Setting Up Wireguard Client with PFSense

Configuring the Client

You need a few pieces of information to configure the client and server. This documentation is just for the client side.

1. Install `wireguard` and `wireguard-tools`

   ```
   sudo apt-get install wireguard wireguard-tools
   ```

2. Generate a public and private key. This can be done on any system that has "wireguard-tools" installed

   ```
   wg genkey | tee privatekey | wg pubkey > publickey
   ```

   The private key goes to the client, the public key goes to the Wireguard server configurations. See the Configuring PFSense section for details on where to use this Public Key.

3. Start with a basic Wireguard template, save as `wg0.conf`

   ```
   [Interface]
   PrivateKey = <Client Private Key from Step 2>
   ListenPort = 51820
   Address = 192.168.50.<NEXT FREE IP>/24
   DNS = 192.168.1.1 #DNS Server available to the network

   [Peer]
   PublicKey = <Tunnel Public Key from Wireguard Server>
   AllowedIPs = 192.168.50.0/24, 192.168.3.0/24, 192.168.1.0/24 # Comma delimited list of networks/hosts to give client routes to
   Endpoint = <Wireguard Public IP Endpoint>:51820
   ```

4. In Ubuntu's case, you must link the `resolvectl` binary to the `resolvconf` binary that `wg-quick` assumes is used.

   ```
   sudo ln -s /usr/bin/resolvectl /usr/local/bin/resolvconf
   ```

5. To test the configuration:

   ```
   wg-quick up ./wg0.conf
   ping 192.168.50.1
   ip route # Look for routes that go through wg0 interfaces
   ```

```
wg-quick down ./wg0.conf
```

6. Make the configuration persistent on the client: Then move your configuration file to the `/etc/wireguard/` directory to enable an auto startup of the VPN on system boot.

```
sudo mv ./wg0.conf /etc/wireguard/wg0.conf
sudo systemctl enable wg-quick@wg0.service
sudo systemctl daemon-reload
sudo systemctl start wg-quick@wg0
```

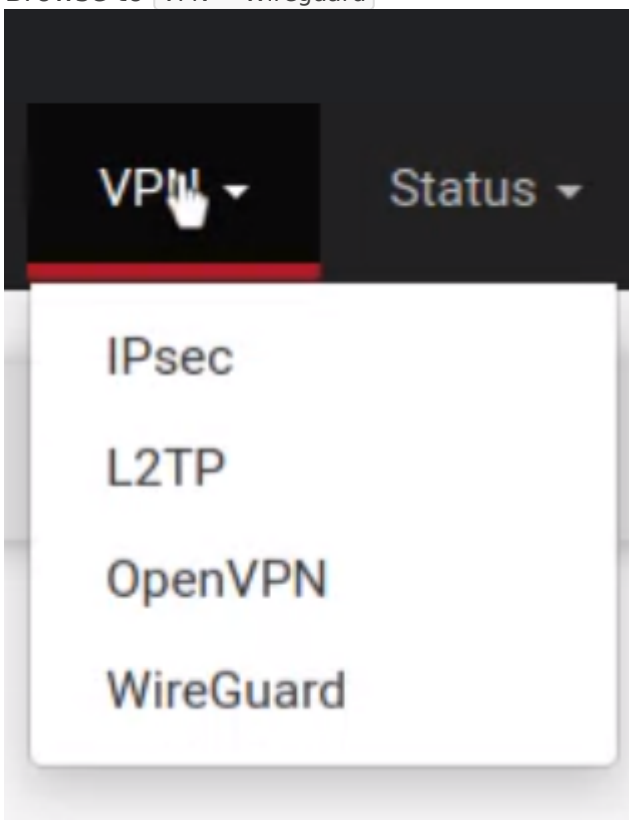
Configuring PFSense

Configuring Wireguard

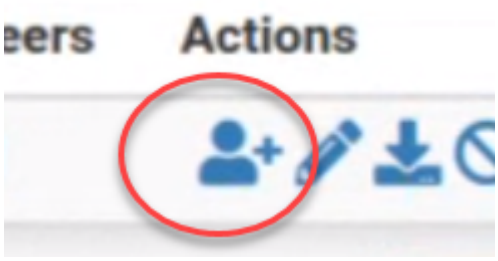
1. Install the package via `System > Package Manager > Wireguard`
2. Browse to `VPN > Wireguard`
3. Add a tunnel
4. Generate a `key pair` (Configuration and Peers to be configured later). The public key from this is needed in Configuring the Peers
5. Set allowed IPs to be a NetworkID/netmask in CIDR notation (`192.168.50.0/24`)
6. Add `Firewall > Rules > WAN` to allow 51280 to an IP on PFSense to be routed to Wireguard.
7. Add `Firewall > Rules > Wireguard/Opt` to allow Wireguard traffic to appropriate resources on other network interfaces.

Configuring Tunnel

1. Browse to `VPN > Wireguard`



2. Click the person+ icon to the right of the tunnel



3. Set a Description, Tunnel (Created in above section), check Dynamic Endpoint, and copy in Public Key from peer. This value comes from the Configuring the Client page.
4. Set an IP address for the peer, this is unique to the peer and should be the IP/Mask in CIDR notation `192.168.50.3/32`