

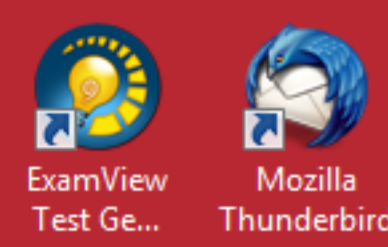
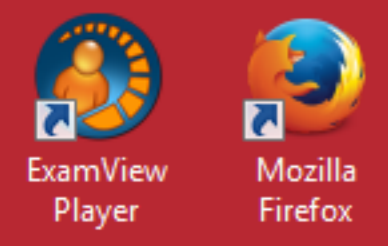
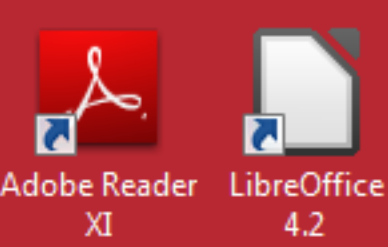
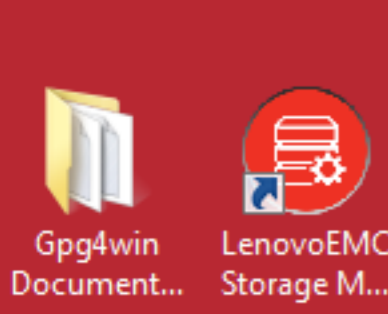
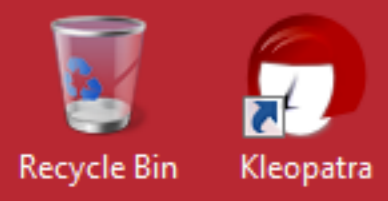
Windows simple IPsec setup

The presentation uses the IPsec Policies to configure a simple IPsec network. One system is a Windows 7 system. The other system is Windows 8.0 system. Both machines are on a IPv4 NAT network.

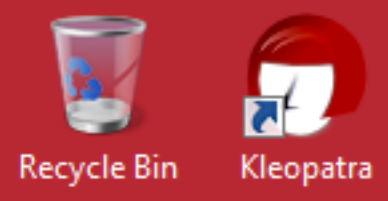
The primary reference is <http://technet.microsoft.com/en-us/library/cc730656%28v=ws.10%29.aspx>

Preuss

5/6/2014



The presentation logs on to Windows 7 as an administrator.



Accessories

- Calculator
- Command Prompt
- Connect to a Network
- Connect to a Project
- Getting Started
- Math Input Panel
- Notepad
- Paint
- Remote Desktop Connection
- Run
- Snipping Tool
- Sound Recorder
- Sticky Notes
- Sync Center
- Windows Explorer
- WordPad
- Ease of Access
- System Tools
- Tablet PC

Back

Search programs and files

Open

- Run as administrator
- Open file location
- 7-Zip
- Scan with Microsoft Security Essentials...
- Sign and encrypt
- More GpgEX options
- Pin to Taskbar
- Pin to Start Menu
- Restore previous versions
- Send to
- Cut
- Copy
- Paste
- Delete
- Rename
- Properties

The presentation starts the command prompt in administrator mode.



Administrator: Command Prompt

```
Microsoft Windows [Version 6.1.7601]  
Copyright (c) 2009 Microsoft Corporation. All rights reserved.  
C:\Windows\system32>mmc_
```

The presentation starts the mmc on the command line.



Console1 - [Console Root]

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 compmgmt.msc
- 2 eventvwr.msc
- 3 WF.msc
- 4 secpol.msc
- Exit

There are no items to show in this view.

Actions

- Console Root
- More Actions

Open this snap-in console.

The presentation selects Add/Remove Snap-in

Console1 - [Console Root]

File Action View Favorites Window Help

Console Root

Name

Actions

Console Root

More Actions

Add or Remove Snap-ins

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...
Group Policy Object ...	Microsoft Cor...
IP Security Monitor	Microsoft Cor...
IP Security Policy M...	Microsoft Cor...
Link to Web Address	Microsoft Cor...

Add >

Selected snap-ins:

- Console Root

Edit Extensions...

Remove

Move Up

Move Down

Advanced...

Cancel

Description:
The IP Security Monitor snap-in is used to monitor the s

The presentation adds the IP Security Monitor and the IP Security Policy.

Console1 - [Console Root]

File Action View Favorites Window Help

Console Root

Name

Actions

Console Root

More Actions

Add or Remove Snap-ins

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 full DNS name or IP address):
- Another computer:
 Browse...

< Back Finish Cancel OK Cancel

The IP Security Policy is run on the local computer.

Console1 - [Console Root]

File Action View Favorites Window Help

← → [Icons]

Console Root	
▶ IP Security Monitor	IP Security Monitor
▶ IP Security Policies on Local Computer	IP Security Policies on Local Computer

Actions

- Console Root ▲
- More Actions ▶

Console1 - [Console Root\IP Security Policies on Local Computer]

File Action View Favorites Window Help

[Icons]

Name	Description	Policy Assigned	Last Modified Time
------	-------------	-----------------	--------------------

Actions

- IP Security Policies o...
- More Actions

Create IP Security Policy...
Manage IP filter lists and filter actions...
All Tasks
View
New Window from Here
New Taskpad View...
Refresh
Export List...
Help

The presentation right clicks IP Security Policy and selects Create IP Security Policy.

IP Security Policy Wizard

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.

< Back **Next >** Cancel

Assigned	Last Modified Time	Actions
----------	--------------------	---------

in this view.

IP Security Policies o... ▲
More Actions ▶

IP Security Policy Wizard

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

Name:
Windows 7 IPsec test 01

Description:
This really is not the first test of the IPsec policy, but it looks good in the presentation.

< Back Next > Cancel

The presentation creates a name and description for the policy.

Assigned	Last Modified Time	Actions
in this view.		
IP Security Policies o...		More Actions

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.

Note: The default response rule is supported only on computers that are running Windows 2003 and Windows XP.

Activate the default response rule (earlier versions of Windows only).

< Back Next > Cancel

Assigned	Last Modified Time	Actions
in this view.		IP Security Policies o... ▲
		More Actions ▶

The presentation selects 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.

< Back Finish Cancel

Assigned	Last Modified Time	Actions
in this view.		IP Security Policies o... ▲
		More Actions ▶

Console1 - [Console Root\IP Security Policies on Local Computer]

File Action View Favorites Window Help



- Console Root
- IP Security Monitor
- IP Security Policies on Local Computer

Name	Description	Policy Assigned	Last Modified Time
Windows 7 IPsec test 01	This really is not the first t...	No...	5/6/2014 4:39:00 PM

Actions
IP Security Policies o...
More Actions

Windows 7 IPsec test 01 Properties

Rules General

Security rules for communicating with other computers

IP Security rules:

IP Filter List	Filter Action	Authentication...	Tu
<input type="checkbox"/> <Dynamic>	Default response (ea...	Kerberos	<N

Add...

The presentation selects Add.

Console Root
IP Security Monitor
IP Security Policies on Local Computer

Name	Description	Policy Assigned	Last Modified Time
Windows 7 IPsec test	This really is not the first t...	No...	5/6/2014 4:39:00 PM

Actions
IP Security Policies o...
More Actions

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.

< Back **Next >** Cancel

Console1 - [Console Root\IP Security Policies on Local Computer]

File Action View Favorites Window Help

Console Root
IP Security Monitor
IP Security Policies on Local Computer

Name	Description	Policy Assigned	Last Modified Time
Windows 7 IPsec test	This really is not the first t	No	5/6/2014 4:39:00 PM

Windows 7 IPsec test Properties

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 network 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 are specified by the following IP addresses:
 - IPv4 tunnel endpoint:
 - IPv6 tunnel endpoint:

< Back OK Cancel

Actions
IP Security Policies on Local Computer
More Actions

The presentation is configuring transport mode.

Name	Description	Policy Assigned	Last Modified Time
Windows 7 IPsec test	This really is not the first t	No	5/6/2014 4:39:00 PM

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

Buttons: Back, Next, Cancel, OK, Cancel

The presentation will select the systems included in the IPsec party.

Name	Description	Policy Assigned	Last Modified Time
Windows 7 IPsec test	This really is not the first t	No	5/6/2014 4:39:00 PM

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
------	-------------

Buttons: Add... Edit... Remove

Navigation: < Back Next > Cancel

The presentation selects Add.

Console1 - [Console Root\IP Security Policies on Local Computer]

File Action View Favorites Window Help

Console Root

- IP Security Monitor
- IP Security Policies on Local Computer

Name	Description	Policy Assigned	Last Modified Time
Windows 7 IPsec test	This really is not the first t	No	5/6/2014 4:39:00 PM

Windows 7 IPsec test Properties

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: NAT 01

Description: This is my computer NAT network.

IP Filters: Use Add Wizard

Mirrored	Description	Source DNS Name	Source Address
----------	-------------	-----------------	----------------

OK Cancel

Actions

- IP Security Policies on Local Computer
- More Actions

The presentation creates a name and description. Then presentation selects Add.

Console1 - [Console Root\IP Security Policies on Local Computer]

File Action View Favorites Window Help

Name	Description	Policy Assigned	Last Modified Time
Windows 7 IPsec test	This really is not the first t	No	5/6/2014 4:39:00 PM

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.

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

To continue, click Next.

< Back Next > Cancel

Console1 - [Console Root\IP Security Policies on Local Computer]

File Action View Favorites Window Help



- Console Root
- IP Security Monitor
- IP Security Policies on Local Computer

Name	Description	Policy Assigned	Last Modified Time
Windows 7 IPsec test	This really is not the first t	No	5/6/2014 4:39:00 PM

- Actions
- IP Security Policies o...
 - More Actions

Windows 7 IPsec test Properties

IP Filter List

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:
This will setup IPsec between two IPv4 hosts.

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

< Back

The presentation creates a description.

Console1 - [Console Root]IP Security Policies on Local Computer

File Action View Favorites Window Help

Name	Description	Policy Assigned	Last Modified Time
Windows 7 IPsec test	This really is not the first t	No	5/6/2014 4:39:00 PM
Windows 7 IPsec test 01 Properties			

IP Filter Wizard

IP Traffic Source
Specify the source address of the IP traffic.

Source address:
A specific IP Address or Subnet

IP Address or Subnet: 192.168.5.132

< Back Next >

The presentation selects a specific source address. In this example, the source IP address is this computer.

Console1 - [Console Root\IP Security Policies on Local Computer]

File Action View Favorites Window Help

Name	Description	Policy Assigned	Last Modified Time
Windows 7 IPsec test	This really is not the first t	No	5/6/2014 4:39:00 PM
Windows 7 IPsec test 01 Properties			

IP Filter Wizard

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

Destination address:
A specific IP Address or Subnet

IP Address or Subnet: 192.168.4.134

< Back Next >

The presentation selects a specific destination address. In this example, the destination IP address is the Windows 8 or other computer.

Note: Later diagnostics found this IP address to be incorrect. It was changed.

Console1 - [Console Root\IP Security Policies on Local Computer]

File Action View Favorites Window Help



- Console Root
 - IP Security Monitor
 - IP Security Policies on Local Computer

Name	Description	Policy Assigned	Last Modified Time
Windows 7 IPsec test	This really is not the first t	No	5/6/2014 4:39:00 PM

Actions

IP Security Policies o...

More Actions

IP 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:

Any

0



The presentation selected Any protocol. This made the wireshark captures much easier.

Console1 - [Console Root\IP Security Policies on Local Computer]

File Action View Favorites Window Help

Console Root

- IP Security Monitor
- IP Security Policies on Local Computer

Name	Description	Policy Assigned	Last Modified Time
Windows 7 IPsec test	This really is not the first t...	No...	5/6/2014 4:39:00 PM

Windows 7 IPsec test Properties

IP Filter List

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.

< Back Finish Cancel

Console1 - [Console Root\IP Security Policies on Local Computer]

File Action View Favorites Window Help



- Console Root
- IP Security Monitor
- IP Security Policies on Local Computer

Name	Description	Policy Assigned	Last Modified Time
Windows 7 IPsec test	This really is not the first t...	No...	5/6/2014 4:39:00 PM

- Actions**
- IP Security Policies on Local Computer
 - More Actions

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: NAT 01

Description: This is my computer NAT network.

IP Filters: Use Add Wizard

Mirrored	Description	Source DNS Name	Source Address
Yes	This will setup IPs...	<A specific IP Add...	192.168.5.132

OK Cancel

The presentation selects OK.

Console1 - [Console Root\IP Security Policies on Local Computer]

File Action View Favorites Window Help

Console Root

- IP Security Monitor
- IP Security Policies on Local Computer

Name	Description	Policy Assigned	Last Modified Time
Windows 7 IPsec test	This really is not the first t...	No...	5/6/2014 4:39:00 PM

Windows 7 IPsec test 01 Properties

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
<input checked="" type="radio"/> NAT 01	This is my computer NAT net...

Buttons: Add..., Edit..., Remove, < Back, Next >, Cancel

Buttons: OK, Cancel

The presentation selects NAT01.
Then the presentation selects next.

Console1 - [Console Root\IP Security Policies on Local Computer]

File Action View Favorites Window Help

Console Root

- IP Security Monitor
- IP Security Policies on Local Computer

Name	Description	Policy Assigned	Last Modified Time
Windows 7 IPsec test	This really is not the first t	No	5/6/2014 4:39:00 PM

Windows 7 IPsec test Properties

Security Rule Wizard

Filter Action
Select the filter action for this security rule.

If no filter action 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
------	-------------

Add...

Cancel

The presentation selects Add.

Console1 - [Console Root\IP Security Policies on Local Computer]

File Action View Favorites Window Help

Name	Description	Policy Assigned	Last Modified Time
Windows 7 IPsec test	This really is not the first t	No	5/6/2014 4:39:00 PM

Filter Action Wizard

Welcome to the IP Security Filter Action Wizard

Use this wizard to specify properties for a new filter action.

A filter action sets the security requirements for a data transfer. These requirements are specified in a list of security methods contained in the filter action.

Data transfer is only possible when the computers involved use the same security methods. Multiple security methods increase the chance that two computers will use the same method.

To continue, click Next.

< Back Next > Cancel

Console1 - [Console Root\IP Security Policies on Local Computer]

File Action View Favorites Window Help

Name	Description	Policy Assigned	Last Modified Time
Windows 7 IPsec test	This really is not the first t	No	5/6/2014 4:39:00 PM

Windows 7 IPsec test 01 Properties

Security Rule Wizard

Filter Action Wizard

Filter Action Name
Name this filter action and provide a brief description.

Name:
NAT Filter 01

Description:
This is the filter list for test 01.

< Back Next >

OK Cancel

The presentation creates a name and description for this filter.

Console1 - [Console Root\IP Security Policies on Local Computer]

File Action View Favorites Window Help



- Console Root
- IP Security Monitor
- IP Security Policies on Local Computer

Name	Description	Policy Assigned	Last Modified Time
Windows 7 IPsec test	This really is not the first t...	No...	5/6/2014 4:39:00 PM

- Actions
- IP Security Policies o...
 - More Actions

Windows 7 IPsec test 01 Properties

Security Rule Wizard

Filter Action Wizard

Filter Action General Options
Set the filter action behavior.

- Permit
- Block
- Negotiate security

OK Cancel

The presentation selects Negotiate security, then select next.

Console1 - [Console Root\IP Security Policies on Local Computer]

File Action View Favorites Window Help



- Console Root
- IP Security Monitor
- IP Security Policies on Local Computer

Name	Description	Policy Assigned	Last Modified Time
Windows 7 IPsec test	This really is not the first t	No	5/6/2014 4:39:00 PM

- Actions
- IP Security Policies o...
 - More Actions

Windows 7 IPsec test 01 Properties

Security Rule Wizard

Filter Action Wizard

Communicating with computers that do not support IPsec
Communicating with computers that do not support IPsec may expose your network to security risks.

Do you want to allow communication with computers that do not support IPsec?

- Do not allow unsecured communication.
- Allow unsecured communication if a secure connection is established.

Use this option if there are computers on your network that have an incompatible IPsec configuration. Allowing unsecured communication may expose your network to security risks.

On a computer with Windows Vista or a later version of Windows, unsecured communication to be sent anytime a secure connection is established.

On a Windows 2000, Windows XP, or Windows 2003 computer, unsecured communications to be sent only when the recipient computer supports IPsec.

< Back

OK Cancel

The presentation selects Do not allow unsecured communication. The presentation selects next.

Console1 - [Console Root\IP Security Policies on Local Computer]

File Action View Favorites Window Help

Name	Description	Policy Assigned	Last Modified Time
Windows 7 IPsec test	This really is not the first t	No	5/6/2014 4:39:00 PM

Windows 7 IPsec test Properties

Security Rule Wizard

Filter Action Wizard

IP Traffic Security
Specify a security method for IP traffic. To add multiple security methods, edit the filter action after completing the wizard.

This filter action requires at least one security method for IP traffic.

- Integrity and encryption
Data will be encrypted, authenticated
- Integrity only
Data will be authenticated and unmod
- Custom

Settings...

OK Cancel

The presentation selects Integrity and encryption.

Console1 - [Console Root\IP Security Policies on Local Computer]

File Action View Favorites Window Help

Console Root
IP Security Monitor
IP Security Policies on Local Computer

Name	Description	Policy Assigned	Last Modified Time
Windows 7 IPsec test	This really is not the first t...	No...	5/6/2014 4:39:00 PM

Windows 7 IPsec test Properties
Security Rule Wizard

Filter Action Wizard

Completing the IP Security Filter Action Wizard

You have successfully completed the IP Security Filter Action Wizard.

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

Edit properties

To close this wizard, click Finish.

< Back Finish Cancel

OK Cancel

- Console Root
- IP Security Monitor
- IP Security Policies on Local Computer

Name	Description	Policy Assigned	Last Modified Time
Windows 7 IPsec test	This really is not the first t	No	5/6/2014 4:39:00 PM

- Actions
- IP Security Policies on Local Computer
 - More Actions

Security Rule Wizard

Filter Action
Select the filter action for this security rule.

If no filter action 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
<input checked="" type="radio"/> NAT Filter 01	This is the filter list for tes

< Back Next >

OK Cancel

The presentation selects NAT Filter 01, then selects next.

- Console Root
- IP Security Monitor
- IP Security Policies on Local Computer

Name	Description	Policy Assigned	Last Modified Time
Windows 7 IPsec test	This really is not the first t...	No...	5/6/2014 4:39:00 PM

- Actions
- IP Security Policies on Local Computer
 - More Actions

Security Rule Wizard

Authentication Method
To add multiple authentication methods, edit the security rule after completing the wizard.

Set the initial authentication method for this security rule:

- Active Directory default (Kerberos V5 protocol)
- Use a certificate from this certification authority (CA):
- Exclude the CA name from the certificate request
- Enable certificate to account mapping
- Use this string to protect the key exchange (preshared key):

< Back

OK Cancel

The presentation selects a very weak shared secret. Then the presentation selects next.

Console1 - [Console Root\IP Security Policies on Local Computer]

File Action View Favorites Window Help

Console Root
IP Security Monitor
IP Security Policies on Local Computer

Name	Description	Policy Assigned	Last Modified Time
Windows 7 IPsec test	This really is not the first t	No	5/6/2014 4:39:00 PM

Windows 7 IPsec test Properties

Security Rule Wizard

Completing the Security 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.

< Back Finish Cancel

- Console Root
 - IP Security Monitor
 - IP Security Policies on Local Computer

Name	Description	Policy Assigned	Last Modified Time
Windows 7 IPsec test 01	This really is not the first t...	No...	5/6/2014 4:39:00 PM

- Actions**
- IP Security Policies on Local Computer
 - More Actions

Windows 7 IPsec test 01 Properties

Rules | General

Security rules for communicating with other computers

IP Security rules:

IP Filter List	Filter Action	Authentication...	Tu
<input checked="" type="checkbox"/> NAT 01	NAT Filter 01	Preshared Key	No
<input type="checkbox"/> <Dynamic>	Default response (ea...	Kerberos	<N

Use Add Wizard

Console1 - [Console Root\IP Security Policies on Local Computer]

File Action View Favorites Window Help

Name	Description	Policy Assigned	Last Modified Time
Windows 7	the first t...	No	5/6/2014 4:43:32 PM

Assign
All Tasks
Delete
Rename
Properties
Help

Actions
IP Security Policies o...
More Actions
Windows 7 IPsec tes...
More Actions

The presentation right clicks on the policy. The presentation selects Assign.

Console1 - [Console Root\IP Security Policies on Local Computer]

File Action View Favorites Window Help

Console Root

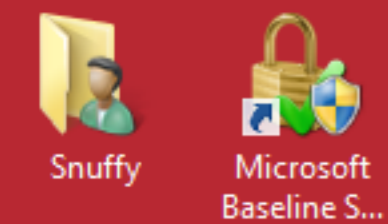
- IP Security Monitor
- IP Security Policies on Local Computer

Name	Description	Policy Assigned	Last Modified Time
Windows 7 IPsec tes...	This really is not the first t...	Yes	5/6/2014 4:43:32 PM

Actions

- IP Security Policies on Local Computer
- More Actions

The presentation's Windows 7 computer is ready.



Administrator: Command Prompt

```
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ver
Microsoft Windows [Version 6.2.9200]

C:\Windows\system32>mmc
```

The presentation logs on the Windows 8.0 computer as administrator. The command prompt is started as administration mode. The mmc is started at the command line.



Console1 - [Console Root]

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 compmgmt.msc
- 2 secpol.msc
- 3 eventvwr.msc
- 4 WF.msc
- Exit

There are no items to show in this view.

The presentation selects Add/Remove Snap-in

Actions

- Console Root
- More Actions

Quits the program and prompts to save documents.

Console1 - [Console Root]

File Action View Favorites Window Help

Console Root

Add or Remove Snap-ins

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:	Selected snap-ins:																												
<table border="1"><thead><tr><th>Snap-in</th><th>Vendor</th></tr></thead><tbody><tr><td>ActiveX Control</td><td>Microsoft Cor...</td></tr><tr><td>Authorization Manager</td><td>Microsoft Cor...</td></tr><tr><td>Certificates</td><td>Microsoft Cor...</td></tr><tr><td>Component Services</td><td>Microsoft Cor...</td></tr><tr><td>Computer Managem...</td><td>Microsoft Cor...</td></tr><tr><td>Device Manager</td><td>Microsoft Cor...</td></tr><tr><td>Disk Management</td><td>Microsoft and...</td></tr><tr><td>Event Viewer</td><td>Microsoft Cor...</td></tr><tr><td>Folder</td><td>Microsoft Cor...</td></tr><tr><td>Group Policy Object ...</td><td>Microsoft Cor...</td></tr><tr><td>IP Security Monitor</td><td>Microsoft Cor...</td></tr><tr><td>IP Security Policy M...</td><td>Microsoft Cor...</td></tr><tr><td>Link to Web Address</td><td>Microsoft Cor...</td></tr></tbody></table>	Snap-in	Vendor	ActiveX Control	Microsoft Cor...	Authorization Manager	Microsoft Cor...	Certificates	Microsoft Cor...	Component Services	Microsoft Cor...	Computer Managem...	Microsoft Cor...	Device Manager	Microsoft Cor...	Disk Management	Microsoft and...	Event Viewer	Microsoft Cor...	Folder	Microsoft Cor...	Group Policy Object ...	Microsoft Cor...	IP Security Monitor	Microsoft Cor...	IP Security Policy M...	Microsoft Cor...	Link to Web Address	Microsoft Cor...	<ul style="list-style-type: none">Console Root
Snap-in	Vendor																												
ActiveX Control	Microsoft Cor...																												
Authorization Manager	Microsoft Cor...																												
Certificates	Microsoft Cor...																												
Component Services	Microsoft Cor...																												
Computer Managem...	Microsoft Cor...																												
Device Manager	Microsoft Cor...																												
Disk Management	Microsoft and...																												
Event Viewer	Microsoft Cor...																												
Folder	Microsoft Cor...																												
Group Policy Object ...	Microsoft Cor...																												
IP Security Monitor	Microsoft Cor...																												
IP Security Policy M...	Microsoft Cor...																												
Link to Web Address	Microsoft Cor...																												

Actions

- Console Root
- More Actions

Buttons: Edit Extensions..., Remove, Move Up, Move Down, Advanced..., Cancel

The presentation adds the IP Security Monitor and the IP Security Policy.

Console1 - [Console Root]

File Action View Favorites Window Help



Console Root

Name

Actions

Add or Remove Snap-ins

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...
Group Policy Object ...	Microsoft Cor...
IP Security Monitor	Microsoft Cor...
IP Security Policy M...	Microsoft Cor...
Link to Web Address	Microsoft Cor...

Selected snap-ins:

- Console Root
- IP Security Monitor

Add >

Edit Extensions...

Remove

Move Up

Move Down

Advanced...

Description:

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

OK

Cancel

Console Root

More Actions



ENG

4:47 PM

5/6/2014

Console1 - [Console Root]

File Action View Favorites Window Help

Console Root

Name

Actions

Console Root

More Actions

Add or Remove Snap-ins

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 full DNS name or IP address)
- Another computer:
 Browse...

set of snap-ins. For

Edit Extensions...

her computers.

< Back Finish Cancel OK Cancel

The IP Security Policy is run on the local computer.



Console1 - [Console Root]

File Action View Favorites Window Help

Console Root

Add or Remove Snap-ins

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...
Group Policy Object ...	Microsoft Cor...
IP Security Monitor	Microsoft Cor...
IP Security Policy M...	Microsoft Cor...
Link to Web Address	Microsoft Cor...

Add >

Selected snap-ins:

- Console Root
- IP Security Monitor
- IP Security Policies on Local Cor...

Edit Extensions...
Remove
Move Up
Move Down
Advanced...

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

OK Cancel

Console1 - [Console Root\IP Security Policies on Local Computer]

File Action View Favorites Window Help



- Console Root
- IP Security Monitor
- IP Security Policies on Local Computer

Name	Description	Policy Assigned	Last Modified Time
------	-------------	-----------------	--------------------

Actions

- IP Security Polici...
- More Actions

- Create IP Security Policy...
- Manage IP filter lists and filter actions...
- All Tasks
- View
- New Window from Here
- New Taskpad View...
- Refresh
- Export List...
- Help

The presentation right clicks IP Security Policy and selects Create IP Security Policy.

IP Security Policy Wizard

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.

< Back

Next >

Cancel

Console1 - [Console Root] IP Security Policies on Local Computer

igned | Last Modified Time

w in this view.

Actions

IP Security Polici...

More Actions



ENG

4:48 PM
5/6/2014

IP Security Policy Wizard

IP Security Policy Name

Name this IP Security policy and provide a brief description

Name:

Windows 8 IPsec test01

Description:

This is Windows 8 IPsec test 01. It really is not the first test, but ...

< Back

Next >

Cancel

The presentation creates a name and description for the policy.

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.

Note: The default response rule is supported only on computers that are running Windows 2003 and Windows XP.

Activate the default response rule (earlier versions of Windows only).

< Back

Next >

The presentation selects next.

Console1 - [Console Root] IP Security Policies on Local Computer

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.

< Back Finish Cancel

igned	Last Modified Time	Actions
-------	--------------------	---------

w in this view.

IP Security Polici... ▲

More Actions ▶

Console1 - [Console Root\IP Security Policies on Local Computer]

File Action View Favorites Window Help



- Console Root
- IP Security Monitor
- IP Security Policies

Name	Description	Policy Assigned	Last Modified Time
Windows 8 IPsec test01			5/6/2014 4:49:38 PM

Actions
IP Security Polici...
More Actions

Windows 8 IPsec test01 Properties

Rules General

Security rules for communicating with other computers

IP Security rules:

IP Filter List	Filter Action	Authentication...	Tu
<input type="checkbox"/> <Dynamic>	Default response (ea...	Kerberos	<N

Add...

The presentation selects Add.

Console1 - [Console Root\IP Security Policies on Local Computer]

File Action View Favorites Window Help

Navigation icons: back, forward, refresh, search, print, etc.

Name	Description	Policy Assigned	Last Modified Time
Windows 8 IPsec test01	5/6/2014 4:49:38 PM

Actions: IP Security Polici... More Actions

Windows 8 IPsec test01 Properties

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.

< Back Next > Cancel

OK Cancel

Console1 - [Console Root\IP Security Policies on Local Computer]

File Action View Favorites Window Help



- Console Root
- IP Security Monitor
- IP Security Policies on Local Computer

Name	Description	Policy Assigned	Last Modified Time
Windows 8 IPsec test01	5/6/2014 4:40:38 PM

- Actions**
- IP Security Policies on Local Computer
 - More Actions

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 network 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 are specified by the following IP

IPv4 tunnel endpoint:

IPv6 tunnel endpoint:

< Back

OK Cancel

The presentation is configuring transport mode.

Console1 - [Console Root\IP Security Policies on Local Computer]

File Action View Favorites Window Help



- Console Root
- IP Security Monitor
- IP Security Policies

Name	Description	Policy Assigned	Last Modified Time
Windows 8 IPsec test			5/6/2014 4:40:38 PM

Actions
IP Security Polici...
More Actions

Windows 8 IPsec test Properties

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

OK Cancel

The presentation will select the systems included in the IPsec party.

Console1 - [Console Root\IP Security Policies on Local Computer]

File Action View Favorites Window Help



- Console Root
- IP Security Monitor
- IP Security Policies on Local Computer

Name	Description	Policy Assigned	Last Modified Time
Windows 8 IPsec test01	5/6/2014 4:40:38 PM

- Actions**
- IP Security Polici...
 - More Actions

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
------	-------------

Buttons: Add... Edit... Remove

Navigation: < Back Next > Cancel

Bottom: OK Cancel

The presentation selects Add.

Console1 - [Console Root\IP Security Policies on Local Computer]

File Action View Favorites Window Help



- Console Root
- IP Security Monitor
- IP Security Policies

Name	Description	Policy Assigned	Last Modified Time
Windows 8 IPsec test	This is the NAT 01 list.		5/6/2014 4:40:38 PM

Actions

- IP Security Polici...
- More Actions

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:

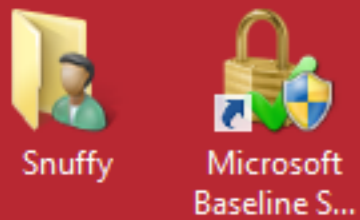
Description:

IP Filters: Use Add Wizard

Mimored	Description	Source DNS Name	Source Address
---------	-------------	-----------------	----------------

OK Cancel

The presentation creates a name and description. Then presentation selects Add.



Windows 8 IPsec test01 Properties

ID Filter List

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.

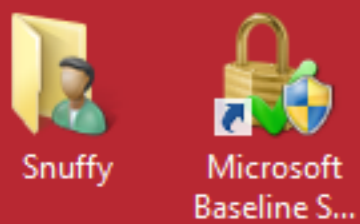
You can add multiple filters to build an IP filter list that matches on IP packets for multiple source or destination computers, or for many different traffic types.

To continue, click Next.

< Back Next > Cancel

```
Microsoft Windows [Version 6.0.6002.18005]
(c) 2012 Microsoft Corporation
C:\Windows\system32>ver
Microsoft Windows [Version 6.0.6002.18005]
C:\Windows\system32>mm
C:\Windows\system32>
```





```

Microsoft Windows [Ver
(c) 2012 Microsoft Cor
C:\Windows\system32>ve
Microsoft Windows [Ver
C:\Windows\system32>mm
C:\Windows\system32>

```

Windows 8 IPsec test01 Properties

ID Filter List

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:

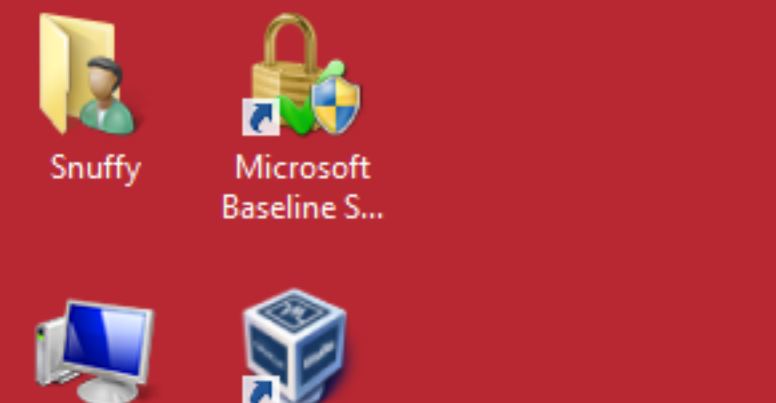
This lists the IP address used for IPsec in this example.

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

< Back

The presentation creates a description.





```
Microsoft Windows [Version 6.0.6002.1.12521.1]
(c) 2012 Microsoft Corporation
C:\Windows\system32>ver
Microsoft Windows [Version 6.0.6002.1.12521.1]
C:\Windows\system32>mm
C:\Windows\system32>
```

Windows 8 IPsec test01 Properties ? x

ID Filter List x

IP Filter Wizard

IP Traffic Source
Specify the source address of the IP traffic.

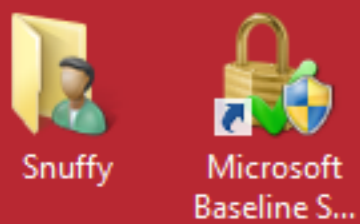
Source address:
A specific IP Address or Subnet

IP Address or Subnet: 192.168.5.134

< Back Next >

The presentation selects a specific source address. In this example, the source IP address is this computer.





```

Microsoft Windows [Ver
(c) 2012 Microsoft Cor
C:\Windows\system32>ve
Microsoft Windows [Ver
C:\Windows\system32>mm
C:\Windows\system32>

```

Windows 8 IPsec test01 Properties

ID Filter List

IP Filter Wizard

IP Traffic Destination

Specify the destination address of the IP traffic.

Destination address:

A specific IP Address or Subnet

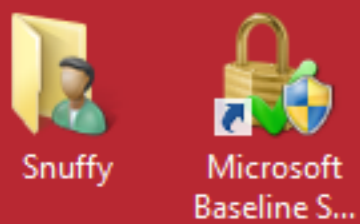
IP Address or Subnet: 192.168.5.132

< Back

Next >

The presentation selects a specific destination address. In this example, the destination IP address is the Windows 7 or other computer.





```
C:\Windows\system32>ve
Microsoft Windows [Ver
(c) 2012 Microsoft Cor
C:\Windows\system32>mm
C:\Windows\system32>
```

Windows 8 IDsec test01 Properties ? x

ID Filter List x

IP 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:

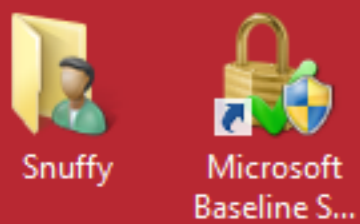
Any v

0 ^ v

< Back Next > Cancel

The presentation selected Any protocol. This made the wireshark captures much easier.





```
Microsoft Windows [Version 6.0.6002.18005]
(c) 2012 Microsoft Corporation
C:\Windows\system32>ver
Microsoft Windows [Version 6.0.6002.18005]
C:\Windows\system32>mm
C:\Windows\system32>
```

Windows 8 IPsec test01 Properties

ID Filter List

IP Filter Wizard

Completing the IP Filter Wizard

You have successfully completed the IP Filter Wizard.

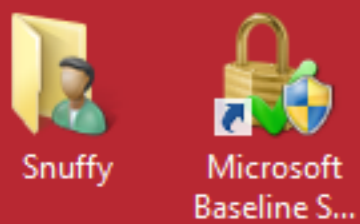
To edit your IP filter now, select the Edit properties check box, and then click Finish.

Edit properties

To close this wizard, click Finish.

< Back Finish Cancel





```

Microsoft Windows [Ver
(c) 2012 Microsoft Cor
C:\Windows\system32>ve
Microsoft Windows [Ver
C:\Windows\system32>mm
C:\Windows\system32>

```

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:

Description:

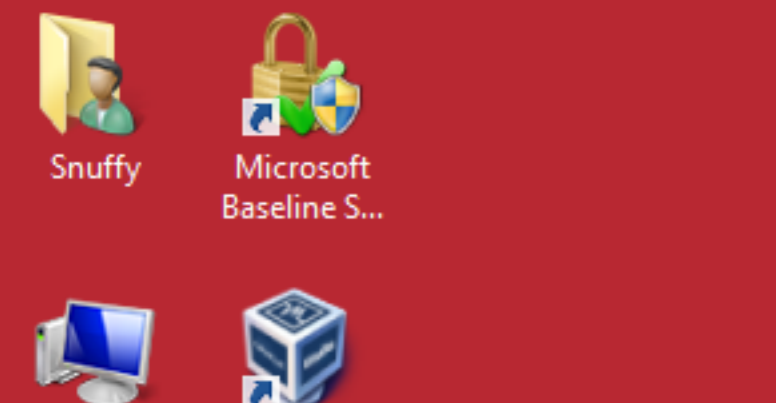
IP Filters: Use Add Wizard

Mimored	Description	Source DNS Name	Source Address
Yes	This lists the IP ad...	<A specific IP Add...	192.168.5.134

Buttons: Add..., Edit..., Remove, OK, Cancel

The presentation selects OK.





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
<input checked="" type="radio"/> Windows 8 NAT 01	This is the NAT 01 list.

Buttons: Add..., Edit..., Remove

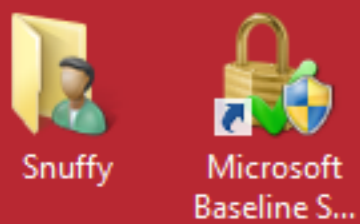
Navigation: < Back, Next >, Cancel

Bottom: OK, Cancel

```
Microsoft Windows [Ver...  
(c) 2012 Microsoft Cor...  
C:\Windows\system32>ve...  
Microsoft Windows [Ver...  
C:\Windows\system32>mm...  
C:\Windows\system32>
```

The presentation selects Windows 8 NAT01. Then the presentation selects next.





```

Microsoft Windows [Ver
(c) 2012 Microsoft Cor
C:\Windows\system32>ve
Microsoft Windows [Ver
C:\Windows\system32>mm
C:\Windows\system32>

```

Security Rule Wizard

Filter Action
Select the filter action for this security rule.

If no filter action 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.

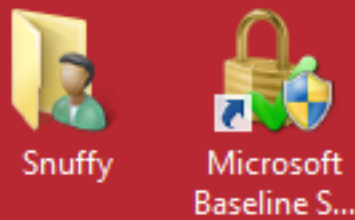
Filter Actions: Use Add Wizard

Name	Description	Add...

Buttons: Edit, Remove, Cancel

The presentation selects Add.





Windows 8 IPsec test01 Properties

Security Rule Wizard

Filter Action Wizard

Welcome to the IP Security Filter Action Wizard

Use this wizard to specify properties for a new filter action.

A filter action sets the security requirements for a data transfer. These requirements are specified in a list of security methods contained in the filter action.

Data transfer is only possible when the computers involved use the same security methods. Multiple security methods increase the chance that two computers will use the same method.

To continue, click Next.

< Back

Next >

Cancel

OK

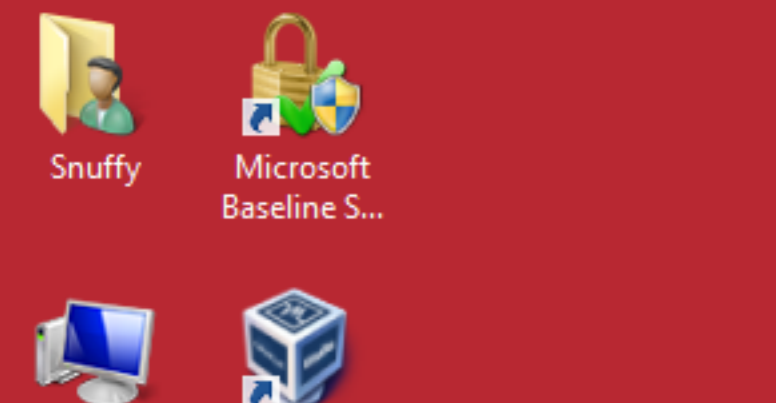
Cancel

```
Microsoft Windows [Version 6.0.6002.1.120617.amd64-x-ww]
(c) 2012 Microsoft Corporation
C:\Windows\system32>ver
Microsoft Windows [Version 6.0.6002.1.120617.amd64-x-ww]
C:\Windows\system32>mm
C:\Windows\system32>
```



Kleopatra





```
Microsoft Windows [Ver...
(c) 2012 Microsoft Cor...
C:\Windows\system32>ve...
Microsoft Windows [Ver...
C:\Windows\system32>mm...
C:\Windows\system32>
```

Windows 8 IDsec test01 Properties ? x

Security Rule Wizard x

Filter Action Wizard

Filter Action Name
Name this filter action and provide a brief description.

Name:
Windows 8 filter

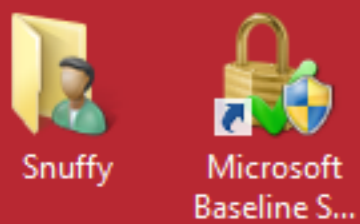
Description:
This is the filter for test 01 on Windows 8. |

< Back Next >

OK Cancel

The presentation creates a name and description for this filter.





```
Microsoft Windows [Version 6.0.6002.18005]
(c) 2012 Microsoft Corporation
C:\Windows\system32>ver
Microsoft Windows [Version 6.0.6002.18005]
C:\Windows\system32>mm
C:\Windows\system32>
```

Windows 8 IDsec test01 Properties ? x

Security Rule Wizard x

Filter Action Wizard

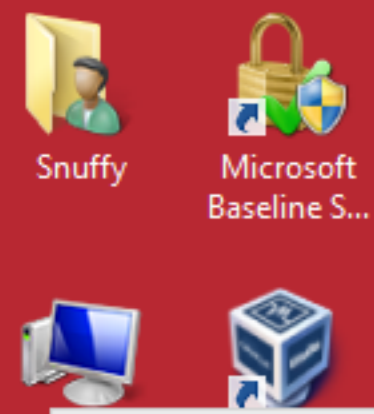
Filter Action General Options
Set the filter action behavior.

- Permit
- Block
- Negotiate security

OK Cancel

The presentation selects Negotiate security, then select next.





```
Microsoft Windows [Version 6.0.6002.18005]
(c) 2012 Microsoft Corporation
C:\Windows\system32>ver
Microsoft Windows [Version 6.0.6002.18005]
C:\Windows\system32>mm
C:\Windows\system32>
```

Windows 8 IPsec test01 Properties ? x

Security Rule Wizard x

Filter Action Wizard

Communicating with computers that do not support IPsec
Communicating with computers that do not support IPsec may expose your network to security risks.

Do you want to allow communication with computers that do not support IPsec?

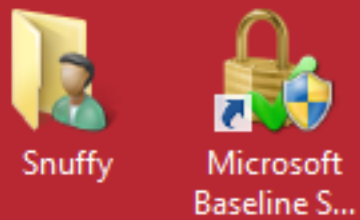
- Do not allow unsecured communication.
- Allow unsecured communication if a secure connection is established.
Use this option if there are computers on your network that have an incompatible IPsec configuration. Allowing unsecured communication may expose your network to security risks.
On a computer with Windows Vista or a later version of Windows, unsecured communication to be sent anytime a secure connection is established.
On a Windows 2000, Windows XP, or Windows 2003 computer, unsecured communications to be sent only when the remote computer supports IPsec.

< Back

OK Cancel

The presentation selects Do not allow unsecured communication. The presentation selects next.





```
Microsoft Windows [Version 6.0.6002.18005]
(c) 2012 Microsoft Corporation
C:\Windows\system32>ver
Microsoft Windows [Version 6.0.6002.18005]
C:\Windows\system32>mm
C:\Windows\system32>
```

Windows 8 IPsec test01 Properties ? x

Security Rule Wizard x

Filter Action Wizard x

IP Traffic Security
Specify a security method for IP traffic. To add multiple security methods, edit the filter action after completing the wizard.

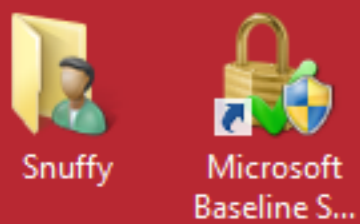
This filter action requires at least one security method for IP traffic.

- Integrity and encryption
Data will be encrypted, authenticated, and unmodified.
- Integrity only
Data will be authenticated and unmodified.
- Custom
Settings...

OK Cancel

The presentation selects Integrity and encryption.





```
Microsoft Windows [Version 6.0.6002.18005]
(c) 2012 Microsoft Corporation
C:\Windows\system32>ver

Microsoft Windows [Version 6.0.6002.18005]
C:\Windows\system32>mm

C:\Windows\system32>
```

Windows 8 IPsec test01 Properties ? x

Security Rule Wizard x

Filter Action Wizard

Completing the IP Security Filter Action Wizard

You have successfully completed the IP Security Filter Action Wizard.

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

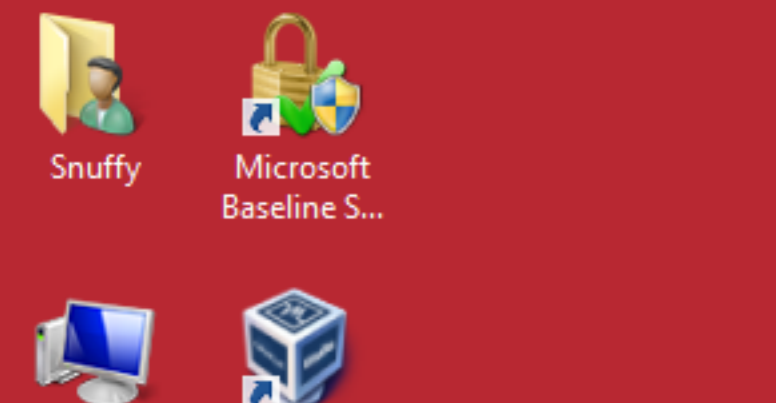
Edit properties

To close this wizard, click Finish.

< Back Finish Cancel

OK Cancel





Security Rule Wizard

Filter Action
Select the filter action for this security rule.

If no filter action 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
<input checked="" type="radio"/> Windows 8 filter	This is the filter for test 01

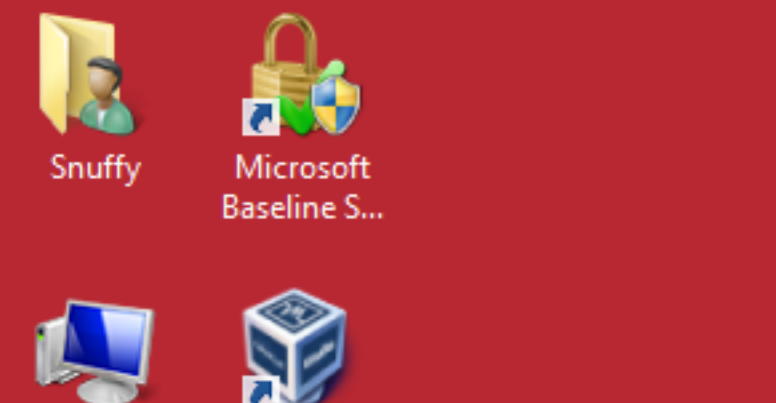
< Back Next >

OK Cancel

```
Microsoft Windows [Version 6.0.6002.18005]
(c) 2012 Microsoft Corporation
C:\Windows\system32>ver
Microsoft Windows [Version 6.0.6002.18005]
C:\Windows\system32>mm
C:\Windows\system32>
```

The presentation selects Windows 8 Filter, then selects next.





Security Rule Wizard

Authentication Method
To add multiple authentication methods, edit the security rule after completing the wizard.

Set the initial authentication method for this security rule:

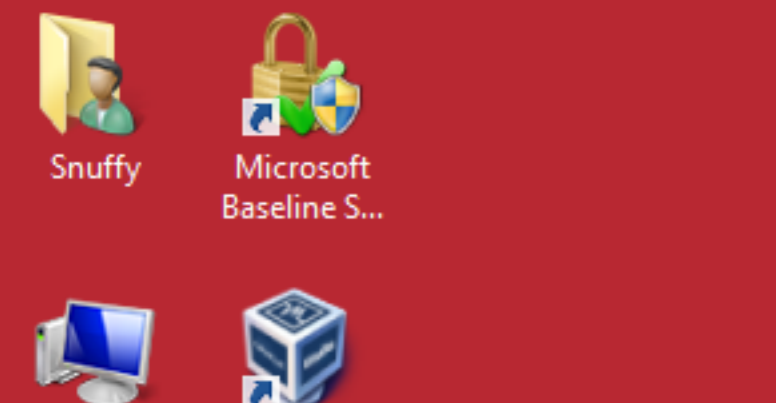
- Active Directory default (Kerberos V5 protocol)
- Use a certificate from this certification authority (CA):
[Text Box] [Browse...]
- Exclude the CA name from the certificate request
- Enable certificate to account mapping
- Use this string to protect the key exchange (preshared key):
[Text Box: Password01]

< Back [Next] OK Cancel

```
Microsoft Windows [Version 6.0.6002.1.80402.0]
(c) 2012 Microsoft Corporation
C:\Windows\system32>ver
Microsoft Windows [Version 6.0.6002.1.80402.0]
C:\Windows\system32>mm
C:\Windows\system32>
```

The presentation selects a very weak shared secret. Then the presentation selects next.

Remember the shared key must be the same for all participating computers.



```
Microsoft Windows [Version 6.0.6002.18005]
(c) 2012 Microsoft Corporation
C:\Windows\system32>ver
Microsoft Windows [Version 6.0.6002.18005]
C:\Windows\system32>mm
C:\Windows\system32>
```

Windows 8 IDsec test01 Properties ? x

Security Rule Wizard

Completing the Security 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.

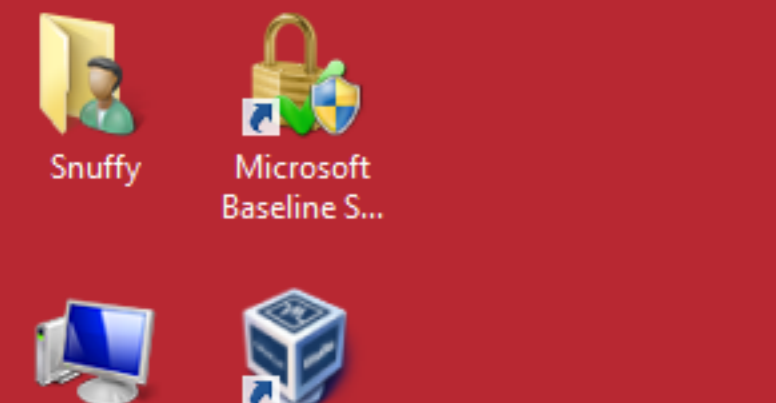
Edit properties

To close this wizard, click Finish.

< Back Finish Cancel

OK Cancel





Windows 8 IPsec test01 Properties

Rules General

Security rules for communicating with other computers

IP Security rules:

IP Filter List	Filter Action	Authentication...	Tu
<input checked="" type="checkbox"/> Windows 8 NAT 01	Windows 8 filter	Preshared Key	No
<input type="checkbox"/> <Dynamic>	Default response (ea...	Kerberos	<N

Use Add Wizard

```

Microsoft Windows [Version 6.0.6002.18005]
(c) 2012 Microsoft Corporation
C:\Windows\system32>ver
Microsoft Windows [Version 6.0.6002.18005]
C:\Windows\system32>mm
C:\Windows\system32>
  
```



Console1 - [Console Root\IP Security Policies on Local Computer]

File Action View Favorites Window Help



- Console Root
- IP Security Monitor
- IP Security Policies on Local Computer

Name	Description	Policy Assigned	Last Modified Time
Windows 8 IPsec...	This is Windows...		2014 4:54:31 PM

- Assign
- All Tasks
- Delete
- Rename
- Properties**
- Help

The presentation right clicks on the policy. The presentation selects Assign.

- Actions**
- IP Security Polici... ▲
 - More Actions ▶
 - Windows 8 IPse... ▲
 - More Actions ▶



ENG

4:54 PM
5/6/2014

Console1 - [Console Root\IP Security Monitor\WIN8-VICTIM02\Quick Mode\Statistics]

File Action View Favorites Window Help



- Console Root
 - IP Security Monitor
 - WIN8-VICTIM02
 - Active Policy
 - Main Mode
 - Quick Mode
 - Generic F
 - Specific F
 - Negotiati
 - Statistics
 - Security A
 - IP Security Policies c

Parameters Statistics

✕ Active Security Associations	0
✕ Offloaded Security Associations	0
✕ Pending Key Operations	0
✕ Key Additions	0
✕ Key Deletions	0
✕ Rekeys	0
✕ Active Tunnels	0
✕ Bad SPI Packets	0
✕ Packets Not Decrypted	0
✕ Packets Not Authenticated	0
✕ Packets With Replay Detection	0
✕ Confidential Bytes Sent	0
✕ Confidential Bytes Received	0
✕ Authenticated Bytes Sent	0
✕ Authenticated Bytes Received	0
✕ Transport Bytes Sent	0
✕ Transport Bytes Received	0
✕ Bytes Sent In Tunnels	0
✕ Bytes Received In Tunnels	0
✕ Offloaded Bytes Sent	0
✕ Offloaded Bytes Received	0

Actions

Statistics

More Actions

The presentation opens the statistics under IP Security Monitor. The monitor is showing no encrypted communication.



```

Administrator: Command Prompt
C:\Windows\system32>mmc
C:\Windows\system32>ping 192.168.5.132
Pinging 192.168.5.132 with 32 bytes of data:
Reply from 192.168.5.132: bytes=32 time<1ms TTL=128
Reply from 192.168.5.132: bytes=32 time<1ms TTL=128
Reply from 192.168.5.132: bytes=32 time<1ms TTL=128
Reply from 192.168.5.132: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.5.132:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Windows\system32>net use \\192.168.5.134
The password or user name is invalid for \\192.168.5.134.

Enter the user name for '192.168.5.134': snuffly
Enter the password for 192.168.5.134:
The command completed successfully.

C:\Windows\system32>_

```

The presentation pings the other computer and maps a drive to the other computer. This will generate traffic.

ExamView	HashCalc	X Transport Bytes Received	2584
Test Manager		X Bytes Sent In Tunnels	0
		X Bytes Received In Tunnels	0
		X ...	0

GPA

Console1 - [Console Root\IP Security Monitor\WIN8-VICTIM02\Quick Mode\Statistics]

File Action View Favorites Window Help

Console Root

- IP Security Monitor
 - WIN8-VICTIM02
 - Active Policy
 - Main Mode
 - Quick Mode
 - Generic F
 - Specific F
 - Negotiati
 - Statistics
 - Security A
 - IP Security Policies c

Parameters	Statistics
Active Security Associations	1
Offloaded Security Associations	0
Pending Key Operations	0
Key Additions	1
Key Deletions	0
Rekeys	0
Active Tunnels	0
Bad SPI Packets	0
Packets Not Decrypted	0
Packets Not Authenticated	0
Packets With Replay Detection	0
Confidential Bytes Sent	2800
Confidential Bytes Received	2192
Authenticated Bytes Sent	3136
Authenticated Bytes Received	2192
Transport Bytes Sent	3136
Transport Bytes Received	2192
Bytes Sent In Tunnels	0
Bytes Received In Tunnels	0

Actions

- Statistics
- More Actions

The IP Security Monitor is now showing encrypted communication between the hosts/computers.

*eth0 [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help



Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
16	12.151912000	192.168.5.134	192.168.5.2	NBNS	110	Refresh NB WIN8-VICTIM02<00>
17	12.574288000	192.168.5.134	192.168.5.132	ESP	270	ESP (SPI=0x1d123a16)
18	12.574776000	192.168.5.132	192.168.5.134	ESP	334	ESP (SPI=0xfb3abee)
19	12.575342000	192.168.5.134	192.168.5.132	ESP	310	ESP (SPI=0x1d123a16)
20	12.575716000	192.168.5.132	192.168.5.134	ESP	286	ESP (SPI=0xfb3abee)
21	12.580409000	192.168.5.134	192.168.5.132	ESP	270	ESP (SPI=0x1d123a16)
22	12.580421000	192.168.5.132	192.168.5.134	ESP	334	ESP (SPI=0xfb3abee)
23	12.580422000	192.168.5.134	192.168.5.132	ESP	182	ESP (SPI=0x1d123a16)
24	12.580423000	192.168.5.132	192.168.5.134	ESP	214	ESP (SPI=0xfb3abee)

Fragment offset: 0
 Time to live: 128
 Protocol: ESP (50)
 Header checksum: 0x0cff [correct]
 Source: 192.168.5.134 (192.168.5.134)
 Destination: 192.168.5.132 (192.168.5.132)
 [Source GeoIP: Unknown]
 [Destination GeoIP: Unknown]

Encapsulating Security Payload
 ESP SPI: 0x1d123a16 (487733782)
 ESP Sequence: 33

```

00b0 df dc 4e 0b ff e4 f4 0a de 09 d0 1f a3 7e 61 7a ..N.....~az
00c0 c0 9d 4a 0b 5a 14 e4 9d 8a 6e 1c 1a 46 1d e4 9e ..J.Z...n..F...
00d0 8e 87 58 e9 27 df 76 7b 0f c1 34 5f 4f 60 f4 99 ..X.'v{..4_0`..
00e0 d1 07 1b 1c 7b d8 f8 72 95 14 3e 22 ae 7e 29 77 ....{..r..>"~)w
00f0 8d 54 90 42 8a 50 96 ed 7e 67 14 02 18 eb 84 78 .T.B.P..~g.....x
0100 03 93 ee 23 3e c9 34 0b 4e fc d0 6d b0 7f ...#>.4. N..m..

```

Wireshark captured ESP packets between the computers/hosts. The encapsulated security packets indicated encrypted communications between the computers/hosts.