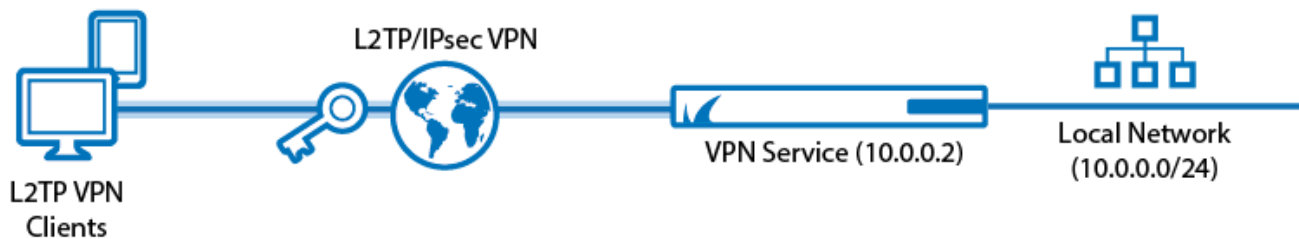


How to Configure a Client-to-Site L2TP/IPsec VPN

<https://campus.barracuda.com/doc/73719153/>

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.

- Open the **L2TP/PPTP Settings** page for the VPN service (**Configuration > Configuration Tree > Box > Virtual Servers > your virtual server > 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 > Virtual Servers > your virtual server > 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 which 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).
 - **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 > Virtual Servers > *your virtual server* > Assigned Services > VPN-Service > VPN Settings**.
2. Click **Lock**.
3. In the **Server Settings** window, click on the **Advanced** tab.
4. In the **IKE Parameter** section enter the IKE PSK key. E.g., pre\$hare\$Key
5. Click **OK**.
6. 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 > Virtual Servers > *your virtual server* > 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.

OP-SRV-VPN-NATedClients

Allows global access to optional VPN service incl. PPTP variant.

☐ Bi-Directional ☐ Dynamic Rule ☒ Deactivate Rule

Source VR Instance: default Destination VR Instance: Same as Source

Source	Service	Destination
Internet	NGF-OP-VPN	ServerIPs
0.0.0.0/0	IPSEC-ESP	
NOT 127.0.0.0/8	IPSEC-AH	
NOT 172.16.0.0/12	TCP 691 692	
NOT 10.0.0.0/8	UDP 691 692	
NOT 192.168.0.0/16	UDP 500	
	Ref: PPTP	
	Ref: ICMP	
	Ref: HTTPS	

Authenticated User: Any

Policies:

- IPS Policy
- Default Policy
- Application Policy
- No AppControl
- SSL Inspection Policy
- N.A.
- Schedule: Always
- QoS Band (Fwd)
- No-Shaping
- QoS Band (Reply)
- Like-Fwd

Connection Method: Original Source IP

Original Source IP (same port)

OK Cancel

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

Views

Rule

Application Control

Advanced

Object Viewer

☒ Object Viewer

Quarantine Policy

LAN Rule Policy	Match
Quarantine Class 1 Rule Policy	Block
Quarantine Class 2 Rule Policy	Block
Quarantine Class 3 Rule Policy	Block

Dynamic Interface Handling

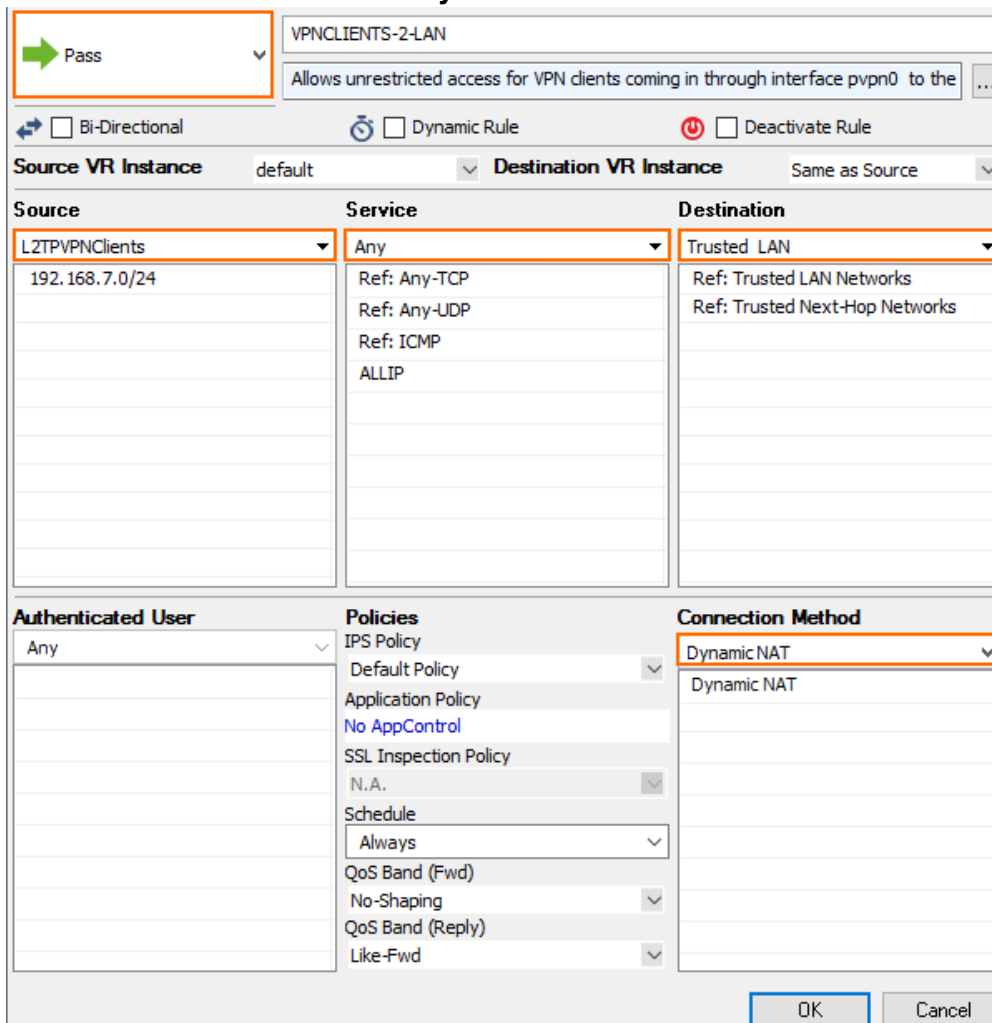
Source Interface	Any
Continue on Source Interface Mismatch	No
Reverse Interface (Bi-directional)	Matching
Interface Checks After Session Creation	Enabled

- Click **OK**.
- Place the host firewall rule directly above the **OP-SRV-VPN** rule in the **Inbound** ruleset.
- 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 > Virtual Server > your virtual server > Assigned Services > Firewall**.
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:
5. **Action** - Select **PASS**.
6. **Source** - Select the network object containing the L2TP VPN clients. Alternatively, use **0.0.0.0/0** with source interface **pvpn0** as the source.
7. **Service** - Select **NGF-OP-VPN**.
8. **Destination** - Select **Trusted LAN**.
9. **Connection Method** - Select **Dynamic NAT**.



Action: **Pass**
 Rule Name: VPNCLIENTS-2-LAN
 Description: Allows unrestricted access for VPN clients coming in through interface pvpn0 to the ...
 Bi-Directional: ☐ Dynamic Rule: ☐ Deactivate Rule: ☐
 Source VR Instance: default Destination VR Instance: Same as Source

Source	Service	Destination
L2TPVPNclients	Any	Trusted LAN
192.168.7.0/24	Ref: Any-TCP Ref: Any-UDP Ref: ICMP ALLIP	Ref: Trusted LAN Networks Ref: Trusted Next-Hop Networks

Authenticated User	Policies	Connection Method
Any	IPS Policy Default Policy Application Policy No AppControl SSL Inspection Policy N.A. Schedule Always QoS Band (Fwd) No-Shaping QoS Band (Reply) Like-Fwd	Dynamic NAT

 OK Cancel

10. In the left menu, click **Advanced**.

11. 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

TCP Policy	
Generic TCP Proxy	OFF
Syn Flood Protection (Forward)	Outbound
Syn Flood Protection (Reverse)	
Accept Timeout (s)	10
Last ACK Timeout (s)	10
Retransmission Timeout (s)	300
Halfside Close Timeout (s)	30
Disable Nagle Algorithm	
Force MSS (Maximum Segment Size)	1320
Generic IPS Patterns	-NONE-
Port Protocol Protection Policy	Use Matching Service Settings
Raw TCP mode	No

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

Miscellaneous	
Authentication	No Inline Authentication
IP Counting Policy	Default Policy
Time Restriction	Deprecated, use schedule
Clear DF Bit	Yes
Set TOS Value	0 (TOS unchanged)
Prefer Routing over Bridging	No
Color	RGB(0,0,0)
Block Page for TCP 80	None; SYN Block
Transparent Redirect	Disable

13. Click **OK**.
 14. Place the access rule so that no rule above it matches this traffic.
 15. Click **Send Changes** and **Activate**.

Troubleshooting

To troubleshoot VPN connections, see the `\YourVirtualServer\VPN\l2tpd` log file. For more information, see [LOGS Tab](#).

Figures

1. Client2SiteL2TP.png
2. FW_Rule_Add01.png
3. l2tp_hostFW01.png
4. l2tp_hostFW02.png
5. FW_Rule_Add01.png
6. l2tp_rule_00.png
7. l2tp_rule_01.png
8. l2tp_rule_02 (1).png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.