Creating a Home Network

And Block Ads!

Overview

In this setup I cover setting up a home network that will use PFSense for the Firewall, DNS, and DHCP. I will cover one way to set up a Virtual Machine Host that allows its guest VMs to grab IP addresses from the router.

TLDR:

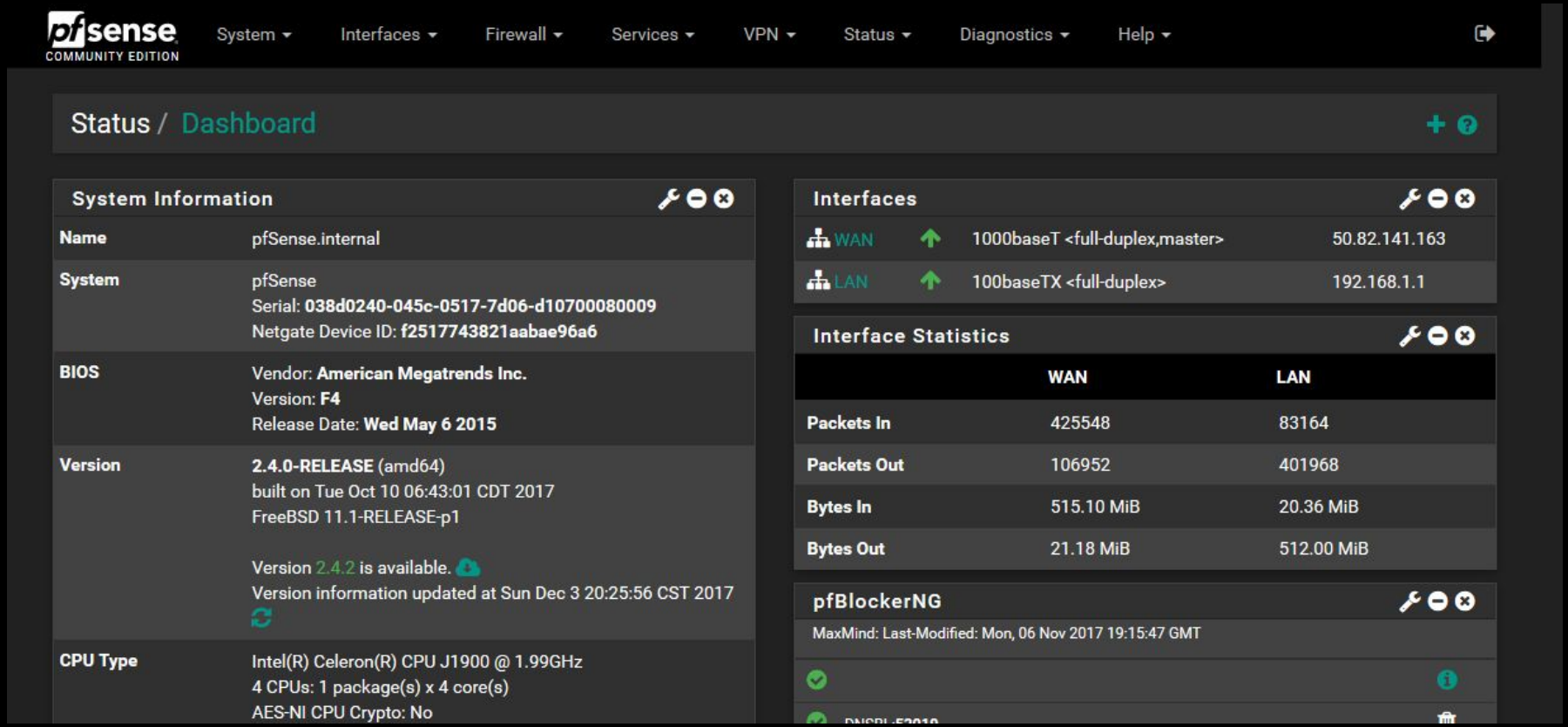
- PFSense: Firewall, Router, DNS, DHPC
- Storage: VM Host (with routable VMs) and Network Attached Storage

Why PFSense?

I chose PFsense because it is an all-inclusive home network solution. Once installed, there is a Web GUI to help with management. PFSense is based on FreeBSD, a UNIX based OS that is well known to be robust in the networking world.

Some Applictions Included:

- DNS/DHCP
- IDS/IDP
- Firewall/Router
- VPN
- Load Balancing and more!



What the home page looks like.

Things to Consider

PFSense will work on almost any hardware but if you want to run the latest versions, you will need a processor with x64 architecture.

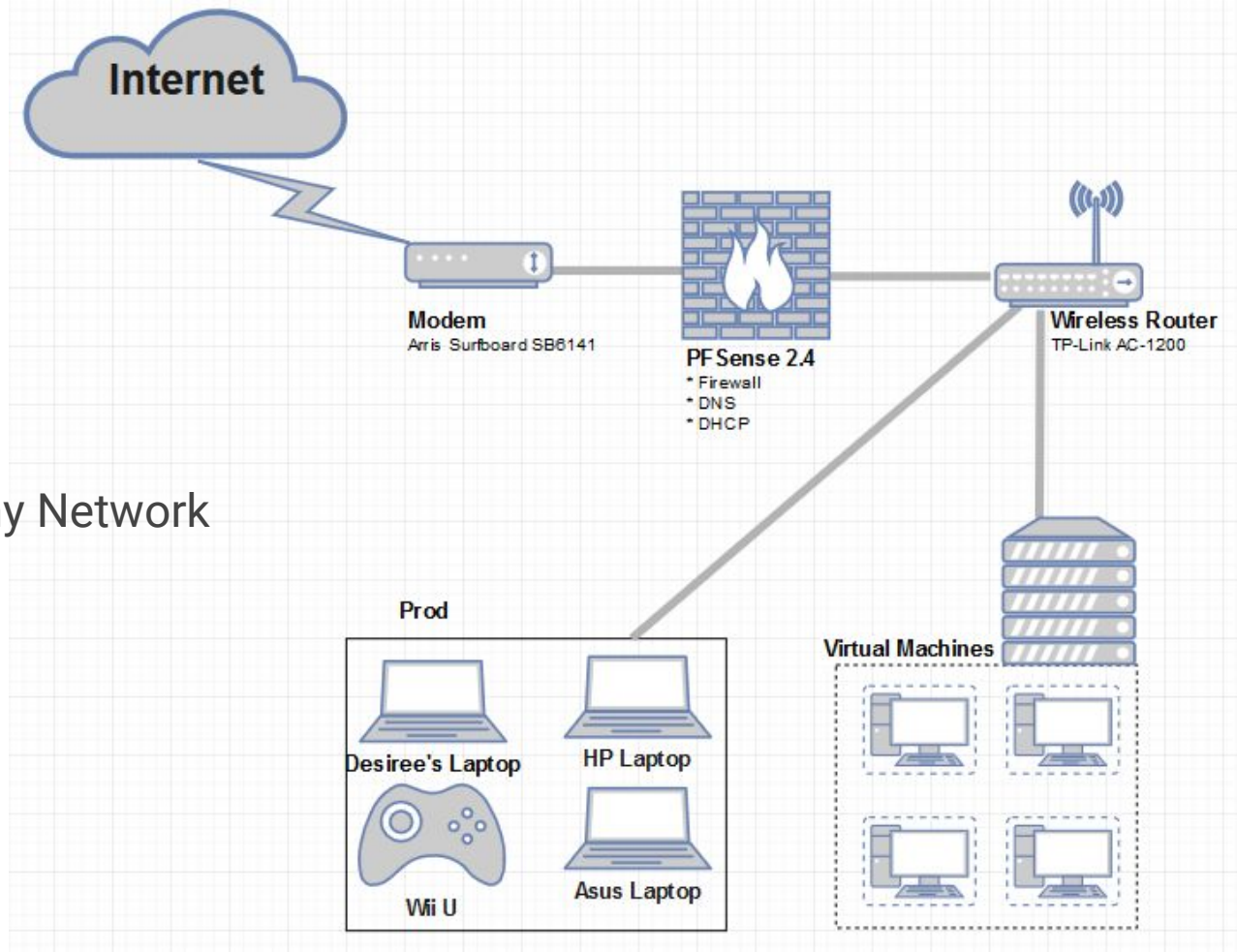
The next version (v2.5) will require a processor with AES-NI support

Requirements on RAM are very low, and should not need more than 2GB.

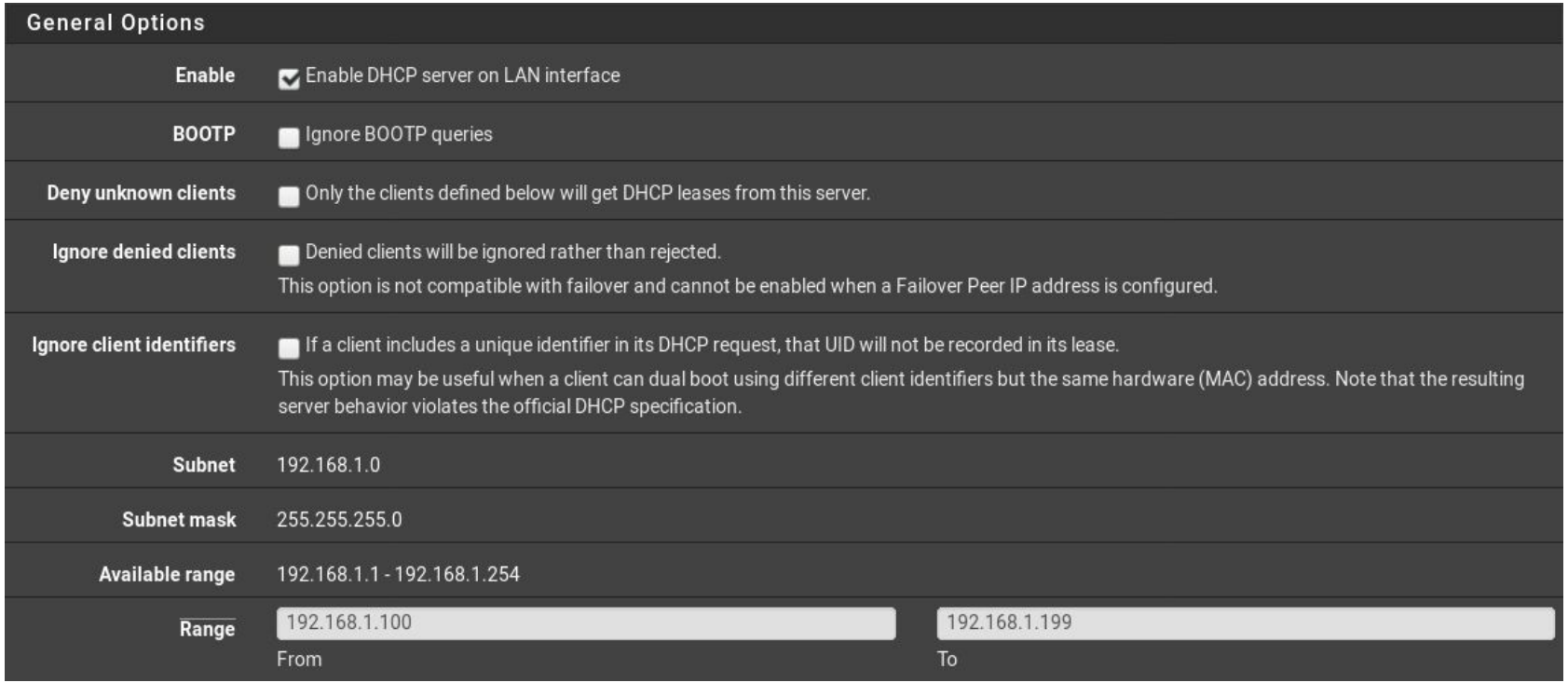
Installing: Outside the scope of this walkthrough, here is a link to the official docs

https://doc.pfsense.org/index.php/Installing_pfSense#Hardware_considerations

Network Map of my Network



DHCP Setup

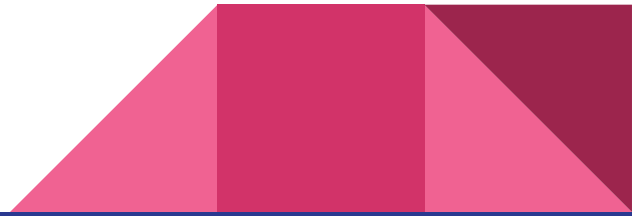


Make Sure these settings are set

DNS Setup

PFSense offers two different DNS services, I have opted to use Unbound as my DNS service because it allows you to use the pfblockerng package.

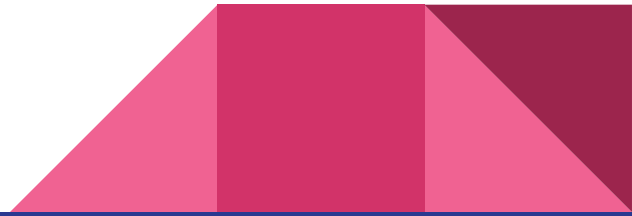
Most of the defaults work well, however make sure to set in the custom options field: server:include: /var/unbound/pfb_dnsbl.*conf



PFBlockerng

This is a package available in FreeBSD that extends the capabilities of the PFSense firewall. Installation is simple, just go to the package manager and click install. I specifically use this package to implement DNS filtering on my home network to mitigate the number of ads.

AD BLOCKING ON YOUR PHONE!

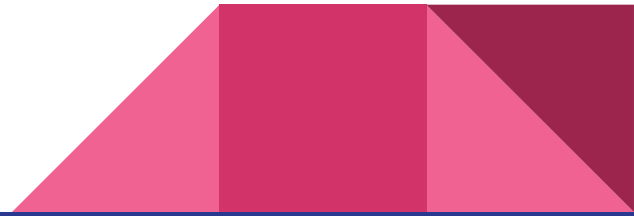


Domain Name Service Block List (DNSBL)

DNSBL Tab in the Firewall section, under the PFBlockerng tab. Here you will configure the package. On the main configuration page, the defaults are pretty sane, make sure to check enable DNSBL.

On the next page, you can make a custom feed which is what I do for my network.

The last tab contains the EasyList settings, which I have not researched so I will not include an explanation here.

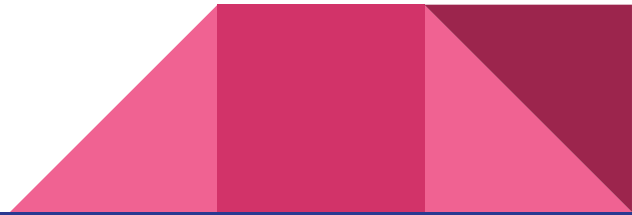


Virtual Networking

Now that we have control over our DHCP and DNS for our LAN network, we can do some neat things.

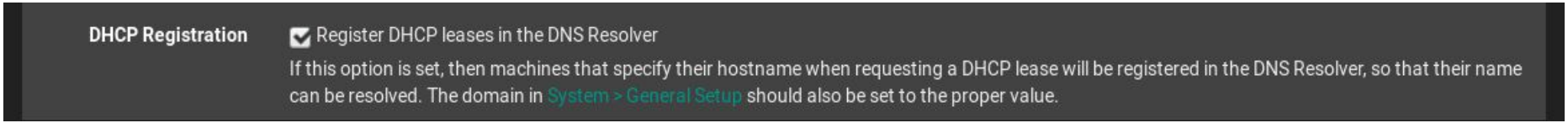
I will go over are setting up use of local DNS and how to setup a Virtual Machine Host that will be routable with the aforementioned local DNS.

After this, you will be able to spin up VMs, then be able to access them using DNS instead of IP Addresses!

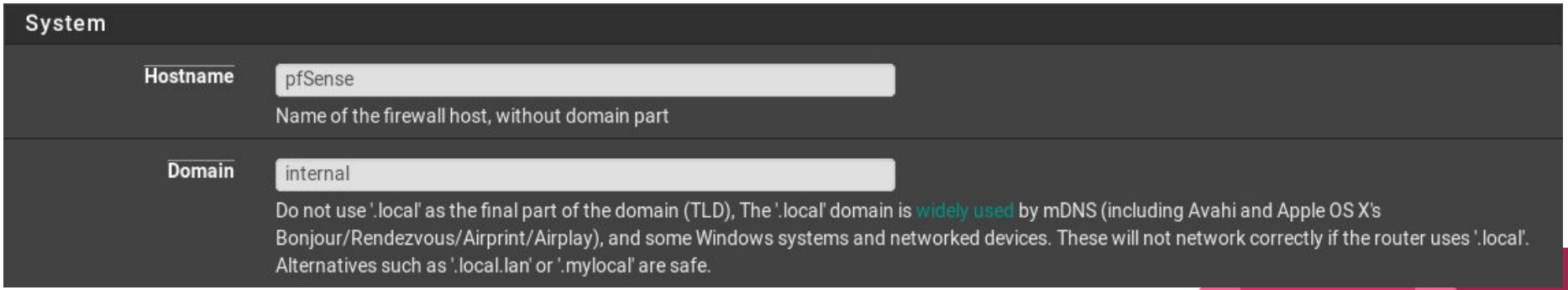


DNS for Local Machines

Located on System/General Setup



Located on Services/DNS Resolver/General Settings



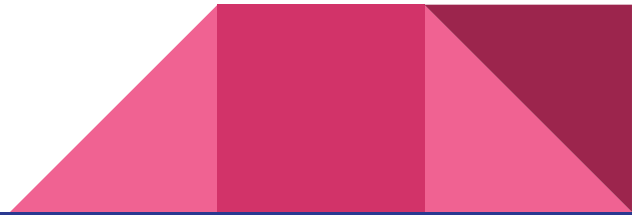
Virtual Machine Host

In my setup I am using CentOS 7.4 running KVM/QEMU virtualization. My VMs are then stored in a ZFS storage pool.

If you want to read on ZFS https://pthree.org/?s=zfs&searchsubmit=Search

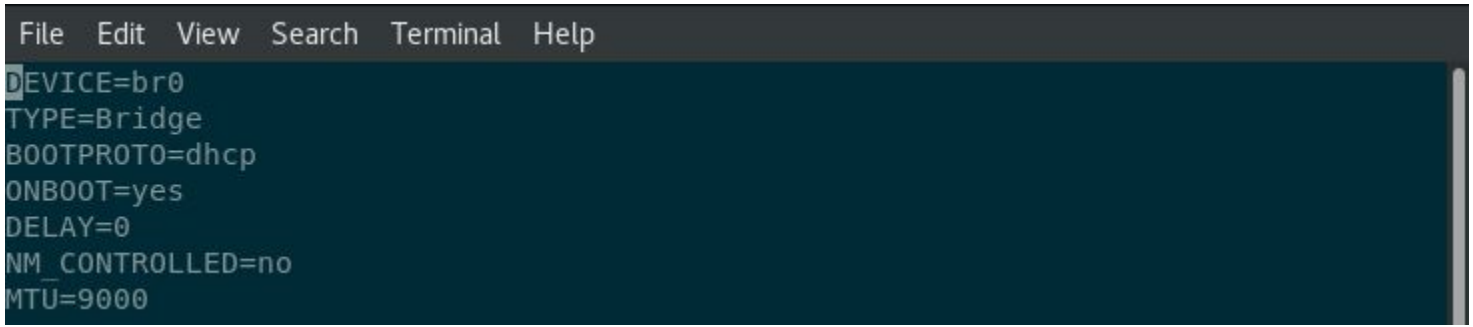
Each VM pulls a IP from PFSense and broadcasts its Hostname back so you can connect by DNS instead of IP.

To achieve this, you must configure the host with a Bridge to the VMs.

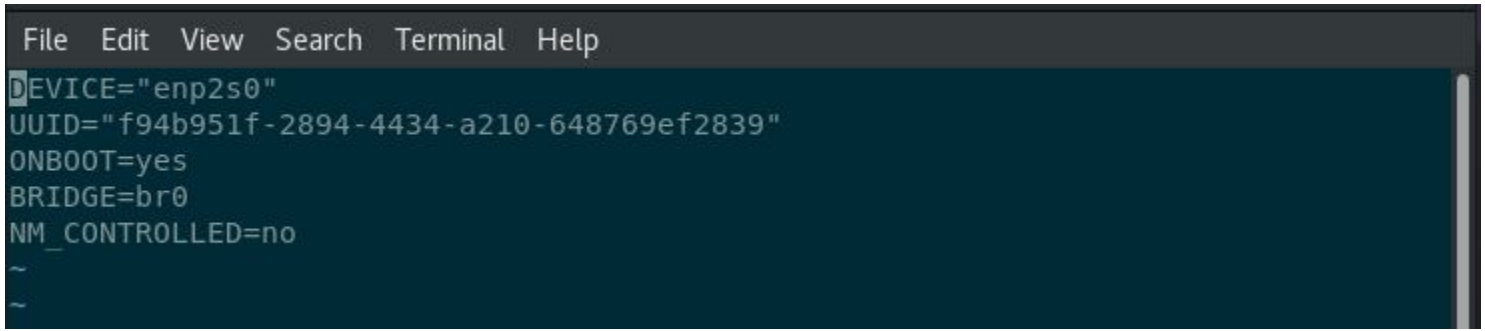


Important Settings

Bridge Settings ifcfg-br0



Ethernet Port Settings ifcfg-enp2s0



Files are located in /etc/sysconfig/network-scripts/

Now create a VM and try it out!