# opnSense Road Warrior

1. Create a Certificate of Authority (hint, use an existing one if you want)
    1. System | Trust | Authorities
    2. Add and select Create Internal
        1. Name - System CA (or something)
        2. Lifetime - 3650 (10 years)
        3. Fill in rest of stuff
        4. Click Save
2. Set up local authentication
    1. System | Settings | Administration | Server = Local Database
3. Create a Server Certificate (recommend you create a new one)
    1. System | Trust | Certificates
    2. Add and select Create Internal
        1. Descriptive Name - VPN Road Warrior Server Certificate
        2. Certificate authority - Select System CA
        3. Type Server Certificate
        4. Lifetime - 3650 (10 years)
        5. Common Name - roadwarriorservercert
4. Server Settings.
    1. VPN | Open VPN | Servers
    2. Use wizard to create
    3. Type of Server - Local User Access
    4. Certificate Authority - System CA
    5. Server Certificate - VPN Road Warrior Server Certificate
    6. General Settings
        1. Interface - WAN
        2. Protocol - UDP
        3. Local Port - Choose one around 1190 which is not used by something else
        4. Description - Road Warrior
    7. Cryptographic Settings - I just leave them at default
    8. Tunnel Settings
        1. IPv4 Tunnel Network - any subnet defined for private use (ie, 10., 172., 192)
        2. IPV6 Tunnel Network - I don't use
        3. Redirect Gateway - check if you want all traffic to be forced through the tunnel. More secure, but uses more bandwidth
        4. IPv4 Local Network - the subnet on your LAN
        5. Concurrent Connections - maximum number of simultaneous VPN connections allowed at one time (all users)
        6. Inter-Client Communication - Check if you want VPN users to “see” each other
        7. Duplicate Connections - Check if you want one user to be able to use the same settings simultaneously on different computers
        8. I generally leave the rest of it alone; you can change it later if you want.
    9. Firewall Rule Configuration
        1. Check the first box to get it to automagically create the firewall rules to allow VPN connections
            1. After creation, you can go to Firewall | Rules | WAN and see the rule to allow entry
            2. You can also go to Firewall | Rules | OpenVPN to see the rule to allow traffic

after the connection is created
2. Check the second if you want users to be forced to pass all traffic through the VPN connection

5. System | Access | Groups (optional, allows RoadWarriors to change their passwords)
6. Add
    1. Group Name - Road Warrior
    2. Description - Road Warrior Users
    3. Save
    4. Edit
    5. Assign Privileges (hint, use the filter
        1. Lobby: Login / Logout / Dashboard
        2. GUI: System:User Password Manager
7. System | Access | Users
    1. Add
        1. Username - I use all lower case, no special chars (including spaces)
        2. Password - Put in a good password (user can change it is if you set up the group)
        3. If the user should be able to log in from the cli or ssh, change login shell
        4. Expiration Date - Leave blank to not expire
        5. Group Memberships - RoadWarrior
        6. Certificate - Click to create a user certificate
        7. Save, it will go to the Create a Certificate page
        8. Method - Create an internal certificate
        9. Lifetime
            1. 3650 = 10 years, or whatever you want
            2. When the Cert expires, user will no longer be able to use VPN and you must generate a new cert
        10. Change the stuff below if you want; the default is usually sufficient
        11. Click Save, you will return to the User screen for that user
        12. Add an SSH authorized_keys file (with public ssh key) if you want.
8. VPN | OpenVPN | Client Export
    1. Change Remote Access Server if you have more than one and want to select one
    2. Host Name Resolution - choose how the client knows what to connect to
        1. Since I try to set up my firewalls using a DNS name as it's name, I usually select “installation hostname”
        2. If you have a static IP, you can use the Interface IP Address
        3. If you need to manually put something in, choose “Other”
    3. You can protect the certificate with a password by checking Use a password to protect pkcs12 file. Users will have to use that password, then use their username/password to make a connection
    4. For each user, select Export type. “Others” fits about anyplace and is a single file, but if you are using Viscosity, or are using on a tablet/phone, use one of the specific options.

# Links

- https://www.kirkg.us/posts/building-an-openvpn-server-with-opnsense/
- https://doc.pfsense.org/index.php/OpenVPN_Remote_Access_Server