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.
The presentation starts the command prompt in administrator mode.
The presentation starts the mmc on the command line.
The presentation selects Add/Remove Snap-in
The presentation adds the IP Security Monitor and the IP Security Policy.
The IP Security Policy is run on the local computer.
The presentation right clicks IP Security Policy and selects Create IP Security Policy.
Welcome to the IP Security Policy Wizard

This wizard helps you create an IP Security policy. You will specify the level of security to use when communicating with specific computers or groups of computers (subnets), and for particular IP traffic types.

To continue, click Next.
The presentation creates a name and description for the policy.

**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.
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).

The presentation selects next.
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.
The presentation selects Add.
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.
The presentation is configuring transport mode.
The presentation will select the systems included in the IPsec party.
The presentation selects Add.
The presentation creates a name and description. Then presentation selects Add.
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.
The presentation creates a description.

**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.
The presentation selects a specific source address. In this example, the source IP address is this computer.
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.
The presentation selected Any protocol. This made the wireshark captures much easier.
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.

If you do not want to edit your IP filter now, click OK.

To close this wizard, click Finish.
The presentation selects OK.
The presentation selects NAT01. Then the presentation selects next.
The presentation selects Add.
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.
The presentation creates a name and description for this filter.

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.
The presentation selects Negotiate security, then select next.
The presentation selects Do not allow unsecured communication. The presentation selects next.
The presentation selects Integrity and encryption.
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.
The presentation selects NAT Filter 01, then selects next.
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.

To close this wizard, click Finish.
## Windows 7 IPsec test 01 Properties

### Rules

#### Security rules for communicating with other computers

**IP Security rules:**

<table>
<thead>
<tr>
<th>IP Filter List</th>
<th>Filter Action</th>
<th>Authentication...</th>
<th>Security Protocol</th>
<th>Action...</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAT 01</td>
<td>NAT Filter 01</td>
<td>Preshared Key</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;Dynamic&gt;</td>
<td>Default response</td>
<td>Kerberos</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Options:

- Add...:
- Edit...:
- Remove:
- Use Add Wizard:

Buttons:

- OK
- Cancel
The presentation right clicks on the policy. The presentation selects Assign.
The presentation's Windows 7 computer is ready.
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.
The presentation adds the IP Security Monitor and the IP Security Policy.

<table>
<thead>
<tr>
<th>Snap-in</th>
<th>Vendor</th>
</tr>
</thead>
<tbody>
<tr>
<td>ActiveX Control</td>
<td>Microsoft Corp</td>
</tr>
<tr>
<td>Authorization Manager</td>
<td>Microsoft Corp</td>
</tr>
<tr>
<td>Certificates</td>
<td>Microsoft Corp</td>
</tr>
<tr>
<td>Component Services</td>
<td>Microsoft Corp</td>
</tr>
<tr>
<td>Computer Management</td>
<td>Microsoft Corp</td>
</tr>
<tr>
<td>Device Manager</td>
<td>Microsoft Corp</td>
</tr>
<tr>
<td>Disk Management</td>
<td>Microsoft Corp</td>
</tr>
<tr>
<td>Event Viewer</td>
<td>Microsoft Corp</td>
</tr>
<tr>
<td>Folder</td>
<td>Microsoft Corp</td>
</tr>
<tr>
<td>Group Policy Object</td>
<td>Microsoft Corp</td>
</tr>
<tr>
<td>IP Security Monitor</td>
<td>Microsoft Corp</td>
</tr>
<tr>
<td>IP Security Policy Monitor</td>
<td>Microsoft Corp</td>
</tr>
<tr>
<td>Link to Web Address</td>
<td>Microsoft Corp</td>
</tr>
</tbody>
</table>

Description:
The IP Security Monitor snap-in is used to monitor the state of the IP Security Policy.
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: [List of available snap-ins]
- Vendor: [Vendor information for each snap-in]

Selected snap-ins:

- Console Root
- IP Security Monitor

Description:
Internet Protocol Security (IPsec) Administration. Manage IPsec policies for secure communication with other computers.
The IP Security Policy is run on the local computer.
The presentation right clicks IP Security Policy and selects Create IP Security Policy.
Welcome to the IP Security Policy Wizard

This wizard helps you create an IP Security policy. You will specify the level of security to use when communicating with specific computers or groups of computers (subnets), and for particular IP traffic types.

To continue, click Next.
The presentation creates a name and description for the policy.

Name:
Windows 8 IPsec test01

Description:
This is Windows 8 IPsec test 01. It really is not the first test, but ....]
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.
The presentation selects Add.
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.
The presentation is configuring transport mode.
The presentation will select the systems included in the IPsec party.
The presentation selects Add.
The presentation creates a name and description. Then presentation selects Add.
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.
The presentation creates a description.
The presentation selects a specific source address. In this example, the source IP address is this computer.
The presentation selects a specific destination address. In this example, the destination IP address is the Windows 7 or other computer.
The presentation selected Any protocol. This made the Wireshark captures much easier.
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.

To close this wizard, click Finish.
The presentation selects OK.
The presentation selects Windows 8 NAT01. Then the presentation selects next.
The presentation selects Add.
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.
The presentation creates a name and description for this filter.
The presentation selects Negotiate security, then select next.
The presentation selects Do not allow unsecured communication. The presentation selects next.
The presentation selects Integrity and encryption.
Microsoft Windows [Version 6.3.9600]
(c) 2012 Microsoft Corporation

C:\Windows\system32\version

Microsoft Windows [Version 6.3.9600]

C:\Windows\system32\mmmsvc

Comapling 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.
The presentation selects Windows 8 Filter, then selects next.
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.
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.
### Windows 8 IPsec test01 Properties

#### Rules

<table>
<thead>
<tr>
<th>IP Filter List</th>
<th>Filter Action</th>
<th>Authentication Method</th>
<th>Modes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 8 NAT 01</td>
<td>Windows 8 filter</td>
<td>Preshared Key</td>
<td>No</td>
</tr>
<tr>
<td>&lt;Dynamic&gt;</td>
<td>Default response (e.g., Kerberos)</td>
<td>&lt;N&gt;</td>
<td></td>
</tr>
</tbody>
</table>

- **Security rules for communicating with other computers**

- **IP Security rules:**

**Add...**  **Edit...**  **Remove**  **Use Add Wizard**

**OK**  **Cancel**
The presentation right clicks on the policy. The presentation selects Assign.
The presentation opens the statistics under IP Security Monitor. The monitor is showing no encrypted communication.
The presentation pings the other computer and maps a drive to the other computer. This will generate traffic.
The IP Security Monitor is now showing encrypted communication between the hosts/computers.
Wireshark captured ESP packets between the computers/hosts. The encapsulated security packets indicated encrypted communications between the computers/hosts.