opnSense Quick Reference

Initial Setup

- Do all firmware updates
- System | Settings | Administration
  - Set console for serial, if you want
  - Enable SSH (Secure Shell)
  - Choose whether to allow root to log in, and whether to allow password auth
  - Set Serial Console if desired
  - Set Authentication Server to Local Database
  - Set parameter for sudo
- System | Settings | Misch
  - Set hardware acceleration if your hardware supports it
  - Add swap file if memory low and you can spare 2G of disk
  - If you have plenty of memory, set /tmp as RAM disk: Generally uses less than a meg.
  - If you have plenty of memory and don't care if your logs survive a reboot, set /var to RAM disk.

Using extra ports on router for switch

https://www.thewichitacomputerguy.com/blog/how-setup-pfsense-opnsense-4-port-nic-switch-bridge

GeoIP blocking

1. Create account at https://www.maxmind.com/en/geolite2/signup
    1. Give valid e-mail address (used to send you the link)
    2. My License Key | Generate Key
    3. Do NOT use geoipupdate
    4. Save key ID someplace safe
2. Create link
    1. https://download.maxmind.com/app/geoip_download?edition_id=GeoLite2-Country-CSV&license_key=My_License_key&suffix=zip (replace My_License_key with yours)
    2. Test by pasting link into browser. It will download a zip file
3. Create alias in opnSense
    1. Firewall | Aliases | GeoIP
        1. Enter URL
        2. Click Apply
    2. Firewall Aliases | New
        1. Name - Something you can remember
        2. Type - GeoIP
        3. Select regions/countries to be included
            1. NOTE: If you are wanting to **exclude everything but** some countries, ie block all but, you can simply list the countries you want to have access, then

use the **NOT** value in the rules

4. Enter an optional description
5. Click Save

3. Firewall | Rules | WAN
    1. Action - Block
    2. Quick - Apply acction immediately on match (check box)
    3. Interface - WAN
    4. Direction - in
    5. Source/Invert - Put a check if you need to invert the GeoIP selection
    6. Source - name of alias you created for GeoIP
    7. Everything else is any/any, ie don't allow to anyplace
    8. Log - put a check in Log Packets if you want them kept in your logs
    9. Category - Attacks
    10. Description - Block access from other countries (or whatever you want

Note: On the rules, order is important. Any Pass rule that exists prior to this rule will negate it. For example, if you have your VPN rules before this, VPN will work from other countries. Put this as high in the list as possible.

Links

- https://docs.opnsense.org/manual/how-tos/maxmind_geo_ip.html
- https://docs.opnsense.org/manual/aliases.html