# How to Configure a Client-to-Site PPTP VPN

https://campus.barracuda.com/doc/79462870/

Barracuda CloudGen Firewall supports PPTP VPNs with 40-, 56-, and 128-bit MPPE.

## Supported VPN Clients

Use a standard-compliant PPTP client, such as the native Windows VPN client.

## Limitations

- As of 2012, PPTP is no longer considered secure. It is highly recommended that you switch away from PPTP.
- Only IPv4 addresses are supported.

## Using PPTP with MPPE on Windows 7 and Above

If you want to establish a PPTP connection with a 40- or 56-bit MPPE using Windows 7 or above, you must configure the AllowPPTPWeakCrypto registry key.

1. Locate the AllowPPTPWeakCrypto registry key: `HKLM\System\CurrentControlSet\Services\Rasman\Parameters\AllowPPTPWeakCrypto`
2. Change the value of the registry key to 1.
3. Reboot your system.

## Step 1. Configure General Settings

Configure the general settings for all L2TP/IPsec and PPTP connections.

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN-Service > L2TP/PPTP Settings**.
2. Click **Lock**.
3. Edit the following general settings for PPTP:
   - **First DNS | Second DNS** – The IP addresses of the first and secondary DNS servers for

use by the VPN clients.
- **First WINS | Second WINS** – The IP addresses of the primary and secondary WINS server.
- **Static IP** – To assign static IP addresses to your VPN clients, select *yes* .

4. Click **Send Changes** and **Activate** .

### Step 2. Configure the PPTP VPN Server

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN-Service > L2TP/PPTP Settings**.
2. In the left menu, select **PPTP**.
3. Click **Lock**.
4. From the **PPTP Enable** list, select **yes**.
5. In the **PPTP Settings** section, configure the following settings:
   - **PPTP  Listen IP** – The IP address on which the Barracuda CloudGen Firewall will listen for PPTP connections.
   - **Local Tunnel IP** – The local IP address that the PPTP client connects to.
   - **Pool IP Begin** – The first IP address from the reserved subnet of the local network range (e.g., *10.0.0.50).*
   - **Pool Size** – The number of IP addresses that are available for PPTP clients. You can specify a maximum of 100 IP addresses.
   - **User Authentication** – The authentication scheme used. If you are using external MS-CHAPv2 authentication, select *external MS-CHAPv2*. Otherwise, select *Local-user-database*.
6. Click **Send Changes** and **Activate**.

### Step 3. (For local authentication or static IP addresses) Configure a User List

If you are not using an external authentication scheme or must assign static IP addresses, you can manage users locally on the Barracuda CloudGen Firewall.

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN-Service > L2TP/PPTP Settings**.
2. In the left menu, select  **User List** .
3. Click **Lock**.
4. In the **Username** table, add users.
   - Usernames must be unique.
   - Only enter an IP address if you enabled **Static IP** in **General Settings**.
5. Click **OK**.
6. Click **Send Changes** and **Activate**.

## Troubleshooting

To troubleshoot VPN connections, see the `/VPN/pptpd` log file. For more information, see LOGS Tab

## PPTP Settings Overview

The following table provides more details on the PPTP settings that you can configure on the **L2TP/PPTP Settings - PPTP** page.

| Settings | Description |
|---|---|
| **PPTP Listen IP** | The IP address that the PPTP service listens on. |
| **Initiation Timeout [s]** | The maximum time for establishing the GRE tunnel. You can keep the default value for this setting. The faster the connection, the shorter this timeout can be set. |
| **Local Tunnel IP** | The server-side network address of the tunnel. For example, `10.0.8.1`.<br>• Do not use a Destination NAT firewall rule to forward PPTP connections to the PPTP server IP address.<br>• Inside the L2TP/PPTP configuration, the PPTP bind IP address must be the IP address of the VPN point of entry (the IP address where the PPTP clients terminate). |
| **Pool IP-Begin** | The first IP address in the address pool that is available to clients. |
| **Pool Size** | The number of network addresses that are available for VPN clients. The maximum number of clients allowed is 100. |
| **MPPE Encryption Strength** | The required encryption strength. You can keep the default value for this setting. Available options are:<br>• **40bit**<br>• **128bit**<br>• **election**<br>• **disable**<br>To use the strongest available encryption, select **election**. |
| **LCP Echo Interval** | The interval between LCP echo requests (default: `0`). |
| **Idle Timeout** | The maximum length of time that the VPN tunnel can remain idle before the connection is terminated (default: `300`). |
| **User authentication** | The user authentication method. You can select either **Local-user-database** or **Remote MS-CHAP-v2**. |
| **Allowed Users** | In this table, add filters to include the names of allowed VPN clients. For no restrictions, leave this table blank. You can also create a statement with the asterisk (*****) and question mark (**?**) as wildcard characters. |

| | |
|---|---|
| **Allowed Groups** | In this table, you can enter groups or create a statement with the asterisk (*****) and question mark (**?**) as wildcard characters.<br>Because MS-CHAP-v2 cannot handle user groups, you must configure an additional authentication helper scheme. Group restrictions require the MSAD authentication scheme. |
| **User info helper scheme** | The helper authentication scheme for gathering user group information. The default scheme is **MSAD**. To use another scheme, select the **Other** check box and then enter the scheme name. |