L2TP over IPSec VPN Setup

This guide is designed to assist you in the setup of the L2TP VPN capabilities of the ZyWALL (ZLD) series routers.

Start by accessing the routers web configurator (http://192.168.1.1), once in the configuration screen you will need to create some address objects as well as user accounts for the L2TP users. An object for the WAN IP will be created as well as an object for a range of IP addresses which will be assigned to L2TP connected users.

To create the address objects click on the "Configuration" menu icon, on the far left. In the configuration menu go to Object > Address and click the "Add" button to insert the IP entries.

1. Create and address object for the WAN IP address. The name can be whatever you like, the Address Type needs to be set to "Interface IP", for Interface select the approriate WAN connection.

![Edit Address Rule WAN1_IP](image)

2. Create a second address object for the L2TP IP range. The L2TP IP addresses has to be unique, it cannot conflict with any other interface that is created on the ZyWALL. (example: LAN1 by default uses 192.168.1.0/24 IP scheme, this means you cannot use 192.168.1.XXX for L2TP IP range) Once you have named the new address entry for the Address Type select "Range", then specify
the starting and ending IP addresses that will be used for the L2TP users.

Now that you have created the address objects go to menu Configuration > Object > User/Group to create user accounts for the L2TP users. In the User tab click on the "Add" button to insert a user entry. Specify the username, User Type should be set to "USER", create a password for the user account.

Click on the "Group" tab and add a user group for the L2TP. Select all the user accounts you have created for the L2TP users and move these user accounts to the "Member" list on the right.
Once all necessary objects have been created go to Configuration > VPN > IPSec VPN to start setting up the L2TP VPN policies. On the "IPSec VPN" menu click on the "VPN Gateway" tab. You will see a default rule called "Default_L2TP_VPN_GW". Click on the rule to highlight it then click the "Edit" button across the top. Once the policy editor is open check the box to "Enable" the rule, under gateway settings select the correct WAN connection interface for L2TP VPN's and create a "Pre-Shared Key" in the authentication option.

**WARNING!! DO NOT CHANGE THE DEFAULT ENCRYPTION OR AUTHENTICATION IN THE VPN GATEWAY OR VPN CONNECTION. THE DEFAULT RULES ARE SET THE WAY THEY ARE BECAUSE THAT IS HOW L2TP NEEDS TO BE SET IN ORDER TO WORK. CHANGING EITHER CAN RESULT IN YOUR TUNNEL NOT ESTABLISHING!**
### General Settings

**Enable**

VPN Gateway Name: **Default_L2TP_VPN_GW**

### Gateway Settings

#### My Address

- **Interface**: [Select Interface]
- **Domain Name/IP**: [Enter IP Address]

#### Peer Gateway Address

- **Primary**: 6.0.0.0
- **Secondary**: 6.0.0.0

**Fall back to Primary Peer Gateway when possible**

- **FailBack Check Interval**: 20 (0-86400 seconds)
- **Dynamic Address**: [Select Dynamic Address]

### Authentication

- **Pre-Shared Key**: yourpassword

#### Certificate

- **Local ID Type**: [Select ID Type]
- **Content**: 0.0.0.0

#### Peer ID Type

- **Content**: [Select Content]

### Phase 1 Settings

- **SA Life Time**: 86400 (1 BE - 30000000 Seconds)
- **Negotiation Mode**: Main
- **Proposal**: [Select Proposal]

#### Encryption

<table>
<thead>
<tr>
<th>#</th>
<th>Encryption</th>
<th>Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DES</td>
<td>SHA1</td>
</tr>
<tr>
<td>2</td>
<td>3DES</td>
<td>MD5</td>
</tr>
<tr>
<td>3</td>
<td>3DES</td>
<td>SHA1</td>
</tr>
</tbody>
</table>

- **Key Group**: [Select Key Group]

#### NAT Traversal

- [Select NAT Traversal]

#### Dead Peer Detection (DPO)

- [Select Dead Peer Detection]

### Extended Authentication

- **Enable Extended Authentication**: [Select Enable]

- **Server Mode**: default

- **Client Mode**
  - **User Name**
  - **Password**
  - **Retype to Confirm**
Now that VPN Gateway is configured click on the "VPN Connection" tab and edit the "Default_L2TP_VPN_Connection" policy. Enable the rule, select "Remote Access (Server Role)" for the application scenario and under Policy select the address object you created for the WAN IP address.
Now that the IPSec VPN portion of the L2TP has been configured go to Configuration > VPN > L2TP VPN to setup the L2TP portion. Check the box to "Enable L2TP Over IPSec", for the VPN Connection option click on the dropdown and select the "Default_L2TP_VPN_Connection" rule that was configured on the previous step. For IP Address Pool click the dropdown and select the address object you created with the range of addresses. For Allowed User click on the dropdown and select the user group you created for the L2TP users. By default L2TP clients are programmed to send all traffic through the VPN connection which means internet traffic from the clients will be sent through the tunnel. Setup DNS servers which the L2TP users will be able to use to access the internet through the ZyWALL.

![General Settings](image)

To allow the L2TP users internet access a policy route needs to be created under Configuration > Network > Routing > Policy Route. This route will specify that Incoming traffic from a "Tunnel", tunnel member being the "Default_L2TP_VPN_Connection", the source address is the range of L2TP IP addresses and the destination being any. The next-hop for this traffic should be Type "Trunk" and the trunk member will be the "SYSTEM_DEFAULT_WAN_TRUNK"
## Edit Policy Route

### Configuration
- **Enable**

### Criteria
- **User:** any
- **Incoming:** Tunnel
- **Source Address:** LTP_POOL
- **Destination Address:** any
- **DSCP Code:** any
- **Schedule:** none
- **Service:** any

### Next-Hop
- **Type:** Trunk
- **Trunk:** SYSTEM_DEFAULT_VLAN_TRUNK