Remote Access

Allowing remote access is just a matter of setting up a new *Wireguard* interface, allowing incoming traffic to that interface, and making sure the firewall allows that traffic to connect to the rest of the network.

Create Interface

```
# cd /etc/wireguard
# umask 077
# wg genkey | tee guard.key | wg pubkey > guard.pub
# printf "[Interface]\PrivateKey = %s\n" `cat guard.key`
```

Then I modified my file to finish configuring the interface and allow a `[Peer]` for my laptop.

```
# /etc/wireguard/guard.conf
[Interface]
PrivateKey = ****
+ Address = 10.0.2.1/28, 2001:db8:2ebf:2::1/64
+ ListenPort = 51820
+
+ [Peer]
+ PublicKey = Iz5ceR0+tCN3BLTWehZxSplzdbABRT8geqifFxubHUA=
+ AllowedIPs = 10.0.2.4/32, 2001:db8:2ebf:1::4/128
+ PresharedKey = ***
```

Line 4: Sets an IPv4 and IPv6 address for this interface. These will be the servers IPs on each virtual subnet.

Line 5: Sets the port to listen to for this interface. It is just the default *Wirgaurd* port and I'll allow traffic through the firewall for it soon.

Line 7-10: Declare a peer, define the public key to use when communicating and validaing any connections, set what IPs the peer is allowed to use on each virtual subnet, and configure a pre-shared key for additional secuirty.

> A preshard key can be generated by running `wg genpsk` and must be the same on both the `[Peer]` block on the server and the `[Interface]` block on the client.

Firewall Configuration

First I had to declare a new interface and since I want it to be as if I was sitting on my laptop at home, I put it in the `lan` zone.

```
# /etc/shorewall/interfaces
...
 #ZONE□INTERFACE□OPTIONS
...
 wg□WGAZSE1_IF□tcpflags,nosmurfs,routefilter,logmartians,physical=wgazse1
+ lan□WGGUARD_IF□tcpflags,nosmurfs,routefilter,logmartians,physical=wgguard
```

```
# /etc/shorewall/interfaces
...
 #ZONE□INTERFACE□OPTIONS
...
 wg□WGAZSE1_IF□tcpflags,nosmurfs,routefilter,logmartians,physical=wgazse1
+ lan□WGGUARD_IF□tcpflags,forward=1,physical=wgguard
```

For outside clients to connect I need to add a rule that allows them to connect to the firewall on port 51820.

```
# /etc/shorewall[6]/rules
+ ACCEPT         wan,lan         $FW             udp             51820
```

The last step is to once again setup masquerading so traffic from clients on the *Wireguard* subnet appear to be originating from the `wgguard` interface which is in the `lan` zone.

```
# /etc/shorewall/snat
+ MASQUERADE□□10.0.2.0/28□□□□WAN_IF,LAN_IF,DMZ_IF
```

```
# /etc/shorewall6/snat
+ MASQUERADE□□fde9:2375:2ebf:2::/64□WAN_IF,LAN_IF,DMZ_IF
```

Revision #8
Created 2 April 2021 02:48:25 by dustin@swigg.net
Updated 10 April 2021 03:45:05 by dustin@swigg.net