iStorage Server and IP SEC

Friday, May 28, 2010

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.

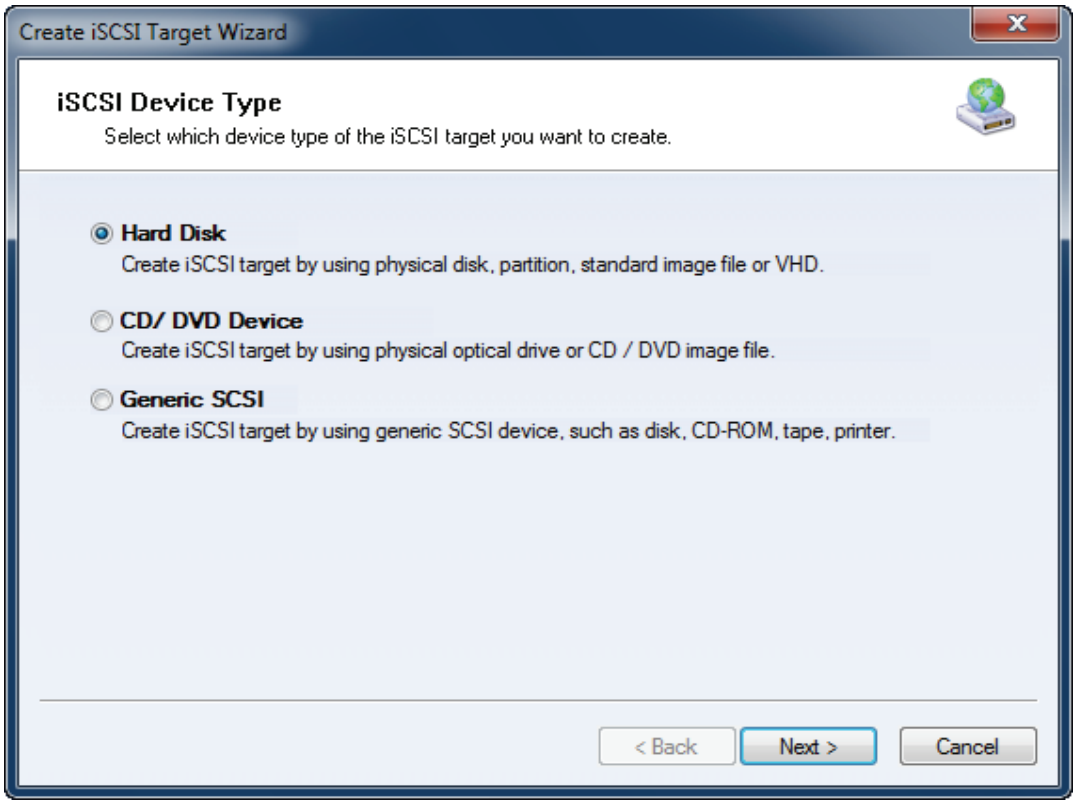
A network is not secure until servers can identify the computers communicating with them. IPSec enables secure, trusted communications between IP addresses. The system behind the IP address has an identity that is verified by using an authentication process. The only computers that must be aware of IPSec 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. Take Windows Server 2003 as an example, It is also similar to Windows 2000, Windows XP, Windows Vista and Windows Server 2008. At the same time, this article 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.

1. iSCSI Target Setting

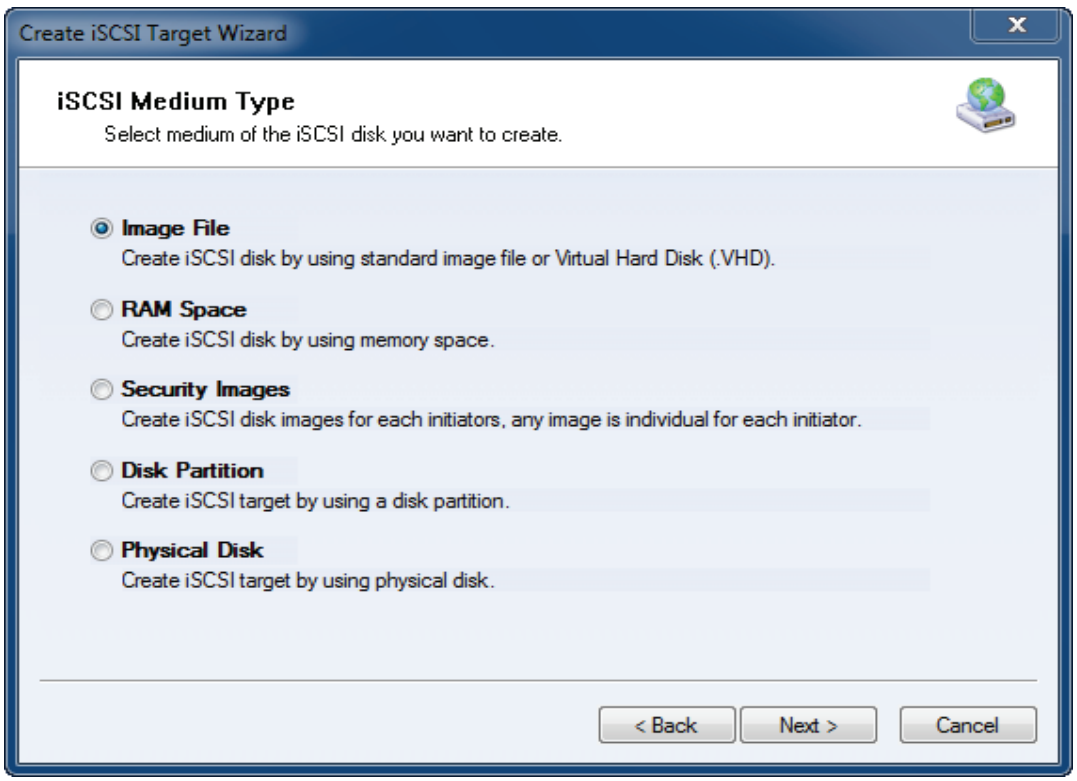
A) Create Target

Launch **KernSafe iStorage Server Management Console**，Select **Storage** -> **Create Targe**t menu item, the **Create Target wizard** is shown.



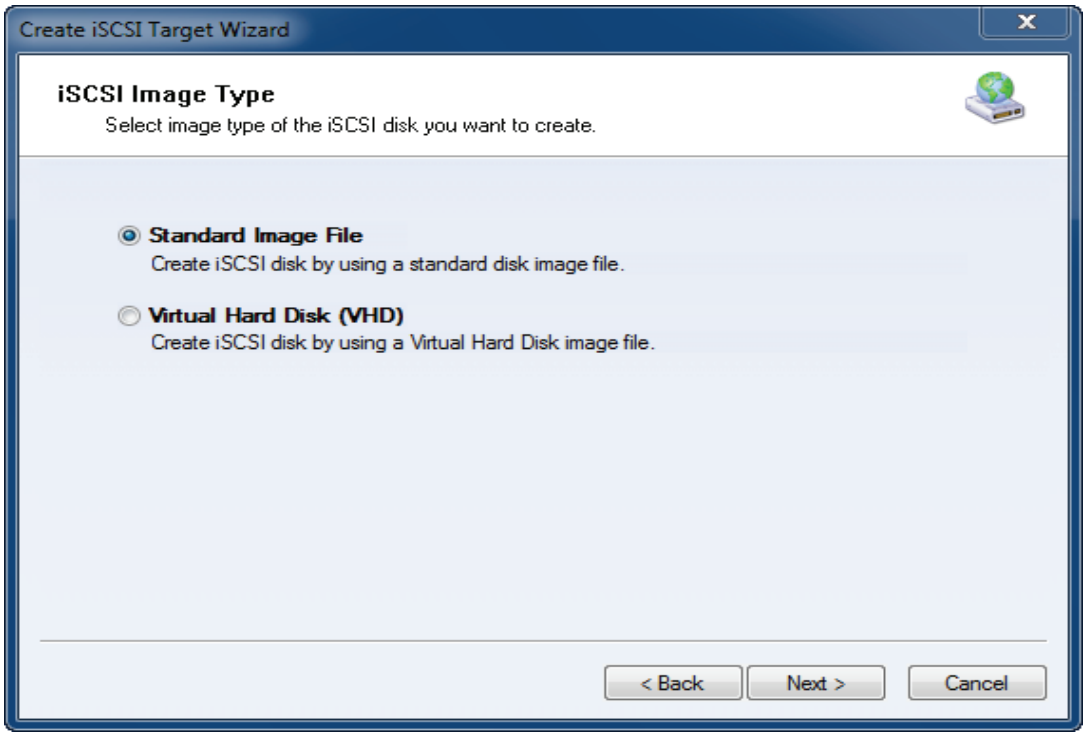
Choose **Hard Disk**.

Press the **Next** button to continue.



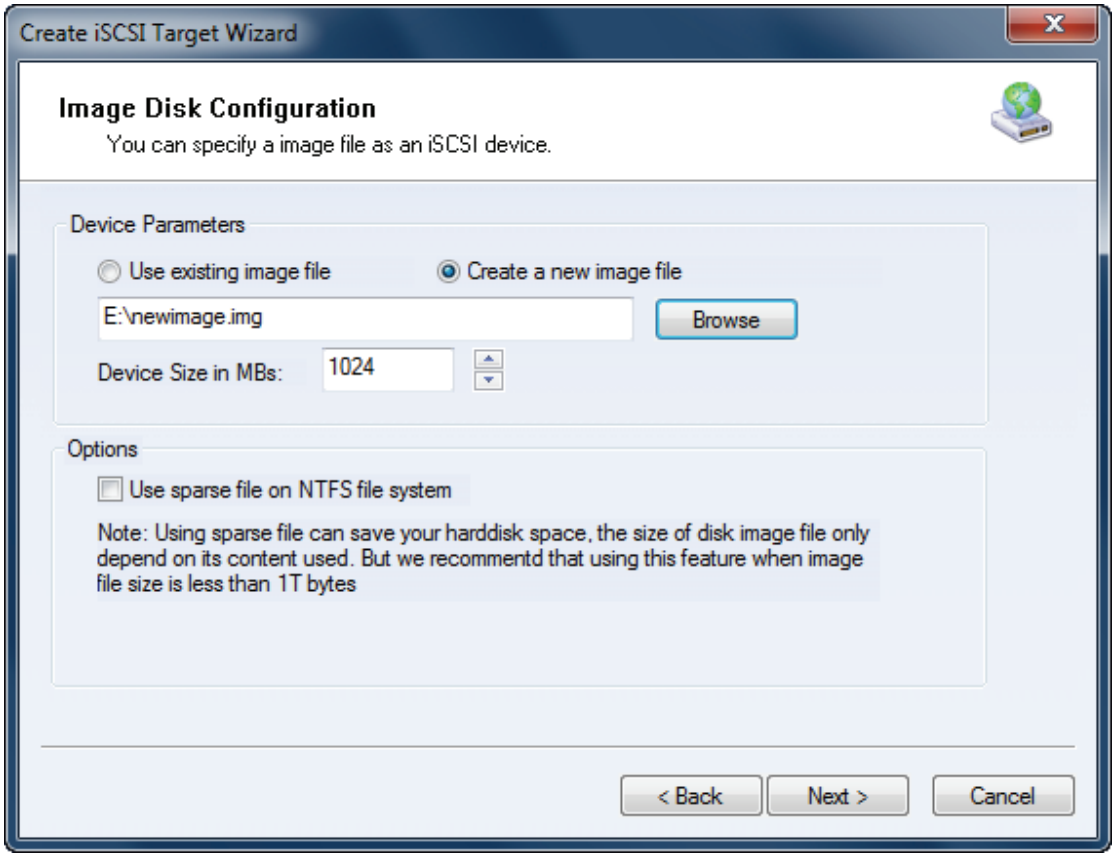
Choose **Image File** in **iSCSI Medium Type** window.

Then press **Next** button to continue.



We choose **Standard Image File** and then press **Next** button.

Set image disk parameters

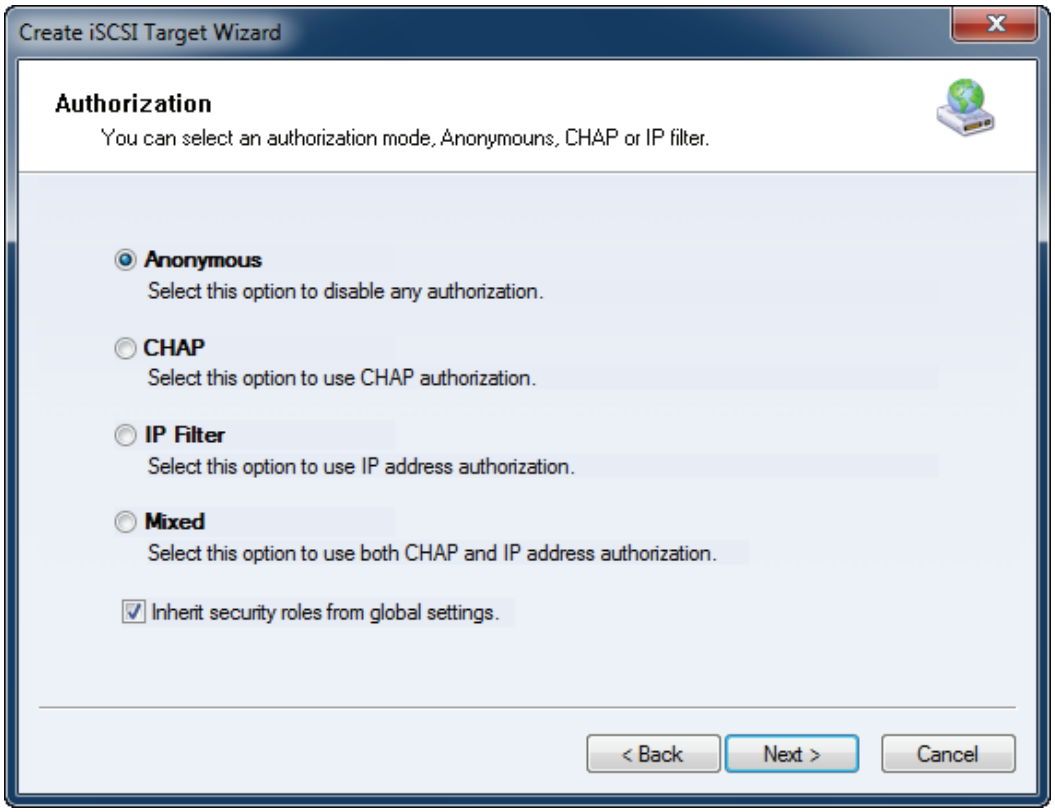


Select **Create a new image file** or **Use existing image file** if you already have a one.

Specify the device size.

Press the **Next** button to continue.

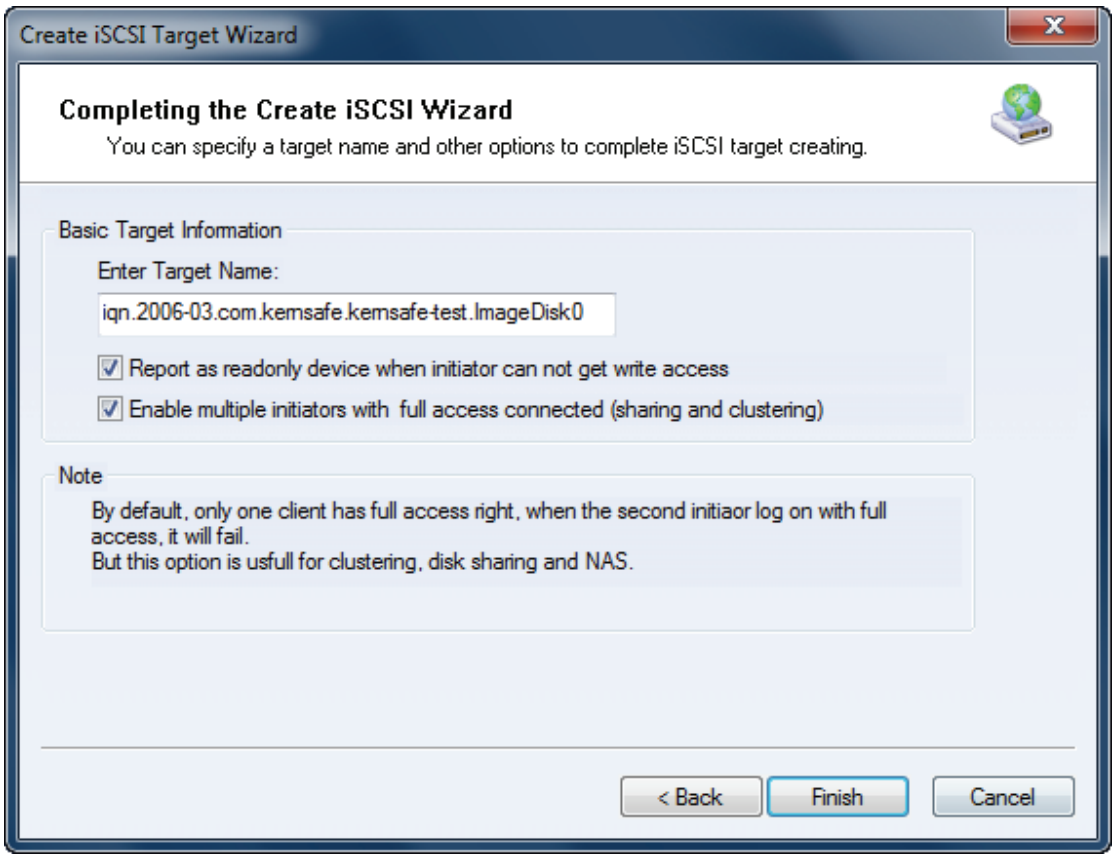
Set Authorization Mode.



Choose authorization mode as you required.

Press the **Next** button to continue.

Finish iSCSI Target Creating.



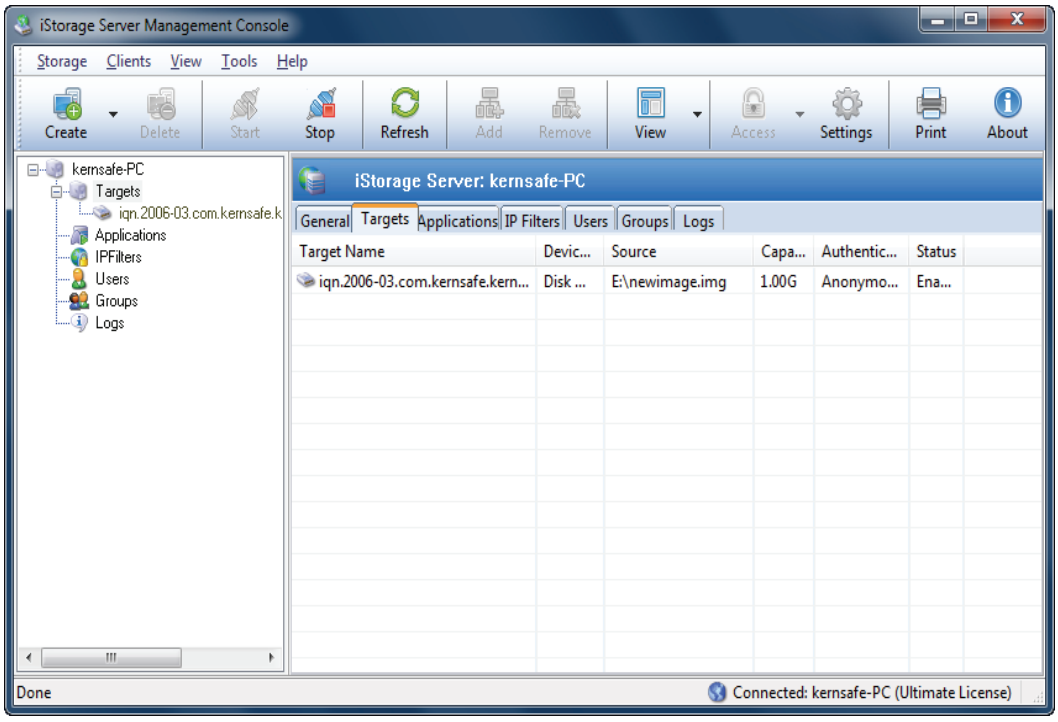
Type the target name or use the default name.

Press the **Finish** button to continue.

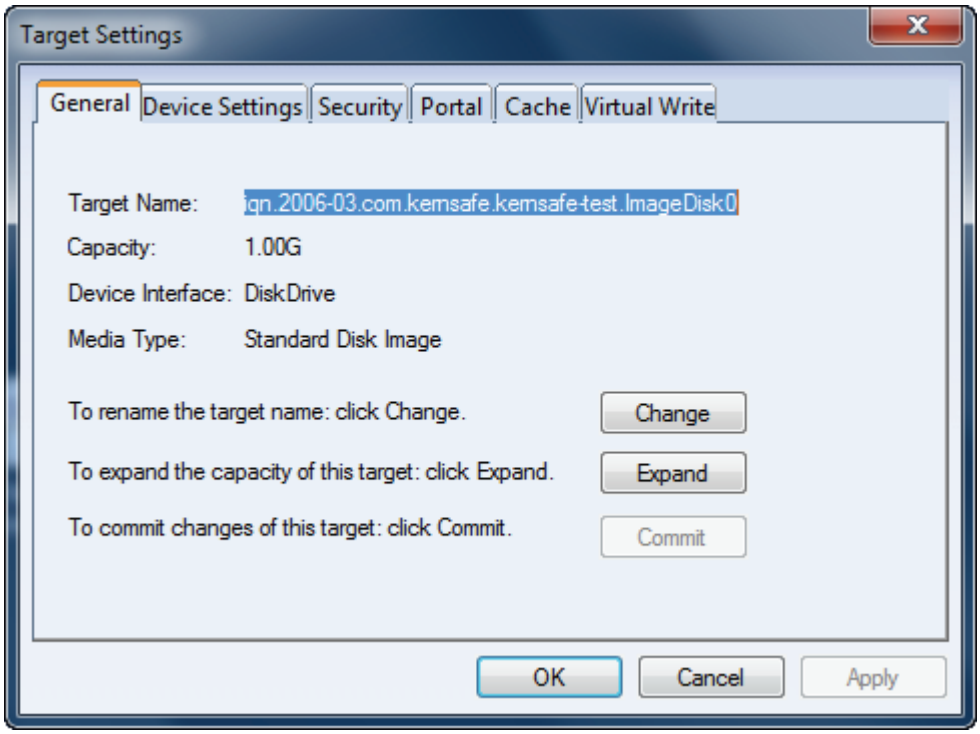
B) iSCSI Target Setting

This chapter is not necessary for every users of iStorage Server.

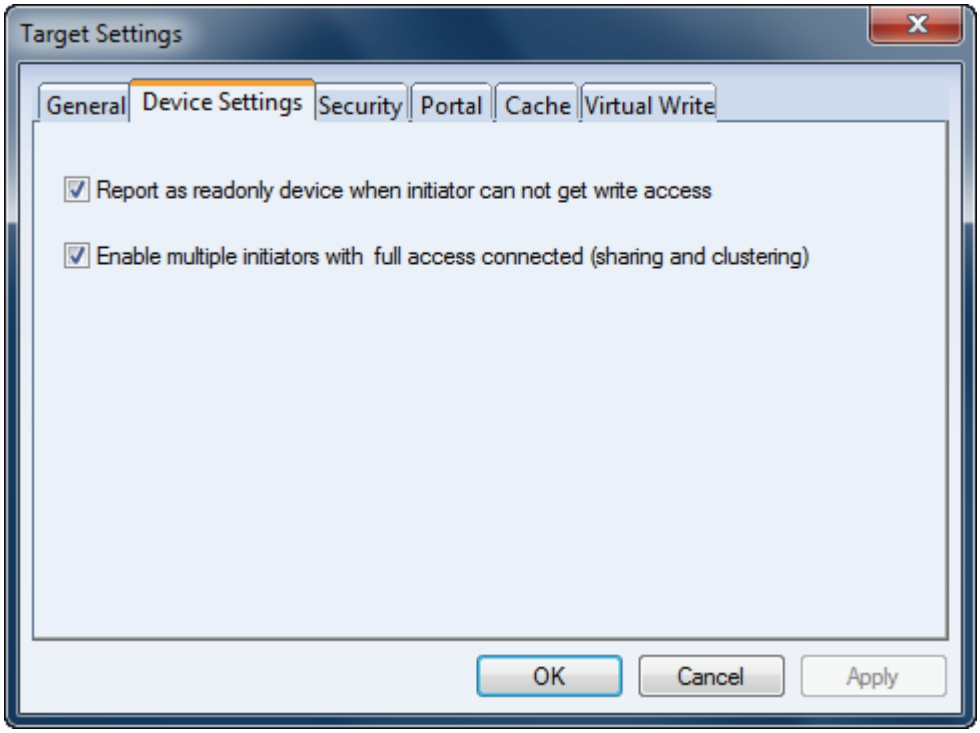
Back to iStorage Server Management Console.



B1. Modify iSCSI Target authorization method. User may modify iSCSI Target settings by through this method. Right click on the Target node, and then select the **Properties** menu item, the **Target Settings** dialog is shown.

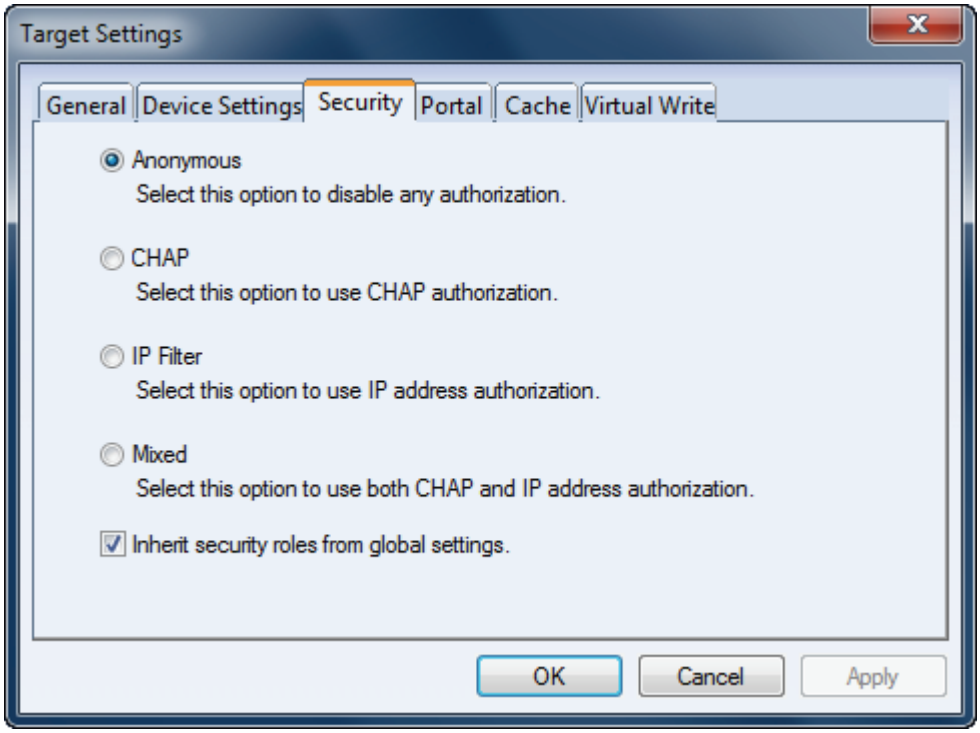


In **General** page, you can change the target name and expand the capacity of the target when it is a standard image file. The **commit** button is only available for RAM target.

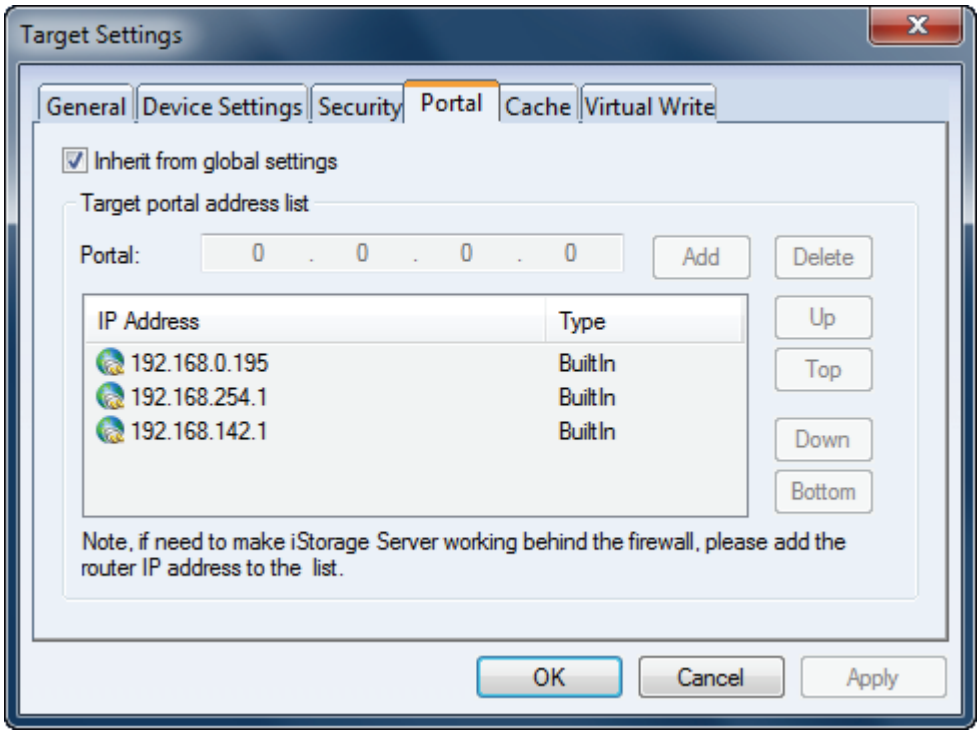


In the **Device Settings** Page, if you check **"Report as readonly device when initiator can not get write access"**, the system will give you a report when you load the target without write access.

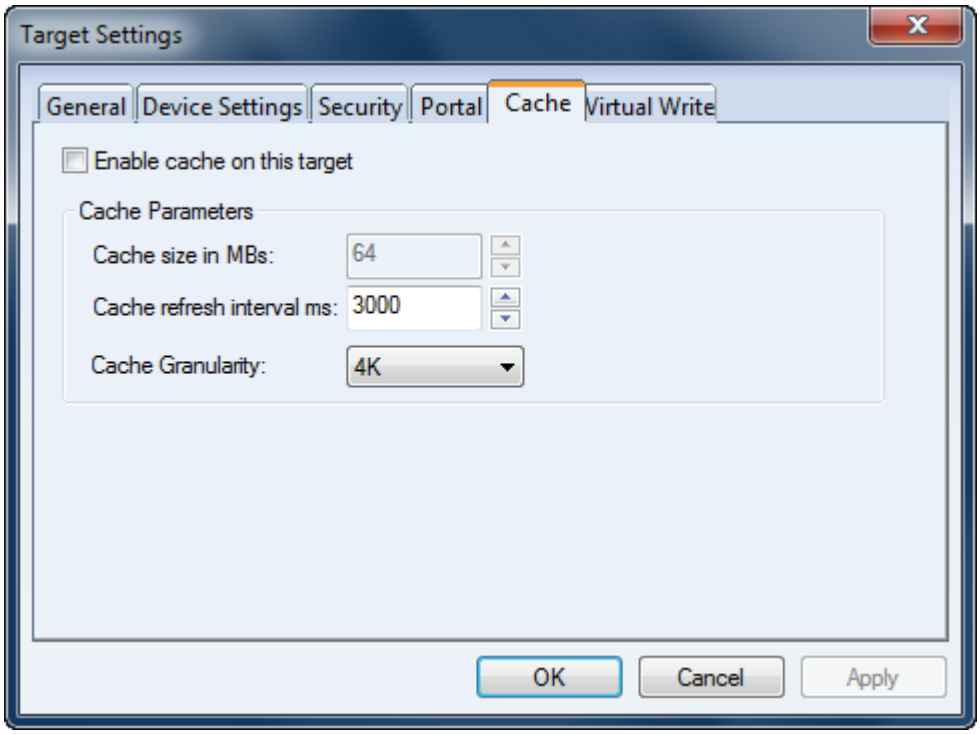
When your storage server is running in the environment of cluster, the function of concurrent writing of multi-users is needed and the writing synchronization control is realized by cluster software. Thus, you need to check **"Enable multiple initiators with full access connected"**



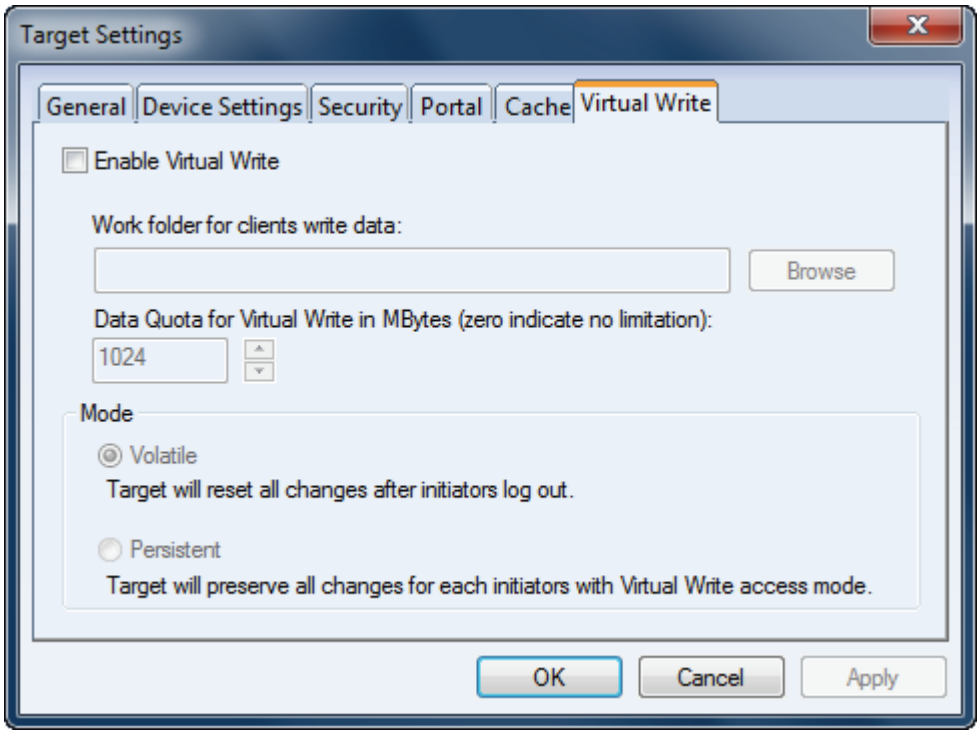
In the **Security** page, you can change the target's authorization mechanism.



In the Portal page, when you check **"Inherit from global settings"** the settings will follow the **"Settings"** in tool bar, otherwise, you can have your own portal address for this target.

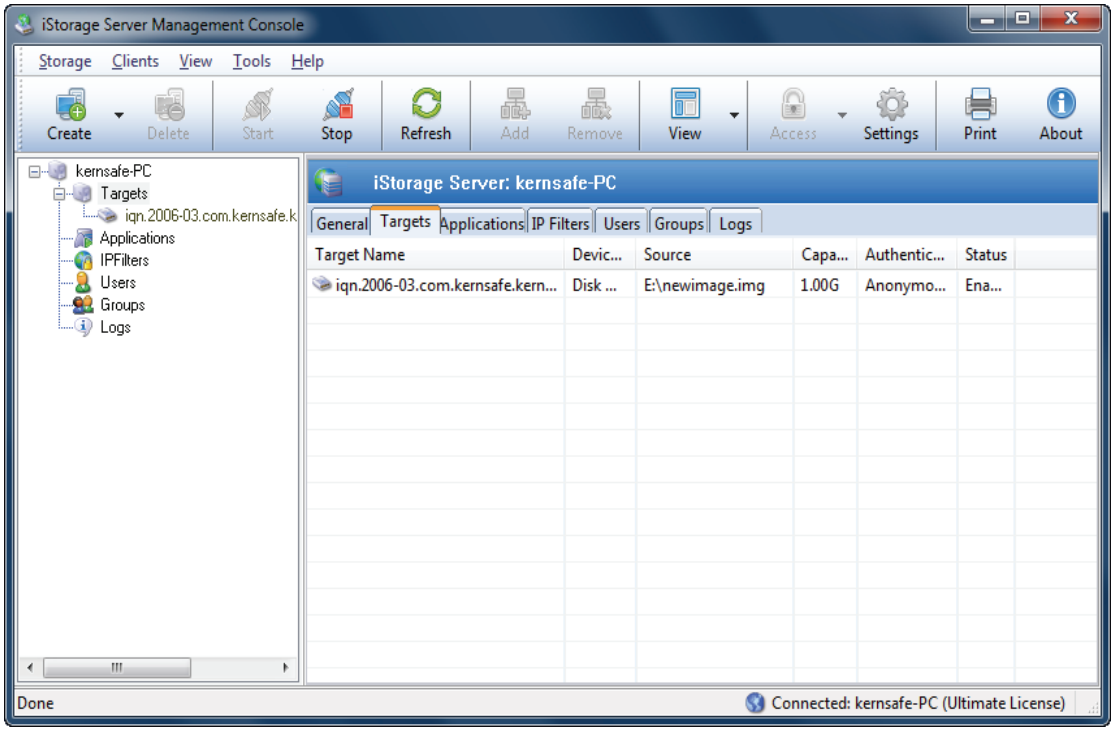


If you want to speed up the read and wire rate, check **Enable cache on this target** in the **Cache** page.

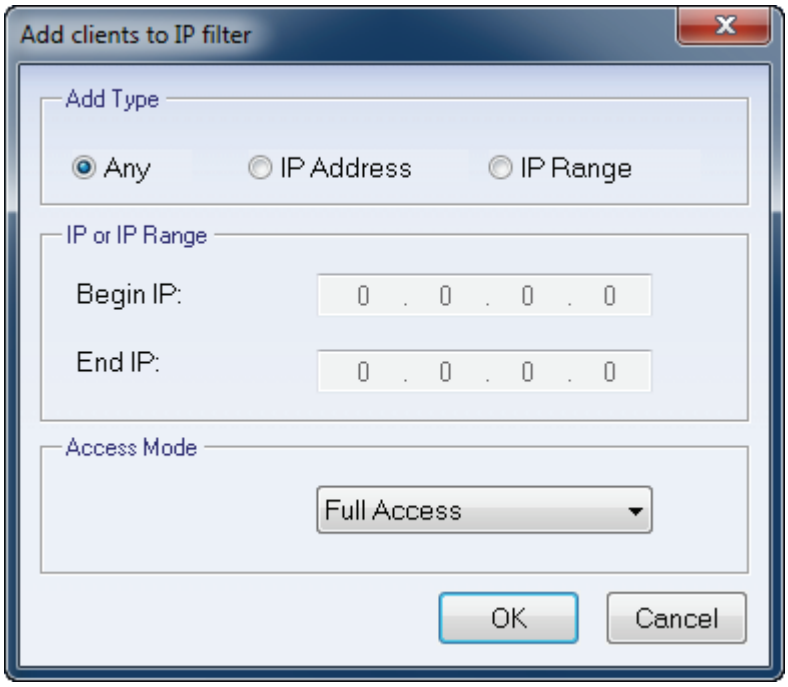


If you want your target has the COW protection, check the **"Enable Virtual Write"** in the **Virtual Write** page.

Once user selected IP filter authorization, he can manage this target's access right by IP filter. Click the View->IP Filters on the toolbar or click IP Filters on the left tree of the main interface.

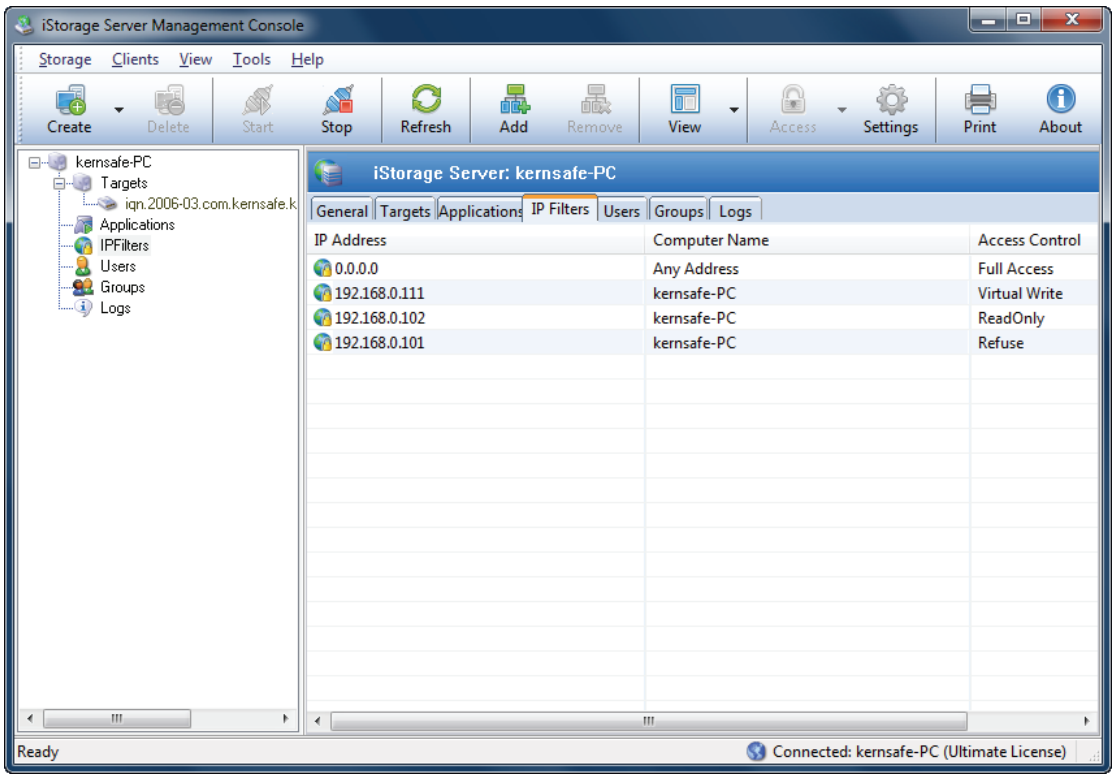


Click the Add button on the Toolbar, the Add clients to IP filter dialog is shown.



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.

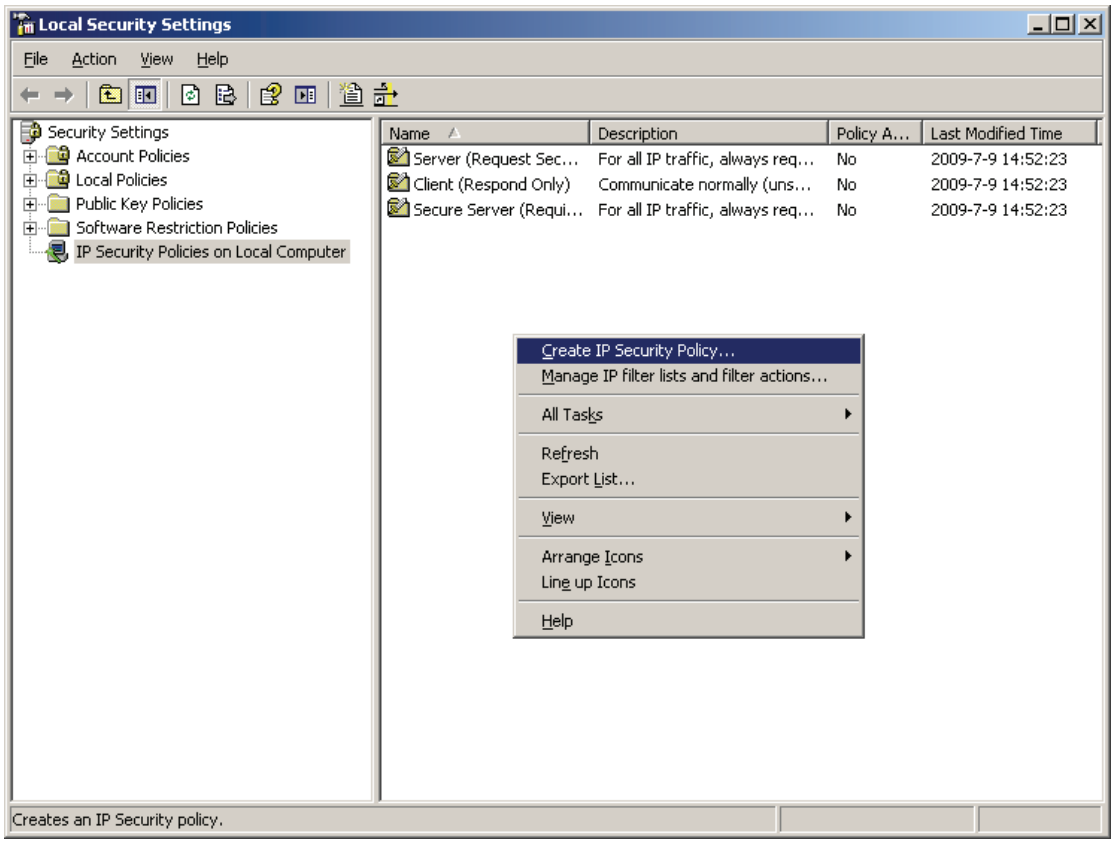
Press the **OK** button to add an IP filter item.



User can modify IP filter item's access right, Read Only, Refuse, Virtual Write and Full Access, or remove some IP filter items if they are not needed.

2. Server Side Local Security Policy Setting

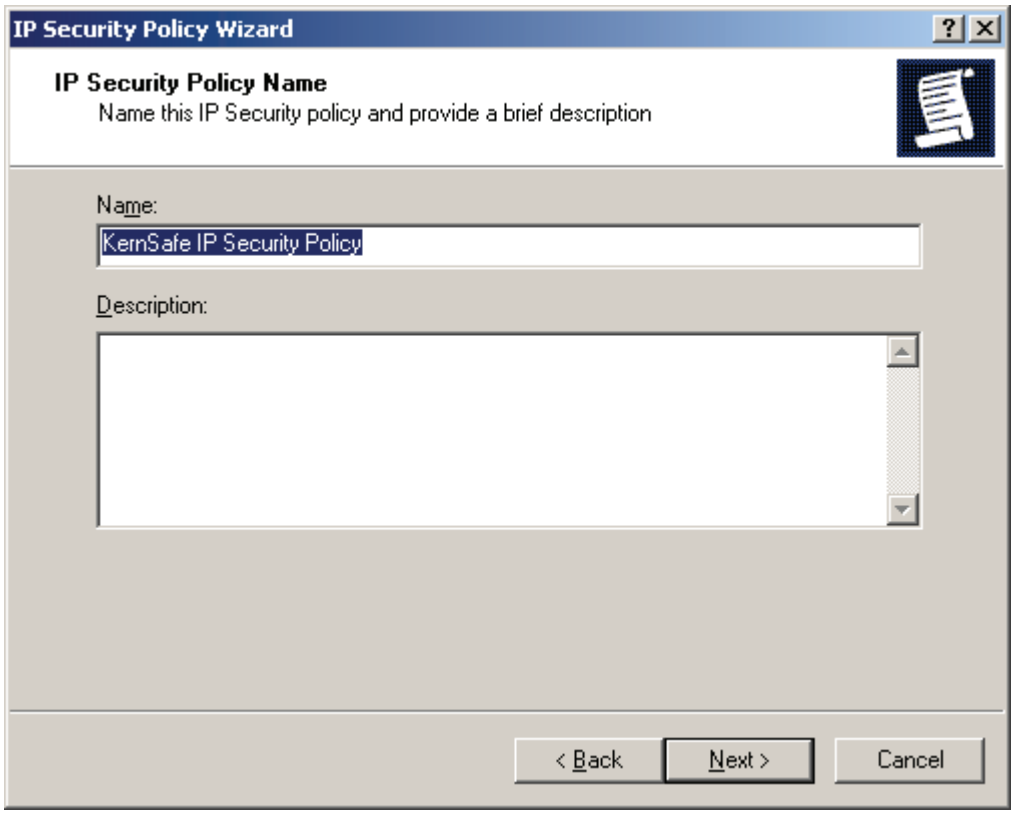
Click “Start -> Control Panel -> Administrative Tools -> Local Security Policy” open the “Local Security Settings Management Console.



Select the **IP Security Policies** on Local Computer, right click on the blank of right panel, then select the **Create IP Security Policy** menu item, the **IP Security Policy Wizard** is shown.

Press the **Next** button to continue.

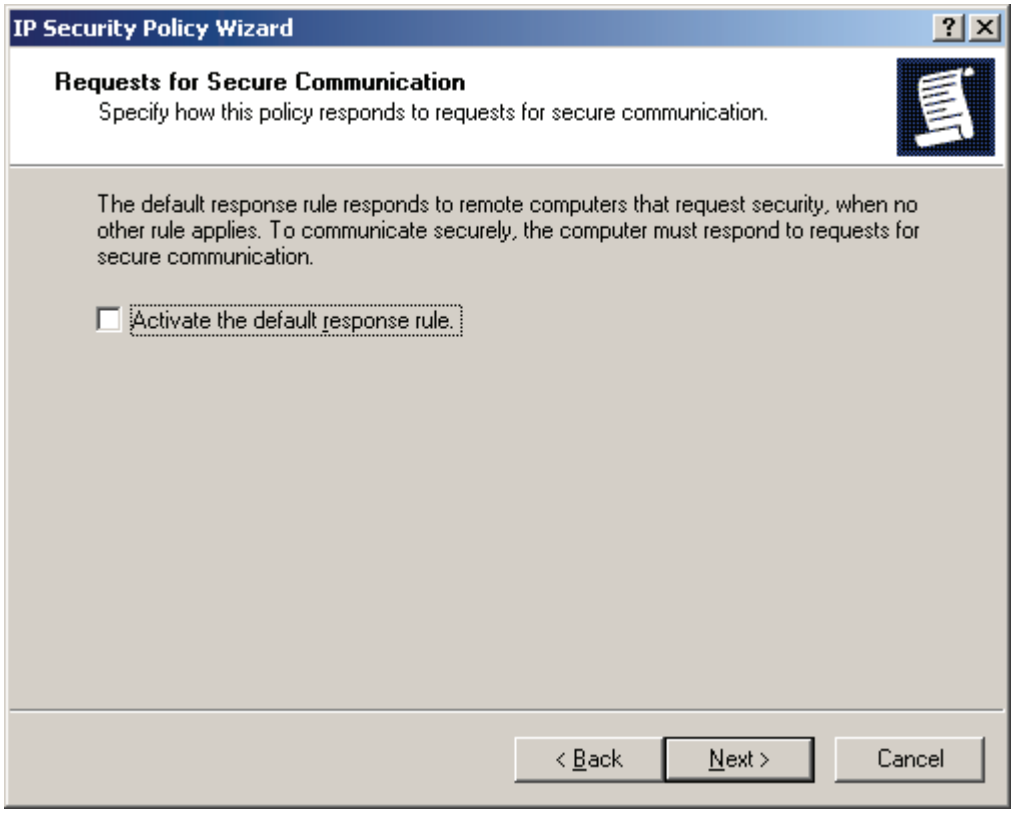
Type IP Security Policy Name



Type “KernSafe IP Security Policy”.

Press the **Next** button to continue.

Specify how this policy responds to requests for secure communication.



Do not select Activate the default response rule.

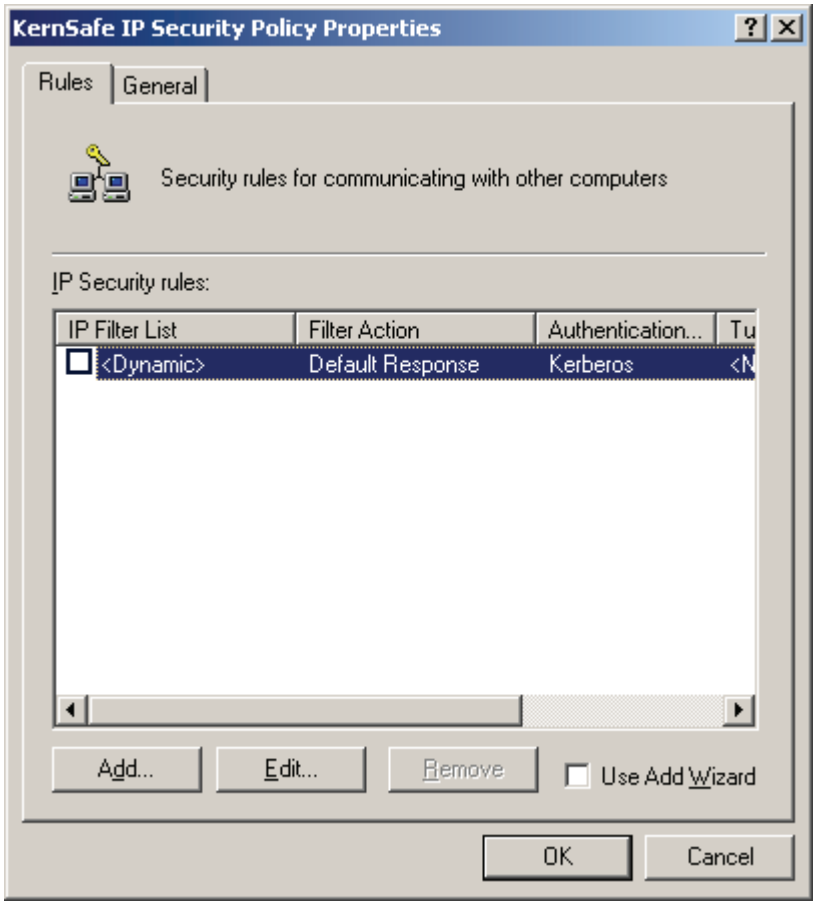
Press the **Next** button to continue.

Completing the IP Security Policy Wizard

Select the **Edit properties** by default.

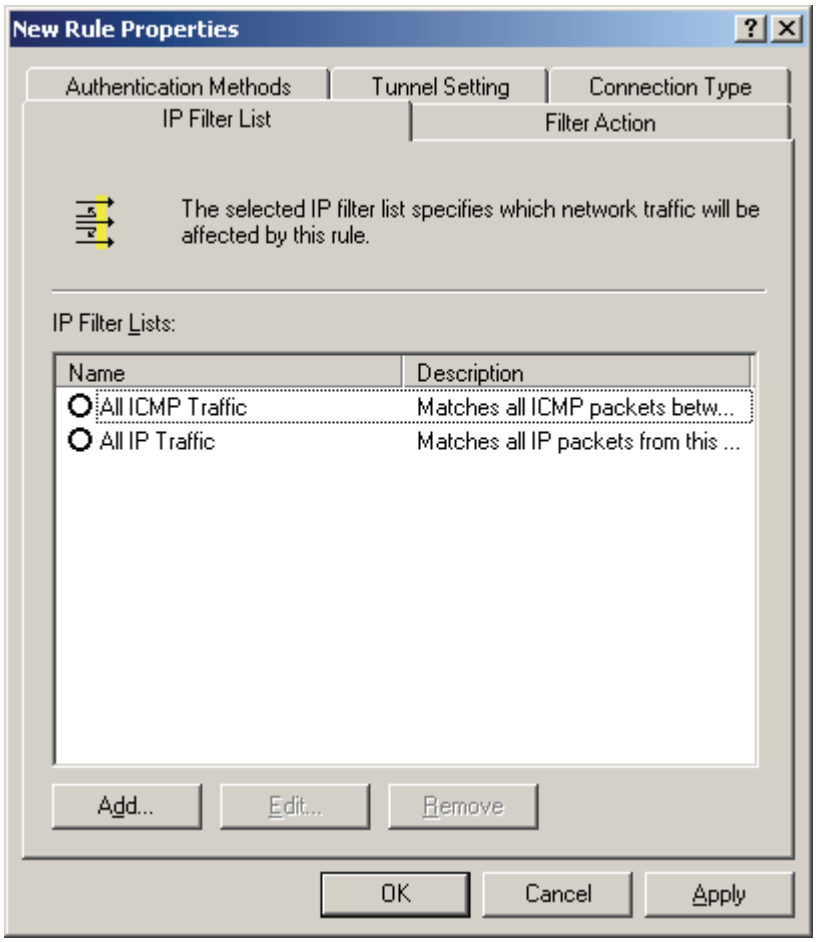
Press the **Finish** to continue.

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



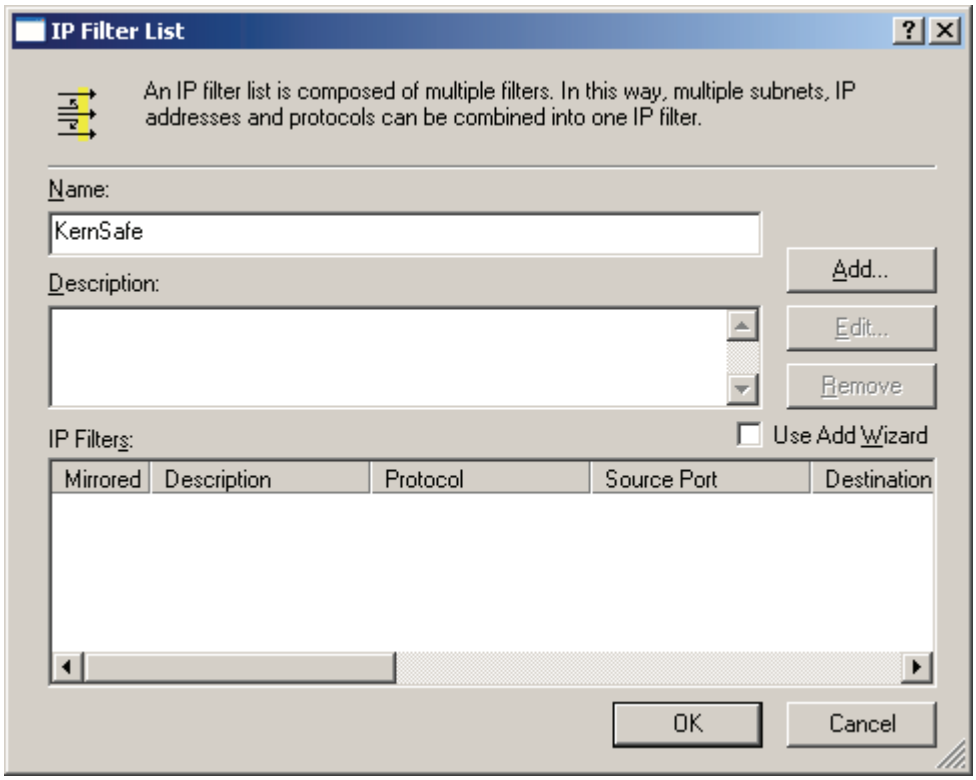
Do not select Use Add Wizard.

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



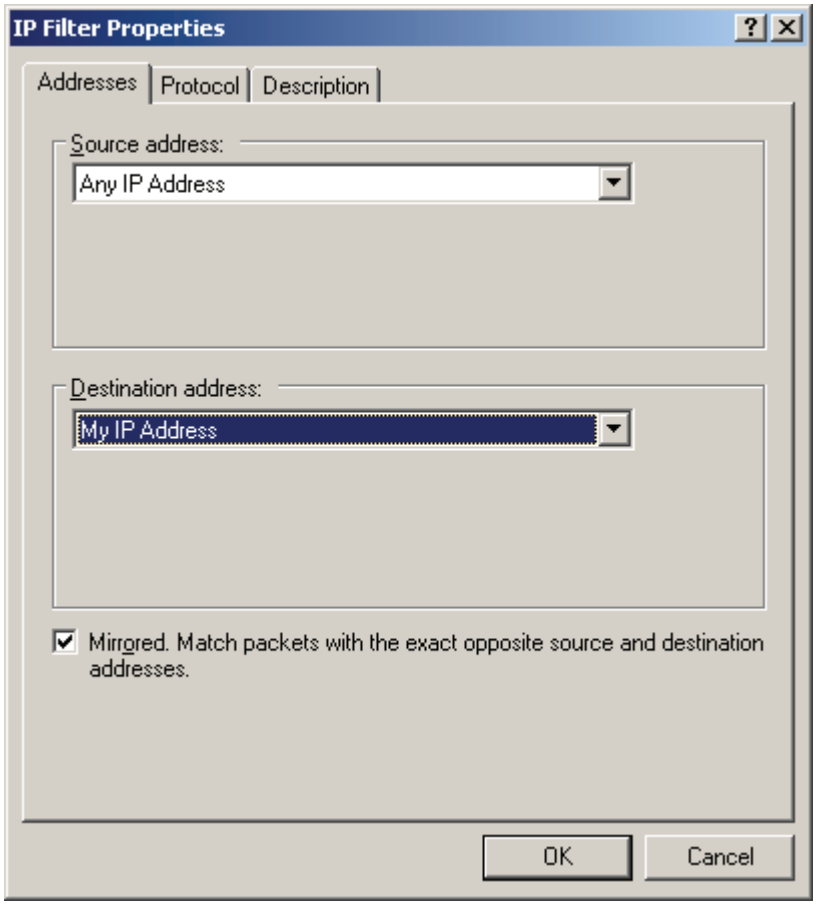
Press the **Add** button, the **IP Filter List dialog** is shown.

Input IP Filter name.



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

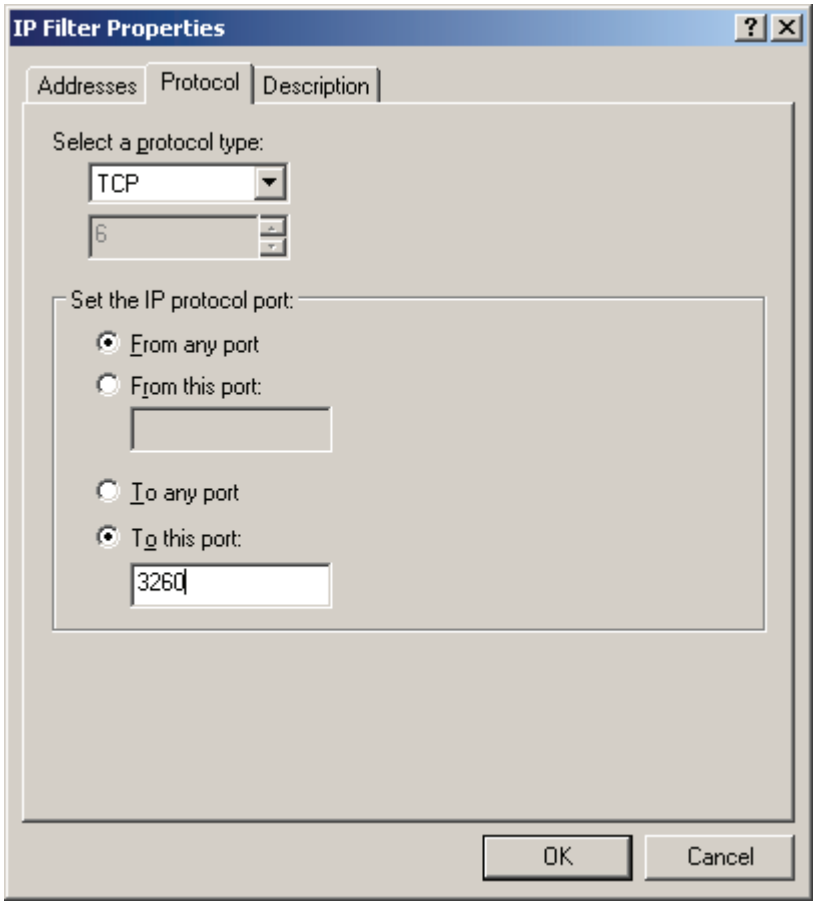
Press the **Add** button to continue.



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

Select My IP Address in the Destination address.

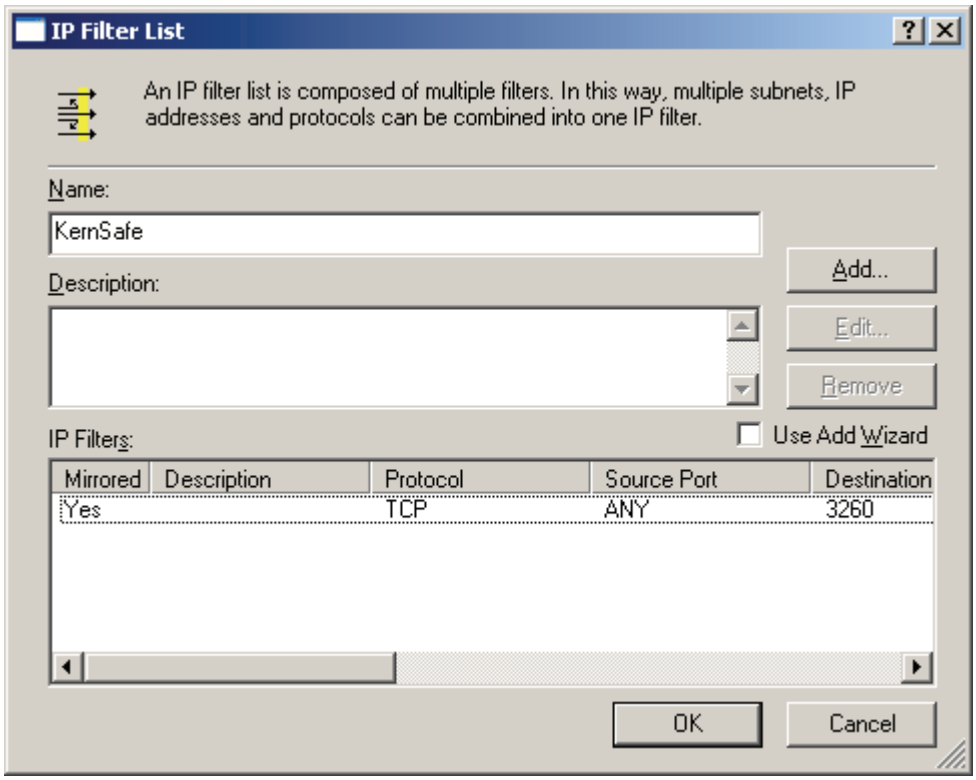
Then change to the **Protocol** page.



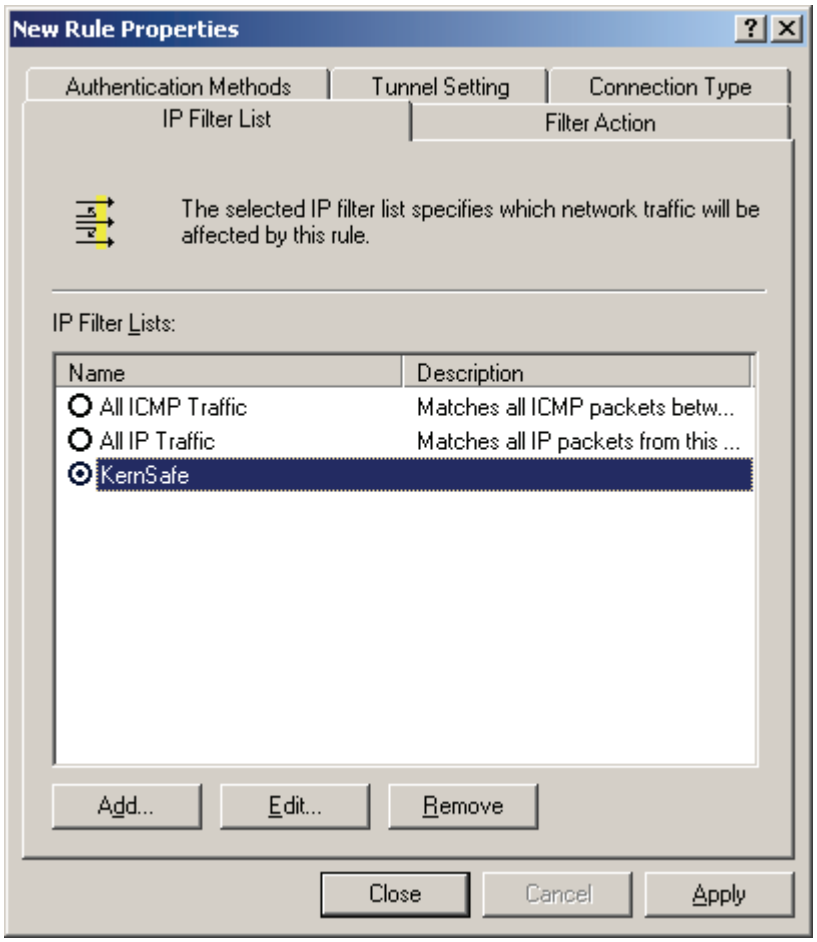
Select TCP in Select a protocol type field.

Type 3260 in the To this port.

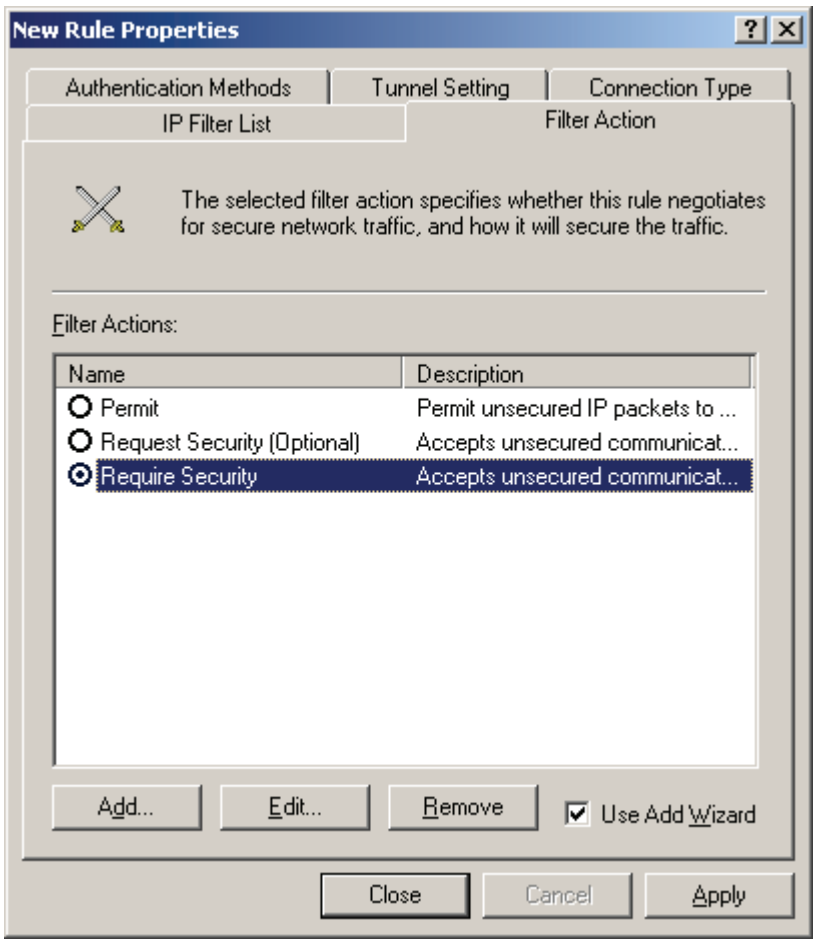
Press the **OK** button to continue.



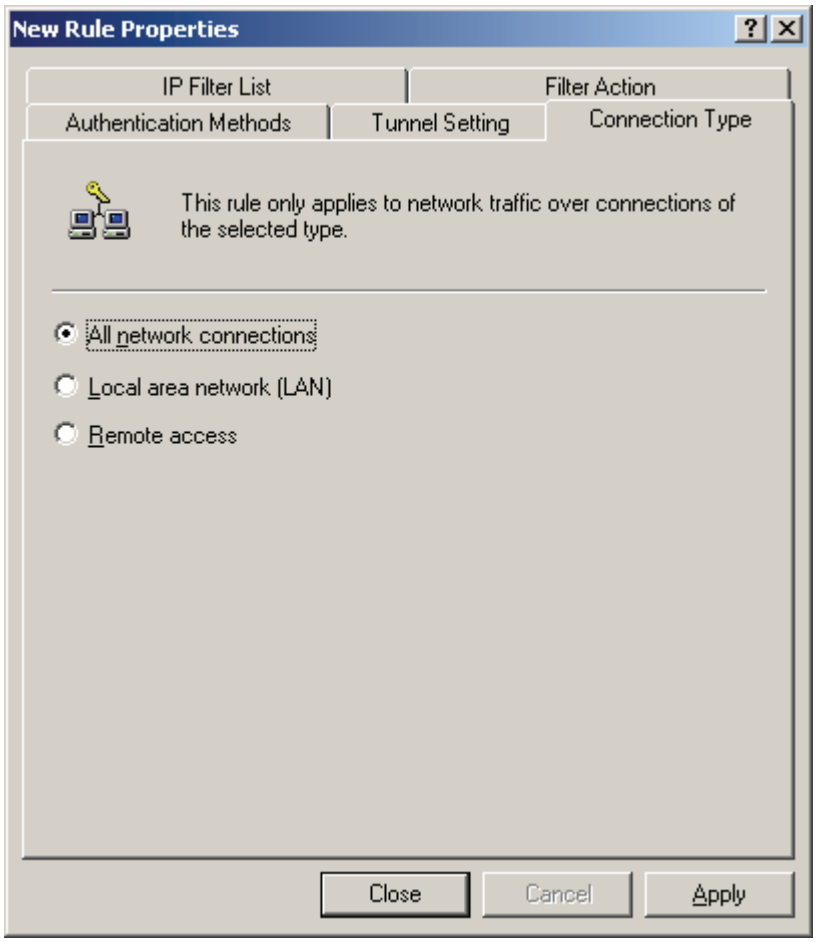
Press the **OK** button to continue.



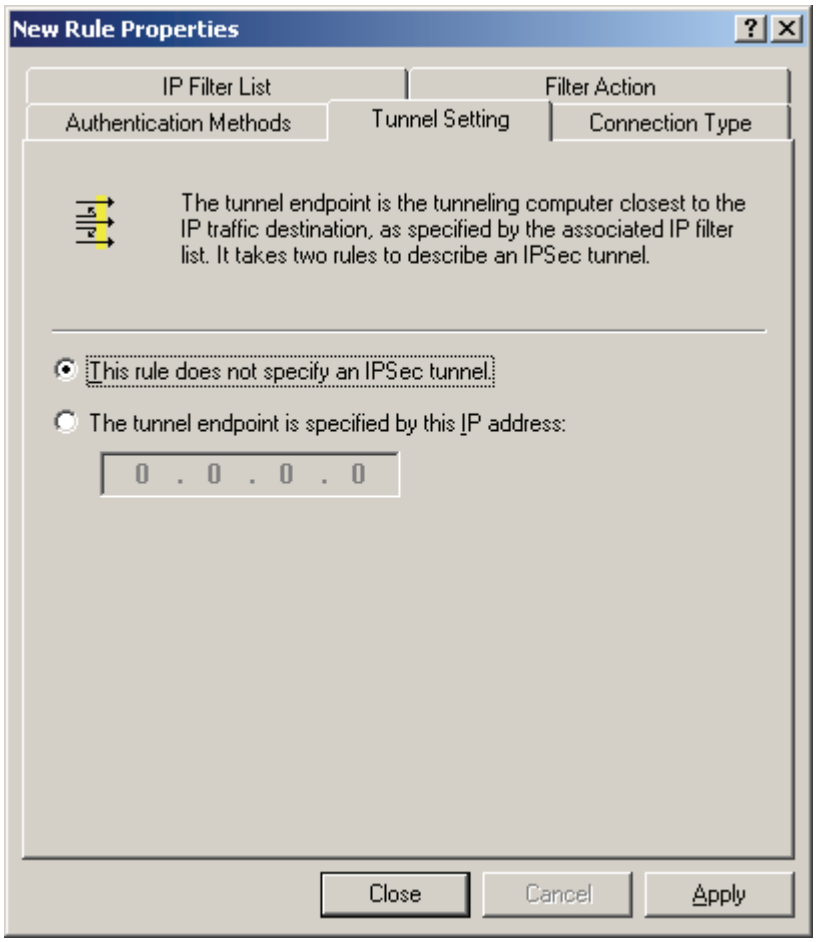
Select the KernSafe IP Filter item which we just created and change to Filter Action page.



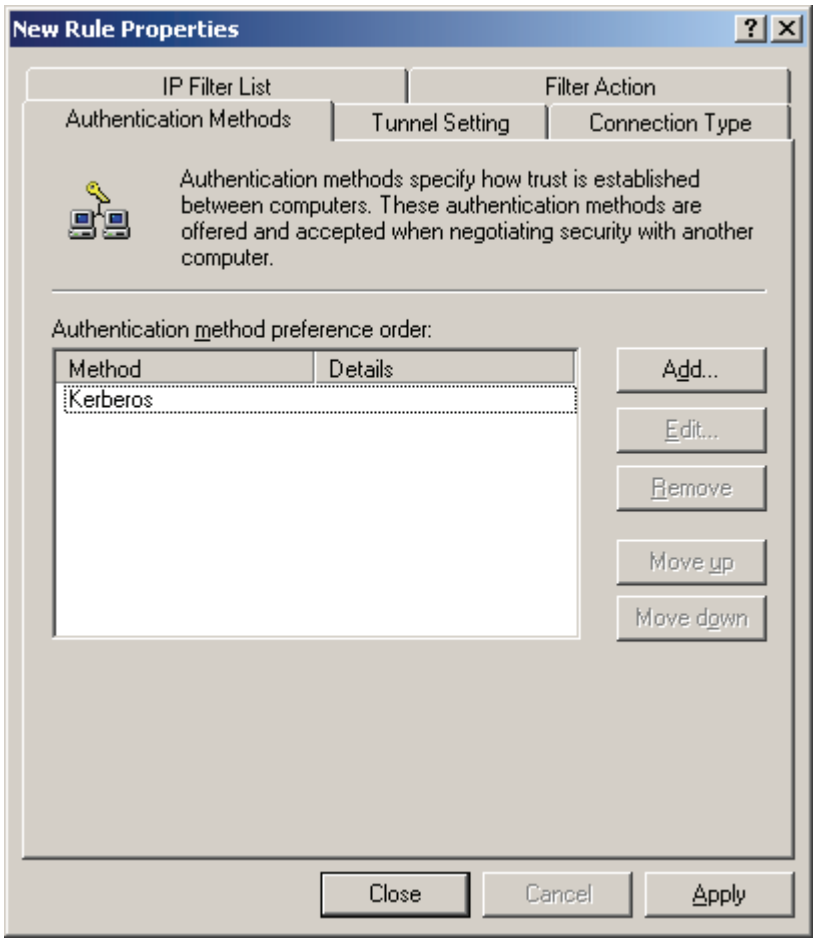
Select Require Security and then change to Connection Type page.



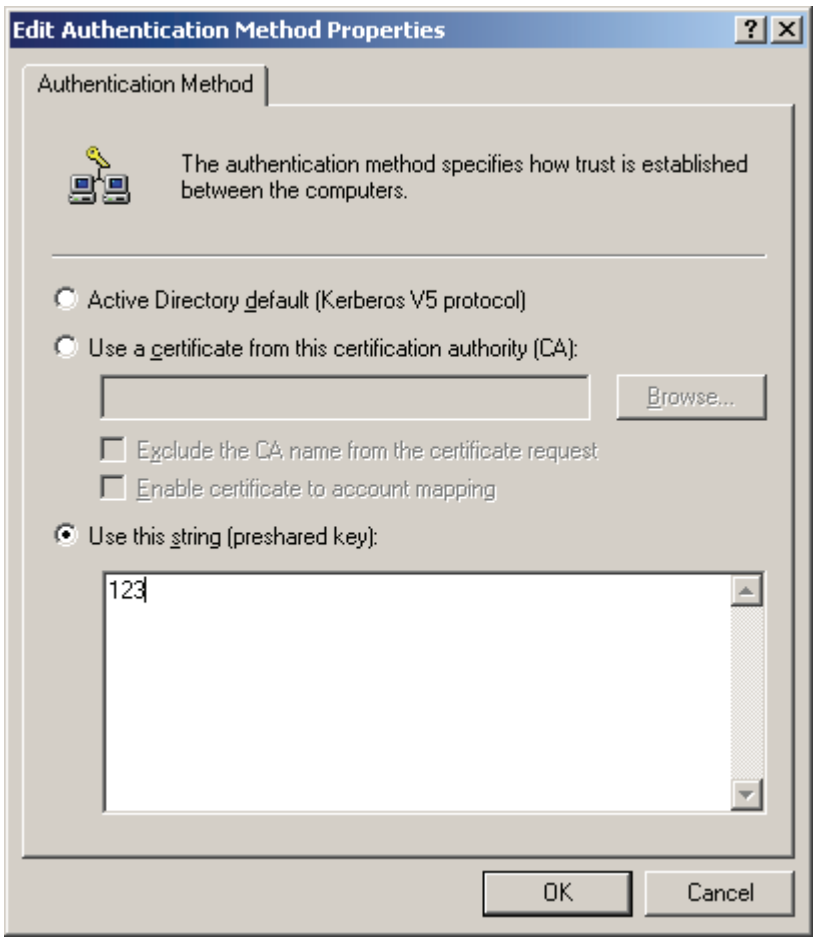
Select the **All network connections**, and then change to **Tunnel Setting** page.



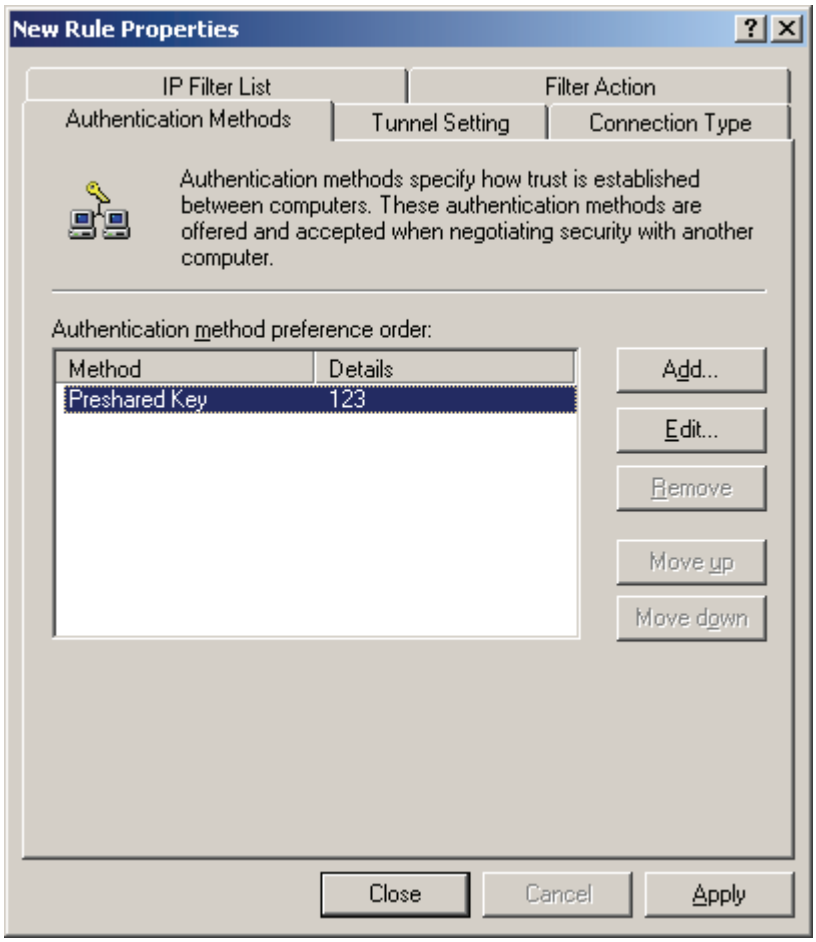
Select **This rule does not specify an IPSec tunnel**, and then change to **Authentication Methods** page.



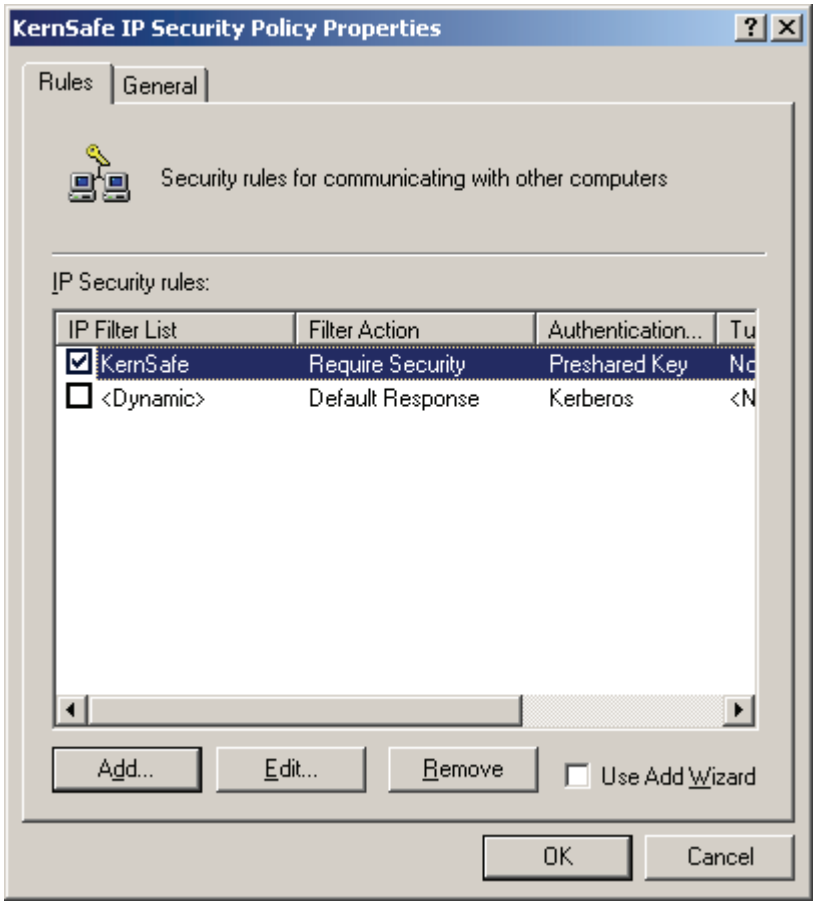
Select Kerberos, press the **Edit** button, the **Edit Authentication Method Properties** dialog is shown.



Select Use this string (preshared key）, type the preshared key, we take “123” as an example.

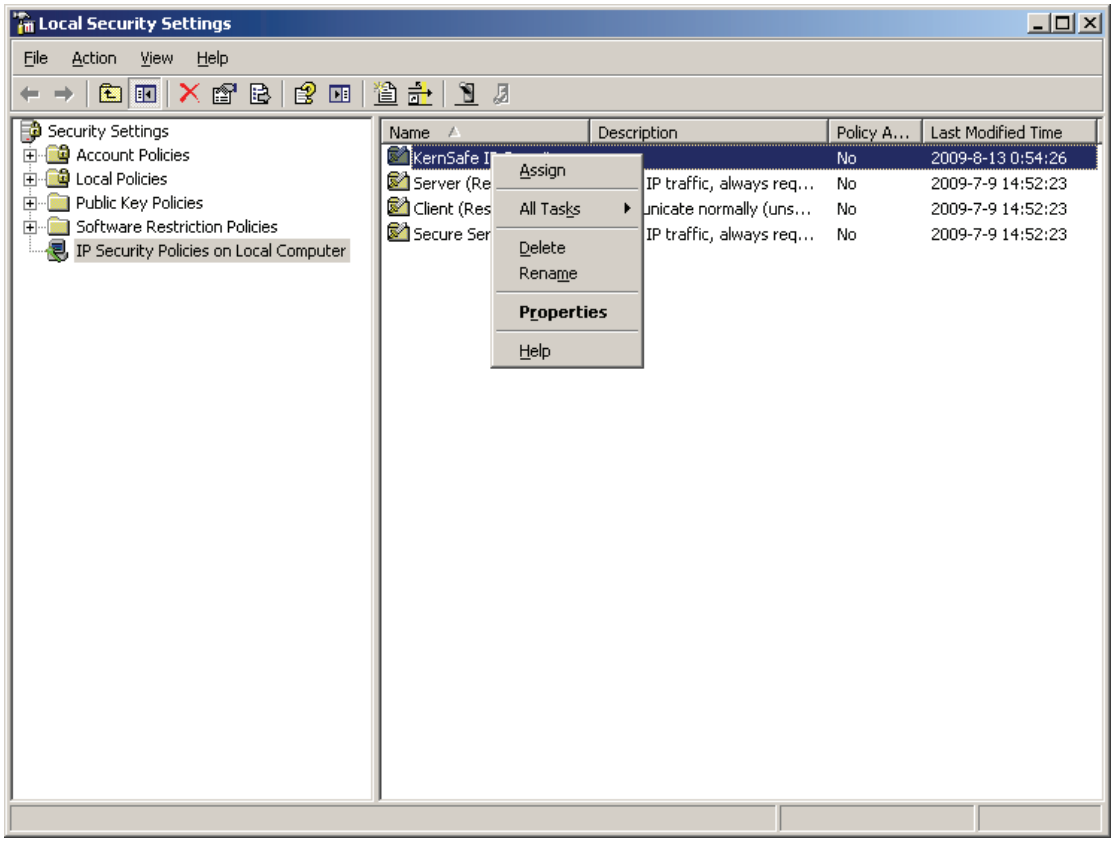


Press the **Apply** button to save settings and press the **Close** button to close this dialog.



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

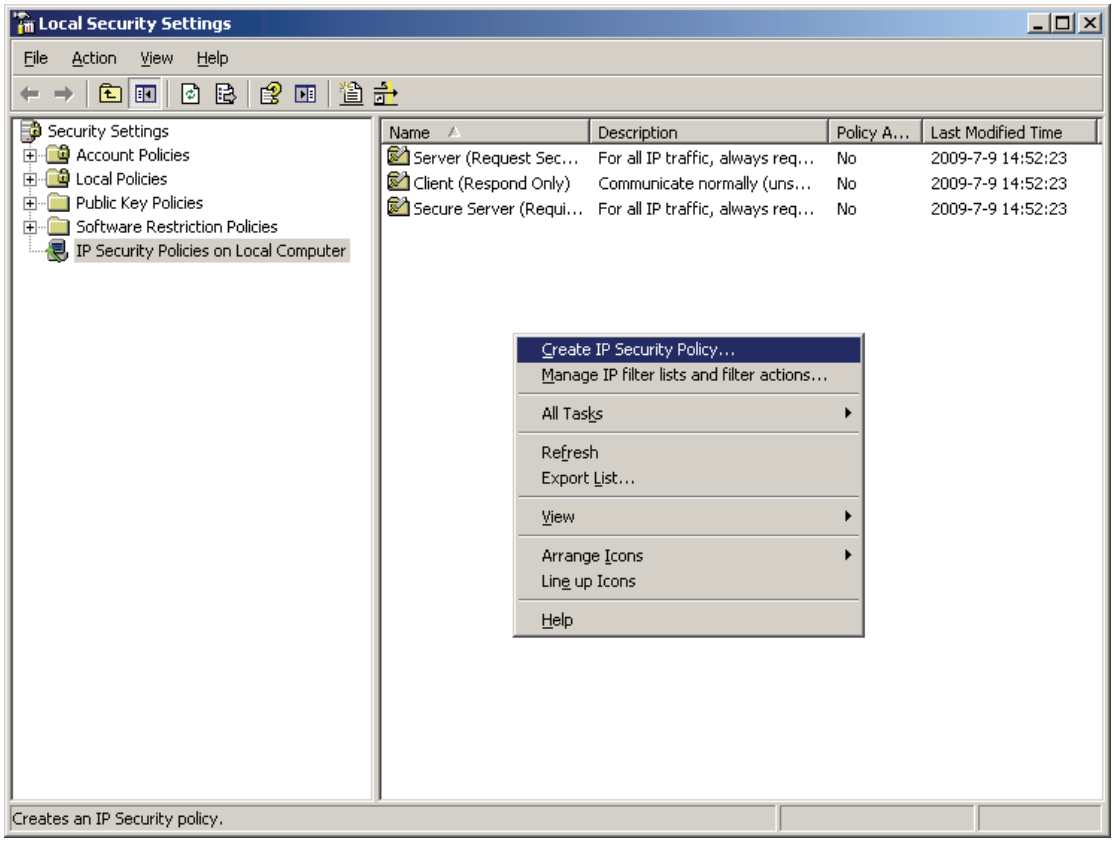
Back to Local Security Settings main interface.



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

3. Client Side Local Security Policy Setting

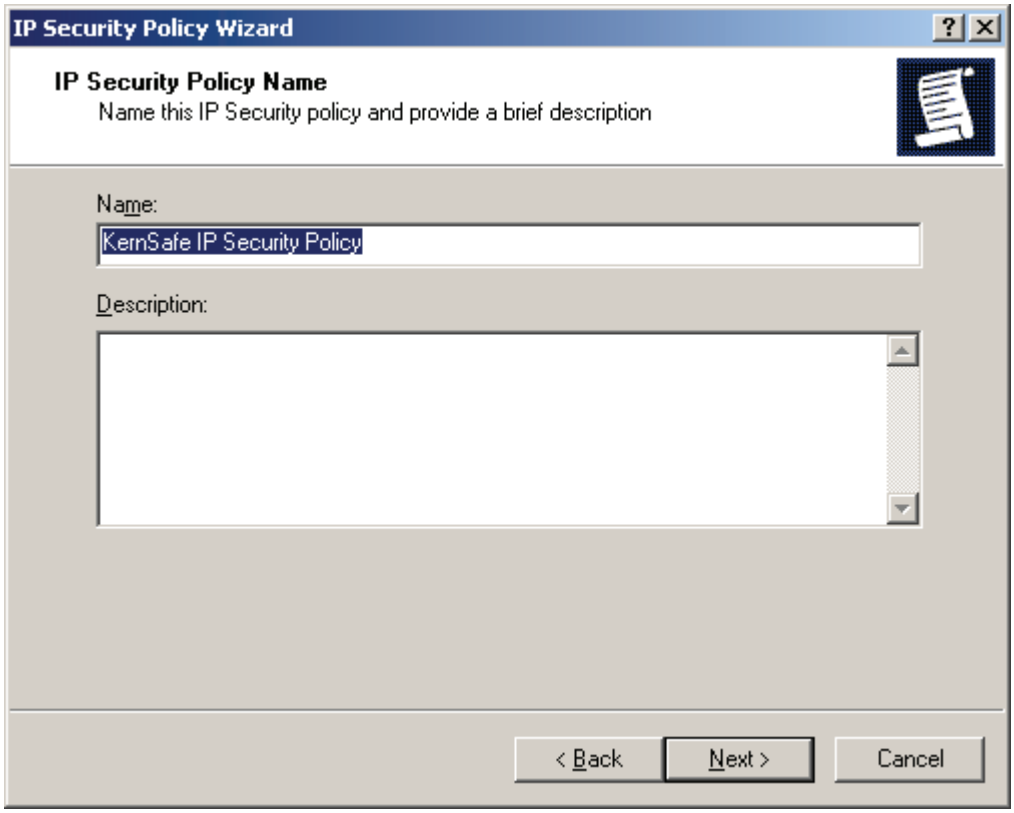
Open Start -> Control Panel -> Administrative Tools -> Local Security Policy, The Local Security Settings Console is shown.



IP Security Policies on Local Computer and right click on the blank of the right panel. Then select **Create IP Security Policy**. The **IP Security Policy Wizard** is shown.

Press the **Next** button to continue.

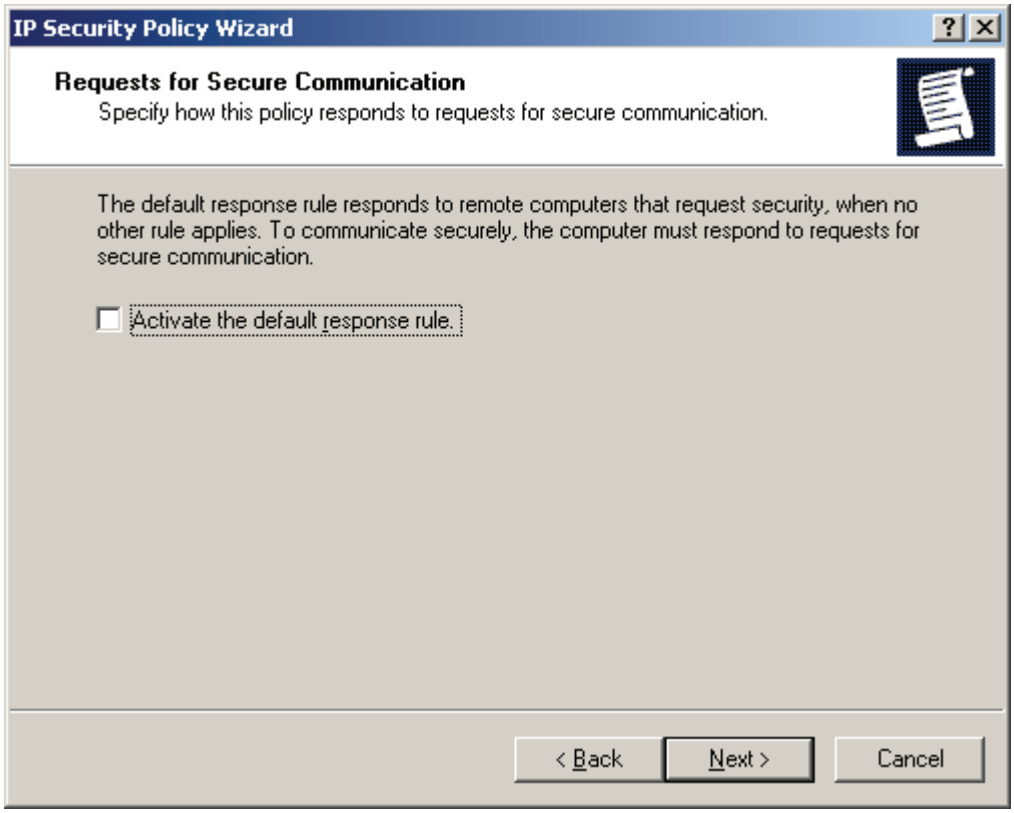
Enter IP Security Policy Name



Type “KernSafe IP Security Policy”.

Press the **Next** button to continue。

Specify how this policy responds to requests for secure communication.



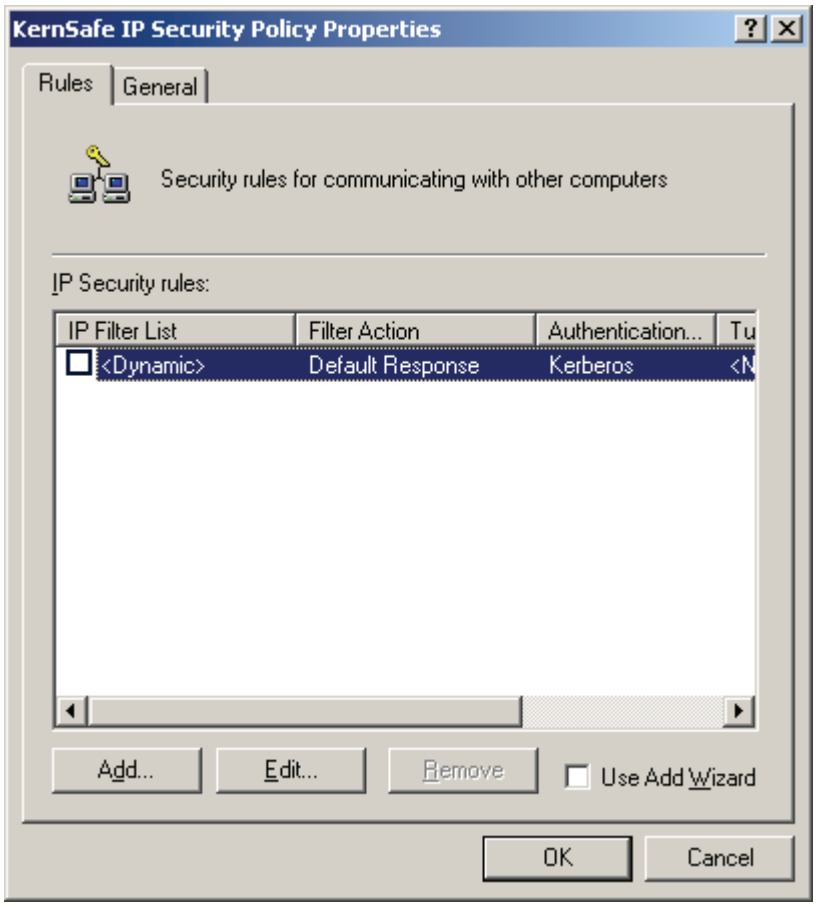
Don’t select the “Activate the default response rule”.

Press the **Next** button to continue.

Completing the IP Security Policy Wizard.

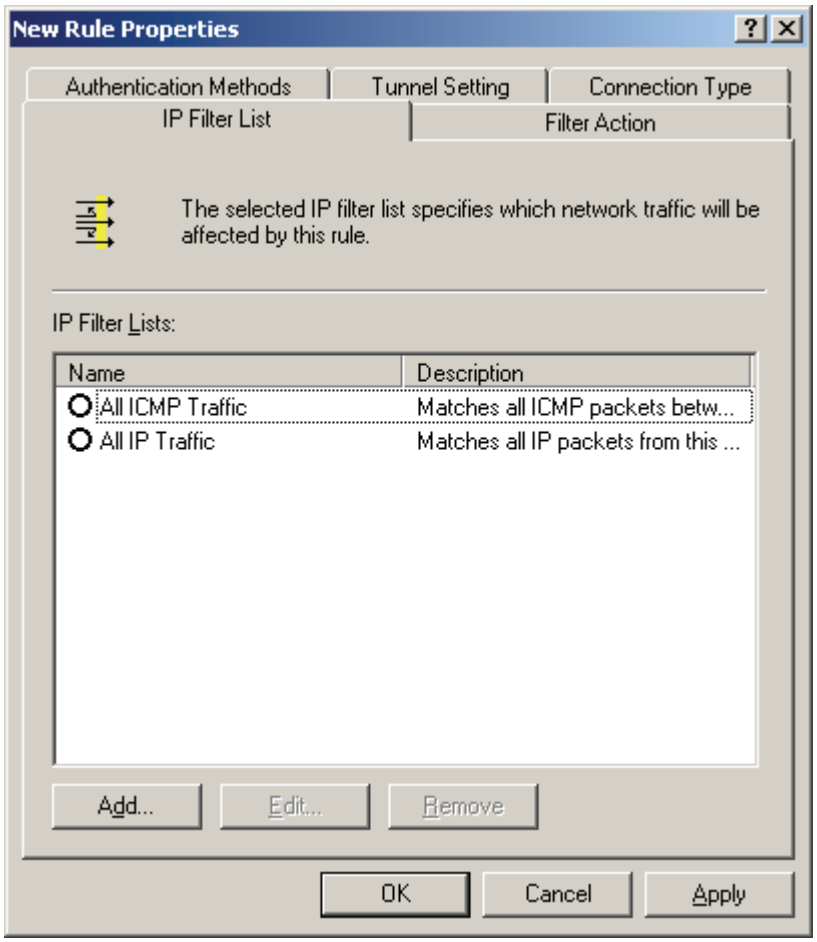
Select the **Edit properties**.
Press the **Finish** button to continue.

The **KernSafe IP Security Policy Properties** Dialog will be shown.



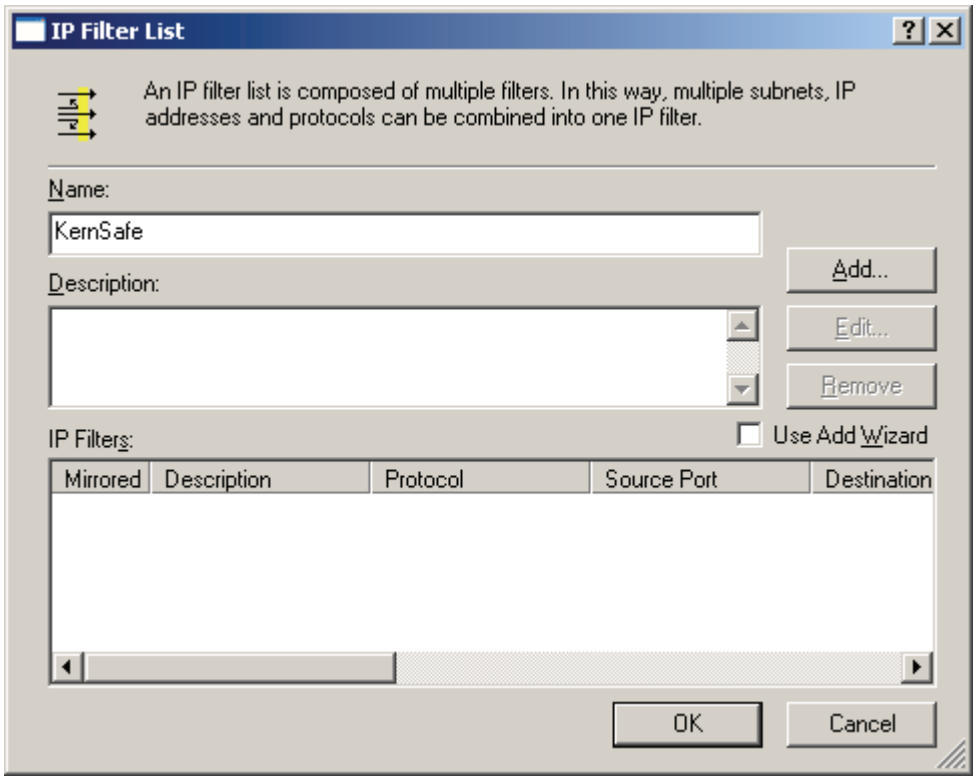
Don’t select the **Use Add Wizard** option.

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



Press the **Add** button to continue.

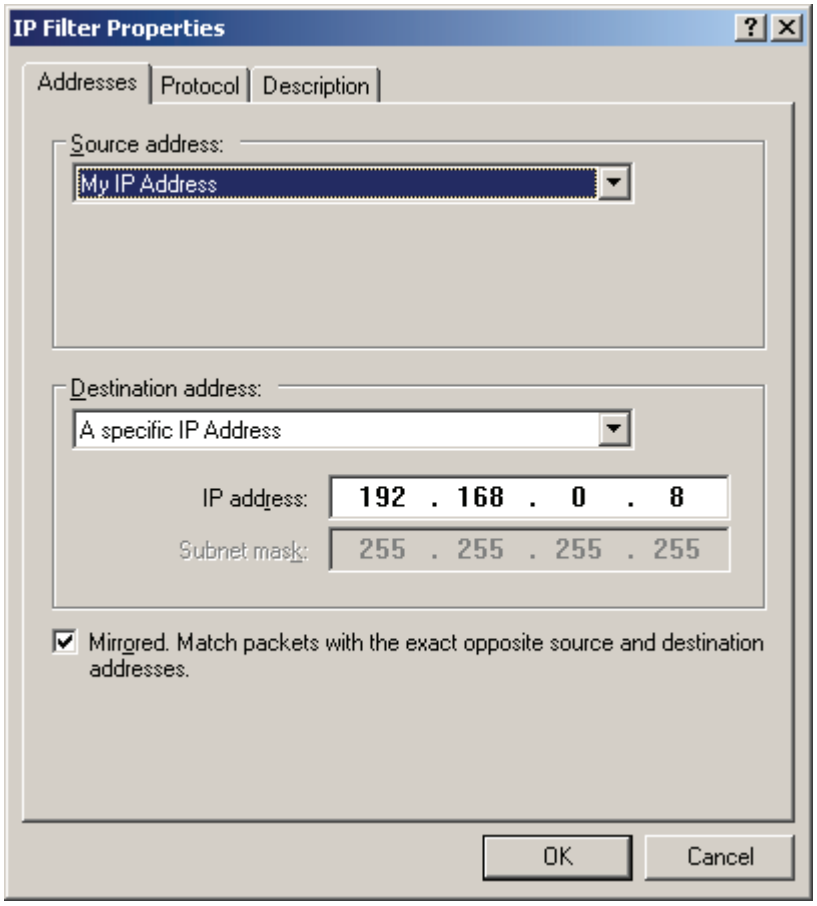
Setting IP Filter List.



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.

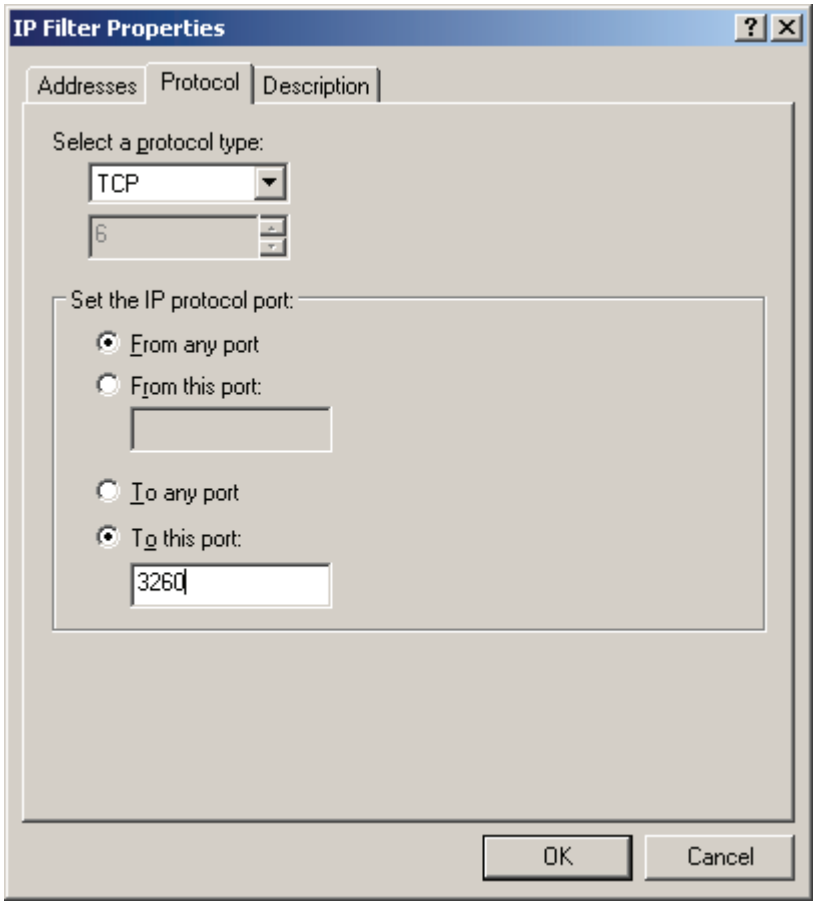


Select **My IP Address** in **Source address** Categories **.**

Select **A specific IP Address** in **Destination address** categories, and then type the IP address of your server machine.

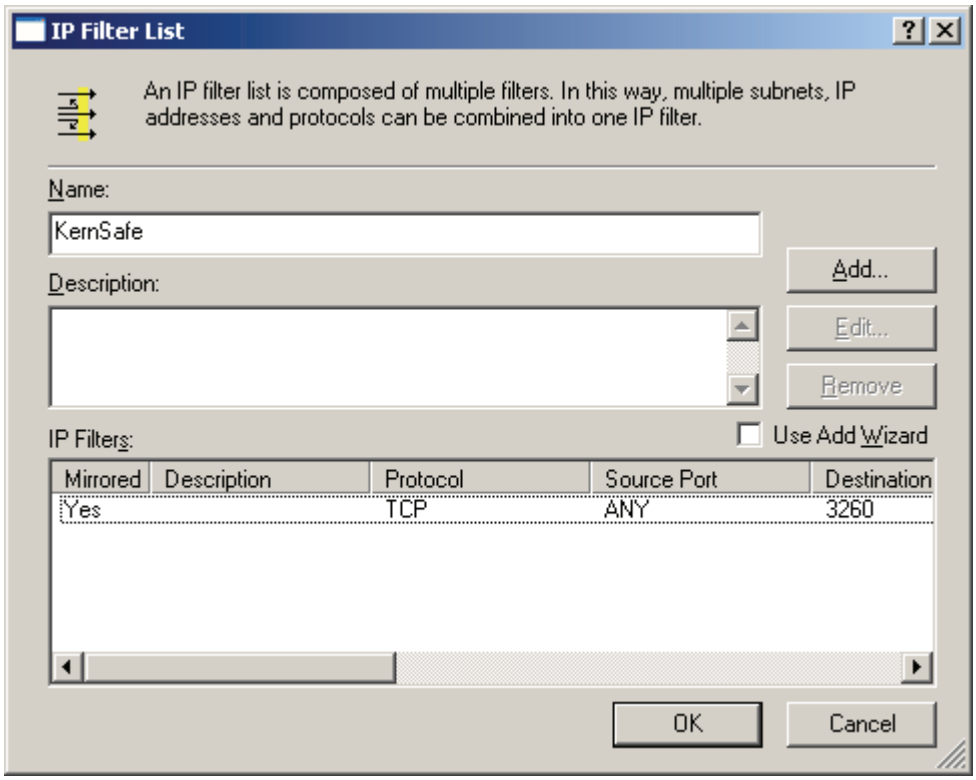
Select the **Protocol** page to continue.

Set protocol properties.

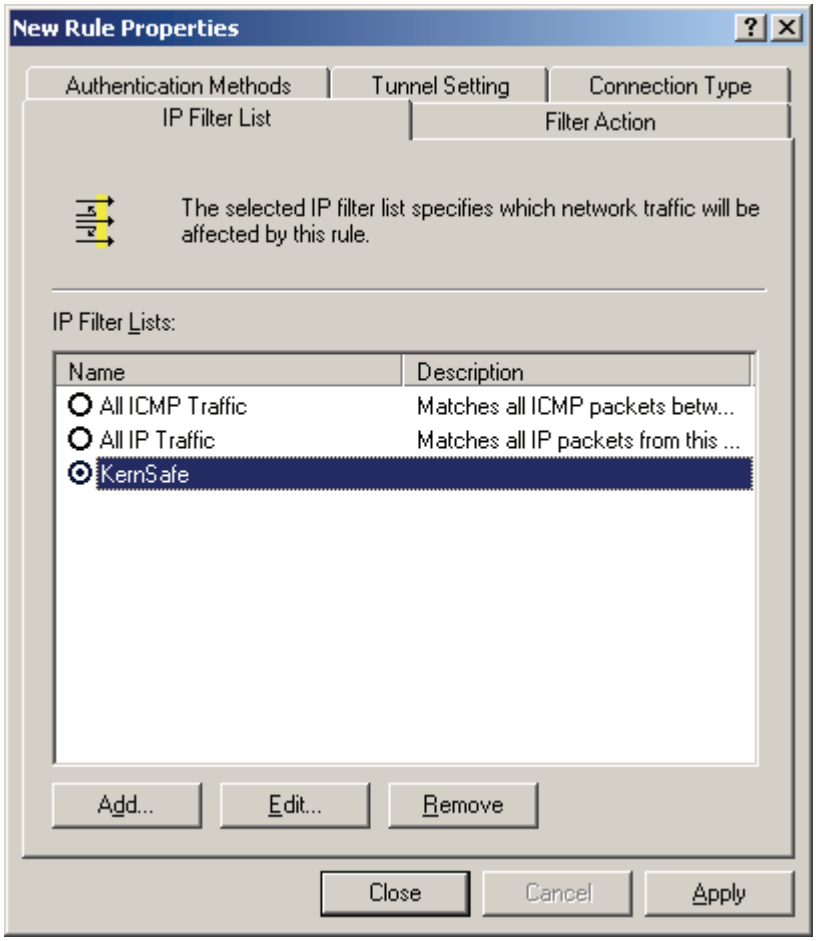


Select **TCP** in the **Select a protocol type** categories, and then type **3260** in the **To this port**. Press the **OK** button to continue.

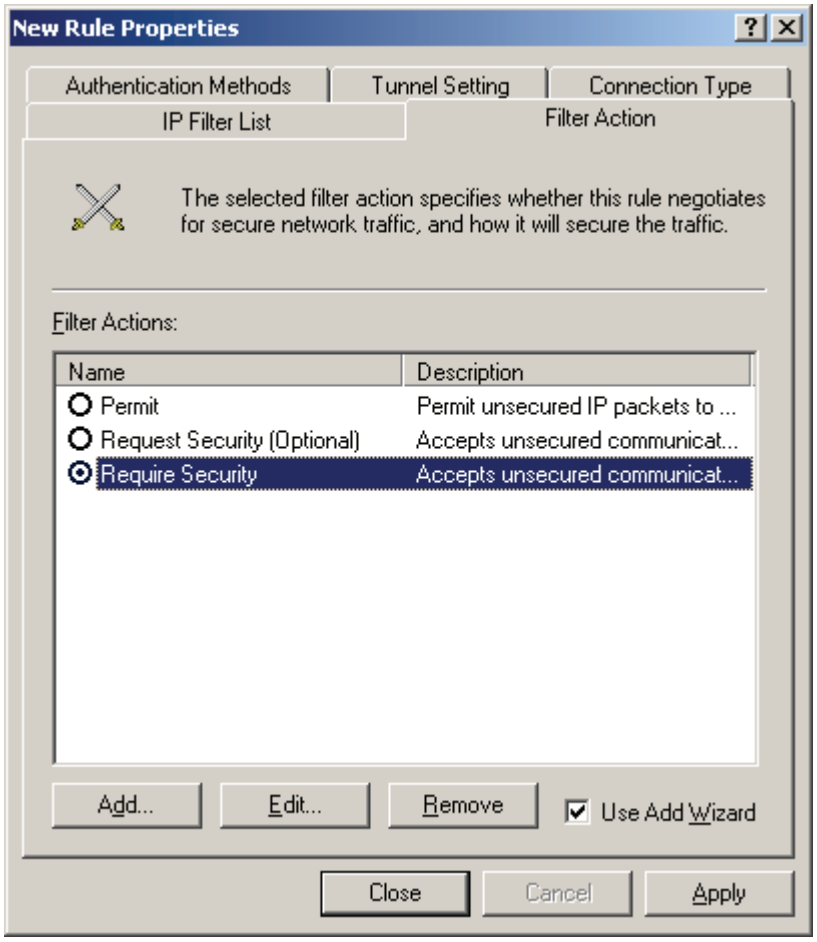
Now we come back to the **IP Filter List** interface.



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

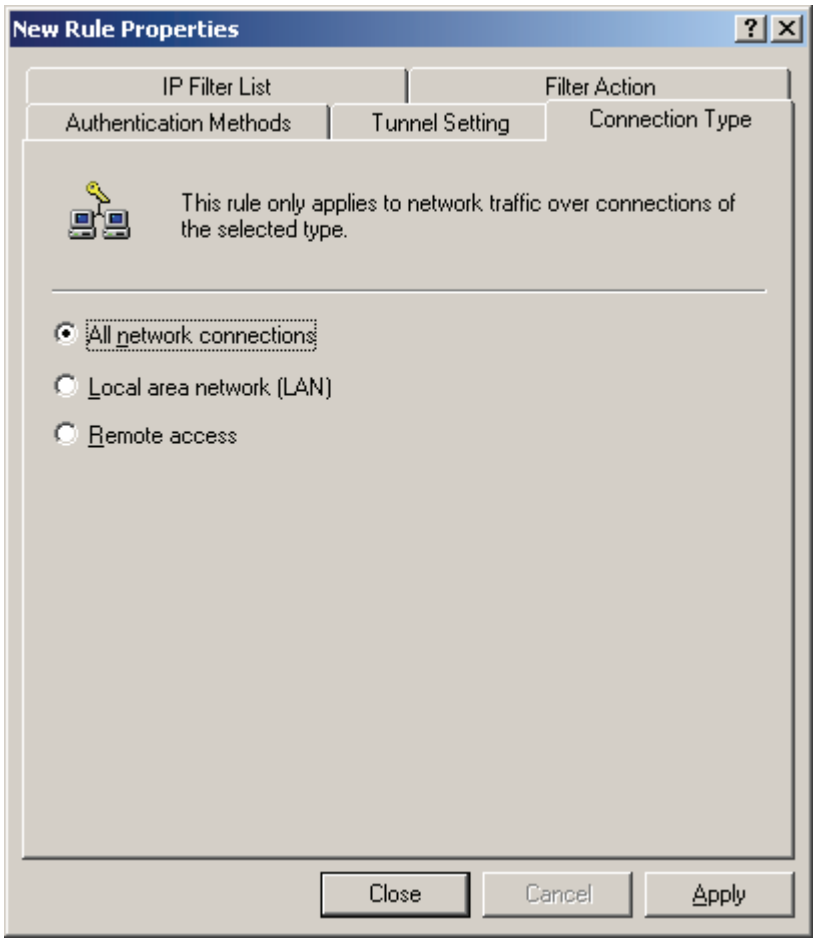


Select the KernSafe IP Filter item we just create. Change to **Filter Action** page.



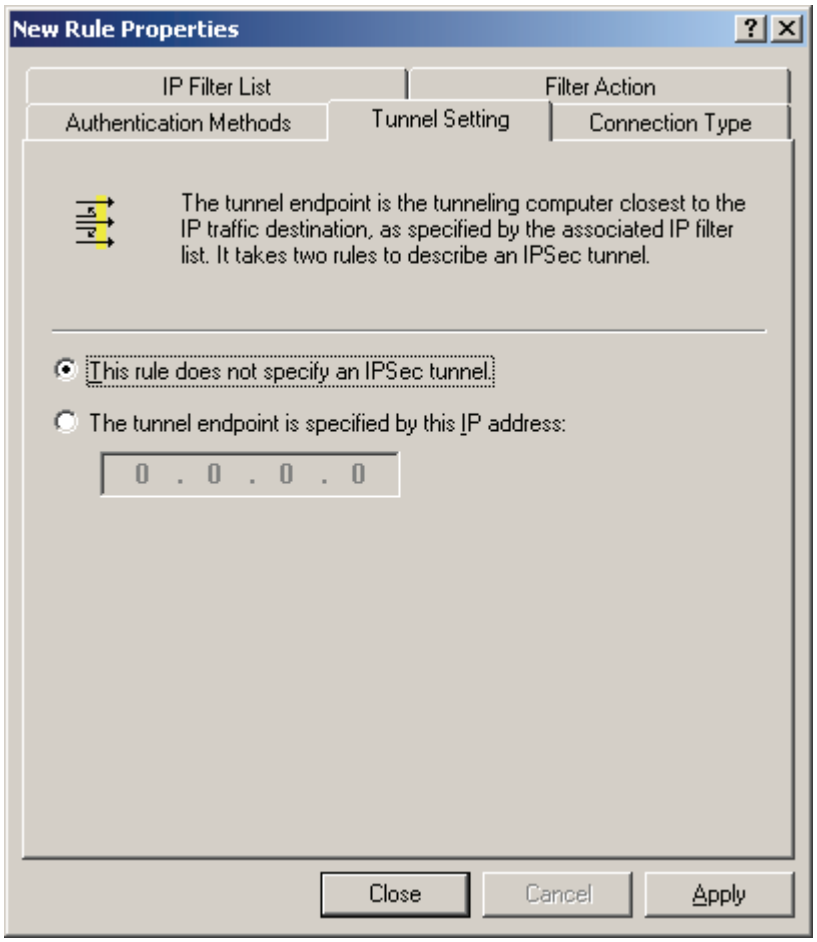
Select **Require Security**.

Change to **Connection Type** page.



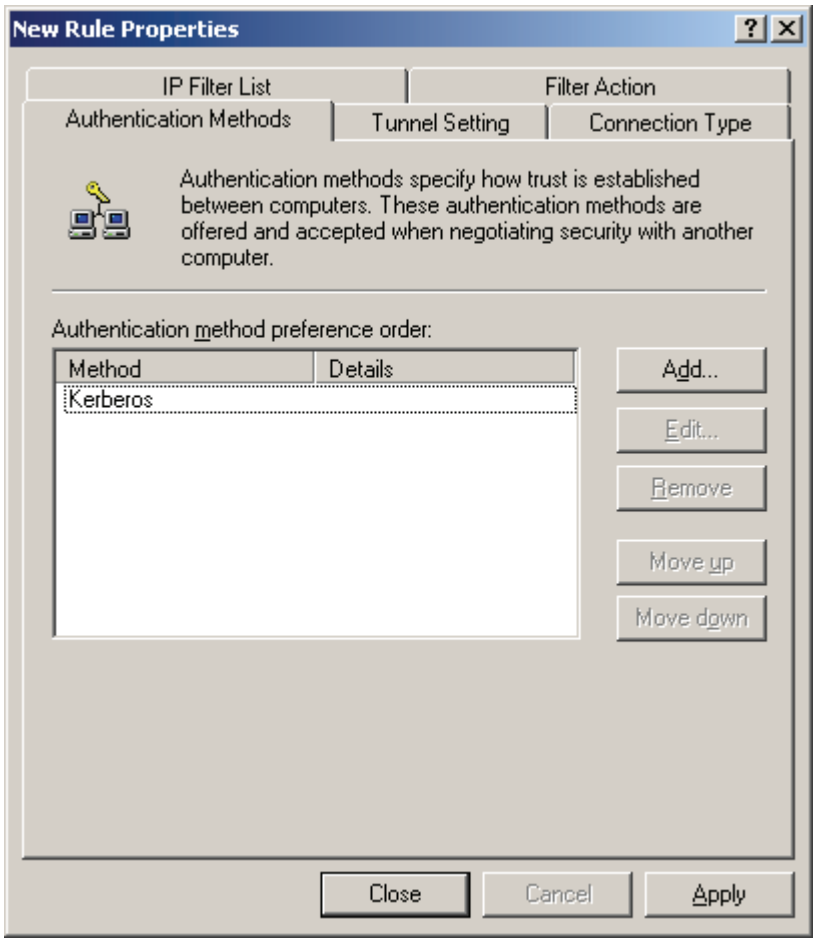
Select **All network connections**.

Change to **Tunnel Setting** page.



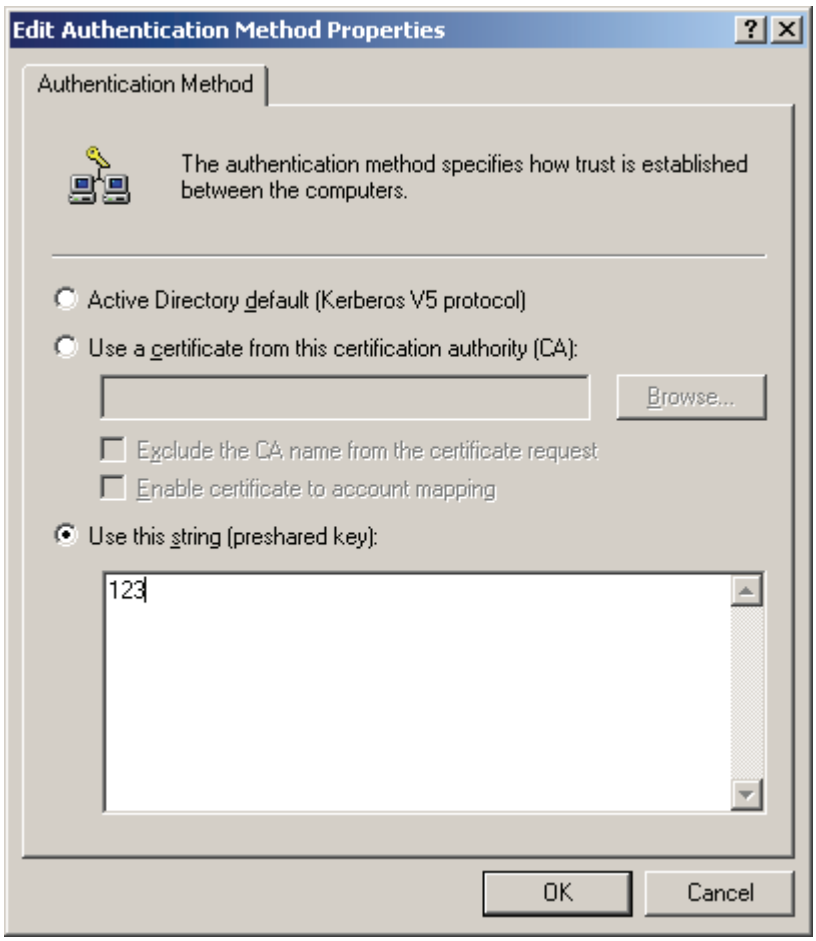
Select **This rule does not specify an IPSec tunnel**.

Change to **Authentication Methods** page.

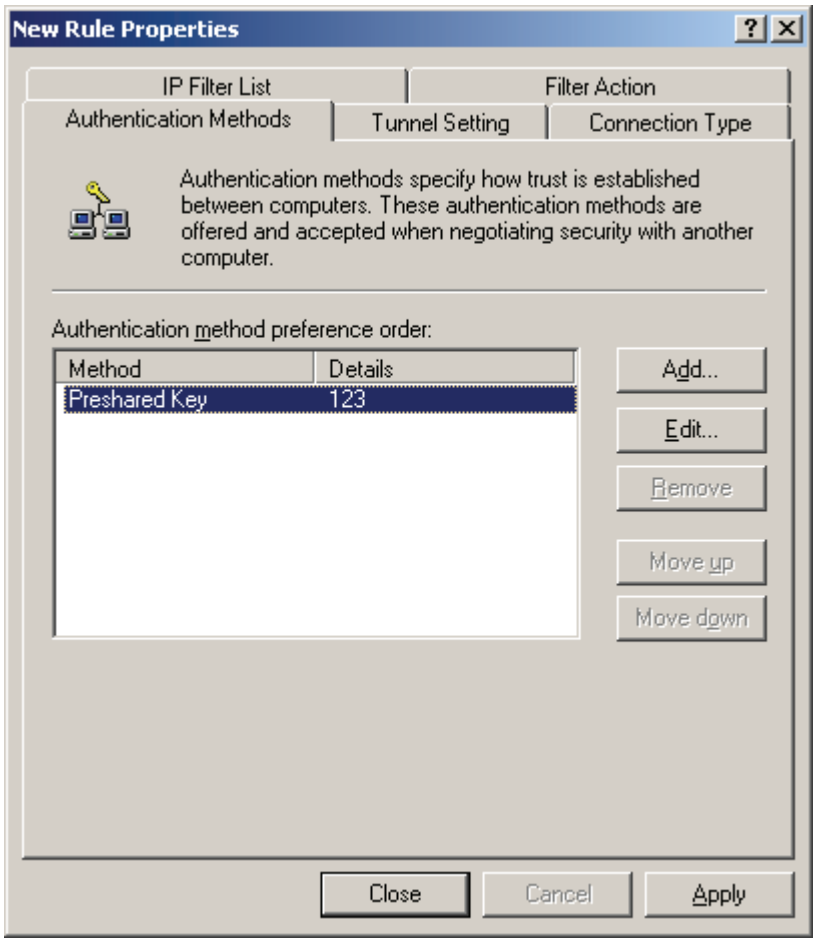


Select **Kerberos**.

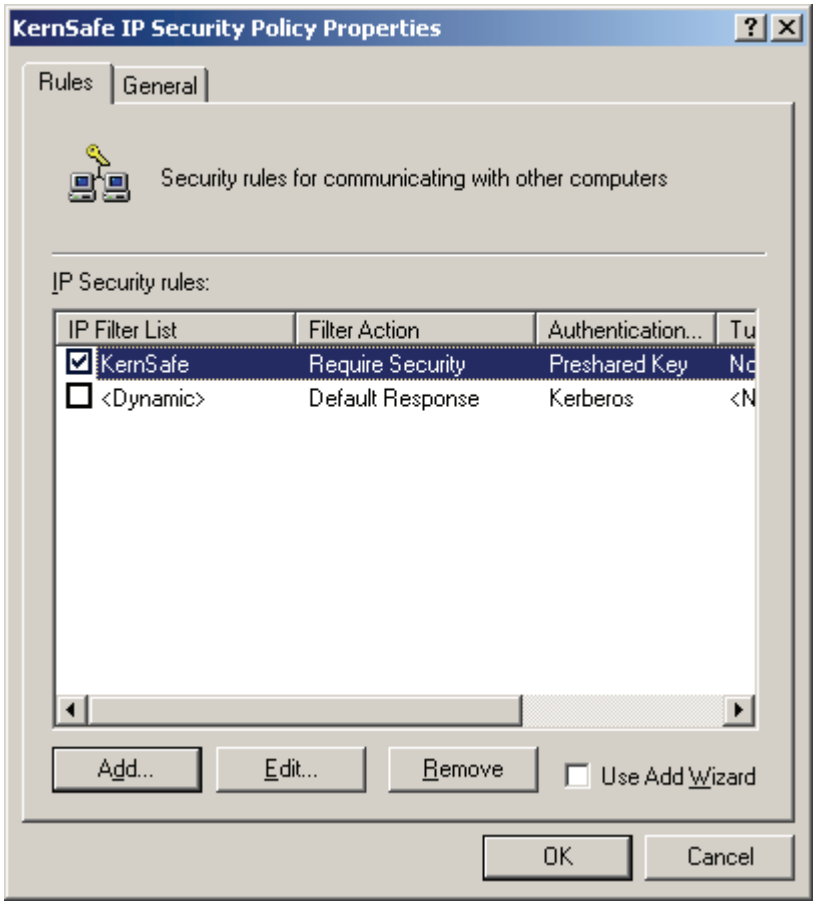
Press the **Edit** button, the **Edit Authentication Method Properties** dialog is shown.



Select **Use this string (preshared key),** then type 123 or other text as password in the input box. Press the **OK** button to apply.

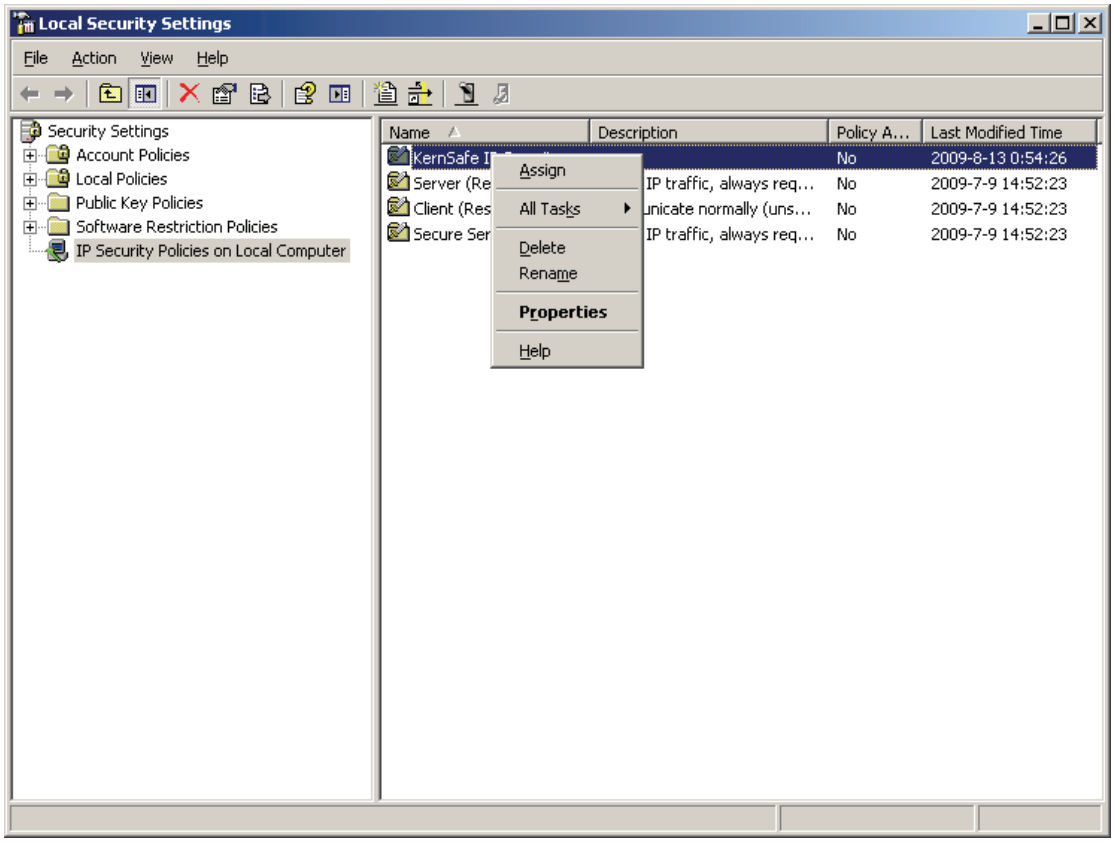


Press the **Apply** button and then press the **Close** button to close this dialog.



Select KernSafe IP Filter item and then press the **OK** button.

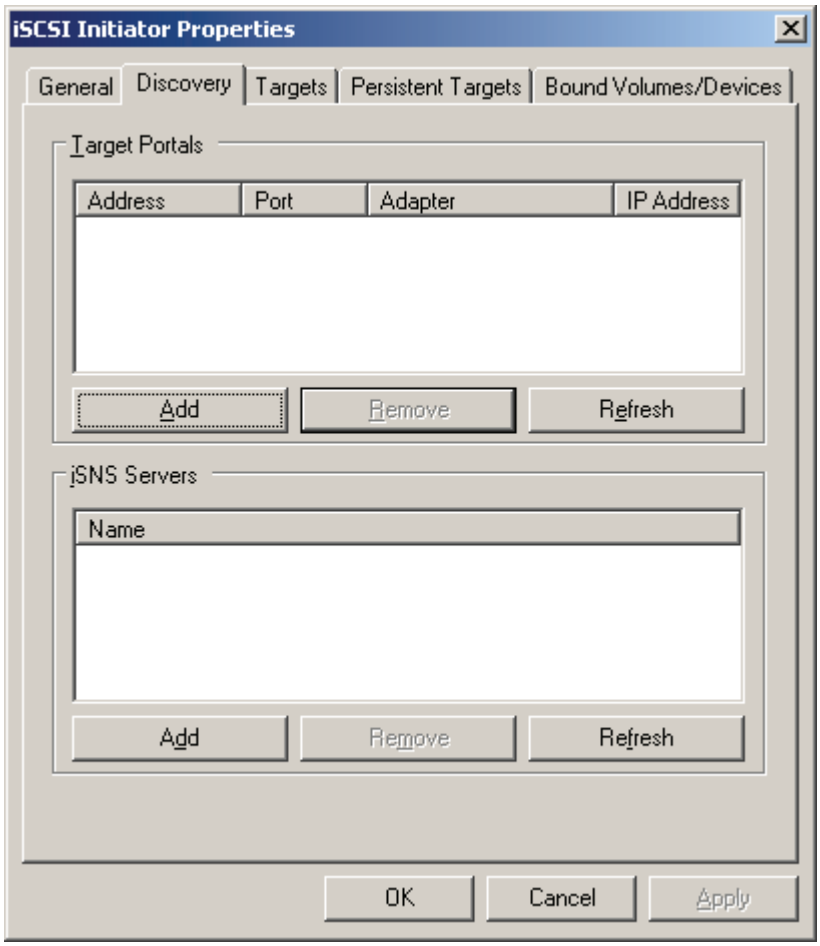
Back to the Local Security Settings Console main interface



Select **IP Security Polices on Local Computer** and then right click on the blank of right panel. Select the **Assign** menu item in the popup menu to make this item enabled.

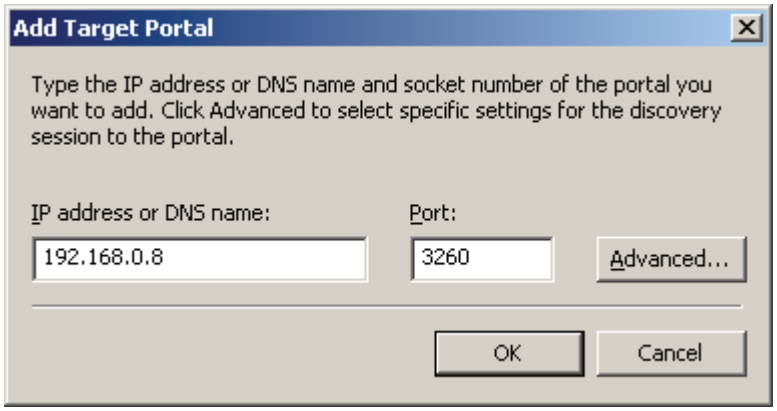
4. Logging on to the target

Open Microsoft Initiator



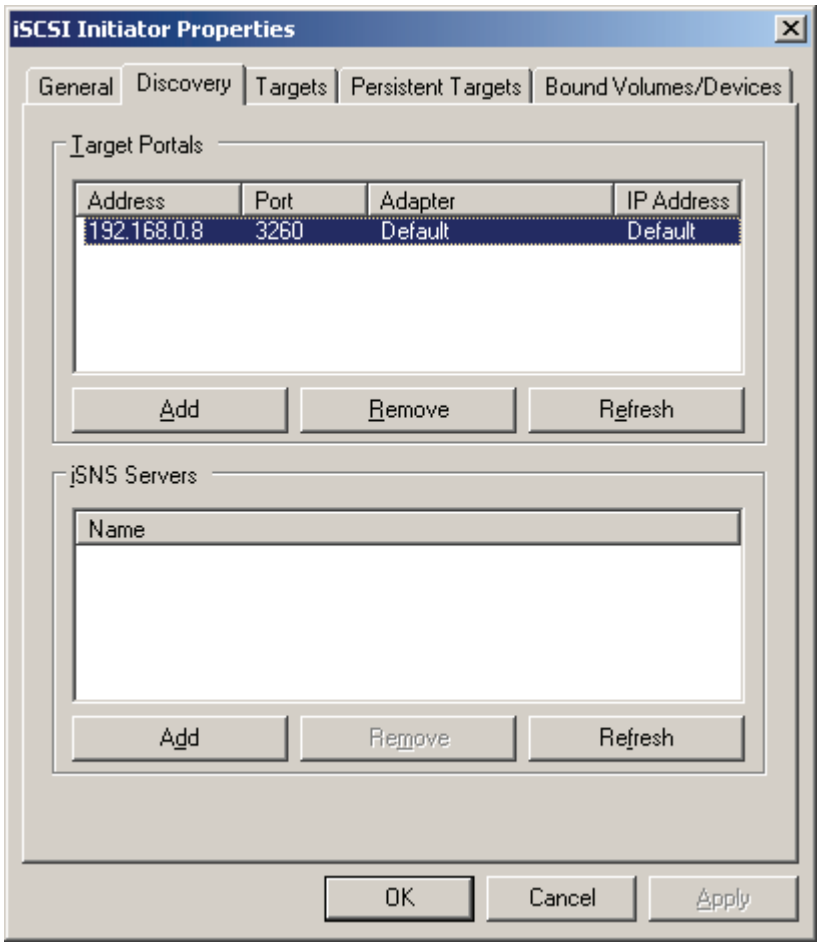
Select the Discovery tab page.

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

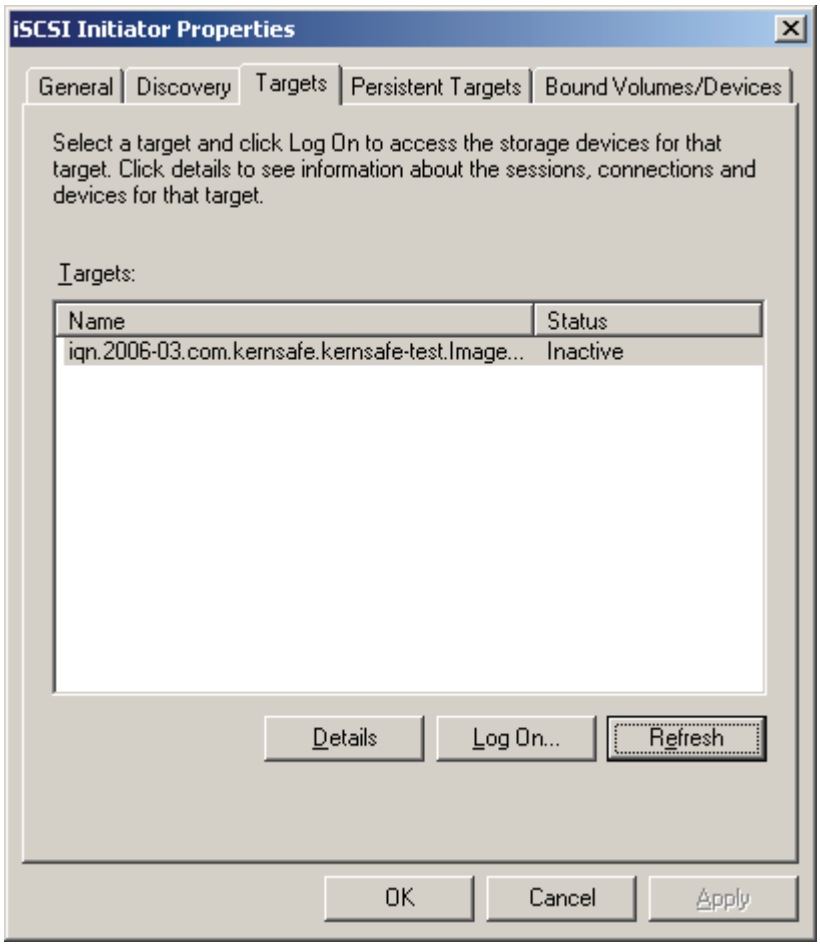


Type the IP address and port of your server.

Press the **OK** button to continue.

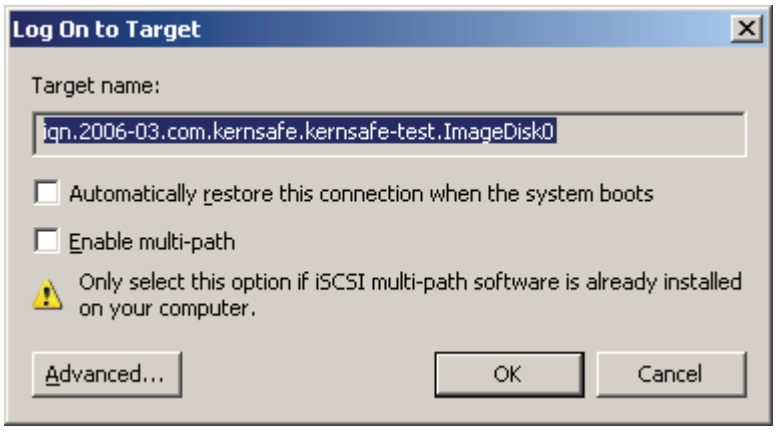


Change to **Targets** page.



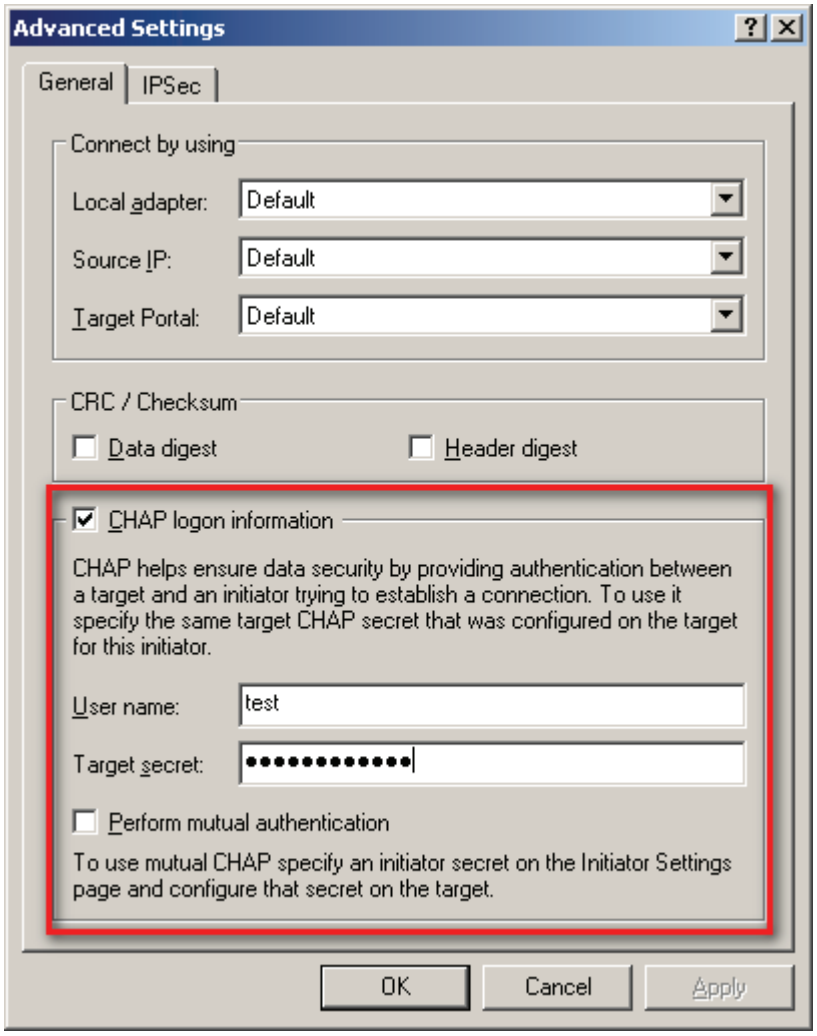
Select the target in the Targets list, and then press the **Log On** button.

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



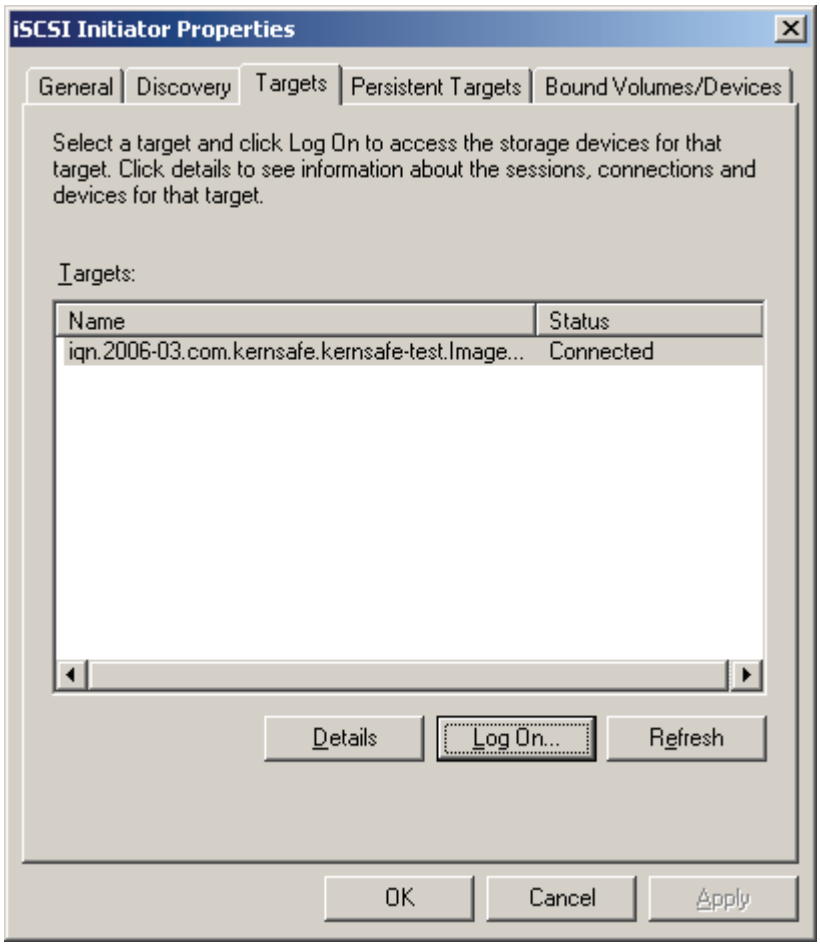
If your iSCSI target using IP filter authorization, just press the **OK** button to continue.

If your iSCSI target using CHAP user authorization, press the **Advance** button, the **Advanced Settings dialog** is shown.



Select CHAP login information and type User name and Target secret.

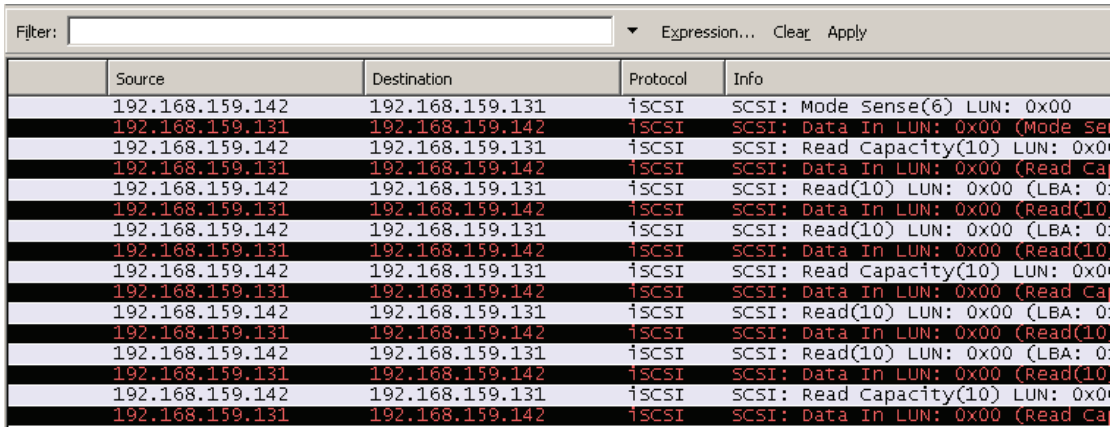
Press the **OK** button to continue.



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

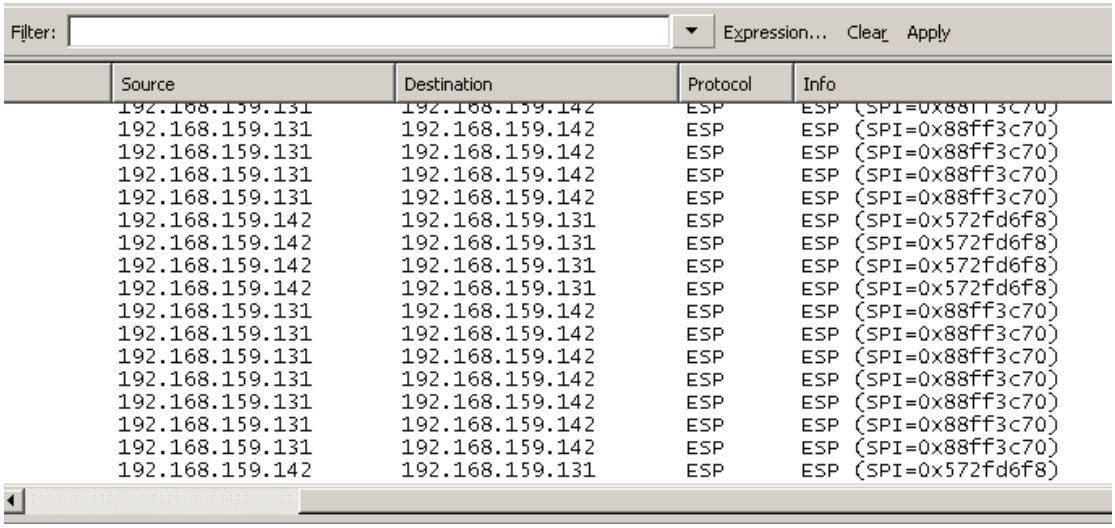
5. Effect

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.