# F-Response with Microsoft IPSEC Configuration Manual

Revision 1 7/1/2008

# Table of Contents

# Welcome to F-Response

Thank you for purchasing F-Response. You have now extended the capabilities of your existing arsenal of tools to enable them to work over an IP network. F-Response accomplishes this through the use of a Patent Pending process; a part of which includes leveraging the Internet Small Computer Systems Interface (iSCSI) protocol standard as defined in RFC 3720 (http://www.ietf.org/rfc/rfc3720.txt).

# Terminology

The iSCSI terms "Target" and "Initiator" are used throughout this manual. The choice of "initiator" and "target" verbiage in the iSCSI definitions may prove confusing to forensics practitioners because "target" carries a different definition in the field of computer forensics versus iSCSI. In computer forensics, the system to be analyzed is generally referred to as the "subject" system, whereas the system to which forensically sound data is collected is generally referred to as the "target" system. In this manual, the forensic "subject" is an iSCSI "target", i.e. F-Response Target code is executed on the machine to be analyzed. For this reason, we want to make clear that the use of the word "target" in this manual refers to the iSCSI definition, and not the forensics definition. The definitions for Target and Initiator used in this manual are as follows:

## *Target*

F-Response Target code is to be executed on the machine(s) to be analyzed. All references to "target" in this manual refer to the machine(s) being analyzed using F-Response target code.

## *Initiator*

An iSCSI "initiator" is used to establish network connections to machines running F-Response Target code. iSCSI initiator software must be installed on the machine from which analysis is to be conducted over the network. F-Response Target code has been tested with Microsoft iSCSI Initiator 2.0 software, included by default with newer Windows operating systems, and freely available for download from the Microsoft web site.

# About F-Response Enterprise Edition

F-Response Enterprise Edition[1] is our premium software offering, and permits use of the entire F-Response software suite, including F-Response Enterprise Edition ("EE") Target Code, F-Response Consultant Edition ("CE") Target code, or F-Response Field Kit ("FK") Target code, depending upon your immediate need. In any case, it utilizes a single stand alone executable ("exe") file, which represents the F-Response Target code. It requires no additional libraries or system updates and is capable of providing remote forensically sound read only physical hard drive connectivity on the following platforms:

- Windows 2000 (Professional, Server, Advanced Server)
- Windows XP (Home, Professional)
- Windows 2003 Server
- Windows Vista (Basic, Home, Business, Premium, Ultimate)
- Windows 2008 (GUI & CLI Versions)

[1] F-Response Enterprise Edition is available at www.f-response.com.

In order to use F-Response Enterprise Edition you will require the following:

1. A valid F-Response License key FOB ("F-Response FOB") which can be purchased from the F-Response Web site www.F-Response.com
2. A copy of the latest F-Response Enterprise Edition ("EE") installation package which is freely available from the F-Response Web site (one-time user registration is required); or a copy of the latest F-Response Consultant Edition ("CE") Target code will be required if you desire to operate in Consultant Edition mode; or a copy of the latest F-Response Field Kit ("FK") Target code will be required if you desire to operate in Field Kit mode.
3. Microsoft iSCSI initiator software, included by default with Windows Vista and Server 2008 operating systems, and freely available for download from the Microsoft web site.

Note: The Microsoft iSCSI Software Initiator is available as a free download from http://www.microsoft.com/downloads for the following operating systems:

- Microsoft Windows 2000
- Microsoft Windows Server 2003
- Microsoft Windows XP

This version should not be installed on the following operating systems:

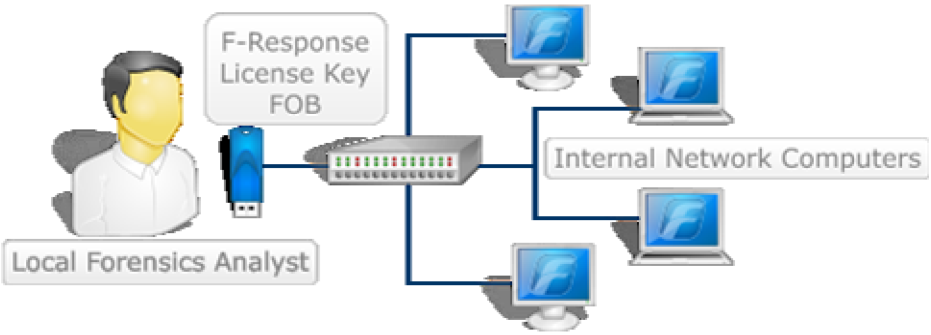
- Windows Vista
- Windows Server 2008

The Microsoft iSCSI Software initiator is integrated into both Windows Vista and Windows Server 2008; therefore there is no need to install this package on those operating system versions.

The Microsoft iSCSI Software initiator configuration utility on Windows Vista and Windows Server 2008 can be accessed from the control panel in classic mode or from administrative tools in Windows Server 2008.

(Source: Microsoft iSCSI Software Initiator 2.x User Guide, Nov 2007)

The diagram below shows a high level architecture for the F-Response Enterprise tool. The F-Response FOB is located at the analysis machine, and the F-Response Target code may be running on any number of corporate networked computers. A command line version of the F-Response Target code may be pre-installed on any number of corporate networked computers so that it is pre-configured and ready for analysis when the need arises. A GUI version of the F-Response Target code is also available for ad hoc use. The Local Forensics Analyst(s) could work remotely if the F-Response FOB is located on a dedicated machine in the enterprise to which they securely (e.g. VPN) connect from remote.

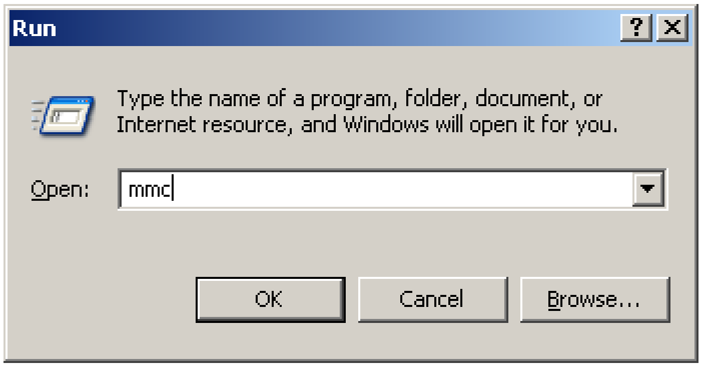


*F-Response Enterprise High Level Architecture*

# F-Response Enterprise Edition and Microsoft IPSEC

This document outlines the procedure required to create Microsoft IPSEC policies for use with F-Response. While the document makes frequent mention of F-Response Enterprise, the Microsoft IPSEC Policies developed using this document would apply to any and all F-Response TCP network traffic on port 3260.

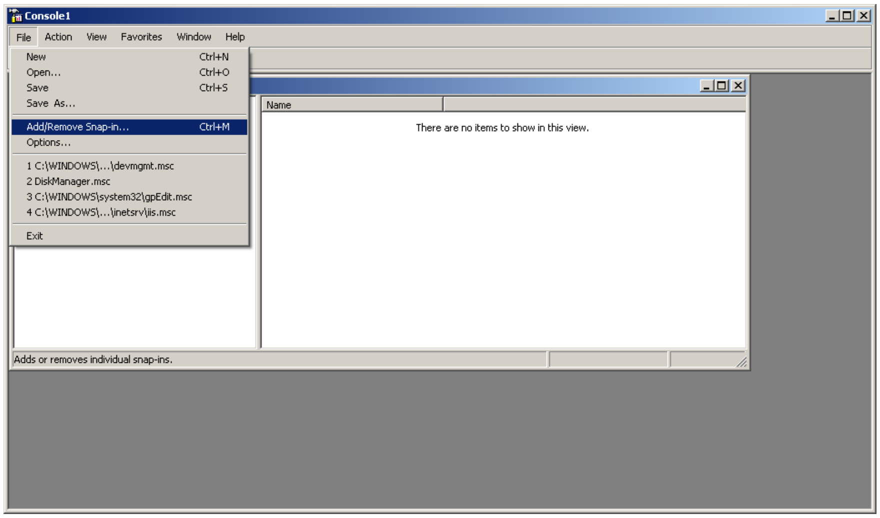
# Configuring an Microsoft IPSEC Policy for the Initiator Workstation



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: mmc

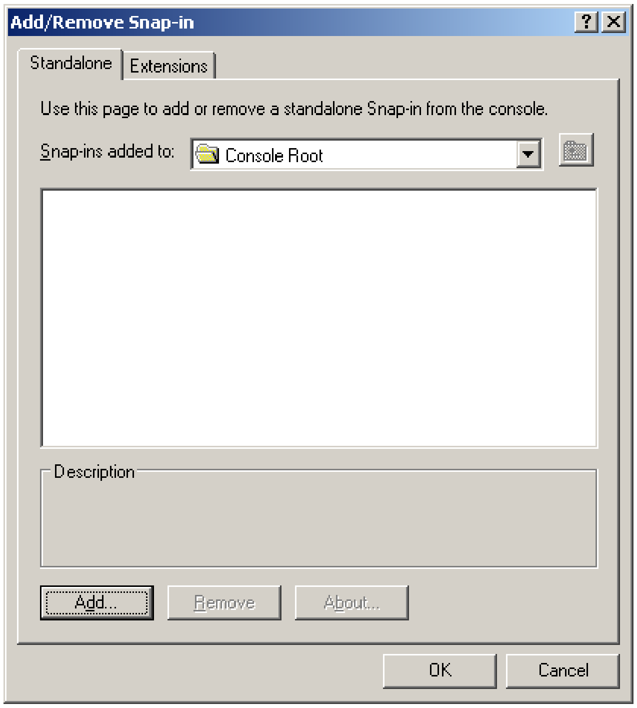
**Start by accessing the Microsoft Management Console or MMC.**



There are no items to show in this view.

Adds or removes individual snap-ins.

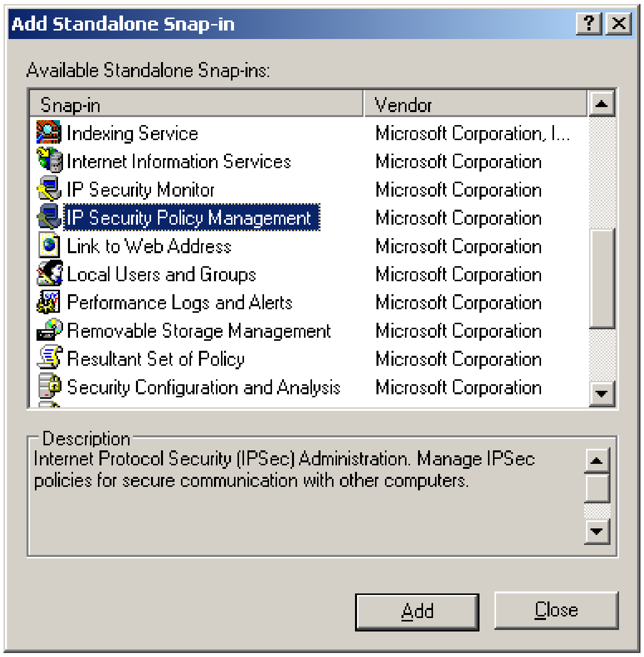
**Next select File Add/Remove Snap-In..**



Use this page to add or remove a standalone Snap-in from the console.

Snap-ins added to: Console Root

**Press the Add.. button to select a Standalone Snap-in**

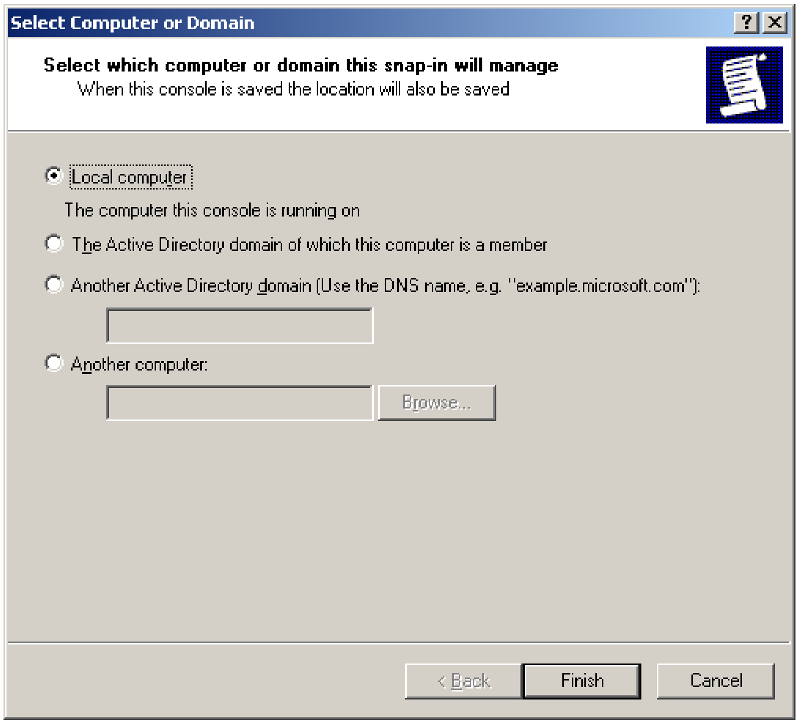


Available Standalone Snap-ins:

| Snap-in | Vendor |
|---|---|
| Indexing Service | Microsoft Corporation, I... |
| Internet Information Services | Microsoft Corporation |
| IP Security Monitor | Microsoft Corporation |
| IP Security Policy Management | Microsoft Corporation |
| Link to Web Address | Microsoft Corporation |
| Local Users and Groups | Microsoft Corporation |
| Performance Logs and Alerts | Microsoft Corporation |
| Removable Storage Management | Microsoft Corporation |
| Resultant Set of Policy | Microsoft Corporation |
| Security Configuration and Analysis | Microsoft Corporation |

Internet Protocol Security (IPSec) Administration. Manage IPSec policies for secure communication with other computers.

**Select the IP Security Policy Management Snap-in.**

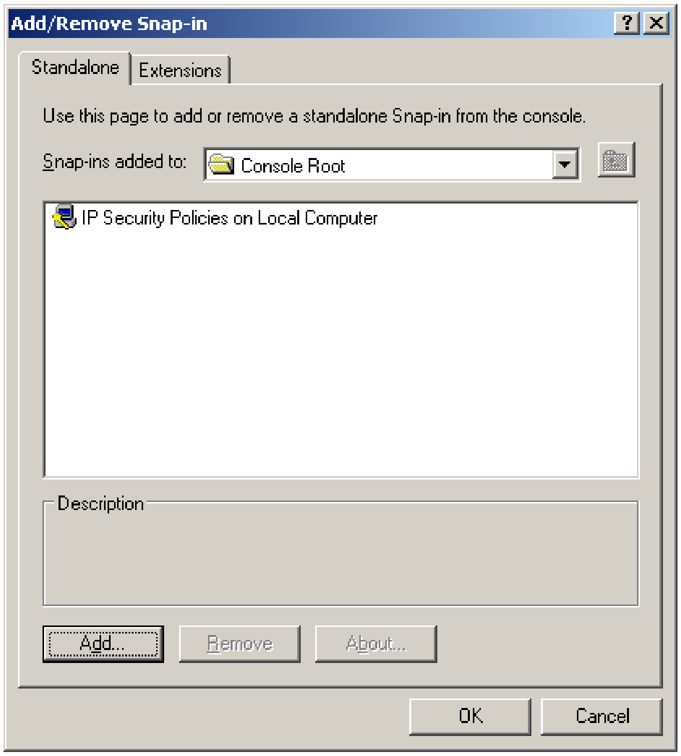


Select Computer or Domain

**Select which computer or domain this snap-in will manage**
When this console is saved the location will also be saved

● Local computer
The computer this console is running on
○ The Active Directory domain of which this computer is a member
○ Another Active Directory domain (Use the DNS name, e.g. "example.microsoft.com"):
○ Another computer:

**Select the computer this Snap-in will manage, in this instance it will be the local computer.**



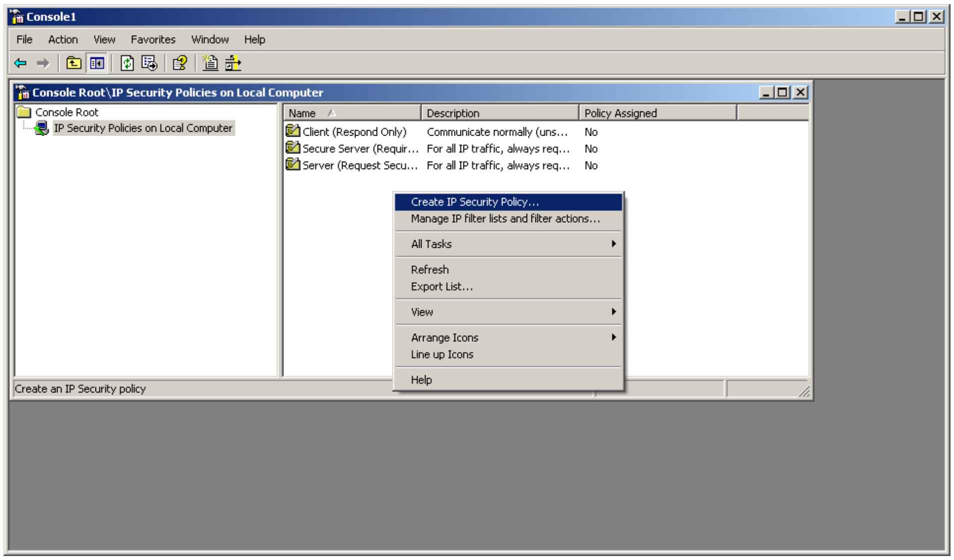
Add/Remove Snap-in

Use this page to add or remove a standalone Snap-in from the console.

Snap-ins added to: Console Root

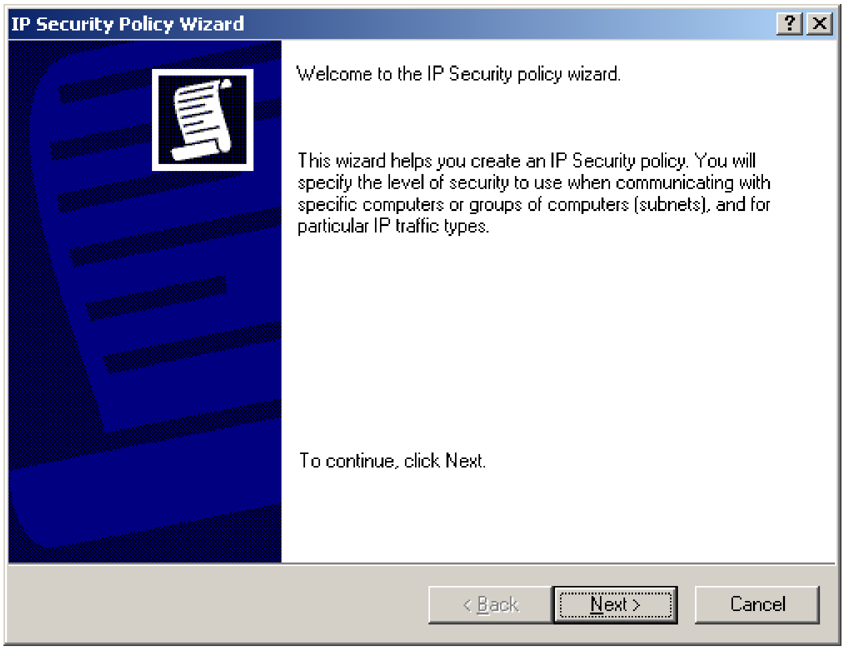
IP Security Policies on Local Computer

**Press Ok to complete the add process and begin using the management console.**


Console1
File Action View Favorites Window Help
Console Root\IP Security Policies on Local Computer
Console Root
IP Security Policies on Local Computer
Create IP Security Policy...
Manage IP filter lists and filter actions...
All Tasks
Refresh
Export List...
View
Arrange Icons
Line up Icons
Help
Create an IP Security policy

| Name | Description | Policy Assigned |
|---|---|---|
| Client (Respond Only) | Communicate normally (uns... | No |
| Secure Server (Requir... | For all IP traffic, always req... | No |
| Server (Request Secu... | For all IP traffic, always req... | No |

**Next right click in the right side pane and select "Create IP Security Policy"**

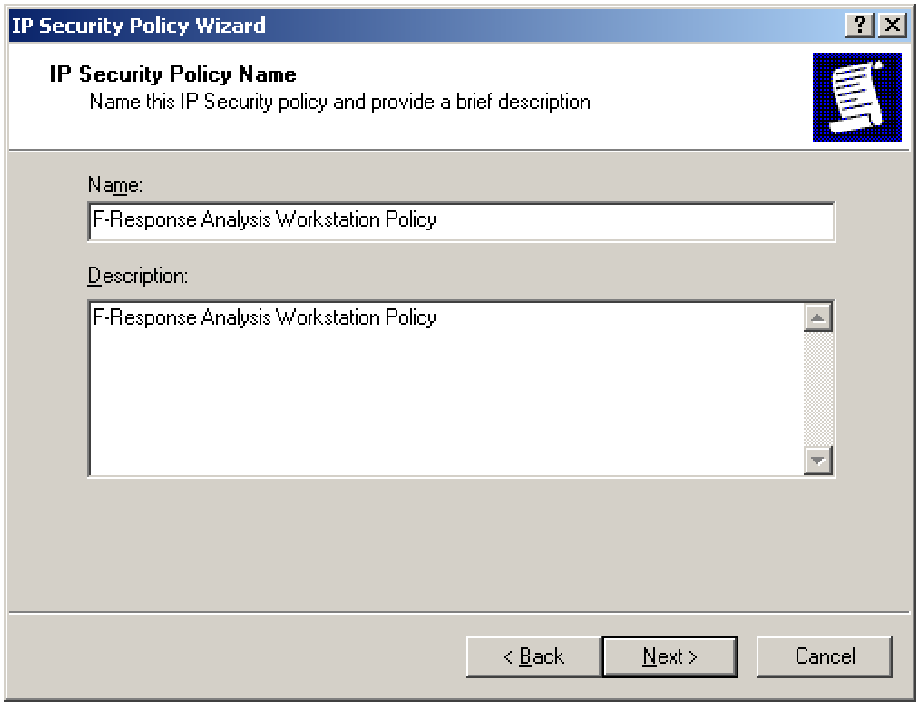


Welcome to the IP Security policy wizard.

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.

**The Microsoft IPSEC Security Policy Wizard will start, press Next to continue.**



IP Security Policy Wizard

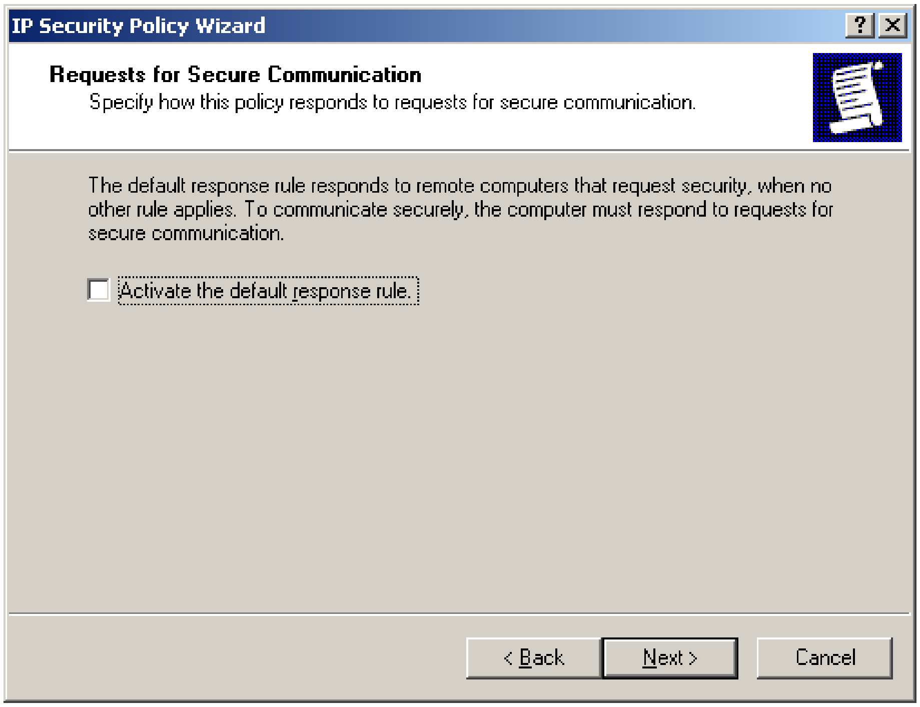
**IP Security Policy Name**

Name this IP Security policy and provide a brief description

Name: F-Response Analysis Workstation Policy

Description: F-Response Analysis Workstation Policy

**Create a new for the new IPSEC policy, since this policy will apply to our analysis workstations we will label this policy accordingly.**



IP Security Policy Wizard

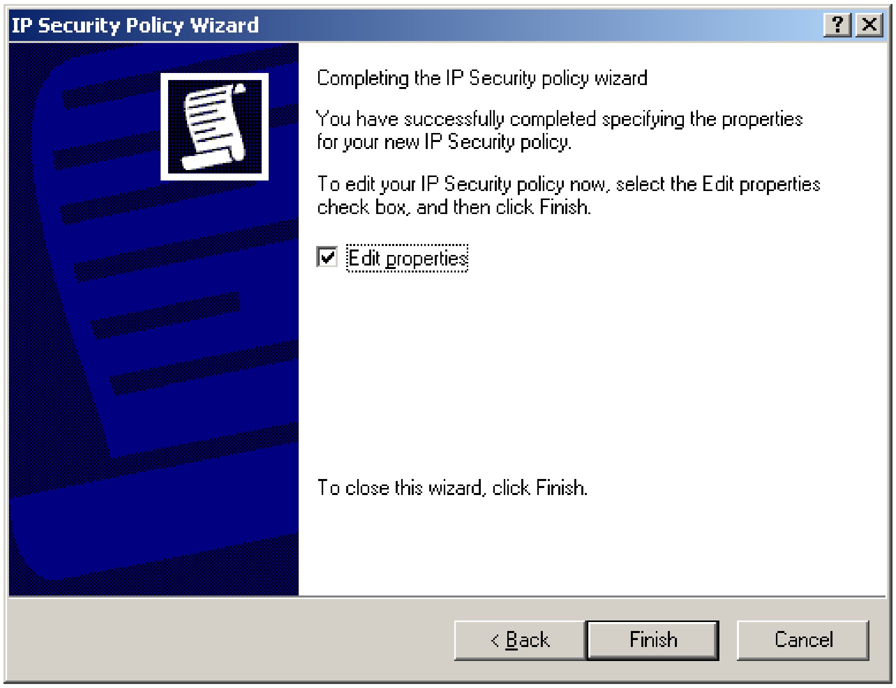
**Requests for Secure Communication**

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.

**Uncheck the option for "Activate the default response rule" and press Next.**



IP Security Policy Wizard

Completing the IP Security policy wizard

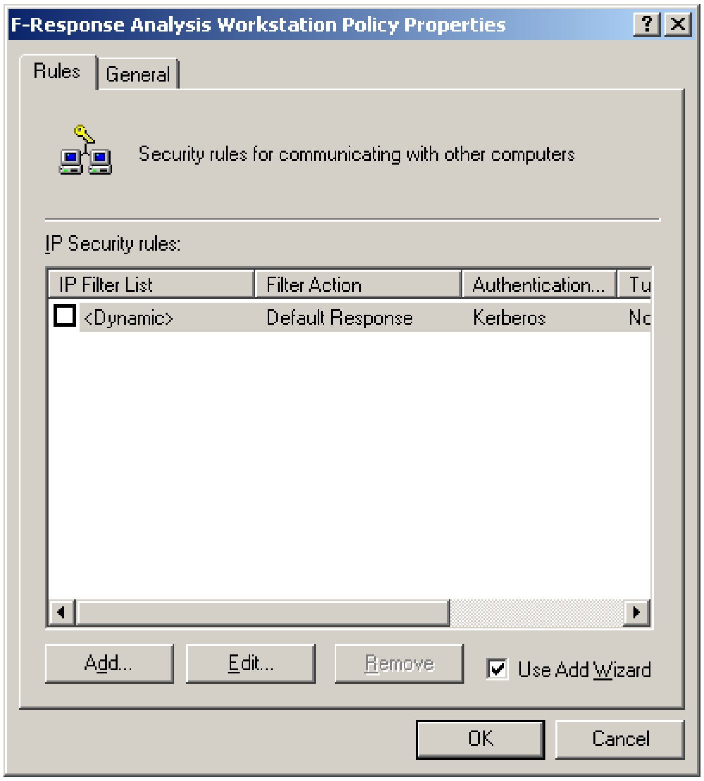
You have successfully completed specifying the properties for your new IP Security policy.

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.

**Leave the "Edit properties" checked and press Finish.**



F-Response Analysis Workstation Policy Properties

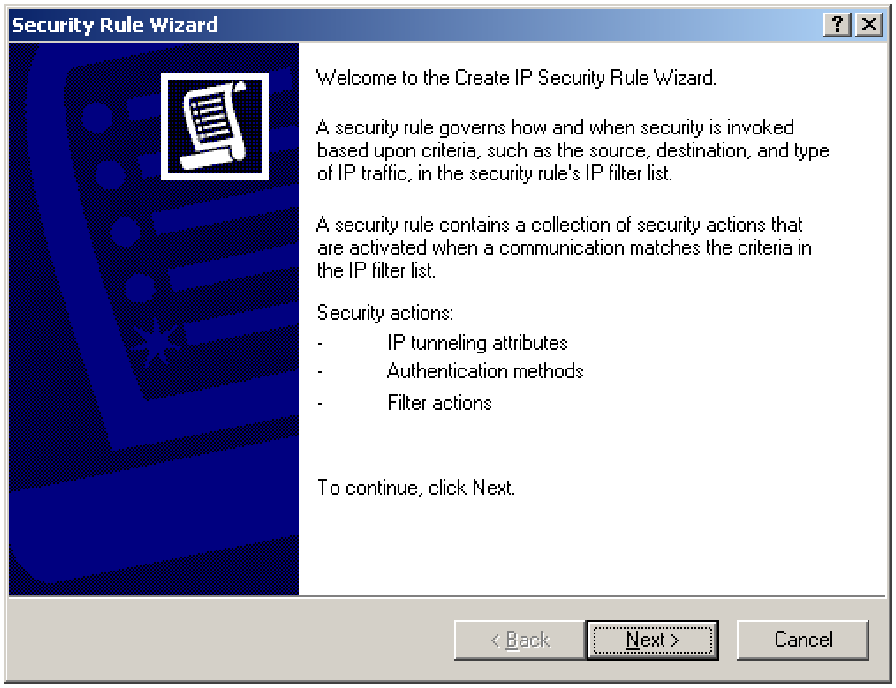
Security rules for communicating with other computers

IP Security rules:

| IP Filter List | Filter Action | Authentication... | Tu |
|---|---|---|---|
| □ <Dynamic> | Default Response | Kerberos | Nc |

☑ Use Add Wizard

**Now we must add a IP Security Rule, press the "Add..." button.**



Welcome to the Create IP Security Rule Wizard.

A security rule governs how and when security is invoked based upon criteria, such as the source, destination, and type of IP traffic, in the security rule's IP filter list.

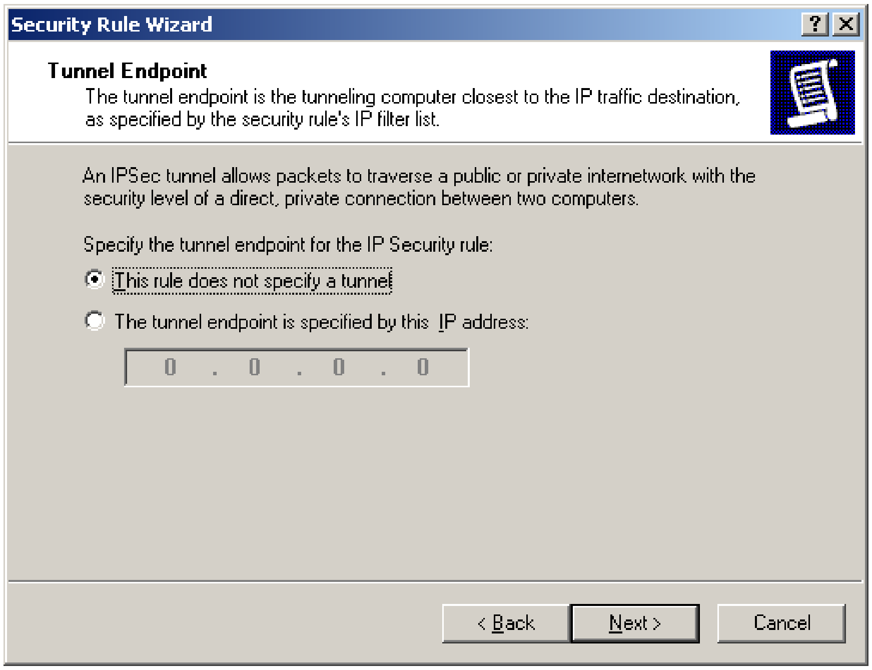
A security rule contains a collection of security actions that are activated when a communication matches the criteria in the IP filter list.

Security actions:

- IP tunneling attributes
- Authentication methods
- Filter actions

To continue, click Next.

**Press Next to continue the IP Security Rule Wizard.**



**Tunnel Endpoint**

The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the security rule's IP filter list.

An IPSec tunnel allows packets to traverse a public or private internetwork with the security level of a direct, private connection between two computers.

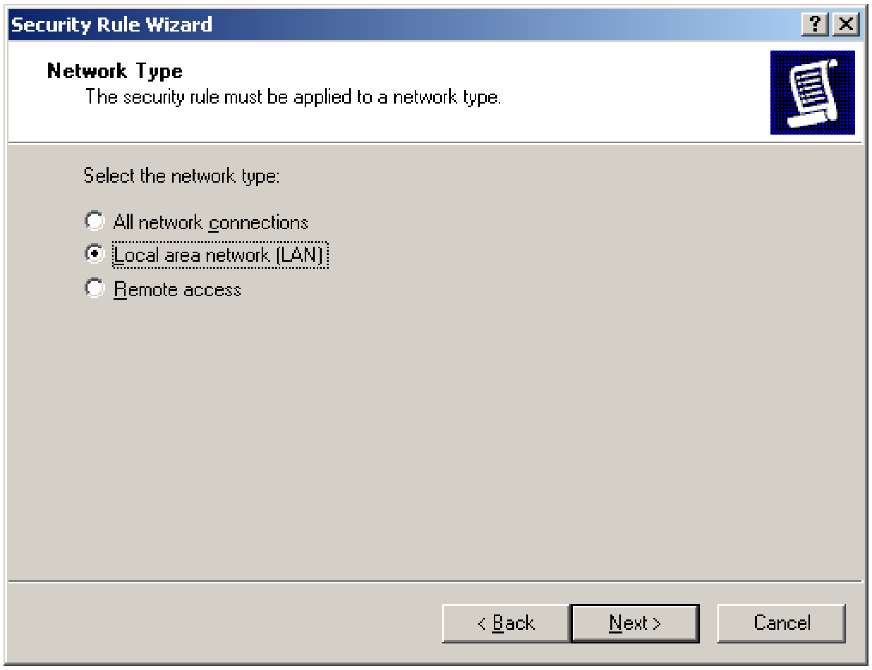
Specify the tunnel endpoint for the IP Security rule:

● This rule does not specify a tunnel

○ The tunnel endpoint is specified by this IP address:

0 . 0 . 0 . 0

**Leave the "This rule does not specify a tunnel" checked.**



Security Rule Wizard

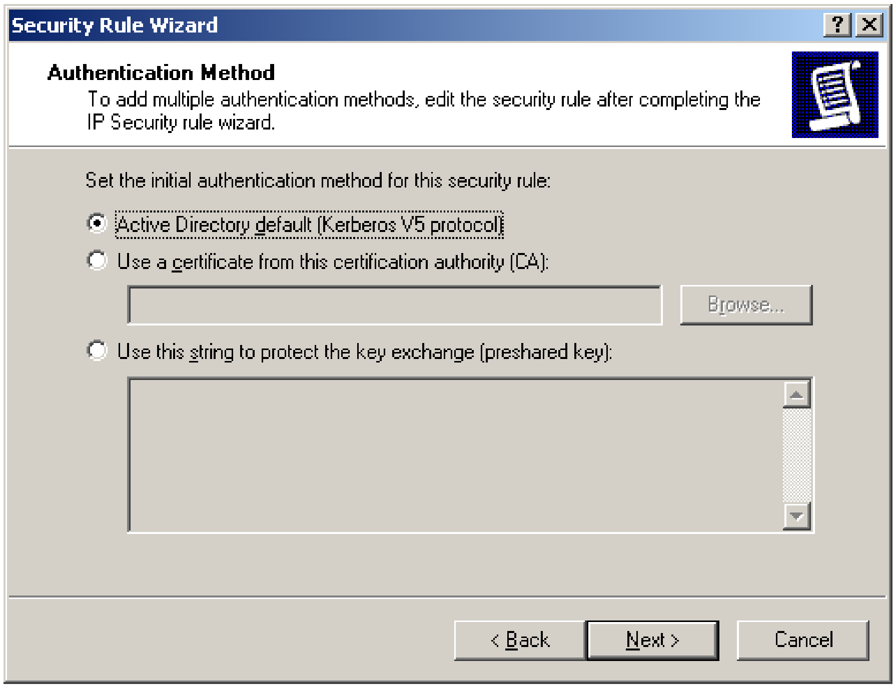
**Network Type**

The security rule must be applied to a network type.

Select the network type:

○ All network connections
● Local area network (LAN)
○ Remote access

**Select the option for "Local area network (LAN)".**



Security Rule Wizard

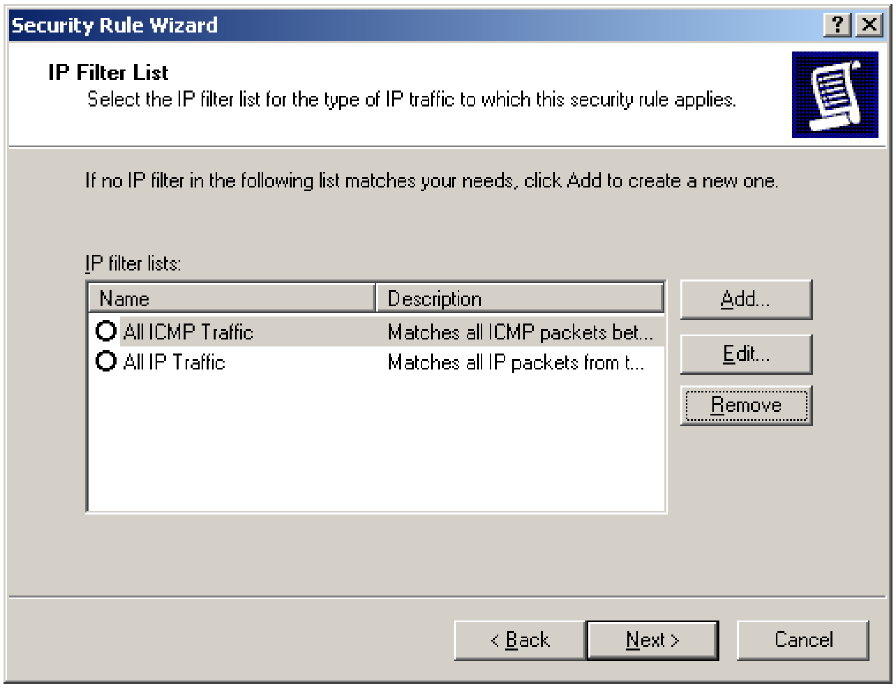
**Authentication Method**

To add multiple authentication methods, edit the security rule after completing the IP Security rule wizard.

Set the initial authentication method for this security rule:

● Active Directory default (Kerberos V5 protocol)
○ Use a certificate from this certification authority (CA):
○ Use this string to protect the key exchange (preshared key):

**If this is a Microsoft AD environment use the "Active Directory default".**



Security Rule Wizard

**IP Filter List**

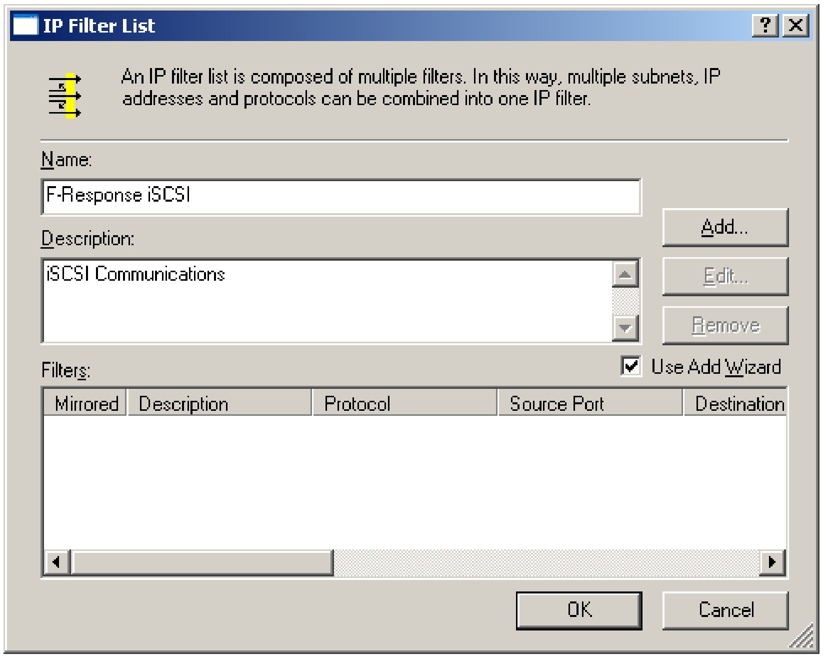
Select the IP filter list for the type of IP traffic to which this security rule applies.

If no IP filter in the following list matches your needs, click Add to create a new one.

IP filter lists:

| Name | Description |
|---|---|
| ○ All ICMP Traffic | Matches all ICMP packets bet... |
| ○ All IP Traffic | Matches all IP packets from t... |

Next we must add an IP Filter List item, select Add…



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.

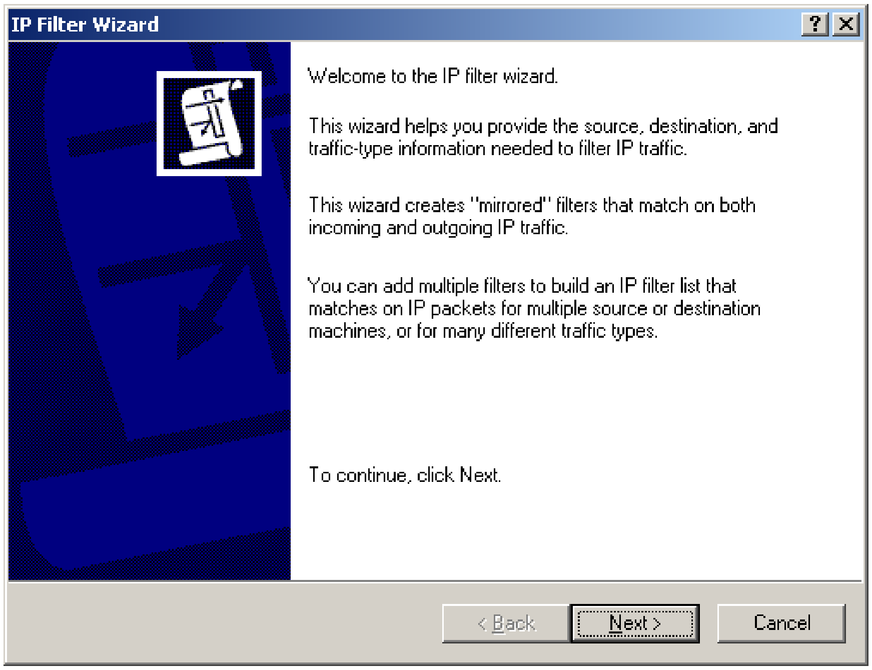
Name: F-Response iSCSI

Description: iSCSI Communications

Filters: ☑ Use Add Wizard

| Mirrored | Description | Protocol | Source Port | Destination |
|---|---|---|---|---|

Create a name for our IP Filter List, in this case we have labeled it "F-Response iSCSI". Next press "Add…" to start the IP Filter Wizard.



IP Filter Wizard

Welcome to the IP filter wizard.

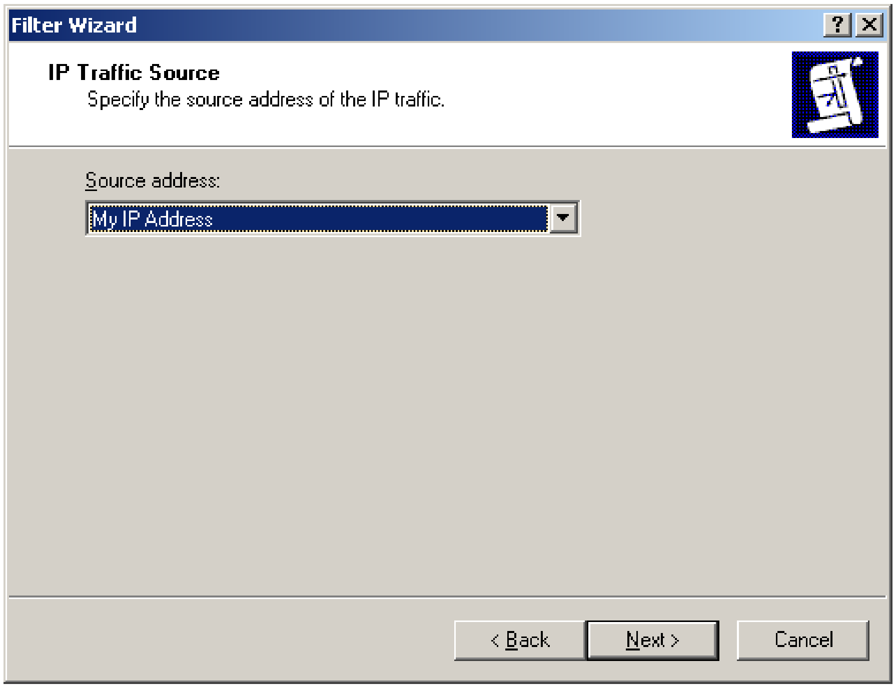
This wizard helps you provide the source, destination, and traffic-type information needed to filter IP traffic.

This wizard creates "mirrored" filters that match on both incoming and outgoing IP traffic.

You can add multiple filters to build an IP filter list that matches on IP packets for multiple source or destination machines, or for many different traffic types.

To continue, click Next.

Press Next to continue.



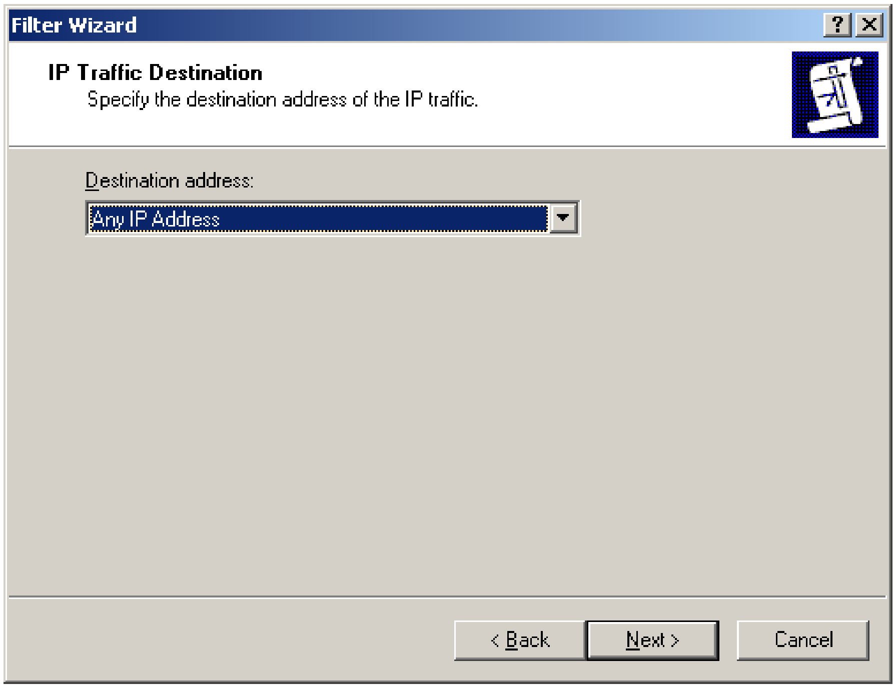
Filter Wizard

IP Traffic Source

Specify the source address of the IP traffic.

Source address: My IP Address

Set the Source address to “My IP Address”.

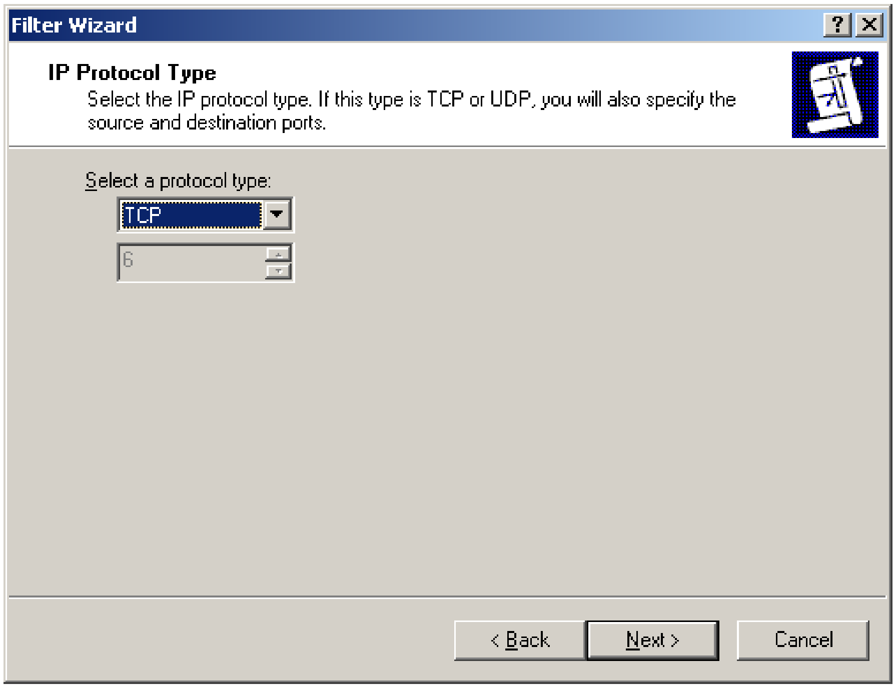


Filter Wizard

**IP Traffic Destination**
Specify the destination address of the IP traffic.

Destination address: Any IP Address

**Since the IP Address of the destination could be any machine in your environment we will want to set the Destination address to "Any IP Address".**



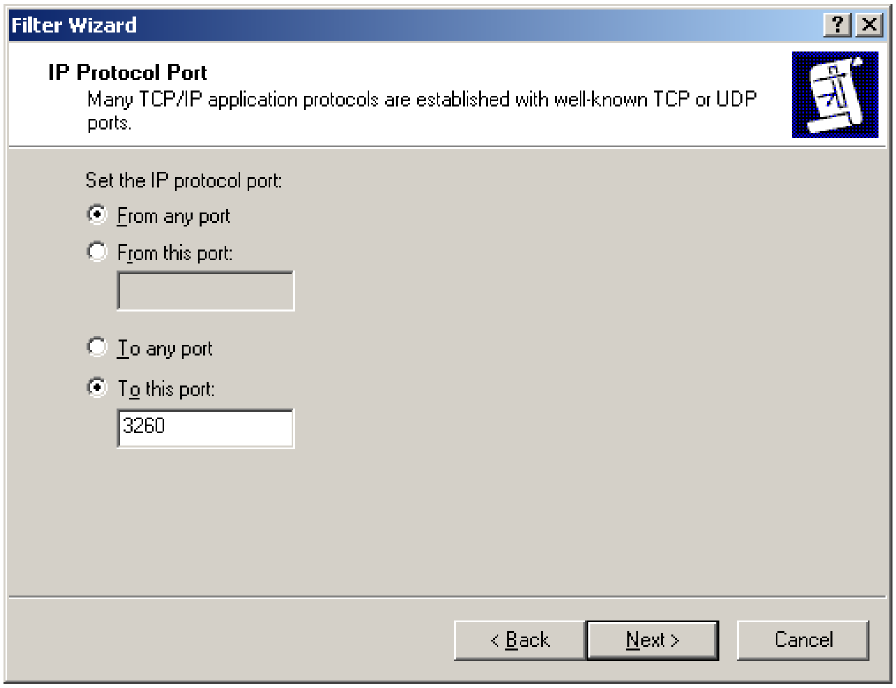
Filter Wizard

**IP Protocol Type**
Select the IP protocol type. If this type is TCP or UDP, you will also specify the source and destination ports.

Select a protocol type: TCP

6

**Select the protocol type as TCP.**



Filter Wizard

**IP Protocol Port**

Many TCP/IP application protocols are established with well-known TCP or UDP ports.

Set the IP protocol port:

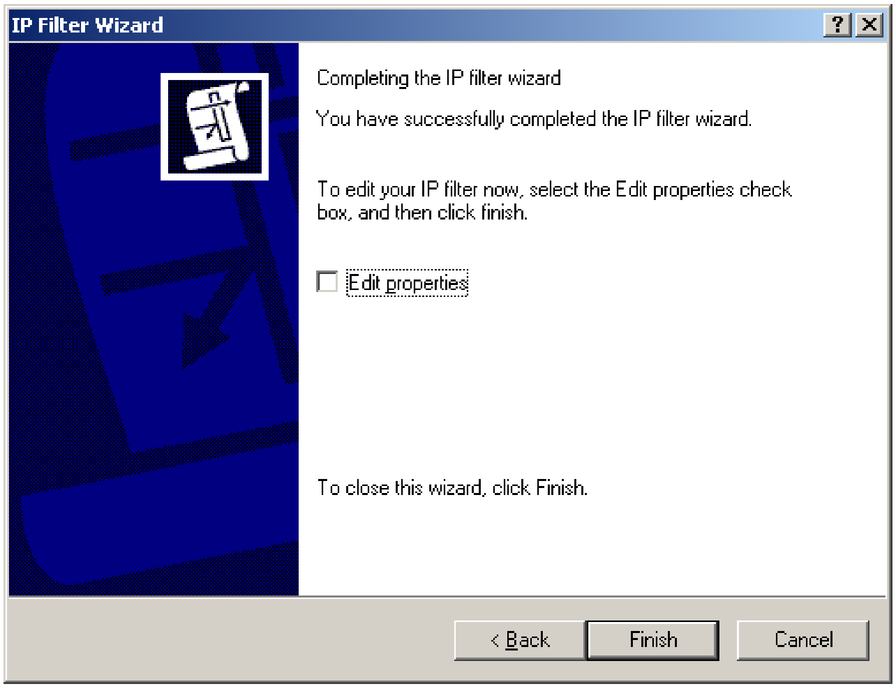
● From any port

○ From this port:

○ To any port

● To this port: 3260

**Set the IP Protocol Port to "From any port"  and "To this port" enter in the value for the F-Response Enterprise client port, in this case we have used the default iSCSI port of 3260. Press Next to continue.**



IP Filter Wizard

Completing the IP filter wizard

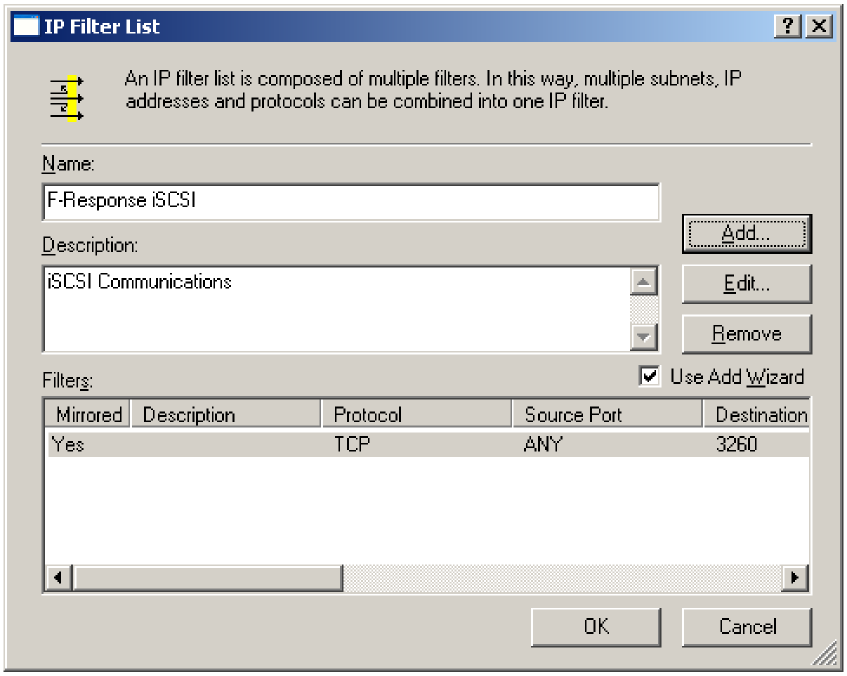
You have successfully completed the IP filter wizard.

To edit your IP filter now, select the Edit properties check box, and then click finish.

□ Edit properties

To close this wizard, click Finish.

**Press Finish to complete the IP Filter Wizard.**



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: F-Response iSCSI

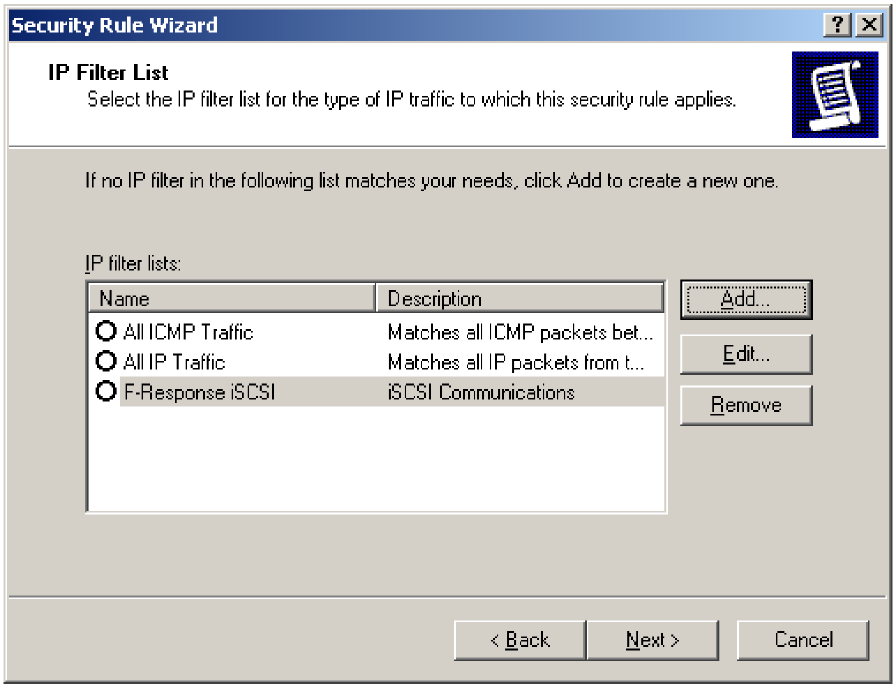
Description: iSCSI Communications

Filters:

☑ Use Add Wizard

| Mirrored | Description | Protocol | Source Port | Destination |
|---|---|---|---|---|
| Yes | | TCP | ANY | 3260 |

The IP Filter List will now show the newly created Filter. Press Ok to continue.



Security Rule Wizard

IP Filter List

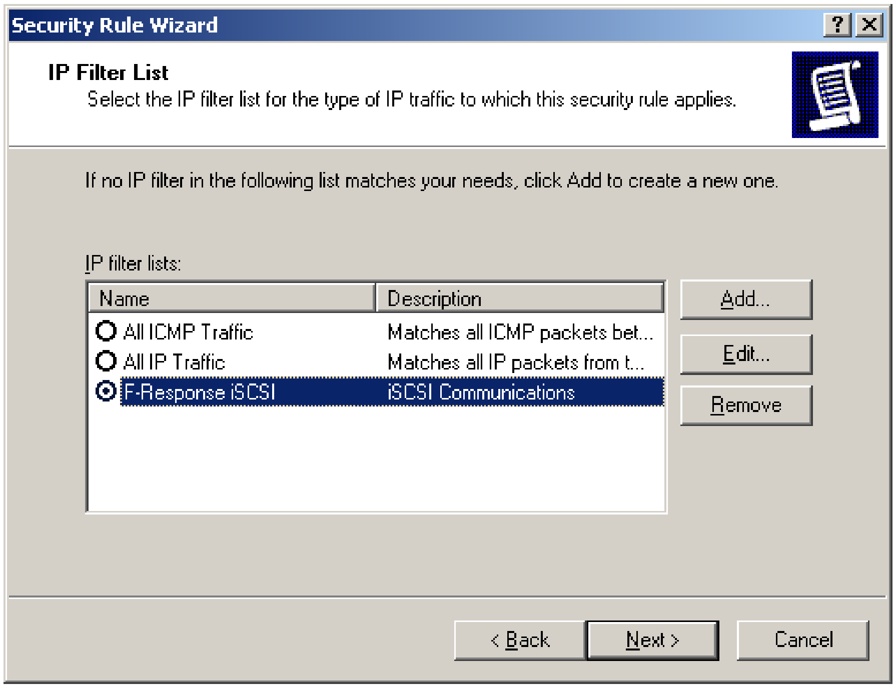
Select the IP filter list for the type of IP traffic to which this security rule applies.

If no IP filter in the following list matches your needs, click Add to create a new one.

IP filter lists:

| Name | Description |
|---|---|
| ○ All ICMP Traffic | Matches all ICMP packets bet... |
| ○ All IP Traffic | Matches all IP packets from t... |
| ○ F-Response iSCSI | iSCSI Communications |

Now enable the F-Response iSCSI IP Filter by selecting the option next to the Name.



Security Rule Wizard

**IP Filter List**

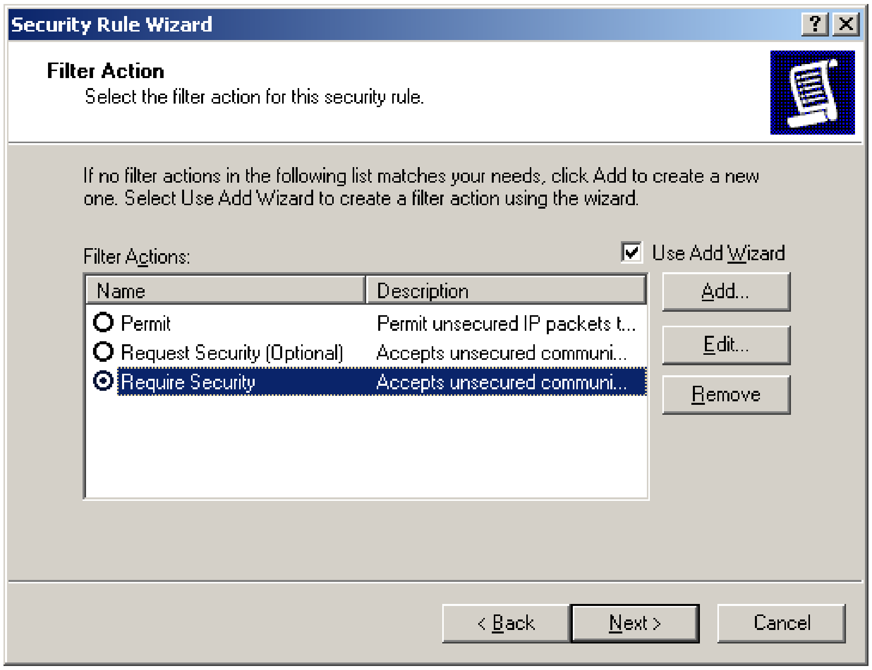
Select the IP filter list for the type of IP traffic to which this security rule applies.

If no IP filter in the following list matches your needs, click Add to create a new one.

IP filter lists:

| Name | Description |
|---|---|
| ○ All ICMP Traffic | Matches all ICMP packets bet... |
| ○ All IP Traffic | Matches all IP packets from t... |
| ● F-Response iSCSI | iSCSI Communications |

Press Next to continue.



Security Rule Wizard

**Filter Action**

Select the filter action for this security rule.

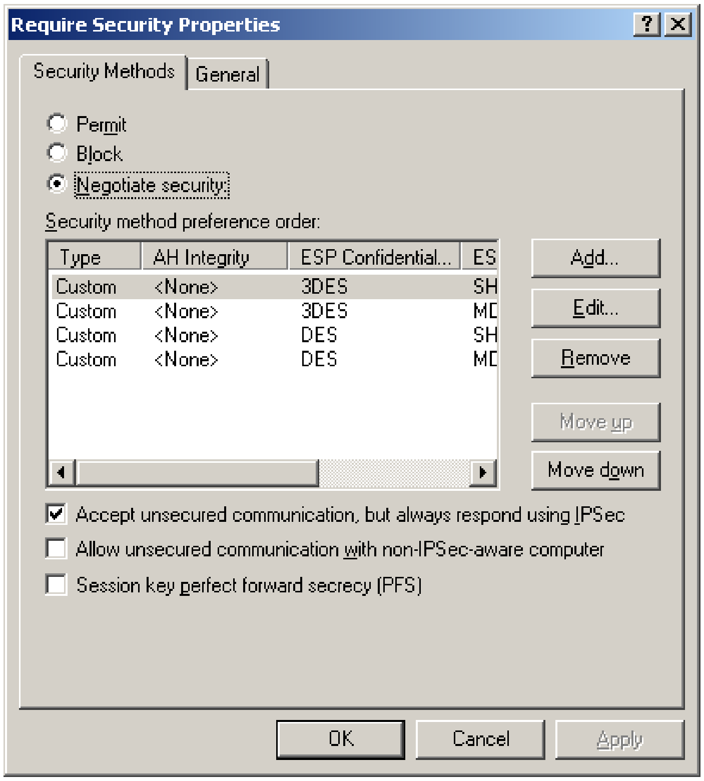
If no filter actions in the following list matches your needs, click Add to create a new one. Select Use Add Wizard to create a filter action using the wizard.

Filter Actions:

☑ Use Add Wizard

| Name | Description |
|---|---|
| ○ Permit | Permit unsecured IP packets t... |
| ○ Request Security (Optional) | Accepts unsecured communi... |
| ● Require Security | Accepts unsecured communi... |

Select the option button next to "Require Security" and press Edit…



Require Security Properties

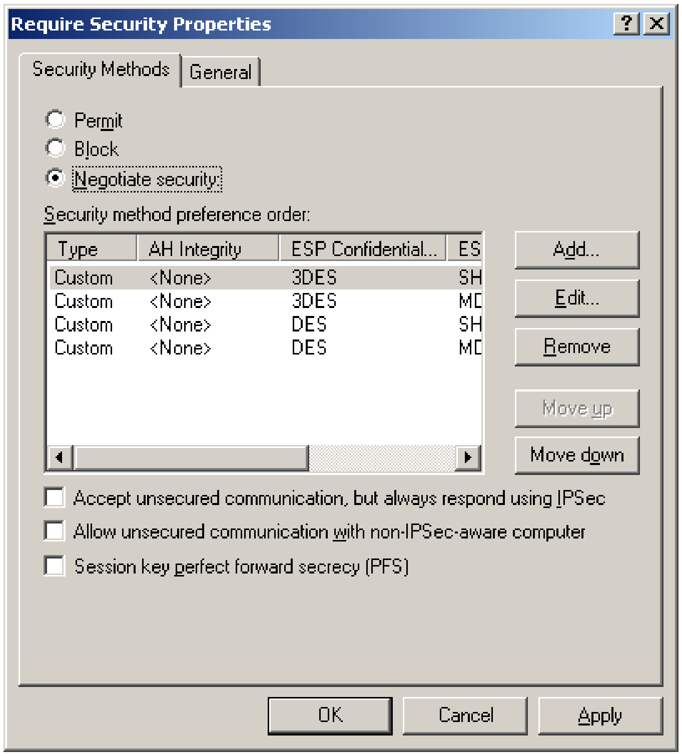
○ Permit
○ Block
● Negotiate security:

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 computer
☐ Session key perfect forward secrecy (PFS)

**Remove the check box next to “Accept unsecured communication..”**



Require Security Properties

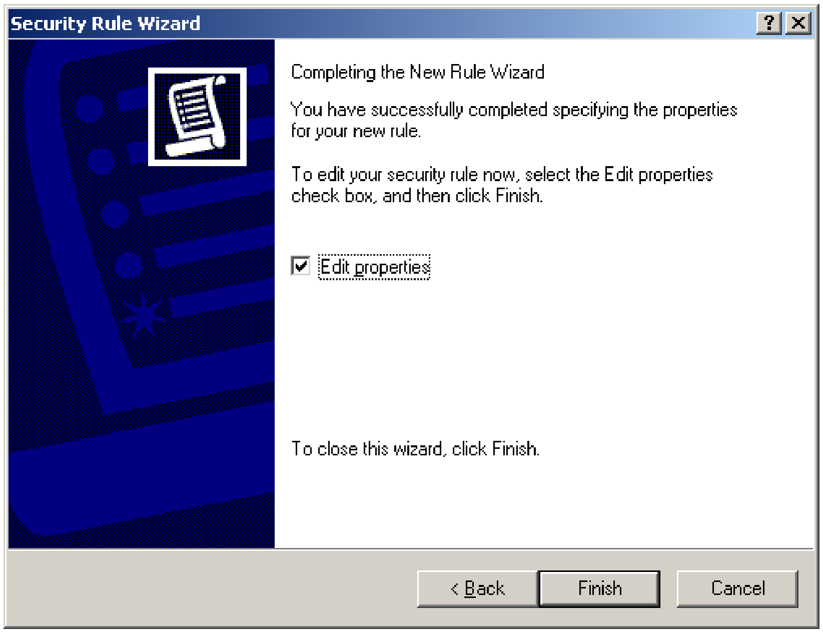
○ Permit
○ Block
● Negotiate security:

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 computer
☐ Session key perfect forward secrecy (PFS)

**Press Ok to continue.**



Security Rule Wizard

Completing the New Rule Wizard

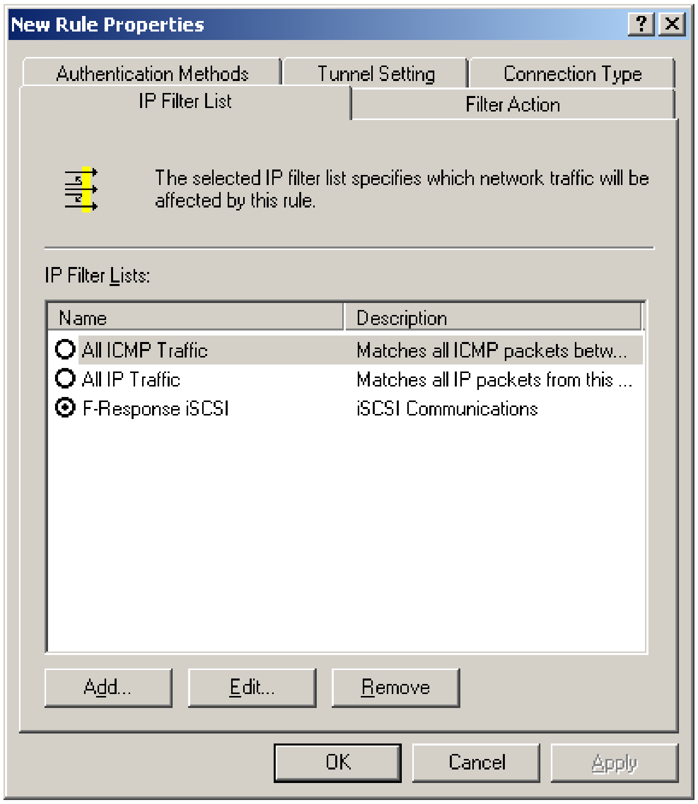
You have successfully completed specifying the properties for your new rule.

To edit your security rule now, select the Edit properties check box, and then click Finish.

☑ Edit properties

To close this wizard, click Finish.

**Press Finish to complete the Security Rule Wizard.**



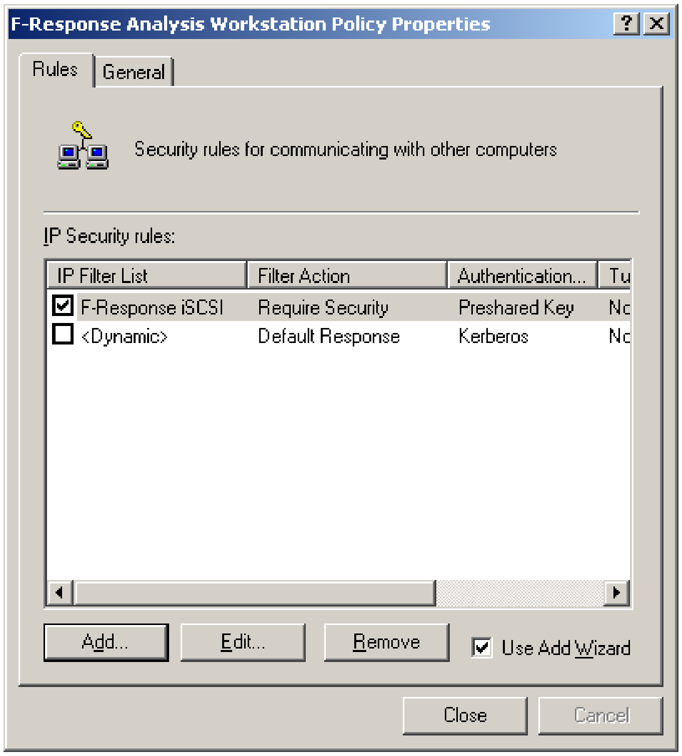
New Rule Properties

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 ... |
| ● F-Response iSCSI | iSCSI Communications |

**Press Ok to close the New Rule Properties window.**



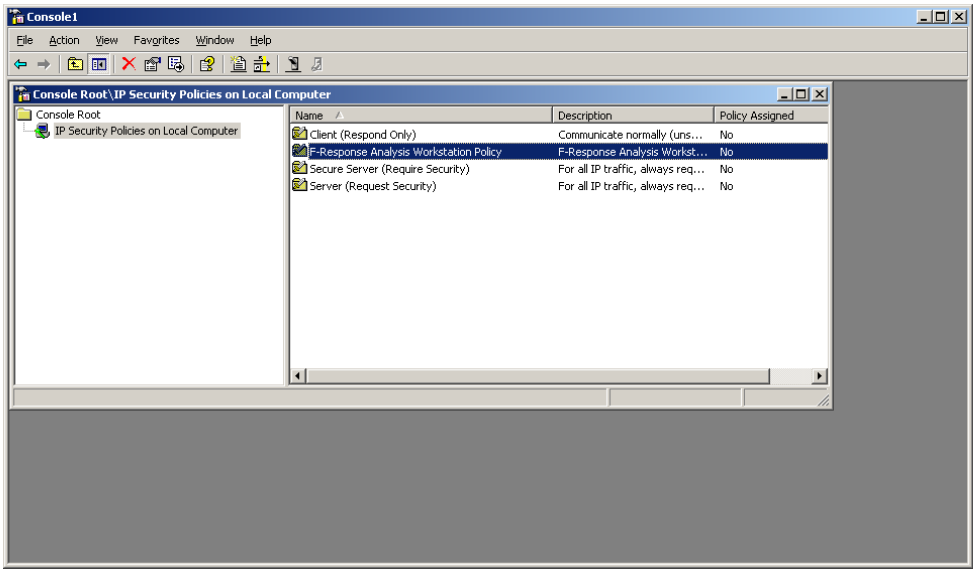
F-Response Analysis Workstation Policy Properties

Security rules for communicating with other computers

IP Security rules:

| IP Filter List | Filter Action | Authentication... | Tu |
|---|---|---|---|
| ☑ F-Response iSCSI | Require Security | Preshared Key | Nc |
| □ <Dynamic> | Default Response | Kerberos | Nc |

Confirm that the F-Response iSCSI IP Filter is checked in the F-Response Analysis Workstation Policy Properties and press Close.



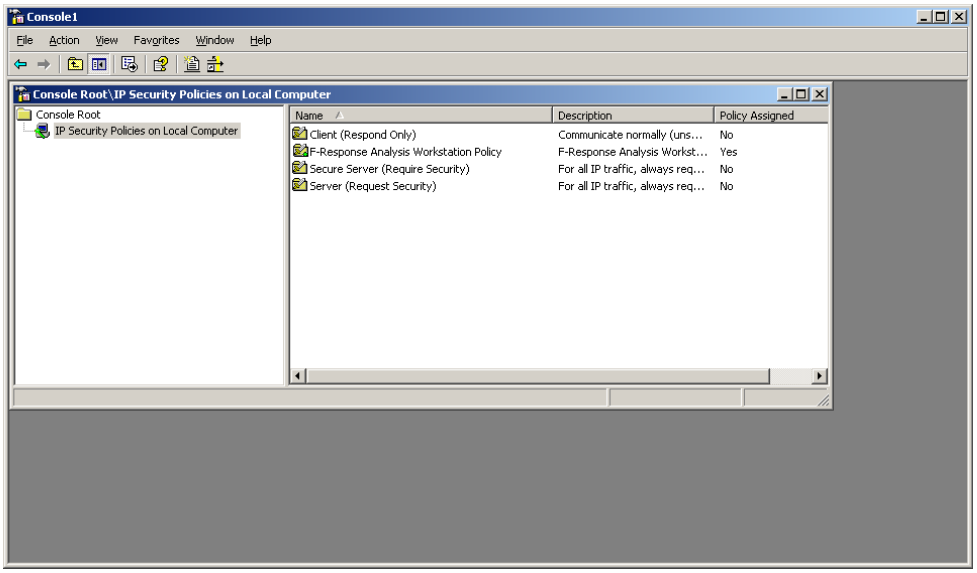
Console1

Console Root\IP Security Policies on Local Computer

Console Root
IP Security Policies on Local Computer

| Name | Description | Policy Assigned |
|---|---|---|
| Client (Respond Only) | Communicate normally (uns... | No |
| F-Response Analysis Workstation Policy | F-Response Analysis Workst... | No |
| Secure Server (Require Security) | For all IP traffic, always req... | No |
| Server (Request Security) | For all IP traffic, always req... | No |

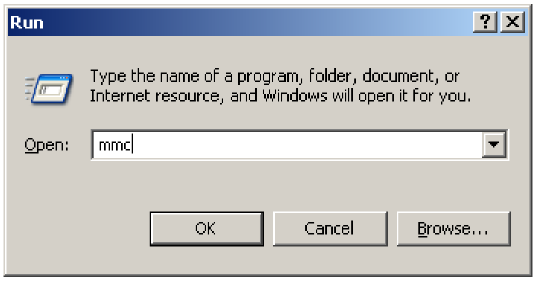
The policy should now be complete and listed in the IP Security Policies panel of the Microsoft Management Console window.


Console1
File
Action
View
Favorites
Window
Help
Console Root\IP Security Policies on Local Computer
Console Root
IP Security Policies on Local Computer

| Name | Description | Policy Assigned |
|---|---|---|
| Client (Respond Only) | Communicate normally (uns... | No |
| F-Response Analysis Workstation Policy | F-Response Analysis Workst... | Yes |
| Secure Server (Require Security) | For all IP traffic, always req... | No |
| Server (Request Security) | For all IP traffic, always req... | No |

**To enable the policy select it, right click and press "Assign".**

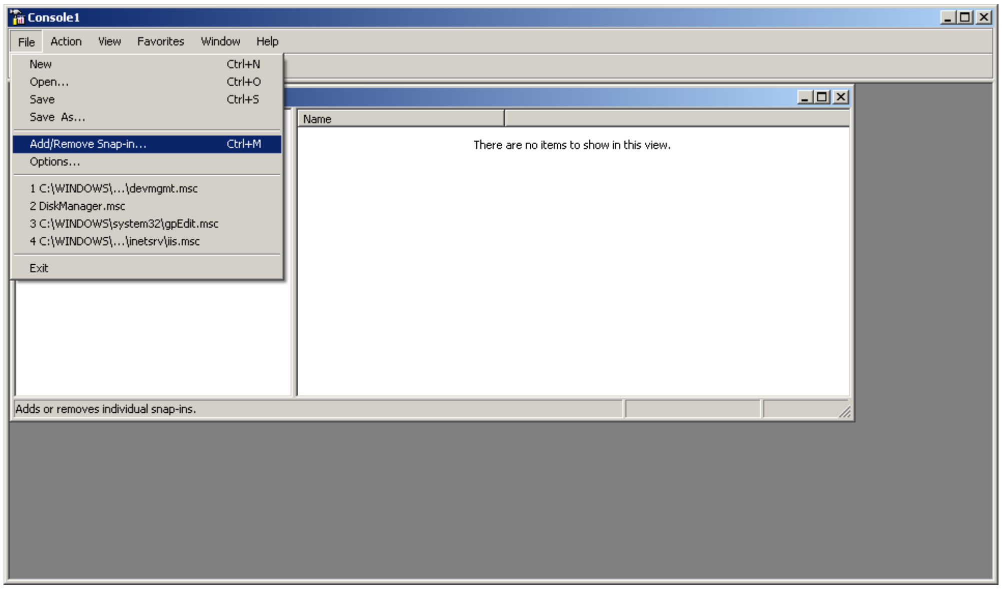
# Configuring an Microsoft IPSEC Policy for the F-Response Enterprise Target Computers


Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: mmc

**Start by accessing the Microsoft Management Console or MMC.**

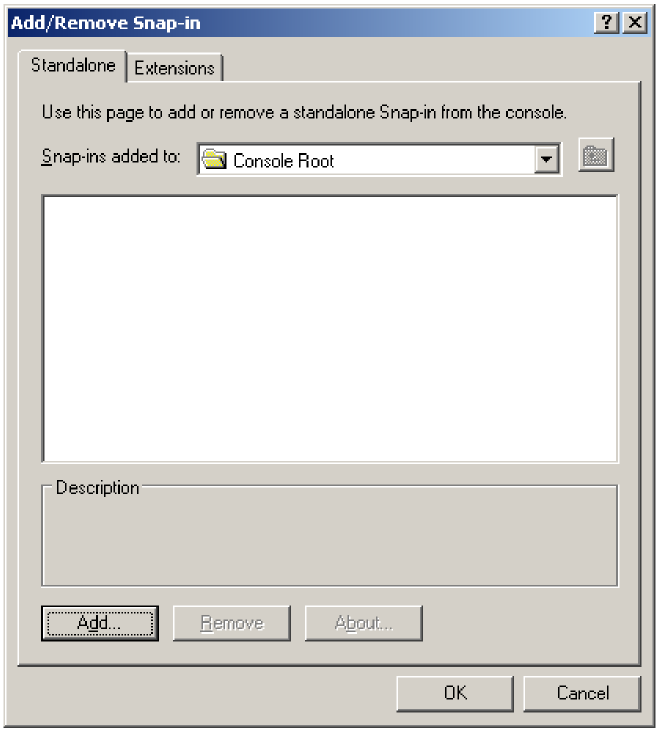

Console1

File
Action
View
Favorites
Window
Help
New Ctrl+N
Open... Ctrl+O
Save Ctrl+S
Save As...
Add/Remove Snap-in... Ctrl+M
Options...
1 C:\WINDOWS\...\devmgmt.msc
2 DiskManager.msc
3 C:\WINDOWS\system32\gpEdit.msc
4 C:\WINDOWS\...\inetsrv\iis.msc
Exit
Name

There are no items to show in this view.

Adds or removes individual snap-ins.

**Next select File Add/Remove Snap-In..**

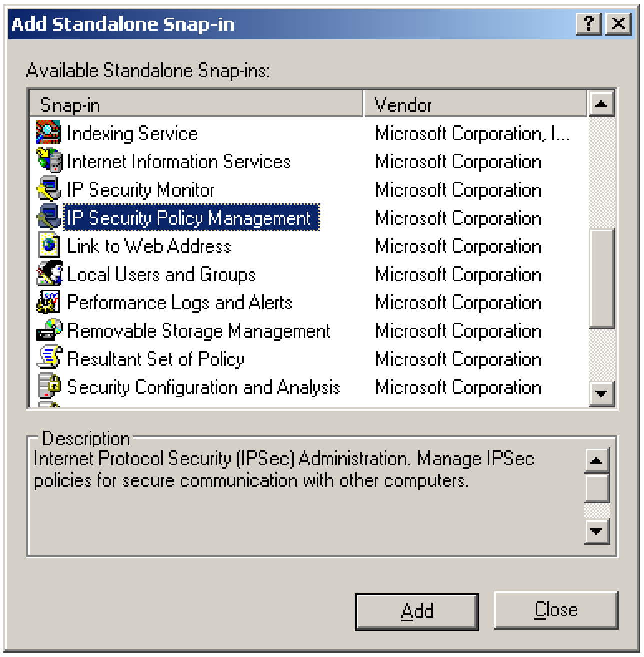


Use this page to add or remove a standalone Snap-in from the console.

Snap-ins added to: Console Root

Description

**Select the IP Security Policy Management Snap-in.**

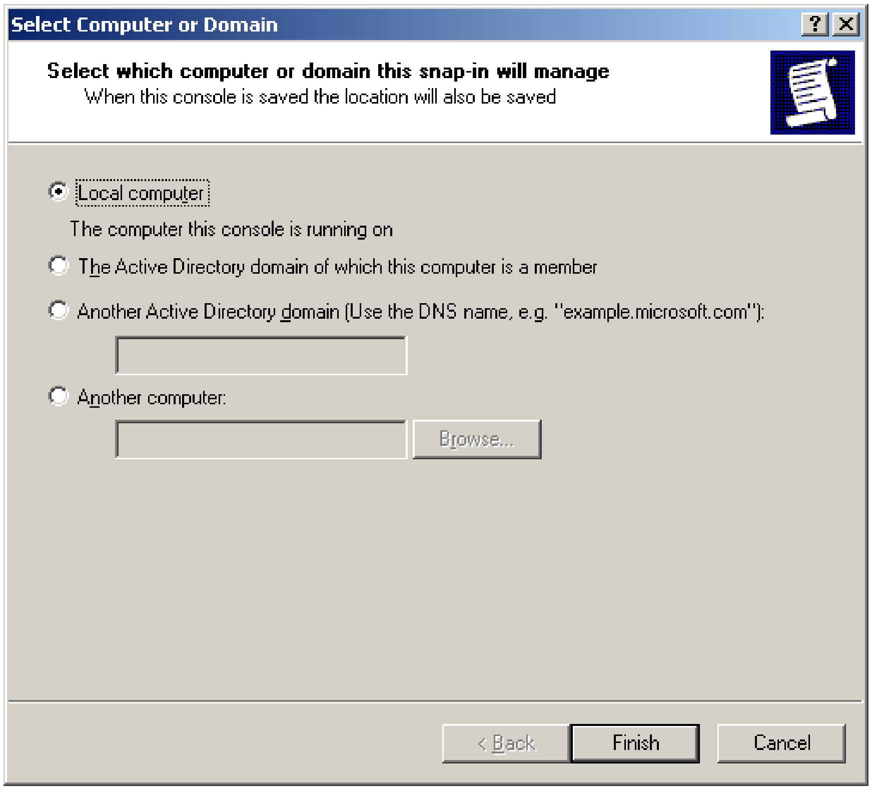


Available Standalone Snap-ins:

| Snap-in | Vendor |
|---|---|
| Indexing Service | Microsoft Corporation, I... |
| Internet Information Services | Microsoft Corporation |
| IP Security Monitor | Microsoft Corporation |
| IP Security Policy Management | Microsoft Corporation |
| Link to Web Address | Microsoft Corporation |
| Local Users and Groups | Microsoft Corporation |
| Performance Logs and Alerts | Microsoft Corporation |
| Removable Storage Management | Microsoft Corporation |
| Resultant Set of Policy | Microsoft Corporation |
| Security Configuration and Analysis | Microsoft Corporation |

Description
Internet Protocol Security (IPSec) Administration. Manage IPSec policies for secure communication with other computers.

**Select the IP Security Policy Management Snap-in.**

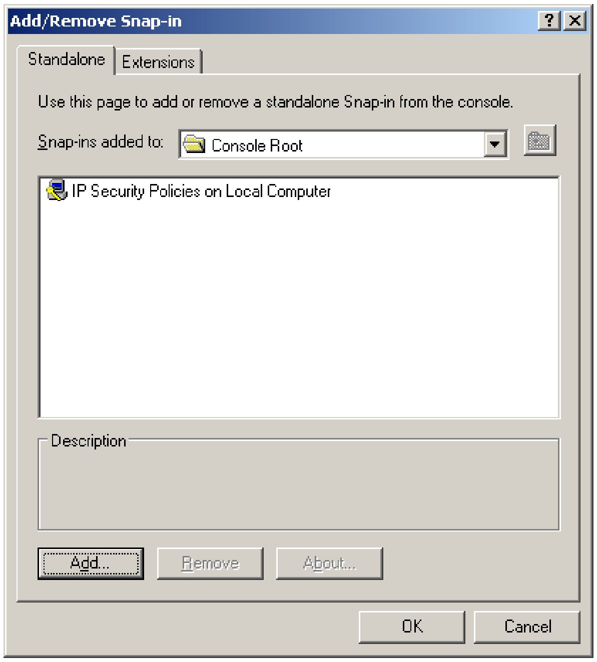


Select Computer or Domain

**Select which computer or domain this snap-in will manage**
When this console is saved the location will also be saved

● Local computer
The computer this console is running on
○ The Active Directory domain of which this computer is a member
○ Another Active Directory domain (Use the DNS name, e.g. "example.microsoft.com"):
○ Another computer:

**Select the computer this Snap-in will manage, in a Microsoft Active Directory environment this could be either a local or remotely managed computer.**



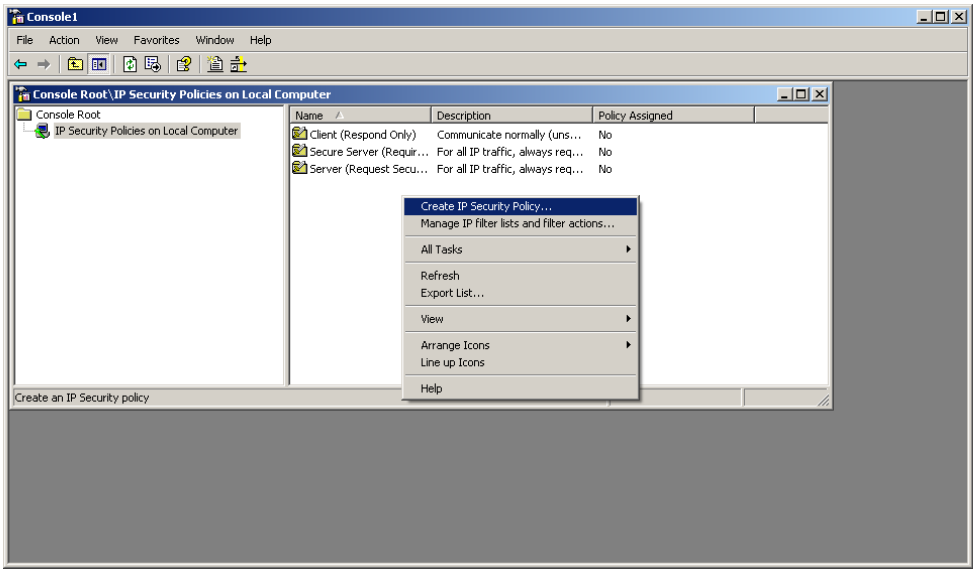
Add/Remove Snap-in

Use this page to add or remove a standalone Snap-in from the console.

Snap-ins added to: Console Root

IP Security Policies on Local Computer

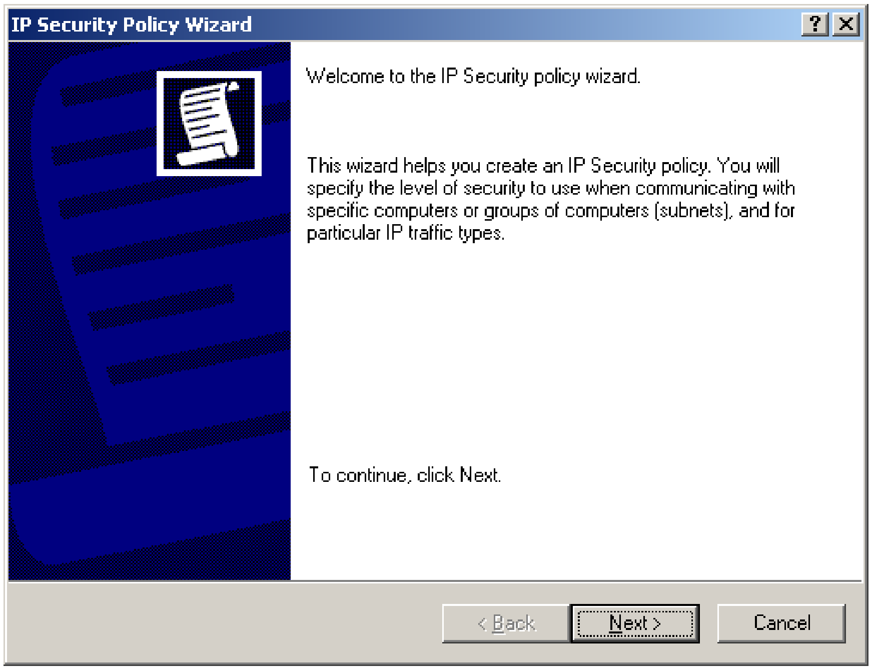
**Press Ok to complete the add process and begin using the management console.**


Console1
File Action View Favorites Window Help
Console Root\IP Security Policies on Local Computer
Console Root
IP Security Policies on Local Computer
Create IP Security Policy...
Manage IP filter lists and filter actions...
All Tasks
Refresh
Export List...
View
Arrange Icons
Line up Icons
Help

| Name | Description | Policy Assigned |
|---|---|---|
| Client (Respond Only) | Communicate normally (uns... | No |
| Secure Server (Requir... | For all IP traffic, always req... | No |
| Server (Request Secu... | For all IP traffic, always req... | No |

Create an IP Security policy

Next right click in the right side pane and select “Create IP Security Policy”

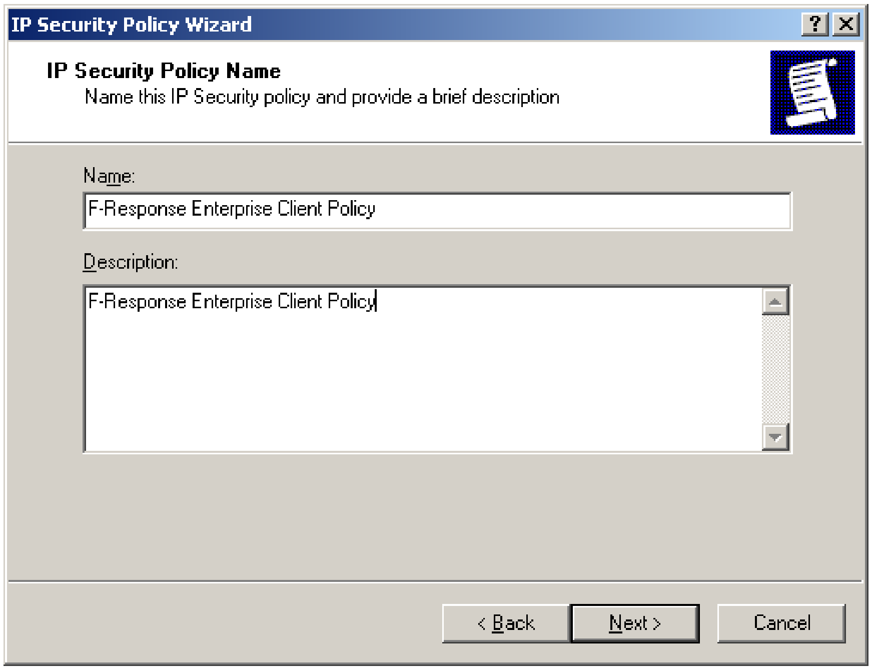


Welcome to the IP Security policy wizard.

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.

The Microsoft IPSEC Security Policy Wizard will start, press Next to continue.



IP Security Policy Wizard

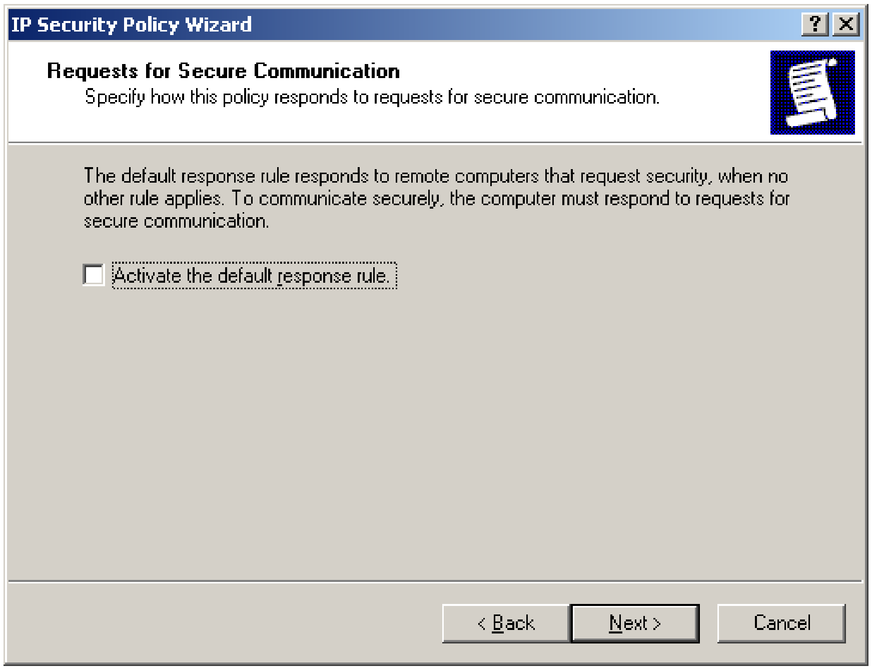
**IP Security Policy Name**

Name this IP Security policy and provide a brief description

Name: F-Response Enterprise Client Policy

Description: F-Response Enterprise Client Policy

**Create a new for the new IPSEC policy, since this policy will apply to our client computers we will label this policy accordingly.**



IP Security Policy Wizard

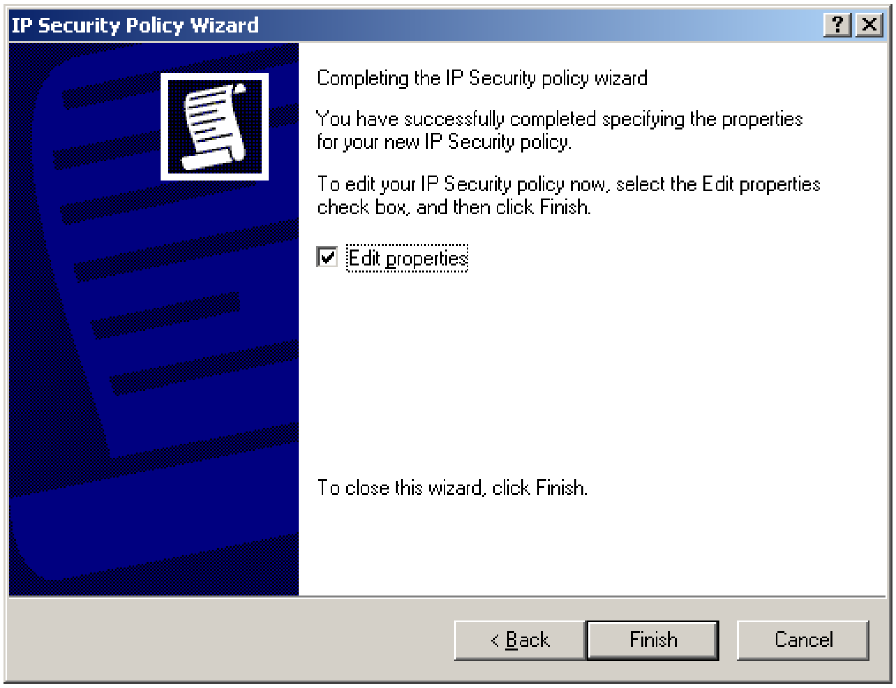
**Requests for Secure Communication**

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.

**Uncheck the option for "Activate the default response rule" and press Next.**



IP Security Policy Wizard

Completing the IP Security policy wizard

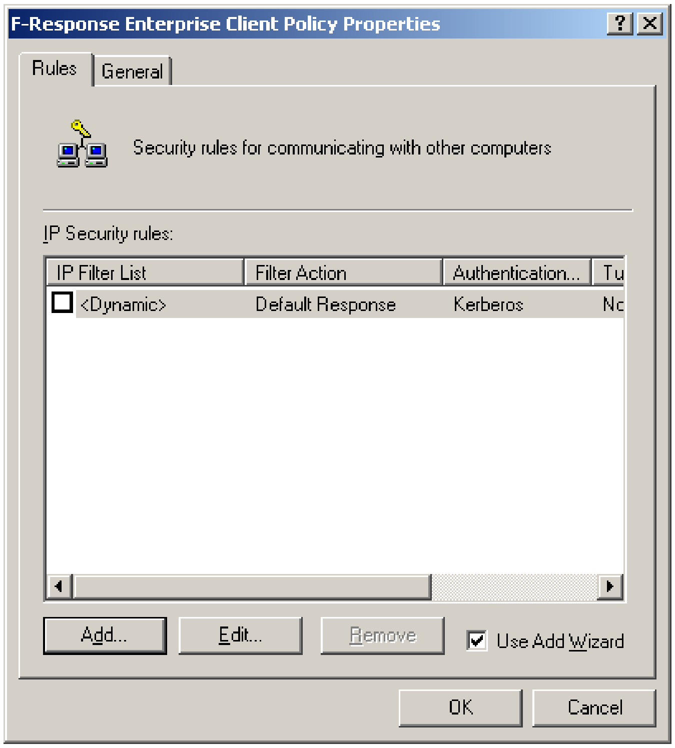
You have successfully completed specifying the properties for your new IP Security policy.

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.

**Leave the "Edit properties" checked and press Finish.**



F-Response Enterprise Client Policy Properties

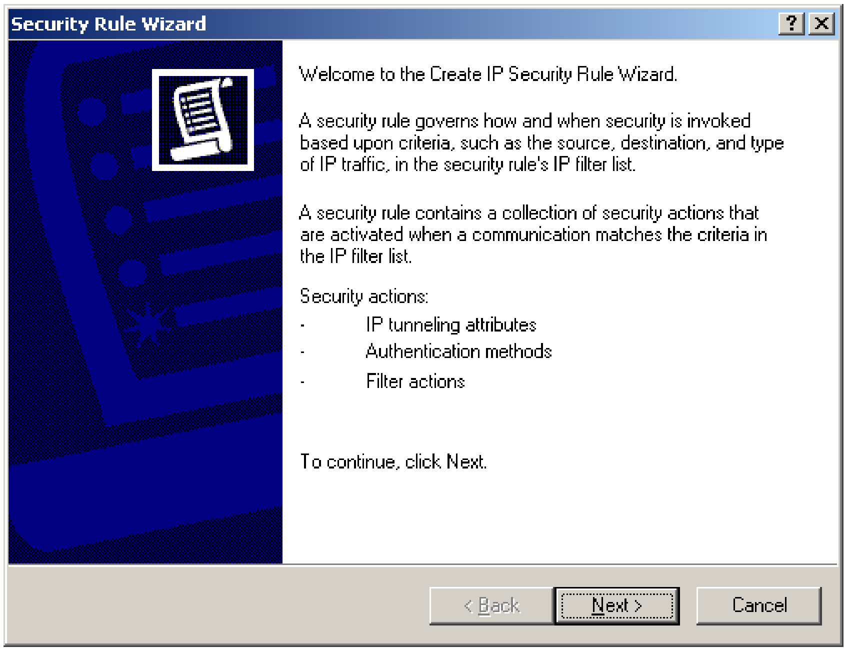
Security rules for communicating with other computers

IP Security rules:

| IP Filter List | Filter Action | Authentication... | Tu |
|---|---|---|---|
| □ <Dynamic> | Default Response | Kerberos | Nc |

☑ Use Add Wizard

**Now we must add a IP Security Rule, press the "Add…" button.**



Security Rule Wizard

Welcome to the Create IP Security Rule Wizard.

A security rule governs how and when security is invoked based upon criteria, such as the source, destination, and type of IP traffic, in the security rule's IP filter list.

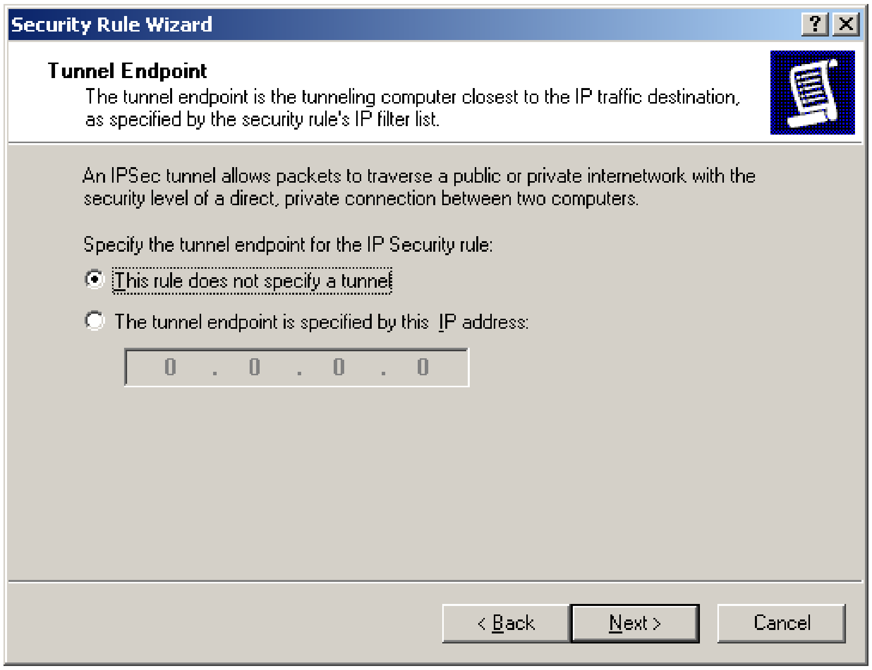
A security rule contains a collection of security actions that are activated when a communication matches the criteria in the IP filter list.

Security actions:

- IP tunneling attributes
- Authentication methods
- Filter actions

To continue, click Next.

**Press Next to continue the IP Security Rule Wizard.**



Security Rule Wizard

Tunnel Endpoint

The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the security rule's IP filter list.

An IPSec tunnel allows packets to traverse a public or private internetwork with the security level of a direct, private connection between two computers.

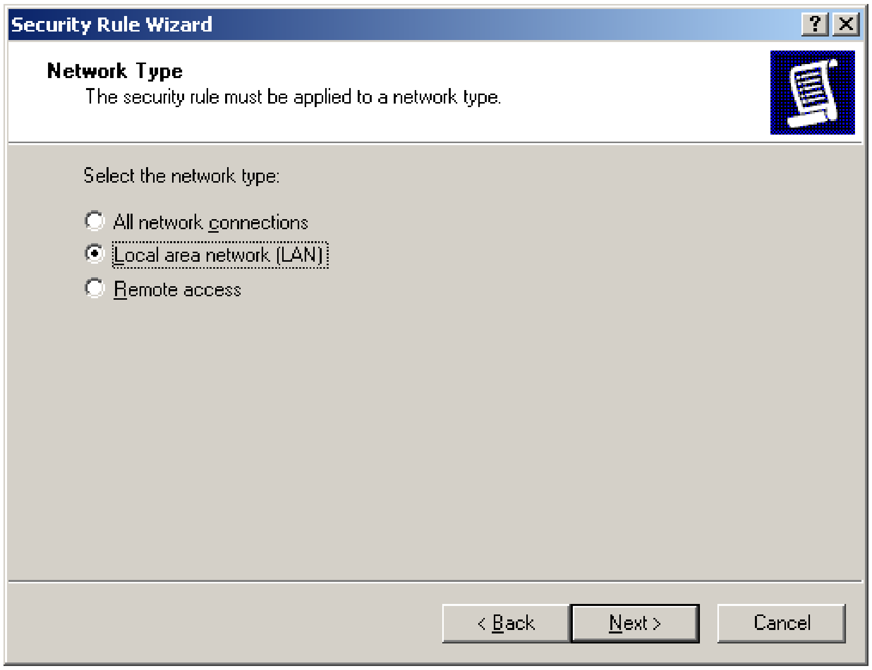
Specify the tunnel endpoint for the IP Security rule:

● This rule does not specify a tunnel

○ The tunnel endpoint is specified by this IP address:

0 . 0 . 0 . 0

**Leave the "This rule does not specify a tunnel" checked.**



Security Rule Wizard

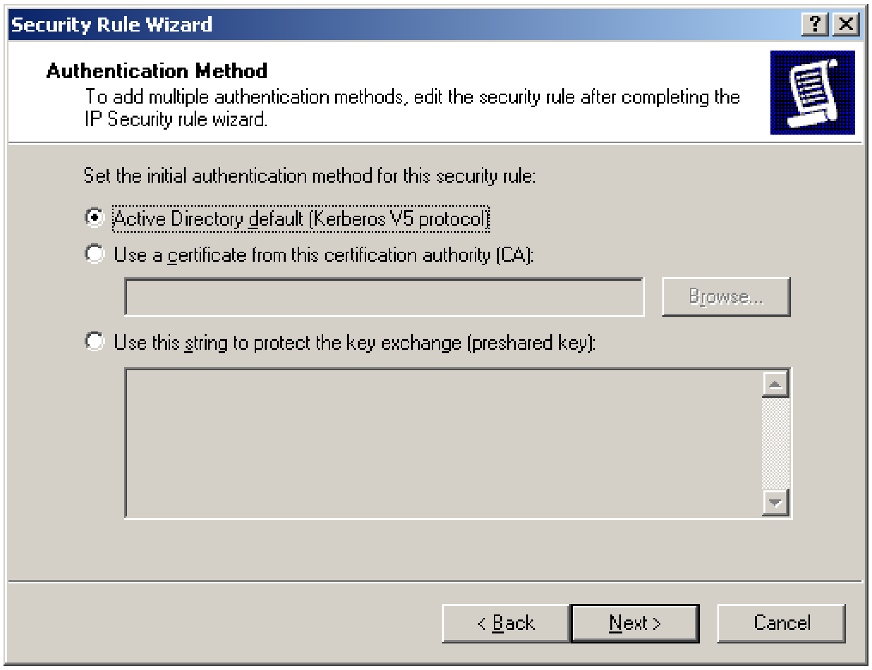
**Network Type**

The security rule must be applied to a network type.

Select the network type:

○ All network connections
● Local area network (LAN)
○ Remote access

**Select the option for "Local area network (LAN)".**



Security Rule Wizard

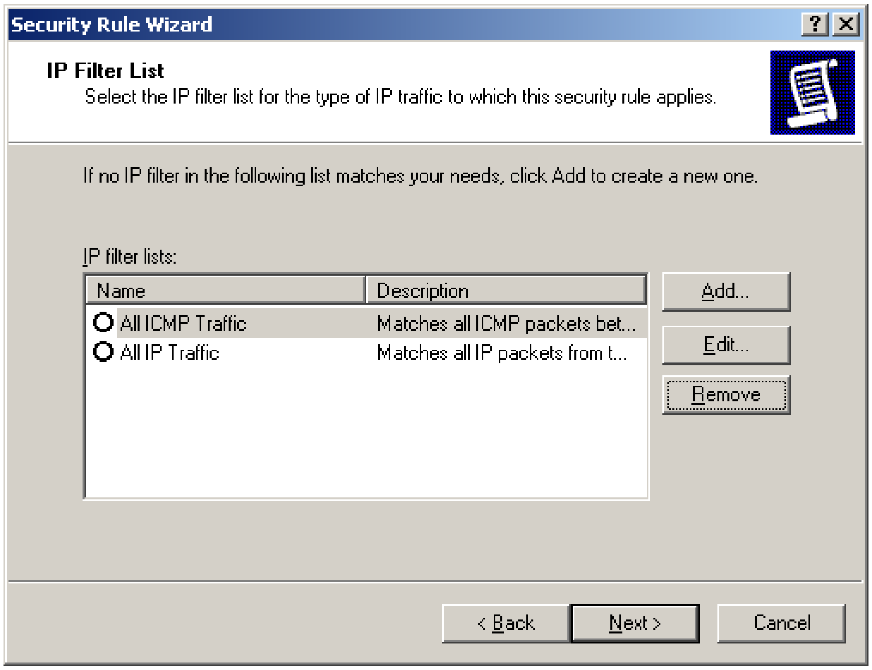
**Authentication Method**

To add multiple authentication methods, edit the security rule after completing the IP Security rule wizard.

Set the initial authentication method for this security rule:

● Active Directory default (Kerberos V5 protocol)
○ Use a certificate from this certification authority (CA):
○ Use this string to protect the key exchange (preshared key):

**If this is a Microsoft AD environment use the "Active Directory default".**



**IP Filter List**

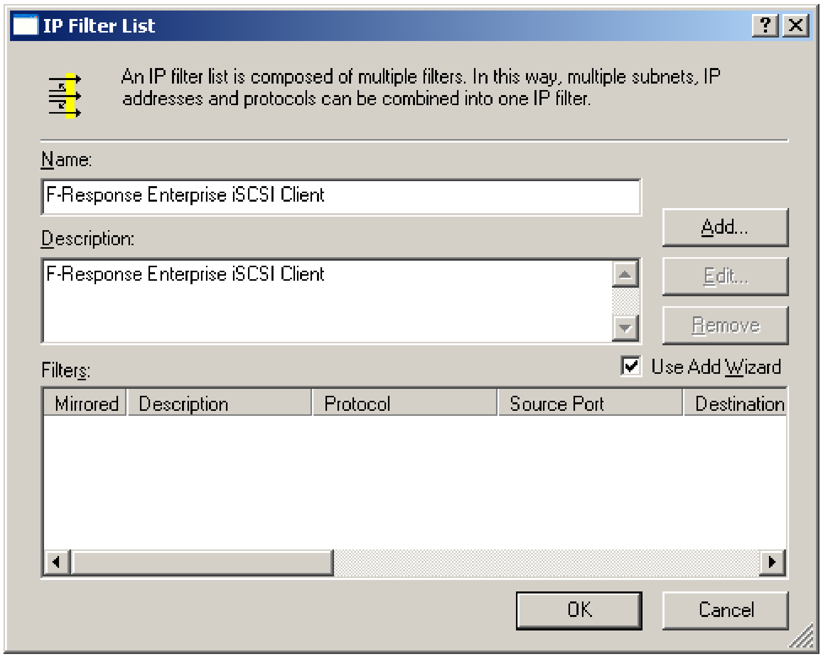
Select the IP filter list for the type of IP traffic to which this security rule applies.

If no IP filter in the following list matches your needs, click Add to create a new one.

IP filter lists:

| Name | Description |
|---|---|
| ○ All ICMP Traffic | Matches all ICMP packets bet... |
| ○ All IP Traffic | Matches all IP packets from t... |

**Next we must add an IP Filter List item, select Add…**



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.

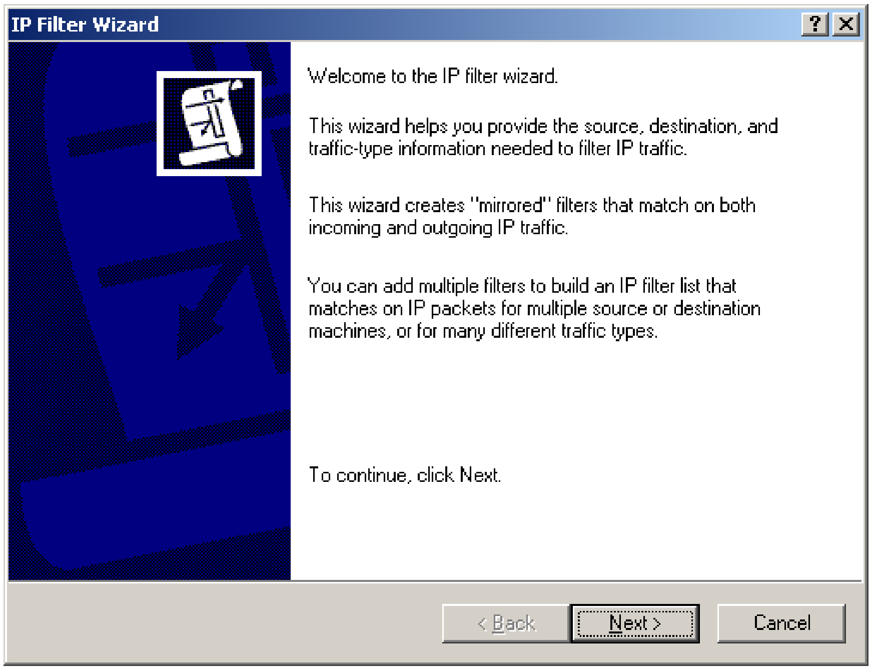
Name: F-Response Enterprise iSCSI Client

Description: F-Response Enterprise iSCSI Client

Filters: ☑ Use Add Wizard

| Mirrored | Description | Protocol | Source Port | Destination |
|---|---|---|---|---|

**Create a name for our IP Filter List, in this case we have labeled it “F-Response Enterprise iSCSI Client”. Next press “Add…” to start the IP Filter Wizard.**


IP Filter Wizard

Welcome to the IP filter wizard.

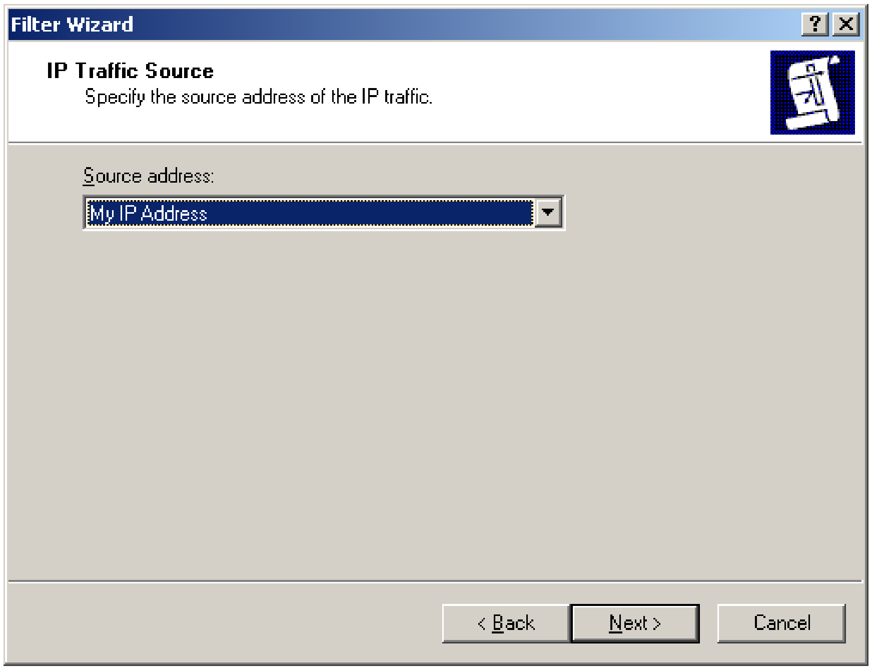
This wizard helps you provide the source, destination, and traffic-type information needed to filter IP traffic.

This wizard creates "mirrored" filters that match on both incoming and outgoing IP traffic.

You can add multiple filters to build an IP filter list that matches on IP packets for multiple source or destination machines, or for many different traffic types.

To continue, click Next.

Press Next to continue.

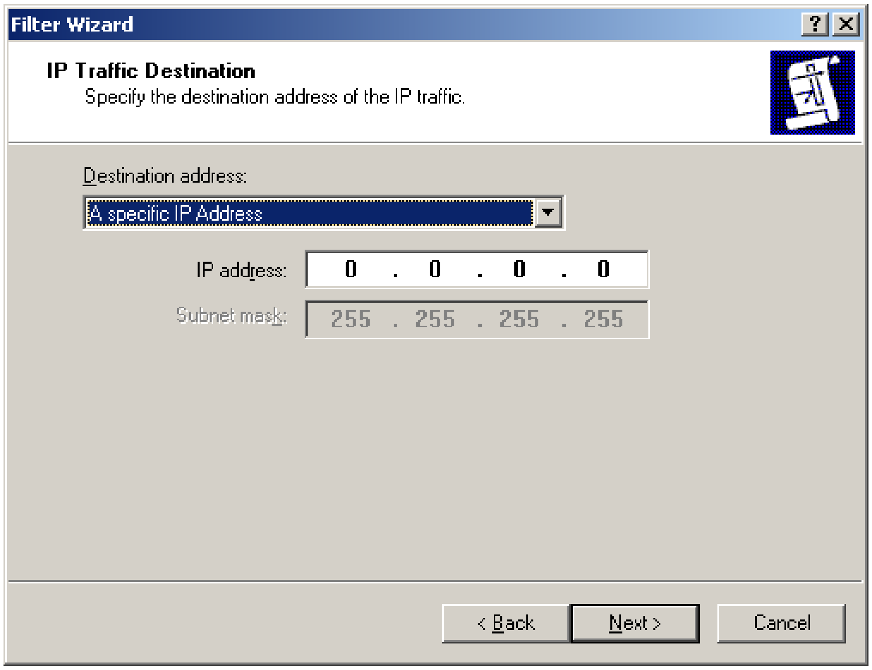

Filter Wizard

IP Traffic Source

Specify the source address of the IP traffic.

Source address: My IP Address

Set the Source address to “My IP Address”.



**IP Traffic Destination**

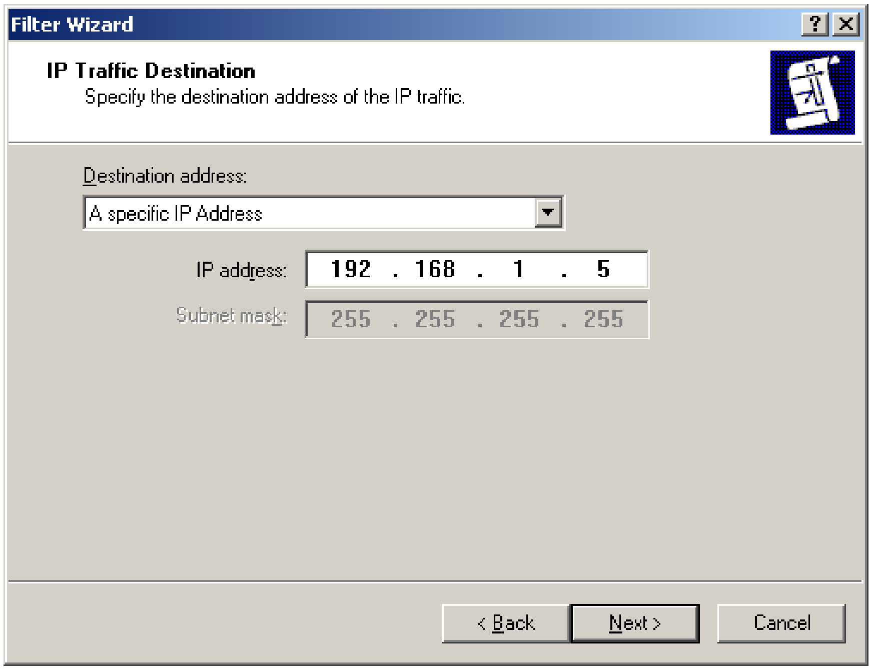
Specify the destination address of the IP traffic.

Destination address: A specific IP Address

IP address: 0 . 0 . 0 . 0

Subnet mask: 255 . 255 . 255 . 255

**Select "A specific IP Address" and enter in the IP address of your analysis workstation.**



**IP Traffic Destination**

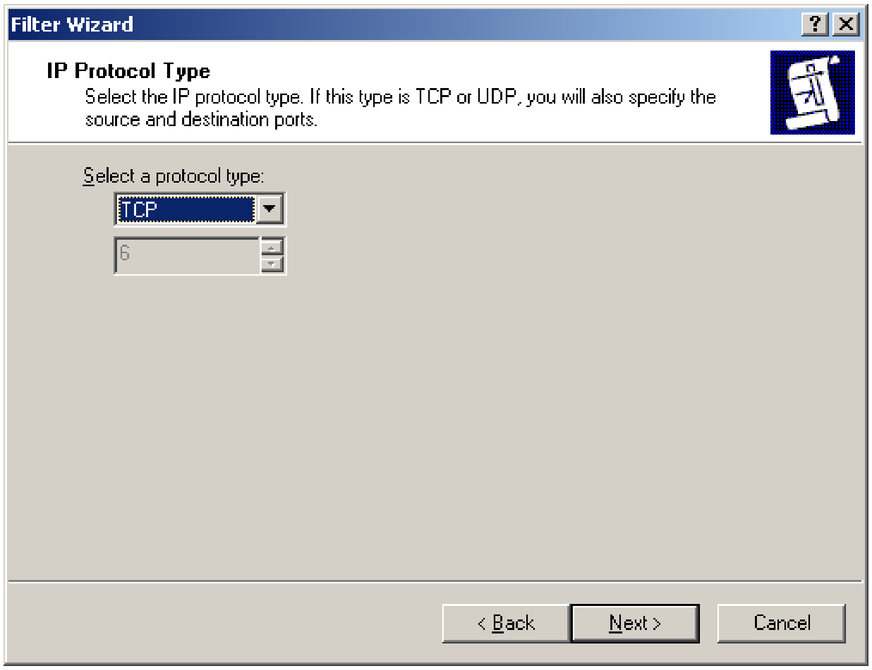
Specify the destination address of the IP traffic.

Destination address: A specific IP Address

IP address: 192 . 168 . 1 . 5

Subnet mask: 255 . 255 . 255 . 255

**In this instance our analysis workstation is at "192.168.1.5".**



**IP Protocol Type**

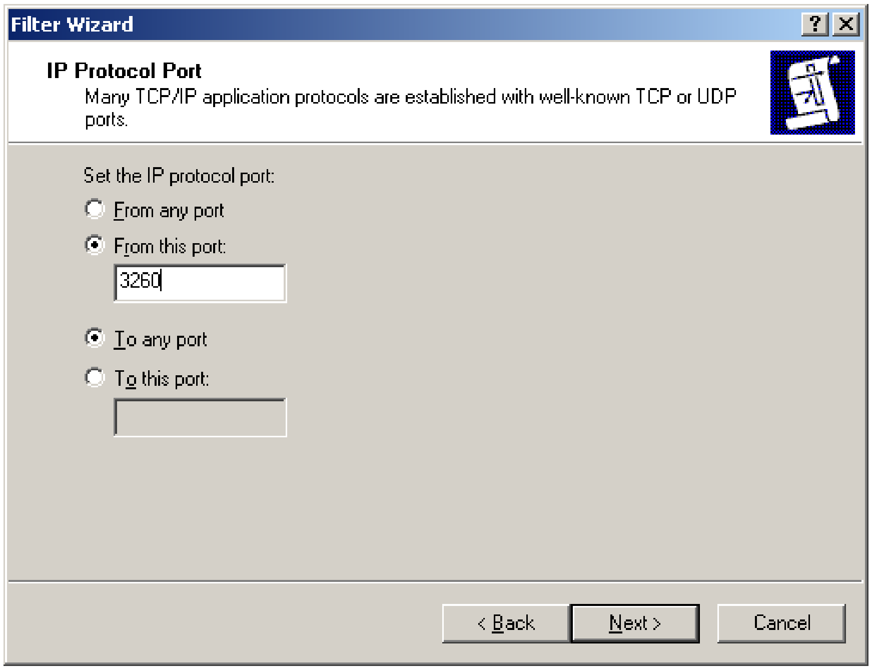
Select the IP protocol type. If this type is TCP or UDP, you will also specify the source and destination ports.

Select a protocol type:

TCP

6

**Select the protocol type as TCP.**



**IP Protocol Port**

Many TCP/IP application protocols are established with well-known TCP or UDP ports.

Set the IP protocol port:

○ From any port

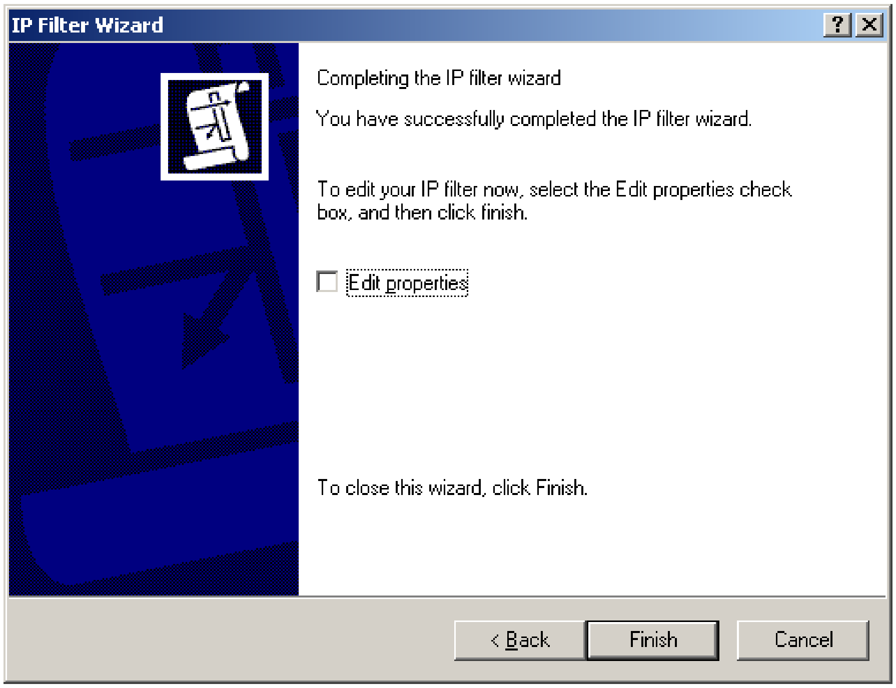
● From this port:

3260

● To any port

○ To this port:

**Set the IP Protocol Port to "To any port" and "From this port" and enter in the value for the F-Response Enterprise client port, in this case we have used the default iSCSI port of 3260. Press Next to continue.**



IP Filter Wizard

Completing the IP filter wizard

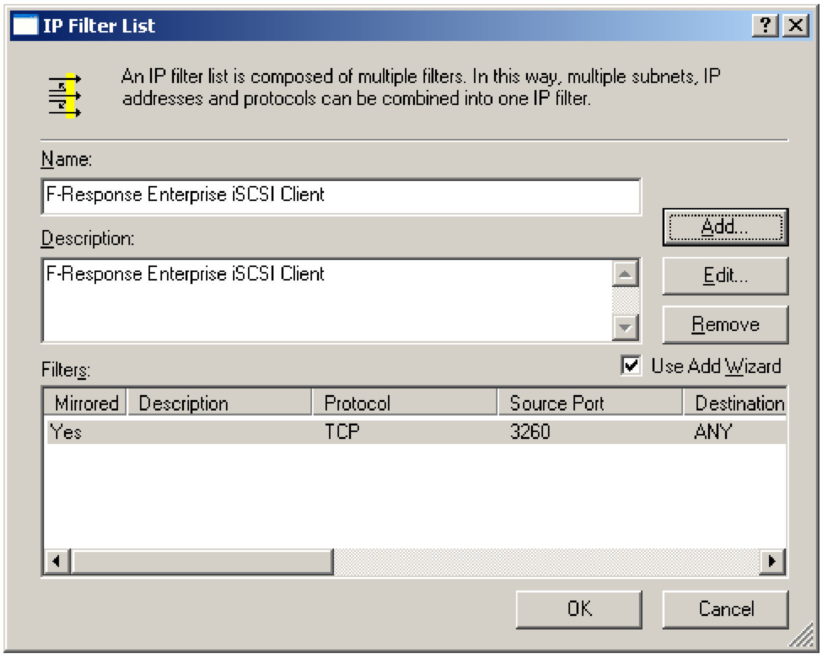
You have successfully completed the IP filter wizard.

To edit your IP filter now, select the Edit properties check box, and then click finish.

☐ Edit properties

To close this wizard, click Finish.

**Press Finish to complete the IP Filter Wizard.**



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:
F-Response Enterprise iSCSI Client

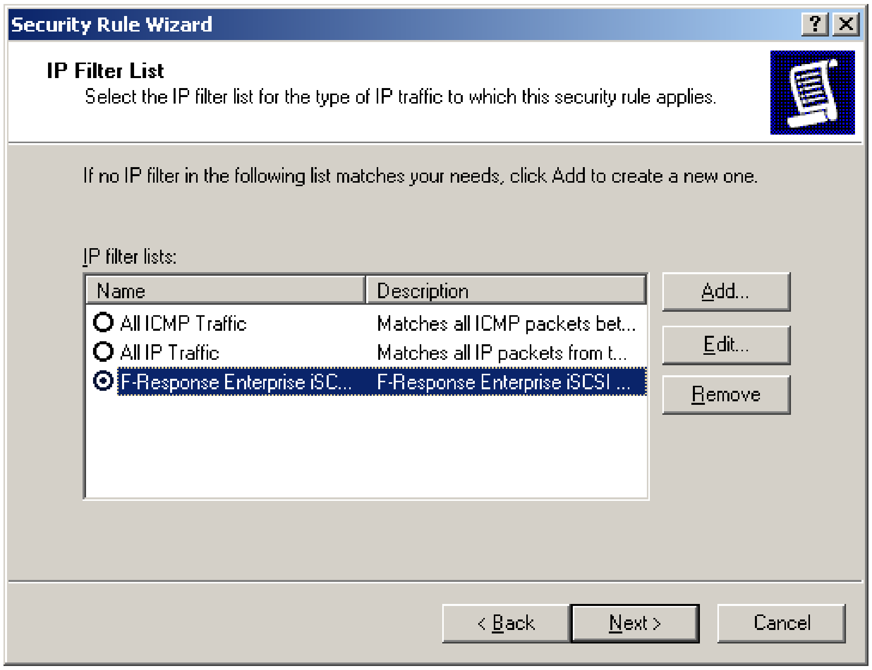
Description:
F-Response Enterprise iSCSI Client

Filters:

☑ Use Add Wizard

| Mirrored | Description | Protocol | Source Port | Destination |
|---|---|---|---|---|
| Yes | | TCP | 3260 | ANY |

**The IP Filter List will now show the newly created Filter. Press Ok to continue.**



Security Rule Wizard

**IP Filter List**

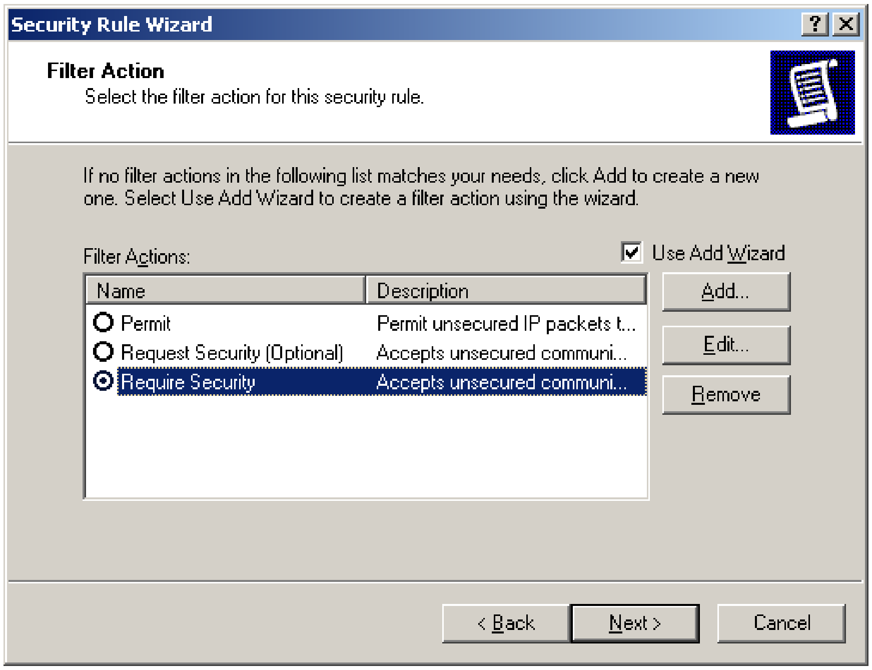
Select the IP filter list for the type of IP traffic to which this security rule applies.

If no IP filter in the following list matches your needs, click Add to create a new one.

IP filter lists:

| Name | Description |
|---|---|
| ○ All ICMP Traffic | Matches all ICMP packets bet... |
| ○ All IP Traffic | Matches all IP packets from t... |
| ● F-Response Enterprise iSC... | F-Response Enterprise iSCSI ... |

**Now enable the F-Response Enterprise iSCSI IP Filter by selecting the option next to the Name.**



Security Rule Wizard

**Filter Action**

Select the filter action for this security rule.

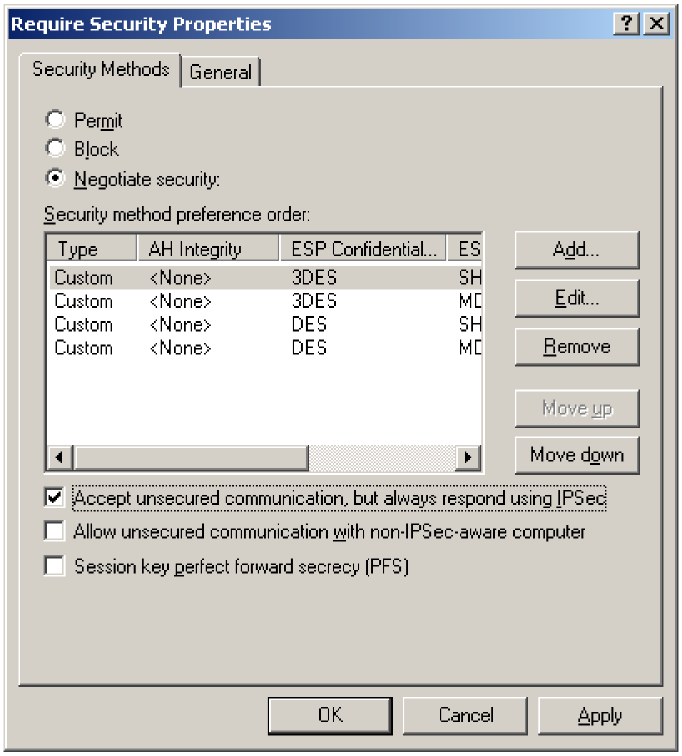
If no filter actions in the following list matches your needs, click Add to create a new one. Select Use Add Wizard to create a filter action using the wizard.

Filter Actions:

☑ Use Add Wizard

| Name | Description |
|---|---|
| ○ Permit | Permit unsecured IP packets t... |
| ○ Request Security (Optional) | Accepts unsecured communi... |
| ● Require Security | Accepts unsecured communi... |

**Select the option button next to "Require Security" and press Edit…**



Require Security Properties

Security Methods | General

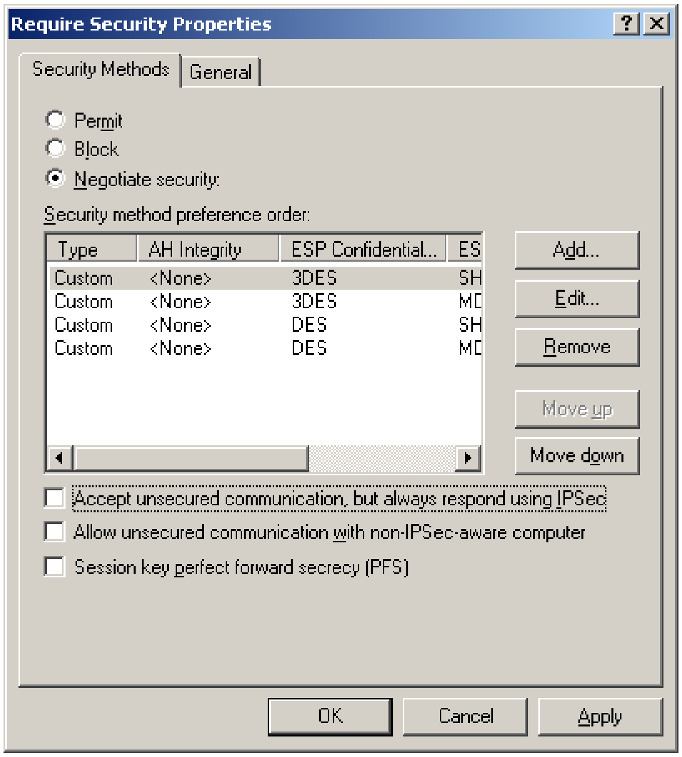
○ Permit
○ Block
● Negotiate security:

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 computer
□ Session key perfect forward secrecy (PFS)

**Remove the check box next to "Accept unsecured communication.."**



Require Security Properties

Security Methods | General

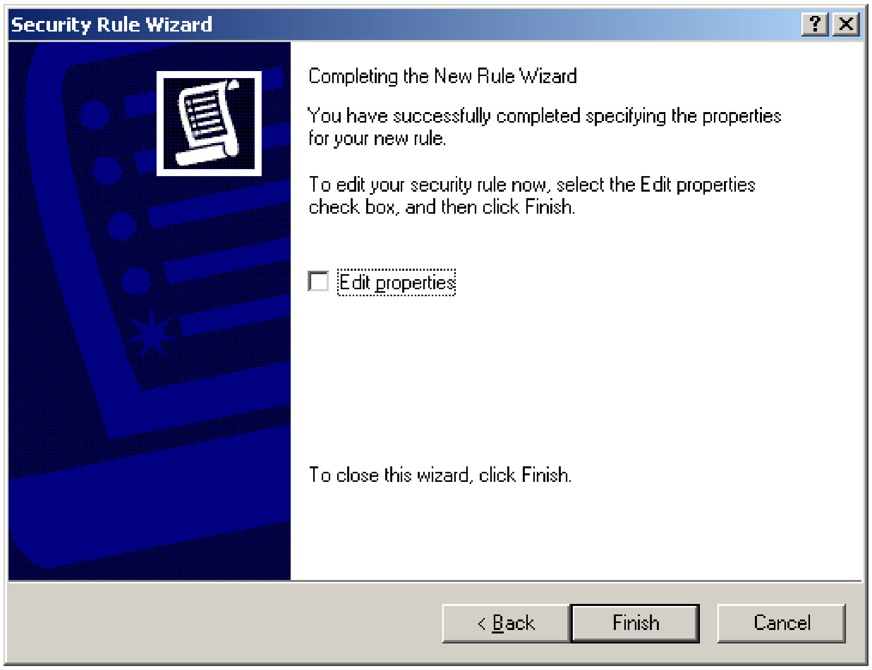
○ Permit
○ Block
● Negotiate security:

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 computer
□ Session key perfect forward secrecy (PFS)

**Press Ok to continue.**



Completing the New Rule Wizard

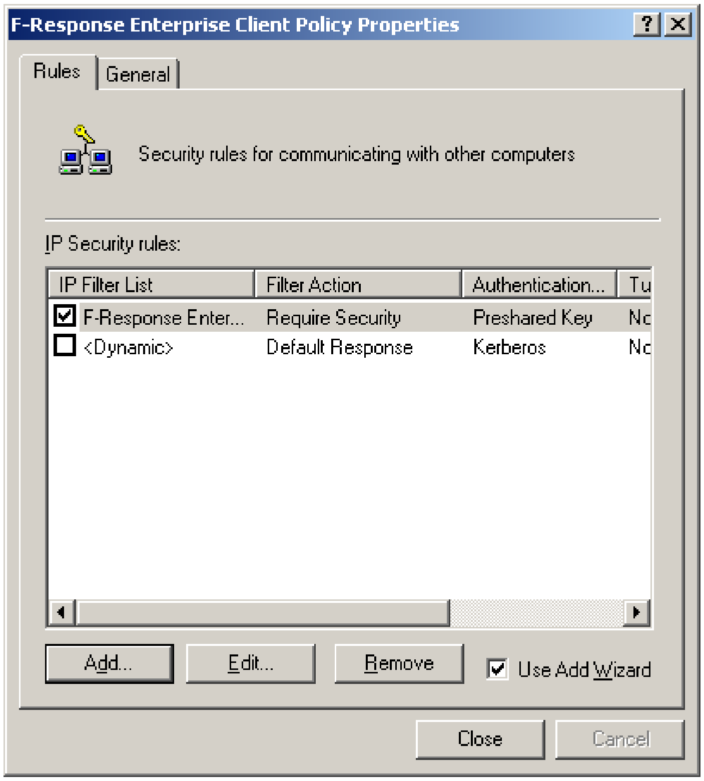
You have successfully completed specifying the properties for your new rule.

To edit your security rule now, select the Edit properties check box, and then click Finish.

☐ Edit properties

To close this wizard, click Finish.

**Press Finish to complete the Security Rule Wizard.**

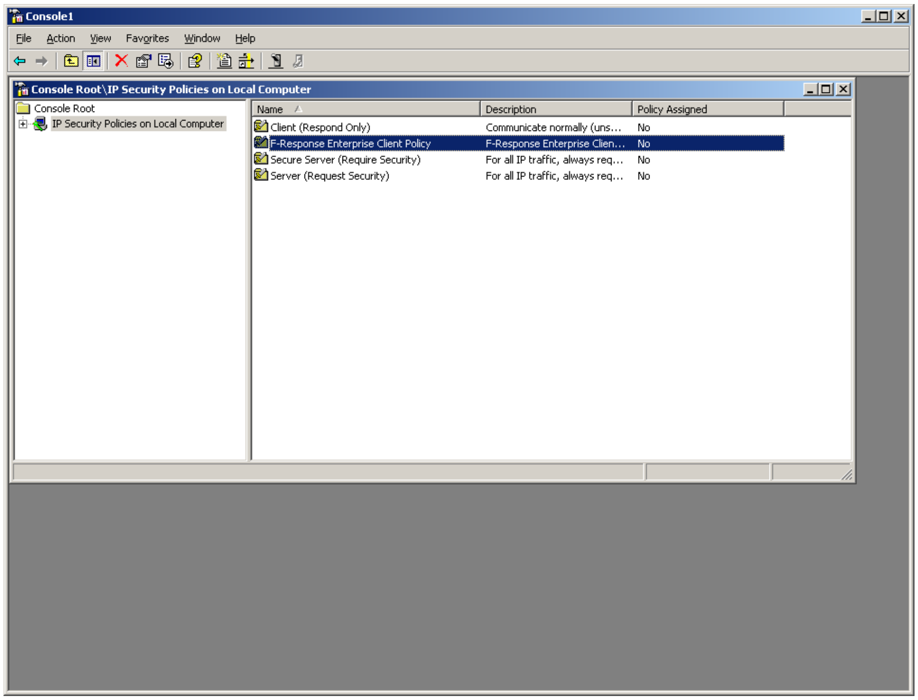


Security rules for communicating with other computers

IP Security rules:

| IP Filter List | Filter Action | Authentication... | Tu |
|---|---|---|---|
| ☑ F-Response Enter... | Require Security | Preshared Key | Nc |
| ☐ <Dynamic> | Default Response | Kerberos | Nc |

**Confirm that the F-Response iSCSI IP Filter is checked in the F-Response Analysis Workstation Policy Properties and press Close.**


Console1
File
Action
View
Favorites
Window
Help
Console Root\IP Security Policies on Local Computer
Console Root
IP Security Policies on Local Computer

| Name | Description | Policy Assigned |
|---|---|---|
| Client (Respond Only) | Communicate normally (uns... | No |
| F-Response Enterprise Client Policy | F-Response Enterprise Clien... | No |
| Secure Server (Require Security) | For all IP traffic, always req... | No |
| Server (Request Security) | For all IP traffic, always req... | No |

**To enable the policy select it, right click and press “Assign”.**

# Frequently Asked Questions

1. Q) Can multiple initiators connect to a single F-Response target machine?
2. Q) Do I change any data on the target computer by using F-Response?
3. Q) I am connected via F-Response and it appears that I just deleted a file on the machine under inspection. I chose a file, hit delete, and now it's gone. Did I really delete the file?
4. Q) I have a personal firewall running on my computers. Do I need to change firewall settings to use F-Response?
5. Q) I have a remote user that accidentally deleted a file. Can I use F-Response to recover deleted files?
6. Q) Is the F-Response iSCSI connection encrypted?
7. Q) Does F-Response work as an agent?
8. Q) Can I deploy F-Response to Linux or Other Operating Systems (OS's)?
9. Q) I established an F-Response connection, tried to view the remote "Documents and Settings" folder and received a message that I don't have permission to view that folder. Why don't I have access?
10. Q) Can I authenticate and tunnel my F-Response session over IPSec?

1. Q) Can multiple initiators connect to a single F-Response target machine?
   A) While the F-Response target code is running, any iSCSI initiator with access to the listening port can connect to the machine; provided, of course, that the proper authentication credentials are provided.

2. Q) Do I change any data on the target computer by using F-Response?
   A) Once the F-Response Target code is executed and the network connection is established, the practitioner conducting the analysis has no capability to edit or alter data on the machine under inspection. Executing or starting the F-Response service does, of course, effect some change to the target computer, but the changes are about as minimal as they can be for analysis that is being conducted on a live machine.

3. Q) I am connected via F-Response and it appears that I just deleted a file on the machine under inspection. I chose a file, hit delete, and now it's gone.
   A) No, you didn't delete the file. You cannot delete files, alter Meta data, or effect any other changes on the machine under inspection using F-Response. What you did do was fool your analysis machine into believing that the file is deleted and thus your analysis machine is no longer presenting the file to you as being available.

4. Q) I have a personal firewall running on my computers. Do I need to change firewall settings to use F-Response?
   A) Yes, personal firewalls are the single most likely cause for a connection failure. F-Response machines must be able to send and receive on port 3260 (this default is changeable) and if using the Consultant Edition, also port 5680 (this default is changeable). We recommend disabling the firewall for the duration of the session during ad hoc usage (e.g. temporary consultant use at a third party site), and tuning the firewall configurations to allow F-Response connectivity for planned enterprise deployment.

5. Q) I have a remote user that accidentally deleted a file. Can I use F-Response to recover deleted files?

A) F-Response will enable you to use your recovery tool of choice to recover the file(s) to a location other than the target machine. You cannot restore the file directly to the target machine via F-Response because you do not have write capability on that machine, but you can recover the file and make it available to the user via email , network share, etc.

6. Q) Is the F-Response iSCSI connection encrypted?
   A) No. F-Response connections are established on your local corporate network, which alleviates the need for the additional overhead of an encrypted connection. If F-Response is being used over the Internet and corporate policy dictates encryption over public networks, then the existing corporate VPN capability should satisfy the encryption policy. If strong user demand calls for encrypted connections, then it is a capability we will consider adding as an option in a future release.

7. Q) Does F-Response work as an agent?
   A) No. It does not collect or store any data on the machine under inspection. It does not report to a management server. It does not have an inherent analysis or reporting capability.

8. Q) Can I deploy F-Response to Linux or Other Operating Systems (OS's)?
   A) We've done some limited testing with the Linux iSCSI Initiator, which enables deployment of Linux-based analysis tools against Windows-based machines under inspection. We have not yet released F-Response target code that would permit analysis of Linux or other OS's under inspection. These are future release items that will be developed as demand dictates.

9. Q) I established an F-Response connection, tried to view the remote "Documents and Settings" folder and received a message that I don't have permission to view that folder. Why don't I have access?
   A) You have the access with the right tools. You probably used Windows Explorer or an equivalent tool that is subject to the file permission settings for those folders. If you use a forensics tool that can take advantage of your raw drive access, then you won't have this issue.

10. Q) Can I authenticate and tunnel my F-Response session over IPSec?
    A) Sure. One method is to use Microsoft IPSec policy manager to create a configuration to enforce an IPSec policy for the F-Response ports (defaults are TCP/UDP 3260 & 5680). This is ideal for those who would prefer to leave the F-Response service running at all times, rather than starting the service only when needed.

# Support

We take pride in providing prompt attention to your support needs, and will support your F-Response product for the period of your license term. F-Response support can be reached via

Email: support@f-response.com
Website: www.f-response.com

Software and documentation updates will be made available for download to registered users on the F-Response web site. E-mail support is available to licensed software users. We typically respond to your queries within 1 business day of receiving your request.

# Appendix A – Legal Notices

## Legal Notice

## Trademarks

F-Response is a trademark of Agile Risk Management, LLC. All other product names or logos mentioned herein are used for identification purposes only, and are the trademarks of their respective owners.

## Statement of Rights

Agile Risk Management, LLC products incorporate technology that is protected by U.S. patent and other intellectual property (IP) rights owned by Agile Risk Management LLC, and other rights owners. Use of these products constitutes your legal agreement to honor Agile Risk Management, LLC's IP rights as protected by applicable laws. Reverse engineering, de-compiling, or disassembly of Agile Risk Management, LLC products is strictly prohibited.

## Disclaimer

While Agile Risk Management LLC has committed its best efforts to providing accurate information in this document, we assume no responsibility for any inaccuracies that may be contained herein, and we reserve the right to make changes to this document without notice.