IPFire OpenVPN Recipes

For the most part, you should visit the IPFire Wiki for a much fuller set of instructions. This contains a limited number of special purpose recipes that I have not yet submitted to that wiki.

Following is very much a work in progress.

OpenVPN commonly breaks connections down into Road Warrior and N2N (aka Site to Site) connections. A Road Warrior connection is a specific machine which connects to a remote OpenVPN server, gaining access to the LAN protected by it as if the machine were physically plugged into that LAN.

N2N connections make permenant connections between two LAN's, often greatly separated geographically. Users on either LAN may freely access IP's on the other LAN when the connection is in place. Obviously, firewall rules can limit access for either scenario.

The following shows a typical setup, where the Road Warrior Workstation is connecting to the Main LAN via the Main Firewall. Additionally, the Primay LAN is connected to the remote locations Site 1 LAN and Site 2 LAN.

Multiple N2N

It is not uncommon for an OpenVPN setup to have one or more N2N connections, connecting multiple sites together to a centralized firewall. This allows several scenarios, including:

1. connecting one or more remote offices to a central office, allowing resource sharing
2. connecting home offices

Road Warrior access to remote N2N sites

On the N2N Server, edit Advanced Server Options and add the remote N2N sites subnet in the Route push options box. NOTE: you must shut down the OpenVPN server to do this, so it must be done from inside the network.

Make the Road Warrior connection to the main OpenVPN router, and you will see several lines like:

```
Thu Nov  8 02:23:27 2018 /sbin/ip route add 10.0.31.0/24 via 10.19.117.1
Thu Nov  8 02:23:27 2018 /sbin/ip route add 10.0.32.0/24 via 10.19.117.1
Thu Nov  8 02:23:27 2018 /sbin/ip route add 10.91.187.0/24 via 10.19.117.1
Thu Nov  8 02:23:27 2018 /sbin/ip route add 10.111.56.0/24 via 10.19.117.1
```

At this point, Road Warriors may access the remote locations, but the remote locations do not know how to respond. You need to create a routing rule that basically says “when you get a connection from *Road Warrior IP* reply via *N2N tunnel*.

Simplest way to figure out what the Road Warrior range of IP's is is to log into the firewall/router, go to the OpenVPN page, and look at it. Top section, right hand side.

I usually log into the command line on the primary firewall and run

route -n | grep 'remote subnet'

and look at its gateway. An example of this on one of my IPFire machines is:

```
[root@ipfire ~]# route -n | grep '10.0.31.0'
10.0.31.0       10.108.229.2    255.255.255.0   UG    0      0        0 tun2
```

showing 10.0.31.0 uses a gateway of 10.108.229.2 on device tun2. 10.108.229.2 is the tunnel IP used by the OpenVPN server, so:

1. Log into the remote firewall and go to Network | Static Routes.
2. Host IP address / Network: subnet of Road Warrior network
3. Gateway: tunnel IP address of connection on OpenVPN Server
4. Click the Add button

Your Road Warrior can now access the remote network without having to log into a machine on the primary LAN.

Security