

# Centrify Isolation and Encryption Service

## *Isolation and Encryption Service Evaluation Guide*

November 2018 (release 18.11)

Centrify Corporation



## Legal Notice

This document and the software described in this document are furnished under and are subject to the terms of a license agreement or a non-disclosure agreement. Except as expressly set forth in such license agreement or non-disclosure agreement, Centrifry Corporation provides this document and the software described in this document “as is” without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability or fitness for a particular purpose. Some states do not allow disclaimers of express or implied warranties in certain transactions; therefore, this statement may not apply to you.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of Centrifry Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of Centrifry Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. Centrifry Corporation may make improvements in or changes to the software described in this document at any time.

© **2004-2018 Centrifry Corporation. All rights reserved.** Portions of Centrifry software are derived from third party or open source software. Copyright and legal notices for these sources are listed separately in the Acknowledgements.txt file included with the software.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government’s rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

Centrifry, DirectControl, DirectAuthorize, DirectAudit, DirectSecure, DirectControl Express, Centrifry for Mobile, Centrifry for SaaS, DirectManage, Centrifry Express, DirectManage Express, Centrifry Suite, Centrifry User Suite, Centrifry Identity Service, Centrifry Privilege Service and Centrifry Server Suite are registered trademarks of Centrifry Corporation in the United States and other countries. Microsoft, Active Directory, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and other countries.

Centrifry software is protected by U.S. Patents 7,591,005; 8,024,360; 8,321,523; 9,015,103; 9,112,846; 9,197,670; 9,442,962 and 9,378,391.

The names of any other companies and products mentioned in this document may be the trademarks or registered trademarks of their respective owners. Unless otherwise noted, all of the names used as examples of companies, organizations, domain names, people and events herein are fictitious. No association with any real company, organization, domain name, person, or event is intended or should be inferred.

# Contents

About this guide .....	4
Intended audience .....	4
Using this guide .....	4
Documentation conventions .....	5
Finding more information about Centrify products .....	5
Contacting Centrify .....	6
Getting additional support .....	6
 Introduction and setup .....	 7
Setting up your environment .....	7
 Installing the isolation and encryption service .....	 9
 Configuring IP security policy in Active Directory .....	 10
Creating the IP security policy: DS-Eval .....	11
Creating and configuring Rule1 .....	13
Creating and Configuring Rule2 (OPTIONAL) .....	22
 Useful tools to use with isolation and encryption service .....	 26
WireShark .....	26
Windows IP Security Monitor .....	29
Microsoft IPSec Diagnostic tool .....	32

# About this guide

The *Isolation and Encryption Service Evaluation Guide* shows you how to configure some example IP security policies using Centrify Isolation and Encryption Service. This service enables you to manage IP Security Policies on UNIX computers using Active Directory group policies. The IP Security Policies protect sensitive information by isolating trusted computers on the network and enabling end-to-end encryption of data in motion.

## Intended audience

The *Isolation and Encryption Service Evaluation Guide* is intended for network administrators who are responsible for securing communication between trusted computers. The guide assumes that you have a functioning IP Security policies configured for at least one Windows domain. If you do not have IP Security policies configured or are unfamiliar with how to configure Active Directory group policies, you should consult the documentation provided by Microsoft. If you are familiar with Active Directory group policies, group policy objects, and how to configure and apply IP Security policies on Windows computers, this guide notes where isolation and encryption service IP Security policies differ from the policies defined on Windows.

## Using this guide

The guide provides the following information:

- [Introduction and setup](#) provides a brief introduction to isolation and encryption service and what you need to setup in your environment.
- [Installing the isolation and encryption service](#) provides information on how to install isolation and encryption service.

- [Configuring IP security policy in Active Directory](#) provides step-by-step details for how to configure a couple of IP security policies.
- [Useful tools to use with isolation and encryption service](#) shows you how to use a few common network administration tools along with isolation and encryption service.

## Documentation conventions

The following conventions are used in Centrify documentation:

- Fixed-width font is used for sample code, program names, program output, file names, and commands that you type at the command line. When *italicized*, this font indicates variables. Square brackets ([ ]) indicate optional command-line arguments.
- **Bold** text is used to emphasize commands or key command results; buttons or user interface text; and new terms.
- *Italics* are used for book titles and to emphasize specific words or terms. In fixed-width font, italics indicate variable values.
- Standalone software packages include version and architecture information in the file name. Full file names are not documented in this guide. For complete file names for the software packages you want to install, see the distribution media.
- For simplicity, UNIX is used to refer to all supported versions of the UNIX and Linux operating systems. Some parameters can also be used on Mac OS X computers.

## Finding more information about Centrify products

Centrify provides extensive documentation targeted for specific audiences, functional roles, or topics of interest. If you want to learn more about Centrify and Centrify products and features, start by visiting the [Centrify website](#). From the Centrify website, you can download data sheets and evaluation software, view video demonstrations and technical presentations about Centrify products, and get the latest news about upcoming events and webinars.



For access to documentation for all Centrify products and services, visit the [Centrify documentation portal](https://docs.centrify.com) at [docs.centrify.com](https://docs.centrify.com). From the Centrify documentation portal, you can always view or download the most up-to-date version of this guide and all other product documentation.

For the most up to date list of known issues, please login to the Customer Support Portal at <http://www.centrify.com/support> and refer to Knowledge Base articles for any known issues with the release.

## Contacting Centrify

You can contact Centrify by visiting our website, [www.centrify.com](http://www.centrify.com). On the website, you can find information about Centrify office locations worldwide, email and phone numbers for contacting Centrify sales, and links for following Centrify on social media. If you have questions or comments, we look forward to hearing from you.

## Getting additional support

If you have a Centrify account, click Support on the Centrify website to log on and access the [Centrify Technical Support Portal](#). From the support portal, you can search knowledge base articles, open and view support cases, download software, and access other resources.

To connect with other Centrify users, ask questions, or share information, visit the [Centrify Community](#) website to check in on customer forums, read the latest blog posts, view how-to videos, or exchange ideas with members of the community.

# Introduction and setup

Centrify Isolation and Encryption Service brings the same 'It Just Works' mode of operation to non-Windows platforms for IPsec deployment across mixed Windows and non-Windows environments.

This document describes two worked examples of the use of Centrify Isolation and Encryption Service. The first example applies within one subnet and allows all ftp and telnet traffic to flow from any machine to any other within that subnet under IPsec security protection. In the second example, a second subnet is brought into the equation. Within in the second subnet all traffic is unencrypted, but traffic between the two subnets will be under IPsec security protection.

The policy described in this document is an application-specific policy that only causes ftp and telnet data to be secured by IPsec. Unlike a blanket policy, exclusions for Domain Controllers, DHCP and DNS computers are not needed.

**Note** If you want to try just the first example, you can ignore the items marked "OPTIONAL" in this document.

Even if you choose to implement the Optional setup and try the second example, it is highly recommended that the first example is run first, before moving on to the more complex example.

## Setting up your environment

Use the Isolation and Encryption Service Evaluation Guide to set up the isolation and encryption service evaluation environment.

The environment needs to be enhanced and adjusted to have the following minimum requirements for the isolation and encryption service examples:

- Use Centrify agent for \*NIX version 4.4.0 or later. You need to use the same version for both the authentication service and the isolation and encryption service.
- You need three Windows machines: two can be workstations, and one can be a server. Refer to the isolation and encryption service release notes for supported versions.
- Two UNIX machines. Refer to the isolation and encryption service release notes for supported versions.

All of the Windows and UNIX machines (after they join Active Directory) should reside in the same Active Directory (AD) domain.

- (OPTIONAL) You need two subnets
  - Subnet1: contains all of the non-optional machines
  - Subnet2: contains all of the optional machines
- Each machine needs an ftp server
- Each machine needs a telnet server

Before starting the worked examples, ensure:

- Centrify Authentication Service is installed on the UNIX machines. The machines should not yet have joined the domain.
- Ftp and telnet should work between all machines. This is worth testing now before enabling IPsec as IPsec will control telnet and ftp traffic flow once enabled.

# Installing the isolation and encryption service

Before installing isolation and encryption service, make sure the UNIX machines are not joined to Active Directory. If necessary, use `adleave` to leave the domain.

Centrify Isolation and Encryption Service is packaged in RPMs specific to the UNIX platform being used. Choose the isolation and encryption service package appropriate to your platform and run the following command as root:

```
rpm -Uvh CentrifyDS-<version>-<platform>.rpm
```

There is no UNIX-side configuration required for isolation and encryption service after installation.

There is also no Windows-side installation required for isolation and encryption service.

The isolation and encryption service will be activated as soon as the UNIX machine joins Active Directory, assuming there is an active IP security policy applied to the UNIX machines (at domain or OU level). If the applicable IP security policy is activated after the UNIX machine joins Active Directory, isolation and encryption service will be activated as soon as the relevant GPO is reflected on the UNIX machine either via the combined "GPO and IP security policy" refreshing cycle or via manual GPO or IP Security update to the UNIX machine using `adgpupdate`.

This is why the UNIX machine should not be joined to the domain during installation. If there was a policy in effect it would take effect on the UNIX machine as soon as isolation and encryption service was installed and that would affect the examples here.

# Configuring IP security policy in Active Directory

There will be one IP security policy at the domain level for these isolation and encryption service examples. The policy is called DS-Eval in this document, but other names can be used, of course.

There are two rules in this policy. Again, other names for rules can be used:

- Rule1: Subnet-wide ftp and telnet
- Rule2: Cross-subnet ftp and telnet (OPTIONAL)

This IP security policy will enable the following two use cases. Rule1 will enable use case 1. Rule1 and Rule2 together will enable use case 2.

- Use case 1 Data privacy and integrity for ftp and telnet traffic within a subnet (Subnet1).
- Use case 2 (OPTIONAL) Data privacy and integrity for ftp and telnet traffic between Subnet1 and Subnet2.

Both rules have multiple filters:

- Rule 1 has filters:
  - Subnet-wide ftp
  - Subnet-wide telnet
- Rule 2 has filters:
  - Cross-subnet ftp1
  - Cross-subnet ftp2
  - Cross-subnet telnet1
  - Cross-subnet telnet2

The following table summarizes these filters:

ID	Source	Port	Destination	Port	ESP/AH	Auth method
Subnet-wide FTP	Subnet1	Any	Subnet1	21	ESP	Kerberos
Subnet-wide Telnet	Subnet1	Any	Subnet1	23	ESP	Kerberos
Cross-subnet FTP1	Subnet1	Any	Subnet2	21	ESP	Kerberos
Cross-subnet FTP2	Subnet2	Any	Subnet1	21	ESP	Kerberos
Cross-subnet Telnet1	Subnet1	Any	Subnet2	23	ESP	Kerberos
Cross-subnet Telnet2	Subnet2	Any	Subnet1	23	ESP	Kerberos

The rest of this section provides instructions for, and screenshots of, the configuration of this IP security policy which includes the above rules and filters.

**Note** Rules in an IP security policy can be turned on or off independent of each other based on the intended use cases.

## Creating the IP security policy: DS-Eval

IP security policies are defined in Group Policies, applied at the domain or OU level. For this guide, a domain-level security group policy is used.

IP security policies are machine policies and can be found in **Computer Configuration->Windows Settings->Security Settings-> IP Security Policies** in Active Directory.

To create a new policy, start the Domain Security Policy tool (NOTE: ensure you do NOT start the Domain Controller Security Policy tool) and right-click on **IPsec Security Policies** on Active Directory in the left pane. Select **Create IP Security Policy** and the IP Security Policy Wizard will start.

Click Next and enter a name and description for the policy name (see screenshot below).

IP Security Policy Wizard

**IP Security Policy Name**  
Name this IP Security policy and provide a brief description

Name:  
DS-Eval IP Security Policy

Description:  
Eval Policy with 2 Rules: Subnet FTP-Telnet and Cross Subnet FTP-Telnet

< Back Next > Cancel

Click Next, and on the next screen unselect the Activate the default response rule checkbox.

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.

< Back Next > Cancel

Click Next, and this will complete the Wizard. Click Finish to create the policy.

.....

After the Wizard completes, the properties page for your new policy will be displayed. There are two tabs for this policy. The rules tab allows you to define the rules for this policy and the general tab is used to configure general parameters for the policy. The general parameters do not need to be changed and we will take the default settings.

## Creating and configuring Rule1

In the DS-Eval IP security policy there are two rules. Rule2 is **OPTIONAL**.

### Creating Rule1

Rules are defined as a filters list with associated filter actions and authentication methods.

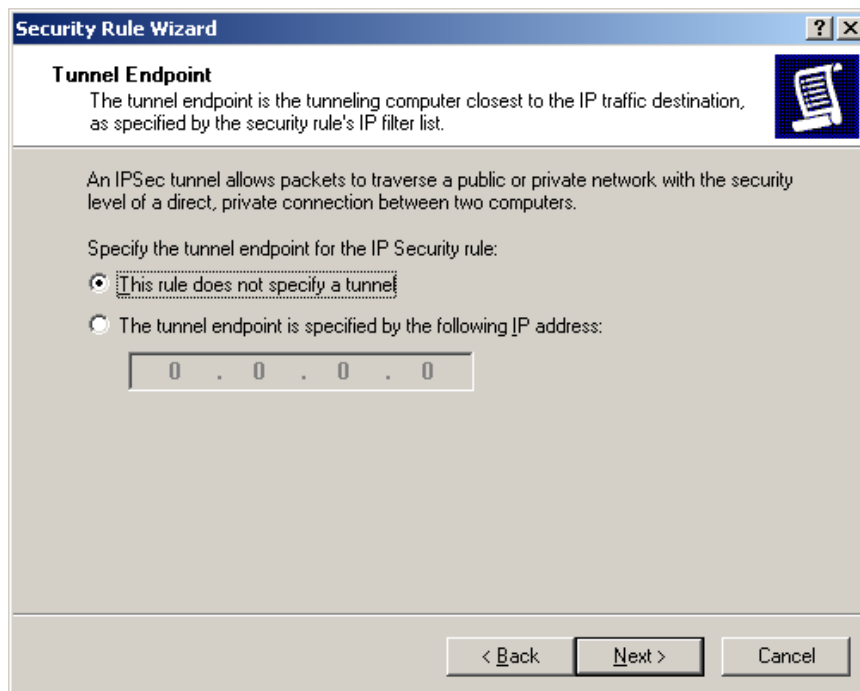
**Note** In the following steps there are two ways to configure rules, one uses a Wizard the other uses property pages. To begin with it is helpful to use the Wizard, and these worked examples will all be wizard based. Before you click “Add” to add new objects, ensure that any “Use Add wizard” checkbox is selected.

To create a new rule, from the policy properties page Rules tab, click Add and you will start the Create IP Security Rule Wizard.



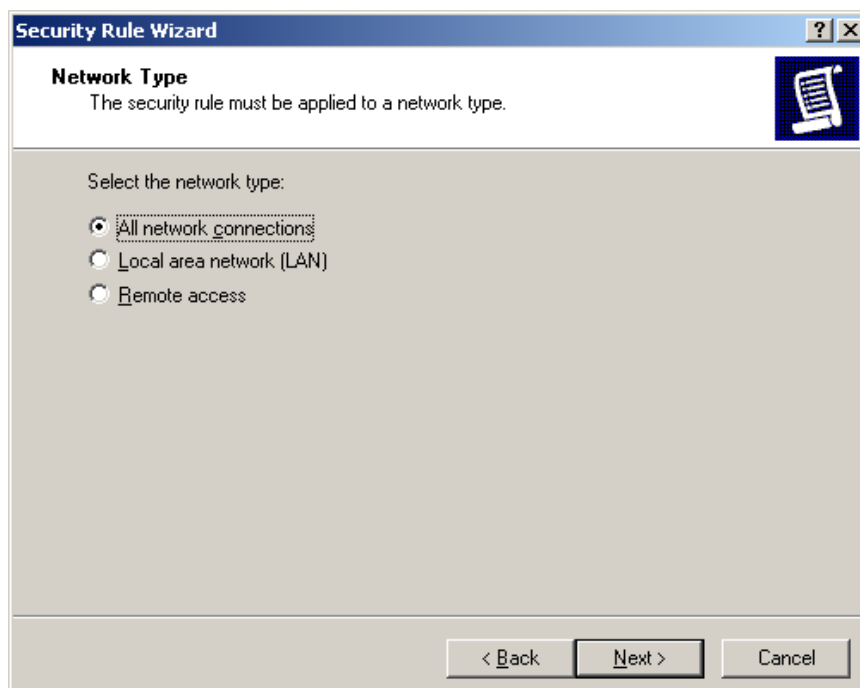
.....

The next Wizard page allows you to define an IP tunnel. Centrify Isolation and Encryption Service is only used for transport mode connections (which is the default for this page), so click Next to accept defaults.



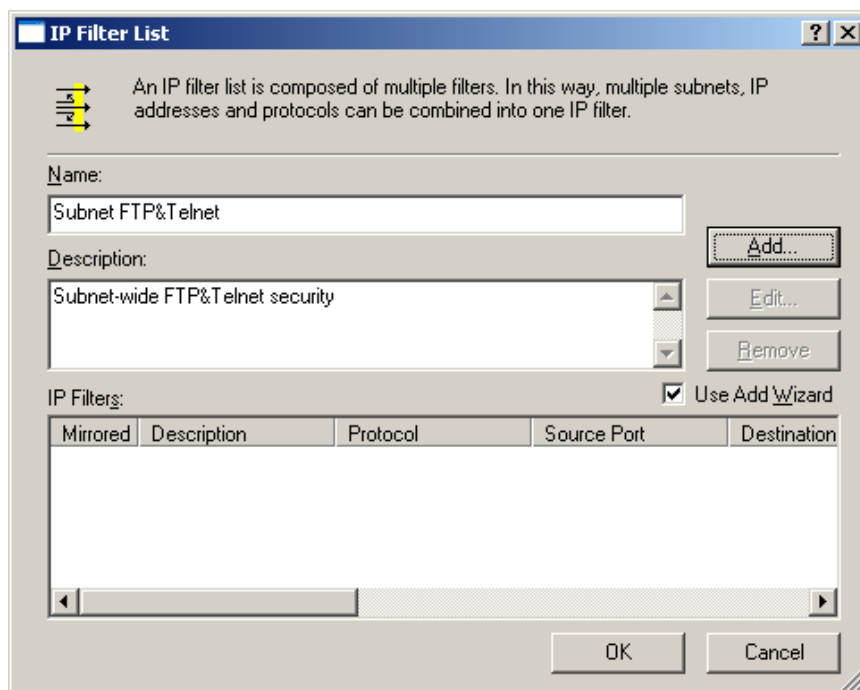
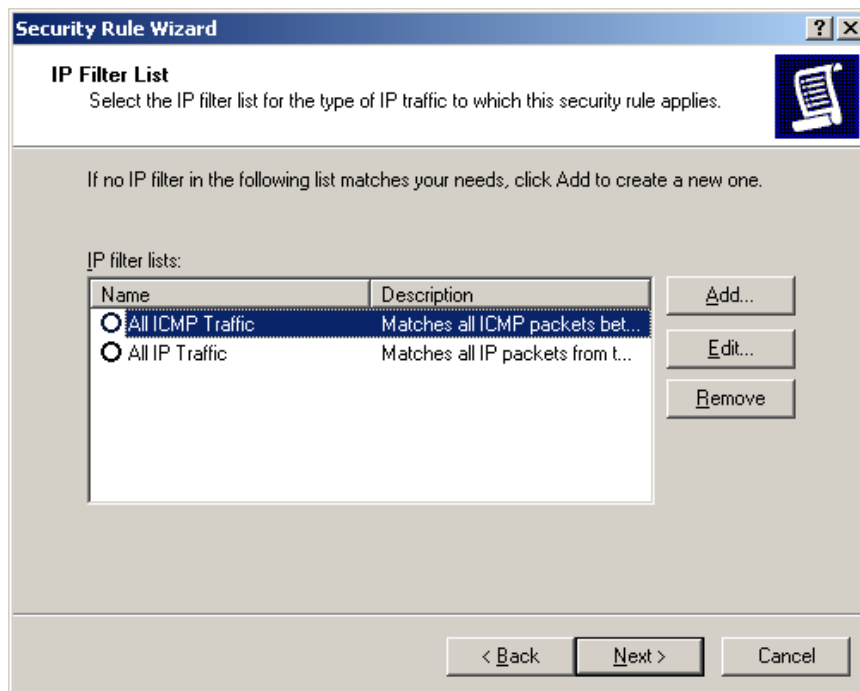
The screenshot shows the 'Security Rule Wizard' window, specifically the 'Tunnel Endpoint' page. The title bar reads 'Security Rule Wizard'. The page has a blue header with the title 'Tunnel Endpoint' and a help icon. Below the header, a text box explains: 'The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the security rule's IP filter list.' A paragraph follows: 'An IPSec tunnel allows packets to traverse a public or private network with the security level of a direct, private connection between two computers.' The instruction 'Specify the tunnel endpoint for the IP Security rule:' is followed by two radio button options. The first option, 'This rule does not specify a tunnel', is selected. The second option is 'The tunnel endpoint is specified by the following IP address:', followed by an input field containing '0 . 0 . 0 . 0'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

The next page allows you to choose the network type. Currently Centrify Isolation and Encryption Service supports only “All network connections”, which is the default. Choose Next to continue.



The screenshot shows the 'Security Rule Wizard' window, specifically the 'Network Type' page. The title bar reads 'Security Rule Wizard'. The page has a blue header with the title 'Network Type' and a help icon. Below the header, a text box explains: 'The security rule must be applied to a network type.' A paragraph follows: 'Select the network type:'. There are three radio button options: 'All network connections' (selected), 'Local area network (LAN)', and 'Remote access'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

On the next page you create an IP filter list. Click Add to add a new list and then enter a name and description for the new filter list, similar to the example below.



Click Add to start the IP Filter Wizard, then click Next. The Wizard will show basic properties for the filter. Ensure the **Mirrored** checkbox is selected and then click Next.

**IP Filter Wizard**

**IP Filter Description and Mirrored property**

Use the Description field to specify a name or a detailed explanation of the IP filter. Select the Mirrored check box to specify a filter in each direction.

Description:

Subnet-wide FTP security

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

< Back   Next >   Cancel

The next page selects the traffic source for the filter. Select A specific IP subnet as the source address and enter your subnet address and netmask; it should look similar to the screenshot below.

**IP Filter Wizard**

**IP Traffic Source**

Specify the source address of the IP traffic.

Source address:

A specific IP Subnet

IP Address: 172 . 27 . 16 . 0

Subnet mask: 255 . 255 . 248 . 0

< Back   Next >   Cancel

Click next to define the IP traffic destination. Again, choose A specific IP subnet, enter your subnet address and netmask, and then click Next.

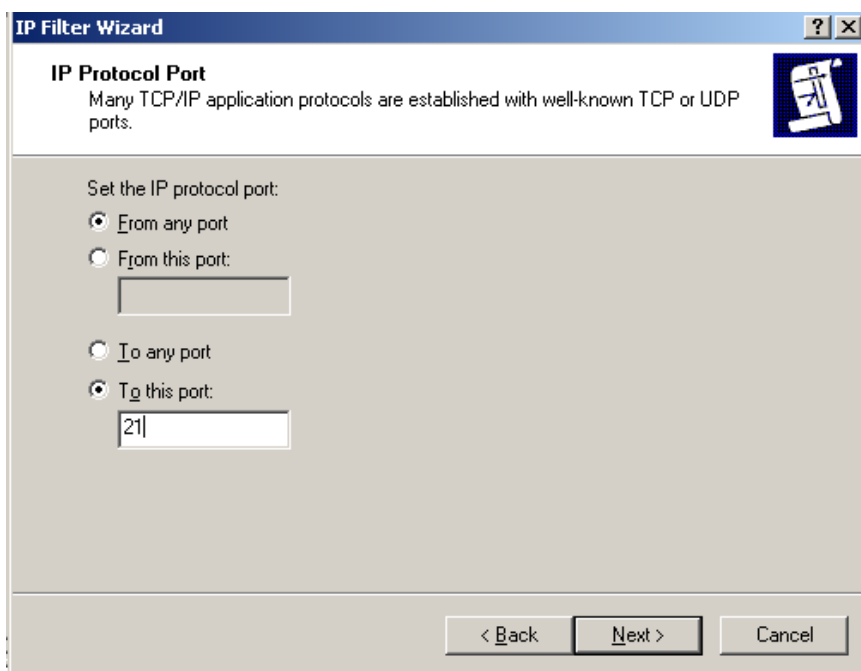
.....

The screenshot shows the 'IP Filter Wizard' window, specifically the 'IP Traffic Destination' step. The title bar reads 'IP Filter Wizard'. Below the title bar, the step is labeled 'IP Traffic Destination' with the instruction 'Specify the destination address of the IP traffic.' and a small icon of a document with a magnifying glass. The main area contains a 'Destination address:' label followed by a dropdown menu currently showing 'A specific IP Subnet'. Below this, there are two input fields: 'IP address:' with the value '172 . 27 . 16 . 0' and 'Subnet mask:' with the value '255 . 255 . 248 . 0'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'. A mouse cursor is hovering over the 'Next >' button.

The next page allows you to choose the IP protocol type that you are filtering. Choose TCP and click Next.

The screenshot shows the 'IP Filter Wizard' window, specifically the 'IP Protocol Type' step. The title bar reads 'IP Filter Wizard'. Below the title bar, the step is labeled 'IP Protocol Type' with the instruction 'Select the IP protocol type. If this type is TCP or UDP, you will also specify the source and destination ports.' and a small icon of a document with a magnifying glass. The main area contains a 'Select a protocol type:' label followed by a dropdown menu currently showing 'TCP'. Below this, there is a small input field containing the number '6'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

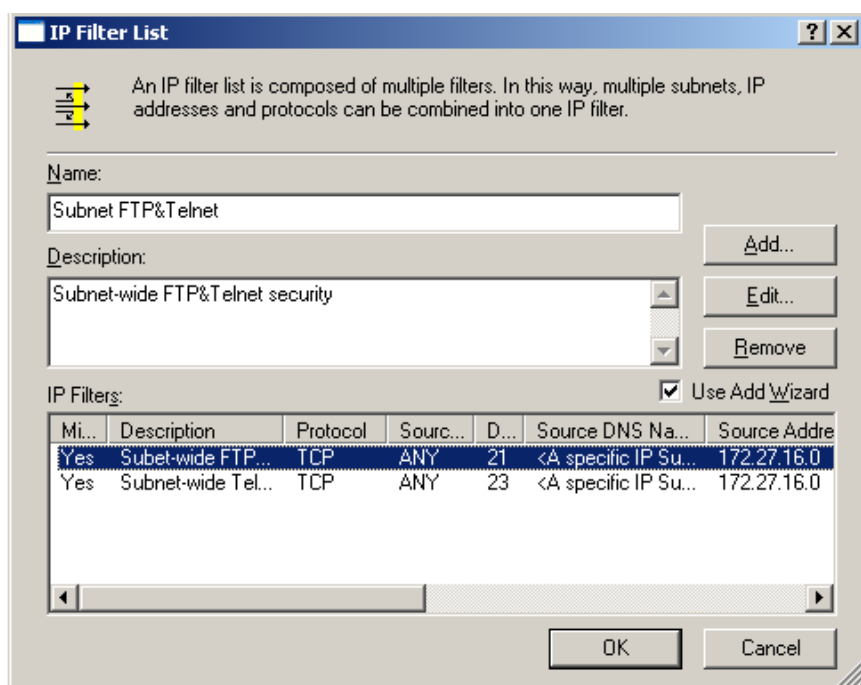
The next page allows you to define source and destination port numbers for your filter. In our case, we will be filtering ftp traffic, so leave the source port as "From any port" and set the destination port to be 21.



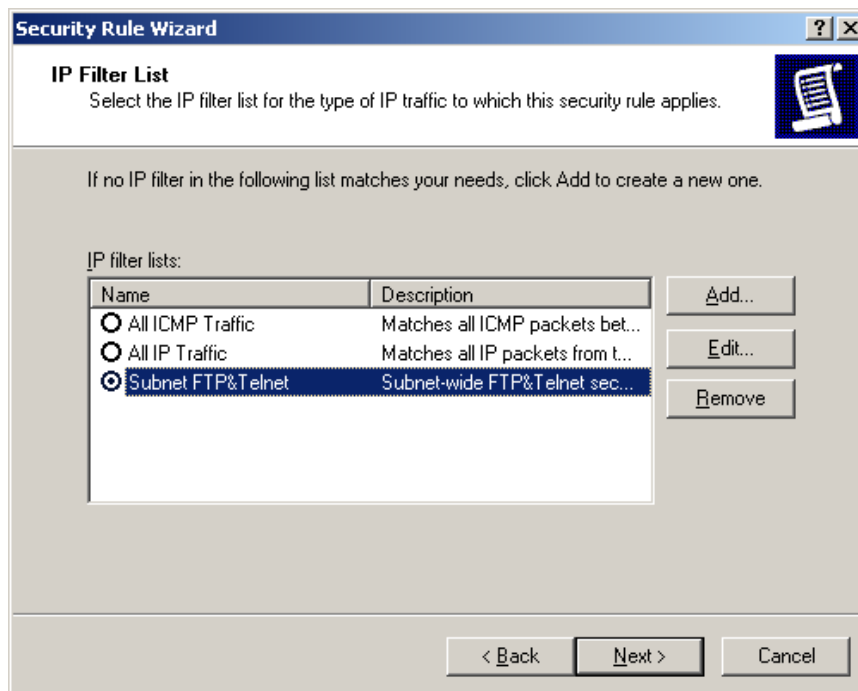
Click Next and then Finish to complete the Wizard and create the IP filter.

A second filter needs to be created to filter Telnet traffic on port 23. Click Add to create this filter using steps similar to those you have just used to create the ftp filter.

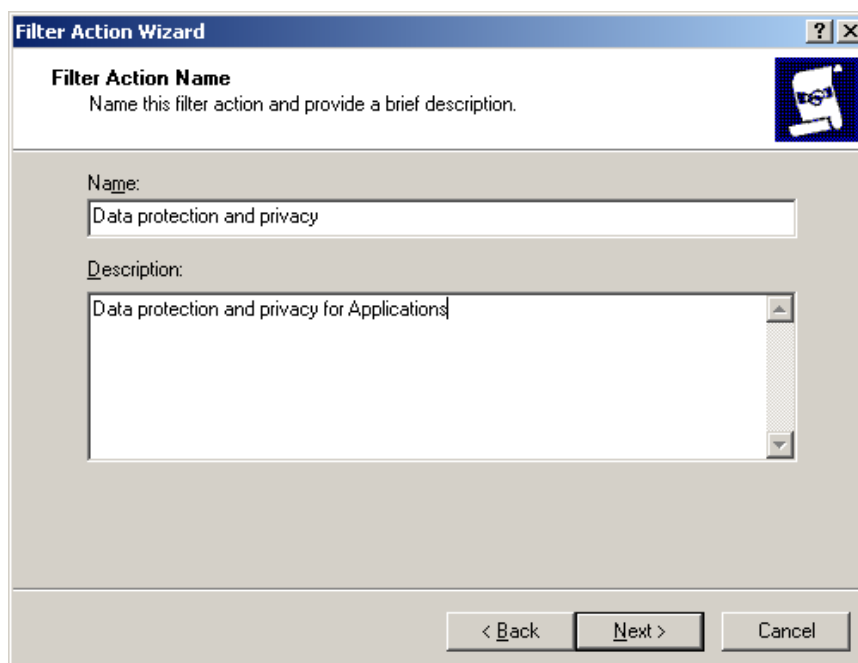
When you have created the second filter, the filter list will look like this:



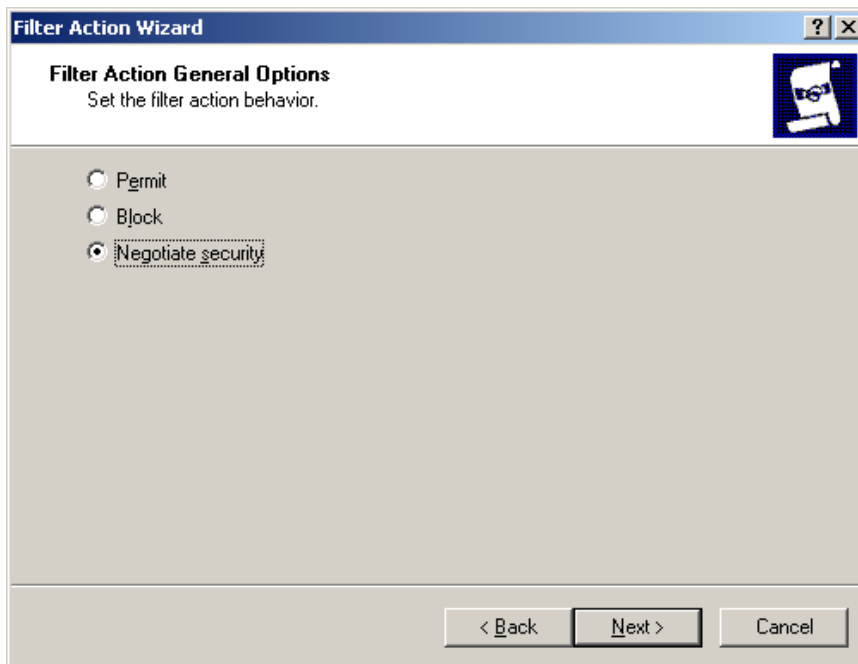
Click OK and you will be taken back to the Security Rule Wizard with the new filter list you have created highlighted but not selected. Click the radio button to the left of the filter list name to select it, and then click Next.



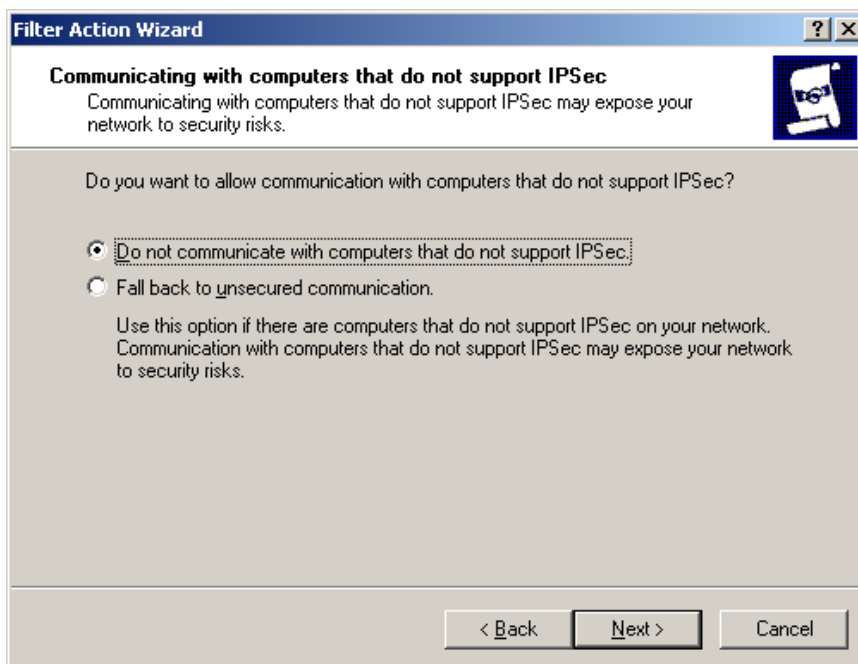
The next page allows you to create a filter action. Click Add to start the IP Security Filter Action Wizard and then click Next to skip past the Welcome screen. Enter a name and description for the filter action as shown below, then click Next to continue.



On the General Options page accept the default value, negotiate security by clicking Next.

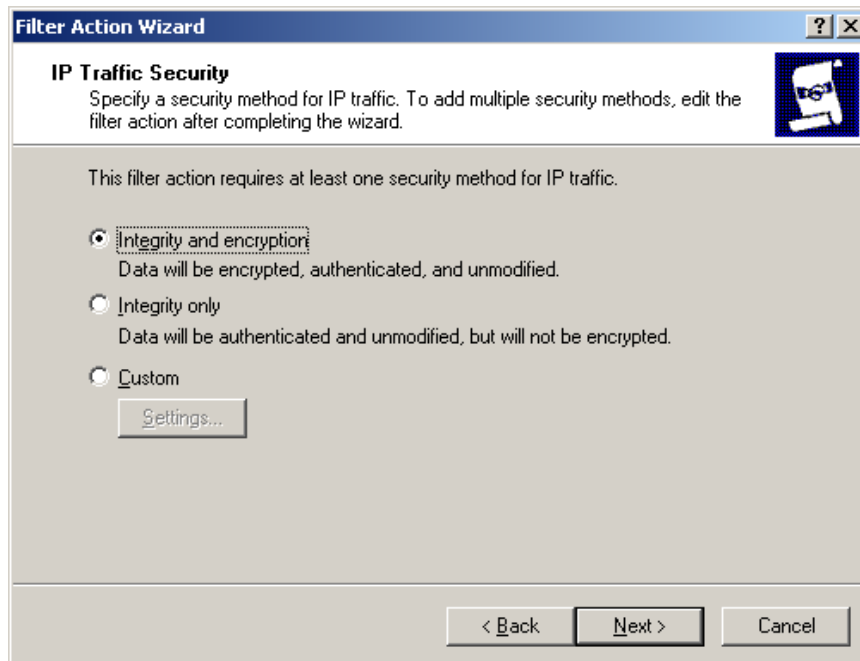


On the next page you define how to communicate with computers matched by this filter list that do not support IPsec. The default means that IPsec is required for all communications, the other option (fall back) means that an IPsec connection will be attempted, but unsecured communication will be allowed if the two sides cannot agree. For this example we will choose the default. Click Next.

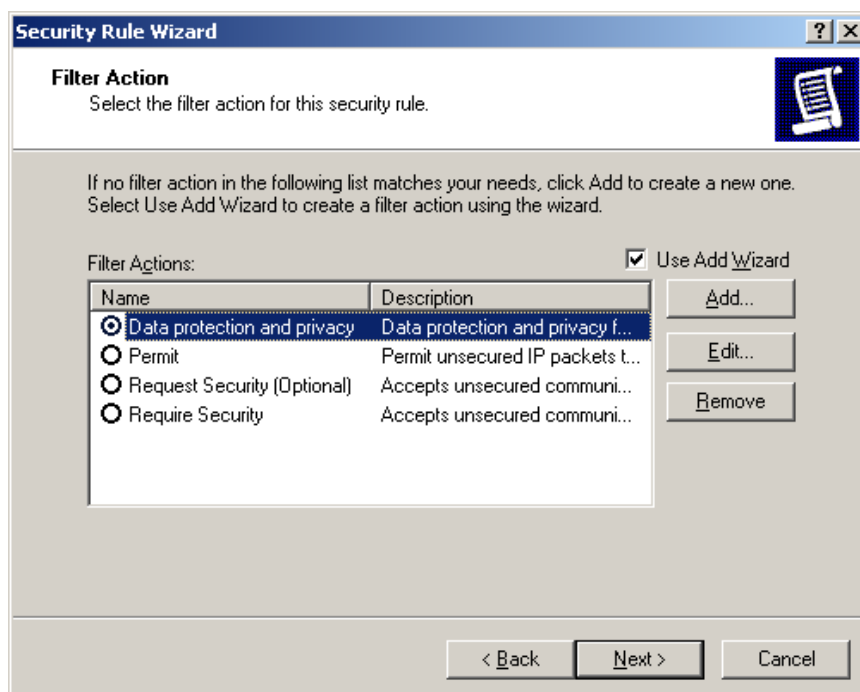


.....

The next page defines the level of security that IPsec should apply to the traffic allowed by this filter. The first option adds packet signing and encryption, the second only adds packet signing. A third option allows multiple security methods to be assigned. Click Next to accept the default.

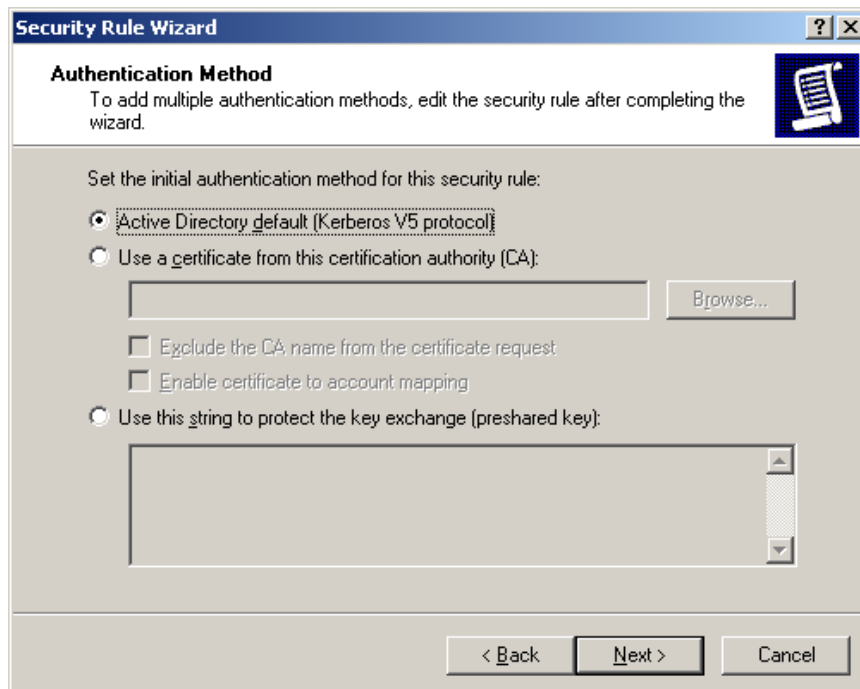


This completes the IP Security Filter Action Wizard; click Finish to create the filter action and return to the Security Rule Wizard. As before, the filter action will be highlighted but not selected. Click the radio button to select and then click Next.



.....

The next page defines the authentication method and we use the default method (Kerberos). Click Next to accept the default and complete the Wizard.



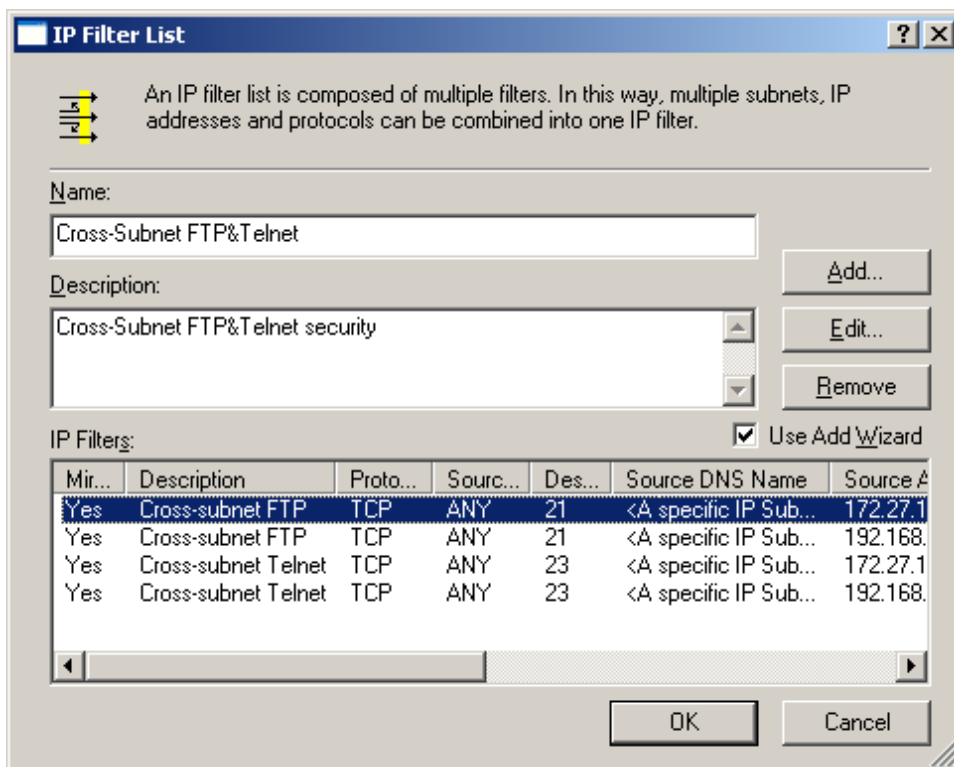
Click Finish to apply the filter list and return to the policy property page.

From here you can create a second rule for the optional part of this evaluation or continue on to activate the policy. To create the second rule, continue to the next section. To activate your policy, go to [Completing the policy definition](#).

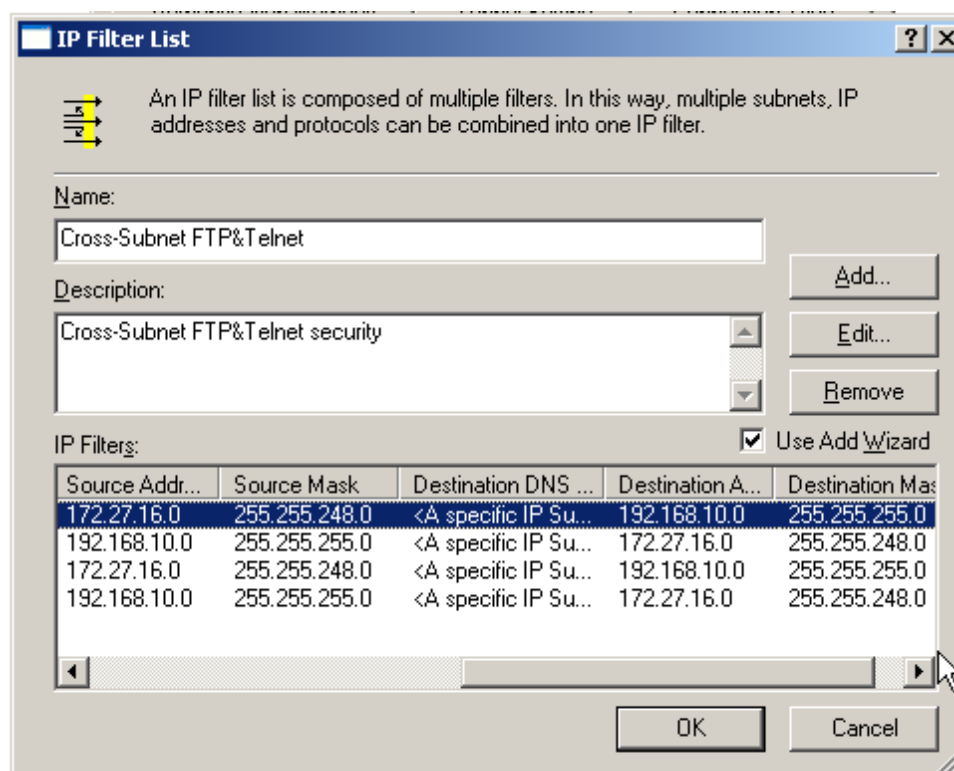
## Creating and Configuring Rule2 (OPTIONAL)

For Rule2 there are four IP filters to define the cross-subnet behavior. Refer to the IP filter summary table at the beginning of Section 4. Other than the filters, the configuration is the same as for Rule1.

Follow the steps in [Creating Rule1](#) to create this second rule. When you have finished creating this rule, your IP filter list should look like this.

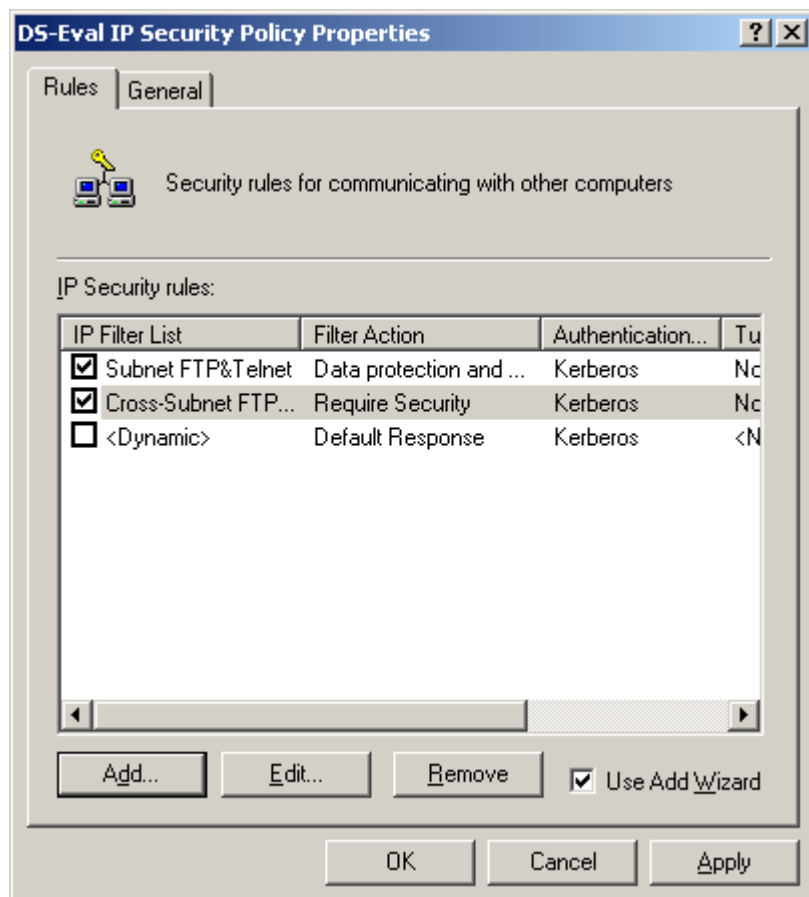


Here is another of the same list, with the filter list scrolled to show IP addresses.

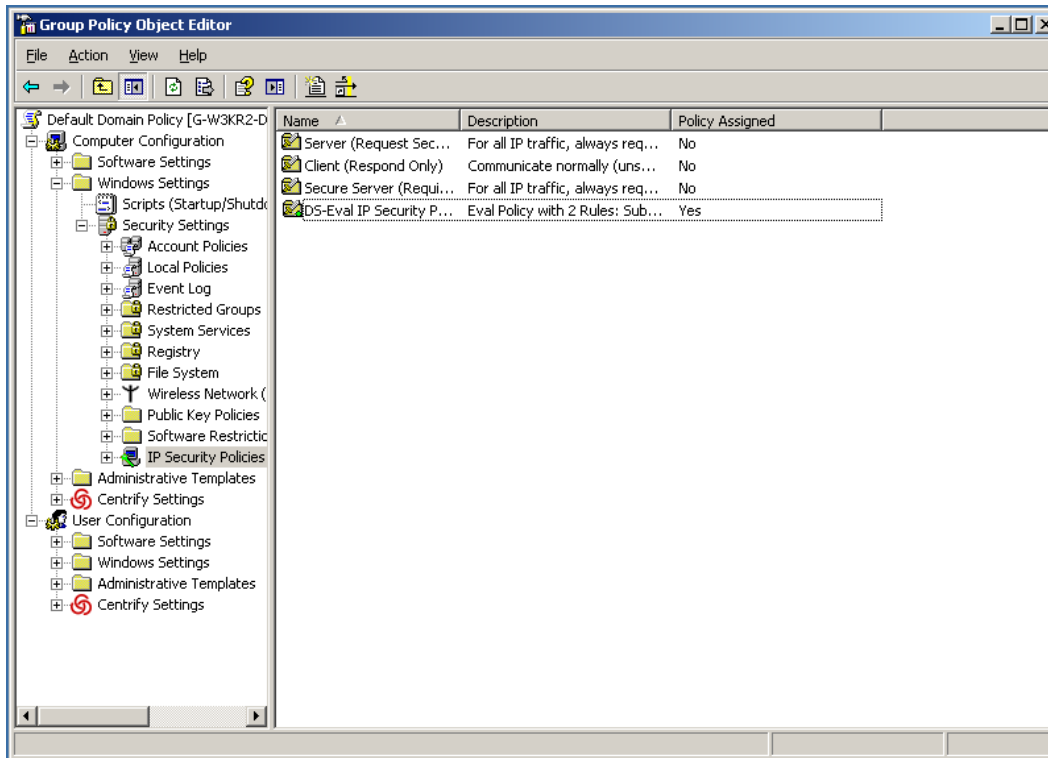


## Completing the policy definition

From the policy property page click OK to save the definition and return to the domain security settings tool.



Right click on the new policy and click Assign.



Now you're ready to move on to test the policy we've defined.

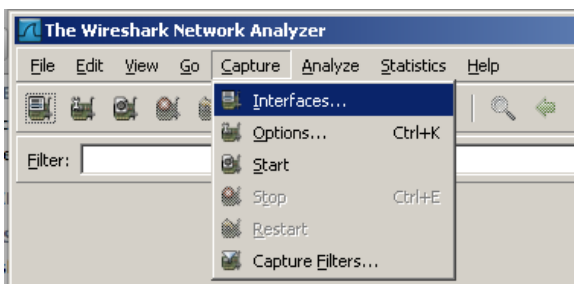
# Useful tools to use with isolation and encryption service

This chapter contains information for some useful tools: WireShark, Windows IP security policy monitor, and the Microsoft IP security diagnostic tool.

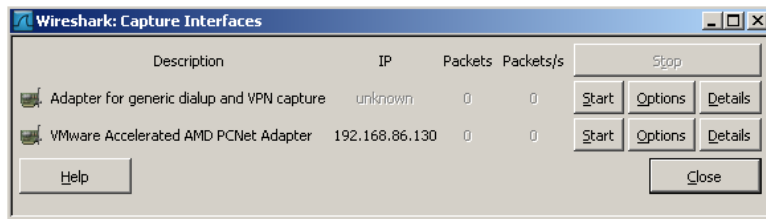
## WireShark

Download WireShark from <http://www.wireshark.org/> and install it. The current stable release of WireShark is 2.4.0. Install WireShark on your **domain controller** with these recommended options:

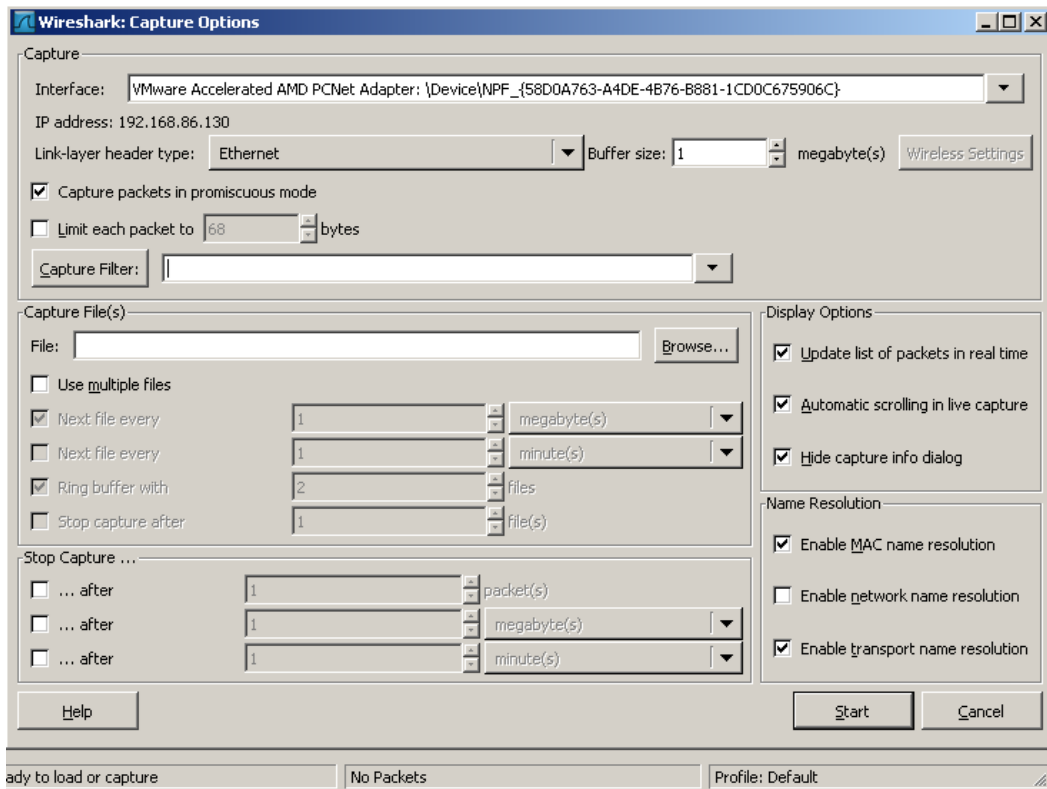
- Install desktop icon
- Start WinPcap service at startup
- Start WireShark and set the interface.



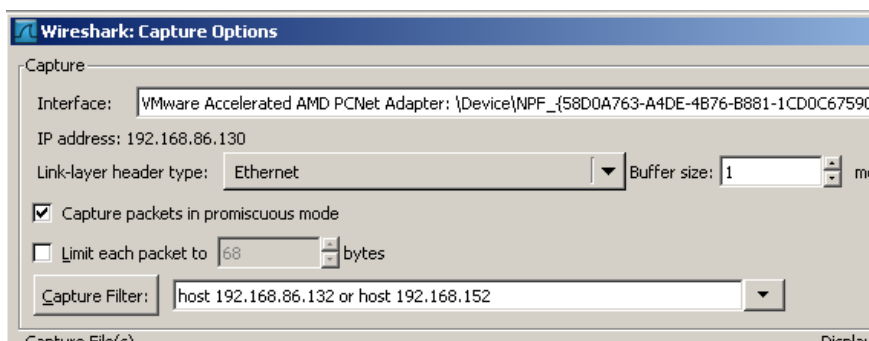
Assuming you are using VMware for these examples, choose the VMware network adapter, and click options.



This brings up the Capture options dialog:



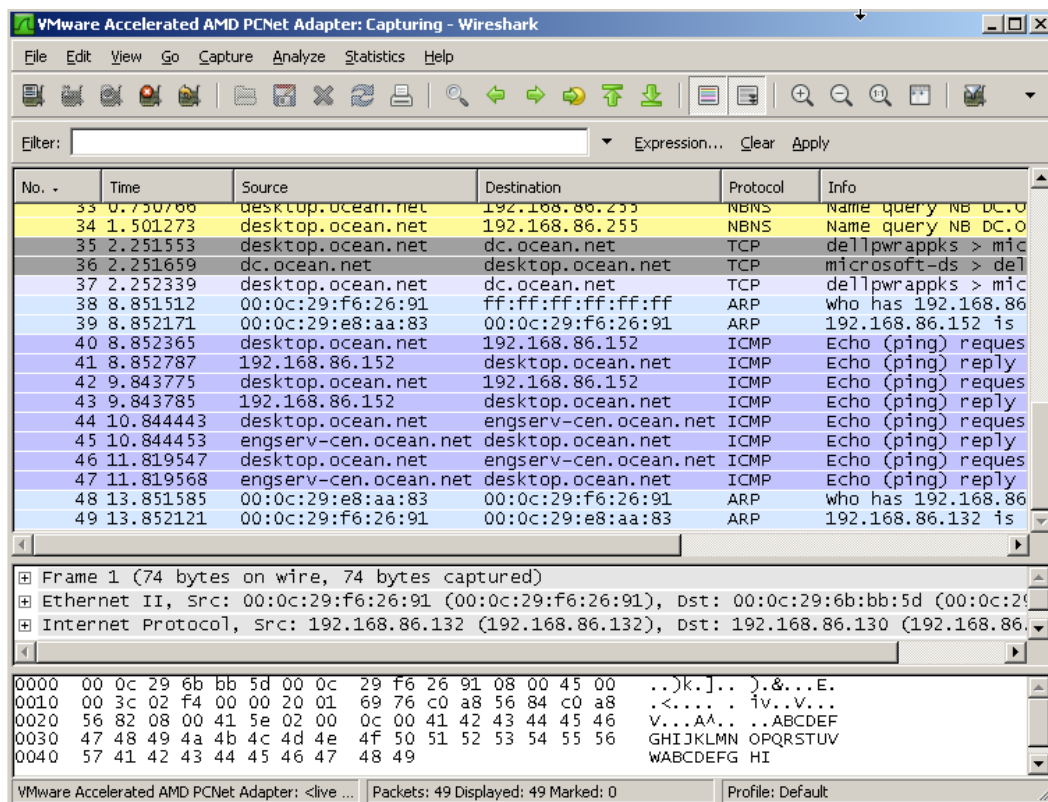
In the capture window type in the IP addresses for the capture filter:



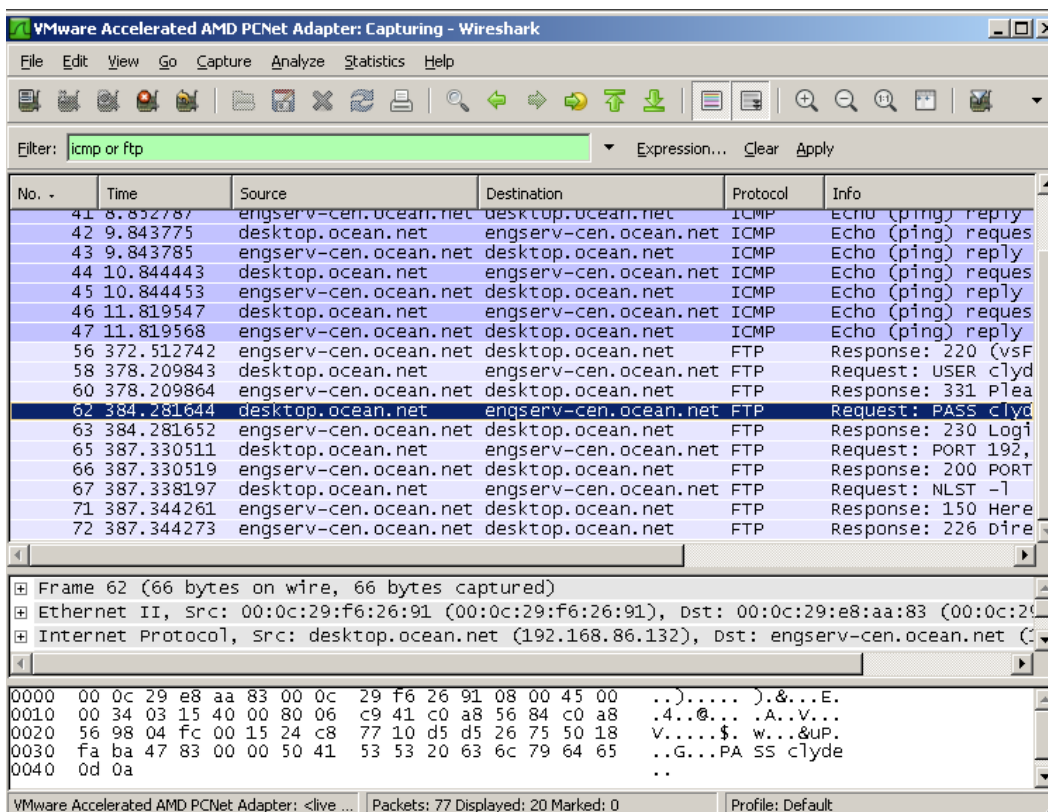
Check enable name resolution check box



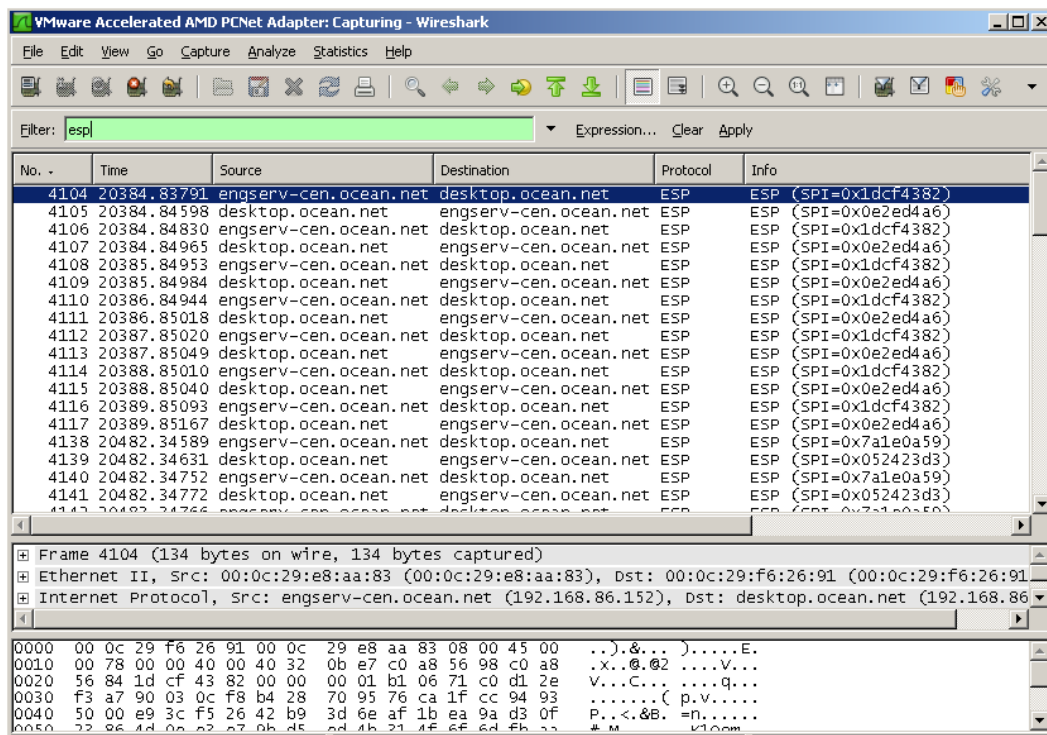
The configuration is now complete. Test the configuration by pinging one box.



Filter the output by protocol by typing “icmp” for Ping and “ftp” for FTP protocol.



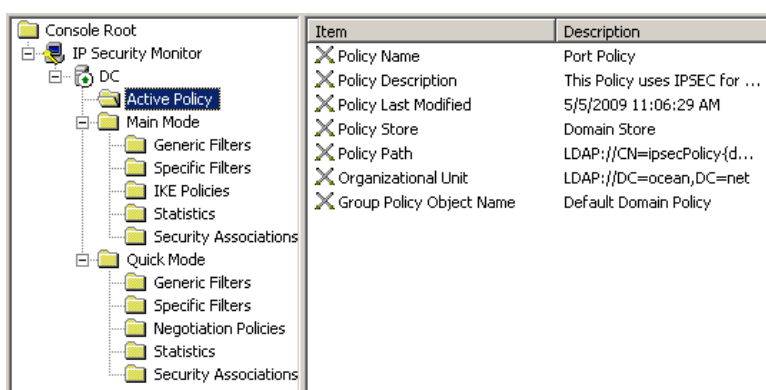
After you assign your policy all packets will be ESP (encrypted and signed)



## Windows IP Security Monitor

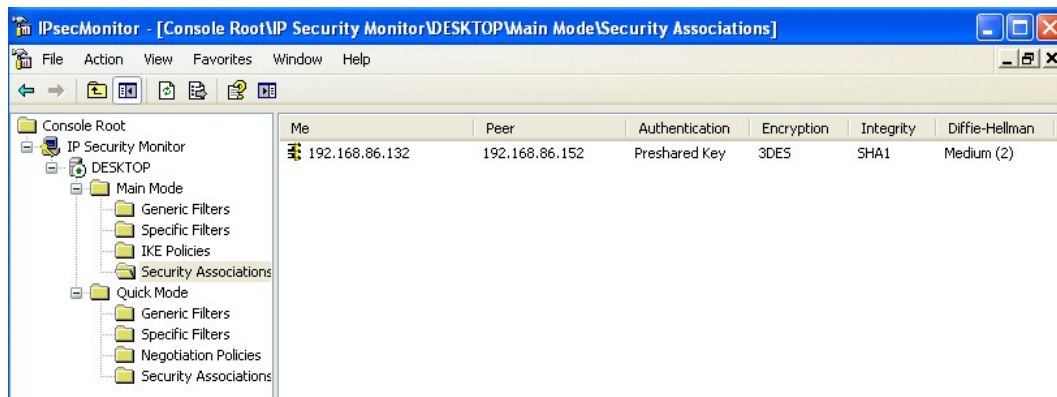
On the Windows machine that is being used for these examples, start the MMC console and add the IP Security Monitor snap-in.

The Policy Monitor displays different information depending on the release of Windows. Main Mode is IKE phase 1 negotiation and Quick Mode is phase 2. This screen shot shows the IPsec console on a Windows 2003 server.

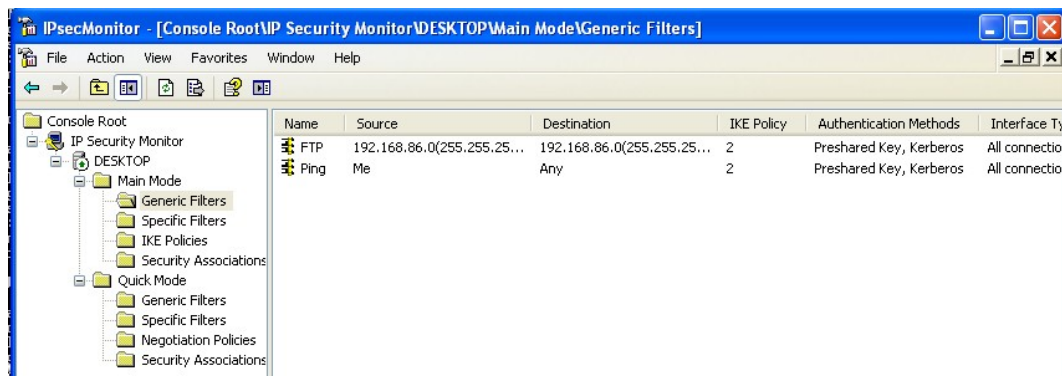


The following screenshots show the IPsec negotiations, policies, and security associations when pinging and ftp-ing from one machine to another.

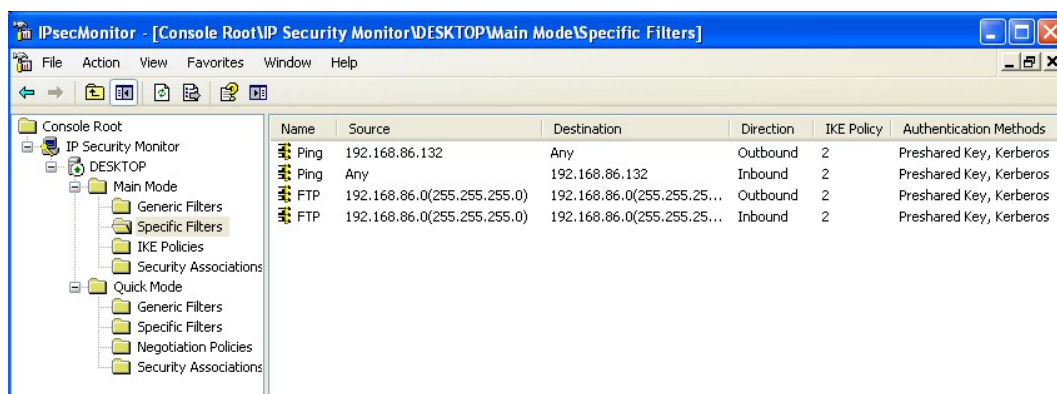
The IPsec monitor is running on the Windows desktop. Notice there is no Active Policy node. This shows the IKE SA for phase 1 of IPsec.



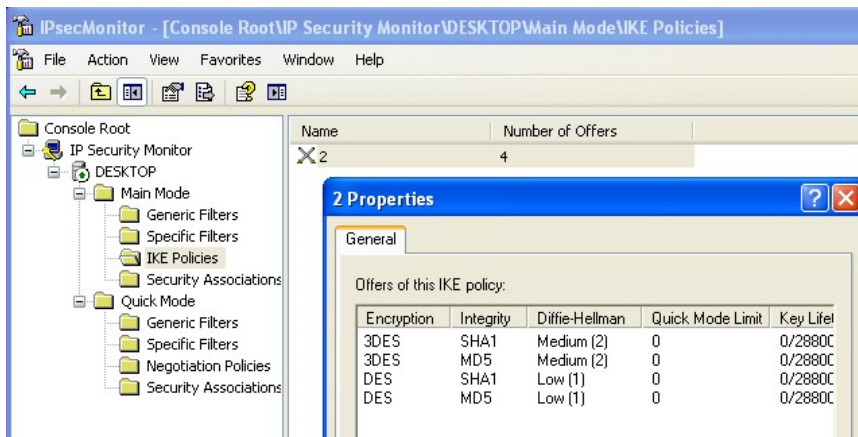
This shows the Generic filters that were defined and are active, I did not do telnet or http.



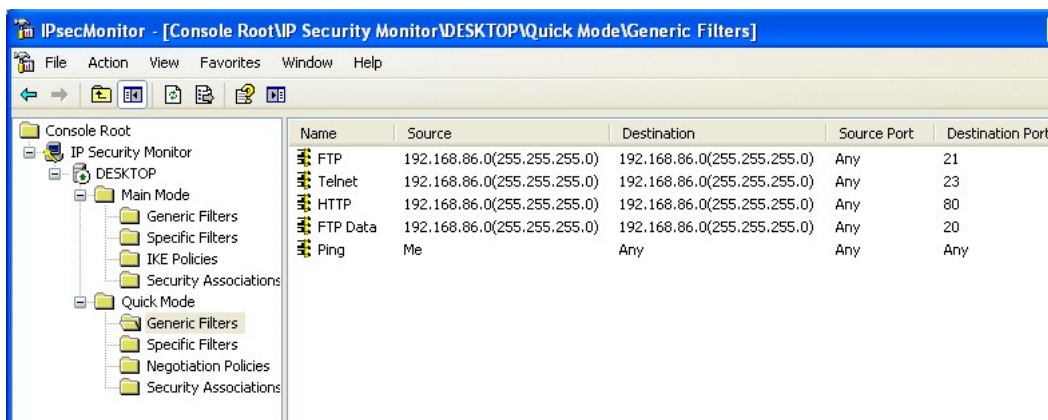
This shows the specific filters that are currently active for phase 1



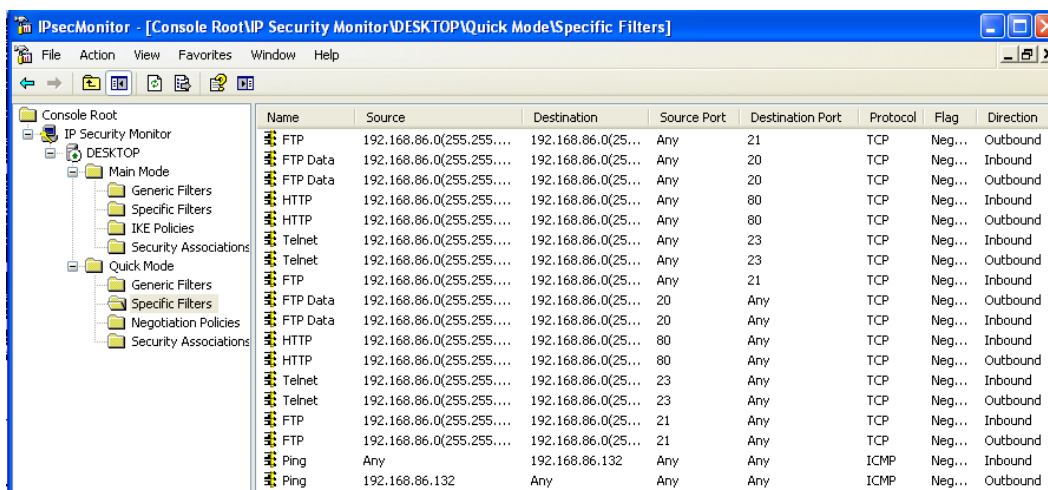
The IKE policy encryption and signing methods (there are 4 defined):



This shows all of the filter lists and how they are defined:

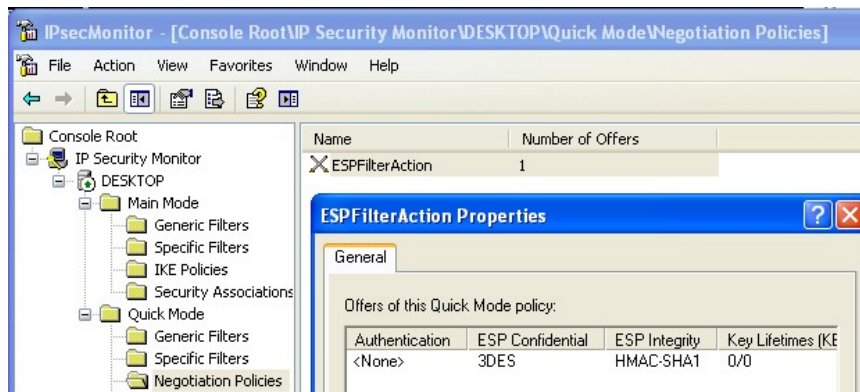


This shows the specific filters that are available from the filter lists defined for IPsec phase 2:

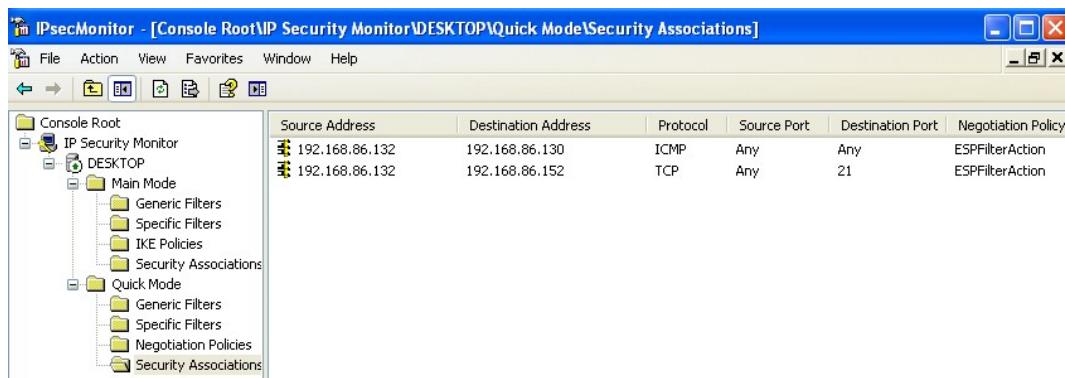


Looking at Negotiation Policies, only one action, ESPFilterAction is available. Only 3DES and SHA1 can be used. If a machine in another domain does not have a policy that matches this filter, the session will fail. It may be possible for

phase 1 to work, but phase 2 will not work unless there is a corresponding filter action in the other domain.



Clicking Security Associations shows the SAs used for phase 2:



## Microsoft IPsec Diagnostic tool

Microsoft's IPsec Diagnostic Tool is used for troubleshooting IPsec on Windows computers. It can be downloaded from Microsoft here:

<https://support.microsoft.com/en-us/help/943862/the-microsoft-ipsec-diagnostic-tool-is-available-for-windows-server-20>