7.4.1

IPSec Security

(Windows XP to XP)

Laboratory Overview

Objective

At the end of this lab students will be able to configure, assign, and test a Windows XP IP Security Policy.

Information for Laboratory

A. Students will utilize the Microsoft Management Console to create, edit, and assign an IPsec policy.

Student Preparation

The student will have completed requisite reading. The student will require paper for notes and should be prepared to discuss the exercises upon completion.

Students will need access to a Windows XP workstation with access to Local Computer IP Security Policies Snap-in.

Warning[s]

An IP Security Policy can completely block all network communications. Be sure to un-assign and remove all IP Security policies created in this lab.

Estimated Completion Time

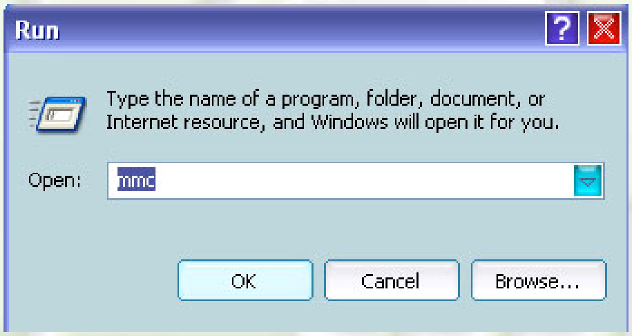
60 Minutes

IP Security Policies in Windows XP

Internet Protocol Security (IPSec) is a framework of open standards for ensuring private, secure communications over Internet Protocol (IP) networks, through the use of cryptographic security services. IPSec supports network-level peer authentication, data origin authentication, data integrity, data confidentiality (encryption), and replay protection. The Microsoft implementation of IPSec is based on standards developed by the Internet Engineering Task Force (IETF) IPSec working group. The strong, cryptographic-based authentication and encryption that IPSec provides is especially useful for securing traffic that must traverse untrusted network paths, such as on a large corporate intranet or the Internet. IPSec is also especially useful for securing traffic that uses protocols and applications that do not provide sufficient security for communications.

Step 1: Load Local Security Policy Management snap-in

From START, Run, Enter 'mmc'

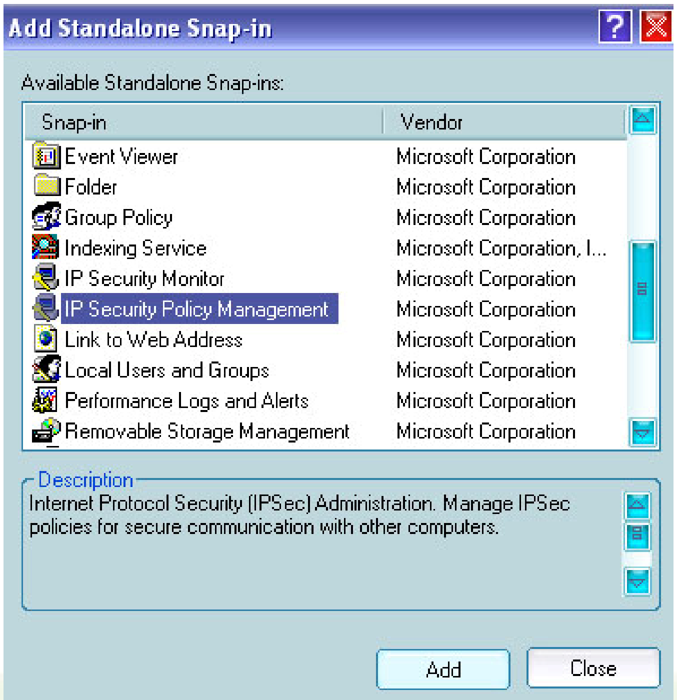


Run

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

Open: mmc

From File, click Add Remove Snap-in. On the Add Remove Snap-in box, click Add on the bottom. Scroll down to the IP Security Policy Management Snap-in, select it, and click Add, then click finish to accept the default settings for Local Computer.



Add Standalone Snap-in

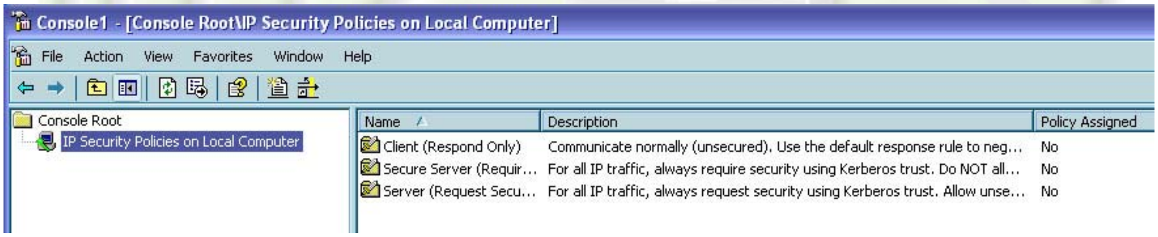
Available Standalone Snap-ins:

Snap-in	Vendor
Event Viewer	Microsoft Corporation
Folder	Microsoft Corporation
Group Policy	Microsoft Corporation
Indexing Service	Microsoft Corporation, I...
IP Security Monitor	Microsoft Corporation
IP Security Policy Management	Microsoft Corporation
Link to Web Address	Microsoft Corporation
Local Users and Groups	Microsoft Corporation
Performance Logs and Alerts	Microsoft Corporation
Removable Storage Management	Microsoft Corporation

Description

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

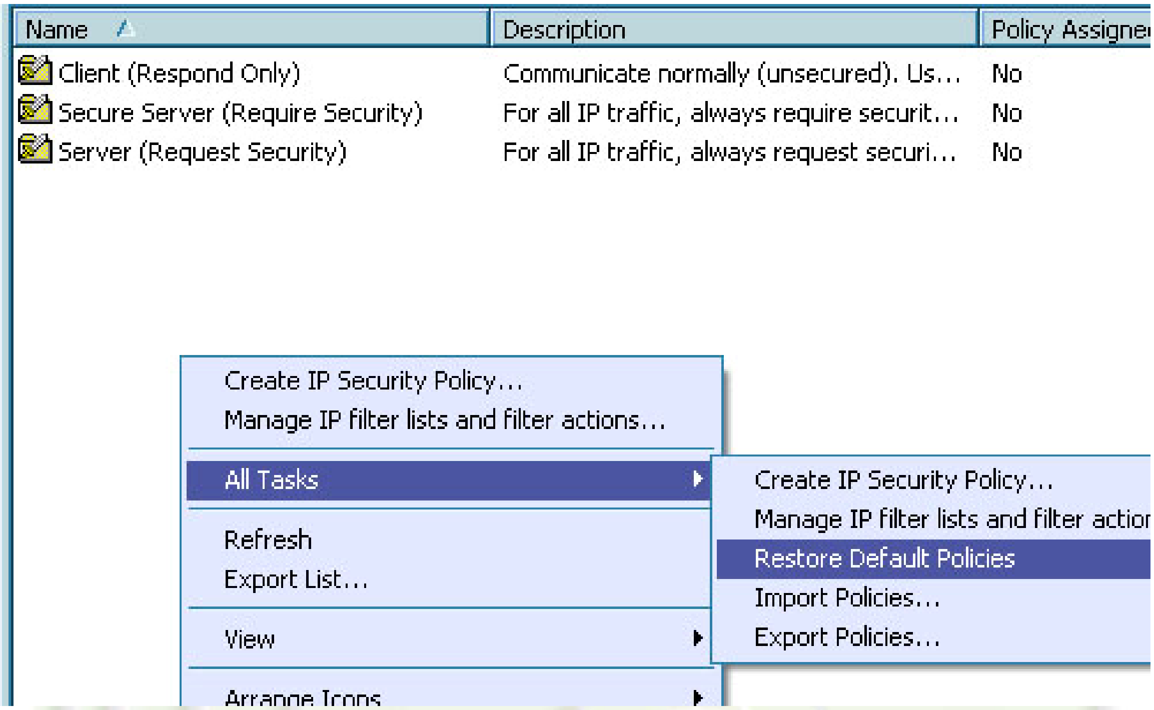
Once back to the Add Remove Snap-in box, click OK again. Now the IP Security Policy Management snap-in is loaded, double click on the IP Security Policies on Local Computer in the Left side. This will show all Security Policies on the Local computer.



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

Name	Description	Policy Assigned
Client (Respond Only)	Communicate normally (unsecured). Use the default response rule to neg...	No
Secure Server (Requir...	For all IP traffic, always require security using Kerberos trust. Do NOT all...	No
Server (Request Secu...	For all IP traffic, always request security using Kerberos trust. Allow unse...	No

On the right side, right click and delete all security policies. Then, right click in the open space, and select All Tasks, and Restore Default Policies. This will clear any changes that may have been previously made to your policies. Click Yes when asked if ok, and click OK to acknowledge that Default security policies have been successfully restored to default values.

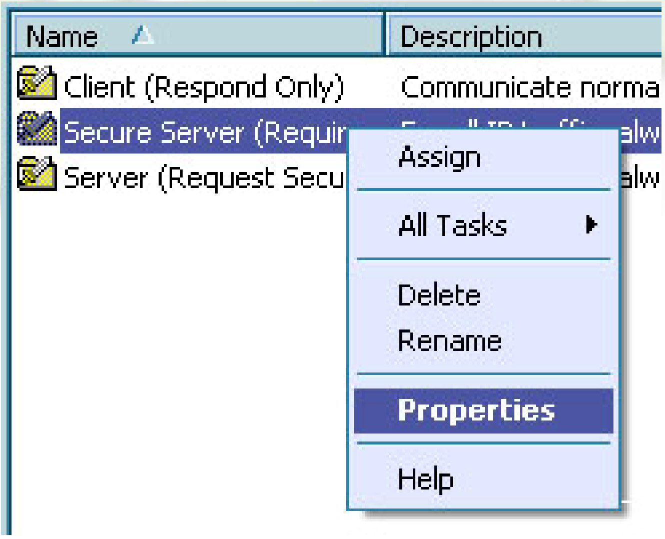


Name	Description	Policy Assigned
Client (Respond Only)	Communicate normally (unsecured). Us...	No
Secure Server (Require Security)	For all IP traffic, always require securit...	No
Server (Request Security)	For all IP traffic, always request securi...	No

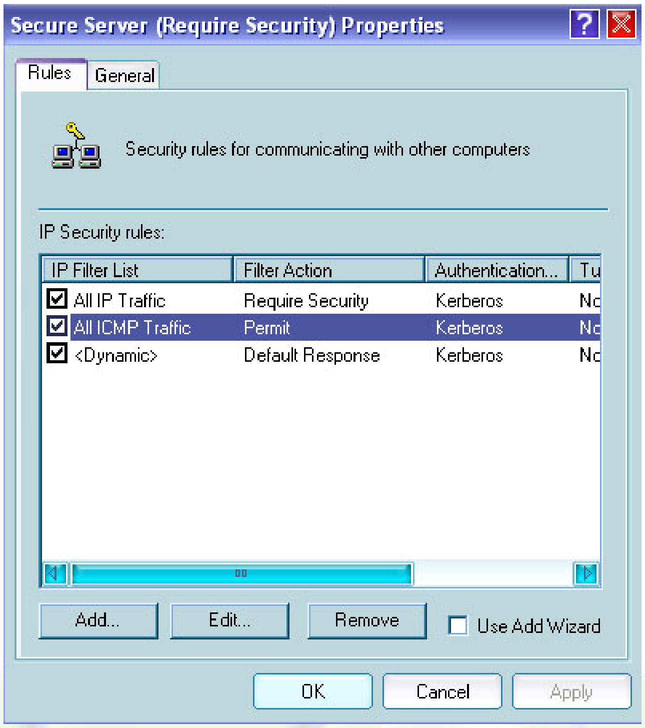
Create IP Security Policy...
Manage IP filter lists and filter actions...
All Tasks
Refresh
Export List...
View
Arrange Icons
Create IP Security Policy...
Manage IP filter lists and filter actior
Restore Default Policies
Import Policies...
Export Policies...

Step 2: Configure an IP Security Policy

Right click on the Secure Server (Require Security) Policy and click properties.



Name	Description
Client (Respond Only)	Communicate norma
Secure Server (Requir	alw
Server (Request Secu	alw



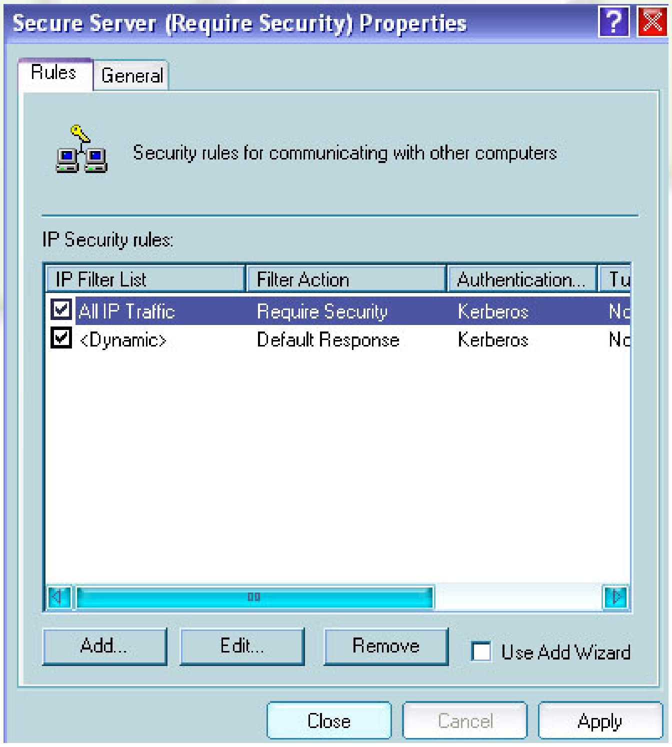
Security rules for communicating with other computers

IP Security rules:

IP Filter List	Filter Action	Authentication...	Tu
☑ All IP Traffic	Require Security	Kerberos	No
☑ All ICMP Traffic	Permit	Kerberos	No
☑ <Dynamic>	Default Response	Kerberos	No

☐ Use Add Wizard

From the properties box, delete the All ICMP Traffic rule by selecting it and clicking remove.



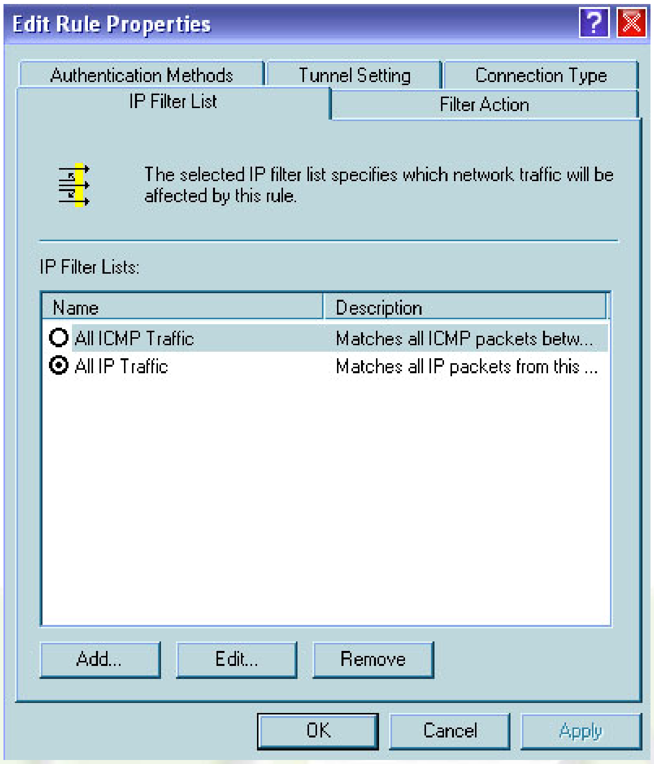
Security rules for communicating with other computers

IP Security rules:

IP Filter List	Filter Action	Authentication...	Tu
☑ All IP Traffic	Require Security	Kerberos	No
☑ <Dynamic>	Default Response	Kerberos	No

☐ Use Add Wizard

Select the All IP Traffic rule, and click edit



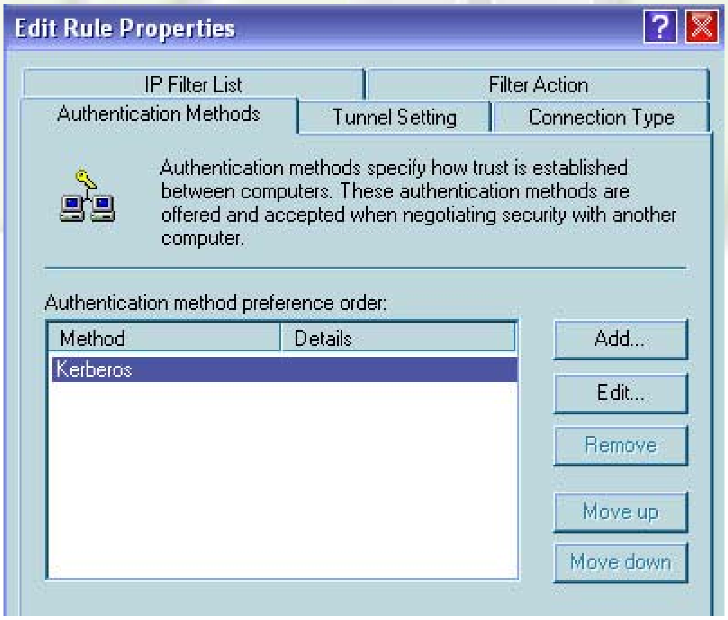
Edit Rule Properties

The selected IP filter list specifies which network traffic will be affected by this rule.

IP Filter Lists:

Name	Description
○ All ICMP Traffic	Matches all ICMP packets betw...
● All IP Traffic	Matches all IP packets from this ...

Click on the Authentication Methods Tab



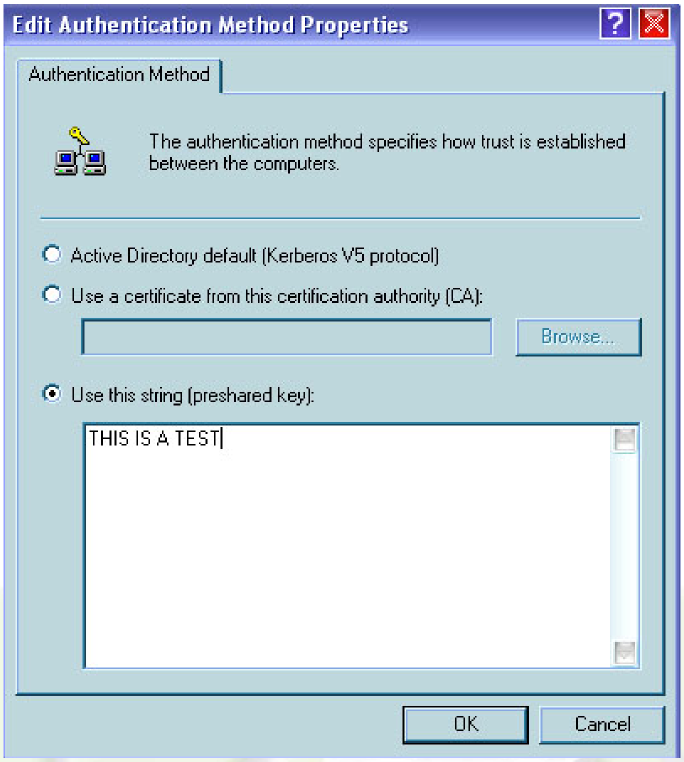
Edit Rule Properties

Authentication methods specify how trust is established between computers. These authentication methods are offered and accepted when negotiating security with another computer.

Authentication method preference order:

Method	Details
Kerberos	

Select Kerberos and click edit…


Edit Authentication Method Properties

Authentication Method

The authentication method specifies how trust is established between the computers.

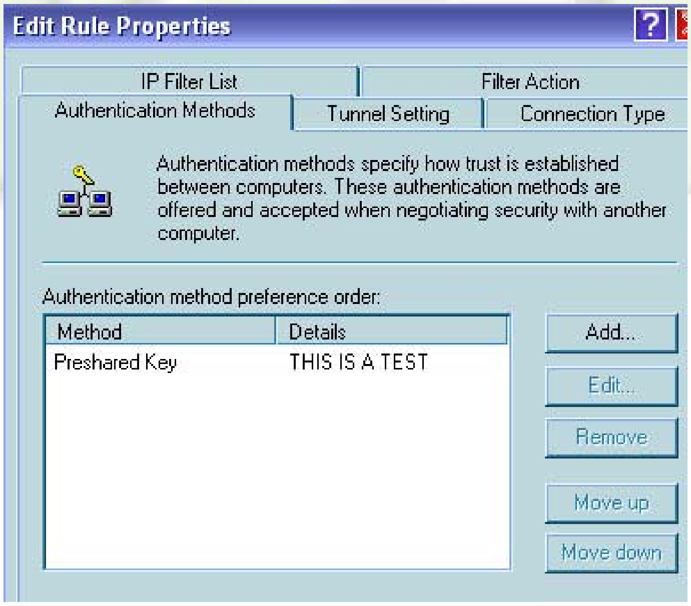
○ Active Directory default (Kerberos V5 protocol)

○ Use a certificate from this certification authority (CA):

● Use this string (preshared key):

THIS IS A TEST

Select the Use this string (preshared key) radio button, and type ‘THIS IS A TEST’ in the box as above and click OK.

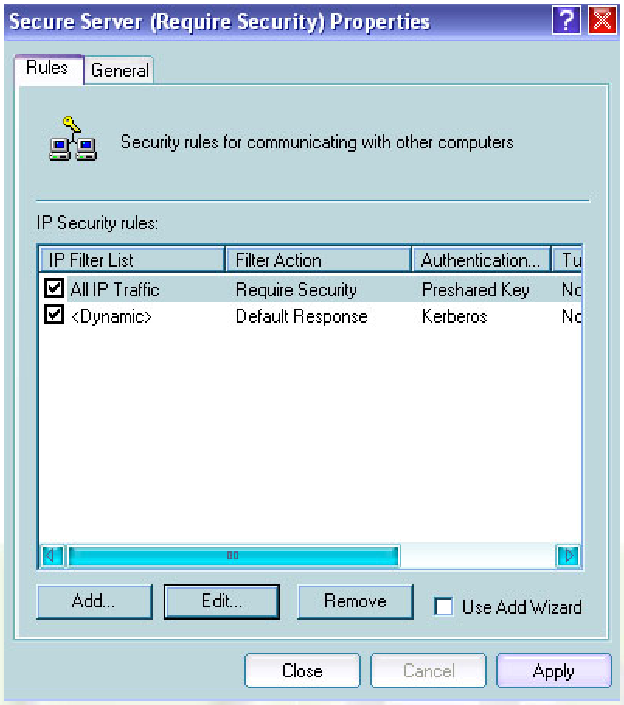

Edit Rule Properties

Authentication methods specify how trust is established between computers. These authentication methods are offered and accepted when negotiating security with another computer.

Authentication method preference order:

Method	Details
Preshared Key	THIS IS A TEST

When back at the Secure Server Properties box, click Apply and then OK.



Secure Server (Require Security) Properties

Security rules for communicating with other computers

IP Security rules:

IP Filter List	Filter Action	Authentication...	Tu
☑ All IP Traffic	Require Security	Preshared Key	Nc
☑ <Dynamic>	Default Response	Kerberos	Nc

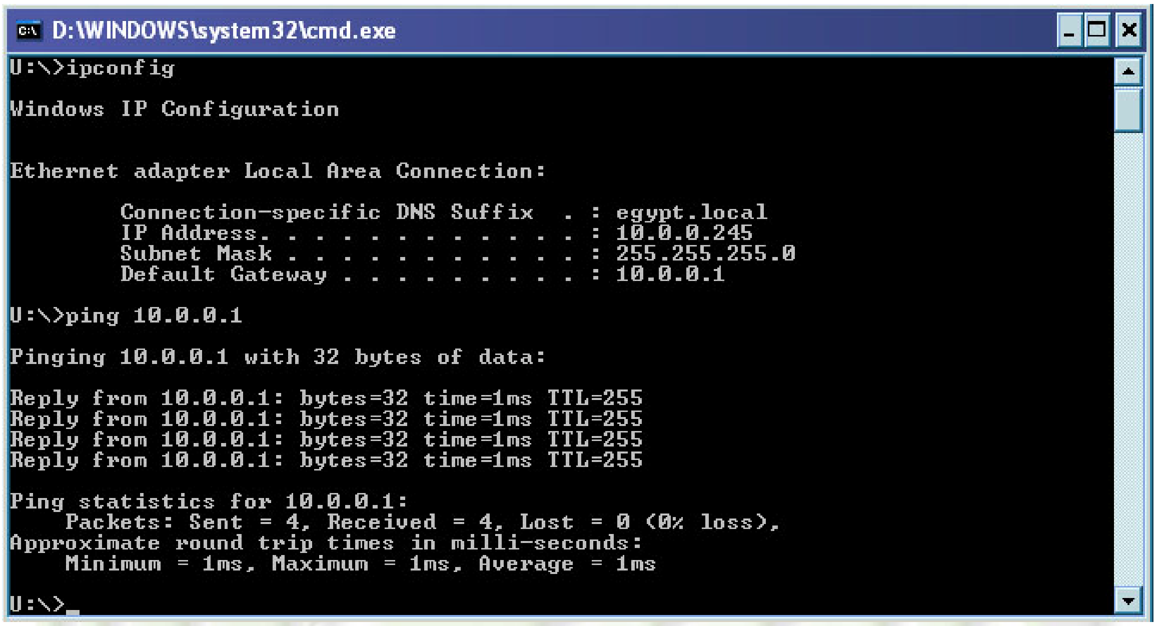
☐ Use Add Wizard

Step 3: Test IP connectivity

From START, Run, type ‘cmd’ in the run box, and click OK.

At the command prompt, type ‘ipconfig’ to view your current IP configuration. Note your IP address and Default gateway.

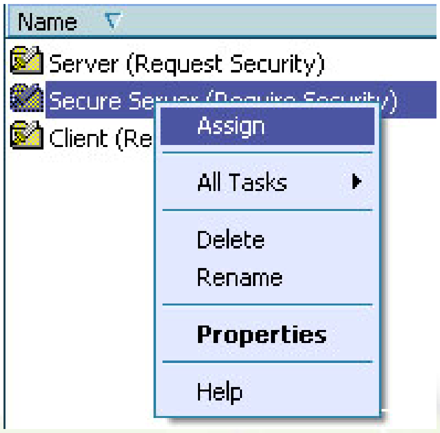
Next try to ping your default gateway, and your neighbor, by entering ‘ping x.x.x.x’ x.x.x.x being your default gateway, or neighbors IP address.



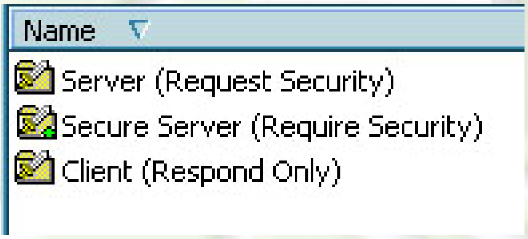
```
U:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : egypt.local
        IP Address. . . . . . . . . . . . : 10.0.0.245
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 10.0.0.1

U:\>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:

Reply from 10.0.0.1: bytes=32 time=1ms TTL=255
Reply from 10.0.0.1: bytes=32 time=1ms TTL=255
Reply from 10.0.0.1: bytes=32 time=1ms TTL=255
Reply from 10.0.0.1: bytes=32 time=1ms TTL=255

Ping statistics for 10.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

U:\>_
```

Step 4: Assign the IP Security Policy

From the Console Root, IP Security Policies on Local Computer, Right Click on the Secure Server (Require Security) Policy and choose Assign.



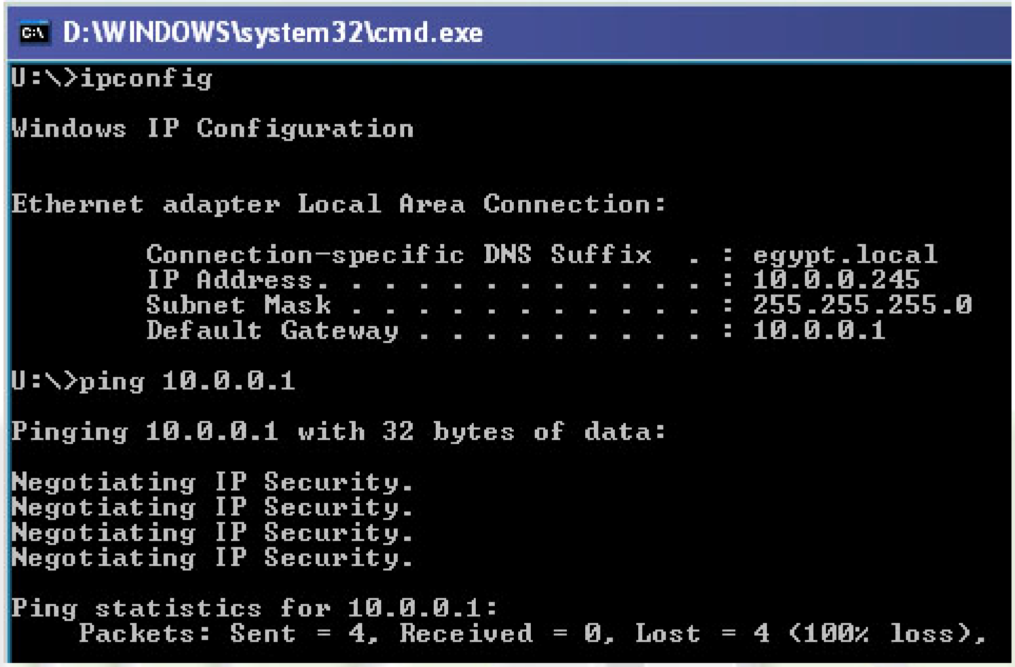
Once the policy is assigned, there will be a green circle on top of the icon, and it will show up as Yes on the Policy assigned column.



Step 5: Test IP connectivity with IPSec policy assigned

Repeat step 3 above.

You should see the following output…



```
U:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : egypt.local
        IP Address. . . . . . . . . . . . : 10.0.0.245
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 10.0.0.1

U:\>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:

Negotiating IP Security.
Negotiating IP Security.
Negotiating IP Security.
Negotiating IP Security.

Ping statistics for 10.0.0.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Step 6: Test IP connectivity with IPSec policy assigned to a neighbor computer (Windows XP to Windows XP)

1. Have your partner repeat steps 1 – 5 on their computer and then try to ping each other. Was the ping successful?

2. Unassign the IPSec Policy from one of the two computers and try to ping again. Was the ping successful?

Step 7: Modifying the Policy

1. With the same IP Security Policy from above assigned on both partner computers, change the Preshared key in step 2 to something different on both computers. Try to ping again. Was the ping successful?

2. Find or make a small text document that you can copy and paste as a new preshared key. Share the document with your partner, and you should both change your preshared keys, and test again.

(Note that policies need to be restored in order to once again connect to the Internet.)

Analysis

1) For which applications are IP Security Policies best suited?

2) After working with Windows IP Security Policies, what about IPSec do you feel you should study further? Why?

3) Why should you use IPSec in a public network environment?

Summary Discussion

A classroom discussion should follow the lab. Review the lab questions and your analyses as a group. Share your experiences and knowledge with the class.

Appendix:

The OS environment for this lab was Windows XP Professional, Version 2002, Service Pack 2 (8/04).