ZyWALL (ZLD) VPN Troubleshooting

L2TP VPN will not connect
No traffic flow through L2TP VPN tunnel

Client-to-Site (RoadWarrior) VPN will not connect
No traffic flow through client-to-site IPSec VPN tunnel (RoadWarrior)

Site-to-Site VPN will not establish
No traffic flow through site-to-site IPSec VPN tunnel

SSL VPN connection will not establish

Connection issues with SSL VPN

L2TP VPN will not connect

Please verify your VPN rule setup with the example provided on the “ZyWALL_L2TP_VPN_Setup.pdf” walkthrough. If your setup is similar to the example provided please check the following:

- Is the ZyWALL behind a NAT (another router)? The L2TP function will not work if the ZyWALL is behind another router. This is a limitation on the devices L2TP capability, the ZyWALL needs direct communication with the public network (internet).

- If the L2TP client is behind a router please make sure that VPN pass-through is enabled or create port forwarding rules so it does not block the L2TP communication to the ZyWALL.

www.zyxel.com
• Does the client have any other VPN clients installed? Only one application can use the IKE/IPSec services at a time, if there is another VPN client installed on the computer (and running) such as Cisco IPSec client, TheGreenBow, ShrewSoft, etc., you will need to close the application completely and restart the IKE/IPSec services so that the L2TP client can use them.

[Windows]
To restart the services on your computer open a RUN dialog box. You can access this by pressing the Windows + R keys on the keyboard.

Type “services.msc” and click OK or hit the Enter/Return key.
Scroll down the list to find the ‘IKE and AuthIP IPsec Keying Modules’ and ‘IPsec Policy Agent’ to restart these services.

- Please check your L2TP clients settings against our setup example(s) [link to Windows, macOS, iOS, etc., setup guides]

- Disable your computers firewall to make sure it is not blocking the VPN connection attempt.

**Windows:** To disable the Windows firewall, open a RUN dialog box. You can access this by pressing the Windows + R keys on the keyboard.
Type “firewall.cpl” and click OK or hit the Enter/Return key.

![Run dialog showing firewall.cpl](image)

Select the option to “Turn Windows Firewall on or off” on the left. Disable the firewall by selecting the “Turn off Windows Firewall” and click the OK button to save the settings.

![Control Panel Home](image)

**Note:** If you’re using a third party software firewall, Trend Micro, Norton, McAfee, etc., please open the software’s control panel and disable the firewall feature.

**macOS:** To disable the firewall on macOS open System Preferences → Security & Privacy, click the Firewall tab and press the “Turn Off Firewall” button to disable.
- Update your computers NIC drivers.

Note: For updates to your computers NIC cards please visit the computer manufacturer or the NIC cards chipset manufacturer.

- Bypass your router (if possible) to make sure it is not blocking the attempt to connect/establish the L2TP VPN.

- Check the ZyWALL’s IKE logs to make sure it is receiving a request to establish the VPN. By default the ZyWALL is programmed to allow VPN traffic, if the IKE logs on the ZyWALL do not show any IKE connection attempts try disabling the ZyWALL’s Firewall/Policy Control. If still no luck, check with your ISP to make sure they are not blocking ports on the service end.

To disable the ZyWALL’s firewall/policy control, go to:
Configuration ➔ Firewall OR Configuration ➔ Security Policy ➔ Policy Control
- Verify the firmware is up to date and contact tech support for further assistance. To check the current version of firmware on the ZyWALL go to **Maintenance → File Manager → Firmware Package**

<table>
<thead>
<tr>
<th>Version</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Boot Module:</td>
<td>1.13</td>
</tr>
<tr>
<td>Current Version:</td>
<td>3.30(AQU.7)</td>
</tr>
<tr>
<td>Released Date:</td>
<td>2015-01-13 16:31:04</td>
</tr>
</tbody>
</table>
No traffic flow through L2TP VPN tunnel

Please follow the instructions below if you have successfully established an L2TP VPN connection but cannot pass traffic through the tunnel.

- By default L2TP clients are programmed to send all traffic through the L2TP connection once established. If you have disabled this option you will need to manually create routes on your devices operating system to route traffic through the tunnel accordingly.

- Make sure there are no IP conflicts. The ZyWALL’s internal (LAN) IP scheme and the L2TP IP pool should be on different subnets, using the same IP scheme can cause routing issues.

- Create a policy route on the ZyWALL to specify that any traffic destined for the L2TP IP Pool needs to take a hop (Next-Hop) at the L2TP VPN tunnel. Configuration → Network → Routing → Policy Route

- Disable the ZyWALL’s Firewall/Policy Control.

To disable the ZyWALL’s firewall/policy control, go to:
• Make sure the L2TP connection has a higher priority than any other route on your computer. On macOS you need to change the service order to give the VPN connection a higher priority than the Ethernet or Wi-Fi connections.

**Windows:** All routes for the L2TP interface should have a higher metric than the standard routes. Open command prompt or PowerShell and type `route print` to view the routing table.

**macOS:** Open System Preferences → Network, click the configuration icon at the bottom of the network interface list and “Set Service Order”.
Verify that the device you are trying to contact across the VPN is pointing to the ZyWALL for its default gateway. If the device is pointing to a different default gateway the traffic will not get sent back through the L2TP VPN tunnel.

Verify the firmware is up to date and contact tech support for further assistance. To check the current version of firmware on the ZyWALL go to Maintenance → File Manager → Firmware Package.

<table>
<thead>
<tr>
<th>Version</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Boot Module:</td>
<td>1.13</td>
</tr>
<tr>
<td>Current Version:</td>
<td>3.30(AQU.7)</td>
</tr>
<tr>
<td>Released Date:</td>
<td>2015-01-13 16:31:04</td>
</tr>
</tbody>
</table>
Client-to-Site (RoadWarrior) VPN will not connect

Please use the walkthrough “Dynamic_VPN_Setup_CR.pdf” as an example to verify the setup on your ZyWALL, to make sure all necessary settings and rules have been created on the router.

- If the ZyWALL is behind a NAT (another router) make sure the first NAT is forwarding the VPN ports to the ZyWALL. IKE UDP:500 and NAT-T UDP:4500

- Make sure your network router is allowing the IPSec ports through (UDP:500 and UDP:4500) or be sure to enable VPN pass-through if the router supports this option. Bypass the router if possible to make sure it is not causing the problem.

- Make sure your ISP is not blocking VPN ports, some providers will block the VPN ports on their end.

- Verify that your computers firewall is allowing communications from the VPN client.

- Update your NIC drivers (Ethernet and/or Wi-Fi).

Note: For updates to your computers NIC cards please visit the computer manufacturer or the NIC cards chipset manufacturer.
- Check the VPN settings on the ZyWALL and make sure they match the software client configuration.

- Check the ZyWALL’s IKE logs to make sure it is receiving a request to establish the VPN. By default the ZyWALL is programmed to allow VPN traffic, if the IKE logs on the ZyWALL do not show any IKE connection attempts try disabling the ZyWALL’s Firewall/Policy Control. If still no luck, check with your ISP to make sure they are not blocking ports on the service end.

To disable the ZyWALL’s firewall/policy control, go to:

Configuration → Firewall OR Configuration → Security
Policy → Policy Control

- Verify the firmware is up to date and contact tech support for further assistance. To check the current version of firmware on the ZyWALL go to Maintenance → File Manager → Firmware Package

<table>
<thead>
<tr>
<th>Version</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Boot Module:</td>
<td>1.13</td>
</tr>
<tr>
<td>Current Version:</td>
<td>3.30(AQU.7)</td>
</tr>
<tr>
<td>Released Date:</td>
<td>2015-01-13 16:31:04</td>
</tr>
</tbody>
</table>
No traffic flow through client-to-site IPSec VPN tunnel (RoadWarrior)

If you have successfully established a VPN connection to the ZyWALL but cannot get traffic across, please try the following:

- Login to the ZyWALL’s WebGUI and disable the “Use Policy Route to control dynamic IPSec rules” in the VPN menu. Configuration → VPN → IPSec VPN → VPN Connection

- Disable the ZyWALL routers Firewall.

  Configuration → Firewall OR Configuration → Security Policy → Policy Control

- Disable the firewall on the remote host (computer/device) to make sure it is not blocking the request.

**Windows:** To disable the Windows firewall, open a RUN dialog box. You can access this by pressing the Windows + R keys on the keyboard.
Type “firewall.cpl” and click OK or hit the Enter/Return key.

Select the option to “Turn Windows Firewall on or off” on the left. Disable the firewall by selecting the “Turn off Windows Firewall” and click the OK button to save the settings.

Note: If you’re using a third party software firewall, Trend Micro, Norton, McAfee, etc., please open the software’s control panel and disable the firewall feature.

**macOS:** To disable the firewall on macOS open **System Preferences ➔ Security & Privacy**, click the Firewall tab and press the “Turn Off Firewall” button to disable.
If you are attempting to access resources using computer hostname, try using the IP address assigned to the computer/device instead. Using a computer hostname requires the NetBIOS broadcast protocol to resolve the computer's IP address, broadcasts are not supported by the IPSec standard. Because broadcasts are not supported by the IPSec VPN standard we cannot guarantee that using hostnames instead of IP’s will work. A workaround for this limitation of the IPSec standard would be to use a WINS server.

Make sure there are no IP conflicts, if the ZyWALL network is configured to use the 192.168.1.0/24 network and the remote user is also using the same IP scheme, traffic will not route through the VPN tunnel properly.

Make sure your network router is allowing the IPSec ports through (UDP:500 and UDP:4500) or be sure to enable VPN pass-through if the router supports this option. Bypass the router if possible to make sure it is not causing the problem.
Verify that the device you are trying to contact is pointing to the ZyWALL for its default gateway. If the device is pointing to a different default gateway the traffic will not get sent back through the VPN tunnel.

Verify the firmware is up to date and contact tech support for further assistance. To check the current version of firmware on the ZyWALL go to Maintenance → File Manager → Firmware Package

<table>
<thead>
<tr>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boot Module:</td>
</tr>
<tr>
<td>Current Version:</td>
</tr>
<tr>
<td>Released Date:</td>
</tr>
</tbody>
</table>
Site-to-Site VPN will not establish

If you have configured an IPSec VPN rule for site-to-site (router-to-router) connection and the tunnel is not being established, please try the following:

- Reboot/Restart the ZyWALL appliance to reload the VPN daemon.

- Check the ZyWALL logs to verify that IKE connection attempts are being sent and received. If the logs show one way IKE traffic, send only for example, check the internet connection to make sure traffic is not being blocked/stopped on the service end.

- Double check the VPN rules on both ends to make sure all settings are matching.

- If using DDNS hostname or domain name to dial the connection instead of the public IP address, please make sure there are DNS servers programmed on the ZyWALL and that they can resolve the DDNS hostname/domain name. To check if the ZyWALL can resolve the name you will need to open a terminal session using SSH/Telnet/Console and run a ping command to the DDNS hostname/domain name.

  Router> ping hostname/domain  
  (ex: Router> ping www.google.com)

  If the ping test fails double check the ZyWALL's DNS settings and try again. If your internet service is DHCP the ZyWALL would have automatically obtained the DNS server settings from your ISP. To check this go to Configuration → System → DNS.
If your WAN IP was statically assigned the DNS settings will show “N/A” for the Default entry (the Default entry is for the WAN ports DHCP client capability only), click the Add button to manually enter your ISP provided or public (OpenDNS, Google DNS, etc.) DNS servers.

- Verify the firmware is up to date and contact tech support for further assistance. To check the current version of firmware on the ZyWALL go to **Maintenance → File Manager → Firmware Package**

<table>
<thead>
<tr>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boot Module:</td>
</tr>
<tr>
<td>Current Version:</td>
</tr>
<tr>
<td>Released Date:</td>
</tr>
</tbody>
</table>
No traffic flow through site-to-site IPSec VPN tunnel

Tunnel established but can’t get traffic across:

- Make sure there are no IP conflicts between the two sites.

- Disable the ZyWALL routers firewall.

  To disable the ZyWALL’s firewall/policy control, go to:

  Configuration → Firewall **OR** Configuration → Security Policy → Policy Control

<table>
<thead>
<tr>
<th>General Settings</th>
<th>General Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>[ ] Enable Firewall</td>
<td>[ ] Enable Policy Control</td>
</tr>
</tbody>
</table>

- Verify that the host you are attempting to reach is pointing to the ZyWALL for the default gateway.

- Check for conflicting policy/static routes. A misconfigured or out of order route can cause problems. To verify the policy/static route rules go to, Configuration → Network → Routing.

- Verify that the host you are attempting to reach is listening for the traffic you are sending to it. Example: If you’re sending a ping request to a device, make sure it is set to respond to ping/icmp requests.

  **Windows:** Open command prompt or powershell and type `netstat -an` for a list of listening ports.
macOS: Open terminal and type `sudo lsof -i -n -P` for a printout of the listening ports.

bash-3.2# sudo lsof -i -n -P

```
COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME
launchd 1 root 23u IPv4 87044d20866d1f5 0t0 UDP 8:137
launchd 1 root 31u IPv4 87044d20866d1f5 0t0 UDP 8:137
launchd 1 root 32u IPv6 87044d20866d1f5 0t0 TCP 8:5900 (LISTEN)
launchd 1 root 40u IPv6 87044d20866d1f5 0t0 TCP 8:5900 (LISTEN)
launchd 1 root 41u IPv6 87044d20866d1f5 0t0 TCP 8:5900 (LISTEN)
launchd 1 root 44u IPv6 87044d20866d1f5 0t0 TCP 8:5900 (LISTEN)
launchd 1 root 45u IPv6 87044d20866d1f5 0t0 TCP 8:5900 (LISTEN)
launchd 1 root 46u IPv6 87044d20866d1f5 0t0 TCP 8:5900 (LISTEN)
launchd 1 root 51u IPv6 87044d20866d1f5 0t0 TCP 8:5900 (LISTEN)
launchd 1 root 52u IPv6 87044d20866d1f5 0t0 TCP 8:5900 (LISTEN)
```

- Manually create a route (Configuration → Routing) to stipulate that traffic destined for the remote network should take its Next-Hop on the appropriate VPN tunnel.
- Verify the firmware is up to date and contact tech support for further assistance. To check the current version of firmware on the ZyWALL go to **Maintenance → File Manager → Firmware Package**

<table>
<thead>
<tr>
<th>Version</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Boot Module:</td>
<td>1.13</td>
</tr>
<tr>
<td>Current Version:</td>
<td>3.30(AQU.7)</td>
</tr>
<tr>
<td>Released Date:</td>
<td>2015-01-13 16:31:04</td>
</tr>
</tbody>
</table>
SSL VPN connection will not establish

SSL VPN connection will not connect or being redirected to a different screen, try the following steps to troubleshoot the issue.

- Make sure you are using a USER account to establish the SSL VPN connection. Users with ADMIN privileges cannot be part of the SSL VPN rule/policy. Administrative users will automatically get redirected to the configuration GUI. To verify the user account type, login to the ZyWALL’s WebGUI and go to **Configuration → Object → User/Group**.

- Make sure the network connection is **not** “Disabled” on Windows. To check this, click the Windows Logo key on your keyboard + the “R” key. This will open the RUN dialog box. Type “ncpa.cpl” and click OK or hit the Enter/Return key. On the Network Connections screen look for the connection using the TAP-Windows adapter for ZyXEL SecuExtender.

- Verify the server IP address the SecuExtender is dialing to and user credentials.

  ```
  Windows               macOS
  ```
Verify the firmware is up to date and contact tech support for further assistance. To check the current version of firmware on the ZyWALL go to **Maintenance → File Manager → Firmware Package**

**Version**

- **Boot Module:** 1.13
- **Current Version:** 3.30(AQU. 7)
- **Released Date:** 2015-01-13 16:31:04
Connection issues with SSL VPN

If you have successfully established an SSL VPN connection to the ZyWALL and are experiencing issues, please try the following.

- Can’t access local network resources when VPN connection is established? Please make sure there are no IP conflicts between the remote and local network. If both sites are using the same IP scheme, 192.168.1.0/24 for example, routing will not work properly. Once the VPN tunnel is established all traffic destined for a 192.168.1.0/24 address will flow through the VPN tunnel. This is because the route the computer operating system created to send traffic through the VPN tunnel has a higher priority/metric that the regular route.

- Disable the ZyWALL’s firewall if you are having problems getting traffic through the tunnel.

To disable the ZyWALL’s firewall/policy control, go to:

Configuration → Firewall OR Configuration → Security Policy → Policy Control

- Disable the computers firewall if you are having problems getting traffic through the tunnel to make sure it is not blocking.

Windows: To disable the Windows firewall, open a RUN dialog box. You can access this by pressing the Windows + R keys on the keyboard.
Type “firewall.cpl” and click OK or hit the Enter/Return key.

Select the option to “Turn Windows Firewall on or off” on the left. Disable the firewall by selecting the “Turn off Windows Firewall” and click the OK button to save the settings.

Note: If you’re using a third party software firewall, Trend Micro, Norton, McAfee, etc., please open the softwares control panel and disable the firewall feature.

macOS: To disable the firewall on macOS open System Preferences → Security & Privacy, click the Firewall tab and press the “Turn Off Firewall” button to disable.
Verify that the workstation is listening to the traffic you are using to access it remotely.

**Windows:** Open command prompt or powershell and type `netstat -an` for a list of listening ports.

```bash
PS C:\> netstat -an
Active Connections

<table>
<thead>
<tr>
<th>Proto</th>
<th>Local Address</th>
<th>Foreign Address</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>0.0.0.0:1335</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:445</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:3389</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:5157</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:5817</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:8732</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:9976</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:49152</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:49153</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:49154</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:49157</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:49158</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:52230</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>127.0.0.1:5939</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
</tr>
</tbody>
</table>
```

**macOS:** Open terminal and type `sudo lsof -i -n -P` for a printout of the listening ports.
Verify the firmware is up to date and contact tech support for further assistance. To check the current version of firmware on the ZyWALL go to Maintenance → File Manager → Firmware Package

<table>
<thead>
<tr>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boot Module: 1.13</td>
</tr>
<tr>
<td>Current Version: 3.30(AQU.7)</td>
</tr>
<tr>
<td>Released Date: 2015-01-13 16:31:04</td>
</tr>
</tbody>
</table>