How to Configure IPsec

https://campus.barracuda.com/doc/39813189/

You can configure the Barracuda SSL VPN to allow L2TP/IPsec connections from remote devices using an L2TP/IPsec client that supports using a pre-shared key (PSK) as an authentication protocol. L2TP/IPsec clients are also standard on most smartphones, including Apple iPhones and iPads, smartphones running Android 1.6 or higher and tablets running Android 3.0 or higher.

Before you begin

On your organization's firewall, allow authentication traffic to and from the Barracuda SSL VPN. UDP over ports 500 and 4500 must be enabled to reach the Barracuda SSL VPN for L2TP/IPsec connections to function.

Step 1. Configure the IPsec server

On the Barracuda SSL VPN, configure the IPsec server to allow your remote users to authenticate and connect to the protected network:

1. Log into the SSL VPN web interface.
2. Navigate to the **RESOURCES > IPsec Server** page.
3. Verify that you have selected the correct user database on the top right of the page.
4. In the **Create IPsec Server** section, enter a descriptive name for your IPsec server.
5. Enter the preshared key. The string must be alphanumeric.
6. In the **IP Range Start/End** fields, enter the first and last IP address of the DHCP range that should be assigned to remote systems connecting via IPsec.
   This IP range must reside in the network range that is configured in the **TCP/IP Configuration** of the applicance interface, and MUST NOT be part of any other DHCP range on your LAN.
7. From the **Policies** list, select the available policies that you want to apply to the IPsec server, and add them to the **Selected Policies** list.
8. Click **Add**.

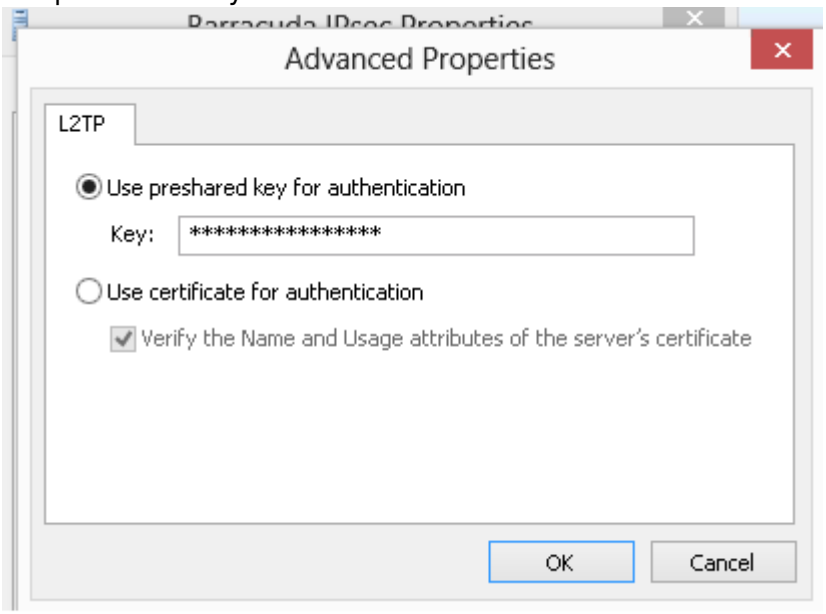
The IPsec Server is now created and appears in the **IPsec Server** section. You can test the configuration by clicking the **Launch** link associated with the entry.

Step 2. Create an L2TP/IPsec connection

On your remote device, create an L2TP/IPsec connection to the Barracuda SSL VPN.

If the remote device has had a VPN client *un*installed at some point, then make sure that the IPsec service has been re-enabled in order to allow connections via L2TP/IPsec.

1. Log into the Barracuda SSL VPN on the client device.
2. Go to the **Resources** tab.
3. From **My Resources**, select the IPsec server and click to launch it.
   During the connection, you will be prompted with a certificate warning message:
   1. Go to your network connections, right click the SSL VPN connection and go to the properties.
   2. Under the **Security** tab, click **Advanced settings** in the **Type of VPN** section, and enter the preshared key.



   3. Click **OK** twice to exit the connection properties.
4. Connect to the IPsec server.

Step 3. Apply the installation to the client device

Once you are successfully connected, provision the device configuration to the client device. Be aware, that, for this procedure, the user must have been granted the appropriate access rights. For more information, see: Provisioning Client Devices.

1. From the **Resources** tab of the client device, go to **Device Configuration**.
2. Tick the checkbox unter the IPsec server entry.

3. Click **Provision** on the bottom of the page.

Figures