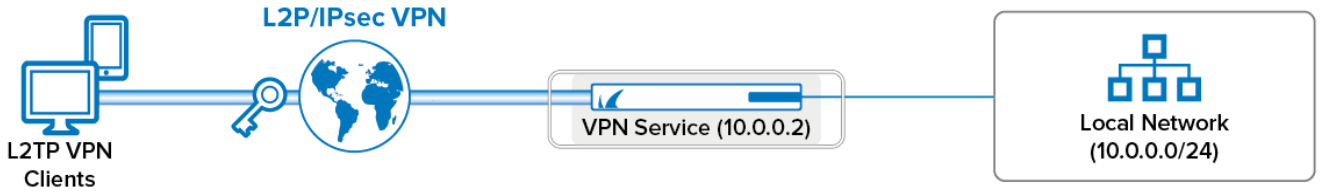
How to Configure a Client-to-Site L2TP/IPsec VPN

https://campus.barracuda.com/doc/17379/

Follow the instructions in this article to configure a client-to-site L2TP/IPsec VPN. With this configuration, IPsec encrypts the payload data of the VPN because L2TP does not provide encryption. L2TP/IPsec VPN connections can only be created between two devices using IPv4 addresses.



Supported VPN Clients

Use a standard-compliant L2TP/IPsec client, such as the native Windows VPN client.

Before You Begin

- Set up the VPN certificates for External CA. For more information, see How to Set Up External CA VPN Certificates.
  In the default server certificate, you must set the SubAltName with the FQDN that resolves to the listening IP address of the VPN service.
- Configure an external authentication scheme. If an authentication service other than MSCHAPv2 or local DB is used, the client must transmit the password in plaintext (PAP). For more information, see Authentication.

Step 1. Configure General Settings

Configure the general settings to be applied to all L2TP/IPsec connections.

1. Open the **L2TP/PPTP Settings** page for the VPN service (**Configuration > Configuration Tree > Box > Assigned Services > VPN-Service**).
2. Click **Lock**.
3. Edit the following general settings for L2TP/IPsec access:
   - **First DNS | Second DNS** – The IP addresses of the first and secondary DNS servers for the VPN client.
   - **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. If you enable this option, you must also configure a user list. See Step 4.

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

Step 2. Configure L2TP/IPsec VPN

Enable L2TP and configure the L2TP-specific settings.

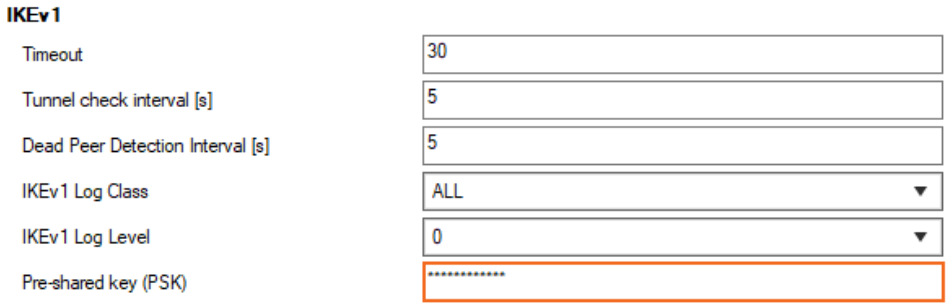
1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN-Service > L2TP/PPTP Settings**.
2. In the left menu, select **L2TP/IPSEC**.
3. Click **Lock**.
4. From the **Enable L2TP** list, select **yes**.
5. In the **L2TP Settings** section, specify the following settings:
   - **L2TP Listen IP** – The IP address that the L2TP/IPsec service will listen on, or, in other words, the public IP address on the WAN that the L2TP client connects to.
     L2TP does not work if client IP address and listen IP reside in the same subnet.
   - **Local Tunnel IP** – The gateway's IP address in the VPN subnet (e.g., `10.0.10.1`).
     When using Barracuda Network Access / VPN Client simultaneously, the VPN client network must not be the same as a VPN network used for NAC connections.
   - **Pool IP-Begin** – The first IP address for L2TP/IPsec clients accessing the VPN subnet (e.g., `10.0.10.2`).
   - **Pool Size** – The number of addresses that are available for L2TP/IPsec clients (e.g., `50`).
6. In the **Authentication Settings** section, specify the L2TP authentication settings:
   - **User Authentication** – The authentication service.
   - **Authentication Scheme (external authentication only)** – The authentication scheme. For more information, see Authentication.
     When using an authentication scheme, the VPN client must be configured to use unencrypted passwords (PAP).
   - **Allowed Users (MS-CHAP-v2 only)** – The specific users who are allowed to connect to the VPN. To allow all users, leave this table empty.
   - **Allowed Groups (MS-CHAP-v2 only)** – The specific groups that are allowed to connect to the VPN. To allow all groups, leave this table empty.
7. Click **Send Changes** and **Activate**.

Step 3. Configure IPsec PSK

You must configure the pre-shared key in the IPSec settings.

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN > VPN**

Settings.
2. Click **Lock**.
3. Verify that the **Default Server Certificate** and **Private key** are both valid (green). If the **Default Server Certificate** and **Private key** are not valid, see How to Set Up Barracuda VPN CA VPN Certificates.
4. In the left menu, select **IPSec**.
5. In the **IKEv1** section, enter the **Pre-shared key**. E.g., `pre$haredKey`



6. Click **OK**.
7. Click **Send Changes** and **Activate**.

Step 4. (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 also create a list of L2TP/IPsec users who can access the VPN. Specify the username, password, and optional static IP address for each user.

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 the L2TP/IPsec users.
5. Click **Send Changes** and **Activate**.

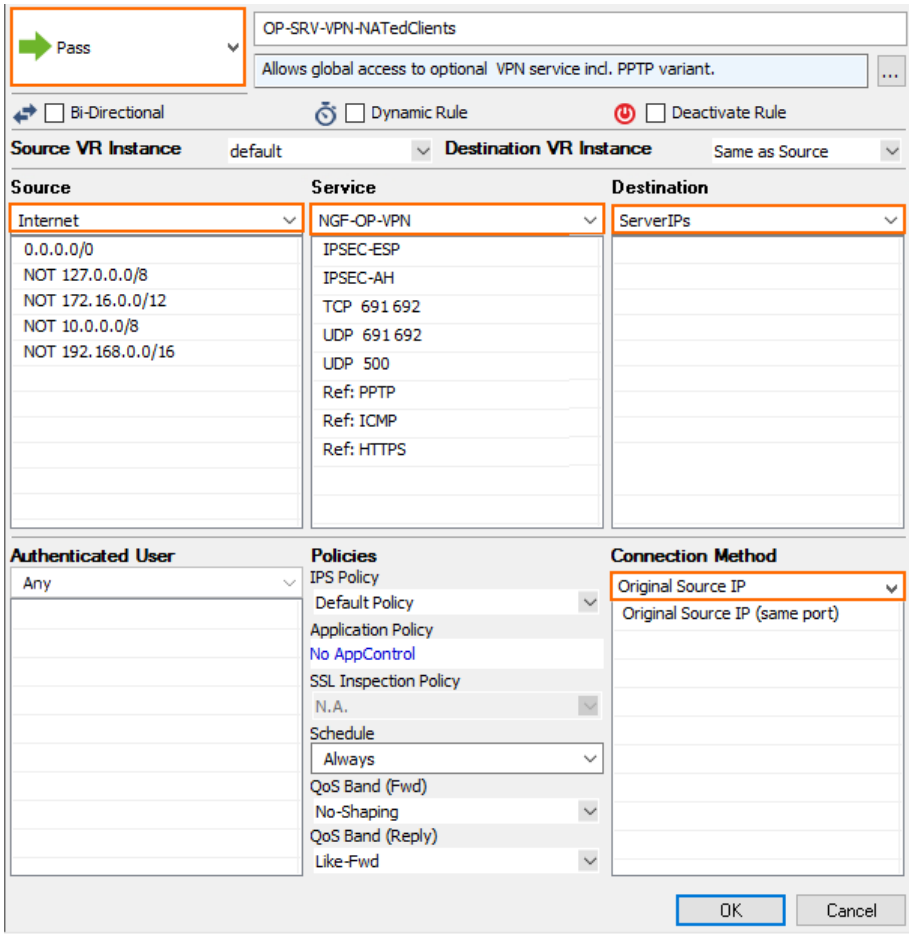
Step 5. Create a Host Firewall Rule

To allow multiple clients behind the same NATed IP address to connect to the CloudGen Firewall, you must create an additional host firewall rule.

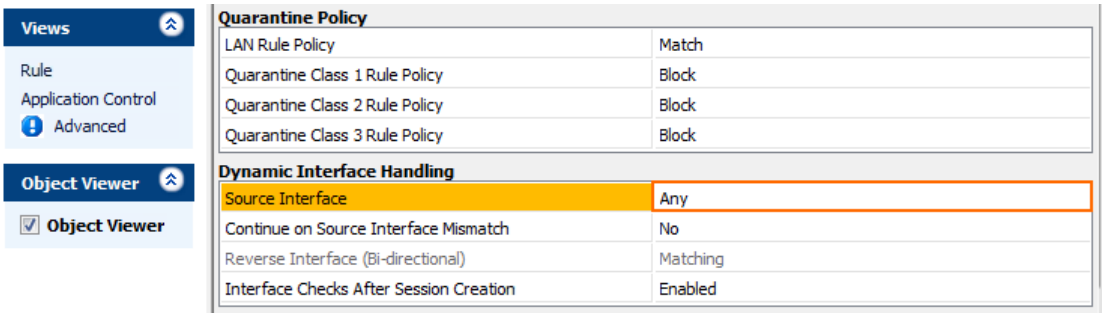
1. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > Host Firewall Rules**.
2. Click **Lock**.

3. Click the plus icon (**+**) at the top right of the ruleset, or right-click the ruleset and select **New > Rule**.

4. Specify the following settings that must be matched by the traffic to be handled by the access rule:
   - **Action** – Select **PASS**.
   - **Source** – Select **Internet**.
   - **Service** – Select **NGF-OP-VPN**.
   - **Destination** – Select **Server IPs**.
   - **Connection Method** – Double click and select **Original Source IP** from the **Translated Source IP** list.



5. In the left menu, click **Advanced**.
6. In the **Dynamic Interface Handling** section, set **Source Interface** to **Any**.



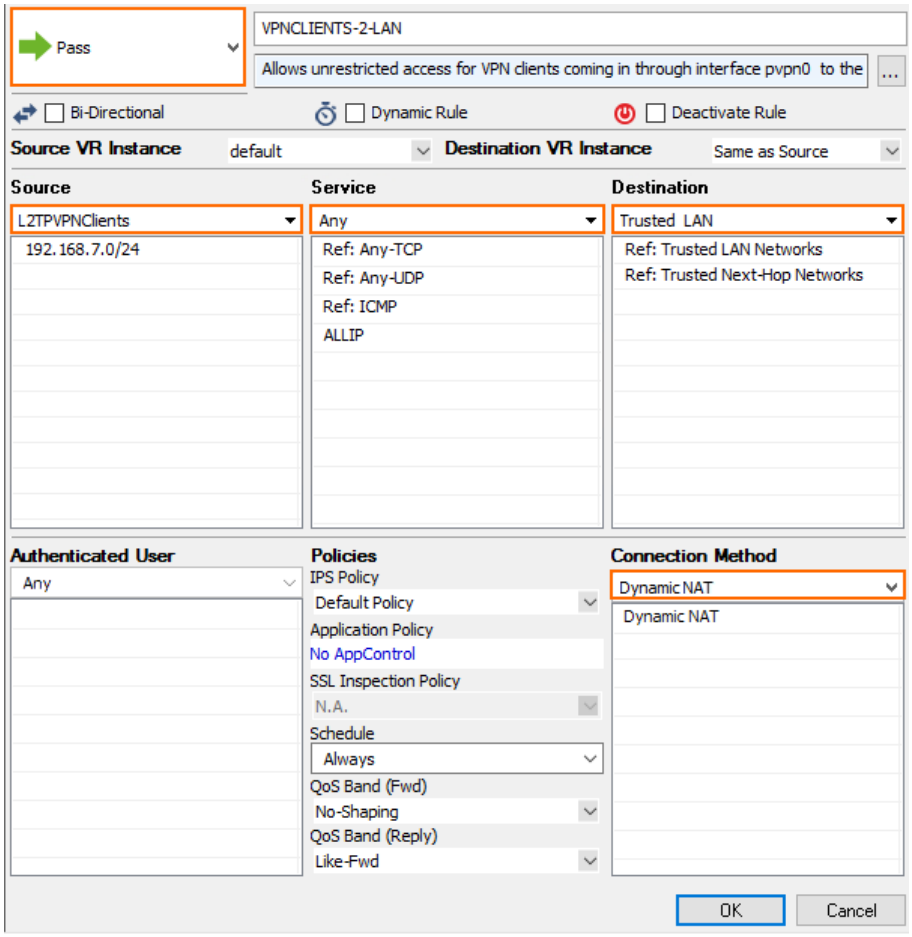
7. Click **OK**.
8. Place the host firewall rule directly above the **OP-SRV-VPN** rule in the **Inbound** ruleset.
9. Click **Send Changes** and **Activate.**

Step 6. Create an Access Rule for L2TP/IPsec Clients

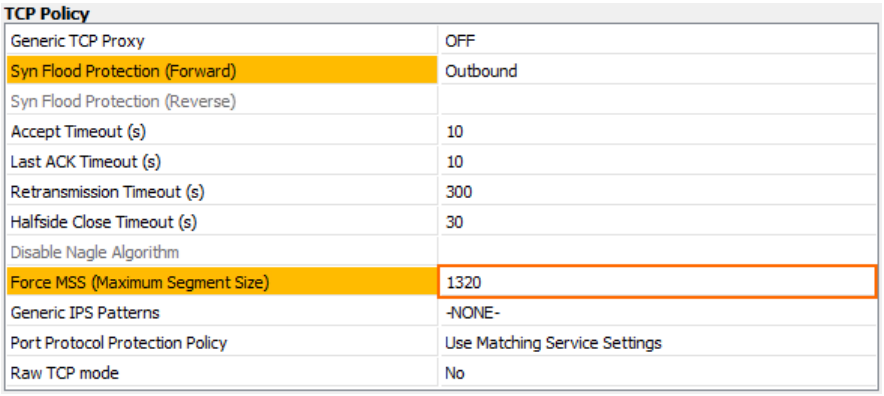
To allow traffic from connected L2TP clients into your network, you must create an access rule.

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Rules**.
2. Click **Lock**.
3. Click the plus icon (**+**) at the top right of the ruleset, or right-click the rule set and select **New > Rule**.

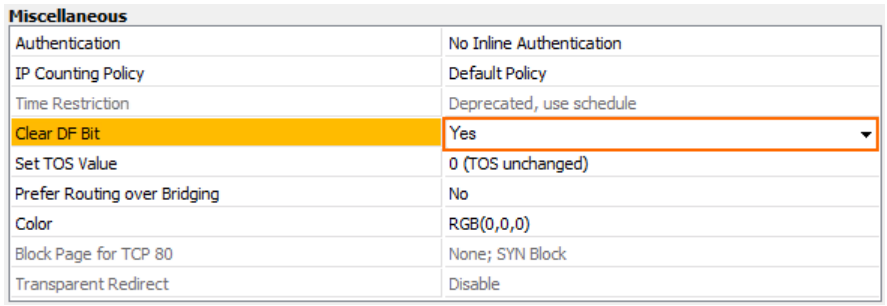
4. Specify the following settings that must be matched by the traffic to be handled by the access rule:
   - **Action** – Select **PASS**.
   - **Source** – Select the network object containing the L2TP VPN clients. Alternatively, use **0.0.0.0/0** with source interface **pvpn0** as the source.
   - **Service** – Select **ANY**.
   - **Destination** – Select **Trusted LAN**.
   - **Connection Method** – Select **Dynamic NAT**.



5. In the left menu, click **Advanced**.
6. In the **TCP Policy** section, set the **Force MSS (Maximum Segment Size)** to at least 40 bytes less than the MTU of the interface. E.g., 1320



7. In the **Miscellaneous** section, set the **Clear DF Bit** to **yes**.



8. Click **OK**.
9. Place the access rule so that no rule above it matches this traffic.
10. Click **Send Changes** and **Activate**.

Troubleshooting

To troubleshoot VPN connections, see the `\VPN\l2tpd` log file. For more information, see LOGS Tab.

Figures

1. Client-2-SiteL2TP.png
2. PSK02.png
3. FW_Rule_Add01.png
4. l2tp_hostFW01.png
5. l2tp_hostFW02.png
6. FW_Rule_Add01.png
7. l2tp_rule_00.png
8. l2tp_rule_01.png
9. l2tp_rule_02 (1).png