

Build VPN server

In this article TipsMake.com will introduce in turn the steps to deploy basic remote VPN access. The first thing you need to decide before building a Windows VPN server is whether or not to use Microsoft Internet authentication service (IAS) to authenticate users connected.

Ryan Bass

In this article TipsMake.com will introduce in turn the steps to deploy basic remote VPN access.

The first thing you need to decide before building a Windows VPN server is whether or not to use Microsoft's Internet authentication service (IAS) to authenticate users connected to the VPN. IAS is the addition of Microsoft's RADIUS and when building the VPN server you can check the user's legitimate IAS access or can allow users to be authenticated directly to Active Directory (AD).

IAS offers a number of utilities. First, it has better accessibility capabilities including sending data directly to the SQL database. Second, IAS provides a centralized destination for you to point to some other VPN servers. This allows maintenance of a set of remote access methods that all VPN servers can use. We do not go into too much detail on remote access methods in this article, but this is described as an effective way to determine who is allowed to access VPN. Assuming that IAS is your choice of authentication, see the configuration of the IAS server.

Follow these steps to install the IAS server. If the hardware on the computer is not enough, IAS can be installed on the same server that you use to access VPN (note that this job does not guarantee security).

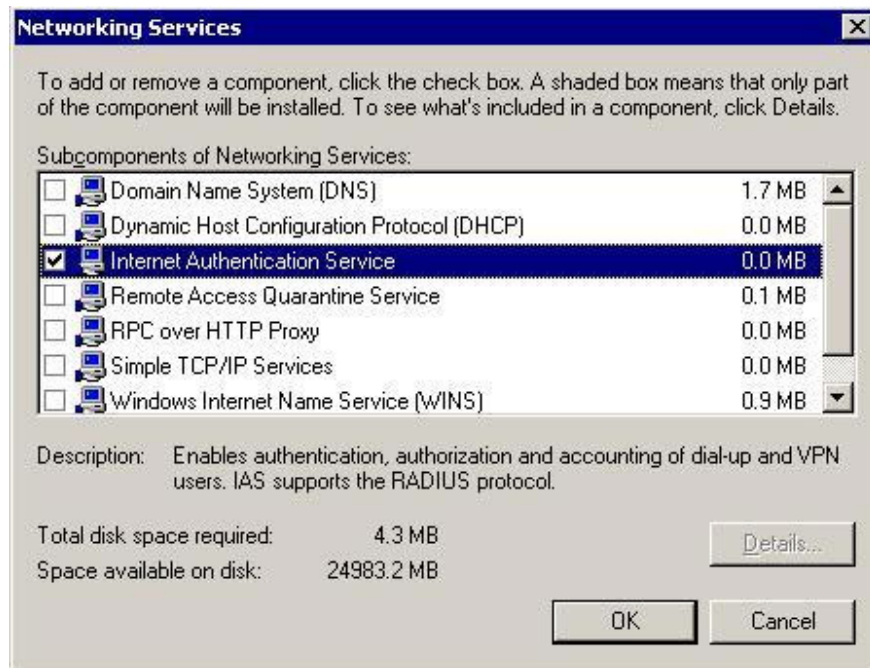


Figure 1

1. **Start » Control Panel » Add or Remove Programs » Add / Remove Windows Components » Networking Services » Details . » Internet Authentication Service**

2. **Start » Administrative Tools » Internet Authentication Service »Right-click Internet Authentication Service (local) » Register Server in Active Directory**

3. **Start » Administrative Tools » Internet Authentication Service » Remote Access Logging » Select the desired option.**

4. **Start » Administrative Tools » Internet Authentication Service »right-click RADIUS Clients » New RADIUS Client »Enter the appropriate information for the VPN server (you will be asked to share the secret, select one and save it to verify it) receive later)**

5. If the IAS server has a firewall enabled, allow UDP port 1812 from the VPN server to not be blocked.

Open the IAS administration interface, follow the steps to add a remote access point to allow access to users in special AD groups (the two default groups do not allow anyone to access the VPN server).

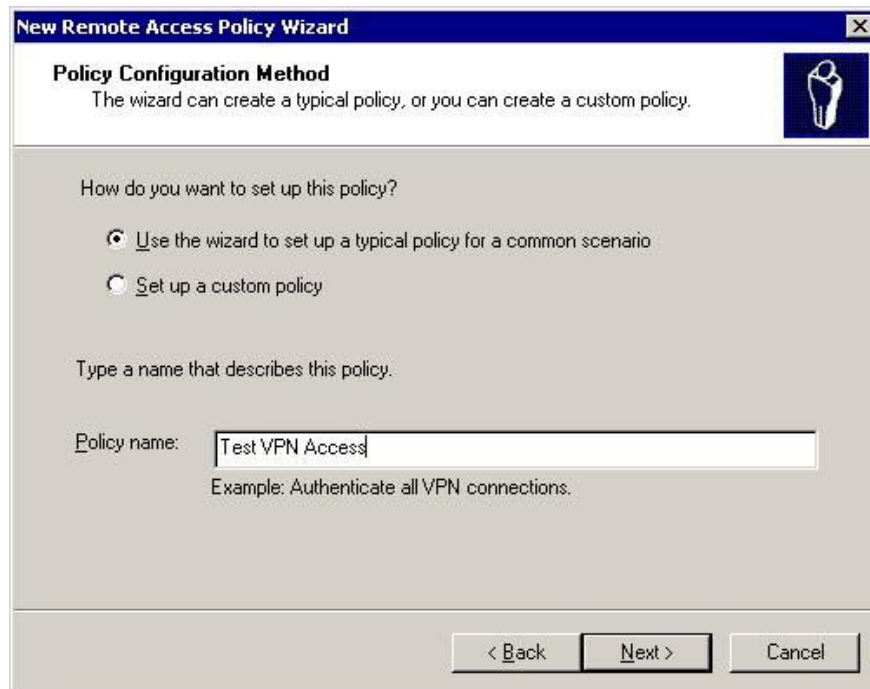


Figure 2

1. **Start » Administrative Tools » Internet Authentication Service »right-click Remote Access Policies » New Remote Access Policy**
2. Select the name » **Next**
3. Select VPN » **Next**
4. Click **Add .**
5. Click **Locations .** and select the domain
6. Add **MyVPNaccessGroup » Next**
7. Retain the only option **MS-CHAPv2 » Next**
8. Retain the only option " **Strongest encryption " » Next » Finish**

Finally, you need to update remote access directions to protect against dangerous computers on remote user networks using packet-based VPN connections through VPN servers. Follow these steps:

Start » Administrative Tools » Internet Authentication Service » Remote Access Policies » right-click the new policy and select properties »click Edit Profile . » select the IP tab » Input Filters . » New . » OK » click " Permit only the packets listed below "» OK » OK » OK

The IAS server is now ready to receive authentication requests from the VPN server. Before you can configure a VPN server, consider the essential requirements of a VPN server:

1. Set up two network interface cards (NICs) on the VPN server, one card connected to the internal protected network and the other card connected to the DMZ or shared network accessible (external NIC).
2. Do not configure DNS or WINS on an external NIC.
3. Do not define the default gateway for the internal NIC, only define a single gateway for the external NIC.

Here are the steps needed to configure a new VPN server:

1. **Start » Administrative Tools » Services » Stop the " Windows Firewall / Internet Connection Sharing " service and set the startup mode to Disabled**
2. **Start » Administrative Tools » Routing and Remote Access**
3. Right-click on the server name and then click **Configure and Enable Routing and Remote Access** (the internal firewall service must not be enabled).
4. Select **Remote Access » Next » select VPN » Next**
5. Select an external NIC (Note the " **Enable security . " checkbox) » Next**
6. Select NIC in » **Next**
7. Select " **Automatically " or " From a specified range of addresses " (this procedure follows the 2nd option) » Next**
8. Click **New . » enter a range for IPs » OK » Next**
9. Select " **Yes, set up this server to work with a RADIUS server " » Next**
10. Enter IAS server and share security » **Next » Finish**
11. **Routing and Remote Access » MAYCHUCUABAN » IP Routing » DHCP Relay Agent » Add the IP address of a DHCP server to the DHCP Relay Agent configuration (Note that the DHCP server is required to return information as default , but should not control any IP address by setting a static address)**
12. If the internal network consists of only one network, you are successful! In other words, a route will need to be added for clients to access other internal networks. **Routing and Remote Access » MAYCHUCUABAN » IP Routing » right-click on the Static Routes » New Static Route . » enter a traffic route of any lower level network in the network. The easiest way is to direct all traffic to the default gateway that the internal NIC is using.**

Next you need to set up a VPN connection from the client. Here are the steps for Windows XP:

- Start » Control Panel » Network Connections » Create a new connection » Next » Connect to a corporate network » Next » Virtual Private Network connection » Next » Select a name » Next » you may want to select " Do not dial the initial connection " » Next » Enter the server name or VPN server IP address » Next » select the connection creation object » Next » Finish**

You should double-click the newly created VPN connection and log in with a user account that is a member of the group that is allowed access to the remote access point created above.

Note that when connecting to a VPN you cannot access the Internet. This is really a problem to consider and the solution to this problem depends on the network topology. One drawback is that IP filters created on the external NIC are configured by route and remote access. You can configure them by route or remote access »MAYCHUCUABAN » **IP Routing** » **General** » right-click on the external interface and select **Properties** »click on **Inbound Filters** or **Outbound Filters** buttons. Be careful when changing these filters when they are set as a security measure.

The following is how to configure the split tunnel from an intact tunnel: **Start** » **Control Panel** » **Network Connections** »right click on the VPN connection» **Properties** »Select the **Networking** tab» select **Internet Protocol (TCP / IP)** » **Properties** » **Advanced** . »select or cancel" **Use Default Gateway On Remote Network** ". Reselecting this option will create a tunnel division when you are new to the VPN connection and unchecking will create an intact tunnel.

Here's how you can force connections using either PPTP or L2TP / IPSec options (Note that L2TP / IPSec requires certificates) **Start** » **Control Panel** » **Network Connections** »right-click on the connection VPN » **Properties** » Select the **Networking** tab »change the **VPN** type.

Here are the last two information to help you run the Windows VPN server conveniently:

- 1) User account settings on the Dial-up tab of an AD user object can override the remote access policy settings created on the IAS server.
- 2) Windows Server 2003 Standard version only supports less than 1000 connections.

You finished reading the article "**Build VPN server**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.