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

https://campus.barracuda.com/doc/13306975/

> 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 Barracuda NextGen Firewall X-Series allows all operating systems with PPTP clients to connect via a client-to-site VPN.

Follow the steps in this article to configure a client-to-site VPN using PPTP.

Step 1. Configure the X-Series Firewall VPN Server

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

Static WAN IP Address

If the X-Series Firewall is connected to the Internet through an ISP that statically assigns the WAN IP address:

1. Go to the **NETWORK > IP Configuration** page.
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 X-Series Firewall, follow the steps in How to Allow VPN Access via a Dynamic WAN IP Address.

Step 2. Configure the PPTP Settings on the X-Series Firewall

Configure PPTP to let remote devices access the X-Series Firewall VPN.

1. Go to the **VPN > PPTP** page.

2. In the **PPTP Settings** section, enable and configure PPTP.
3. On the same page, configure the user authentication method:
   - For local authentication, configure the settings in the **Local PPTP Users** section.
   - For MS-CHAPv2 and NTLM authentication, configure the settings in the **User and Group Conditions (MS-CHAPv2/NTLM)** section.

For more information on the PPTP and authentication settings, click **Help** on the **VPN > PPTP** page.

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 the **VPN > PPTP** page.
2. In the **Local PPTP User** 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.
3. Click **Save Changes**.

MS-CHAPv2/NTLM

With **MS-CHAPv2/NTLM**, you can allow access on a per-user or per-group basis.

1. Go to the **VPN > PPTP** page.
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.
   > Note that successful authentication is only possible for users that are matching the conditions in **Allowed Users** AND **Allowed Groups**.
3. Click **Save Changes**.

Step 4. Add the Firewall Rule to Allow Traffic Between VPN Clients and LAN

Create a new firewall rule to let PPTP traffic in the VPN tunnel pass between the VPN clients and the trusted LAN. The pre-installed VPNCLIENTS-2-LAN firewall rule does not match PPTP connections because they do not use the pvpn0 virtual interface. As a result, PPTP traffic is blocked by default.

Create a new firewall rule that lets VPN traffic from the PPTP clients access the Trusted LAN:

1. Go to the **FIREWALL > Firewall Rules** page and add this rule:

Action	Source	Destination	Service	Connection
Allow	The network range assigned to the PPTP clients (configured in **VPN > PPTP > Client IP Pool Begin/Client IP Pool Size**)	**Trusted LAN**	**Any** (or the allowed/required services)	**No SNAT** (the original source IP address is used)

2. At the top of the **Add Access Rule** window, click **Add**.

Step 5. Verify the Order of the Firewall Rules

New rules are created at the bottom of the firewall rule set. Because rules are processed from top to bottom in the rule set, arrange your rules in the correct order. You must especially ensure that your rules are placed above the BLOCKALL rule; otherwise, the rules are blocked.

After adjusting the order of rules in the rule set, click **Save**.