Knowledge Base

How to Configure IPSec Tunneling in Windows 2000

PSS ID Number: 252735

Article Last Modified on 3/17/2004

The information in this article applies to:

- Microsoft Windows 2000 Server
- Microsoft Windows 2000 Advanced Server
- Microsoft Windows 2000 Datacenter Server

This article was previously published under Q252735

SUMMARY

You can use IP Security (IPSec) in tunnel mode to encapsulate Internet Protocol (IP) packets and optionally encrypt them. The primary reason for using IPSec tunnel mode (sometimes referred to as "pure IPSec tunnel") in Microsoft Windows 2000 is for interoperability with third-party routers or gateways that do not support Layer 2 Tunneling Protocol (L2TP)/IPSec or PPTP Virtual Private Networking (VPN) tunneling technology.

MORE INFORMATION

Windows 2000 supports IPSec tunneling for situations where both tunnel endpoints have static IP addresses. This is primarily useful in gateway-to-gateway implementations, but may also work for specialized network security scenarios between a gateway/router and a server (like a Windows 2000 router routing traffic from its external interface to an internal Windows 2000-based computer securing the internal path by establishing an IPSec tunnel to the internal server providing services to the external clients).

Windows 2000 IPSec tunneling is not supported for client remote access VPN use because the IETF IPSec RFCs do not currently provide a remote access solution in the Internet Key Exchange (IKE) protocol for client-to-gateway connections. The IETF RFC 2661 for Layer 2 Tunneling Protocol (L2TP) was specifically developed by Cisco, Microsoft, and others for the purpose of providing client remote access VPN connections. In Windows 2000, client remote access VPN connections are protected using an automatically generated IPSec policy that uses IPSec transport mode (not tunnel mode) when the L2TP tunnel type is selected.

Windows 2000 IPSec tunneling also does not support protocol and port-specific tunnels. While the Microsoft Management Console (MMC) IPSec Policy snap-in is very general and allows you to associate any type of filter with a tunnel, make sure you use only address information in the specification of a filter for a tunnel rule.

Details on how the IPSec and IKE protocols work can be found in the *Microsoft Windows 2000 Resource Kit* and in the Windows 2000 IPSec end-to-end walkthrough. Information about where you can find these documents is included at the end of this article.

This article explains how to configure an IPSec tunnel on a Windows 2000 gateway. Because the IPSec tunnel secures only traffic specified in the IPSec filters you configure, this article also describes how to configure filters in Routing and Remote Access Service (RRAS) to prevent traffic outside the tunnel from being received or forwarded. This article outlines the following scenario to make it easy to follow the configuration steps:

```
NetA - Windows 2000 gateway --- Internet --- third-party gateway - NetB
       W2KintIP     W2KextIP         3rdExtIP               3rdIntIP
```

NetA is the network ID of the Windows 2000 gateway internal network.

W2KintIP is the IP address assigned to the Windows 2000 gateway internal network adapter.

W2KextIP is the IP address assigned to the Windows 2000 gateway external network adapter.

3rdExtIP is the IP address assigned to the third-party gateway external network adapter.

3rdIntIP is the IP address assigned to the third-party gateway internal network adapter.

NetB is the network ID of the third-party gateway internal network.

The goal is for the Windows 2000 gateway and the third-party gateway to establish an IPSec tunnel when traffic from NetA needs to be routed to NetB or when traffic from NetB needs to be routed to NetA so traffic is routed over a secure session.

You need to configure an IPSec policy. You must build two filters; one to match packets going from NetA to NetB (tunnel 1), and one to match packets going from NetB to NetA (tunnel 2). You need to configure a filter action to specify how the tunnel should be secured (a tunnel is represented by a rule, so two rules are created).

How to Create IPSec Policy

Typically, a Windows 2000 gateway is not a member of a domain, so a local IPSec policy is created. If the Windows 2000 gateway is a member of a domain that has IPSec policy applied to all members of the domain by default, this prevents the Windows 2000 gateway from having a local IPSec policy. In this case, you can create an Organizational Unit (OU) in Active Directory, make the Windows 2000 gateway a member of this OU, and assign the IPSec policy to the Group Policy Object (GPO) of the OU. For more information, refer to the "Assigning IPSec Policy" section of Windows 2000 online help.

1. Use the MMC to work on the IP Security Policy Management snap-in (a quick way to load this is to click **Start**, click **Run**, and then type `secpol.msc`).
2. Right-click **IP Security Policies on Local Machine**, and then click **Create IP Security Policy**.
3. Click **Next**, and then type a name for your policy (for example, IPSec Tunnel with third-party Gateway).

   NOTE: You can also type more information in the **Description** box.
4. Click to clear the **Activate the default response rule** check box, and then click **Next**.
5. Click **Finish** (keep the **Edit** check box selected).

NOTE: The IPSec policy is created with default settings for the IKE main mode (phase 1) on the **General** tab, in **Key Exchange**. The IPSec tunnel consists of two rules, each of which specifies a tunnel endpoint. Because there are two tunnel endpoints, there are two rules. The filters in each rule must represent the source and destination IP addresses in IP packets that are sent to that rule's tunnel endpoint.

How to Build a Filter List from NetA to NetB

1. In the new policy properties, click to clear the **Use Add Wizard** check box, and then click **Add** to create a new rule.
2. On the **IP Filter List** tab, click **Add**.
3. Type an appropriate name for the filter list, click to clear the **Use Add Wizard** check box, and then click **Add**.
4. In the **Source address** area, click **A specific IP Subnet**, and then fill in the **IP Address** and **Subnet mask** boxes to reflect NetA.
5. In the **Destination address** area, click **A specific IP Subnet**, and fill in the **IP Address** and **Subnet mask** boxes to reflect NetB.
6. Click to clear the **Mirrored** check box.
7. On the **Protocol** tab, make sure the protocol type is set to **Any**, because IPSec tunnels do not support protocol-specific or port-specific filters.
8. If you want to type a description for your filter, click the **Description** tab. It is generally a good idea to give the filter the same name you used for the filter list. The filter name is displayed in the IPSec monitor when the tunnel is active.
9. Click **OK**, and then click **Close**.

How to Build a Filter List from NetB to NetA

1. On the **IP Filter List** tab, click **Add**.
2. Type an appropriate name for the filter list, click to clear the **Use Add Wizard** check box, and then click **Add**.
3. In the **Source address** area, click **A specific IP Subnet**, and then fill in the **IP Address** and **Subnet mask** boxes to reflect NetB.
4. In the **Destination address** area, click **A specific IP Subnet**, and fill in the **IP Address** and **Subnet mask** boxes to reflect NetA.
5. Click to clear the **Mirrored** check box.
6. If you want to type a description for your filter, click the **Description** tab.
7. Click **OK**, and then click **Close**.

How to Configure a Rule for a NetA-to-NetB Tunnel

1. On the **IP Filter List** tab, click the filter list you created.
2. On the **Tunnel Setting** tab, click **The tunnel endpoint is specified by this IP Address** box, and then type *3rdextip* (where *3rdextip* is the IP address assigned to the third-party gateway external network adapter).
3. On the **Connection Type** tab, click **All network connections** (or click **LAN connections** if *W2KextIP* is not an ISDN, PPP, or direct connect serial connection).
4. On the **Filter Action** tab, click to clear the **Use Add Wizard** check box, and then click **Add** to create a new filter action because the default actions allow incoming traffic in the clear.
5. Keep the **Negotiate security** option enabled, and click to clear the **Accept unsecured communication, but always respond using IPSec** check box. You must do this to ensure secure operation.

   NOTE: None of the check boxes at the bottom of the **Filter Action** dialog box should be checked as an initial configuration for a filter action that applies to tunnel rules. Only the **Perfect Forward Secrecy (PFS)** check box is a valid setting for tunnels if the other end of the tunnel is also configured to use PFS. The other two check boxes are not valid for tunnel filter actions.
6. Click **Add**, and keep the **High (ESP)** option selected (or you can select the **Custom (for expert users)** option if you want to define specific algorithms and session key lifetimes). Encapsulating Security Payload (ESP) is one of the two IPSec protocols.
7. Click **OK**. On the **General** tab, type a name for the new filter action (for example, IPSec tunnel: ESP DES/MD5), and then click **OK**.
8. Select the filter action you just created.
9. On the **Authentication Methods** tab, configure the authentication method you want (use preshared key for testing, otherwise, use certificates). Kerberos is technically possible if both ends of the tunnel are in trusted domains, and that trusted domain's IP address (IP address of a domain controller) is reachable on the network by both ends of the tunnel during IKE negotiation of the tunnel (before it is established). This is a rare case.
10. Click **Close**.

How to Configure a Rule for a NetB-to-NetA Tunnel

1. In IPSec policy properties, click **Add** to create a new rule.
2. On the **IP Filter List** tab, click the filter list you created (from NetB to NetA).
3. On the **Tunnel Setting** tab, click **The tunnel endpoint is specified by this IP Address** box, and then type *w2kextip* (where *w2kextip* is the IP address assigned to the Windows 2000 gateway external network adapter).
4. On the **Connection Type** tab, click **All network connections** (or click **LAN connections** if *W2KextIP* is not an ISDN, PPP, or direct connect serial connection). Any outbound traffic on the interface type that matches the filters attempts to be tunneled to the tunnel endpoint specified in the rule. Inbound traffic that matches the filters is discarded because it should be received secured by an IPSec tunnel.
5. On the **Filter Action** tab, click the filter action you created.
6. On the **Authentication Methods** tab, configure the same method used in the first rule (same method must be used in both rules).
7. Click **Close**, make sure both rules you created are enabled in your policy, and then click **Close**.

How to Assign Your New IPSec Policy to Your Windows 2000 Gateway

In the IP Security Policies on Local Machine MMC snap-in, right-click your new policy, and then click **Assign**. A green arrow appears in the folder icon next to your policy.

After your policy is assigned, you have two additional active filters (RRAS automatically creates IPSec filters for L2TP traffic). To see the active filters, type the following command at a command prompt:

```
netdiag /test:ipsec /debug
```

You can optionally redirect the output of this command to a text file so you can view it with a text editor (such as Notepad) by typing the following command:

```
netdiag /test:ipsec /debug > filename.txt
```

The **netdiag** command is available after you install the Microsoft Windows 2000 Resource Kit, which you can install from your Windows 2000 CD-ROM. To install the kit, locate the Support\Tools folder, and then double-click the Setup.exe file. After installation, you may need to run the **netdiag** command from the %SystemRoot%\Program Files\Support Tools folder (where %SystemRoot% is the drive where Windows 2000 is installed).

The tunnel filters look similar to the following example:

```
Local IPSec Policy Active: 'IPSec tunnel with {tunnel endpoint}' IP Security Policy Path:
SOFTWARE\Policies\Microsoft\Windows\IPSec\Policy\Local\ipsecPolicy{-longnumber-}

There are two filters
From NetA to NetB
Filter ID: {-long number-}
Policy ID: {-long number-}
IPSEC_POLICY PolicyId = {-long number-}
Flags: 0x0
Tunnel Addr: 0.0.0.0
PHASE 2 OFFERS Count = 1
Offer #0:
ESP[ DES MD5 HMAC]
Rekey: 0 seconds / 0 bytes.
AUTHENTICATION INFO Count = 1
Method = Preshared key: -actual key-
Src Addr: NetA Src Mask: -subnet mask-
Dest Addr: NetB Dest Mask: -subnet mask-
Tunnel Addr: 3rdExtIP Src Port: 0 Dest Port: 0
Protocol: 0 TunnelFilter: Yes
Flags : Outbound
From NetB to NetA
Filter ID: {-long number-}
Policy ID: {-long number-}
IPSEC_POLICY PolicyId = {-long number-}
Flags: 0x0
Tunnel Addr: 0.0.0.0
PHASE 2 OFFERS Count = 1
Offer #0:
ESP[ DES MD5 HMAC]
Rekey: 0 seconds / 0 bytes.
AUTHENTICATION INFO Count = 1
Method = Preshared key: -actual key-
Src Addr: NetB Src Mask: -subnet mask-
Dest Addr: NetA Dest Mask: -subnet mask-
Tunnel Addr: W2KextIP Src Port: 0 Dest Port: 0
Protocol: 0 TunnelFilter: Yes
Flags: Inbound
```

How to Configure RRAS Filtering

If you want to prevent traffic that does not have a source or destination address matching NetA or NetB, create an output filter for the external interface in the RRAS MMC so it drops all traffic except packets from NetA to NetB, and an input filter so it drops all traffic except packets from NetB to NetA. You also need to allow traffic to/from *W2KextIP* and *3rdExtIP* to allow IKE negotiation when the tunnel is being created. RRAS filtering is performed above IPSec, you do not have to allow the IPSec protocol because it never reaches the IP packet filter layer. The following example is a very simple representation of the Windows 2000 TCP/IP architecture:

```
Application layer
Transport layer (TCP|UDP|ICMP|RAW)
---- Network layer start ----
IP Packet Filter (where NAT/RRAS filtering is done)
IPSec (where IPSec filters are implemented)
Fragmentation/Reassembly
---- Network layer end ------
NDIS Interface
Datalink layer
Physical layer
```

To configure the filters in RRAS, load the RRAS MMC and use the following steps:

1. Expand your server tree under **Routing and Remote Access**, expand the **IP Routing** subtree, and then click **General**.
2. Right-click ***W2KextIP***, and then click **Properties**.
3. Click **Output Filters**, and then click **Add**.
4. Click to select the **Source network** and **Destination network** check boxes.
5. In the **Source network** area, fill in the **IP address** and **Subnet mask** boxes to reflect NetA.
6. In the **Destination network** area, fill in the **IP address** and **Subnet mask** boxes to reflect NetB.
7. Keep the protocol set to **Any**, and then click **OK**.
8. Click **Add**, and then click to select the **Source network** and **Destination network** check boxes.
9. In the **Source network** area, fill in the **IP address** and **Subnet mask** boxes to reflect *W2KextIP*.
10. In the **Destination network** area, fill in the **IP address** and **Subnet mask** boxes to reflect *3rdExtIP* (for IKE negotiation use subnet mask of 255.255.255.255).
11. Keep the protocol set to **Any**, and then click **OK**.
12. Click to select the **Drop all packets except those that meet the criteria below** check box, and then click **OK**.
13. Click **Input Filters**, click **Add**, and then click to select the **Source network** and **Destination network** check boxes.
14. In the **Source network** area, fill in the **IP address** and **Subnet mask** boxes to reflect NetB.
15. In the **Destination network** area, fill in the **IP address** and **Subnet mask** boxes to reflect NetA.
16. Keep the protocol set to **Any**, and then click **OK**.

17. Click **Add**, and then click to select the **Source network** and **Destination network** check boxes.
18. In the **Source network** area, fill in the **IP address** and **Subnet mask** boxes to reflect *3rdExtIP*.
19. In the **Destination network** area, fill in the **IP address** and **Subnet mask** boxes to reflect *W2KextIP* (or IKE negotiation use subnet mask of 255.255.255.255).
20. Keep the protocol set to **Any**, and then click **OK**.
21. Click to select the **Drop all packets except those that meet the criteria below** check box, and then click **OK** twice.

NOTE: If the RRAS server has more than one interface connected to the Internet, or if you have multiple IPSec tunnels, type RRAS exempt filters for each IPSec tunnel (each source and destination IP subnet) for every Internet interface.

How to Configure Static Routes in RRAS

The Windows 2000 gateway needs to have a route in its route table for NetB, which you can configure by adding a static route in the RRAS MMC. If the Windows 2000 gateway is multihomed with two or more network adapters on the same external network (or two or more networks that can reach the destination tunnel IP *3rdExtIP*), the potential exists for the following:

- Outbound tunnel traffic leaves on one interface, and the inbound tunnel traffic is received on a different interface. Even if you use IPSec offload network adapters, receiving on a different interface (than outbound tunnel traffic is sent on) does not allow the receiving network adapter to process the encryption in hardware, because only the outbound interface gets to offload the Security Association (SA).
- Outbound tunnel traffic leaves on an interface that is different than the interface that has the tunnel endpoint IP address. The source IP of the tunneled packet is the source IP on the outbound interface. If this is not the source IP that is expected by the other end, the tunnel is not established (or packets are dropped by the remote endpoint if the tunnel has already been established).

To address the issue of sending outbound tunnel traffic on the wrong interface, define a static route to bind traffic to NetB to the appropriate external interface:

1. In the RRAS MMC, expand your server tree, expand the **IP Routing** subtree, right-click **Static Routes**, and then click **New Static Route**.
2. In the **Interface** area, click ***W2KextIP*** (if this is the interface you want to always use for outbound tunnel traffic).
3. Fill the **Destination** and **Network Mask** boxes to reflect NetB.
4. In the **Gateway** box, type *`3rdextip`*.
5. Keep the **Metric** value set to its default (1), and then click **OK**.

NOTE: To address the issue of receiving inbound tunnel traffic on the wrong interface, do not advertise the interface's IP address using a routing protocol and configure a filter in RRAS to drop packets to NetA or *W2KextIP* as indicated in the "How to Configure RRAS Filtering" section of this article.

Testing Your IPSec Tunnel

You can initiate the tunnel by pinging from a computer on NetA to a computer on NetB (or from NetB to NetA). If you created the filters correctly and assigned the correct policy, the two gateways establish an IPSec tunnel so they can send the ICMP traffic from the **ping** command in encrypted format.

Even if the **ping** command works, you should verify that the ICMP traffic was sent in encrypted format from gateway to gateway. You can use the following tools to accomplish this.

Enable Auditing for Logon Events and Object Access

This logs events in the security log informing you if IKE security association negotiation was attempted, and if was successful or not.

1. Using the Group Policy MMC snap-in, expand **Local Computer Policy**, and go to Computer Configuration/Windows Settings/Security Settings/Local Policies/Audit Policy.
2. Enable success and failure auditing for "Audit logon events" and "Audit object access."

NOTE: If the Windows 2000 gateway is a member of a domain and if you are using a domain policy for auditing, the domain policy overwrites your local policy. In this case, modify the domain policy.

IP Security Monitor

This tool shows IPSec statistics and active SAs. After you attempt to establish the tunnel using the **ping** command, you can see if an SA was created (if the tunnel creation is successful, an SA is displayed). If the **ping** command is successful but there is no SA, the ICMP traffic was not protected by IPSec. If you see a "soft association" that did not previously exist, then IPSec agreed to allow this traffic to go on the clear (without encryption).

To load IP Security Monitor, click **Start**, click **Run**, and then type `ipsecmon`.

Network Monitor

You can use Network Monitor to capture traffic going through the *W2KextIP* interface while you attempt to ping the computer. If you can see ICMP packets in the capture with source and destination IP addresses corresponding to the IP address of the computer from which you are pinging and the computer you are trying to ping, then IPSec is not protecting the traffic. If you do not see this ICMP traffic but see ISAKMP and ESP packets instead, IPSec is protecting traffic. If you are using just the Authentication Header (AH) IPSec protocol, you will see the ISAKMP traffic followed by the ICMP packets. ISAKMP packets are the actual IKE negotiation taking place, and ESP packets are the payload data encrypted by the IPSec protocol.

You can install Network Monitor from your Windows 2000 Server CD-ROM. It is not available on the Windows 2000 Professional CD-ROM, but you can install the tool on a computer running Windows 2000 Professional if you have Microsoft Systems Management Server (SMS).

For additional information about installing Network Monitor in Windows 2000, click the following article number to view the article in the Microsoft Knowledge Base:

> 243270 How to install Network Monitor in Windows 2000

Actual Test

1. Before you attempt to ping from a computer on one subnet to the other (NetA or NetB), type `ipconfig` at a command prompt. The network interfaces that are initialized in the TCP/IP stack are displayed.
2. Run the IP Security Monitor tool.
3. Load Network Monitor, click **Capture/Network**, and then click the W2KextIP interface (you can start a capture by clicking **Capture/Start**).

4. Attempt to ping the computer. The first ICMP echo packets may timeout while the IPSec tunnel is being built. If the ping attempt is not successful, check the security and system logs.
5. If the ping attempt is successful, stop the Network Monitor capture and see if the ICMP traffic went on the clear or if you just see the ISAKMP and IPSec protocol packets. Check IP Security Monitor to see if an SA was created using the NetA to NetB filter you created. Also check the security log. You should see Event ID 541 (IKE security association established).
6. Type `ipconfig` at a command prompt again so you see that there is no additional TCP/IP interface while the tunnel is up. This is because IPSec is actually protecting the traffic going through the physical interface (*W2KextIP*).

If the remote gateway is also a Windows 2000 node, keep in mind the following information:

- The default gateway for clients in NetA should be *W2KextIP*; the default gateway for clients in NetB should be *3rdIntIP*.
- An IPSec tunnel does not change the way traffic is routed in the Windows 2000 gateway (which is able to route packets because routing is enabled in RRAS; the actual LAN or WAN interface metrics are still used.

Note IPSec tunnel mode does not work directly with an endpoint that runs Network Address Translation (NAT) or Microsoft Internet Security Acceleration Server (ISA). For additional information about this limitation, click the following article number to view the article in the Microsoft Knowledge Base:

314764 Using Internet Protocol Security with Network Address Translation and Internet Security Acceleration Server

For more information about RRAS, see Windows 2000 Help. To access Help online, visit the following Microsoft Web site:

http://www.microsoft.com/windows2000/techinfo/proddoc/default.asp

You can find the Windows 2000 Resource Kit, walkthroughs, and other technical documentation at the following Microsoft Web site:

http://www.microsoft.com/windows2000/techinfo/planning/

For additional information about soft associations, click the following article number to view the article in the Microsoft Knowledge Base:

234580 'Soft associations' between IPSec-enabled and non-IPSec-enabled computers

For IETF standards information, refer to the appropriate Web sites:

- IPSec

  http://www.ietf.org/html.charters/ipsec-charter.html
- L2TP

  http://www.ietf.org/html.charters/pppext-charter.html

  ftp://ftp.isi.edu/in-notes/rfc2661.txt

  http://www.ietf.org/html.charters/l2tpext-charter.html

Microsoft provides third-party contact information to help you find technical support. This contact information may change without notice. Microsoft does not guarantee the accuracy of this third-party contact information.

Additional query words: nic

Keywords: kb3rdparty kbhowto kbnetwork KB252735
Technology: kbwin2000AdvServ kbwin2000AdvServSearch kbwin2000DataServ kbwin2000DataServSearch kbwin2000Search kbwin2000Serv kbwin2000ServSearch kbWinAdvServSearch kbWinDataServSearch

Send feedback to Microsoft