How to Configure a Client-to-Site PPTP VPN

https://campus.barracuda.com/doc/73700268/

> As of 2012, PPTP is no longer considered secure. It is highly recommended that you switch away from PPTP because of the security risks involved.

Using VPNs, mobile workers can securely access corporate information and resources. The CloudGen Firewall allows all operating systems with PPTP clients to connect via a client-to-site VPN.

Step 1. Configure the Firewall VPN Server

The VPN server that runs on the firewall must listen on the appropriate IP address for the clients. Depending on whether the firewall is connected to the Internet through an ISP that statically or dynamically assigns the WAN IP address, complete the steps in the appropriate section.

Static WAN IP Address

If the firewall is connected to the Internet through an ISP that statically assigns the WAN IP address:

1. Go to **NETWORK > IP Configuration**.
2. In the **Static Interface Configuration** section, or on any **Secondary IP Address** of the management IP address, verify that the **VPN Server** check box for the interface is selected.

Dynamic WAN IP Address

To allow VPN connections using a dynamically assigned WAN IP address on the firewall, follow the steps in How to Configure VPN Access via a Dynamic WAN IP Address.

Step 2. Enable PPTP on the Firewall

1. Go to **VPN > PPTP**.
2. In the **PPTP Settings** section, set **Enable PPTP VPN** to **Yes**.
3. Enter the **PPTP Listen IP** address for clients to connect to.
4. In the **Pool IP Begin** field, enter the starting IP address for the pool of IP addresses made available for clients.
5. In the **Pool Size** field, enter the number of IP addresses made available for clients, starting with the IP address configured in **Pool IP Begin**.
6. In the **Local Tunnel IP** field, enter the server-side IP address of the tunnel.
7. Enter the address of the server(s) that will be assigned to the clients.

8. Configure encryption settings according to your requirements.
9. Click **Save**.

Step 3. Configure User Authentication

For user authentication, you can use local authentication or MS-CHAPv2/NTLM.

Local Authentication

To configure user access permissions with **Local Authentication**:

1. Go to **VPN > PPTP**.
2. In the **Local PPTP Users** section, add the username and password for each user who is allowed to connect to the VPN. If required, specify a static IP address for the user. Click **Add** after each entry.
3. Click **Save**.

MS-CHAPv2/NTLM

With **MS-CHAPv2/NTLM**, you can allow access on a per-user or per-group basis. Successful authentication is only possible for users that are matching the conditions in **Allowed Users** AND **Allowed Groups**.

1. Go to **VPN > PPTP**.
2. In the **User and Group Conditions (MS-CHAPv2/NTLM)** section, add the users and groups who are allowed to connect to the client-to-site VPN. Click **Add** after each entry.
3. Click **Save**.

Step 4. Add an Access Rule to Allow Traffic Between VPN Clients and LAN

Create a new access rule to let PPTP traffic in the VPN tunnel pass between the VPN clients and the trusted LAN.

1. Go to **FIREWALL > Access Rules**.
2. Click **Add Access Rule**. The **Add Access Rule** window opens.
3. Enter a **Name** for the rule. For example: `PPTP-to-LAN`
4. Specify the following settings:
   - **Action** – Select **Pass**.
   - **Connection** – Select **Original Source IP**.
   - **Source** – Select the network range assigned to the PPTP clients (configured in **VPN > PPTP > Client IP Pool Begin/Client IP Pool Size**).

- **Network Services** – Select **Any** (or the allowed/required services).
- **Destination** – Select **Trusted LAN**.

5. Click **Save**.
6. Move the access rule above the BLOCKALL rule so it is the first access rule to match incoming VPN traffic.
7. Click **Save**.