

Internet Protocol Security (IPSec)

Introduction

Internet Protocol Security (IPSec) provides application-transparent encryption services for IP network traffic as well as other network access protections for the Windows® 2000 operating system.

This guide focuses on the fastest way to use IPSec transport mode to secure application traffic between a client and a server. It demonstrates how to enable security using IPSec default policies between two Windows 2000-based systems that belong to a Windows 2000 domain. Once the two computers have joined the domain, you should complete the first part of the walkthrough, which demonstrates default policies in 30 minutes or less. Notes are included on how to enable non-IPSec clients to communicate to the server. Steps are provided on how to use certificates, and how to build your own custom policy for further interoperability testing, or to demonstrate IPSec when a Windows 2000 domain is not available.

Using Internet Protocol Security (IPSec), you can provide data privacy, integrity, authenticity, and anti-replay protection for network traffic in the following scenarios:

- Provide for end-to-end security from client-to-server, server-to-server, and client-to-client using IPSec transport mode.

- Secure remote access from client-to-gateway over the Internet using Layer Two Tunneling Protocol (L2TP) secured by IPSec.

IPSec provides secure gateway-to-gateway connections across outsourced private wide area network (WAN) or Internet-based connections using L2TP/IPSec tunnels or pure IPSec tunnel mode. IPSec tunnel mode is not designed to be used for virtual private network (VPN) remote access. The Windows® 2000 Server operating system simplifies deployment and management of network security with Windows 2000 IP Security, a robust implementation of IP Security (IPSec). Designed by the Internet Engineering Task Force (IETF) as the security architecture for the Internet Protocol (IP), IPSec defines IP packet formats and related infrastructure to provide end-to-end strong authentication, integrity, anti-replay, and (optionally) confidentiality for network traffic. An on-demand security negotiation and automatic key management service is also provided using the IETF-defined Internet Key Exchange (IKE), RFC 2409. IPSec and related services in Windows 2000 have been jointly developed by Microsoft and Cisco Systems, Inc.

Windows 2000 IP Security builds upon the IETF IPSec architecture by integrating with Windows 2000 domains and the Active Directory™ services. Active Directory delivers policy-based, directory-enabled networking using Group Policy to provide IPSec policy assignment and distribution to Windows 2000 domain members.

The implementation of IKE provides three IETF standards-based authentication methods to establish trust between computers:

- Kerberos v5.0 authentication provided by the Windows 2000-based domain infrastructure, used to deploy secure communications between computers in a domain or across trusted domains.
- Public/Private Key signatures using certificates, compatible with several certificate systems, including Microsoft, Entrust, VeriSign, and Netscape.
- Passwords, termed *pre-shared authentication keys*, used strictly for establishing trust—not for application data packet protection.

Once peer computers have authenticated each other, they generate bulk encryption keys for the purpose of encrypting application data packets. These keys are known only to the two computers, so their data is very well protected against modification or interpretation by attackers who may be in the network. Each peer uses IKE to negotiate what type and strength of keys to use, as well as what type of security with which to protect the application traffic. These keys are automatically refreshed

according to IPSec policy settings to provide constant protection under the administrator's control.

Scenarios for Using IPSec End to End

Internet Protocol Security (IPSec) in Windows 2000 is designed to be deployed by network administrators so that users' application data can be transparently secured. In all cases, using Kerberos authentication and domain trusts is the easiest choice for deployment. Certificates or pre-shared keys can be used for untrusted domain or third-party interoperability. You can use Group Policy to deliver the IPSec configuration, called an *IPSec policy*, to many clients and servers.

Secure Servers

IPSec security for all unicast IP traffic is either *requested but optional*, or *requested and required*, as established by the administrator's configuration of the server. Using this model, clients need only a default policy for how to respond to security requests from servers. Once IPSec security associations (one in each direction) are established between the client and server, they remain in effect for 1 hour after the last packet was sent between them. After that hour, the client cleans up the security associations and return to the initial "respond only" state. If the client sends unsecured packets to the same server again, the server will re-establish IPSec security. This is the easiest approach to take, and can be done safely as long as the first packets sent to the server by the application do not contain sensitive data, and as long as the server is permitted to receive unsecured, clear text packets from clients.

Caution: *This server-side configuration is appropriate for internal network servers ONLY, because the server is configured by IPSec policy to allow incoming, clear text, unsecured packets. If the server is placed on the Internet, then it must NOT have this configuration because of the opportunity for denial of service attacks that take advantage of the server's ability to receive incoming unsecured packets.*

Lockdown Servers

If the server is directly accessible from the Internet, or if the first client packets contain sensitive data, then the client must receive an IPSec policy so that it requests IPSec security for traffic when it attempts to send data to the server. This walk-through will not demonstrate this configuration, but it can be easily enabled using the steps explained in the section [Configure an IPSec Filter Action](#).

Clients and servers can have specific rules for permitting, blocking, or securing only certain network packets (protocol or port specific). This approach is more difficult to configure and prone to error because it requires in-depth knowledge of the type of network traffic that an application sends and receives, and administrative coordination to be sure that all clients and servers have compatible policy.

Prerequisites

This guide is designed as a lab for network and system administrators to gain understanding and knowledge of how Windows 2000 IPSec works. You can configure an IP security policy locally on each computer, and then implement this policy and test the results to see secure network communications.

To complete this walkthrough, you need the following hardware:

- Two computers running the Windows 2000 operating system. You can use two Windows 2000 Professional systems as the domain members, one to act as a client and the other as a server in the IPSec sense. The two test systems must be members of the same (or a trusted) domain.
- A Windows 2000 Server domain controller.
- A LAN or WAN to connect these three computers.

The common infrastructure assumed in this guide is covered in the "Step-by-Step Guide to a Common Infrastructure for Windows 2000 Server Deployment" ([Part 1](#) and [Part 2](#)). If you are not using the common infrastructure, you need to make the appropriate changes to this set of instructions. The computer names you see throughout this document are based upon the common infrastructure.

The Advanced Section requires the ability to contact a certification authority (CA) server. If you need to install a CA server on your network, see [Step by Step Guide to Setting Up a Certification Authority](#).

If you have an MIT-compatible Kerberos v5 server and wish to test Windows 2000 IPSec using that Kerberos trust, please refer to [Step-by-Step Guide to Kerberos 5 Interoperability](#).

You must have two domain members to use the built-in policies, because they require Kerberos authentication provided by the domain controller. You can also use IP Security without the two computers being domain members. To achieve this, see the section on building a custom policy.

After completing this walkthrough, you will be able to:

- Use a built-in IPsec policy.
- Create your own IPsec policy.
- Check the status of IP Security.

Collecting Information

You will need the following information for both test computers:

- Your host name (right-click the **My Computer** icon on the desktop, click **Properties**, and click the **Network Identification** tab.)
- Your IP address (click **Start**, click **Run**, type **cmd**, and click **OK**. Type **ipconfig** at the command prompt and press **Enter**. After retrieving your IP address, type **exit** and press **Enter**.)

Preparing for Testing

Creating a Custom Console

Log on to the first test computer as a user with administrative privileges. In our example, this is the computer named HQ-RES-WRK-01.

Note: *For the remainder of this document, HQ-RES-WRK-01 will refer to the first test computer, and HQ-RES-WRK-02 will refer to the second test computer. If your machines have different names, be sure and track the steps using the proper name.*

Create a custom MMC console

1. From the Windows desktop, click **Start**, click **Run**, and in the **Open** textbox type **mmc**. Click **OK**.
2. On the **Console** menu, click **Add/Remove Snap-in**.
3. In the **Add/Remove Snap-in** dialog box, click **Add**.
4. In the **Add Standalone Snap-in** dialog box, click **Computer Management**, and then click **Add**.
5. Verify that **Local Computer** is selected, and click **Finish**.

6. In the **Add Standalone Snap-in** dialog box, click **Group Policy**, and then click **Add**.
7. Verify that **Local Computer** is selected in the **Group Policy** Object dialog box, and click **Finish**.
8. In the **Add Standalone Snap-in** dialog box, click **Certificates**, and then click **Add**.
9. Select **Computer Account**, and click **Next**.
10. Verify that **Local Computer** is selected, and click **Finish**.
11. To close the **Add Standalone Snap-in** dialog box, click **Close**.
12. To close the **Add/Remove Snap-in** dialog box, click **OK**.

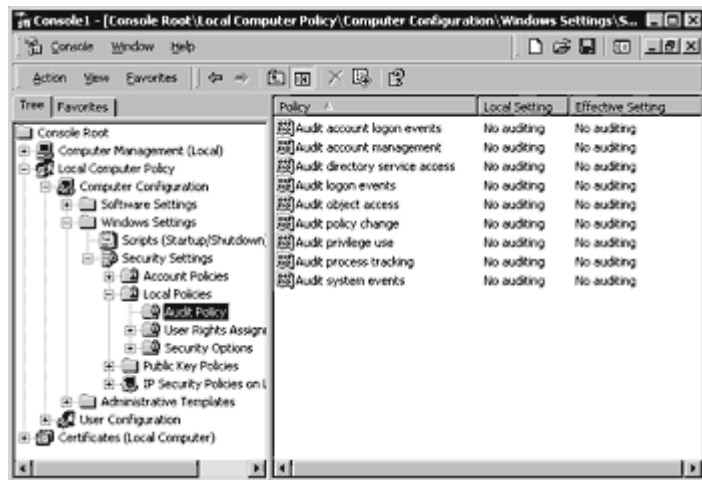
Enabling Audit Policy for Your Computer

In the next procedure, you will configure auditing, so that an event will be logged when IPSec is involved in communication. Later, this will be a useful confirmation that IPSec is working properly.

To enable audit policy

1. In the **MMC console**, select **Local Computer Policy** from the left pane and click + to expand the tree. Navigate to **Computer Configuration**, to **Windows Settings**, to **Security Settings**, then to **Local Policies**, and select **Audit Policy**.

FIGURE 1.



2. From the list of **Attributes** displayed in the right pane, double-click **Audit Logon Events**. The **Audit Logon Events** dialog box appears.
3. In the **Audit Logon Events** dialog box, click to select both the **Audit these attempts: Success** and **Failed** check boxes, and click **OK**.
4. Repeat steps 2 and 3 for the **Audit Object Access** attribute.

Configuring the IP Security Monitor

To monitor the successful security connections that the IPSec policy will create, use the IP Security Monitor tool. Before creating any policies, first start and configure the tool.

To start and configure the IP Security Monitor

1. To start the IP Security Monitor tool, click **Start**, click **Run**, and type **ipsecmon** into the **Open** text box. Click **OK**.
2. Click **Options** in the IP Security Monitor tool, and change the default value for **Refresh Seconds** from 15 to 1. Click **OK**.
3. **Minimize** the **IP Security Monitor** window.

You will use this minimized tool to monitor the policies later in this walkthrough.

Return to the beginning of this section, [Creating a Custom Console](#) and repeat all steps to this point for the second computer (in our example, this is the machine named HQ-RES-WRK-02).

Using a Built-in IPSec Policy

In this exercise, you will activate one of the built-in IPSec policies to secure traffic between the two computers. The default policies use Kerberos as the initial authentication method. Because both machines are members of a Windows 2000 domain, a minimal amount of configuration is required.

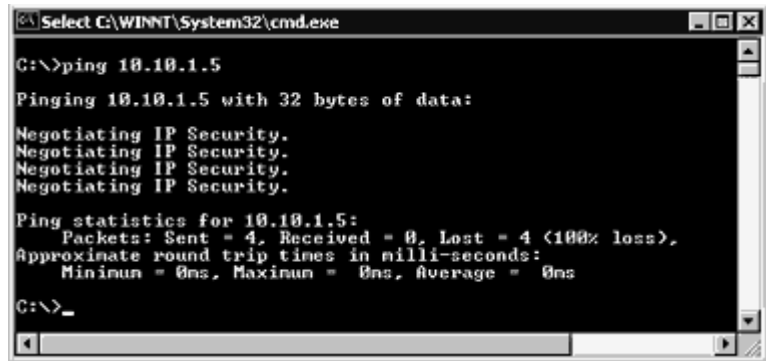
To activate the policy on HQ-RES-WRK-01:

1. In the **MMC** console you created earlier, select **IP Security Policies on Local Machine** from the left pane. There are three entries in the right pane: **Client, Secure Server, and Server**.
2. Right-click **Secure Server**, and then choose **Assign**. The status in the **Policy Assigned** column should change from **No** to **Yes**.
3. Repeat step 1 on HQ-RES-WRK-02. Right-click **Client**, and then choose **Assign**. The status in the **Policy Assigned** column changes from **No** to **Yes**.

Now you have one computer (HQ-RES-WRK-01) acting as a secure server, and the other (HQ-RES-WRK-02) acting as a client. The client will initially send unprotected ICMP Echo packets (using the ping utility) to the server, but the server will request security from the client, after which the rest of the communication will be secure. If the server were to initiate the ping, then the ping would have to be secured to the client before the server would allow it on the network. If the client computer had a secure server policy as well, it would not send unprotected pings or any other traffic; rather, it would request IPSec protection before any application data was sent. If both computers had client policies, no data would be protected, because neither side requests security.

4. On HQ-RES-WRK-02, click **Start**, click **Run**, type **cmd** in the text box, and click **OK**. Type **ping IP1**(the IP address ofHQ-RES-WRK-01).In this example, IP1 is 10.10.1.5. As shown in figure 2 below, the ping response will indicate that IPSec is being negotiated.

FIGURE 2.



```
C:\>Select C:\WINNT\System32\cmd.exe

C:\>ping 10.10.1.5

Pinging 10.10.1.5 with 32 bytes of data:

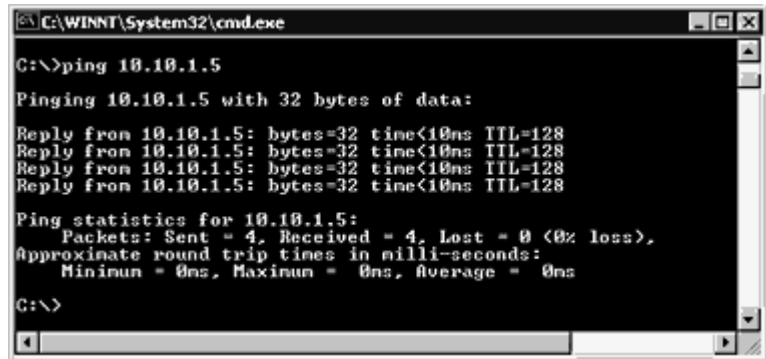
Negotiating IP Security.
Negotiating IP Security.
Negotiating IP Security.
Negotiating IP Security.

Ping statistics for 10.10.1.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>_
```

5. Restore the **IP Security Monitor** window, which you minimized earlier. You should see details of the Security Association that is currently in use between your two machines, as well as statistics on the number of Authenticated and Confidential bytes transmitted.
6. Repeat the ping command. Now that the two computers have established IPSec security associations between them, you should receive four successful replies as shown in figure 3 below. In this example, IP1 is 10.10.1.5.

FIGURE 3.



```
C:\>C:\WINNT\System32\cmd.exe

C:\>ping 10.10.1.5

Pinging 10.10.1.5 with 32 bytes of data:

Reply from 10.10.1.5: bytes=32 time<10ms TTL=128
Reply from 10.10.1.5: bytes=32 time<10ms TTL=128
Reply from 10.10.1.5: bytes=32 time<10ms TTL=128
Reply from 10.10.1.5: bytes=32 time<10ms TTL=128

Ping statistics for 10.10.1.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

7. Still working on HQ-RES-WRK-02, from the left pane in the **MMC**, click the + next to **Computer Management** to expand it, then expand **System Tools**,

expand **Event Viewer**, and click **Security Log**. Double-click the top instance of **Success Audit** in the right pane.

8. You should see the successful establishment of an IPSec Security Association (SA). Use the scroll bar to view the entire description. It should read something like the following code sample (machine names and IP addresses may differ depending on your configuration):

```
IKE security association established
Mode:
Data Protection Mode (Quick Mode)
```

```
Peer Identity:
Kerberos based Identity: hq-res-wrk-01$@RESKIT.COM
Peer IP Address: 10.10.1.5
```

```
Filter:
Source IP Address 10.10.1.6
Source IP Address Mask 255.255.255.255
Destination IP Address 10.10.1.5
Destination IP Address Mask 255.255.255.255
Protocol 0
Source Port 0
Destination Port 0
```

```
Parameters:
ESP Algorithm DES CBC
HMAC Algorithm SHA
AH Algorithm None
Encapsulation Transport Mode
InboundSpi <a large number>1128617882
OutBountSpi <a large number>865899841
Lifetime (sec) 900
Lifetime (kb) 100000
```

You have successfully configured and used IP Security between the two computers.

Impact of Secure Server Policy on a Computer

Only IPSec clients that can successfully negotiate can communicate with the secure server computer. Also, the secure server will not be able to talk to any other systems, such as Domain Name System (DNS) servers, unless that traffic can be secured using IPSec. Because many services are running in the background on the server, they will probably fail to communicate and generate event log messages.

This is normal, because the default Secure Server policy is very severe and attempts to secure almost all IP packets before letting them into the network. For actual use in production environments, you must create a custom policy that has the behavior you want according to your security requirements, network topology, and specific server application usage.

Allowing Non-IPSec Clients To Talk with A Server

To allow non-IPSec clients to communicate as well, you should assign the **Server** policy, instead of **Secure Server**. This always requests security, but allows unsecured communication with clients, by falling back to clear text if the client does not reply to the IKE negotiation request. If at any time the client does reply, then a negotiation is in progress and must succeed completely. If negotiation fails the communication will be blocked for one minute, whereupon another negotiation will be attempted. See the section, [Configuring an IPSec Filter Action](#), for more explanation on the settings that are used to control this behavior.

Unassign the **Secure Server** or **Server** and **Client** policies to return your computers to their previous states, by right-clicking the policy in the right pane (under **IP Security Policies on Local Machine** in the left pane), and then clicking **Unassign**.

Building A Custom IPSec Policy

In the previous section, you used one of the built-in IPSec policies to secure traffic between two domain members. If you want to secure traffic between two computers that are not domain members, you need to create a custom policy because the built-in policies require Kerberos authentication provided by the domain controller. There are other reasons for creating a custom policy; for example, if you wanted to secure traffic based on network address. In this section, you will create a custom IPSec policy, first by defining a security rule, then by defining a filter list, then finally by specifying the filter action.

Configuring an IPSec Policy

Before configuring the IPSec Authentication Method, Filter List, or Negotiation method, you must first create a new policy.

To create an IPSec Policy

1. Using HQ-RES-WRK-01, in the left pane of the **MMC Console**, right-click **IP Security Policies on Local Machine**, and then click **Create IP Security Policy**. The IP Security Policy Wizard appears.
2. Click **Next**.
3. Type **Partner** as the name of your policy, and click **Next**.
4. Clear the **Activate the default response rule** check box, and then click **Next**.
5. Make sure the **Edit Properties** check box is selected (it is by default), and then click **Finish**.
6. In the **Properties** dialog box for the policy you have just created, ensure that **Use Add Wizard** check box in the lower-right corner is selected, and then click **Add** to start the **Security Rule Wizard**.
7. Click **Next** to proceed through the **Security Rule Wizard**, which you started at the end of the previous section.
8. Select **This rule does not specify a tunnel**, (selected by default) and then click **Next**.
9. Select the radio button for **All network connections**, (selected by default) and click **Next**.

Configuring an IKE Authentication Method

Next you specify how the computers will trust each other, by specifying how they will authenticate themselves, or prove their identities to each other when trying to establish a security association. IKE for Windows 2000 provides three authentication methods to establish trust between computers:

- Kerberos v5 authentication provided by the Windows 2000 domain that serves as a Kerberos v5 Key Distribution Center (KDC). This provides easy deployment of secure communications between Windows 2000 computers who are members in a domain or across trusted domains. IKE only uses the authentication properties of Kerberos. Key generation for IPSec security associations is done using IKE RFC 2409 methods. This is documented in draft-ietf-ipsec-isakmp-gss-auth-02.txt.
- Public/Private key signatures using certificates, compatible with several certificate systems, including Microsoft, Entrust, VeriSign, and Netscape.
- Pre-shared key, which is a password used strictly for establishing trust between computers.

In this exercise, you use pre-shared key authentication. This is a text word or phrase that both computers, the sender and the receiver, must know in order to be trusted by each other. Both sides of the IPSec communication must know this value. It is not used to encrypt the application data. Rather, it is only used during negotiation to establish whether the two computers will trust each other. The IKE negotiation uses this value, but does not pass it across the network. However, the authentication key is stored in plain text form within the IPSec policy. Anyone with administrative access to the computer (or any valid domain user id for a computer that is a member of the domain where the IPSec policy is stored in the Active Directory) can see the authentication key value. The domain administrator must set custom access controls on the directory IPSec policy to prevent normal users from reading the IPSec policy. Therefore, Microsoft does not recommend use of a pre-shared key for IPSec authentication unless for testing, or in cases where it is required for interoperability with third-party vendor IPSec implementations. Instead, Microsoft recommends using either Kerberos or certificate authentication instead.

To configure the authentication method for the rule

1. Choose **Use this string to protect this key exchange** and enter **ABC123** as the string. You must not use a blank string. Click **Next**.

***Note:** If you want to use certificates for authentication, see the instructions for obtaining a certificate for testing from Microsoft using the Internet available certificate servers.*

Configuring an IPSec Filter List

IP Security is applied to IP packets as they are sent and received. Packets are matched against filters when being sent (outbound) to see if they should be secured, blocked, or passed through in clear text. Packets are also matched when received (inbound) to see if they should have been secured, should be blocked, or should be permitted into the system. There are two types of filters: those that control IPSec transport mode security, and those that control IPSec tunnel mode security. IPSec tunnel filters are applied first to all packets. Then, if none match, the IPSec transport mode filters are searched. A few types of IP traffic cannot be secured by the design of IPSec transport filters in Windows 2000, including:

- Broadcast addresses—usually ending with .25—with appropriate subnet masks.
- Multicast-addresses from 224.0.0.0 through 239.255.255.255.

- RSVP-IP protocol type 46. This is to allow RSVP to signal Quality of Service (QoS) requests for application traffic that may then be IPSec protected.
- Kerberos-UDP source or dest port 88. Kerberos is itself a secure protocol, which the IPSec's IKE negotiation service uses for authentication of other computers in a domain.
- IKE-UDP dest port 500. This is required to allow IKE to negotiate parameters for IPSec security.

These exemptions apply to IPSec transport mode filters. Transport mode filters apply to host packets that have a source address of the computer that is sending the packet, or a destination address of the computer that is receiving the packet. IPSec tunnels can only secure unicast IP traffic. Filters used for IPSec tunnels must be based on addresses only, not on protocol and port fields. If the tunnel filter were to be protocol or port specific, then fragments of the original packet would not be carried by the tunnel, and the original full IP packet would be lost. If unicast Kerberos, IKE, or RSVP packets are received on one interface, and routed out of another interface, (using packet forwarding, or the Routing and Remote Access Service), then they are not exempt from IPSec tunnel mode filters, and thus could be carried inside the tunnel. IPSec tunnel mode filters cannot filter multicast or broadcast packets, so these would not be carried inside the IPSec tunnel.

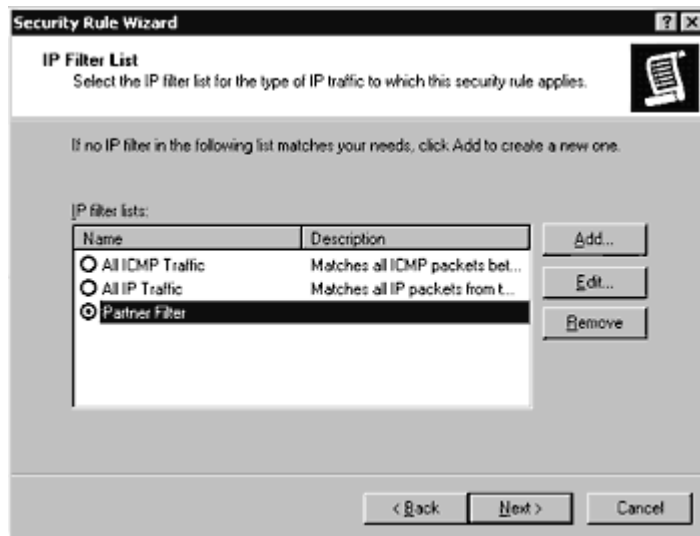
Individual filter specifications are grouped into a filter list to enable complex patterns of traffic to be grouped and managed as one named filter list, such as *Building 7 File Servers*, or *All blocked traffic*. Filter lists can be shared as necessary between different IPSec rules in the same policy or different IPSec policies.

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.

You will be configuring filters between your computer and your partner's computer. You must configure an outbound filter specifying your IP address as the source address and your partner as the destination address. Then the mirror processing configuration will automatically configure an inbound filter specifying your partner's computer as the source address, and your computer's IP address as the destination. In this simple case, there will be only one mirrored filter specification in the filter list.

The same filter list will need to be defined on both computers. To configure an IP Filter List

1. In the **IP Filter List** dialog box, click **Add**. An empty list of IP filters is displayed. Name your filter **Partner Filter**.
2. Make sure **Use Add Wizard** is selected in the center-right area of the screen and then click **Add**. This starts the **IP Filter Wizard**.
3. Click **Next** to continue.
4. Accept **My IP Address** as the default sourceaddress by clicking **Next**.
5. Choose **A Specific IP address** from the drop-down list box, enter your **Partners IP Address**, and then click **Next**.
6. Click **Next** to accept the protocol type of **Any**.
7. Make sure the **Edit Properties** check box is cleared (this is the default setting), and click **Finish**.
8. Click **Close** to leave the **IP Filter List** dialog box, and return to the **New Rule Wizard**.
9. In the **IP Filter List** dialog box, select the radio button next to **Partner Filter**.

FIGURE 4.

10. Click Next.

Read the following section before proceeding to the steps involved in configuring the filter action.

Configuring an IPSec Filter Action

You have just configured both the input and output filters for matching TCP/IP packets. The second step is to configure the action to take for those packets. You can permit, block, or secure the packets that match the filters. If you want to secure the traffic, both computers must have a *compatible* negotiation policy configured. The built-in defaults should serve well for trying out different features. If you want to experiment with specific capabilities, you should create your own new filter action.

Two methods allow communication with computers that are not able to do IPSec:

- Use the filter action **Permit** to let the packets go in the clear, or unsecured. Use this action in combination with a filter that matches the traffic you want to permit in its own rule within the IPSec policy. Typical uses would be to permit traffic types of ICMP, DNS, or SNMP, or to permit traffic to certain destinations, such as the default gateway, DHCP and DNS servers, or other non-IPSec systems.
- Configure your filter action to use the setting **Fall back to unsecured communication**. You will see this option presented in the wizard. Selecting this option in the wizard will enable the filter action parameter **Allow unsecured communication with non-IPSec aware computer**. Using this setting allows unsecured communication with a destination, by falling back to clear text if the destination *does not reply to the IKE negotiation request*. If at any time the client does reply, then a negotiation is in progress and must succeed completely. If IKE negotiation fails, the outbound packets that matched the filter will be discarded (blocked) for one minute, whereupon another outbound packet will cause another IKE negotiation to be attempted. This setting only affects IKE negotiations that are initiated by the computer. It has no effect on computers that receive a request and thus respond. The IKE RFC 2409 standard does not provide a method for both sides to negotiate to normal, or unsecured, or clear text mode.

To configure the filter action

1. In the **Filter** dialog shown in figure , click to select the **Use Add Wizard** check box, and then click **Add**.

FIGURE 5.



2. Click **Next** to proceed through the **Filter Action Wizard**.
3. Name this filter action **Partner Filter Action**, and click **Next**.
4. In the **Filter Action General Options** dialog box, select **Negotiate Security**, and then click **Next**.
5. Click **Do not communicate with computers that do not support IPSec** from the next wizard page, and then click **Next**.
6. Select **Medium** from the list of security methods, and click **Next**.
7. Make sure the **Edit Properties** check box is cleared (this is the default setting), and then click **Finish** to close this wizard.
8. In the **Filter Action** dialog , click the radio button next to **Partner Filter Action**, and then click **Next**.
9. Make sure the **Edit properties** check box is cleared (this is the default setting), and then click **Finish**.

You have just configured the filter action that will be used during negotiations with your partner. Note that you can re-use this filter action in other policies.

10. In the **Properties** page that is now displayed, click **Close**. You have successfully configured an IPSec Policy.
11. Repeat all steps in this procedure on HQ-RES-WRK-02 before proceeding.

Testing Your Custom IPSec Policy

Now that you have built an IPSec policy, you should test it before applying it in a network.

To test your custom IPSec policy

1. In the left pane of the MMC console, select **IP Security Policies on Local Machine**. Note that in addition to the three built-in policies, the Partner policy you just configured is listed in the right pane.
2. Right-click **Partner**, and then click **Assign** from the context menu. The status in the **Policy Assigned** column should change from **No** to **Yes**. Do this step on both machines before continuing.
3. Open a command prompt window, and type **ping partners-ip-address**. You should receive four **Negotiating IP Security** responses. Repeat the command, and you should receive four successful ping replies.
4. Restore the **IP Security Monitor** window (which you minimized earlier). You should see details of the Security Association that is currently in use between your two computers, as well as statistics on the number of Authenticated and Confidential bytes transmitted among others. Minimize this window again.
5. In the left pane of the MMC console, select **Computer Management**, and navigate to **System Tools**, to **Event Viewer**, and then select **Security**. In the security log, you should see event 541, which notes the establishment of an IPSec security association (SA).
6. Repeat step three to unassign the Partner policy, and return both computers to their previous states. This time, when you right-click the policy, click **Unassign**.

Using Certificate Authentication

The Windows 2000 IPSec implementation provides the ability to authenticate computers during IKE using certificates. All certificate validation is performed by the Cryptographic API (CAPI). IKE simply serves to negotiate which certificates to use and provides security for the exchange of the certificate credentials. The IPSec policy specifies which root certificate authority (CA) to use, not which specific certificate to use. Both sides must have a common root CA in their IPSec policy configuration.

Here are the requirements for the certificate to be used for IPSec:

- Certificate stored in computer account (machine store)
- Certificate contains an RSA public key that has a corresponding private key that can be used for RSA signatures.
- Used within certificate validity period
- The root certification authority is trusted
- A valid certification authority chain can be constructed by the CAPI module

These requirements are quite basic. IPSec does not require the machine certificate to be an IPSec type of certificate because existing certificate authorities may not issue these type of certificates.

Obtaining a Microsoft Certificate for Testing

You must first obtain a valid certificate from a certificate server. Even if you have another certificate server you want to use, obtain a Microsoft certificate first for testing. Any valid computer certificate can be used. User-based certificates are not used. We have tested compatibility with several certificate systems, including Microsoft, Entrust, VeriSign, and Netscape.

Note: *Not all certificate servers automatically enroll your computer with a certificate. The certificate must appear in the local computer account under personal certificates, and have the root CA certificate in the Trusted Root Certification Authorities store. Consult the [Certification Authority step-by-step guides on the Windows 2000 Step-by-Step Guides Web site](#) for more information on how to obtain machine certificates from non-Microsoft certificate servers.*

To obtain a certificate

1. Open **Internet Explorer** and go to the certification authority site. If you do not have another site from which to receive certificates, use:

<http://sectestca1.rte.microsoft.com>

This site provides access to four certification authorities. For simplicity, this procedure uses a certificate issued from the stand-alone root CA, sectestca3.

2. Select **Standalone Root (RSA 2048)**.
3. Select **Request a Certificate**, and then click **Next**.
4. Select **Advanced Request**, and then click **Next**.
5. Select **Submit a Certificate Request Using a Form**.
6. In the **Advanced Certificate Request** form, enter the following responses:
 - Identifying Information: as desired.
 - Intended Purpose: Client Authentication or Server Authentication.

This field sets the **extended key usage** field in the certificate. There is also an **IPSec Certificate** field to support the specification that is still being developed by the standards groups. You can use this type if you want to inter-operate with other IPSec implementations that require it. However, Windows 2000 IPSec certificate authentication uses any valid certificate in the computer account, meaning any setting of extended key usage will be acceptable. There is no way in IPSec policy to restrict the use to only **IPSec certificates**. If there are multiple machine certificates in the personal certificates folder on the local machine, only one will be chosen. Starting with the first root CA in the Authentication Method of the rule, the chosen certificate will be the first certificate found that has a trust path back to that root CA.

- **Cryptographic Service Provider**: Microsoft Base Cryptographic Provider v1.0
- **Key Usage**: Signature.
- **Key Size**: 1024

You can choose a larger key size if you choose the Microsoft Enhanced Cryptographic Provider. However, the enrollment request may fail because the version of Windows 2000 does not have the Strong Cryptography Pack installed. If this certificate will be used for interoperability with other IPSec implementations, be sure to check if the third-party IPSec product is able to process a signature with a key size larger than 1024. Some third-party products may also place limits in

IPSec policy on the size of the key used.

Note: *This setting determines what the private key can be used to do—encryption of data or signatures only. The current implementation of IKE uses certificate private keys only for signatures. Thus, a certificate issued with a usage limited to exchange (for data encryption) will not work. Certificates with a usage of both will work.*

- **Create A New Key Set:** enabled
 - **Use local machine store:** enabled
 - **Additional Options:** *fill in as desired*
 - **Hash Algorithm:** SHA1/RSA
7. Submit the request. You will receive a message stating that the certificate was issued to you.
 8. Click **Install this certificate**.
 9. You will get a message stating that the certificate has been successfully installed. Close Internet Explorer.
 10. Open the **IPSec Management MMC** console to which you added a snap-in to manage **Certificates (Local Computer)**.

Verify that the certificate enrollment succeeded

1. The Personal Certificates folder should contain the computer's certificate name that you selected for *your name* **IPSec** testing.
2. Click the + next to **Certificates (Local Computer)** to expand it. Expand the **Personal** folder, and click the **Certificates** folder. You should see a certificate in the right pane that was issued to **Administrator** (or the username you logged on with).
3. Double-click this certificate in the right pane. It should contain the message, **You have a private key that corresponds to this certificate**. Note the name of the CA where it says **Issued by:** (in our example, **SectestCA3**). Click **OK**.

Note: *If the computer certificate properties say "You do not have a private key that corresponds to the certificate," then enrollment has failed and the certificate will not work for IPSec IKE authentication. You must successfully get a private key that corresponds to the public key in the machine certificate.*

4. Expand **Trusted Root Certification Authorities**, and click the **Certificates** folder. Scroll down and find a certificate in this store with the name of the **Issued By** certification authority.

5. Repeat all the steps in this procedure to retrieve a certificate on the other test machine.

Note: *If a certificate was obtained from the Microsoft Certificate Server with the option set for **Strong Private Key Protection**, a user must enter a PIN number to access the private key each time that the private key is used to sign data in the IKE negotiation. Because the IKE negotiation is being done in the background by a system service, there is no window available to the service to prompt the user. Therefore, certificates obtained with this option will not work for IKE authentication.*

Configuring Certificate Authentication for a Rule

If you are creating a new rule, you can browse for a certification authority to use. This is a list of certification authority certificates that are in the Trusted Root Certification Authorities folder, not a list of your computer personal certificates. This root CA specification in an IPSec rule serves two purposes. First, it provides IKE with a root CA that it trusts. IKE on your computer will send a request for a valid certificate from this root CA to the other computer. Second, the CA specification provides the name of the root CA that your computer will use to look for its own personal certificate to offer in response to a request from the peer.

Caution: You must at least select the certification authority root that your computer certificate chains back to, that is, the top level CA in the certification path of the computer certificate in your computer's personal store.

1. Return to the **IP Security Policies** folder in the MMC.
2. Double-click the **Partner** policy in the right pane.
3. Make sure **Partner Filter** option is selected, and click **Edit**.
4. Select the radio button for **All IP Traffic**.
5. Click **Edit**.
6. Make sure the **New Rule Wizard** check box is selected, and click **OK**.
7. Click the **Authentication Methods** tab.
8. Select the **Preshared Key** with details **ABC123**, and click **Edit**.
9. Select the option **Use a certificate from this certification authority (CA)** and click **Browse**. Click to select the CA you used before: in our example, this is SecTestCA3.

FIGURE 6.



10. Click **OK**.

The IPsec Rule editor allows you to build an ordered list of certification authorities that your computer will send in a request to the peer computer during IKE negotiation. The peer computer must have a personal certificate issued by one of the root CAs in your list in order for the authentication to succeed.

You can continue to add and arrange certification authorities as you wish.

11. Click **OK** twice and click **Close**.

12. On the other test machine, repeat this full procedure. Now have each computer ping the other.

You can order the list of authentication methods to specify certificates first, then Kerberos or pre-shared key. However, you cannot break up the list of certificates by adding a non-certificate method in the middle.

By adding additional root CAs, you are able to build a list of root CAs that you trust, which is a greater list than the one (or few) that has issued your computer a certificate. This is necessary for interoperability in many enterprise scenarios.

It is important to understand that your computer may receive certificate requests from a destination peer that may or may not include a root CA in the list of root

CAs you have specified in IPSec policy. Coordination with the administrator of the destination is required to agree on which root CAs each side will be using.

- If the destination's request to you does include a certification authority in this list, then IKE will check to see if your computer has a valid personal certificate that chains back to this root CA. If you do, then it will choose the first valid computer personal certificate it finds and send that as the computer's identity.
- If your computer receives a certificate request for a root CA that **was not** specified in this IPSec policy rule, then your computer will send the first certificate it finds that chains back to the root CA name that is specified in its own IPSec policy rule. Because certificate requests are optional in the RFC 2409 standard, once your computer agrees to certificate authentication, your computer must send a certificate even if it did not receive an IKE certificate request, or if the certificate request yielded no match with your computer's root CA names in policy. In this case, it is likely that the IKE negotiation will fail because the two computers could not agree on a common root CA. If the destination's request to you does not include one of the certificate authorities here, then the IKE negotiation will fail.

Certificate Revocation List Checking

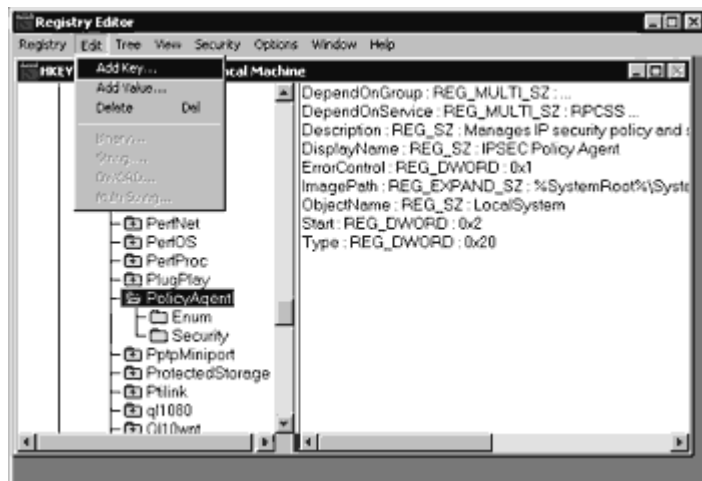
Most certificate servers issue certificates that contain a Certificate Revocation List (CRL) Distribution Point (sometimes wholly abbreviated as CDP). In order for a computer to validate a certificate completely, it must check to see that the certificate has not been revoked by the issuer. Since the standards for making this check have been evolving, and various certificate servers and PKI systems are already in use, not all of the certificate systems support the same method and functionality of CRL checking. Therefore CRL checking is disabled by default. Before enabling CRL checking, make sure you are successfully authenticating using certificates, and you have examined the Oakley .log trace file to see how the log shows this. (Step 3 below shows you where this file is located.)

IKE specifies to CAPI how to handle CRL checking when it requests a certificate to be validated. To enable CRL checking, the computer administrator must change the value of the registry key below. The proper setting of this value should be determined by the IPSec policy administrator, and the certificate server administrator.

To enable CRL checking by IKE

1. On the **Start** menu, click **Run**, and enter **regedt32**. Click **OK**. This starts the Registry Editor.
2. Navigate to **HKEY_LOCAL_MACHINE** on **Local Machine**.
3. Navigate to the following location: *System\CurrentControlSet\Services\PolicyAgent*
4. Double-click **PolicyAgent**.
5. On the **Edit** menu, click **Add Key**.

FIGURE 7.



6. Enter the **Key Name** (case sensitive): **Oakley**.
7. Leave **Class** blank, and click **OK**.
8. Select the new key, **Oakley**.
9. On the **Edit** menu, click **Add Value**.
10. Enter the **Value Name** (case sensitive): **StrongCrlCheck**.
11. Select Data Type: **REG_DWORD** and click **OK**.
12. Enter a value, either **1** or **2**, according to the behavior you want to enable:
 - Use **1** to fail the certificate validation only if the CRL check returns that the certificate has been revoked (the normal form of CRL checking).

- Use **2** to fail the certification validation on any CRL check error. This is the strongest form, and is used when the CRL distribution point must be reachable on the network, and must not say that it never issued the certificate or provide any other error. Effectively, a certificate will pass this level of check only if the CRL processing can positively conclude that the certificate is not revoked.
13. Click **Hex** as the Radix. Click **OK**
 14. Exit from the Registry Editor.
 15. At the Windows 2000 command prompt, type **net stop policyagent**, then type **net start policyagent** to restart the IPSec related services.

Note: *If your system is configured as a VPN server for L2TP/IPSec, you must restart Windows 2000.*

To disable the CRL checking, simply delete the **StrongCRLCheck** value under the **Oakley** key, and restart the service or Windows 2000 as necessary.

Understanding IKE Negotiation (Advanced Users)

This section is provided for those who want to learn more about the details of IKE negotiation behavior. It is not required to complete the steps in this guide. Detailed explanations of IPSec, IKE and other aspects of the implementation are available in the online help for both Windows 2000 Server and Professional versions. (The same help content is provided on both Professional and Server though a different table of contents is used. Simply start the **IPSec Policy Management** snap-in and choose **Help**).

Failure and **Success** of IKE, along with a reason for the failure, are events audited in the Security event log. The procedure for enabling auditing is given at the start of this walkthrough. If the server is using the built-in policy **Server (request security)**, (or actually any custom policy that has a rule which uses the built-in filter action **Request Security (optional)**), then the IKE negotiation may fall back to clear for destinations that do not reply to the IKE request. This is tracked by an audit event for what is called a *soft security association*. This appears in the IPSec monitor as having a **Security** column value of **<none>**. If the server is using Secure Server and gives up trying to reach a destination with no IKE response from that destination, a failure audit event in the security log will show that **no response from peer** was the reason.

You can use the **Server (request security)** policy and the audit log on a server to discover and track the destinations that the server communicates with in normal operation over time. Thus, you can better understand how to build a custom policy that will secure to the right destinations, while permitting other maintenance and infrastructure communication to go unprotected in the clear.

IKE Main Mode (Phase 1)

The initial long form of the IKE negotiation (main mode, or phase 1) performs the authentication and establishes an IKE security association (SA) between machines, which involves generating the master key material. The result is referred to as an *IKE security association*. IKE main mode is controlled by the IPSec policy rules by the system using just the source and destination address information from the filters in the rules. Once successful, default settings in the default policies (see Key Exchange on the policy's **General** tab) will make the IKE SA last for 8 hours. If data is actively being transferred at the end of the 8 hours, then the main mode security association will be renegotiated automatically. The IKE main mode security association is not visible in the IPSec monitor tool. However, it may be displayed by the local administrator using the **netdiag.exe /test:ipsec /v** command line. Netdiag.exe is a support tool, located on the Windows 2000 Professional and Server CDs, in the \Support folder.

IKE Quick Mode (Phase 2)

The shorter version of IKE negotiation (quick mode) occurs after main mode to establish an IPSec security association to secure particular traffic according to the source and destination addresses (and if present, protocol and port) parts of the packet filters in the policy's rules. The IPSec SA negotiation involves choosing algorithms, generating session keys, and determining the Security Parameter Index (SPI) numbers used in the packets. Two IPSec security associations are established, each with its own SPI (the label in the packet), one for inbound traffic, one for outbound traffic. The IPSec monitor shows only one IPSec security association, the outbound one. After five minutes of idle time on the inbound SA, both IPSec SAs are cleaned up, causing the outbound SA to disappear from the IPSec monitor display. If traffic is sent again that requires IPSec security, then an IKE quick mode negotiation occurs to re-establish two new IPSec security associations, which will use new keys and SPIs. The default values set in the default security methods require new quick mode IPSec security associations every 1 hour (3600 seconds) or after 100 megabytes have been transferred. If data has been actively transferred within the previous 5 minutes, then the IPSec security associations will be automat-

ically renegotiated before they expire. The side that has transmitted more data or that initiated the previous quick mode will initiate the new quick mode.

Troubleshooting

Troubleshooting Policy Configuration

This guide is intended to cover only local computer IPSec policy that uses IPSec transport (not tunneling) to secure traffic between a source computer and a destination computer. It does not cover using Group Policy in the Active Directory to distribute IPSec policy. IPSec policy configuration is very flexible and very powerful, though proper settings require understanding of the IKE and IPSec protocols themselves. There are a number of security configuration issues that you will want to be aware of. Please read the online help, and search the Microsoft Knowledge Base for IPSec related articles. Then read the additional notes below to help clarify what is not supported in policy configurations by design. If you are not able to get any IPSec communication to work, then follow the steps provided below to build the simplest policy, and use it for testing.

Only One Authentication Method Between a Pair of Hosts

IPSec policy is designed so that only one authentication method can be used between a single pair of hosts, regardless of how many are configured. If you have multiple rules that apply to the same pair of computers (look at the source and destination IP addresses only), you must make certain those rules allow that pair of computers to use the same authentication method. You must also make sure the credential used for that authentication method is valid. For example, the IPSec snap-in allows you to configure one rule that uses Kerberos to authenticate just TCP data between two host IP addresses, and to create a second rule with the same addresses but specifying UDP data to use certificates to authenticate. This policy will not work properly, because outbound data traffic can more specifically select a rule (because it matches the protocol UDP, not just the addresses) than the IKE negotiation on the destination computer can use when it tries to find a matching rule in policy to respond with in main mode (which can use only the source IP address of the IKE packet). Thus, this policy configuration uses two different authentication methods between a single pair of IP addresses (hosts). To avoid this problem, don't use protocol- or port-specific filters for the purpose of negotiating security for traf-

fic. Instead, use protocol and port specific filters mainly for permit and block actions.

One-Way IPSec Protection of Traffic Not Allowed

IPSec policy is not designed to allow one-way protection of traffic by IPSec. If you create a rule to protect traffic between IP addresses of hosts A and B, then you must specify both traffic from A to B and traffic from B to A in the same filter list. You can do this by creating two filters in the same filter list. Alternatively, you can go to the **Filter Specification Properties** dialog box in the **IPSec** snap-in and select the **Mirrored** box. This option is selected by default, because protection must be negotiated for both directions, even if the data traffic itself only flows one way most of the time.

You can create one-way filters to block or permit traffic, but not to secure traffic. To secure traffic, you have to specify the filter mirror manually or have the system generate it for you automatically using the mirror checkbox.

Computer Certificates Must Have a Private Key

Incorrectly obtained certificates may result in a condition in which the certificate exists, and is chosen to be used for IKE authentication, but fails to work because the private key corresponding to the certificate's public key is not present on the local computer.

To verify that the Certificate has a private key

1. On the **Start** menu, click **Run**, and then type **mmc** in the text box. Click **OK**.
2. On the **Console** menu, click **Add/Remove Snap-in**, and then click **Add**.
3. In the **Snap-in** list, double-click **Certificates**. Click **Close**, and then click **OK**.
4. Expand the **Certificates-User (local computer)**, and then expand **Personal**.
5. Click the **Certificates** folder.
6. In the right pane, double-click the certificate you want to check.

On the **General** tab, you should see the text **You have a private key that corresponds to this certificate**. If you don't see this message, the system won't use this certificate successfully for IPSec.

Depending upon how the certificate was requested and populated into the host's local certificate store, this private key value may not exist, or may not be available to be used during the IKE negotiation. If the certificate in the personal folder does not have a corresponding private key, then certificate enrollment has failed. If a certificate was obtained from the Microsoft Certificate Server with the option set for **strong private key protection**, the user must enter a PIN number to access the private key each time that the private key is used to sign data in the IKE negotiation. Because the IKE negotiation is being done in the background by a system service, there is no window available to the service to prompt the user. So certificates obtained with this option will not work for IKE authentication.

Build and Test the Simplest End-to-End Policy

Most problems, particularly interoperability problems, can be resolved by creating the simplest policy rather than by using the default policies. When you create a new policy, do not enable an IPSec tunnel, or the default response rule. Edit the policy on the **General** tab; edit the key exchange to have only one option that the destination will accept. For example, use the RFC 2049 required options of DES, SHA1, with the Low (1) 1 Diffie Hellman group. Create a filter list with one mirrored filter that specifies source *My IP Address* and destination of the IP address that you are trying to with communicate securely. We recommend testing by creating a filter containing only IP addresses. Create your own filter action to negotiate security using only one security method. If you want to see the traffic in the IPSec formatted packets with a packet sniffer, use Medium Security (AH format). Otherwise, choose custom, and build one single security method. For example, use the RFC 2049 required set of parameters such as format ESP using DES with SHA1, with no lifetimes specified, and no Perfect Forward Secrecy (PFS). Make sure both check boxes are cleared in the security method, so that it requires IPSec for the destination, and will not communicate with non-IPSec computers, and does not accept unsecured communications. Use an authentication method of pre-shared keys for the rule, and make sure there are no white spaces in the string of characters. The destination must use exactly the same pre-shared key.

Note: *The same configuration must be configured on the destination also, only the IP addresses are reversed for source and destination.*

You should assign this policy on a computer, then ping the destination from that computer. You should see the ping return **Negotiating security**. This indicates that the policy's filter is being matched and that IKE should be trying to negotiate security with the destination for the ping packet. If you continue to see **Negotiating IP**

Security from multiple tries to ping the destination, then you probably do not have a policy problem; rather, you may have an IKE problem. See the section [Troubleshooting IKE Negotiation](#), below.

Troubleshooting IKE Negotiation

The IKE service runs as part of the IPSec Policy Agent service. Be sure that this service is running.

Make sure that auditing is enabled for success and failure for the audit attribute **Audit Logon Events**. The IKE service will make audit entries and provide an explanation for why negotiation failed in the security event log.

Clearing IKE State: Restarting the IPSec Policy Agent Service

To completely clear the state of IKE negotiation, it is necessary to stop and start the policy agent service using the commands below from a command shell prompt when logged in as a local administrator:

```
net stop policyagent
```

```
net start policyagent
```

Retry your steps to secure traffic.

Caution: *When you stop the IPSec Policy Agent Service, the IPSec filter protections will be deactivated. Active VPN tunnels will no longer be IPSec protected. If you were also running the Routing or Remote Access services, or if you have enabled incoming VPN connections, you must stop and restart the remote access service, **net start remoteaccess**, after restarting the IPSec Policy Agent service.*

Using the Security log To See IKE Errors

The Security event log records the reason for failure when an IKE negotiation fails. Use these messages to detect that a negotiation failed and why. You must enable auditing using the procedure at the start of this walkthrough.

Using A Packet Sniffer

If none of the above has helped, and you have not read the section, [Understanding IKE Negotiation](#), do so now.

For more detailed investigations, use a packet sniffer, such as Microsoft Network Monitor, to capture the packets being exchanged. Remember that most of the content of the packets used in IKE negotiation is encrypted and cannot be interpreted by a packet sniffer. Still, it may be worthwhile to sniff all traffic to and from the computer to be sure that you see the traffic you are expected to see. A limited version of Microsoft Network Monitor is provided with Windows 2000 Server. It is not installed by default, so you must go into **Control Panel, Add/Remove Windows Components, Management and Monitoring Tools**, then select **Network Monitor Tools**, and follow the steps required.

Using IKE Debug Tracing (Expert Users)

The security log is the best place to determine the failure reason for an IKE negotiation. However, for experts in the IKE protocol negotiation, the debug tracing option for IKE negotiation is enabled using a registry key. The logging is disabled by default. To enable debug logging, you must stop and start the IPSec Policy Agent Service.

To enable debug logging by IKE

1. From the Windows desktop, click **Start**, click **Run**, and type **regedt32** in the text box. Click **OK**. This starts the **Registry Editor**.
2. Navigate to **HKEY_LOCAL_MACHINE on Local Machine**.
3. Navigate to the following location: **System\CurrentControlSet\Services\PolicyAgent**.
4. Double-click **PolicyAgent**.
5. If the Oakley key doesn't exist, on the **Edit** menu, click **Add Key**.
6. Enter the **Key Name** (case sensitive): **Oakley**.
7. Leave **Class** blank, and click **OK**.
8. Select the new key, **Oakley**.
9. On the **Edit** menu, click **Add Value**.
10. Enter the **Value Name** (case sensitive): **EnableLogging**
11. Select Data Type: **REG_DWORD** and click **OK**.

12. Enter value **1**
13. Click **Hex** as the Radix. Click **OK**
14. Exit from the **Registry Editor**.
15. At the Windows 2000 command prompt, type **net stop policyagent**, then type **net start policyagent** to restart the IPsec related services.

The file will be written to **windir\debug\oakley.log** by default, and the file oakley.log.sav is the previous version of the log after the policy agent service is restarted.

The log is limited to 50,000 entries, which usually limits the file size to less than 6 megabytes.

For More Information

For the latest information on Microsoft Windows 2000 operating system, visit our World Wide Web site at <http://www.microsoft.com/windows2000/> and the [Windows NT Server Forum on the Microsoft Network](#) (GO WORD: MSNTS).

IPSec Tools and Information

On the Windows 2000 platform CD

- IPsec snap-in for policy configuration
- IPsecmon.exe monitor to show active state
- Network Connections UI IPsec property
- Event log snap-in
- Group Policy snap-in to show local security audit policy
- IKE logging in oakley.log
- Online Help
- Context Sensitive Help
- netdiag/test:ipsec /v /debug

As part of the Windows 2000 Resource Kit

- IPSec chapter
- ipsepol.exe — command line policy create, delete
- group policy tools to show which GPO policy is applied
- IPSec end-to-end walkthrough (this document)
- Deployment scenarios available online

This guide is intended to cover only local computer IPSec policy that uses IPSec transport (not tunneling) to secure traffic between a source computer and a destination computer. It does not cover using Group Policy in the Active Directory to distribute IPSec policy. IPSec policy configuration is very flexible and thus very powerful, though proper settings require understanding of the IKE and IPSec protocols themselves. There are a number of security configuration issues that you will want to be aware of. Please read the Online Help, and search the Microsoft Knowledge Base for IPSec-related articles. Then read the additional notes below to help clarify what is not supported in policy configurations by design.

For information about default security settings in Windows 2000, see the white paper [Default Access Control Settings](#).