IP Security in Windows 2000: Step-by-Step

Timothy Rogers

IP Security in Windows 2000: Step-by-Step
Timothy J. Rogers
April 4, 2001

Overview of IPSec

Internet Protocol Security (IPSec) is a structure built of standards to provide secure communications and ensure privacy over Internet Protocol (IP) networks. IPSec is an Internet Engineering Task Force (IETF) standard defined in Requests for Comments (RFCs) 2401-2411. Based on the assumption that most networks are not secure, and thus require additional components to protect data as it travels over the wire, IPSec provides source authentication, integrity checking, and content confidentiality.

Authentication

One of the protocols IPSec uses is called the Authentication Header (AH). The AH contains a cryptographic checksum on the entire datagram and is inserted after the original IP header in the IPSec datagram. AH consists of:

- Next Header
  - The protocol number of the original IP header.
- Payload Length
  - The length of the Authentication Header.
- Security Parameter Index (SPI)
  - A 32-bit serial number that makes it possible to distinguish the Authentication Header connection from others to the same destination.
- Sequence Number
  - A serial number of the Authentication Header datagram that provides replay protection.
- Integrity Check Value (ICV)
  - A cryptographic integrity checksum of the AH datagram.

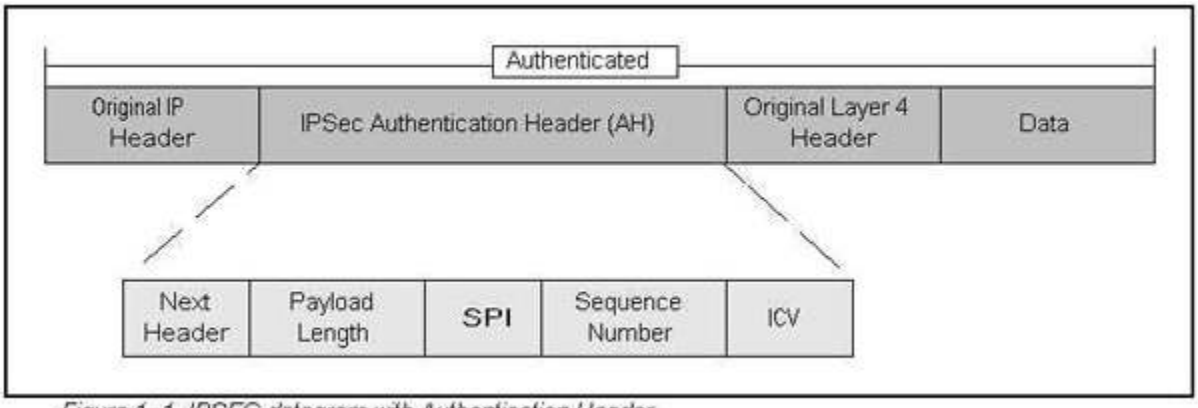

Figure 1 -1. IPSEC datagram with Authentication Header

The Authentication Header (AH) protects a network against three types of attacks:

- Replay Attacks, where a "non-friendly" person captures some packets, saves them for a future time, and then resends them. These types of attacks give an attacker the opportunity to impersonate a machine after that machine's no longer on the network. AH prevents replay attacks by adding a keyed hash to the packet, not allowing anyone else to retransmit that packet.
- Tampering. The keyed hash that IPSec uses, provides assurance that the contents of the packets have not been altered after it was sent.
- Spoofing. The AH protocol offers a two-way authentication, allowing the client and server to both verify each other's identity.

Confidentiality

The Authentication Header provides authentication against attacks. IPSec can also uses the Encapsulating Security Payload (ESP) protocol, to encrypt the data with a negotiated algorithm for confidentiality. The ESP protocol encrypts the

entire contents of each packet, though it does not provide any encryption or checksum on the IP header. The ESP header contains the following data:

- Security Parameter Index (SPI)
  - Identifies, when used in combination with the destination address and the security protocol (AH or ESP), the correct security association for the communication. The receiver uses this value to determine the security associations with which this should be identified.
- Sequence Number
  - Provides anti-replay protection for the SA. It is 32-bit, incrementally increasing number (starting from 1) that indicates the packet number sent over the security associations for the communication. The sequence number is never allowed to cycle. The receiver checks this field to verify that a packet for a security association with this number has not been received already. If one has been received, the packet is rejected.
- Padding
  - Alters the length of the data to match a multiple of the block size of the block cipher being used. 0 to 255 bytes.
- Pad Length
  - Then length of the padding field in bytes. This field is used by the receiver to discard the Padding field.
- Next Header
  - The protocol number of the original IP header. Used to identify the nature of the payload, such as TCP or UDP.

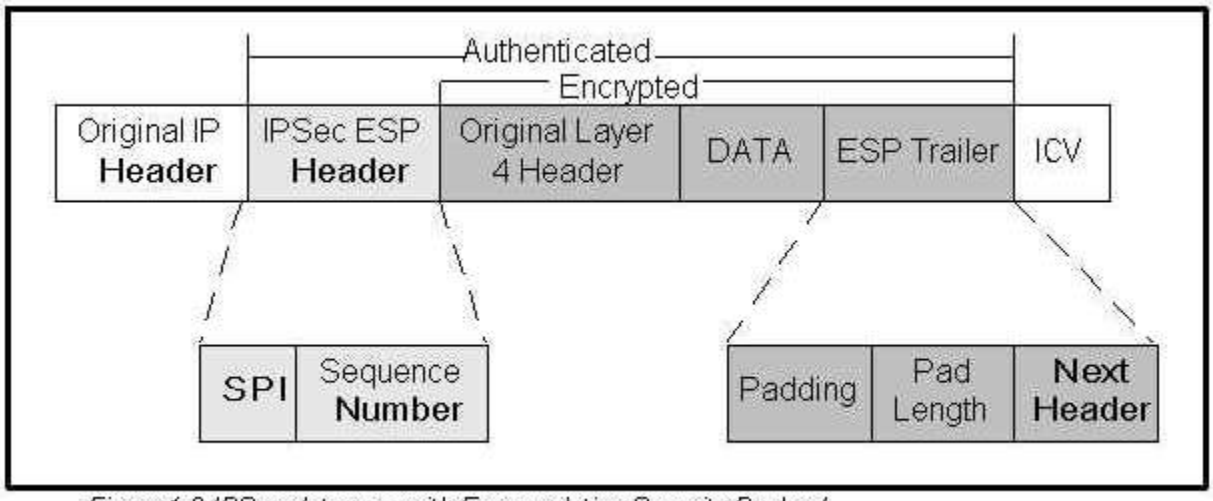

Figure 1-2 IPSec datagram with Encapsulating Security Payload

ESP is inserted after the IP header and before an upper layer protocol, such as TCP, UDP or ICMP, or before any other IPSec headers that have already been inserted. Everything following ESP (the upper layer protocol, the data, and the ESP trailer) is signed. The IP header is not signed, and therefore not necessarily protected from modification. The upper layer protocol information, the data, and the ESP trailer are encrypted.

IPSec Modes

Both protocols may be used in one of two modes, transport and tunnel modes. The operations of AH and ESP are not different based on the mode, the only change being that the data is signed for integrity purposes. There are four possible combinations of modes and protocol. AH may be used in Tunnel or Transport mode as well as ESP. AH is not used in tunnel mode in practice though, because AH protects the same data that transport mode protects.

- Transport Mode - In transport mode, AH and ESP protect the transport header. In this mode, AH and ESP intercept the packets flowing from the transport layer into the network layer and provide the configured security. The transport mode of IPSec can be used only when security is desired end to end.

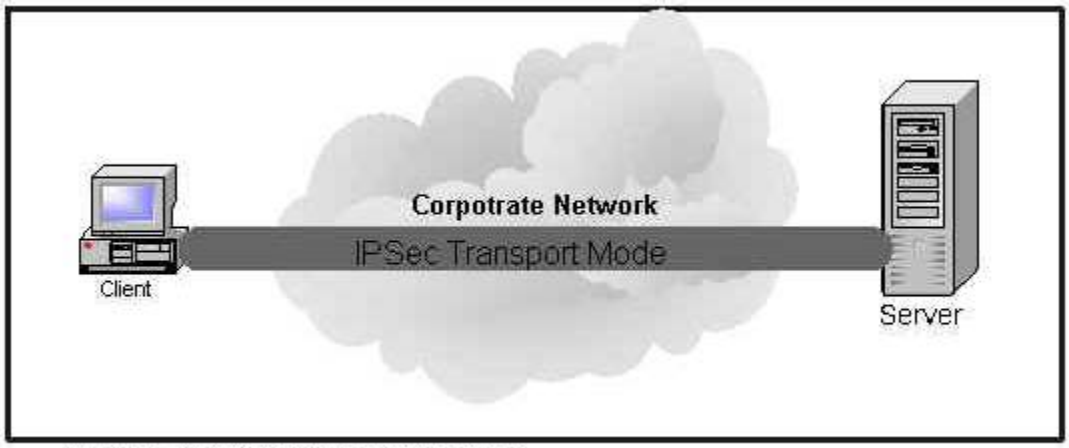

Figure 1 - 3 IPSec transport mode ESP

- Tunnel Mode - The tunnel mode is used in cases when security is provided by a device that did not originate packets - as in the case of VPNs - or when the packet needs to be secured to a destination that is different from the actual destination. The cryptographic endpoint is a security gateway providing security on behalf of another network. Figure 1 - 4 shows and edge-to-edge example of an IPSec Tunnel mode ESP.

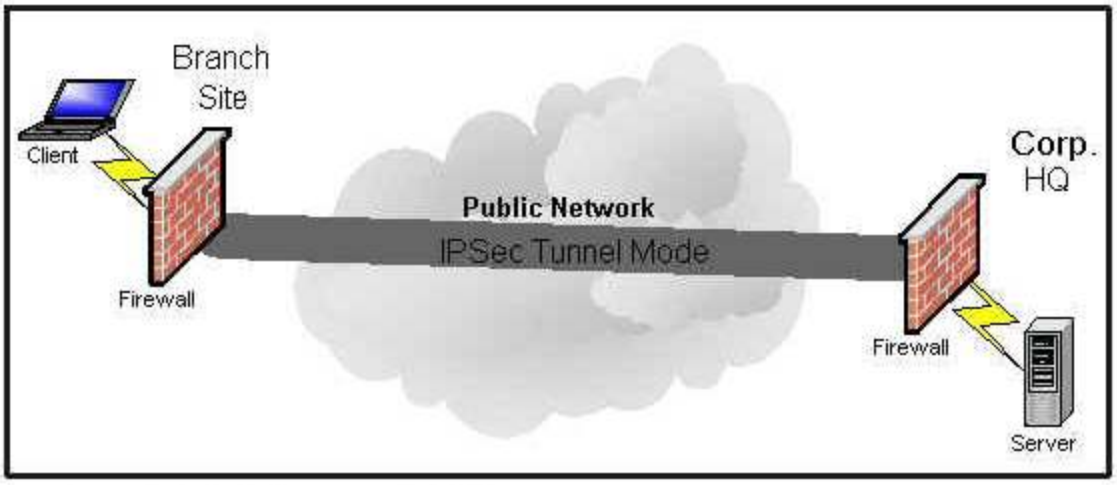

Figure 1 - 4 IPSec tunnel mode ESP

Within Windows 2000 SHA-1 and MD5 cryptographic checksums are available for use with AH. Windows 2000 also supports 56-bit DES and 3-DES for ESP as well as SHA-1 and MD5 for optional data integrity.
*3-DES is currently only available in the domestic versions of Windows 2000

Security Associations

Before two hosts may communicate using IPSec, they must authenticate each other as well as negotiate an encryption method. Hosts do this by establishing one or more Security Associations (SA). The Security Association may be thought of as an agreement between two hosts, based on the specific security settings to be used. The AH and the ESP can't share the same SA, typically in a bi-directional communications between two parties, two SAs are needed. Security Associations are stored on each IPSec computer in a specific database. Within the specific database the SA is identified by a Security Parameter Index (SPI) that can be found in every AH or ESP header.

Windows 2000 uses the Internet Key Exchange (IKE) protocol to establish the SAs needed. IKE handles the creation of SAs and generates the keys used to secure the information. Diffie-Hellman is used by IKE to generate and manage keys. This technique offers the ability to generate the symmetric keys used to encrypt and decrypt the data. IKE provides a secure channel for Diffie-Hellman to work by which is required.

Windows 2000 and IPSec

IPSec is fully supported within Windows 2000. Any Windows 2000 client may act as an IPSec client, and if it is member of

an Active Directory environment, IPSec policies can be defined to govern how network machines uses IPSec. Windows 2000 has several interesting components that are used when working with IPSec.

IPSec Driver

The IPSec driver is loaded during the Windows 2000 startup if an IP policy had been defined for that machine. The IPSec driver monitors all IP traffic and secures packets based on the requirements of the IPSec policy.

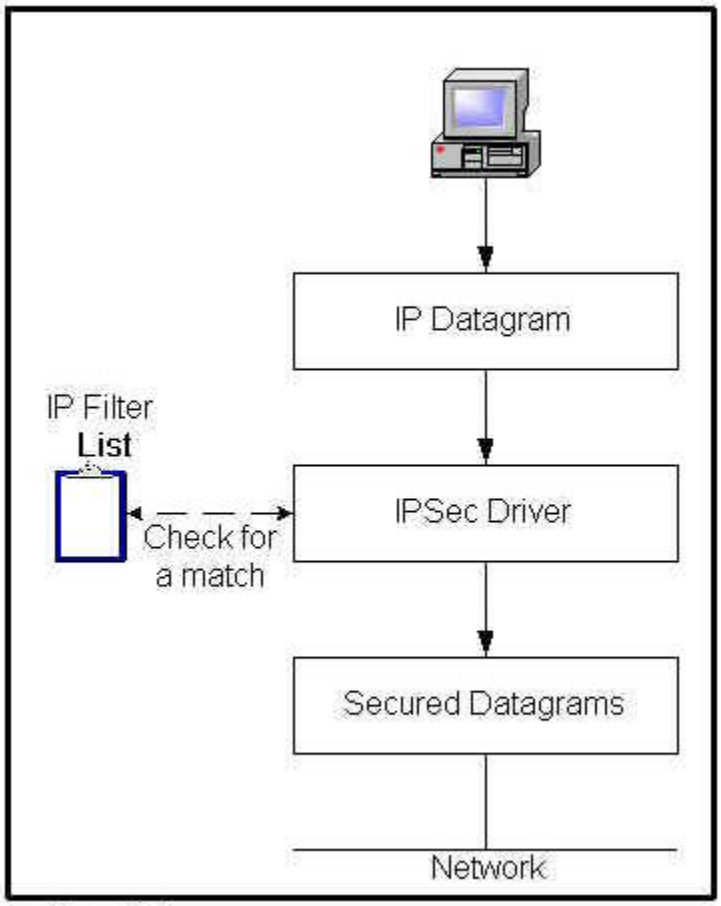

Figure 2 -1

The main responsibilities for the IPSec driver include:

- Examining each IP packet that arrives or leaves for a match to a specific IP policy filter.
- Requesting security associations for new connections.
- Using the method of authentication that is specified by the policy.
- Keeping the security associations up to date.

IPSec Policy Agent

The IPSec Policy Agent is a mechanism that resides on each Windows 2000 computer that appears in the list of system services. The Policy Agent retrieves the active IPSec policy information, and passes it to the other IPSec mechanisms, which require that information to perform security services. The Policy Agent starts automatically at system start time. If there are no active IPSec policies, or if the Policy Agent cannot connect to Active Directory for some reason, the Policy Agent will continue to poll Active Directory for an assigned policy, or check the registry for a locally-assigned policy. The IPSec Policy Agent controls the IPSec behavior. The Policy Agent looks for policies and delivers them to the IPSec driver.

Group Policy Objects (Active Directory)

IPSec policy can be applied to the GPO of an Active Directory object. This propagates that IPSec policy to any computer accounts affected by that Group Policy Object.

Windows 2000 Certificate Service

The Certificate Services deployed on a Windows 2000 Server is used to issue and manage certificates. Certificate Services for Windows 2000 supports two types of Certificate Authorities (Cas): enterprise and stand-alone CAs. Stand-alone CAs does not require Active Directory to function and they do not use certificate templates. The enterprise certificate authority integrates with Active Directory and use certificate templates.

IPSec Monitor

The IPSec Monitor provided by Windows 2000 is used to confirm whether the secured communications are successful. The monitor displays the active security associations on local or remote computers.

Setting up IPSec in Windows 2000

The following section is used to setup IPSec End-to-End communications between two Windows 2000 Clients. Both of the Windows 2000 clients should be members of a Windows 2000 domain, which uses Kerberos as the initial authentication method.

Build a Custom Console

The Microsoft Management Console is a tool used to create, save, and open collections of administrative tools, called consoles. Consoles contain items such as snap-ins, extension snap-ins, monitor controls, tasks, wizards, and documentation required to manage many of the hardware, software, and networking components of your Windows 2000 system. You can add items to an existing MMC console, or you can create new consoles and configure them to administer a specific system component.

Using the Microsoft Management Console (MMC), a custom console can be created with the components that will be needed for setting up and using IPSec Policies.

1. At the Windows desktop click on Start, then Run. In the Open textbox type MMC then click OK.

2. When the Console opens select the Console menu, click Add/Remove Snap-in.

3. Using the Add/Remove Snap-in dialog box, click Add

4. Management, and then click Add.

Figure 3-1 Add Standalone Snap-in

5. Making sure that Local Computer is selected, click Finish.

6. Using the Add Standalone Snap-in dialog box, click Group Policy, then click Add.

7. Making sure that Local Computer is selected, click Finish.

8. Using the Add Standalone Snap-in dialog box, click Certificates, then click Add.

9. Select Computer Account, then click Next.

10. Making sure that Local Computer is selected, click Finish.

11. Close the Add Standalone Snap-in dialog box

12. Close the Add/Remove Snap-in dialog box by clicking OK.

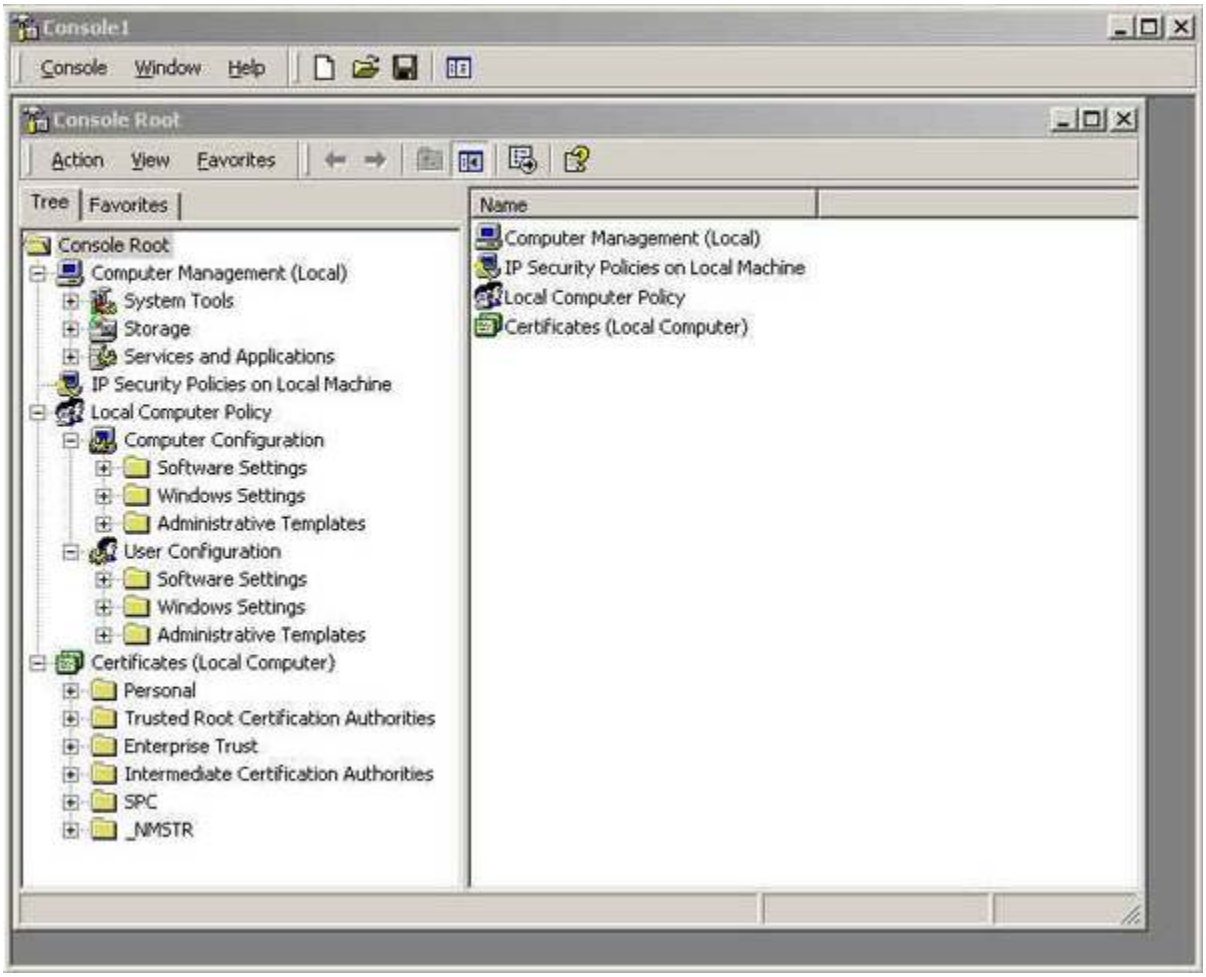

Figure 3-2 MMC custom console

Using the Audit Policy

Auditing should be enabled to track successful and unsuccessful IPSec sessions.

1. Using the MMC custom console created previously (see Figure 3-2). Navigate from Local Computer Policy, Computer Configuration, Windows Settings, Security Settings, Local Polices and then Audit Policy

2. In the right pane of the MCC select Audit Logon Events by double clicking on it.

3. Within the Audit Logon Events dialog box, select both Success and Failure check boxes, then OK

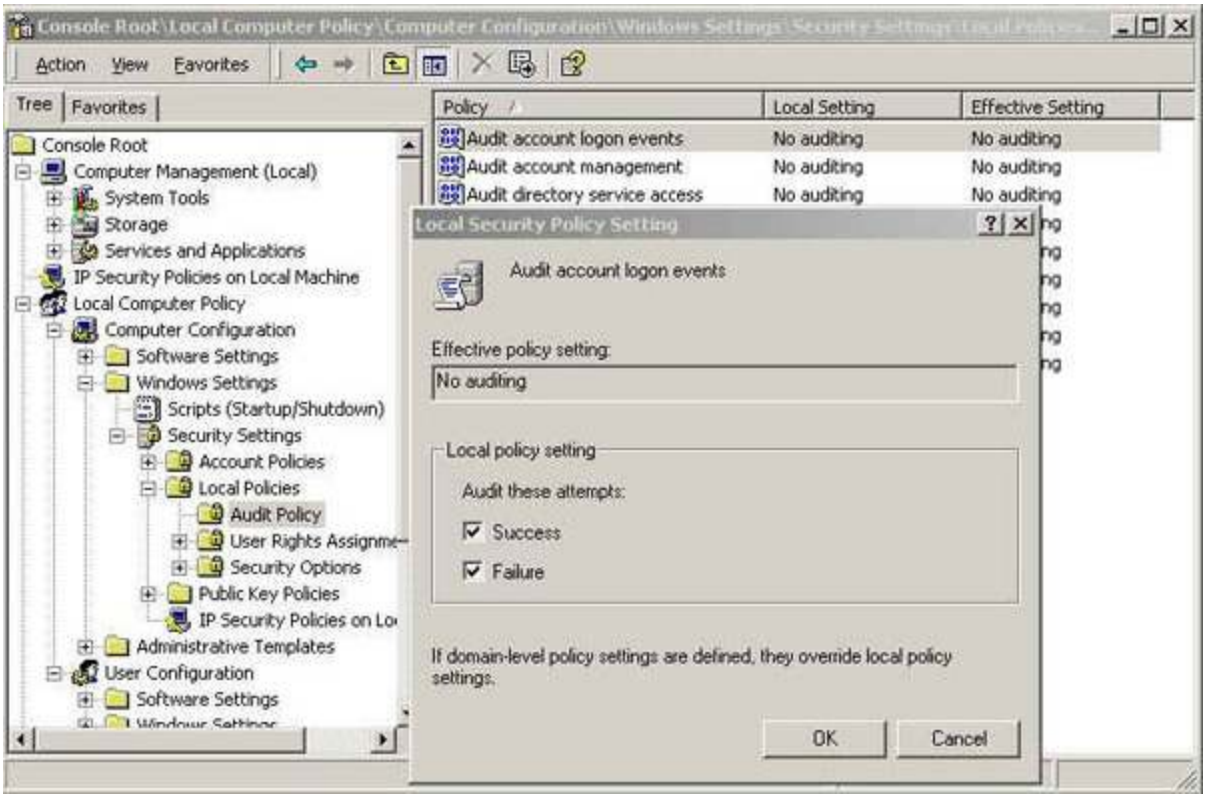

Figure 3-3 Audit policy

4. In the right pane of the MCC select Audit Object Access by double clicking on it.

5. Within the Audit Object Access dialog box, select both Success and Failure check boxes, then OK

Built-in IPSec Policies

Windows 2000 comes with built-in policies for IPSec secure communications. Computers within a Windows 2000 domain with little effort can use these policies. The predefined Windows 2000 policies include: Client, Secure Server and Server defined as follows:

- Client (Respond Only) allows the client to respond to other computers requesting security according to the settings in the default response rule. With this policy active, the client will never request security, but will negotiate IPSec based on the connecting host.
- Secure Server (Require Security) allows the server to require IPSec negotiation prior to allowing a connection. This policy will allow unsecured incoming communications, but outgoing traffic will always be secured.
- Server (Request Security) allows the server to request IPSec negotiation, but will allow unsecured communications if the other computer is not IPSec aware.

Setting Up

1. Open the MMC custom console used earlier (Figure 3-2). Select IP Security Policies on Local Machine found in the left pane.

2. Right-click Secure Server on the right pane, and select Assign. This will change the Policy Assigned column from No to Yes.

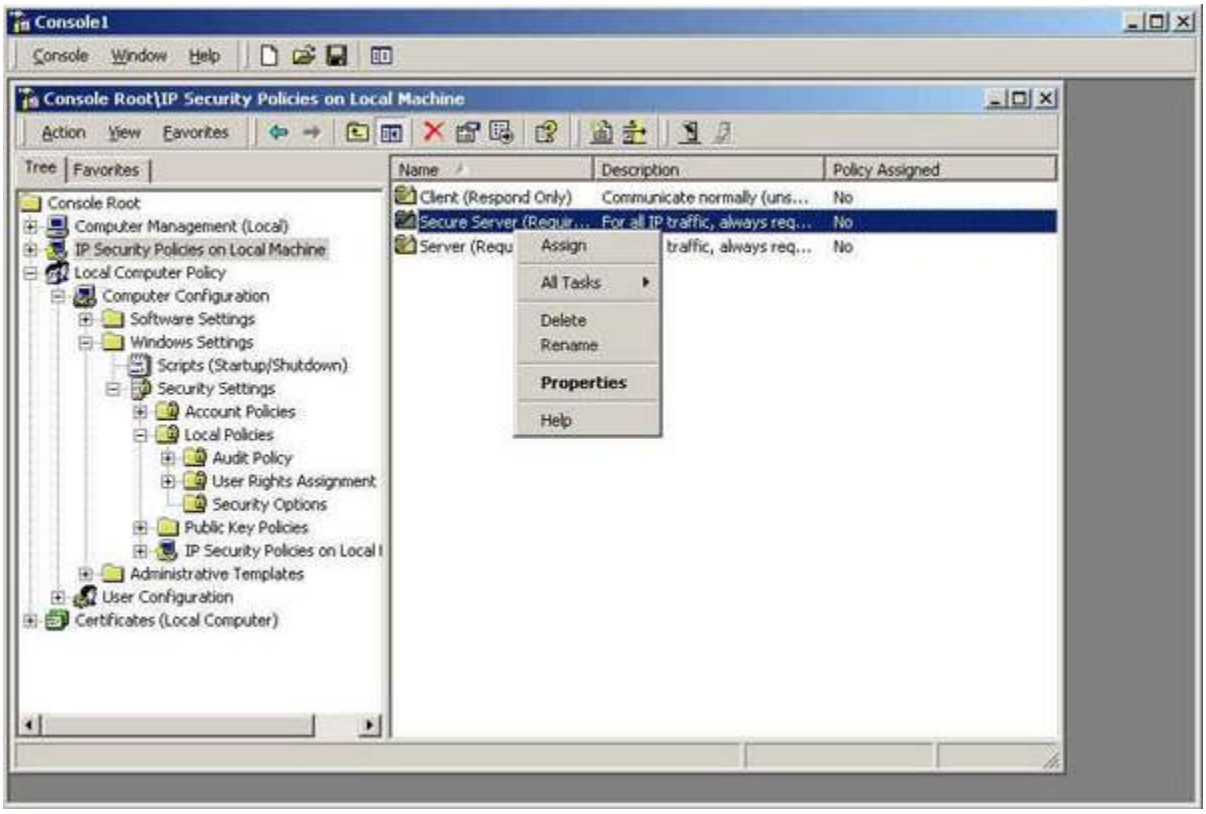

Figure 3-4 IPSec Secure Server Policy

3. On the client computer (assuming a MMC custom console has been setup identical to the server computer) open the MMC custom console select IP Security Policies on Local Machine found in the left pane.

4. Right-click client on the right pane, and select Assign. This will change the Policy Assigned column from No to Yes. (Refer to Figure 3-4)

The previous steps enable one computer as a secure server and another computer as a secure client residing within the Windows 2000 domain. At this point the client will start to send unprotected ICMP Echo packets to the server, and the server will request security from the client. Once a connection is established the rest of the communications will be secure. If both computers were setup with client policies, neither would send secured data, because neither side would request security.

Testing the Secure Connection (Built-in IPSec Policy)

1. Using the computer setup as the client, click on Start, then Run. In the Run text box, type cmd for the Command Prompt.

2. In the Command window issue the ping command followed by the IP address of the Server Computer. (Figure 3-5)

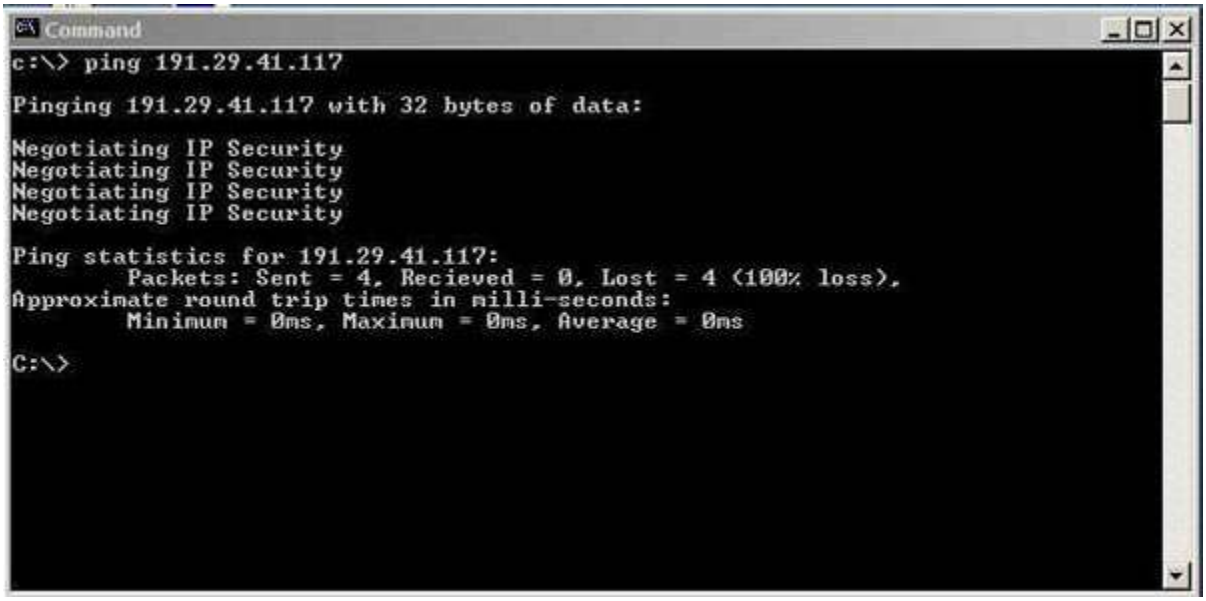

Figure 3-5 Ping the computer setup as server

3. Notice the ping response indicating that IPSec is being negotiated.

4. Repeating the ping command to the server computer will know that the IPSec security associations have been established, should show four successful replies similar to:

Reply from 191.29.41.117: bytes=32 time<10ms TTL=128
Reply from 191.29.41.117: bytes=32 time<10ms TTL=128
Reply from 191.29.41.117: bytes=32 time<10ms TTL=128
Reply from 191.29.41.117: bytes=32 time<10ms TTL=128

5. Using the MMC on the client computer, locate on the left pane Computer Management and expand it.

6. Expand System Tools, Event Viewer, and click Security Log. Double click on the top instance of Success Audit in the right pane.

7. The log should show the successful establishment of an IPSec Security Association (SA). The log should look similar to the following:

IKE security association established
Mode:
Data Protected Mode (Quick Mode)

Peer Identity:
Kerberos based Identity: C0092828@domain.com
Peer IP Address: 191.29.41.117

Filter:
Source IP Address 191.29.213.14
Source IP Address Mask 255.255.0.0
Destination IP Address 191.29.41.117
Destination IP Address Mask 255.255.0.0
Protocol 0
Source Port 0
Destination Port 0

Parameter:
ESP Algorithm DES CBC
HMAC Algorithm SHA
AH Algorithm None

Encapsulation Transport Mode
InboundSpi <long number>2217628991
OutboundSpi <long number>9656722734
Lifetime (sec) 900
Lifetime (kb) 100000

Using the IP Security Monitor

The IP Security Monitor is an application that comes with Windows 2000 to monitor the successful security connections that the IPSec policy has created.

1. To open Security Monitor tool on the computer setup as the client, click on Start, Run. In the Open Text box type ipsecmon and click OK

2. Click on the Options button on the right side, and change the default value for Refresh Seconds from 15 to 1. Click OK. (Figure 3-6)

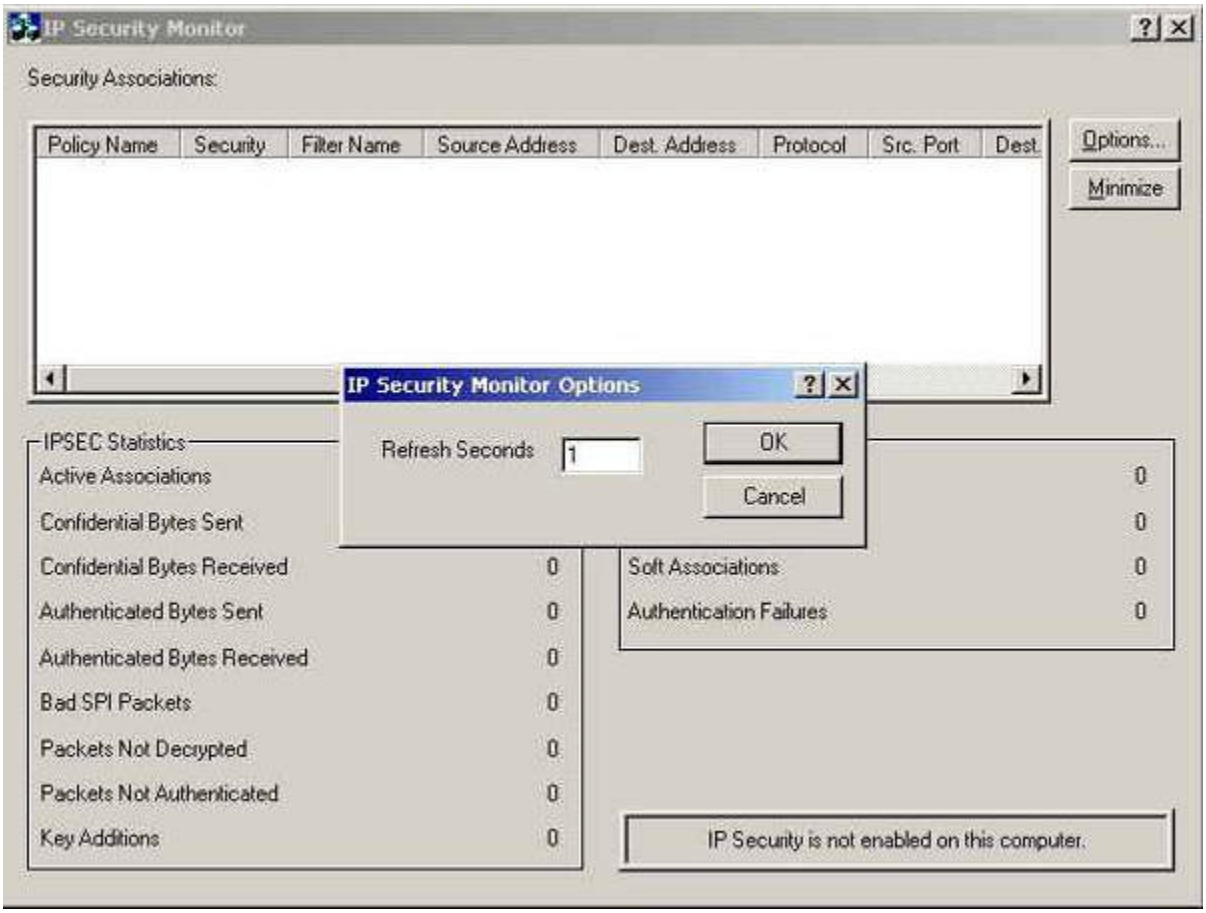

Figure 3-6 ipsecmon

3. Re-issue the ping command from the secure client to the secure server as done in steps 3 and 4 above.

4. Looking at the ipsecmon, it should show details of the Security Associations that are currently in use between the secure client and server machines.

Now the two machines have successfully been configured and are using IPSec between them with a built-in IPSec Policy.

Creating a Custom IPSec Policy

For secured traffic between two computers that are not members of the domain, a custom policy needs to be created. Built-in policies that come with Windows 2000 require Kerberos authentication provided by the domain controller. Another reason to create a custom policy would be if you wanted to secure traffic based on a machines network address.

1. Open the MMC on the machine previously used as the client. Right click on IP Security Policies on Local Machine, and then click Create IP Security Policy. This will start up the IP Security Policy Wizard. (Figure 3-7)

Figure 3-7 IP Security Policy Wizard

2. Click Next in the IP Security Policy Wizard

3. The next frame asks for a name and description of the policy. Type in "a name" for the policy.

4. Uncheck the Activate the default response rule box, and then click Next.

5. Leave the Edit Properties check box selected and click Finish.

6. A Properties box for the policy just created is displayed. Make sure the Use Add Wizard at the bottom right of the frame is selected.

7. Click Add at the bottom of the Policy Properties box to start the Security Rule Wizard. (Figure 3-8)

Figure 3-8 Security Rule Wizard

8. Click Next in the Security Rule Wizard.

9. Select the radio button for "This rule does not specify a tunnel", and then click Next.

10. Select "All network connections", and click "Next" in the next frame.

11. The next frame asks for the Authentication Method that will be used. This may be whatever is setup for the domain the computers exist on. For simplicity select the radio button: "Use this string to protect the key exchange (preshared key)".

12. Enter "a string" that will be used as the preshared key in the text box, a blank string may not be used, then click Next.

13. The next frame is for the IP Filter List. There should be two predefined filter, All ICMP Traffic and All IP Traffic in the list already. Click the Add button on the right side to create a new filter.

14. A new window will be displayed with the title IP Filter List (Figure 3-9) with and empty list of filters. In the Name text box type in "a name" for the filter.

15. Make sure the Use Add Wizard check box is selected, found below the remove button. (Figure 3-9)

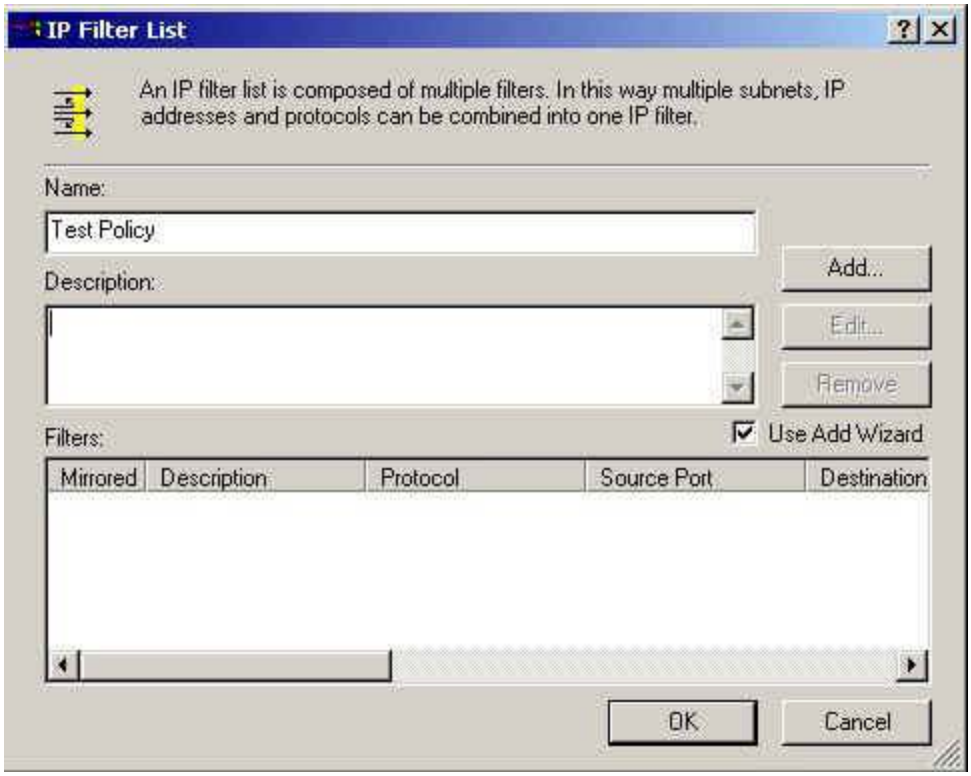

Figure 3-9 IP Filter List

16. Click Add in the IP Filter List window to start the IP Filter Wizard.

17. Click Next in the IP Filter Wizard.

18. Make sure the Source address pull down says My IP Address, and click Next.

19. Select A specific IP Address from the Destination address pull down. Enter the IP Address of the machine setup as a server earlier and click Next.

20. Select Any for protocol type from the pull down, then click Next.

21. Click Finish and make sure the Edit Properties check box is cleared.

22. Click on Close to leave the IP Filter List dialog box.

23. The Filter that was just created should now be in the IP filter lists of the Security Rule Wizard. (Figure 3-10)

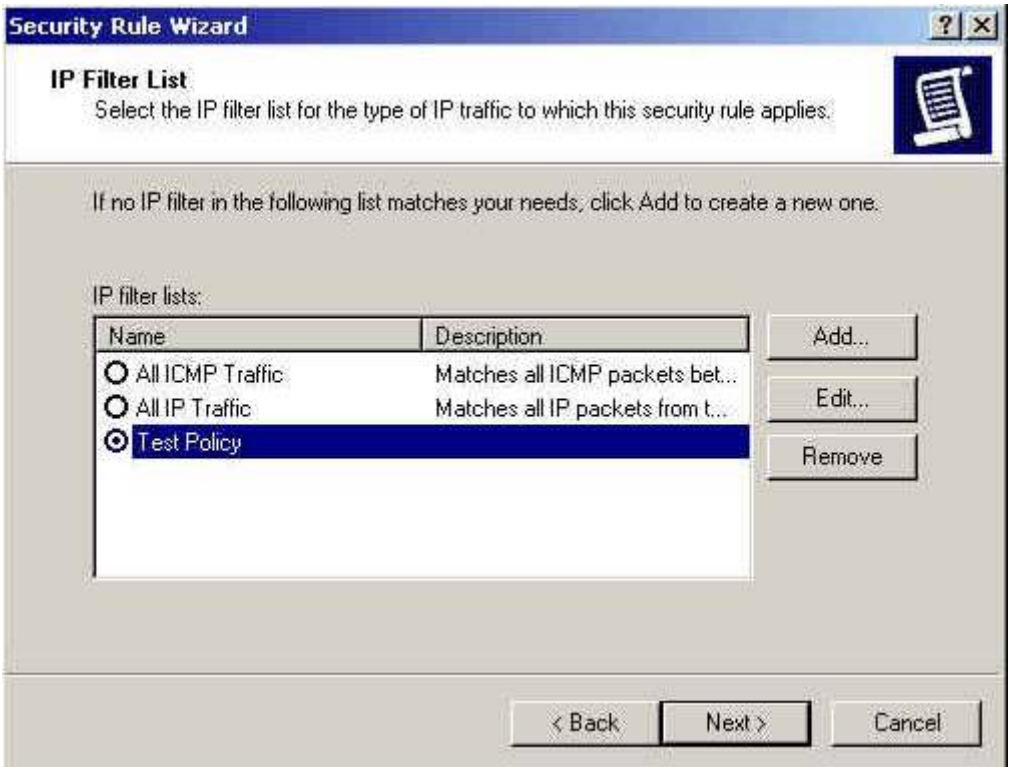

Figure 3-10 Security Rule Wizard with new filter added

24. Select the new filter, just created above and click Next.

25. In the next frame of the Security Rule Wizard make sure to select the Use Add Wizard check box, and then click Add.

26. Another Wizard will pop-up, the Filter Action Wizard, and click Next.

27. Enter "a name" for the filter action in the Name text box, and click Next.

28. Select Negotiate security radio button for the Filter Action General Options, and click Next.

29. Select Do not communicate with computers that do not support IPSec in the Communicating with computers that do not support IPSec frame, and click Next.

30. In the IP Traffic Security frame, select Medium (Authenticated Header) from the list of security methods, and click Next.

31. Make sure the Edit properties check box is cleared and click Finish to close the Filter Action Wizard.

32. In the Filter Action frame of the Security Rule Wizard, click the radio button next to the filter just created in the steps above (Figure 3-11), and then click Next.

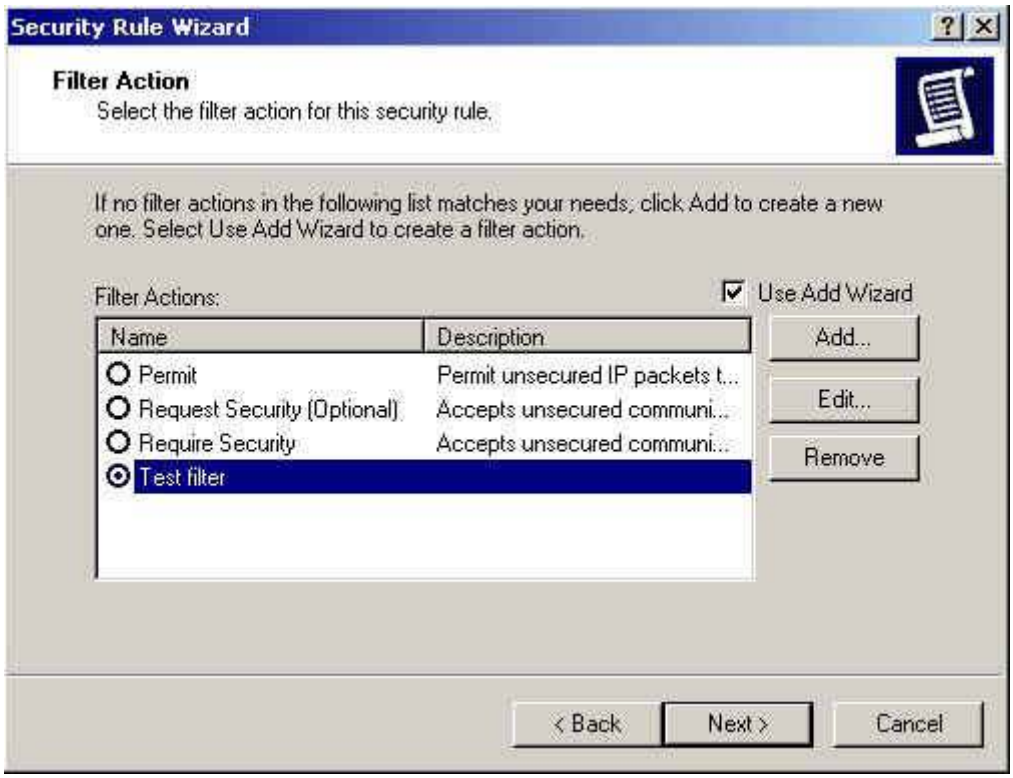

Figure 3-11 Filter Action Frame with new filter

33. Click Finish and, make sure the Edit properties check box is unchecked.

34. All of the items defined above are now visible in the IP Security Rules: section of the Properties Window. Click Close to finish with the policy.

35. Using the server computer from earlier, repeat the preceding steps.

The above steps involve setting up a complete custom IPSec policy for Windows 2000. It is important to understand what is being done to understand how to create more policies.

In Steps 11 and 12 is the configuration for the IKE Authentication Method. This is used to specify how the computers will trust each other, by specifying how they will authenticate themselves when trying to establish a security association. IKE for Windows 2000 provides three authentication methods to establish trust between computers. These are Kerberos v5 authentication, public/private key signatures using certificates and a preshared key.

Steps 13 through 22 are used to configure an IPSec filter list. IP Security is applied to IP packets as they are sent and received. These packets are matched against filters when being sent out to see if they should be secured, blocked, or passed through in clear text. Packets are also matched when received to see if they should be blocked, or permitted into the system. There are two types of filters used, those for IPSec transport mode security and IPSec tunnel mode security. IPSec tunnel filters are applied to all packets first, and if there is no match then IPSec transport mode filters are searched. When configuring IP filters for traffic that must be secured, always be sure to mirror the filters. Mirroring the filters automatically configures both inbound and outbound filters.

Filter Actions are configured in steps 26 through 31. Filter Actions are used to configure the action to be taken on the Filter List that was created in steps 13 - 22. Filters Actions are setup to permit, block or secure the packets that match the filters created. In order to have secure traffic, the computers that will communicate must have a compatible negotiation policy configured. There are two methods that allow communication with computers that are not able to do IPSec. A Filter Action Permit is used to let packets go in the clear, or a Filter Action can be configured to use the setting Fall back to unsecured communication.

Testing the Secure Connection (Custom IPSec Policy)

1. Using the MMC custom console, select IP Security Policies on Local Machine.

2. Right click on the policy created above and then click Assign from the menu.

3. Notice the value for the status of Policy Assigned is now, Yes. Repeat steps 1 and 2 on the second computer.

4. Open up ipsecmon as mentioned in an earlier procedure. Minimize this window.

5. Open a Command window by going to Start, then Run, and typing cmd in the Run text box.

6. Issue the ping command from computer 1 to computer 2. The ping command should reply with four Negotiating IP Security responses.

7. Repeat the ping command from the same command window. This time ping should reply with four successful ping replies. Now the two computers have established IPSec Security Associations between them.

8. Restore the IP Security Monitor windows. The details of the Security Association between the two computers should be visible.

9. Using the MMC window, select Computer Management from the left pane. Expand to System Tools, Event Viewer, and then select Security. The security log should be showing an event 541, which is for the establishment of an IP Security Association.

10. Using the MMC custom console, select IP Security Policies on Local Machine.

11. Right click on the policy created above and then click Un-Assign from the menu.

12. Notice the value for the status of Policy Assigned is now, No. Repeat steps 1 and 2 on the second computer

Windows 2000 IPSec Tools

IPSec snap-in for policy configuration

Internet Protocol Security Policy Management is used to create and configure IPSec policies through the Microsoft Management Console (MMC). It can manage policy centrally (for Active Directory clients), manage policy locally (the computer on which you are running the snap-in), or manage policy remotely for a computer or domain.

You must add the snap-in to the MMC. A wizard guides you through the correct snap-in configuration. The customized console can then be saved so that it is available to you again at any time.

IPSecmon.exe monitor to show active state

IPSecMon is the IP Security Monitor, which is distributed with Windows 2000. It is a Windows GUI tool used to confirm whether IPSec communications are successful. By displaying active security associations for local or remote computers, a user can quickly confirm if their connection is using IPSec. To activate the IP Security Monitor open the start menu then click Run, and type ipsecmon <computer name> .

Network Connections UI IPSec property

The Network Connections UI IPSec property is an advanced window found within the properties of an Internet Protocol (TCP/IP) connection setting. The IPSec property can be found by:

- Open My Network Places from the Windows Desktop
- Select a network connection that uses the Internet Protocol
- Click on Properties for the Internet Protocol
- At the bottom right of the General tab window click on Advanced
- Select Options tab in the Advanced TCP/IP Settings Window
- Select IP security from the Optional settings and click the Properties button found at the lower right of the settings text-box.

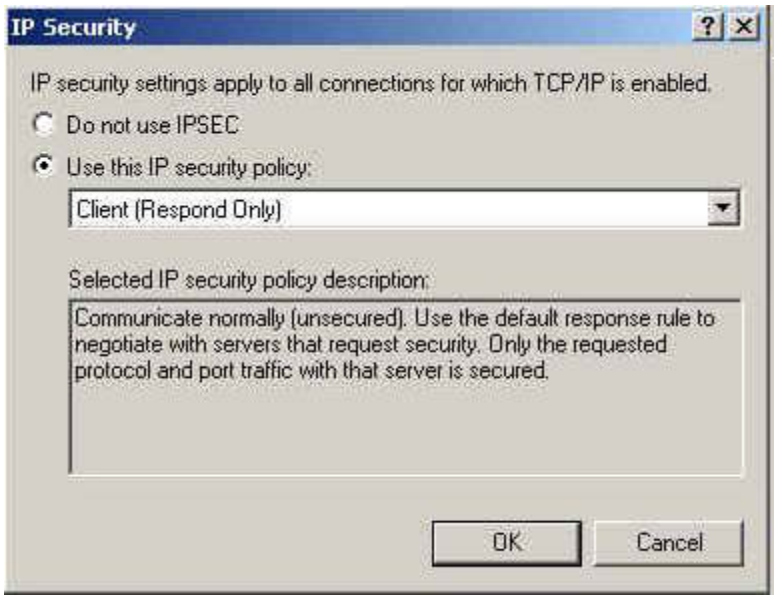

Figure ?-? IP Security Property

The IPSec Properties window allows a user to specify if they do or do not want the machine to use Internet Protocol security (IPSec) to provide authentication, integrity, and confidentiality services for data sent from this connection. If IPSec is to be used a policy needs to be selected from the pull-down policy list.

Ipsecpol.exe Internet Security Policies Tool

The Internet Security Policies Tools is an application found in the Microsoft Windows 2000 Resource Kit. Ipsecpol is a command-line tool that is used to configure IPSec policies found either in the directory service or in a local or remote registry. Ipsecpol has all of the features found in the IPSec Snap-in policy configuration tool for MMC.
Ipsecpol is useful if there is a large and/or complex IPSec policy that needs to be configured. Ipsecpol can help by providing a scriptable way to create a policy by putting Ipsecpol commands into a batch file. Ipsecpol can also provide just-in-time policies with its batch ability. If a user needs a secured channel with a server, an administrator can simply send the user the tool binaries and the command line or batch file to run.

References:

Microsoft Corp. Microsoft Windows 2000 Professional Resource Kit: Chapter 13 Security. Redmond, WA: Microsoft Press, 2000.

Microsoft Corp. Microsoft Windows 2000 Server Resource Kit Distributed Systems Guide. Redmond, WA: Microsoft Press, 2000.

Microsoft Corp. Microsoft Windows 2000 Server Resource Kit Planning Distributed Security. Redmond, WA: Microsoft Press, 2000.

Microsoft Corp. Microsoft Windows 2000 Server Resource Kit TCP/IP Core Networking Guide. Redmond, WA: Microsoft Press, 2000.

Microsoft Corp. Microsoft Windows 2000 Server Resource Kit Deployment Planning Guide. Redmond, WA: Microsoft Press, 2000.

Microsoft TechNet: Step-by-Step Guide to Internet Protocol Security (IPSec), www.microsoft.com/TechNet/win2000/win2ksrv/technote/ispstep.asp?a=printable, 2/2000.

RFC 2401: Security Architecture for the Internet Protocol.

RFC 2402: IP Authentication Header (AH).

RFC 2406: IP Encapsulating Security Payload (ESP).

Doraswamy, Naganand and Harkins, Dan: IPSec, Prentice Hall, 2000.

Norbeg, Stefan. Securing Windows NT/2000 Servers for the Internet, O'Reilly & Associates, Inc. 2001

Rhine, Joanie. Microsoft TechNet: IP Security for Local Communications Systems, www.microsoft.com/TechNet/security/ipsecloc.asp?a=printable, 2000 .