OPNSense Install and Initial Setup

https://www.youtube.com/embed/Qrglquxw-6I

I've been wanting to switch away from my Eero mesh wireless network for almost a year and a half. I really wanted a system that I had more control over, and an open source option was my ideal situation. I have made several attempts to do this over the past six months, but each time I found I just wasn't able to get everything setup the way I needed.

First, I tried to setup just DD-WRT on a few routers, using one as the main router and the rest as APs. The system functioned, but for whatever reason DHCP was not working, and none of my DHCP devices would get an address.

I then tried pfSense with the DD-WRT Routers set as APs only, and pfSense set to assing out DHCP addresses. This initially seemed to work, but then I ran into multiple issues trying to get it setup to route my traffic via NAT Reflection (sometimes called NAT Redirection or Hairpinning). Essentially when I call the services running on my home machines by a URL that is running inside the same network. This was a huge bust and a bit soul-crushing as I read more and more documentation, articles, forum posts, and so on of people trying to make it work in all kinds of situations, and nothing I tried worked.

I shelved the idea for a few months, then came back to it again a week or so ago. This time, I went with OPNSense. It's a forked version of pfSense, but over time the two have gottem some real separation in the way the work. The user experience is similar, the menus and options are almost identical beyond their placement on the screen, but a few things in OPNSense felt easier to me.

Again, I was able to get it setup for DHCP, and I was able to get my DD-WRT APs setup easily, and got them working with no issue. Initially, my iPhone wouldn't pull an address, and I feared I was about to hit my original issue all over again, but with a bit of testing I realized the wired connection in my wall was not working properly, and the jack i had my AP plugged into wasn't actually allowing it to communicate with the OPNSense router (Not the same issue I had with my first setup by the way).

So, with those hardware issues out of the way, my devices were all connecting and getting DHCP addresses. Yay! Now to the task of getting my self-hosted services to be reachable from the outside world.

Installation

What You'll Need

- A hardware device or VM you want to run OPNSense on.
- at least 2 NICs - Network Interface Cards - or at least 2 ports (1 for WAN/Internet connectivity, 1 for LAN / Local Area Network)
- A USB you can flash with the OPNSense ISO and a USB Drive, or burnable DVD and DVD Drive.
- A machine with a modern web-browser on your network.
- Potentially a couple of ethernet cables.
- About an hour of your time.

Getting the ISO Image

It's important to know which media type you'll be using to boot from for the initial install. You need to know whether it's USB or DVD.

Visit https://opnsense.org/download/ and fill out the form. Select the architecture type (though it appears to only have amd64). Next, choose an ISO type. DVD for an actual DVD, or VGA if you plan to use a USB to install. Finally, pick a mirror close to your physical location. Then click the Download button.

Once the download completes, unpack the compressed archive file. NOTE: this will be about 320 MB compressed, and just over 1 GB uncompressed. Once uncompressed, you'll want to burn the ISO to your DVD or USB using a program like Balena Etcher (for USB).

Once burned, place your DVD or USB into the machine and boot it up. You'll want to make sure to boot from the DVD or USB, so you may need to press a special key to get the boot device list. This key differs based on manufacturer, model, and motherboard in most cases.

Once the boot process starts you'll want to go through the options to select your

- When presented with the initiall login prompt, you'll want to use the username "installer", and the password "opnsense" in order to start the install process.
- Keyboard map (if you need something beyond the default for your system, highlight the language support you want, press the spacebar to select it, then press Enter).
- Select the drive you want to install OPNSense onto. NOTE: da0 is usually your internal hard drive, and ada0 is usually the USB drive..
- Allow the installation to proceed.
- Enter an admin password, and confirm it.

- Reboot the system. NOTE: Remove the flash drive / DVD when the system starts to boot back up.
- Allow the system to boot. You again can login with the admin user "root" and the password you just set.

Once logged into the terminal, you may want to re-assign your interfaces. You want to ensure the WAN interface is plugged into the correct ethernet port, and the same for the LAN interface.

To change the assignments, you'll press "1", then Enter.

the system will provide a list of detected interfaces. Unless you need LAGGs or VLAN support, you can answer "n" for both of these questions.

Now enter the interface name for the WAN (internet connection) port. Then press Enter.

Next, enter the interface name for the LAN (local area network) port, and again press Enter.

If you have more ports, and want to assign them for other purposes, then you can enter those next, or leave the final entry blank, and just press Enter to save and confirm your changes.

Give the system about 15 seconds to bring you back to the main menu. If it doesn't you can likely use CTRL + C to get back to the menu. Now you can logout of the CLI, making note of your LAN interface IP address.

In my case, after the re-assignment task, my LAN was on 192.168.1.100, though yours may be different.

Now, on another machine, go to your web browser, and browse to the LAN IP address. NOTE: You can not browse to the web interface for OPNSense from the WAN address by default, and it is better if you don't allow access via the WAN interface.

The Web UI and Setup

If you only want to use this box to get internet access out from your network, and you have no internal servers / services running, you are essentially done, and do not need to make any further changes to your new OPNSense firewall / router. You can adjust the default dashboard if you like, but other than than you are set, and should be able to access the internet if you have your ports set properly, and pluggied into your ISP modem.

If you wish to access your internal servers, there is more to do.

System -> Settings -> Administration

Navigate, in the left menu, to System -> Settings -> Administration and change the port setting from 443 to 440. OPNSense, by default is setup to provide access to the WebGUI on port 443. We, however, want to get access to our self hosted sites on port 80 and 443, so we need to change the SSL port for OPNSense to something else. We'll use 440 for this purpose.

Scroll down, and find the "Alternate Hostnames" section. Add any domain names you will be using on your internal network from outside to this box separated by spaces. It's important you add these here, or OPNSense will assume an attempt to reach the site may be some sort of attack.

Now scroll all the way to the end of the page and Save. After saving, always check to see if an Apply option shows up at the top of the page as well, and click it if necessary.

Once you save this page it should redirect you automatically after about 30 seconds, back around to the new port 440. If it doesn't you can access it via the IP address and port 440 by typing in `https://ip.of.your.firewall:440`, where you put the actual IP in place of my place-holder text here.

Check for Updates

Go to System -> Firmware -> Updates, and let the system check for any updates, then install the updates. It's important to do this as there may be security patches and other fixes that will help make the system better.

(Optional) Change your LAN IP

Next, we'll go to Interfaces -> LAN (NOTE: this step is optional). If you want to change the subnet IP addresses for your local network (defaults to 192.168.1.x), then you can do that here. Scroll down to the "IPv4 Address" fiels and put in the address you prefer. Then scroll to the bottom and change it. Click 'Save', then go to Services -> DHCPv4 and change your DHCP range if needed so that you have addresses in the same IP. Again click 'Save', and 'Apply' if necessary.

You may need to disable and re-enable your connection to get it to pull a new address from the updated IP range.

Setup Firewall Rules for Access from Outside your Network

First we'll setup an Alias, as this will let us create fewer separate firewall rules.

Go to Firewall -> Aliases and click the "+" to add a new Alias. Call the alias web_server_ports, then select the Type as "Port(s)". Now in the Content field enter 80, then press Tab, and it should turn into a chip icon. Next enter 443 and again press Tab. Give this a description of "web server ports"

and Save / Apply.

Add another Alias, and call it 'web_server_host' and give it a Type of "Host(s)". Next, in the content, enter the IP of your web server machine. Finally, give it a description of "web server host", and click Save / Apply.

Now navigate to Firewall -> NAT -> Port Forward. Here we want to add a new rule, so click on the "+" icon, and make sure it's Enabled, and "WAN" is selected.

Next, we'll make sure we select the following:

- TCP/IP Version = IPv4
- Protocol = TCP
- Destination = WAN Address (in the video I say WAN Net, but we want WAN Address)
- Destination Port Range = (choose your alias) web_server_ports
- Redirect Target IP = web_server_host
- Redirect Target Port = web_server_ports
- Feel free to enter a Description like "http(s) port forward"
- NAT Reflection = Enable

Save this rule, and Apply.

Now we need to setup our final piece for NAT Redirection to work properly. Navigate in the left menu to Firewall -> Settings ->Advanced.

Enable the following by checking their associated checkbox:

- Reflection for port forwrads = checked
- Reflectionf or 1:1 = checked
- Automatic outbound NAT for reflection = checked.

Scroll to the bottom, and Save. Apply if necessary.

You may need to update host addresses in your proxy manager after changing your DHCP settings. But once your proxy manager is setup (assuming you're using one) you should be able to reach all of your self hosted services from inside, or outside of your network.

Support me on Patreon

Support my Channel and ongoing efforts through Patreon:

https://www.patreon.com/bePatron?u=234177

Revision #1
Created 30 September 2022 17:25:57 by Brian McGonagill
Updated 30 September 2022 17:26:50 by Brian McGonagill