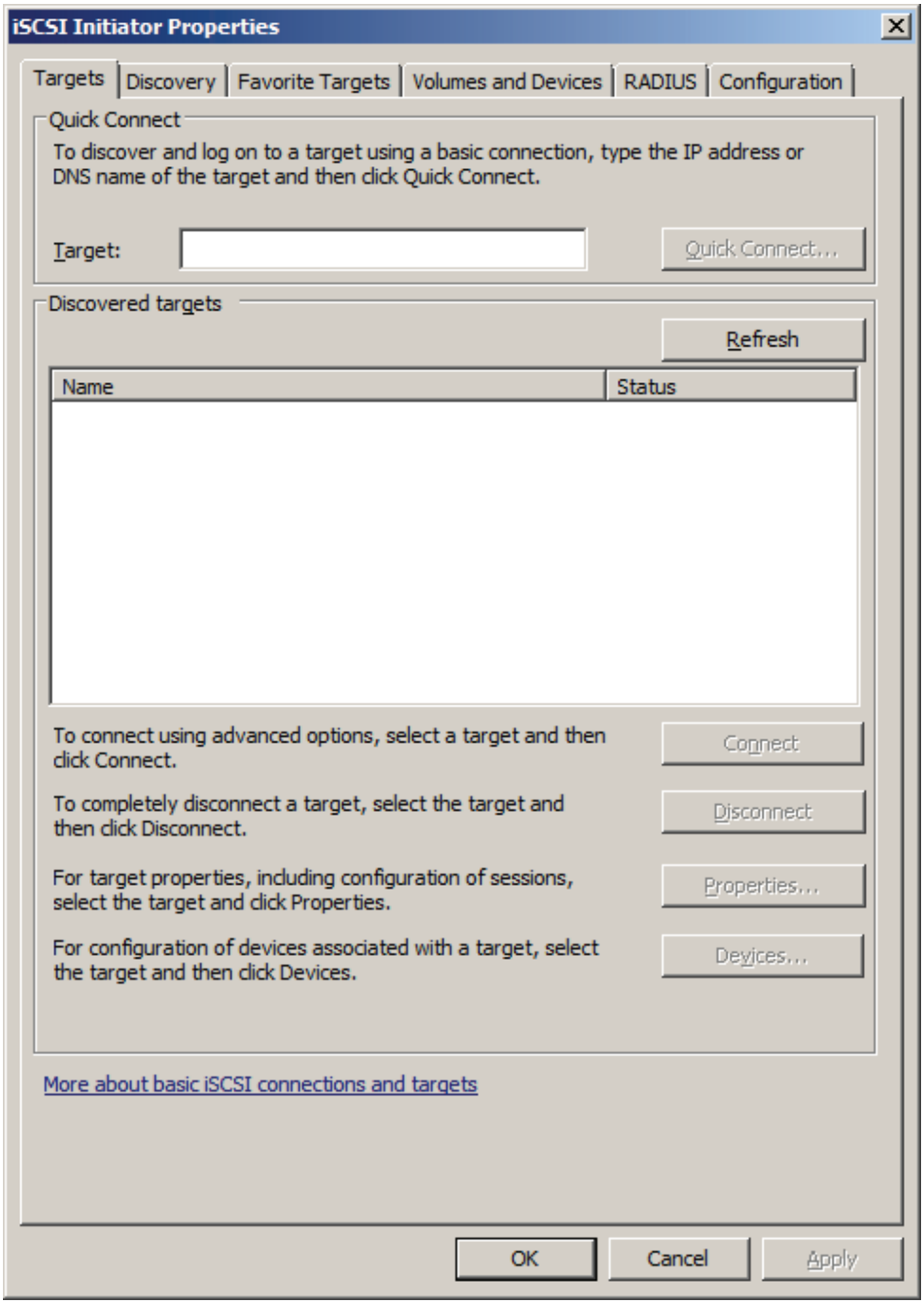
Check **KernSafe** in the **IP Filter List** and then press the **OK** button to continue.

Back to **Local Security Settings** main interface.



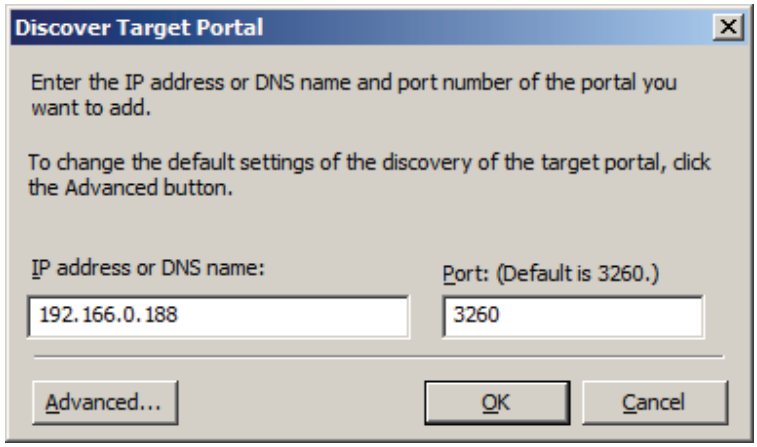
Right click on the **KernSafe IP Security Policy** item and then select **Assign** to make this item enabled.

Logging on to the target



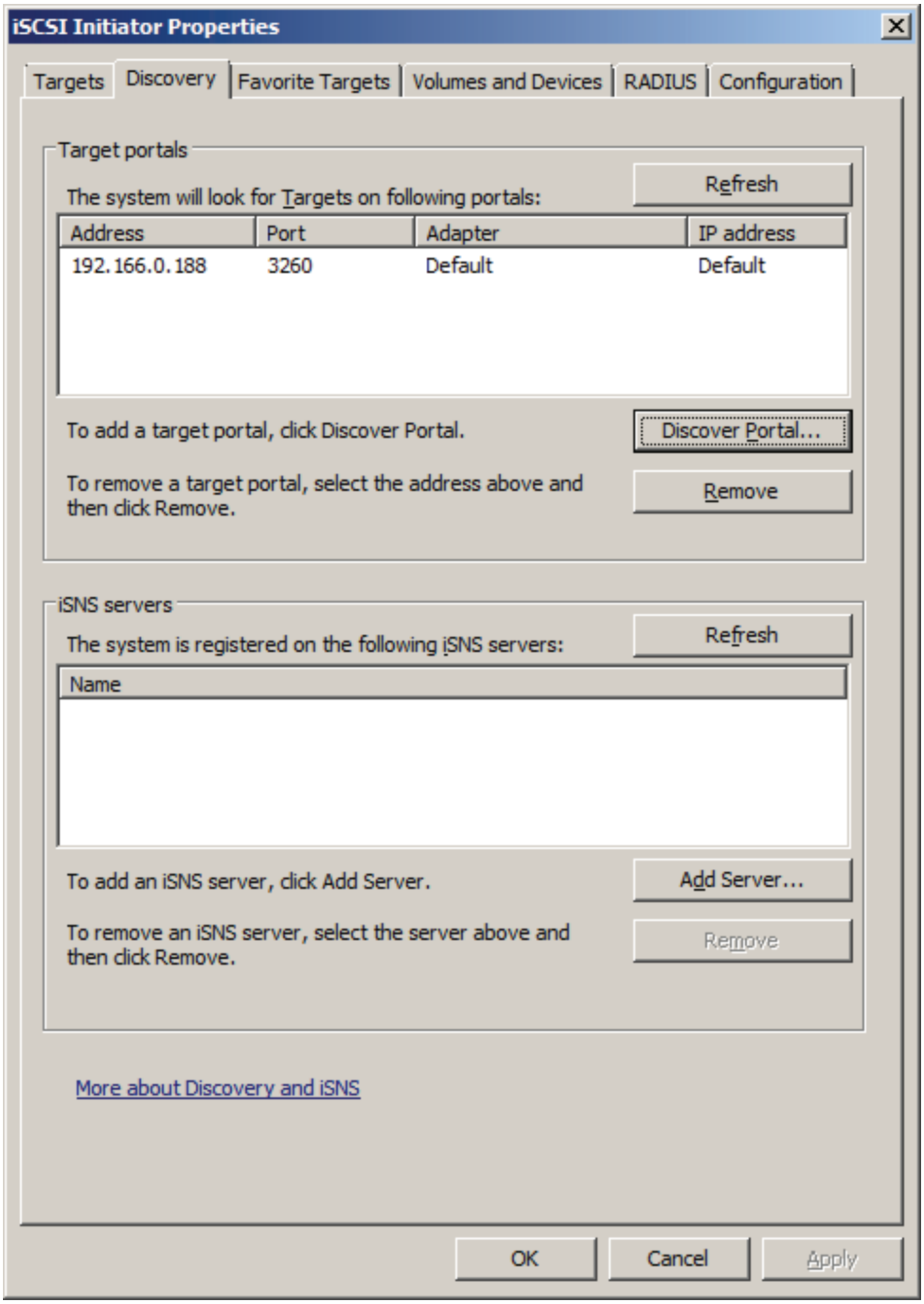
Switch to the **Discovery** tab page.

Press the **Discover Portal** button in the **Target Portals**, the **Discover Target Portal** dialog is shown.

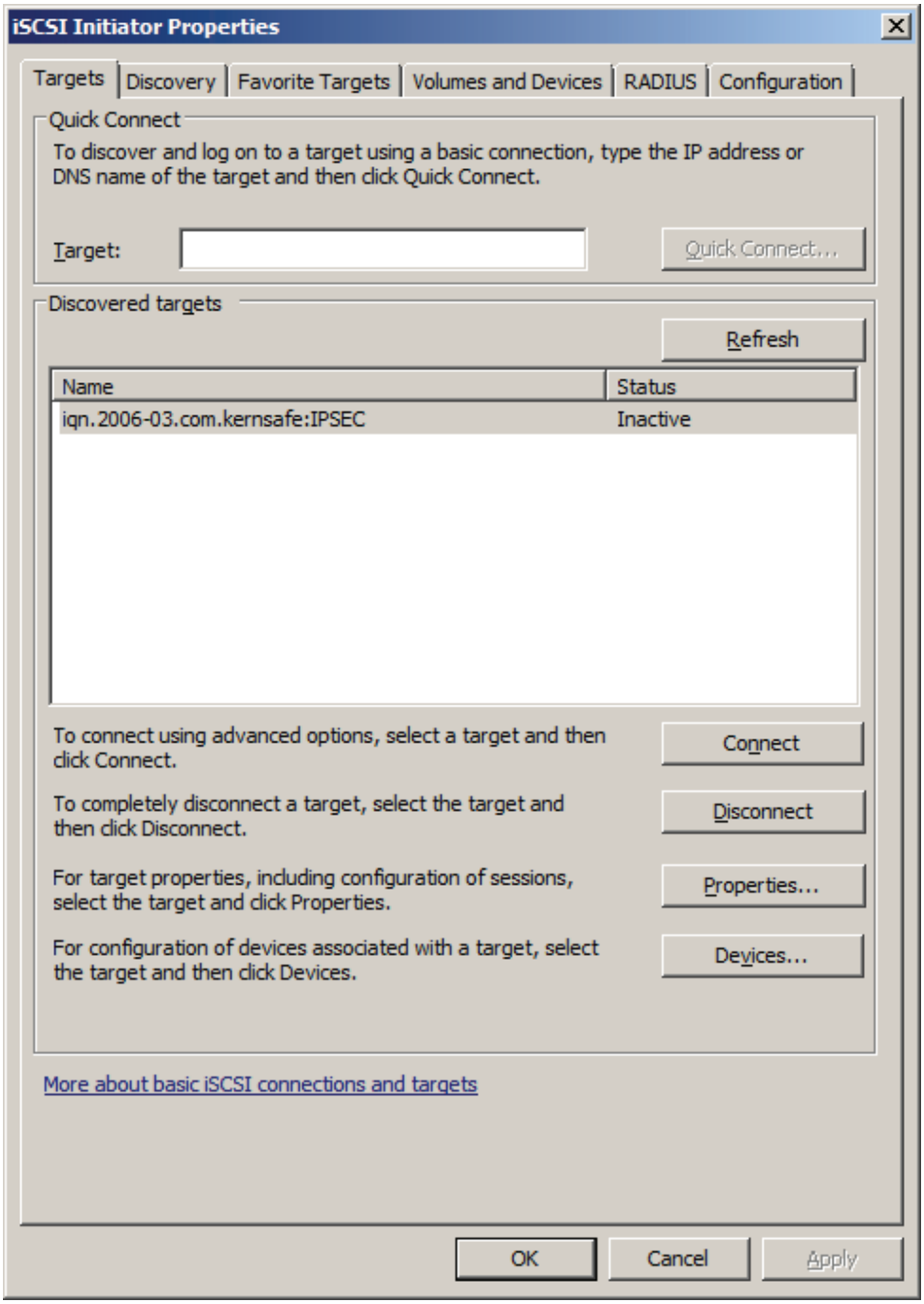


Type the **IP address** and **port** of your server.

Press the **OK** button to continue.

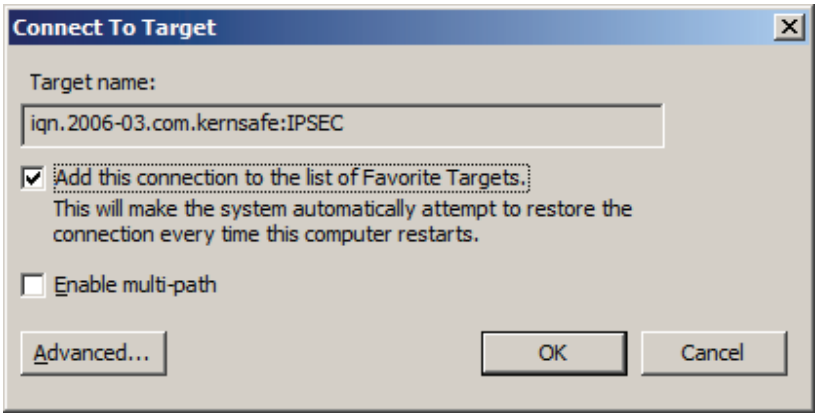


Switch to **Targets** tab.



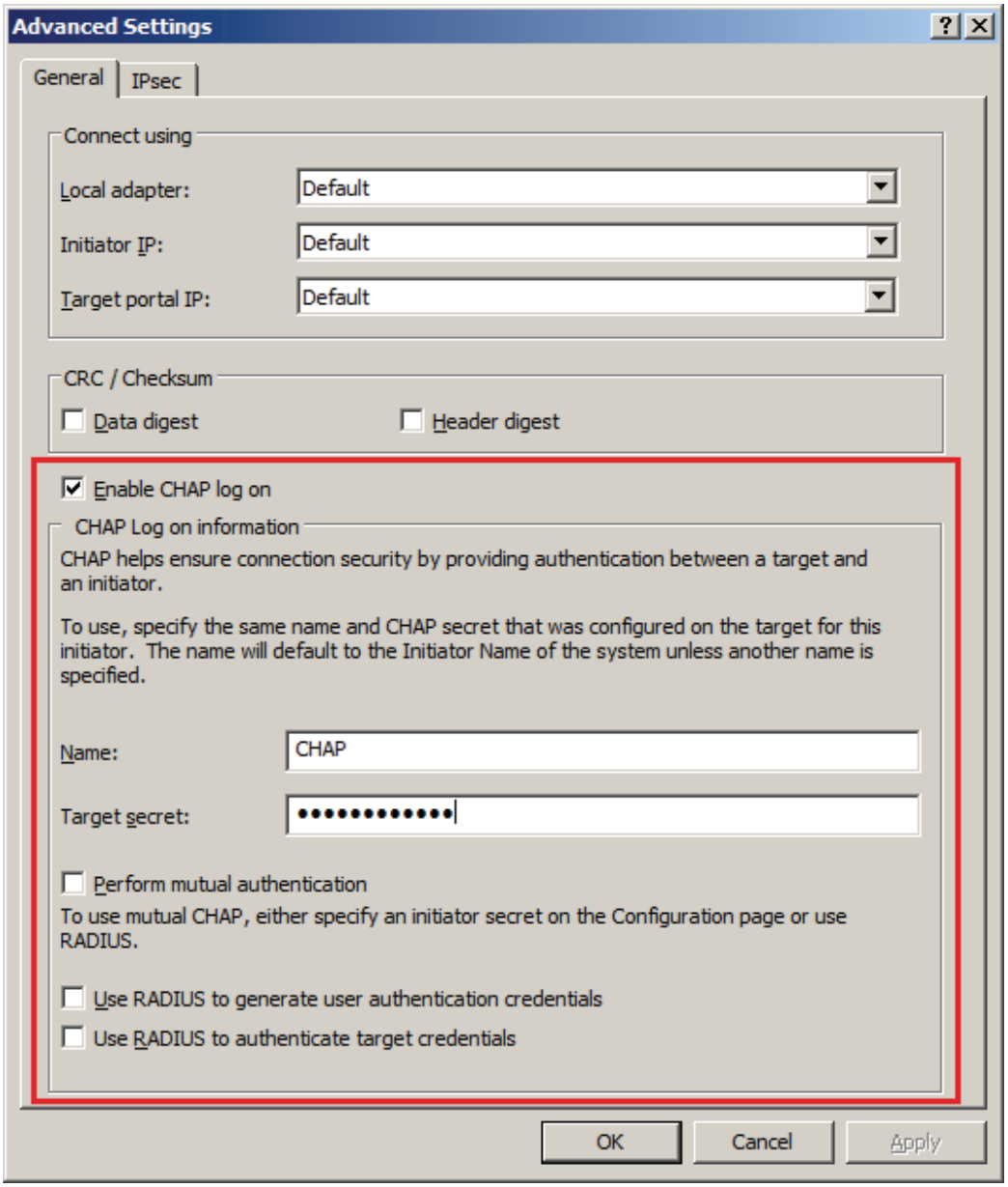
Select the target in the **Targets** list, and then press the **Connect** button.

Then the **Log On to Target** dialog is shown.



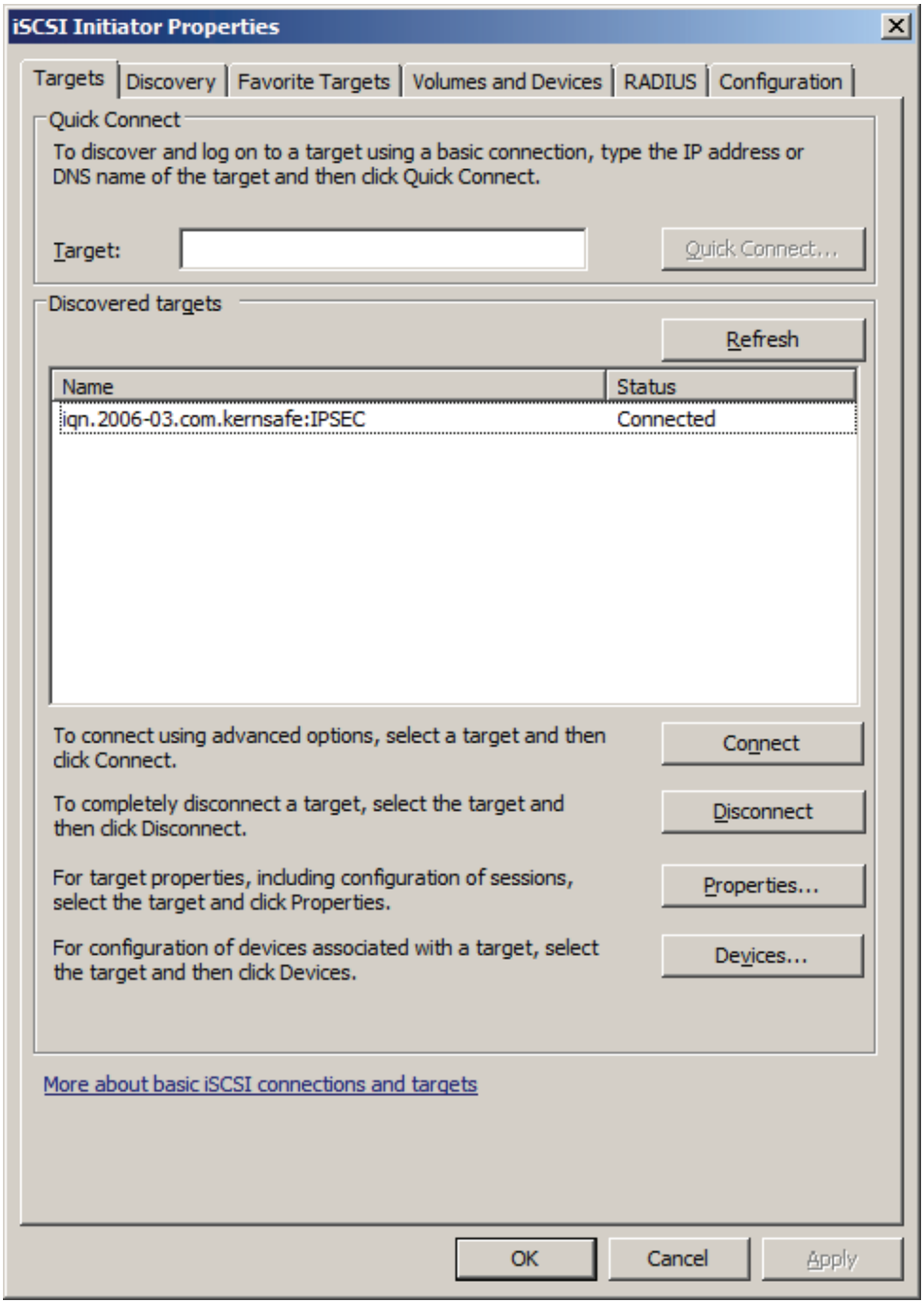
If your iSCSI target is using IP filter authorization, just press the **OK** button to continue.

If your iSCSI target is using CHAP user authorization (and IP filter authorization), press the **Advanced** button, the **Advanced Settings** dialog is shown.



Select **EnableCHAP log on** information and type **Name** and **Target secret**.

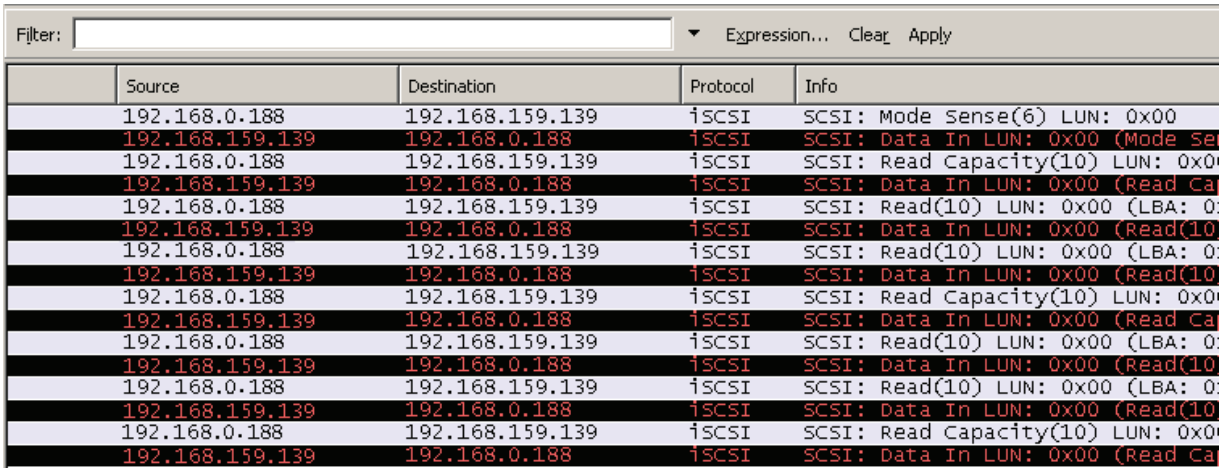
Press the **OK** button to continue.



When the connection is created, you will see the connection in the Status column. Now, you may operate the iSCSI disk just as a normal disk.

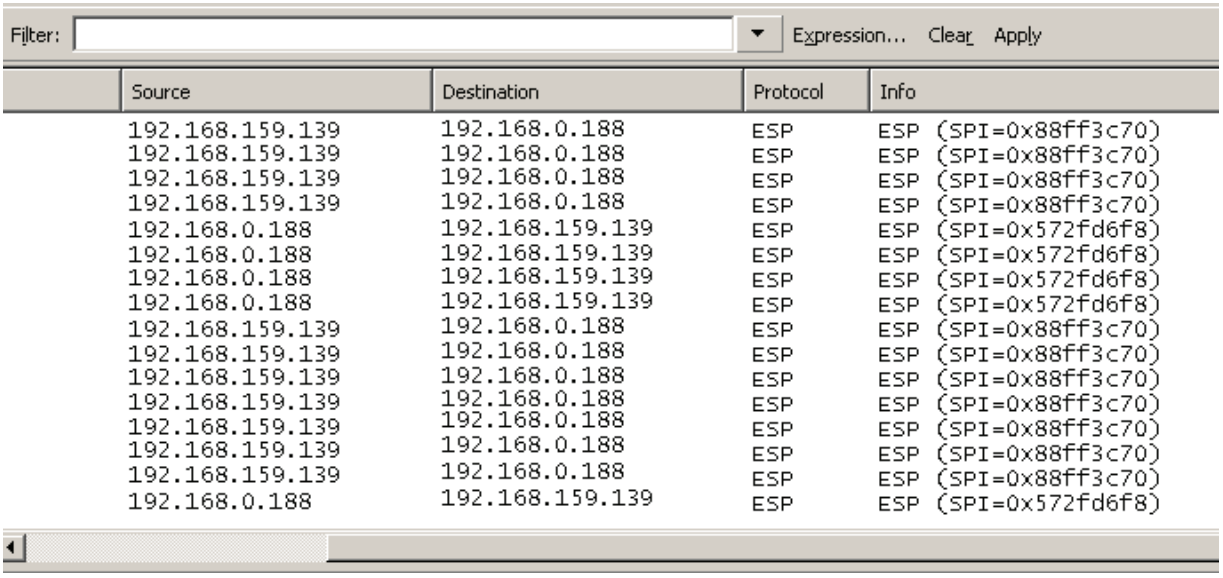
Effect

TCP/IP online traffic when not using IP SEC.



We will “see” all the information when initiators communication with targets.

TCP/IP online traffic when using IP SEC.



All the information is encrypted.

Contact

Support:	support@kernsafe.com
Sales:	sales@kernsafe.com
Marketing:	marketing@kernsafe.com
Home Page:	http://www.kernsafe.com
Product Page:	http://www.kernsafe.com/product/istorage-server.aspx
Licenses	http://www.kernsafe.com/product/istorage-server/license-compares.aspx
Forum:	http://www.kernsafe.com/forum

KernSafe Technologies, Inc.

www.kernsafe.com