How to configure an L2TP/IPsec server behind a NAT-T device in Windows Vista and in Windows Server 2008

https://support.microsoft.com/en-us/help/926179/how-to-configure-an-l2tp-ipsec-server-behind-a-nat-t-device-in-windows-vista-and-in-windows-server-2008

INTRODUCTION

Important This section, method, or task contains steps that tell you how to modify the registry. However, serious problems might occur if you modify the registry incorrectly. Therefore, make sure that you follow these steps carefully. For added protection, back up the registry before you modify it. Then, you can restore the registry if a problem occurs. For more information about how to back up and restore the registry, click the following article number to view the article in the Microsoft Knowledge Base: 322756 How to back up and restore the registry in Windows

By default, Windows Vista and the Windows Server 2008 operating system do not support Internet Protocol security (IPsec) network address translation (NAT) Traversal (NAT-T) security associations to servers that are located behind a NAT device. Therefore, if the virtual private network (VPN) server is behind a NAT device, a Windows Vista-based VPN client computer or a Windows Server 2008-based VPN client computer cannot make a Layer Two Tunneling Protocol (L2TP)/IPsec connection to the VPN server. This scenario includes VPN servers that are running Windows Server 2008 and Microsoft Windows Server 2003.

Because of the way in which NAT devices translate network traffic, you may experience unexpected results when you put a server behind a NAT device and then use an IPsec NAT-T environment. Therefore, if you must have IPsec for communication, we recommend that you use public IP addresses for all servers that you can connect to from the Internet. However, if you have to put a server behind a NAT device and then use an IPsec NAT-T environment, you can enable communication by changing a registry value on the VPN client computer and the VPN server.

To create and configure the **AssumeUDPEncapsulationContextOnSendRule** registry value, follow these steps:

1. Log on to the Windows Vista client computer as a user who is a member of the Administrators group.
2. Click **Start**, point to **All Programs**, click **Accessories**, click **Run**, type regedit, and then click **OK**. If the **User Account Control** dialog box is displayed on the screen and prompts you to elevate your administrator token, click **Continue**.
3. Locate and then click the following registry subkey:

   ```
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PolicyAgent
   ```

   Note You can also apply the **AssumeUDPEncapsulationContextOnSendRule** DWORD value to a Microsoft Windows XP Service Pack 2 (SP2)-based VPN client computer. To do this, locate and then click the following registry subkey:

   ```
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\IPSec
   ```

4. On the **Edit** menu, point to **New**, and then click **DWORD (32-bit) Value**.
5. Type AssumeUDPEncapsulationContextOnSendRule, and then press ENTER.
6. Right-click **`AssumeUDPEncapsulationContextOnSendRule`**, and then click **Modify**.
7. In the **Value Data** box, type one of the following values:

   - **0 -** A value of 0 (zero) configures Windows so that it cannot establish security associations with servers that are located behind NAT devices. This is the default value.
   - **1 -** A value of 1 configures Windows so that it can establish security associations with servers that are located behind NAT devices.
   - **2** -A value of 2 configures Windows so that it can establish security associations when both the server and the Windows Vista-based or Windows Server 2008-based VPN client computer are behind NAT devices.

8. Click **OK**, and then exit Registry Editor.
9. Restart the computer.