How To Configure IPSec Tunneling in Windows Server 2003

↑ Back to the top

For a Microsoft Windows 2000 version of this article, see 252735 (/EN-US/help/252735).
↑ Back to the top

IN THIS TASK

↑ Back to the top

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 Windows Server 2003 is for interoperability with non-Microsoft routers or gateways that do not support Layer 2 Tunneling Protocol (L2TP)/IPSec or PPTP virtual private network (VPN) tunneling technology.

back to the top
↑ Back to the top

Windows Server 2003 supports IPSec tunneling for situations where both tunnel endpoints have static IP addresses. This is primarily useful in gateway-to-gateway implementations. However, it may also work for specialized network security scenarios between a gateway or router and a server. (For example, a Windows Server 2003 router that routes traffic from its external interface to an internal Windows Server 2003-based computer that secures the internal path by establishing an IPSec tunnel to

the internal server that provides services to the external clients).

Windows Server 2003 IPSec tunneling is not supported for client remote access VPN use because the Internet Engineering Task Force (IETF) IPSec Requests for Comments (RFCs) do not currently provide a remote access solution in the Internet Key Exchange (IKE) protocol for client-to-gateway connections. IETF RFC 2661, Layer Two Tunneling Protocol "L2TP," was specifically developed by Cisco, Microsoft, and others to provide client remote access VPN connections. In Windows Server 2003, 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 Server 2003 IPSec tunneling also does not support protocol-specific 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 that you use only address information in the specification of a filter for a tunnel rule.

For more information about how the IPSec and IKE protocols work, see the Microsoft Windows Server 2003 Resource Kit.

This article describes how to configure an IPSec tunnel on a Windows Server 2003 gateway. Because the IPSec tunnel secures only traffic that is specified in the IPSec filters that you configure, this article also describes how to configure filters in the Routing and Remote Access service to prevent traffic outside the tunnel from being received or forwarded. This article uses the following scenario to make it easy to follow the configuration steps:

NetA- WIN2003intIP-	-Windows Server 2003 gateway- -WIN2003extIP-	-Internet-	-non-Microsoft gateway- -3rdExtIP-	-NetB -3rdIntIP

NetA is the network ID of the Windows Server 2003 gateway internal network.

WIN2003intIP is the IP address that is assigned to the Windows Server 2003 gateway internal network adapter.

WIN2003extIP is the IP address that is assigned to the Windows Server 2003 gateway external network adapter.

3rdExtIP is the IP address that is assigned to the non-Microsoft gateway external network adapter.

3rdIntIP is the IP address that is assigned to the non-Microsoft gateway internal network adapter.

NetB is the network ID of the non-Microsoft gateway internal network.

The goal is for the Windows Server 2003 gateway and the non-Microsoft gateway to establish an IPSec tunnel when traffic from **NetA** must be routed to **NetB** or when traffic from **NetB** must be routed to **NetA** so traffic is routed over a secure session.

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

back to the top

Create IPSec Policy

Typically, a Windows Server 2003 gateway is not a member of a domain, so a local IPSec policy is created. If the Windows Server 2003 gateway is a member of a domain that has IPSec policy applied to all members of the domain by default, this prevents the Windows Server 2003 gateway from having a local IPSec policy. In this case, you can create an organizational unit in Active Directory, make the Windows Server 2003 gateway a member of this organizational unit, and assign the IPSec policy to the Group Policy object (GPO) of the organizational unit. For more information, see the "Creating, modifying, and assigning IPSec policies" section of Windows Server 2003 online Help.

1. Click **Start**, click **Run**, and then type secpol.msc to start the IP Security Policy Management snap-in.
2. Right-click **IP Security Policies on Local Computer**, and then click **Create IP Security Policy**.
3. Click **Next**, and then type a name for your policy (for example, IPSec Tunnel with non-Microsoft Gateway). Click **Next**.

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

Note The IPSec policy is created with default settings for the IKE main mode. The IPSec tunnel is made up of two rules. Each rule 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.

back to the top

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. Click the **IP Filter List** tab, and then 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** box, click **A specific IP Subnet**, and then type the **IP Address**and **Subnet mask**to for **NetA**.
5. In the **Destination address** box, click **A specific IP Subnet**, and then type the **IP Address** and **Subnet mask** for **NetB**.
6. Click to clear the **Mirrored** check box.
7. Click the **Protocol** tab. Make sure that 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 that you used for the filter list. The filter name appears in the IPSec monitor when the tunnel is active.
9. Click **OK**.

back to the top

Build a Filter List from NetB to NetA

1. Click the **IP Filter List** tab, and then 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** box, click **A specific IP Subnet**, and then type the **IP Address**and **Subnet mask** for **NetB**.
4. In the **Destination address** box, click **A specific IP Subnet**, and then type the **IP Address** and **Subnet mask** for **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**.

back to the top

Configure a Rule for a NetA-to-NetB Tunnel

1. Click the **IP Filter List** tab, and then click to select the filter list that you created.
2. Click 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 that is assigned to the non-Microsoft gateway external network adapter).
3. Click the **Connection Type** tab, click **All network connections** (or click **Local area network (LAN)** if **WIN2003extIP** is not an ISDN, PPP, or direct-connect serial connection).
4. Click 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 clear text.
5. Keep the **Negotiate security** option enabled, and then click to clear the **Accept unsecured communication, but always respond using IPSec** check box. You must do this for secure operation.

   Note None of the check boxes at the bottom of the **Filter Action** dialog box are selected as an initial configuration for a filter action that applies to tunnel rules. Only the **Use session key 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.
6. Click **Add**, and keep the **Integrity and encryption** 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**. Click the **General** tab, type a name for the new filter action (for example, IPSec tunnel: ESP DES/MD5), and then click **OK**.
8. Click to select the filter action that you just created.
9. Click the **Authentication Methods** tab, configure the authentication method that you want (use **preshared key** for testing, and otherwise use **certificates**). Kerberos is technically possible if both ends of the tunnel are in trusted domains, and each 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). But this is rare.
10. Click **Close**.

back to the top

Configure a Rule for a NetB-to-NetA Tunnel

1. In IPSec policy properties, click **Add** to create a new rule.
2. Click the **IP Filter List** tab, click to select the filter list that you created (from **NetB** to **NetA**).
3. Click the **Tunnel Setting** tab, click **The tunnel endpoint is specified by this IP Address** box, and then type **WIN2003extIP** (where **WIN2003extIP** is the IP address that is assigned to the Windows Server 2003 gateway external network adapter).
4. Click the **Connection Type** tab, click **All network connections** (or click **Local area network (LAN)** if **WIN2003extIP** is not an ISDN, PPP, or direct-connect serial connection). Any outbound traffic on the interface type that matches the filters tries to be tunneled to the tunnel endpoint that is specified in the rule. Inbound traffic that matches the filters is discarded because it must be received secured by an IPSec tunnel.
5. Click the **Filter Action** tab, and then click to select the filter action that you created.
6. Click the **Authentication Methods** tab, and then configure the same method that you used in the first rule (the same method must be used in both rules).

7. Click **OK**, make sure both rules that you created are enabled in your policy, and then click **OK** again.

back to the top

Assign Your New IPSec Policy to Your Windows Server 2003 Gateway

In the IP Security Policies on Local Computer 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 (Routing and Remote Access 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 Server 2003 Support Tools. To install the Support Tools, locate the Support\Tools folder on your Windows Server 2003 CD-ROM, right-click the Suptools.msi file, and then click **Install**. After installation, you may have to run the **netdiag** command from the **%SystemRoot%**\Program Files\Support Tools folder (where **%SystemRoot%** is the drive where Windows Server 2003 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
```

back to the top

Configure Routing and Remote Access Filtering

If you want to prevent traffic that does not have a source or destination address that matches **NetA** or **NetB**, create an output filter for the external interface in the Routing and Remote Access MMC so that the filter drops all traffic except packets from **NetA** to **NetB**. Also create an input filter so the filter drops all traffic except packets from **NetB** to **NetA**. You also have to allow traffic to and from **WIN2003extIP** and **3rdExtIP** to allow IKE negotiation when the tunnel is being created. Routing and Remote Access filtering is performed over IPSec. You do not have to specifically allow the IPSec protocol because it never reaches the IP packet filter layer. The following example is a very simple representation of the Windows Server 2003 TCP/IP architecture:

```
Application layer
Transport layer (TCP|UDP|ICMP|RAW)
---- Network layer start ----
IP Packet Filter (where NAT/Routing and Remote Access 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 the Routing and Remote Access service, load the Routing and Remote Access MMC and follow these steps:

1. Expand your server tree under **Routing and Remote Access**, expand the **IP Routing** subtree, and then click **General**.
2. Right-click **WIN2003extIP**, and then click **Properties**.
3. Click **Outbound Filters**, and then click **New**.
4. Click to select the **Source network** and **Destination network** check boxes.
5. In the **Source network** box, type the **IP address** and **Subnet mask** for **NetA**.
6. In the **Destination network** box, type the **IP address** and **Subnet mask** for **NetB**.
7. Keep the protocol set to **Any**, and then click **OK**.
8. Click **New**, and then click to select the **Source network** and **Destination network** check boxes.
9. In the **Source network** box, type the **IP address** and **Subnet mask** for **WIN2003extIP**.
10. In the **Destination network** box, type the **IP address** and **Subnet mask** for **3rdExtIP** (for IKE negotiation use a 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** box, type the **IP address** and **Subnet mask** for **NetB**.
15. In the **Destination network** box, type the **IP address** and **Subnet mask** for **NetA**.
16. Keep the protocol set to **Any**, and then click **OK**.
17. Click **New**, and then click to select the **Source network** and **Destination network** check boxes.
18. In the **Source network** box, type the **IP address** and **Subnet mask** for **3rdExtIP**.
19. In the **Destination network** box, type the **IP address** and **Subnet mask** for **WIN2003extIP** (for IKE negotiation use a 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** two times.

Note If the Routing and Remote Access server has more than one interface that is connected to the Internet, or if you have multiple IPSec tunnels, create Routing and Remote Access exempt filters for each IPSec tunnel (each source and destination IP subnet) for every Internet interface.

back to the top

Configure Static Routes in Routing and Remote Access

The Windows Server 2003 gateway must have a route in its route table for **NetB**. To configure this route, add a static route in the Routing and Remote Access MMC. If the Windows Server 2003 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 the outbound tunnel traffic is sent on) does not allow the receiving network adapter to process the encryption in hardware, because only the outbound interface can offload the Security Association (SA).
- Outbound tunnel traffic leaves on an interface that is different from 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 avoid 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 Routing and Remote Access MMC, expand your server tree, expand the **IP Routing** subtree, right-click **Static Routes**, and then click **New Static Route**.
2. In the **Interface** box, click **WIN2003extIP** (if this is the interface that you want to always use for outbound tunnel traffic).
3. Type the **Destination network** and **Network mask** for **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 by using a routing protocol. Also, configure a filter in the Routing and Remote Access service to drop packets to **NetA** or **WIN2003extIP** as indicated in the "Configure Routing and Remote Access Filtering" section of this article.

back to the top

Test 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, verify that the ICMP traffic was sent in encrypted format from gateway to gateway. You can use the following tools to do this.

back to the top

Enable Auditing for Logon Events and Object Access

This logs events in the security log. This tells you if IKE security association negotiation was tried and if it was successful or not.

1. Using the Group Policy MMC snap-in, expand **Local Computer Policy**, expand **Computer Configuration**, expand **Windows Settings**, expand **Security Settings**, expand **Local Policies**, and then click **Audit Policy**.
2. Enable **Success** and **Failure** auditing for **Audit logon events** and **Audit object access**.

   Note If the Windows Server 2003 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.

back to the top

IP Security Monitor

The IP Security Monitor console shows IPSec statistics and active security associations (SA). After you try to establish the tunnel by 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). For additional information about "Soft Associations", click the following article number to view the article in the Microsoft Knowledge Base:

234580 (/EN-US/help/234580) "Soft Associations" Between IPSec-Enabled and Non-IPSec-Enabled Computers

Note In Microsoft Windows XP and the Windows Server 2003 family, IP Security Monitor is implemented as a Microsoft Management Console (MMC) console. To add the IP Security Monitor snap-in, follow these steps:

1. Click **Start**, click **Run**, type **MMC**, and then click **OK**.
2. Click **File**, click **Add/Remove Snap-in**, and then click **Add**.
3. Click **IP Security Monitor**, and then click **Add**.
4. Click **Close**, and then click **OK**.

back to the top

Network Monitor

You can use Network Monitor to capture traffic going through the
WIN2003extIP interface while you try to ping the computer. If you can see ICMP packets in the capture file that have source and destination IP addresses that correspond to the IP addresses of the computer that you are pinging from and the computer you are trying to ping, then IPSec is not protecting the traffic. If you do not see this ICMP traffic but do see ISAKMP and ESP packets instead, IPSec is protecting the traffic. If you are using only the Authentication Header (AH) IPSec protocol, you will see the ISAKMP traffic followed by the ICMP packets. ISAKMP packets are the actual IKE negotiation occurring, and ESP packets are the payload data encrypted by the IPSec protocol.

To install Network Monitor, follow these steps:

1. Click **Start**, click **Control Panel**, click **Add or Remove Programs**, and then click **Add/Remove Windows Components**.
2. In the Windows Components wizard, click **Management and Monitoring Tools**, and then click **Details**.
3. In **Subcomponents of Management and Monitoring Tools**, click to select the **Network Monitor Tools**check box, and then click **OK**.
4. If you are prompted for additional files, insert the installation CD for your operating system, or type a path of the location of the files on the network.

back to the top

Actual Test

1. Before you try 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. Start the IP Security Monitor tool.
3. Start Network Monitor, and then on the **Capture** menu, click **Networks**. Click the **WIN2003extIP** interface, and then click **OK**.
4. Try to ping the computer. The first ICMP echo packets may time out while the IPSec tunnel is being built. If the ping is not successful, check the security and system logs.
5. If the ping 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 to verify that there is no additional TCP/IP interface while the tunnel is in use. This behavior occurs because IPSec is protecting the traffic that is going through the physical interface (**WIN2003extIP**).

   If the remote gateway is also a Windows Server 2003 node, remember that:
   - The default gateway for clients in **NetA** is **WIN2003extIP**. The default gateway for clients in **NetB** is **3rdIntIP**.
   - An IPSec tunnel does not change the way traffic is routed in the Windows Server 2003 gateway. (This gateway can route packets because routing is enabled in Routing and Remote Access. The actual LAN or WAN interface metrics are still used.)

back to the top
↑ Back to the top

References

For more information about the Routing and Remote Access service, see Windows Server 2003 online Help.

To view the Windows Server 2003 Resource Kit and other technical documentation, visit the following Microsoft Web site:
http://www.microsoft.com/windowsserver2003/default.mspx (http://www.microsoft.com/windowsserver2003/default.mspx)

For IETF standards information, visit the following sites:

- IPSec
  http://www.ietf.org/rfc/rfc2401.txt (http://www.ietf.org/rfc/rfc2401.txt)
- L2TP
  http://www.ietf.org/html.charters/pppext-charter.html (http://www.ietf.org/html.charters/pppext-charter.html)
  ftp://ftp.isi.edu/in-notes/rfc2661.txt (ftp://ftp.isi.edu/in-notes/rfc2661.txt)
  http://www.ietf.org/html.charters/l2tpext-charter.html (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.
↑ Back to the top

Keywords: kb, kbbillprodsweep, kbentirenet, kbhowtomaster

↑ Back to the top

Article Info

Article ID	:	816514
Revision	:	6
Created on	:	8/20/2020
Published on	:	8/20/2020
Exists online	:	False
Views	:	79