**Secure Microsoft Windows**

**Practical 6**

**Planning and Deploying Security for Network Communications**

|  |
| --- |
| **Objectives:**  After completing this lab, you should be able to:   1. Understand the basic procedures of IPsec Configuration 2. Define IPsec Policy Rule to filter ICMP packets between hosts. 3. Deploy IPsec Policy with GPO. 4. Configure firewall settings with GPO and LPO. 5. Understand the relationship between, Rule, Filter List, Filter Action, and Authentication Methods in IPsec operation. 6. Use netsh command line tool to examine IPsec settings 7. Introduction to use Windows Firewall Advanced Security Rule Settings 8. Apply GPUPDATE and GPRESULT commands to monitor GPO deployment status. |
|  |

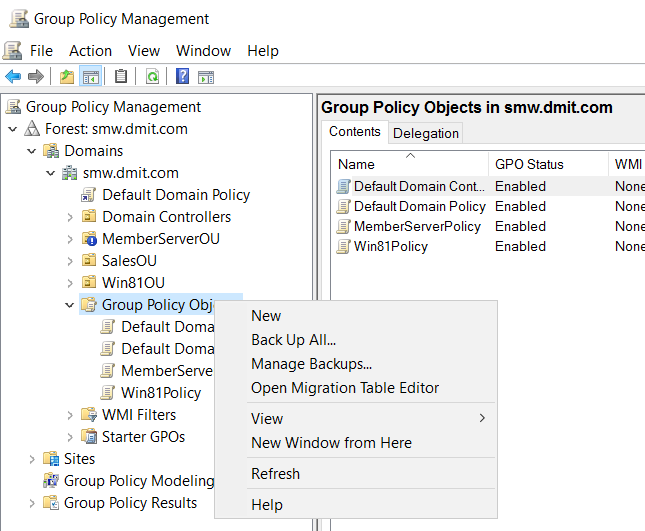
Lab Prerequisites:

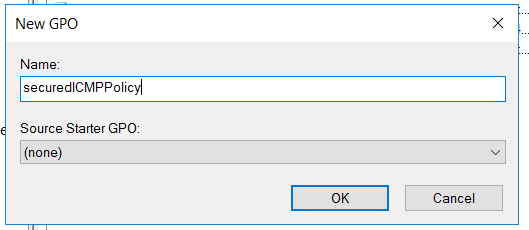
In this Lab, you will need your Domain Controller, a Member Server (you can use your webserver Server1 – created at Practical 3) and the Windows 10 Workstation.

Usage of gpupdate /force and gpresult /r commands (need to run in administrative cmd/powershell).

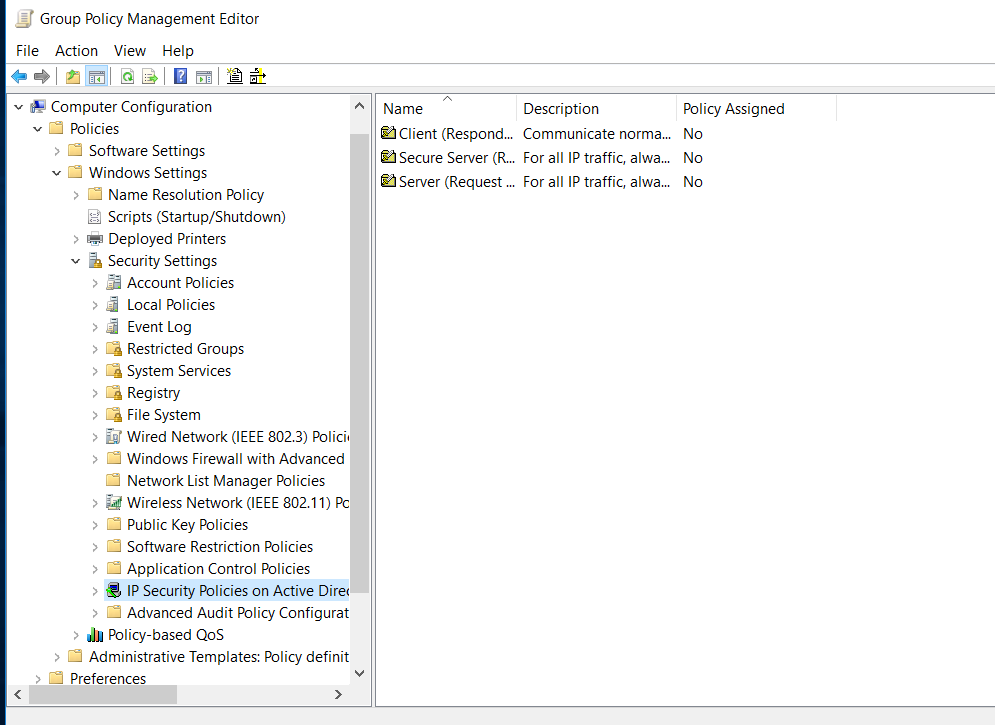
**Lab Exercise 6-1: Create an IPsec Policy**

1. Log on to the Domain Controller as Domain Administrator.
2. Start Group Policy Management Console. Right-click on Group Policy Objects and create a new GPO with the name “securedICMPPolicy”.



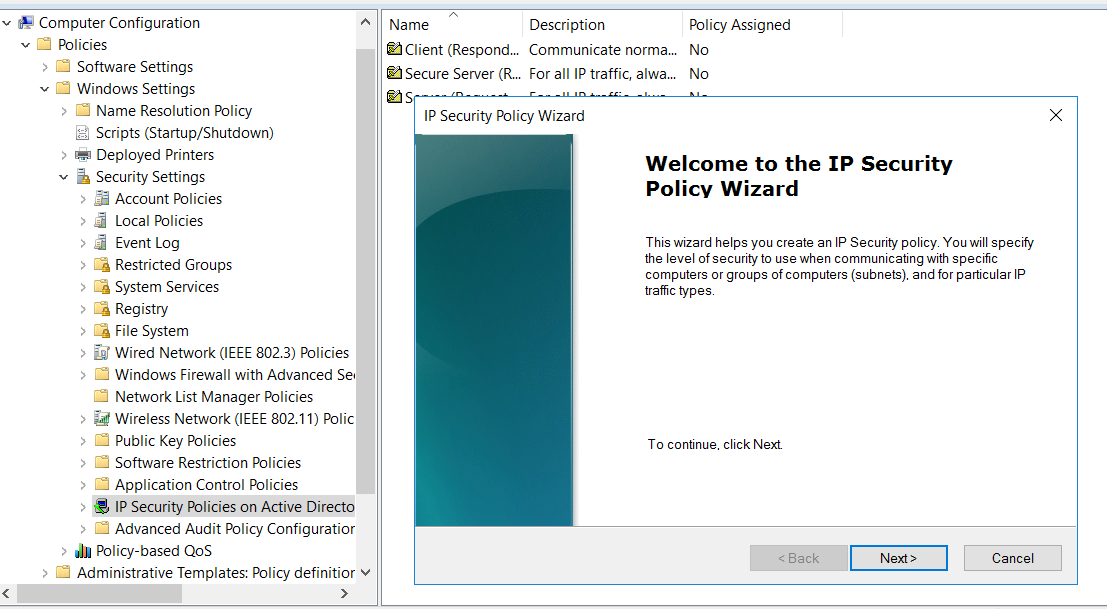


1. Edit the newly created GPO and add in the IPsec Policy. Refer to the screen shot at below, to locate the IPsec Policy Setting menu. Note that there are three default IPsec policies.



The three default IPsec policies

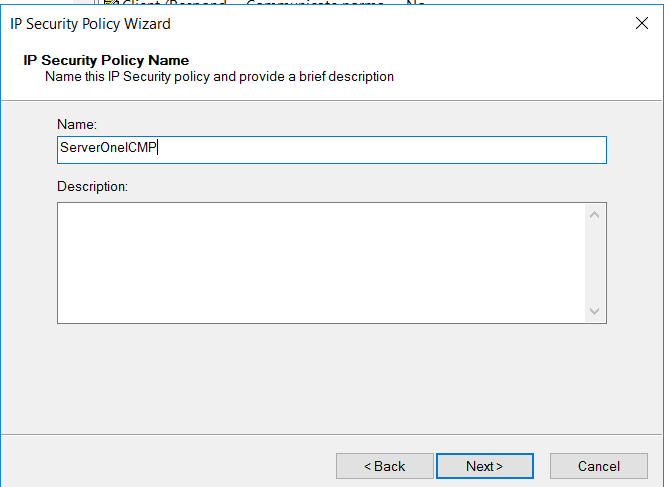
1. Right-click on 'IP Security Policies on Active Directory' and choose Create IP Security Policy to start the IP Security Policy Wizard:



Click Next.

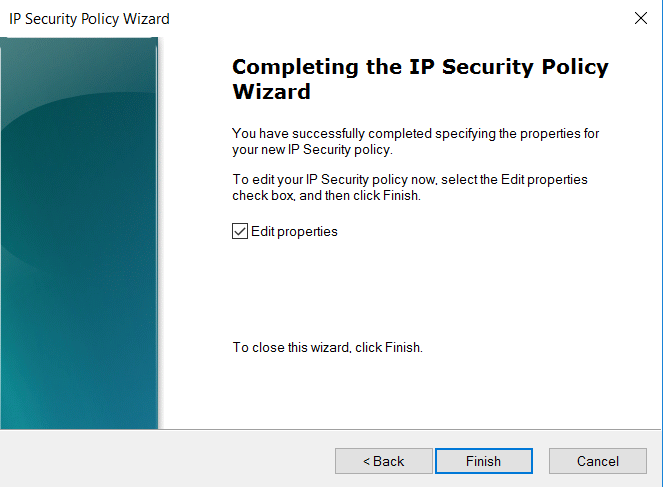
* 1. Note : You are creating a new IPsec policy within a Group Policy Object.

1. Set the name of the new IP Security Policy to “ServerOneICMP”.

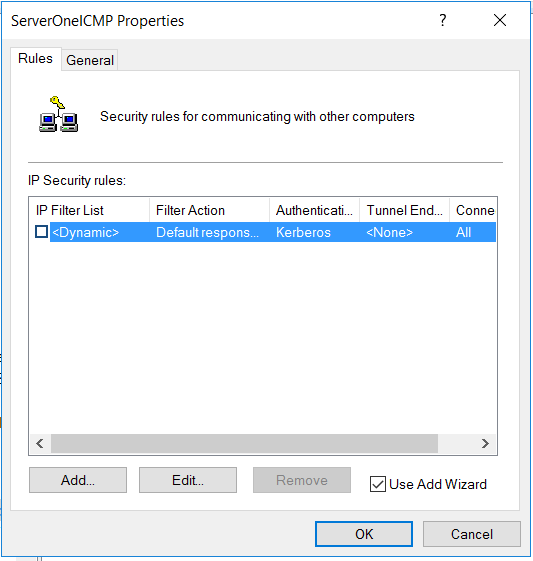


Click Next.

1. On the Requests for secure Communication screen, take the default, ie. leave the ‘Activate the default response rule’ option unchecked. Click Next.
2. On the Completing the IP Security Policy Wizard Page, verify that the **edit properties** box is checked. Click Finish.



1. After the wizard is ended, the ServerOneICMP Properties setting window will be activated, you can update the properties via this. (More details will be described in the next exercise).

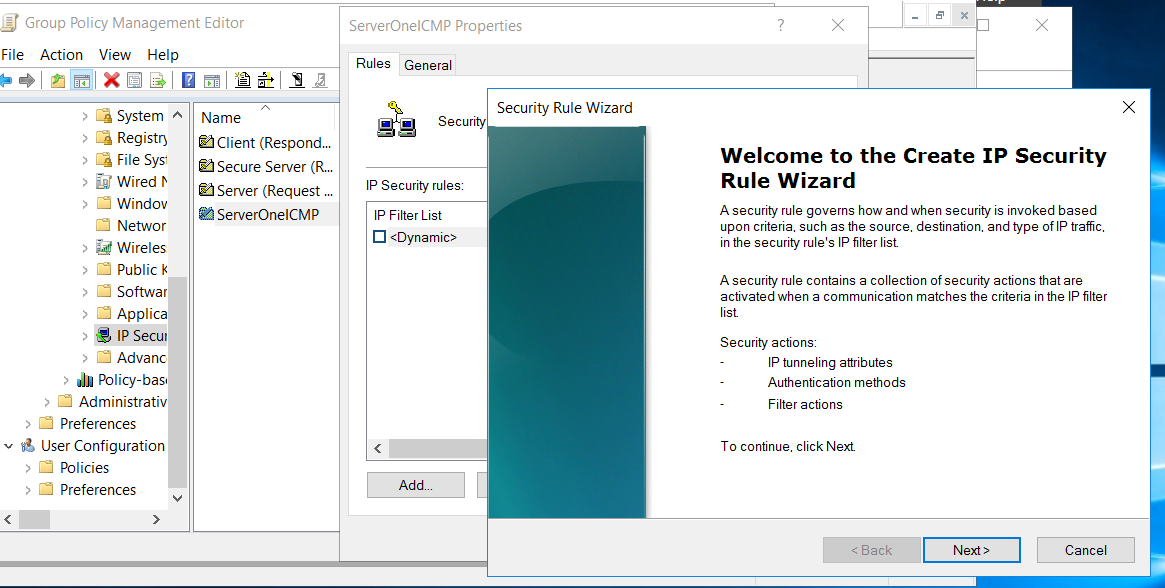


For now, click OK to close this window.

**Lab Exercise 6-2: Configure Authentication, Encryption Methods and Protocol for IPsec**

We will modify the Server1ICMP IPsec Policy to enforce IPsec communication using pre-shared key authentication for ICMP traffic between two machines.

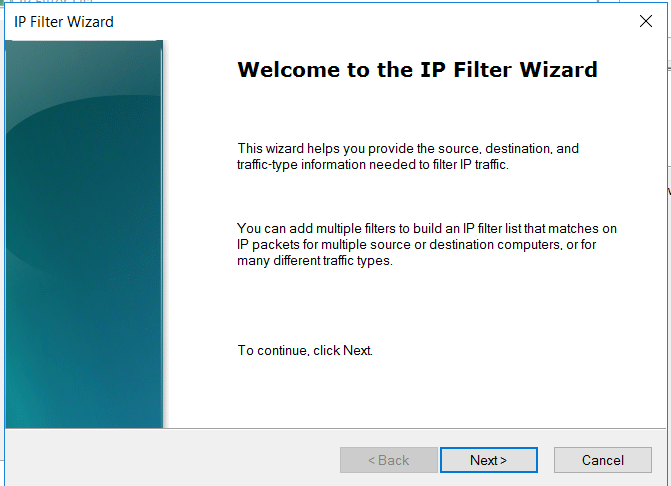
1. To Edit the properties of the securedOneCMPPolicy.
   1. Activate the GPO editor for securedICMPPolicy.
   2. Go to Computer Configuration->Policies->Windows Settings->Security Settings->IP Security Policies
2. Right-click on the ServerOneICMP IPsec Policy, and choose **Properties**.
3. There are two tabs menu in the Properties setting window. In the IP Security Rules Tab, ensure the default entry is unchecked. Click **Add** to bring up the Security Rule Wizard.



Ensure this entry is unchecked and click the Add button.

1. On the Security Rule Wizard screen, choose **Next**.
2. Apply the following configuration parameters when being prompted by the Security Rule Wizard :
   1. Tunnel Endpoint : This rule does not specify a tunnel.
   2. Network Type : Local area network (LAN).
   3. IP Filter List:

Add in a new IP Filter List with the name ,'ServerOneICMP Traffic'. Click Add will bring up the IP Filter Wizard :

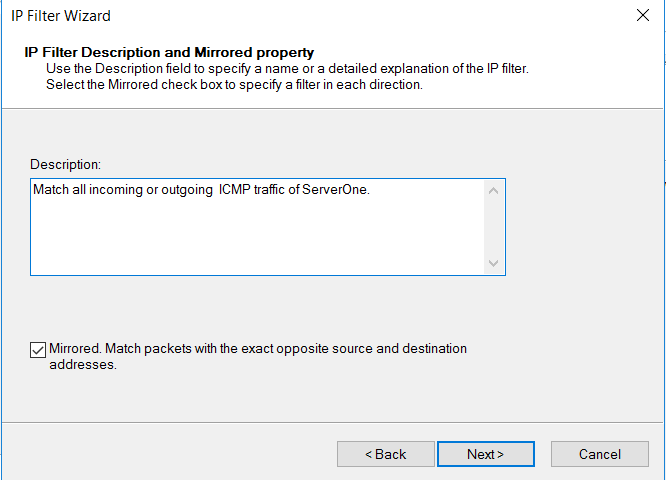


Define the detail settings of the 'ServerOneICMP Traffic' based on the followings:

* + 1. IP Filter Description and Mirrored property

Description: Match all incoming or outgoing ICMP traffic of ServerOne.

Mirrored : Yes (Check).



* + 1. IP Traffic Source –

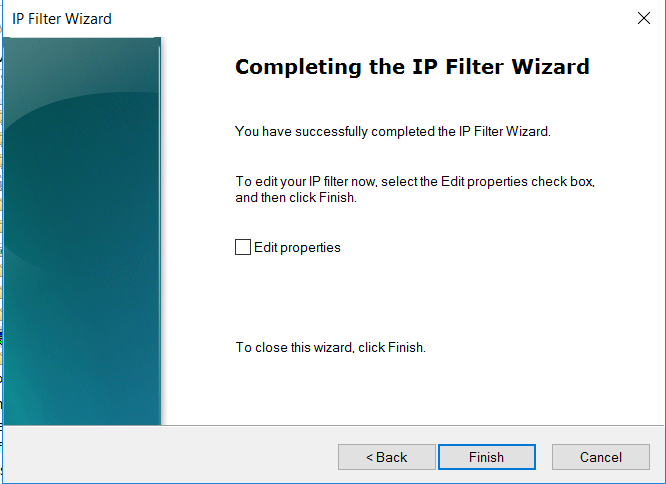
Source address: A specific IP Address or Subnet

*< IP address of your Server1>*

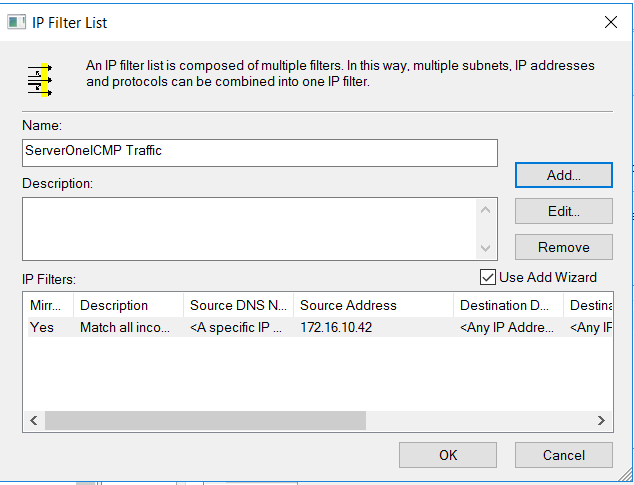
* + 1. IP Traffic Destination –

Destination Address : Any IP Address

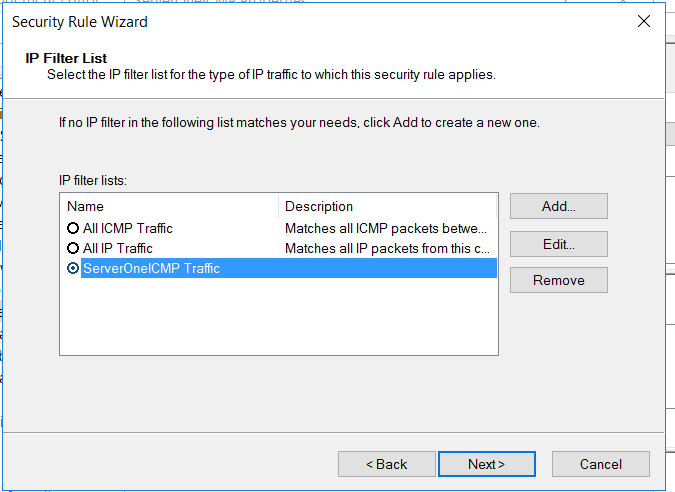
* + 1. IP Protocol type – ICMP
    2. Click 'Finish' to end the Wizard :



* + 1. In the next screen click 'OK' to close the ServerOneICMP Traffic Filter list and continue the next step offered by the 'Security Rule Wizard'.



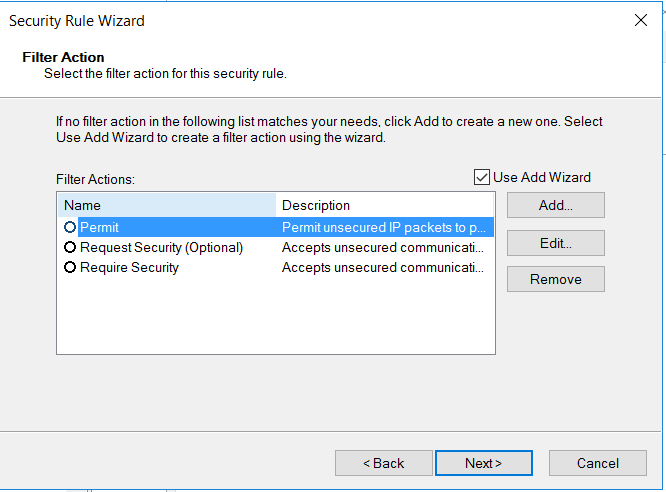
* 1. After the above is done. Select 'ServerOneICMP Traffic' Filter List as the default IP Filter List.



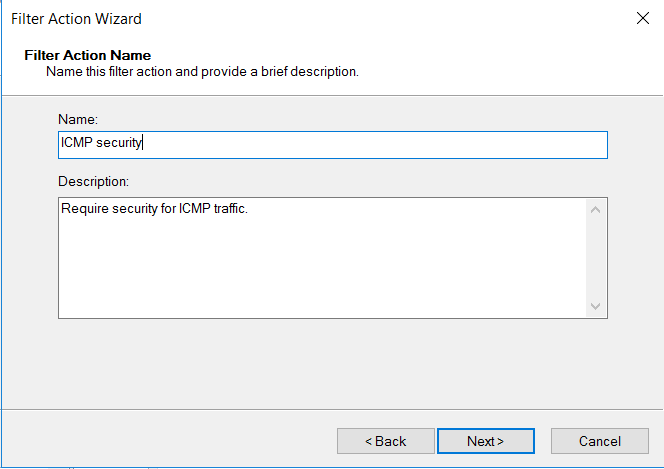
2

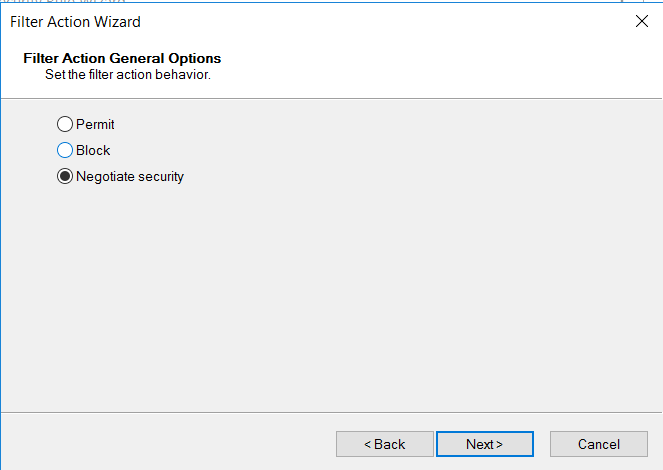
1

* 1. Click Next to go to the Filter Action screen.

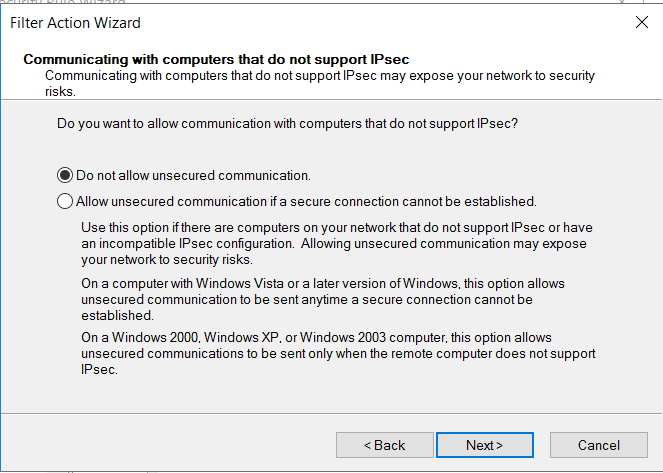


* 1. In the Filter action screen (as shown in the above), there are three default Filter actions. However, we need to create a new one for our exercise, to do that, click 'Add' to add a new Filter Action and name it ‘ICMP security’. The setting of this new Action is shown in the following screenshots:

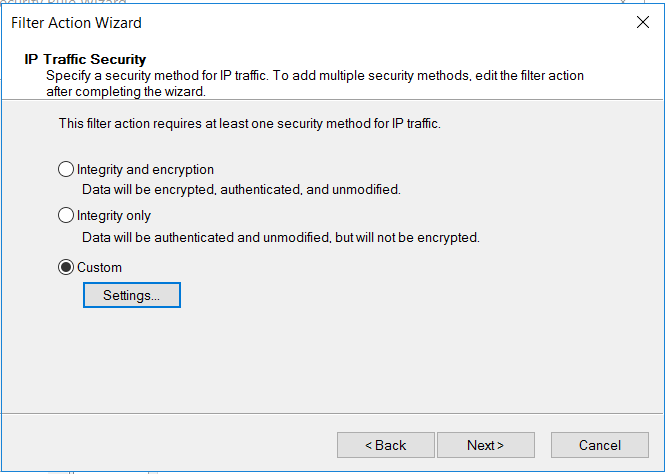




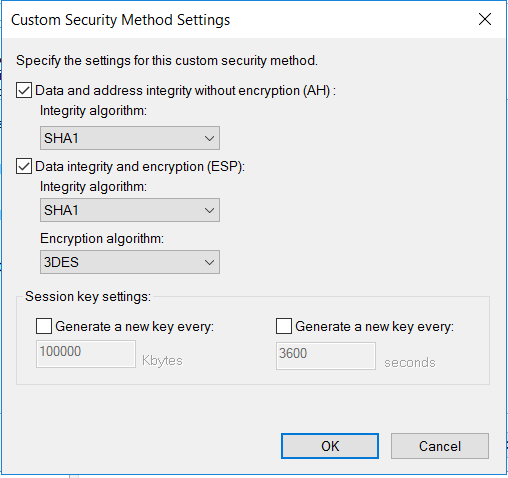
[Select Negotiate Security for filter Action Behavior]



[Do not allow unsecured communication]

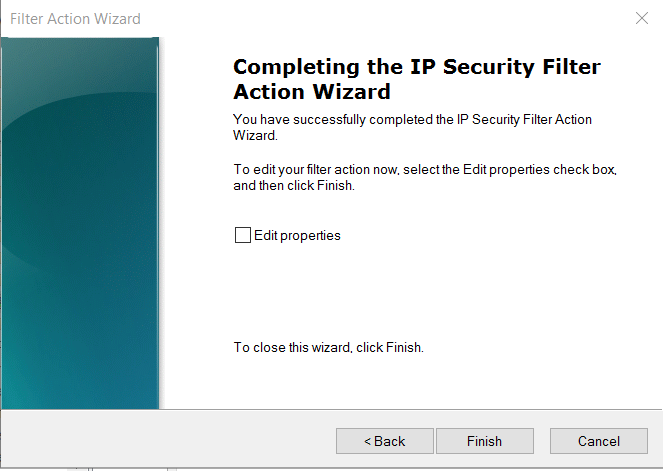


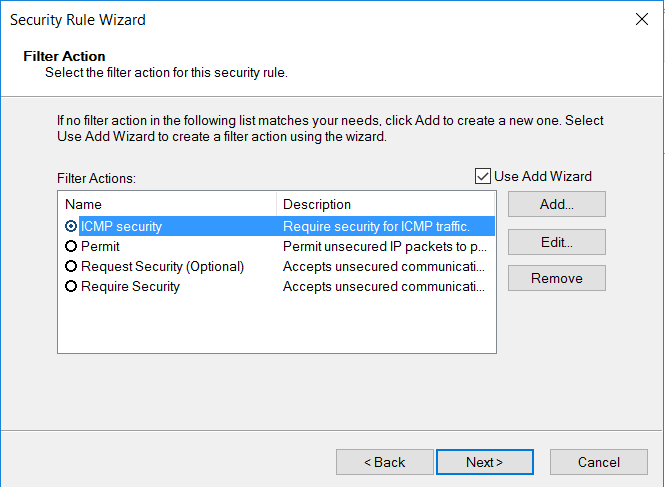
[For IP Traffic Security - use Custom settings – Click on the Settings button to bring up the customization screen]



[Enable both of the (AH) and (ESP) methods and click 'OK'. ]

After back to the IP Traffic Security setting screen, click 'Next' will bring to the last page of the Filter Action Wizard. Click 'Finish' to exit.

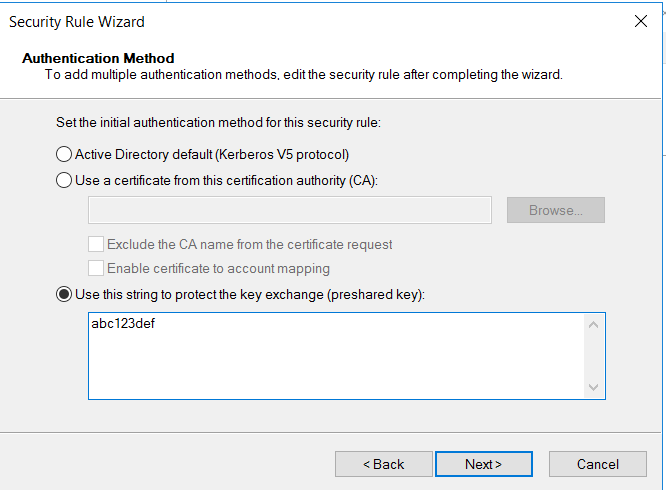




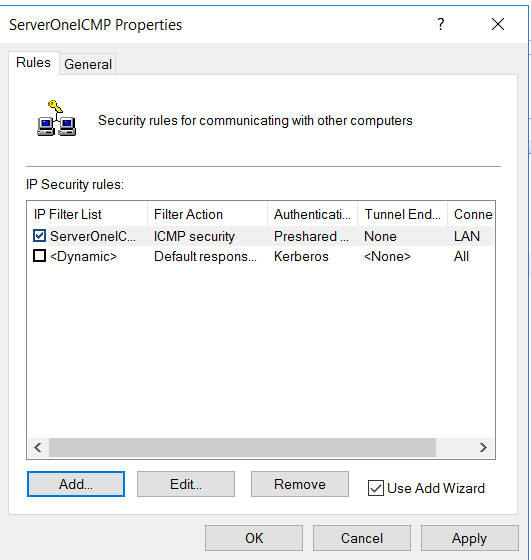
Now you can select "ICMP security" as the Filter Action of the rule.

Click 'Next' to proceed to the next step offered by the Security Rule Wizard.

* 1. For Authentication Method, select (pre-shared key) and set the string value to “abc123def”.



* 1. Click Next and you will complete with the Security Rule Wizard.



As show at the above, we only select and enable one IPsec 'rule' for this IPsec policy.

The rule comprises of the 'ServerOneICMP Traffic' IP Filter list, the 'ICMP security' Filter Action, the settings of the Authentication, Tunnel Endpoint and the Connection Type.

At this point, you have prepared a set of usable IPsec Policy in your Domain. In the following exercises, you are going to deploy this policy to the targeted domain machines to apply the IPsec features.

In conclusion:

You have created:

* A IPsec Policy – ServerOneICMP
* A new IPsec rule which contains
  + A Filter list – ServerOneICMP Traffic.
  + A Filter Action – ICMP security.
  + Authentication Method : Preshared key.
  + Tunnel Endpoint: None.
  + Connection Type: LAN.

**Lab Exercise 6-3: Setting up the Testing Environment**

Before we are assigning the ServerOneICMP IPsec Policy to the Server1 and the Win 10 workstation,

you should prepare a controlled testing environment: Such that you can compare the before and after effects of your IPsec Policy experiment.

1. Before deploying the IPsec Policy, do the following Ping tests. Remember to adjust the firewalls to allow ICMP traffic first.

(Note: Use Group Policy to adjust your VMs firewall settings. Use Local Policy to adjust your own Notebook firewall settings. Hints: To enable ping: look for the File and Printer Sharing Rule)

* 1. Ping from your Win10 image to Server1.
  2. Ping from Server1 to your Win10 image.
  3. Ping from your Domain Controller to Server1.
  4. Ping from Server1 to your Domain Controller.
  5. Ping from your Domain Controller to Win10 image.
  6. Ping from your Win10 image to your Domain Controller.
  7. Optionally, you can include your actual notebook to be part of the experiment.

All the pings using ips or machine names should be successful.

Windows 10(vm)

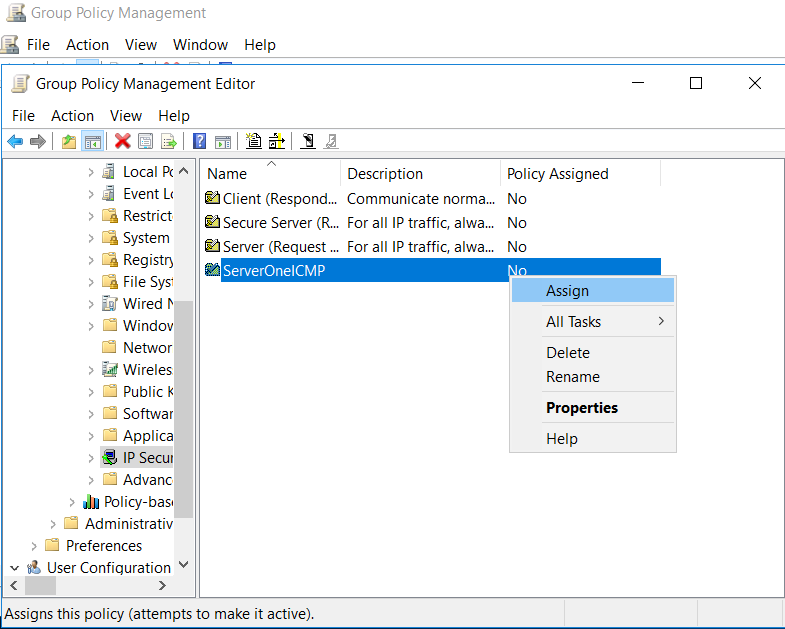
Domain Controller Win 2016(vm)

Your Actual Notebook Win 10 ?(optional)

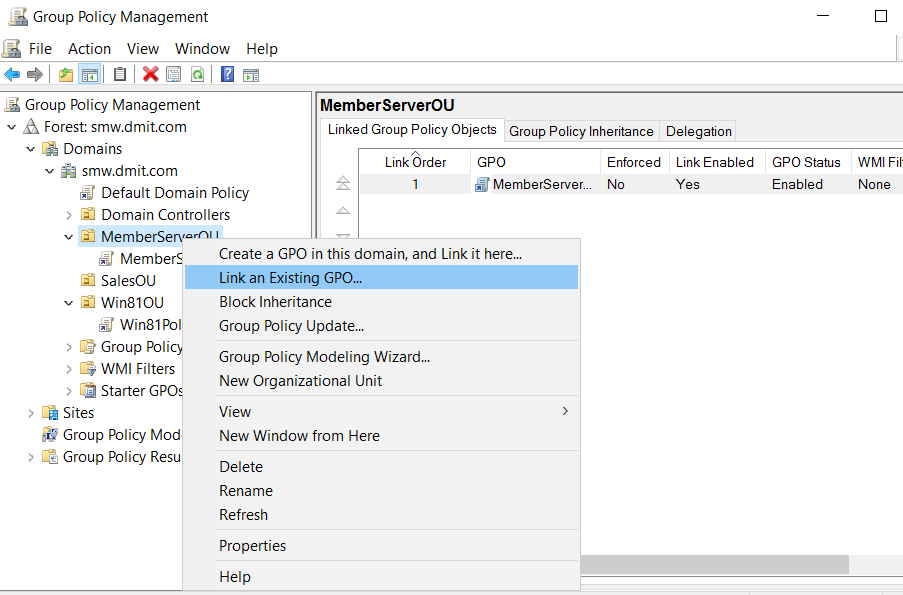
Server1 Win 2012R2(vm)

Reflection prompt: You may share your firewall settings procedures (GPO based vs LPO based)

1. We will now assign the ‘ServerOneICMP’ IPsec Policy – Remember that the Server1ICMP IPsec Policy is defined in securedICMPPolicy GPO.
2. Use GPMC to edit the securedICMPPolicy. Locate the IP Security Policies container.
3. Right click ServerOneICMP and choose Assign.



1. Close the GPO editor. Link the securedICMPPolicy to the OU that hosts Server1.



If Server1 is in the memberServerOU, then right-click on memberServerOU and choose Link an existing GPO

1. Use gpupdate at Server1 to activate the newly linked GPO.
2. Repeat the ping tests.

This time, verify if only the pings between your Domain Controller and Windows 10 image are successful. **(STOP HERE)**

ping ok?

Server1

Domain Controller

Windows 10

Your Actual Notebook (optional)

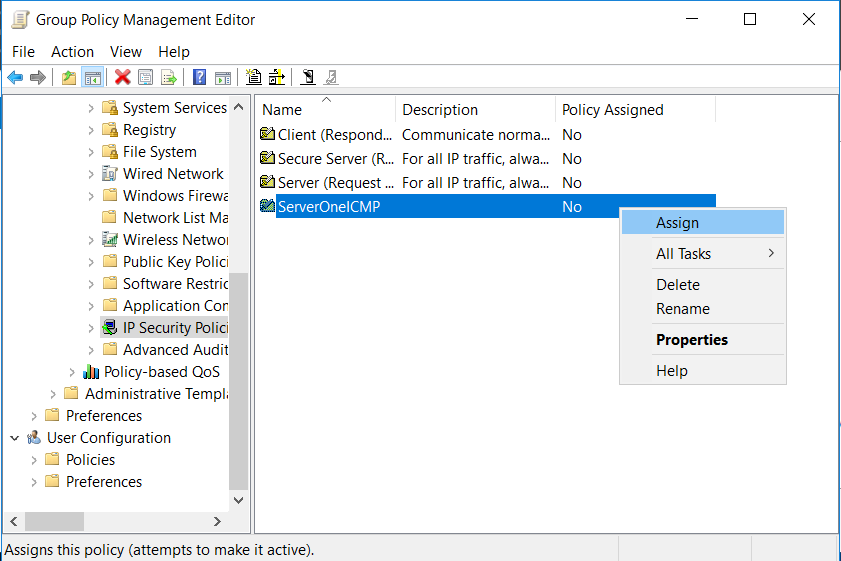
IPsec Policy : ICMP traffic to/from Server1 must be secured

1. In order to let the Win10 workstation able to ping Sever1, we need to apply the ServerOneICMP IPsec policy to the Win10 workstation.

To do this, we can link the SeverOneICMPPolicy GPO to the OU that houses the Win10 , or we can try the following:

Edit the GPO that is already linked to the OU that houses the Win10 , e.g. Win10\_Policy.

You will see find the ServerOneICMP IPsec policy already listed in the GPO. (but it is in unassigned state). It is because, the IPsec policy is independent to GPOs. Once you have added an IPsec Policy to the Active Directory, it will become available for all GPOs.



Turn it on, then your Win10 will be armed (assigned) with the same IPsec Policy as the Server1.

Reflection Prompt: You may record down the fact that, all IPsec policy objects is applicable cross all the existing GPOs. Each GPO can only assign up to one IPsec policy.

1. Remember to use “gpupdate” at your Server1 and Win 10. to ensure they have received the updated GPO settings.
2. Now that serverOneICMP IPsec policy is applied to both Server1 and Win 10, which of the following ping tests will be successful? Try to answer the following before taking the actual test.
   1. Ping from your Win10 image to Server1.
   2. Ping from Server1 to your Win10 image.
   3. Ping from your Domain Controller to Server1.
   4. Ping from your Actual notebook to Win10 image.
   5. Ping from your Domain Controller to Win10 image.
   6. Ping from your Win10 image to your Domain Controller.
3. Carry out the 5 ping tests. Are the results what you expected?

Domain Controller

Windows 10

Server1

Your Actual Notebook (optional)

1. Explore and use netsh command to examine and verify both of the Server1 and Win 10 workstations are loaded with the IPsec policy accordingly. You must start a command prompt or powershell console as Administrator in order to run the netsh command.

Without the admin right, the netsh command can work but it will not display any IPsec related information.

If you are not sure what to type at the netsh prompt, type “help” or “?” to show a list of available commands.

**Reset settings:**

1. In GPMC, un-assign the ServerOneICMP IPsec policy from all the relevant GPOs.

(Do not delete the ServerOneICMP IPsec policy, you need it in the next Practical.)

**Demonstration of an alternate approach to deploy IPsec using Windows Firewall Advanced Security rules:**

Please watch this [Demo video](https://web.microsoftstream.com/video/545eb053-e289-458e-b6ba-6d9c046073f8).

**Lab Exercise 6-4: (Optional and highly recommended Exercises)**

There are two optional exercises you may try to help deepen your understanding of IPsec applications.

* Use the wireshark program in one of your domain clients to monitor and explore the effect of IPsec.
* Apply the techniques you have learned in this practical, try if you can setup an IPsec policy to protect a host to host http traffic. (e.g. Win 10 to Server1 http web pages)

~ End of Practical 6 ~