

With the increasing number of road warriors and telecommuters relying on mobile devices such as smartphones and netbooks for work, it is vital that a secure method exists for them to connect from their remote location to the protected, internal network. Many of the devices in use today already support two of the most popular protocols for secured communications.

L2TP, or Layer 2 Tunneling Protocol, enables point-to-point connections from one device or system to another. Security for these L2TP connections is taken care of with IPsec (Internet Protocol Security), which provides authentication and encryption of all packet traffic. The term **L2TP/IPsec** refers to the combination of these two protocols when they are used to secure connections such as those made from remote devices, such as smartphones and laptops, to systems on a protected network. **PPTP**, or Point-to-Point Tunneling Protocol, enables authorized mobile devices, including smartphones, to access your organization's private network in a secure manner. The Barracuda SSL VPN can be easily configured to work with either protocol in just a few simple steps.

### Requirements for Connecting with L2TP/IPsec or PPTP

To allow connections using L2TP/IPsec or PPTP, three separate items must be configured:

- A client on the **remote device**
- Your organization's **firewall**
- The **L2TP/IPsec or PPTP server** on your Barracuda SSL VPN

The **remote device** must have an appropriate client that supports the desired protocol. For L2TP/IPsec, the client must support PSK, or Pre-Shared Key, as an authentication protocol. For PPTP, the client must support a Challenge-handshake authentication protocol, preferably MSCHAPv2.

The following chart indicates the operating systems that have built-in clients:

L2TP/IPsec	PPTP
Microsoft Windows 2000 or higher	Microsoft Windows XP or higher
Microsoft Windows Mobile 2003 (Ozone) Premium Edition, or higher	Microsoft Windows Mobile 2003 (Ozone) or higher
Mac OS X 10.3 (Panther) or higher	Mac OS X 10.2 (Jaguar) or higher
Linux 2.0 (or equivalent) or higher, with Openswan (implementation of IPsec)	SuSE Linux 10 (or equivalent), or higher
Apple iPhones and iPads running iOS 4.2.1 and higher	
Smartphones running Android 1.6 (Donut) or higher	
Tablets running Android 3.0 (Honeycomb) or higher	

Next, if your deployment includes a firewall between the Barracuda SSL VPN and the Internet, then that **firewall** must be configured to allow the following authentication traffic to the Barracuda SSL VPN.

- for **L2TP/IPsec**: UDP over ports 500 and 4500
- for **PPTP**: TCP over port 1723 and GRE (IP protocol 47)

Finally, the appropriate **IPsec** and/or **PPTP server** must be enabled on the Barracuda SSL VPN to allow your remote users to authenticate and connect to the protected network. **Important:** Due to the nature of IPsec, the remote system must not be using an IP address that falls into a range that is used inside the protected network.

Support for connecting via L2TP/IPsec or PPTP is on all Barracuda SSL VPN models starting with the 2.1 firmware release.

## The Barracuda SSL VPN IPsec Server

The Barracuda SSL VPN acts as its own IPsec server, authenticating remote users and assigning to them an IP address from a specified DHCP range. The maximum number of total concurrent users, whether connecting via IPsec or otherwise, is determined by the model of your Barracuda SSL VPN.

All configurations are done from the **RESOURCES > IPsec Server** page, by the *ssladmin* administrative user.

The only items that are required to enable the IPsec server are the following:

- **Name** – A label for this IPsec server configuration. This will also be the Resource name of the Barracuda SSL VPN IPsec Configuration Tool that authorized users will see on their **My Resources** page.
- **Pre-Shared Key** – The passphrase that is required along with user authentication.
- **IP Address Range Start** and **End** fields – The first and last IP addresses of a DHCP range that can be assigned to remote devices. To prevent IP conflicts, the specified range cannot be a part of any other existing DHCP range such as one used for the Barracuda Network Connector or for PPTP connections.
- **Policies** – The Policies that contain the users who will be allowed access to this IPsec server configuration.

If you have a dual NIC configured, the Barracuda SSL VPN will only listen on the public interface, and assign IP addresses from the private interface.

Additional items that can also be configured are:

- **Primary** and **Secondary DNS Server** – The DNS servers used to resolve all supplied hostnames.
- **Primary** and **Secondary WINS Server** – The WINS servers used to resolve all supplied hostnames.

**Note:** If the IP address of the remote device is one that falls into an IP address space used by the secured network, then IP address conflicts may result.

The IPsec server is enabled by default as soon as it is configured, but can be temporarily disabled if so desired. Disabling the IPsec server immediately disconnects all remote users that are currently connected at the time.

### Authentication Methods

Only those users in a Policy associated with the IPsec server configuration will be allowed to connect via L2TP/IPsec to the Barracuda SSL VPN. In addition, every connecting device must also be configured with the **PSK**, or Pre-Shared Key, that was specified on the IPsec server, before the Barracuda SSL VPN will accept and process the connection request. All authorized accounts will use the same PSK.

Because all usernames and passwords are sent over IPsec which is inherently secure, password authentication is done via PAP, with the user validity verified via L2TP against the active User Database on the Barracuda SSL VPN.

## The Barracuda SSL VPN PPTP Server

The Barracuda SSL VPN also acts as its own PPTP server, authenticating remote users and assigning to them an IP address from a specified DHCP range. The maximum number of total concurrent users, whether connecting via PPTP or otherwise, is determined by the model of your Barracuda SSL VPN.

All configurations are done from the **RESOURCES > PPTP Server** page, by the *ssladmin* administrative user.

The only items that are required to enable the IPsec server are the following:

- **Name** – A label for this PPTP server configuration.
- **IP Address Range Start** and **End** fields – The first and last IP addresses of a DHCP range that can be assigned to remote devices. This range must be reachable from the Barracuda SSL VPN, and to prevent IP conflicts no part of this range should overlap with any other existing DHCP range, such as one used for the Barracuda Network Connector or for IPsec connections.
- **Policies** – The Policies that contain the users who will be allowed access to this PPTP server configuration.

If you have a dual NIC configured, the Barracuda SSL VPN will only listen on the public interface, and assign IP addresses from the private interface.

Additional items that can also be configured are:

- **Primary** and **Secondary DNS Server** – The DNS servers used to resolve all supplied hostnames.
- **Primary** and **Secondary WINS Server** – The WINS servers used to resolve all supplied hostnames.

The PPTP server is enabled by default as soon as it is configured, but can be temporarily disabled if so desired. Disabling the PPTP server immediately disconnects all remote users that are currently connected at the time.

### Authentication Method

Only those users in a Policy associated with the PPTP server configuration will be allowed to connect via PPTP to the Barracuda SSL VPN. A remote user is authorized against the User Database that is active at the time of connection, and by default the Barracuda SSL VPN will use **MSCHAPv2 with MPPE** (128-bit Microsoft Point-to-Point Encryption) to authenticate passwords. This protocol is the most secure since it also provides encryption of the PPTP session, but other methods are also available (from the **RESOURCES > Configuration** page, in the PPTP section):

## Remote Device Configurations

**L2TP/IPsec** connections are not possible if you are already within the protected network, or if the remote device has an IP address that falls into an IP address space belonging to the protected network.

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

Users wishing to connect via **PPTP** must first log into the Web interface of the Barracuda SSL VPN, and also after any password change, prior to attempting a PPTP connection from a remote device. In a Web browser, go to the login page of the Barracuda SSL VPN; e.g.:

`https://sslvpn.example.com`

Once the prerequisites have been met, the remote device simply needs to have a VPN connection configured to connect to the Barracuda SSL VPN. In most cases, the remote user will only need the following information:

- the FQDN or IP address of the Barracuda SSL VPN; e.g., `sslvpn.example.com`
- the account name for the connecting user; e.g., `psmith`
- the password for the username specified above.
- (for L2TP connections only): the PSK for the Barracuda SSL VPN

For remote systems using Windows XP or higher, the Barracuda SSL VPN IPsec Configuration Tool will automatically configure an L2TP/IPsec connection on that system. All the remote user needs to do is log into Web interface of the Barracuda SSL VPN and click the Resource to automatically create an IPsec connection for your protected network.