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 (Plus Sign)
        1. Name - Something you can remember, alpha-numeric and underscored only
        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 Apply

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.

OpenVPN DNS Issues

On a Chromebook, we have had an issue where making a VPN Connection using OpenVPN kills DNS. Sites can not be reached on the Chromebook while the VPN is active.

It appears ChromeOS will kill its DNS entries when a VPN connection is made, even if no DNS is in the configuration. Once the VPN connection is stopped, DNS resumes.

The solution is to add a DNS entry to your Road Warrior (Remote Access) vpn server.

1. VPN | OpenVPN | Servers
2. Select the server in question for edit
3. Find DNS Servers (under client) and enter one or more DSN servers (by IP address)
    1. Hint: if you put a forwarding DNS server within the network you are connecting to, some Operating Systems will allow you to connect by FQDN
    2. Adding DNS Default Domain will allow you to find “acme.example.local” by simply entering “acme”
    3. Adding multiple domains separated by comma's will allow you to find the same, but across multiple domains.
    4. Putting a check mark in *Force DNS cache update* will help Windows machines to use the new server list
    5. Putting a check in *Prevent DNS leaks* will disable all other DNS servers for the duration of the VPN session (Windows only)
    6. Save, then re-export the client configuration files

Admin User

In many cases for small business, you want to have a user who can perform administrative functions on the router. This is an excellent alternative to supplying everyone with the root password. You can

not, however, simply give all permissions, as some conflict. Following will give a group admin rights, without making them a member of the admin group and keeping the root password secure.

1. System | Access | Groups
2. Add new group by clicking the plus sign
3. Create a name (I called it sysadmin), set a description, then add one or more users.
4. Save
5. Edit new group
6. Edit permissions (pencil, under Assigned Privileges)
7. Search for *All Pages* and select that (GUI All pages)
8. Do not add or remove anything else
9. Save
10. The users you have added to this group can not log in, with their own credentials, and manage the router

Limited access user

In some cases, you need to give an end user limited rights. They need to be able to log into the router's WebUI and perform some limited functions. This will show you how to allow a user to A) change their own password and B) reboot the router.

1. System | Access | Groups
2. Create new group by clicking plus sign
3. Group Name: Reboot, Description: whatever, Add users to group
4. Click Save
5. Edit the new group
6. Click the pencil under *Assigned Privileges*
7. Search for, and enable, reboot (*GUI Diagnostics: Reboot System*)
8. Search for, and enable, password (*GUI System: User Password Manager*)
9. Search for, and enable, login (*GUI Lobby: Login / Logout / Dashboard*)
10. Save

The user(s) you have as a member of this group will be able to login, change their password, and reboot the system.

Links

- https://docs.opnsense.org/manual/how-tos/maxmind_geo_ip.html
- https://docs.opnsense.org/manual/aliases.html
- https://forum.opnsense.org/index.php?topic=38493.0

From:
https://kb.unixservertech.com/ - **Unix Server Tech Knowledge Base**

Permanent link:
https://kb.unixservertech.com/other/networking/opnsense/quickreferences

Last update: **2025/01/11 01:59**