Remote Access VPN Setup (IPSec)

This guide provides an example on creating an IPSec VPN rule to allow user access to local network resources.

Supported Devices

ZyWALL USG 20 – running firmware 3.30 and newer
ZyWALL USG 20W – running firmware 3.30 and newer
ZyWALL USG 50 – running firmware 3.30 and newer
ZyWALL USG 100 – running firmware 3.30 and newer
ZyWALL USG 100 PLUS – running firmware 3.30 and newer
ZyWALL USG 200 – running firmware 3.30 and newer
ZyWALL USG 300 – running firmware 3.30 and newer
ZyWALL USG 1000 – running firmware 3.30 and newer
ZyWALL USG 2000 – running firmware 3.30 and newer
ZyWALL 110 – running firmware version 3.10 and newer
ZyWALL 310 – running firmware version 3.10 and newer
ZyWALL 1100 – running firmware version 3.10 and newer
ZyWALL USG 40 – running firmware version 4.10 and newer
ZyWALL USG 40W – running firmware version 4.10 and newer
ZyWALL USG 60 – running firmware version 4.10 and newer
ZyWALL USG 60W – running firmware version 4.10 and newer
ZyWALL USG 110 – running firmware version 4.10 and newer
ZyWALL USG 210 – running firmware version 4.10 and newer
ZyWALL USG 310 – running firmware version 4.10 and newer
ZyWALL USG 1100 – running firmware version 4.10 and newer
ZyWALL USG 1900 – running firmware version 4.10 and newer

Overview

A VPN (virtual private network) provides a secure communication between sites without the expense of leased lines. VPN’s are used to
transport traffic over the internet of any insecure network that uses TCP/IP communications. A remote access VPN (client-to-site) allows employees who are traveling or teleworkers, secure access to company network resources. There multiple types of VPN protocols/technologies, that can be used to establish a secure link to company network, L2TP, PPTP, SSL, OpenVPN, etc.. This guide will reference the IPSec protocol to establish a secure VPN tunnel between external hosts (users connected to the internet outside the company network structure) and the ZyWALL router. Third party IPSec software is required to establish the VPN connection as current operating systems lack a built-in IPSec client.
VPN Gateway (Phase 1)

Login to the ZyWALL’s web configuration page and go to menu **Configuration → VPN → IPSec VPN**. In the IPSec VPN menu click the VPN Gateway tab to add Phase 1 of the tunnel setup. Click the **Add** button to insert a new rule. On the top left of the window click the **Show Advance Settings** button to view all options in the menu.

- Check the box to enable the VPN rule and provide a name
- Select the WAN interface you wish to use to connect the VPN under the **My Address** dropdown field
- Make sure the **Peer Gateway Address** is set to “Dynamic Address”
- Enter/Create a VPN authentication “Pre-Shared Key”
- Under the **Phase 1 Settings** set the Negotiation Mode dropdown to use “Main” mode
- Set the “Encryption” and “Authentication” proposal you wish to use (Encryption options are DES, 3DES, AES128, AES192, AES256) (Authentication options are MD5, SHA1, SHA256, SHA512)
- Select the Diffie-Hellman key group (options are DH1, DH2, DH5)

Note: The caution symbol to the right will appear on areas where input is required or if there is a mistake with the entry, such as illegal/unsupported characters.
VPN Connection (Phase 2)

Now that the VPN Gateway (Phase 1) rule has been created click on the VPN Connection tab to insert the Phase2 rule for the VPN tunnel. Click the Add button to insert a rule. On the top left of the window click the Show Advance Settings button to view all options in the menu.

- Check the box to enable the rule and give it a name
- Set the VPN Gateway application scenario to use “Remote Access (Server Role)”
- For the application scenario, set the VPN Gateway dropdown to use the Phase1 policy that was created on the previous step. (RoadWarrior for this example)
- Scroll down to the Policy option and set the Local Policy to use the “LAN1_SUBNET” address object, this will give the VPN user access over all devices connected to LAN1
- Active Protocol under the Phase 2 Setting should be set to “ESP”
- The Encapsulation is “Tunnel”
- Set the “Encryption” and “Authentication” proposal you wish to use
  (Encryption options are DES, 3DES, AES128, AES192, AES256)
  (Authentication options are MD5, SHA1, SHA256, SHA512)
- **Perfect Forward Secrecy (PFS)** is an added level of encryption, it is not necessary to enable it, but, if you wish to use the added encryption level the options are None, DH1, DH2 and/or DH5
- Under Related Settings make sure the Zone is set for “IPSec_VPN”
**General Settings**

- **Enable**: Checkbox selected
- **Connection Name**: RoadWarrior_Connection

**VPN Gateway**

- **Application Scenario**:
  - Site-to-site
  - Site-to-site with Dynamic Peer
  - Remote Access (Server Role)
  - Remote Access (Client Role)
- **VPN Gateway**: RoadWarrior, wan1 0.0.0.0 0.0.0.0

**Manual Key**

- **Manual Key**
- **My Address**
- **Secure Gateway Address**
- **SPI**: (255 - 4095)
- **Encapsulation Mode**: Tunnel
- **Active Protocol**: ESP
- **Encryption Algorithm**: DES
- **Authentication Algorithm**: SHA1

**Policy**

- **Local policy**: LOCAL_SUBNET, INTERFACE_SUBNET, 192.168.23.0/24

**Phase 2 Setting**

- **SA Life Time**: 86400 (180 - 3000000 Seconds)
- **Active Protocol**: ESP
- **Encapsulation**: Tunnel
- **Proposals**
<table>
<thead>
<tr>
<th>#</th>
<th>Encryption</th>
<th>Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3DES</td>
<td>SHA1</td>
</tr>
</tbody>
</table>
- **Perfect Forward Secrecy (PFS)**: DH1

**Related Settings**

- **Zone**: IPSec_VPN
Now that Phase 1 and Phase 2 of the VPN rule have been completed, uncheck the box to “Use Policy Route to control dynamic IPSec rules”. Unchecking this option will allow the ZyWALL to automatically create routes for connected VPN users.
Configuration Provisioning

Certain VPN clients such as the “ZyWALL IPSec VPN Client” and “TheGreenBow VPN Client” have a provisioning option that allows them to download the settings you have configured for the VPN rule instead of having to manually configure the client. To setup the VPN provisioning for the RoadWarrior dynamic VPN rule we just created click the Configuration Provisioning tab in the IPSec VPN menu (Configuration → VPN → IPSec VPN).

Before we set up the provisioning we need to create a user account to allow download of settings. Go to Configuration → Object → User/Group and click the Add button to insert a “User” level account, administrative accounts cannot use the configuration provisioning download option.

Now that the user account has been created go to Configuration → VPN → IPSec VPN and click the Configuration Provisioning tab to insert a rule to allow download of the RoadWarrior VPN settings via the VPN client.

- Enable the VPN Configuration Provisioning menu
- Click the Add button to create a rule to allow provisioning of the “RoadWarrior_Connection” VPN Connection for the “vpn-user” Allowed
User. Make sure the rule is enabled and click **Apply** to save the settings.
ZyWALL VPN Client

To download the VPN configuration provisioning settings configured on the router, open the client software and click the **Configuration** menu, select the “Get from Server” option.

Type in the public IP address, domain name or DDNS name associated with the ZyWALL router. The client downloads the setting via SSL, by default the ZyWALL is programmed to use port 443 for SSL, if you have changed the port please provide the new SSL port. Type in the username and password associated with the provisioning configuration and click **Next**.
Note: This only works while remote management is enabled on the ZyWALL router, if remote management has been disabled the configuration provisioning feature will not be able to retrieve the VPN configuration settings automatically from the ZyWALL router.

The client will send the request to download the VPN configuration settings to the ZyWALL router.
Now that the configuration has been downloaded you can establish a VPN tunnel between your computer and ZyWALL router. Right click the phase2 portion of the configuration and select “Open Tunnel” to initiate the VPN dialer.
Testing & Troubleshooting

Attempt to establish a VPN connection to the router. Once the connection is established; try pinging or accessing any resources from the remote network.

1. If you cannot get traffic through the VPN tunnel:
   - Disable the firewall on the remote host to make sure it is not blocking the request.
   - Attempting to access resources using computer hostname? Try using the IP address assigned to the computer instead. Using a computer hostname requires the NetBIOS broadcast protocol to resolve the computers 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.
   - Disable the ZyWALL routers firewall.
   - 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.
   - Check the host network gateway, if the local router (not the ZyWALL) does not have VPN pass-through enabled or necessary ports opened, the VPN may not function properly.
   - Contact tech support for further assistance.

2. VPN tunnel will not establish/connect:
- 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 is 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 computer firewall is allowing communications from the VPN client.

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

- Check the VPN settings on the ZyWALL and make sure they match the software client configuration.

- Contact tech support for further assistance.