VPNease

Configuration Guide for Client Platforms

Windows 2000 (SP4)
Windows XP (no SP, SP1, SP1a, SP2)
Windows Vista
Apple Mac Os X
Linux
Pocket PC / Windows Mobile

Table of Contents

Introduction....3
Windows XP....4
Prerequisites....4
General Requirements....4
Windows XP with Service Pack 2 (SP2), Recommended....4
Windows XP with Service Pack 1 (SP1 or SP1a)....4
Windows XP without a Service Pack....5
Known Limitations....6
Configuration....6
Testing....8
Apple Mac Os X....9
Prerequisites....9
Known Limitations....9
Configuration....9
Testing....10
Windows Vista....11
Prerequisites....11
Known Limitations....11
Configuration....11
Testing....13
Linux....14
Windows 2000 (SP4)....15
Prerequisites....15
Known Limitations....15
Configuration....15
Step 1: Configure L2TP/IPsec Connection....15
Step 2: Disable Automatic L2TP/IPsec IPsec Policy....16
Step 3: Create a New L2TP/IPsec IPsec Policy....16
Testing....18
Pocket PC / Windows Mobile....19
Other Platforms....20
Windows 95, Windows 98, Windows ME....20
Open Source Clients....20

Introduction

VPNease is a clientless VPN product which allows you to use the existing built-in client of your operating system for secure remote access. VPNease supports the built-in L2TP/IPsec remote access clients of the following platforms:

- Windows 2000 (SP4)
- Windows XP (without SP, SP1, SP1a, SP2)
- Windows Vista
- Apple Mac Os X (Panther, Tiger, Leopard)
- Linux
- Pocket PC / Windows Mobile

You will need the following basic information from your administrator:

- **Server address**: The DNS name or public IP address of the remote access server you are connecting to.
  - Examples: vpn.company.com, 123.123.123.123
- **Pre-shared key**: The group pre-shared key (GPSK) of the remote access server.
  - Example: aY7bCa6g
- **Username & password**: The username and password configured for your remote access account.
  - Example: username: john.doe, password: qYfgaCX5

Windows XP

Prerequisites

VPNease supports all Windows XP versions. However, each Service Pack has different prerequisites, described below.

General Requirements

- Ensure you have administrator privileges to your compute. Remote access connection cannot be configured without administrator privileges.

Windows XP with Service Pack 2 (SP2), Recommended

- Windows XP SP2 supports NAT Traversal (NAT-T) directly without the need for an update.
- If remote access server is behind address translation (port forwarding), a registry change is required to ensure Windows XP SP2 can connect properly.
    - The update is required even when the client is not behind a NAT device. The problem is caused by a change in NAT-T behavior in XP SP2, and is documented by Microsoft KB article http://support.microsoft.com/kb/885407/.
    - Start registry editor (**Start** => **Run**, enter **regedit** and press **Return**). Add the following registry value with type **REG_DWORD** to Windows registry:

        HKEY_LOCAL_MACHINE \
        System \
        CurrentControlSet \
        Services \
        IPSec \
        AssumeUDPEncapsulationContextOnSendRule

    - Set the value of the new key to **2** to enable NAT Traversal compatibility.
    - Reboot your computer to ensure that the change takes effect.
    - Please see the KB article for more details.

Windows XP with Service Pack 1 (SP1 or SP1a)

- Install NAT Traversal (NAT-T) update to ensure product works correctly through NAT devices (typically required functionality):
    - Go to "Windows Update Catalog" through Microsoft Update site: http://update.microsoft.com/. Select **Use administrator options**, and then **search the**

Windows Update Catalog.

- Note that you need administrator rights to install (or search for) updates. Also ensure that you have up-to-date Windows Update; otherwise update search may be disabled.
- The search page requires you to install an ActiveX component (Windows Update).

- Search for the NAT-T Update
  - Select **Find Microsoft Windows updates**.
  - Select **Operating system**. Typical choices are **Windows XP SP1** (regardless of you Windows variant, i.e. for both Professional and Home editions).
  - Select **Language**. Typical choice is **English**.
  - Click **Advanced search options**.
  - Enter the update number "**818043**" in the **Contains these words** field.
  - Click **Search**.
  - Select **Recommended Updates**, and add the above update to your list of updates. (Leave other fields to default values.)
  - Click **Go to Download Basket**.
  - Download the update to your desktop: select **Browse**, select your Desktop, and click **Download Now**. Accept download license. **Note**: you need to allow popups from Microsoft Update for the download to work.
- Enter the folder, and browse through successive folders within the update package, looking for the update EXE file named **WindowsXP-KB818043-x86-ENU.EXE**. The full path to the update is similar to: (download folder) / WU / Software / en / com.microsoft.windowsxp / x86WinXP / com_microsoft.818043_Recommended_XPSP2_WinSE_35746 / WindowsXP-KB818043-x86-ENU.EXE.
- Execute the update, and reboot your computer for the update to take effect.

Windows XP without a Service Pack

- There is no NAT Traversal (NAT-T) support for Windows XP without a Service Pack.
  - Without NAT-T support remote access connections are not possible if the client computer is behind a NAT device (i.e., has a private address) or if the server computer is behind a NAT device (port forwarding).

  - Although remote access connections are possible without NAT-T support, such use is not recommended.

- **We recommend you update your Windows XP to SP2 (or at least SP1/SP1a).**

Known Limitations

None.

Configuration

To configure remote access for Windows XP, do as follows:

- Open **Control panel** => **Network connections** and click **Create new connection**. (Classic and XP theme have a slightly different layout.)

- You may be prompted for dialing information if you haven't configured it before. If you are not actually using a dialup modem connection, you can enter any information accepted by Windows; the settings have no effect on the remote access connection. You can enter the following information, for instance:

  - **What country/region are you in now?** => United States

  - **What area code (or city code) are you in now?** => 123

  - **If you need to specify a carrier code, what is it?** => 123

  - **If you dial a number to access an outside line, what is it?** => 123

  - **The phone system at this location uses:** => Tone dialing

  - **NOTE**: If you do need dialing rules for your actual modem connection, you do not need to enter “dummy” information.

- Start the connection creation wizard by clicking **Next**.

  - Select **Connect to the network at my workplace** and click **Next**.

  - Select **Virtual Private Network connection** and click **Next**.

  - Enter **Company Name** and click **Next**. The company name will become the name of your connection profile. Example: **Test Connection**.

  - You may be asked about initial connection dialing. If so, select **Do not dial the initial connection**, which is a good default for typical networks. Click **Next**. (If you are using GPRS or other dialup as a transport for your remote access connection, make the appropriate choice here).

- Enter the remote access server DNS name or IP address into the **Host name or IP address**... field. Click **Next**. Example: **vpn.company.com**.

- Select **Add a shortcut to this connection to my desktop**, and click Finish.

- Windows opens the connection windows automatically.

  - Click **Properties**.

  - Select **Security** tab and click **IPsec settings**. Check **Use pre-shared key for authentication** and enter the pre-shared key of the remote access server. Click **OK**. Example: **aY7bCa6g**.

  - Select **Networking** tab and change **Type of VPN** to **L2TP IPSec VPN**. This step is optional for Windows XP SP2, but required for other Windows versions. If left to default setting **Automatic**, first connection will take about 30 seconds to form while Windows autodetects the VPN connection type, but later connections will work normally.

  - Select **Internet Protocol (TCP/IP)** (still in **Networking** tab) and click **Properties**. Click **Advanced...** and ensure that **Use default gateway on remote network** is selected. This setting ensures that all traffic will be sent to the remote access connection when the connection is active. This is typically the desired behavior. Click **OK** to close the advanced settings dialog, then click **OK** to close the Internet Protocol (TCP/IP) dialog.

  - **OPTIONAL:** If you wish to improve the reliability of your remote access connection, you can enable automatic redialing. Select the **Options** tab. Alter settings e.g. as follows:

    - **Redial attempts** => 50

    - **Time between redial attempts** => 10 seconds

    - **Idle time before hanging up** => never

    - Check the **Redial if line is dropped** check box

  - These settings ensure that Windows automatically reconnects if the server is temporarily unavailable. However, other settings may be more appropriate for your environment.

  - Finally, click **OK** to close the properties window.

- If you wish to use fully automatic redialing:

  - Enter the username and password in the connection dialog. Check the **Save this user name and password for the following users** checkbox and select **Anyone who uses**

this computer option. These settings ensure that redialing does not require interaction (password entry).

- If the computer is used by several people, do not select **Save this user name and password for the following users** checkbox, as it may be a security risk.

- Close the connection dialog by clicking **Cancel**.

Testing

Test your newly configured remote access connection profile as follows:

- Double click the connection icon on your desktop, or use **Control panel** => **Network connections** to open your connection.

- Enter your username and password to the dialog (if not added previously) and click **Connect**. If your settings are correct, the connection window will disappear and tray balloon will indicate that the connection is active.

- You should ensure that connectivity to your remote network resources work correctly. One simple test is to the use the **ping** command in the command prompt.

Apple Mac Os X

Prerequisites

None.

Known Limitations

The following limitations apply to Mac Os X use:

- When switching from one user to another, the VPN connection is automatically dropped by the operating system for security reasons.
- When suspending and resuming (by closing laptop lid, for instance), the VPN connection will drop due to protocol timeouts but the OS will not notice this immediately when resuming. Disconnect and reconnect the VPN connection when resuming from suspend mode.

Configuration

- Open **System Preferences**. Select **Internet & Network** => **Network**.
- Select **VPN (L2TP)**. Click **Configure...**.
- Open the **Configuration** drop-down menu Select **Edit Configurations** from the menu.
- Enter remote access information into the configuration fields. Example:
  - **Description** => Test Connection
  - **Server Address** => vpn.company.com
  - **Account Name** => john.doe
  - **User Authentication** => **Password** (enter your password here)
  - **Machine Authentication** => **Shared Secret** (enter server pre-shared key here)
- Click **OK** to finish configuration.
- The newly created profile is shown in the user interface. Check that the profile values are correct. Check the **Show VPN status in menu bar** check box to make the VPN connection accessible directly from the menu.
- Click **Connect** to activate the connection. You can also activate the connection directly from the top menu.

Testing

- Activate the connection from the top menu.
- Open a terminal.
- Check the reachability of a server behind the remote access connection using the **ping** command.

Windows Vista

Prerequisites

NOTE: These instructions are based on Windows Vista Beta 2 and RC1 and may differ slightly from the final Vista release version.

Vista prompts for administrative confirmation several times during the configuration process. Allow all operations required by the configuration process. The confirmation dialogs are not described in the configuration process below.

Known Limitations

None.

Configuration

- Open **Network Center** through **Start** => **Network** => **Network Center**.
- Click **Set up a connection or network** to start the connection creation wizard.
  - Select **Connect to a Workplace** and click **Next**.
  - If you have an existing connection of this type, Windows will prompt whether you want to use the existing connection or create new one. Select **No, create a new connection** and click **Next**.
  - Click **Use my Internet connection (VPN)**.
  - Enter the remote access server address into the **Internet address** field and a name for this profile (example: **Test Connection**) into the **Destination name** field.
  - Ensure that the **Use a smart card** check box is cleared.
  - Select whether you want to share this connection with other Windows Vista users. If so, select the **Allow other people to use this connection** check box, otherwise clear it.
  - Check the **Don't connect now; just set it up so I can connect later** check box.
  - Click **Next**.
  - Vista will ask for a username and password. Click **Create** without entering any information (username and password will be entered later).
  - Click **Close** to complete basic configuration.

- Click **Manage network connections** (**Network Connections**) from **Network Center**.
    - Press F5 to ensure network list has been refreshed. (This was sometimes necessary in Windows Vista Beta 2, but may not be necessary in later versions.)
    - Select the newly created remote access connection, right click to get the context menu, and select **Properties**.
    - Select **Networking** tab and do the following:
        - Click **IPSec settings**. Check **Use pre-shared key for authentication** and enter the pre-shared key of the remote access server (example: **aY7bCa6g**). Click **OK**.
        - Check that **Type of VPN** is set to **L2TP IPsec VPN**.
            - You can also use the **Automatic** VPN type, but automatic VPN type detection adds unnecessary delay to connection setup. We recommend you select the **L2TP IPsec VPN** type.
        - Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**. Click **Advanced...** and ensure that **Use default gateway on remote network** is selected. This setting ensures that all traffic will be sent to the remote access connection when the connection is active. This is typically the desired behavior. Click **OK** to close the advanced settings dialog, then click **OK** to close the Internet Protocol Version 4 (TCP/IPv4) dialog.
    - **OPTIONAL:** If you wish to improve the reliability of your remote access connection, you can enable automatic redialing. Select the **Options** tab. Alter settings e.g. as follows:
        - **Redial attempts** => 50
        - **Time between redial attempts** => 10 seconds
        - **Idle time before hanging up** => never
        - Check the **Redial if line is dropped** check box
        - **Note:** Windows Vista Beta 2 has an **Idle threshold** setting which is disabled. This has no effect on the connection.
        - **Note: Redial if line is dropped** is enabled by default in Vista. The setting is disabled by default in Windows XP and Windows 2000.
    - These settings ensure that Windows automatically reconnects if the server is temporarily unavailable. However, other settings may be more appropriate for your environment.
    - Finally, click **OK** to close the properties window.

Testing

Test your connection profile as follows:

- Open **Network Connections** (**Start** => **Network**, then click **Manage network connections**).
- Start the connection by selecting your connection profile, clicking right mouse button to open the context menu, and by selecting the **Connect** option from the menu.
    - Enter the username and password in the connection dialog. Check the **Save this user name and password for the following users** checkbox and select **Anyone who uses this computer** option. These settings ensure that redialing does not require interaction (password entry).
    - If the computer is used by several people, do not select **Save this user name and password for the following users** checkbox, as it may be a security risk.
- Click **Connect**.
- You should ensure that connectivity to your remote network resources work correctly. One simple test is to the use the **ping** command in the command prompt.

Linux

Linux remote access requires a free, open source remote access client available from http://www.codebay.fi/. Please request installation and configuration information from info@codebay.fi.

Windows 2000 (SP4)

Prerequisites

Please check the following prerequisites before starting configuration:

- Ensure that you have administrator privileges.
- Upgrade Windows 2000 to latest service pack (currently SP4)
- Ensure that you have High Encryption Pack (HEP) installed. Some export versions of Windows 2000 require a separate HEP pack to enable 3DES encryption support. Without this support, remote access connections will fail silently. If unsure, download and install HEP to be sure.
- Install Windows 2000 NAT traversal update. The update can be downloaded through Microsoft Update. See Windows XP SP1 instructions for details. Select **Windows 2000 Professional SP4** as **Operating system** when searching for the update.

Known Limitations

Windows 2000 SP4 interoperates with VPNease remote access server with the following limitations:

- NAT-T update is required from Microsoft Update. See instructions for Windows XP SP1 for details, using **Windows 2000 Professional SP4** as **Operating system** in the advanced search.
- Windows 2000 does not support easy configuration of pre-shared key IPsec authentication. IPsec policies for encryption must be created manually using Microsoft Management Console (mmc).
- Remote access server can only be specified using IP address, not a DNS name, because of limitations in the IPsec policy model.
- When Windows 2000 changes network point of attachment (current IP address), it takes some time before Windows 2000 can re-establish the remote access connection. This is caused by Windows 2000 IPsec implementation limitations. By using short IPsec renegotiation period this limitation can be minimized so that reconnection is possible after 5 minutes.

Detailed configuration instructions are given below.

Configuration

Step 1: Configure L2TP/IPsec Connection

First configure an L2TP/IPsec remote access connection following the Windows XP instructions with the following differences:

- Pre-shared key cannot be entered at this stage as Windows 2000 does not support pre-shared key authentication for remote access directly.

- The VPN server address should be entered as an IP address (e.g. **123.123.123.123**) because of Windows 2000 IPsec policy limitations.

Step 2: Disable Automatic L2TP/IPsec IPsec Policy

- Add the following registry **REG_DWORD** value using **regedit**:

```
HKEY_LOCAL_MACHINE\
  System\
    CurrentControlSet\
      Services\
        Rasman\
          Parameters\
            ProhibitIpSec
```

- Set the **REG_DWORD** value to **1**.

- Reboot your computer.

Step 3: Create a New L2TP/IPsec IPsec Policy

- Start the Microsoft Management Console by clicking **Start => Run**, entering **mmc**, and pressing **Enter**.

- Select **Console => Add/Remove Snap-In**. Click **Add** and select **IPsec Security Policy Management**. Click **Add** followed by **Finish**. Click **Close**, then **OK**.

- Right click on **IP Security Policies on Local Machine** to open the context menu, and select **Create IP Security Policy** from the menu. Click **Next** to start the wizard.

  - Enter a name for the policy in the **Name** field (example: **L2TP/IPsec Policy**). Click **Next**.

  - Clear the **Activate the default response rule** check box and click **Next**.

  - Ensure that the **Edit properties** check box is checked and click **Finish**.

  - Select **Rules** tab, click **Add** followed by **Next** to start the wizard.

  - Click **This rule does not specify a tunnel** and click **Next**.

  - Click **All network connections** and click **Next**.

  - Click **Use this string to protect the key exchange (pre-shared key)**, type in your server pre-shared key (example: **aY7bCa6g**). Click **Next**.

- Click **Add** in the IP filter list window.
    - Enter a name for the filter (example: **L2TP/IPsec Filter**). Click **Add** followed by **Next** to start the wizard.
    - In IP traffic source window, select **Any IP Address** from the drop-down menu. Click **Next**.
    - In IP traffic destination window, select **A specific IP Address** from the drop-down menu. Enter the remote access server IP address (example: **123.123.123.123**) into the field. Click **Next**.
    - In IP protocol type window, select **UDP** from the drop-down menu. Click **Next**.
    - In IP protocol port window, select **From this port** and enter **1701** in the text field below. Select **To any port**. Click **Next**.
    - Ensure that the **Edit properties** check box is checked and click **Finish**.
        - Ensure that the check box **Mirrored. Also match packets with the exact opposite source and destination addresses.** is checked. Click **OK**. Click **Close** to get back to the IP filter list window.
    - Select the newly created IP filter and click **Next**.
- Click **Add** and **Next** to start the wizard in the IP filter action window.
    - Enter a name for the filter action (example: **L2TP/IPsec Action**) and click **Next**.
    - Select **Negotiate security**. Click **Next**.
    - Select **Do not communicate with computers that do not support IPSec**. Click **Next**.
    - Select **Custom** and click **Settings...**. Make the following settings:
        - Data and address integrity without encryption (AH) => not checked
        - Data integrity and encryption => checked
        - Select **MD5** integrity algorithm
        - Select **3DES** encryption algorithm
    - Click **OK**, followed by **Next**, and finally **Finish**.
- Select the newly created action and click **Edit**.

    - Uncheck **Accept unsecured communication, but always respond using IPSec**.

    - Select the topmost entry in the **Security Method preference order** list. Click **Edit**. Select **Custom (for expert users)** and click **Settings...**. Check **Generate a new key every** and enter **300** (5 minutes) in the text field. Click **OK** three times to close the nested windows.

  - Select the action again and click **Next**, **Finish**, and **Close** to complete the policy creation wizard.

  - Select the filter action just created (ensure that the radiobutton becomes active) and click **Next**, then click **Finish.**

  - Finally, click **Close** to complete the wizard.

- Right click the newly created IPsec policy and select **Assign** from the context menu.

- Close the Microsoft Management Console.

Testing

Please follow the Windows XP testing procedure to test the new remote access connection.

Pocket PC / Windows Mobile

Pocket PC 2003SE and Windows Mobile 5.0 devices have L2TP/IPsec compatible VPN remote access clients. VPNease supports these built-in clients. Please request installation and configuration information from info@codebay.fi.

Other Platforms

Windows 95, Windows 98, Windows ME

The Microsoft L2TP/IPsec VPN Client ("MSL2TP") supports L2TP/IPsec remote access connections, but is no longer supported by Microsoft. VPNease does not support these clients.

Open Source Clients

Because the L2TP/IPsec protocol is based on open standards (IPsec, L2TP, PPP), open source client software can be made to interoperate with VPNease. Getting the IPsec configuration to work is usually the most challenging part, especially with regards to NAT traversal. The following web page has useful configuration information:

- http://www.jacco2.dds.nl/networking/freeswan-l2tp.html

General requirements include:

- IPsec: main mode and quick mode with pre-shared key authentication, transport mode, NAT traversal (draft or RFC version) in transport mode.
- L2TP: capable of acting as an L2TP initiator.
- PPP: no known impediments to compatibility.
- Root or sudo privileges are usually required to configure and use remote access on UNIX platforms.

The following open source projects are known to work in L2TP/IPsec client configuration:

- IPsec: pluto (openswan), racoon
- L2TP: openl2tp, l2tpd
- PPP: pppd