Analysis and Upgrade of a Household Network during COVID

by

Nick Taddei

Table of Contents

Figures

Appendix A: Acronym List

AP:	Access point
CD:	Compact Disc
COVID:	Corona Virus
DHCP:	Dynamic Host Configuration Protocol
DNS:	Domain Name Service
IoT:	Internet of Things
IP:	Internet Protocol
ISP:	Internet Service Provider
LAN:	Local Area Network
OSI:	Open Systems Interconnection model
UFS:	Unix File System
USB:	Universal Serial Bus
VLAN:	Virtual Local Area Network
VPN:	Virtual Private Network
WAN:	Wide Area Network
ZFS:	Z File System

Introduction

In March 2020, COVID turned our world upside down. Many people were forced into working from home. Everyone from K-12 schools to colleges who were forced to return home were also now forced to have class fully online. While most households have internet and WIFI, few networks were meant to carry the load expected from this new norm. This report outlines the steps I took and what I experienced when I analyzed and upgraded a household to meet the overnight network demands due to COVID.

Section 1: Know What You Currently Have Versus What You Need.

The first thing to do is to determine what you currently have for users and a network.

Know Your Users

First, determine all of the users and what each of them need. In this project, the number of users remained the same but their needs changed dramatically. For example, one user who was at school during the day and online in the evening for homework and gaming was now online most of the day for online schooling. That included not just reading and writing assignments, but also videoconferencing throughout the day. To determine user needs means more than just asking them. Determining their needs involves discussion and observation because they do not realize all their needs. As another example, one user who worked from home already said he did not need anything additional. He had one computer with a wired connection to the network and that was sufficient. After further discussion, I realized he had 2 other computers connected via WIFI and complained about lag whenever another user was gaming. I also observed other devices in his office that may need a wired connection as well. With some users it may be easy to identify all their needs, while others may not. One also has to consider the impact of a user onto other users. For instance, with COVID, people were forced to stay at home. This resulted in additional online entertainment such as streaming and gaming which can congest network bandwidth. Once you have determined all the user needs, you then consider the hardware and what ISP (Internet Service Provider) fits those needs.

Know Your Network

In user discussions, you should have determined how many computers, printers, mobile devices, etc. as well as who uses them and for what purpose. Realize that these items are likely to change, so allow for additional capabilities in your planning so you do not outgrow the network in the near future.

Another consideration that was important due to COVID was that the users not only needed wired connections, but they also needed their areas to be appropriatly spaced as physically apart from each other as possible due to noise when videoconferencing. In other words, the connection ideally could not be in a high traffic area such as a kitchen or where users conferencing at the same time could impact each other.

I recommend creating a diagram or ‘map’ of this network. I found it helpful when communicating with the users about the network. Having the diagram can also help later on with determining the best option for running cables and extending the reach of your network.

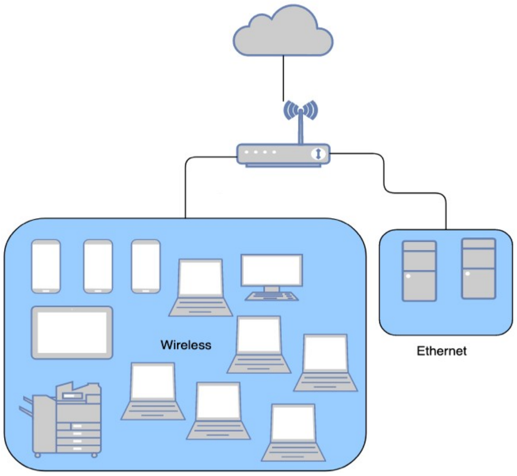


Figure 1. Sample network map

Section 2: Wireless

Basics

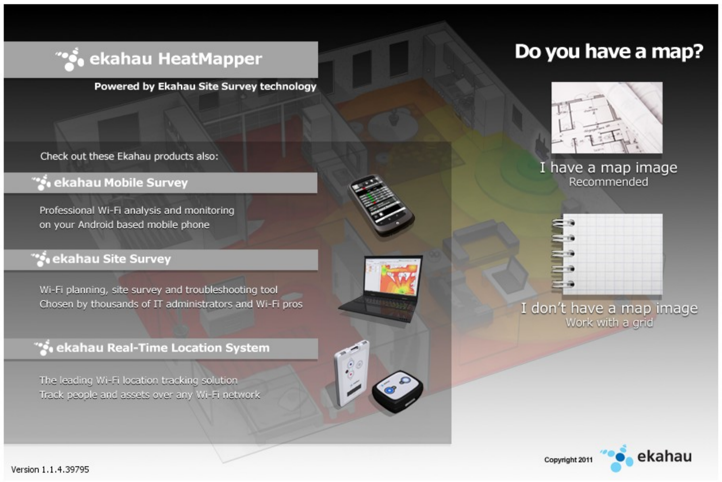
One of the most popular ways to have internet connectivity in the home is via wireless connections or WiFi. A majority of the time the wireless radio or Access Point (AP) is located where coax cable tv originally entered the house and is not the optimal location. This potentially creates a section of the house/apartment/living space that has little to no reception to that network access point. For instance, in the house I did this project on, the AP was located in a corner room. This means that half the WIFI signal was lost to the outside of the house and to the neighbor next door. The signal on the other side of the house was weak due to distance and obstacles such as a refrigerator and hidden things within some walls as well as the walls themselves. This includes things like pipes, ductwork, electrical and even steel beams.

The most effective way to alleviate this is either move the existing access point or have a separate AP at a more central location within the house. If you are using a combination device that provides you with a router/access point, it is best to split them and install an external access point that could be used instead of the one included on the combination device. Another option is to use the AP with the existing access point thus creating a multi access point network providing coverage in more than one location. In this project, I first separated out and then moved the AP from near an outside wall to the hallway. It now is more central to the whole house and also has less obstacles for the devices on that floor. I then added another AP in the basement as that area had a lot of user need for entertainment devices as well as mobile devices.

Heatmapping

In trying to decide the optimal place to put the AP for the most coverage, I used a great tool which is a piece of software called ekahau HeatMapper. The software allows the mapping out of the signal strength of your network relative to your location.

The software itself is easy to use. Upon opening it, you are greeted with a menu asking you if you want to use an image of a floor plan.



ekahau HeatMapper

Powered by Ekahau Site Survey technology

Check out these Ekahau products also:

ekahau Mobile Survey

Professional Wi-Fi analysis and monitoring
on your Android based mobile phone

ekahau Site Survey

Wi-Fi planning, site survey and troubleshooting tool
Chosen by thousands of IT administrators and Wi-Fi pros

ekahau Real-Time Location System

The leading Wi-Fi location tracking solution
Track people and assets over any Wi-Fi network

Do you have a map?

I have a map image
Recommended

I don't have a map image
Work with a grid

Version 1.1.4.39795

Copyright 2011

Figure 2. The program ekahau HeatMapper used to map signal strength

Upon selecting an image to use, you then walk around the space to gather data on the wireless signal strength at different locations, marking each location on the image until satisfied.

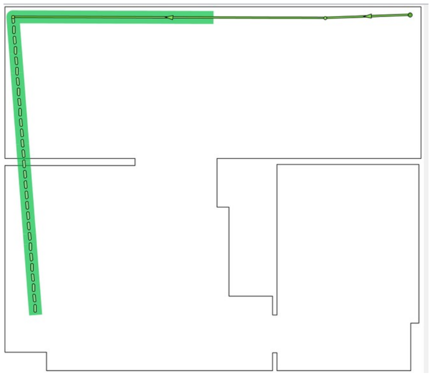


Figure 3. In-progress mapping of a floor using an image

Pressing the enter key will then generate a ‘heatmap’ of the signal strength data with green meaning excellent and red meaning poor.

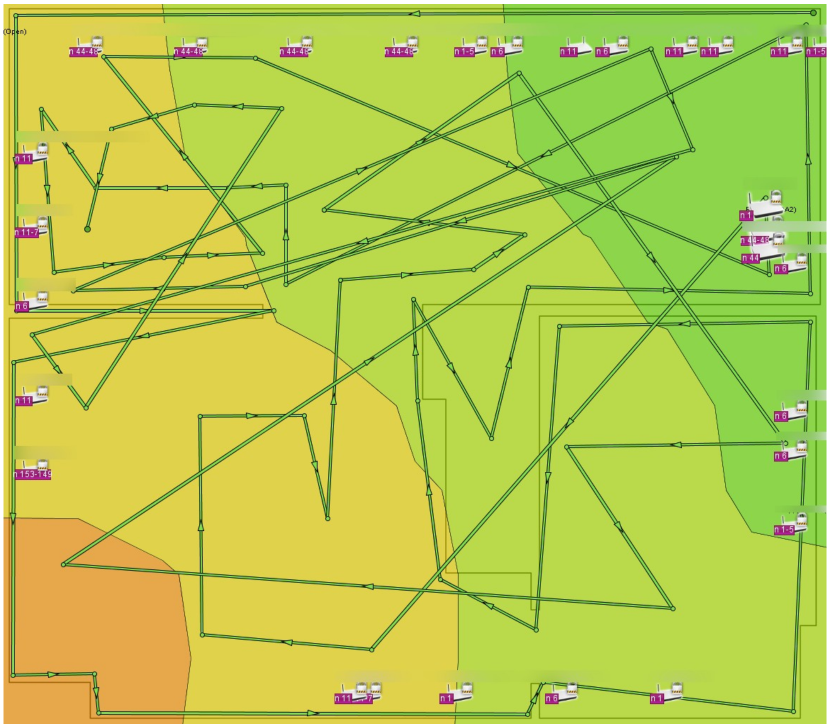


Figure 4. A completed heatmap

The use of the heatmaps will allow for planning out the best spots to install the previously mentioned access points as well as devices. The map will look chaotic, but you want to make sure you are not just testing the middle of a room, but rather testing all the spots a device will possibly be located such as on a desk in a corner, sitting on a couch, or on a counter, etc. While I knew the AP was not in the best location, based on the heatmap I created I was able to identify unseen obstacles. For instance, while standing by the couch you could see (even with your eyes) the AP through the kitchen, but when you sat down, the dishwasher behind the counter was a huge obstacle.

Section 3: Wiring

WIFI is great, however, it is not always the best solution. You need to look at the overall picture. For this project, I had four devices/areas that needed Ethernet connection so that they would not be competing for bandwidth. Since I was going to run those Ethernet cables, I ran additional lines at the same time to nearby areas for future expansion. How to run the cables can be a large undertaking on its own as you have to be concerned with what is already in the walls/ceiling/floors such as electrical, ductwork, pipes, and insulation. One definitely wants to avoid running cables within 16 inches of electrical wiring and only cross them at right angles to prevent interference. With the AP, I was also concerned about how I was going to mount it. I chose to mount it on a standard access panel (normally used for access to plumbing) that snaps into place. It worked very well, looks great, and can be removed easily if needed for service.

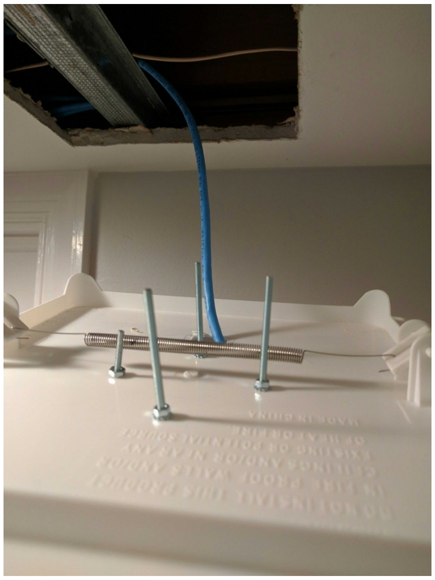


Figure 5. AP mounting bracket attached via screws

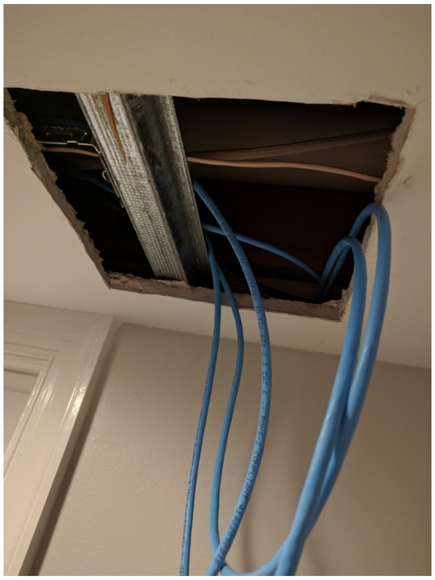


Figure 6. Ethernet cabling ran through the ceiling

For the wall Ethernet port outlets, the best option is to get what are known as a ‘old work bracket box’ that allows you to cut a hole in drywall and mount to a wall without having to nail anything. The cover plate then screws onto it. A tip for minimizing drywall dust from making a mess is to secure a piece of painters’ tape below the hole before cutting.

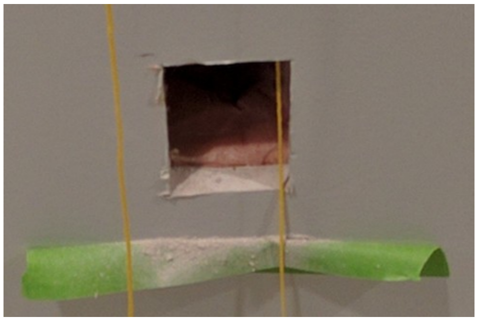


Figure 7. Method of reducing drywall dust via tape

Dropping lines

The easiest way for routing cable vertically through walls is via a string and a weight that you can then attach to the cable you want to run to any outlet cut out you have made and snake the cable down through the wall.

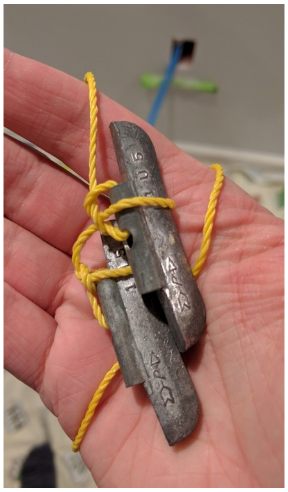


Figure 8. Lead weight used to pull cable

T-568A vs. T-568B

Once you have got all your wires run, it is now time to terminate and add connectors to them. There are two different pinouts that can be used, T-568A & T-568B, and they are the standards for Ethernet jacks. The reason for the two different standards is because of the old Bell telephone system and the creation of the registered jack types to try and standardize phones and their connections to the bell system in the 1960s. By the time ethernet was introduced, AT&T created their own standard for wiring connections which was slightly different than previous (T-568A). T-568A provided backwards compatibly with two sets of these old connections while T-568B allowed for only one, yet allowed for improvement. Today the rule of thumb is to use T-568B for new installations and rework, if T-568A is being used in existing wiring to continue to use T-568A and not change between both standards. There is not any functional difference between either standard. The only thing to be aware of is that all the network connections must be all one or the other else you will have crossover cables which are meant for connecting devices directly together.

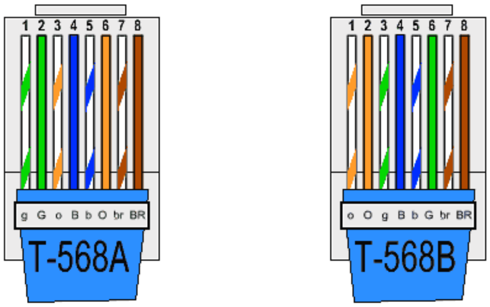


Figure 9. The two standardized ways of wiring Ethernet

Section 4: Routing

Routing might seem like this big thing that makes no sense but it is actually incredibly helpful when creating a new network or organizing an existing one.

Subnets

The purpose of subnets is to allow you to subdivide your network into different sections, like slices of a cake or pie. This dividing of a network into segments has a lot of advantages including an increased overall routing efficiency as well as being able to identify and trace back any kind of threats that could originate on the network. One way to implement this, for instance, would be to have all your wireless devices on one specific subnet while all wired devices are on another. A downside to having subnets is that if someone were to have access to your router they could see all the network traffic.

VLANs

VLANs are functionally the same as Subnets. They both deal with the segmentation or partitioning of a network but the difference is that the VLANs operate at the data link layer and subnets operate on the network layer of what is known as the OSI (Open Systems Interconnection) model. VLANs are different in that they do the same job as a subnet but virtually in software. A case for using VLANs instead of subnets is the security benefits that a VLAN has over a subnet. Devices on separate VLANs are unable to communicate with one another.

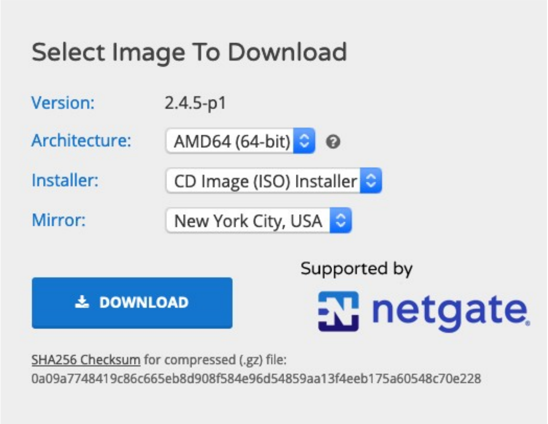
Section 5: Firewalls

pfSense

Currently every network needs a firewall to at the very least be safe online. If you have an old desktop computer sitting around gathering dust, one of the best options is to use it with the open source firewall software pfSense. pfSense itself can handle a lot more traffic than the average consumer grade router/switch combination – it can handle VPN, traffic routing, traffic shaping, and much more.

Setup

To begin with, go to pfSense.org/download then download the latest version of the software. For most computers you will want to pick the AMD64 (64-bit) option for the architecture.



Select Image To Download

Version: 2.4.5-p1

Architecture: AMD64 (64-bit)

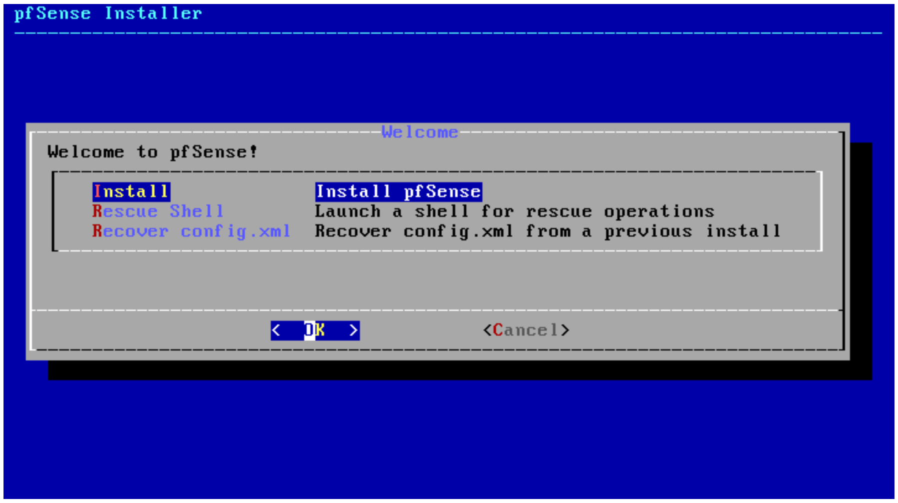
Installer: CD Image (ISO) Installer

Mirror: New York City, USA

SHA256 Checksum for compressed (.gz) file:
0a09a7748419c86c665eb8d908f584e96d54859aa13f4eeb175a60548c70e228

Figure 10. Selecting the right installer image

After downloading the image file of your choosing, create an installer USB or CD that you can then plug in to the computer that you will be installing pfSense to. Upon booting into the installer, you are greeted with the following prompt:

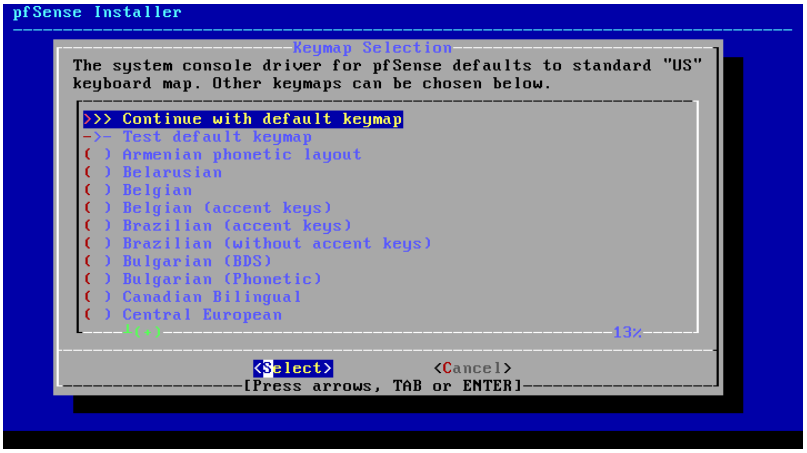


```
pfSense Installer

Welcome to pfSense!

    Install               Install pfSense
    Rescue Shell          Launch a shell for rescue operations
    Recover config.xml    Recover config.xml from a previous install
```

Figure 11. Starting pfSense installation

Hit ‘enter’ to start the install process.

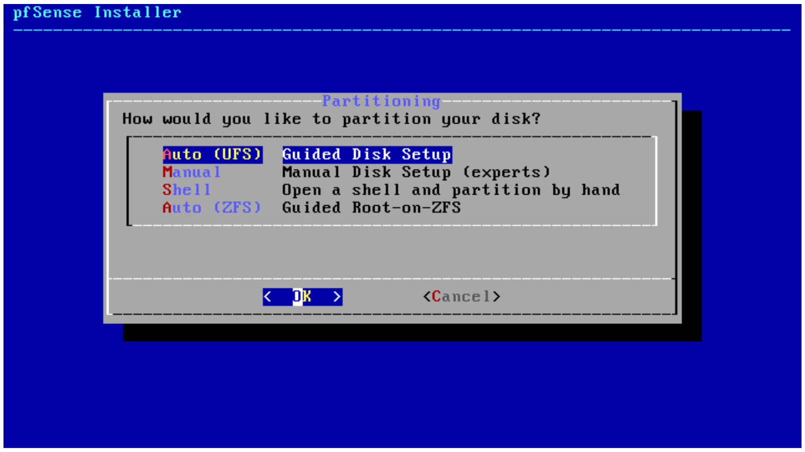
Select your choice of keyboard



```
pfSense Installer

Keymap Selection
The system console driver for pfSense defaults to standard "US"
keyboard map. Other keymaps can be chosen below.

>>> Continue with default keymap
->- Test default keymap
( ) Armenian phonetic layout
( ) Belarusian
( ) Belgian
( ) Belgian (accent keys)
( ) Brazilian (accent keys)
( ) Brazilian (without accent keys)
( ) Bulgarian (BDS)
( ) Bulgarian (Phonetic)
( ) Canadian Bilingual
( ) Central European
   ↓(+)                                             13%

          <Select>          <Cancel>
          [Press arrows, TAB or ENTER]
```

Figure 12. Selecting input language

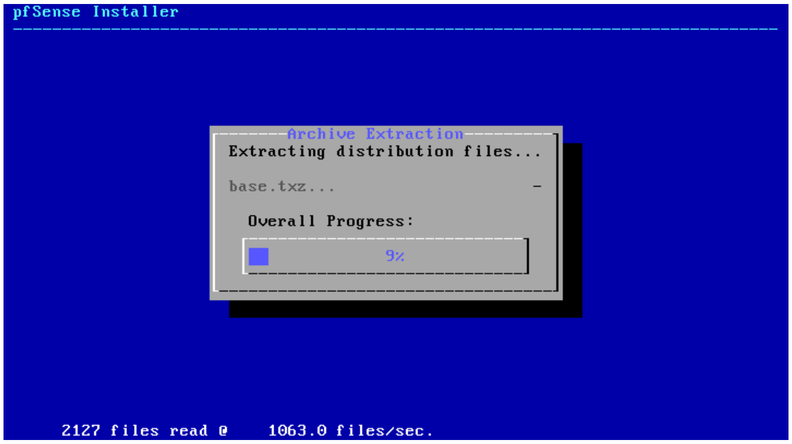
Select *Auto (UFS)* from the list. Note: partitioning the list with UFS over ZFS doesn't really offer much of a difference on a single disk pfSense system.



```
pfSense Installer

Partitioning
How would you like to partition your disk?

  Auto (UFS)  Guided Disk Setup
  Manual      Manual Disk Setup (experts)
  Shell       Open a shell and partition by hand
  Auto (ZFS)  Guided Root-on-ZFS

          <  OK  >          <Cancel>
```

Figure 13. Selecting the filesystem type

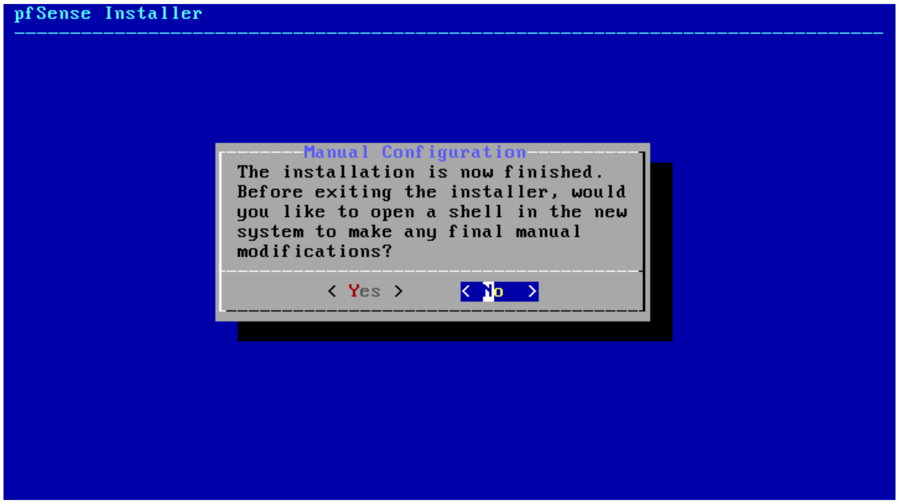
After selecting the filesystem type, pfSense will now install itself to the system disk.



```
pfSense Installer

Archive Extraction
Extracting distribution files...

base.txz...                              -

  Overall Progress:
           9%

    2127 files read @    1063.0 files/sec.
```

Figure 14. The installer installs with little issue

Lastly, for the installation you are asked about wanting to make any manual setup changes. For basic use just hit ‘NO’, and the system will restart.

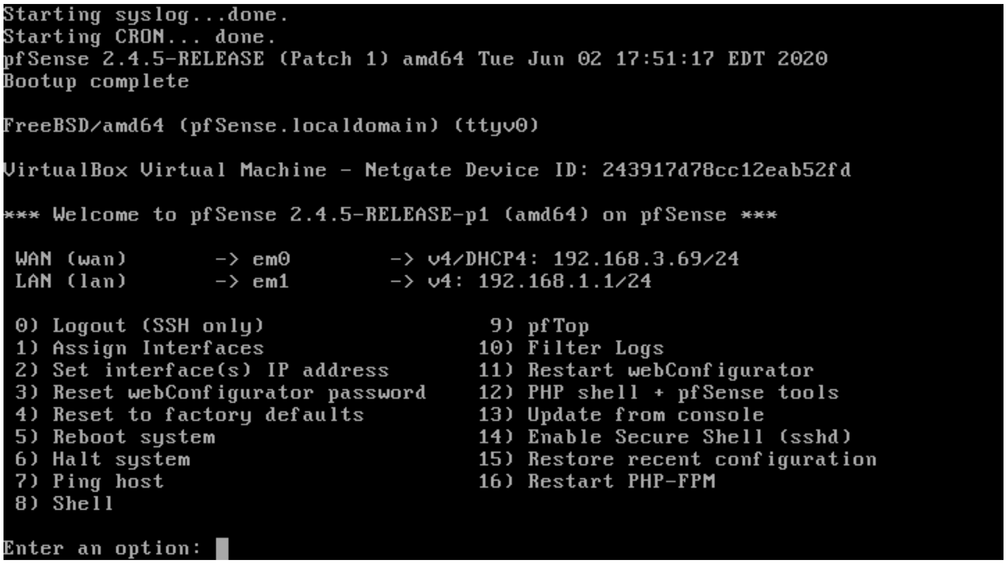


Manual Configuration

The installation is now finished. Before exiting the installer, would you like to open a shell in the new system to make any final manual modifications?

Figure 15. Exiting the installer

After restarting, you will be shown this screen. This is the console screen that allows for fine tuning of pfSense via the command line.

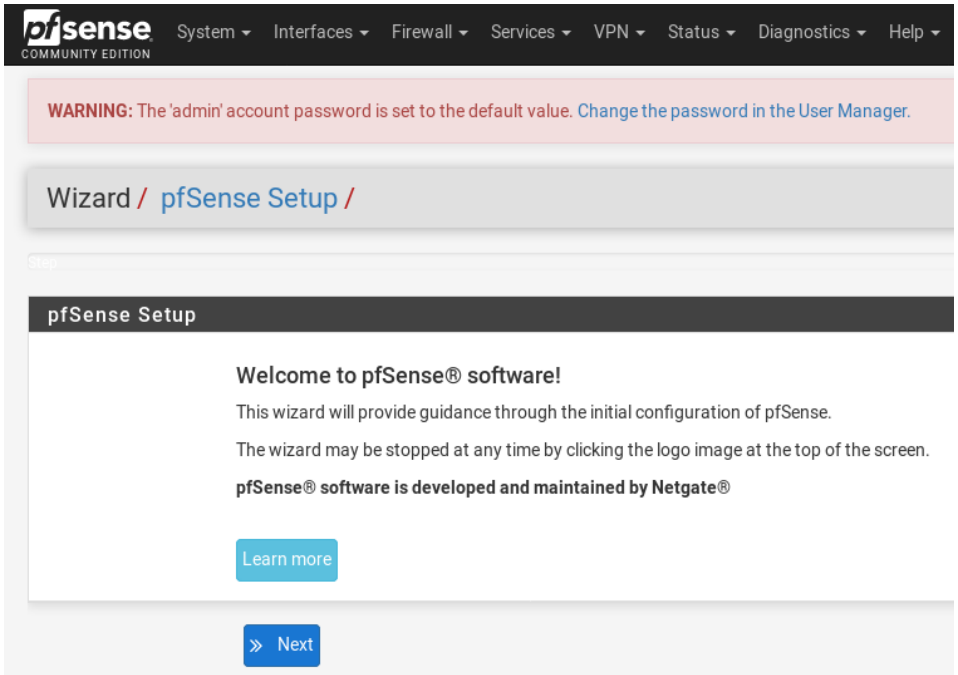


```
Starting syslog...done.
Starting CRON... done.
pfSense 2.4.5-RELEASE (Patch 1) amd64 Tue Jun 02 17:51:17 EDT 2020
Bootup complete

FreeBSD/amd64 (pfSense.localdomain) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: 243917d78cc12eab52fd

*** Welcome to pfSense 2.4.5-RELEASE-p1 (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4/DHCP4: 192.168.3.69/24
 LAN (lan)       -> em1        -> v4: 192.168.1.1/24

 0) Logout (SSH only)                   9) pfTop
 1) Assign Interfaces                  10) Filter Logs
 2) Set interface(s) IP address        11) Restart webConfigurator
 3) Reset webConfigurator password     12) PHP shell + pfSense tools
 4) Reset to factory defaults          13) Update from console
 5) Reboot system                      14) Enable Secure Shell (sshd)
 6) Halt system                        15) Restore recent configuration
 7) Ping host                          16) Restart PHP-FPM
 8) Shell

Enter an option:
```

Figure 16. The pfSense console view

For a basic setup, pay attention to which Ethernet port you have selected as your LAN network, as it currently is your only way to access the pfSense web console. From this console you can configure quite a few things including manually setting of interface IP addresses if they have not been set by DHCP.

Once you've gone to the IP of the LAN network that pfSense has started, you are greeted with the startup wizard for pfSense. Click ‘next’ to get started.



WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Wizard / pfSense Setup /

pfSense Setup

Welcome to pfSense® software!

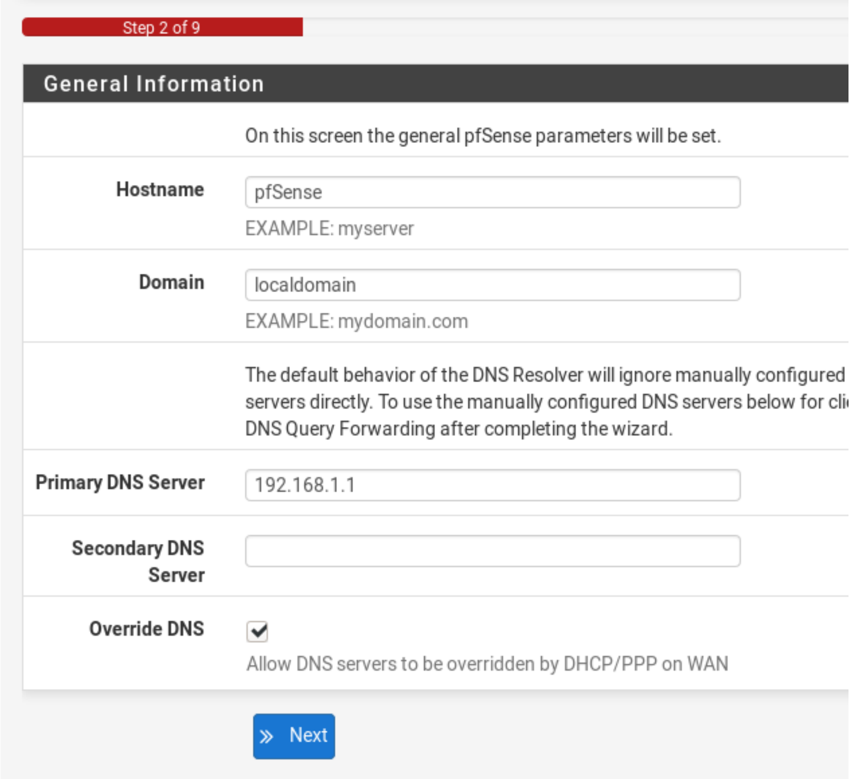
This wizard will provide guidance through the initial configuration of pfSense.

The wizard may be stopped at any time by clicking the logo image at the top of the screen.

pfSense® software is developed and maintained by Netgate®

Figure 17. Starting the pfSense wizard

Set your primary DNS to your preferred DNS server and click ‘next’



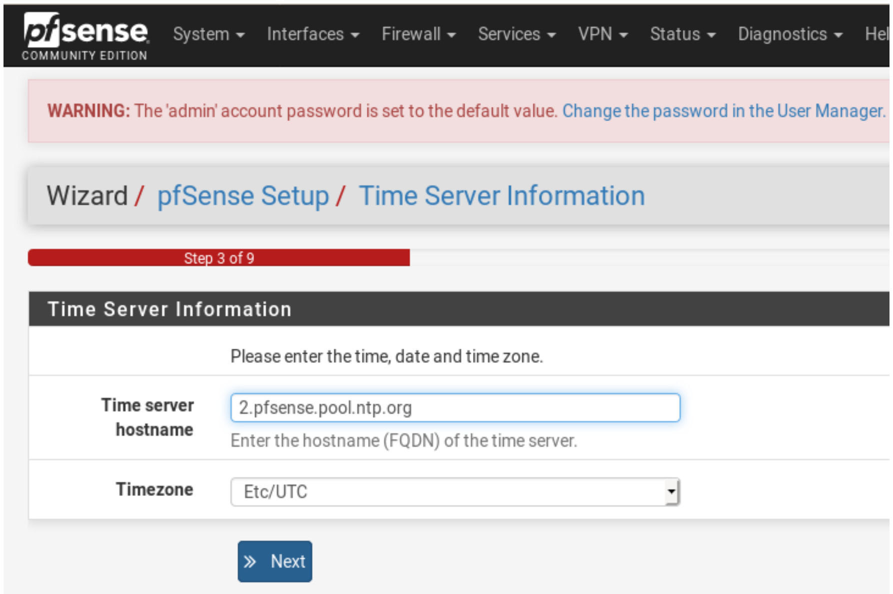
General Information

On this screen the general pfSense parameters will be set.

Hostname	pfSense EXAMPLE: myserver
Domain	localdomain EXAMPLE: mydomain.com
	The default behavior of the DNS Resolver will ignore manually configured servers directly. To use the manually configured DNS servers below for cli DNS Query Forwarding after completing the wizard.
Primary DNS Server	192.168.1.1
Secondary DNS Server	
Override DNS	☑ Allow DNS servers to be overridden by DHCP/PPP on WAN

Figure 18. Setting the DNS settings for pfSense

click ‘next’ unless you wish to change the time server



WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Wizard / pfSense Setup / Time Server Information

Step 3 of 9

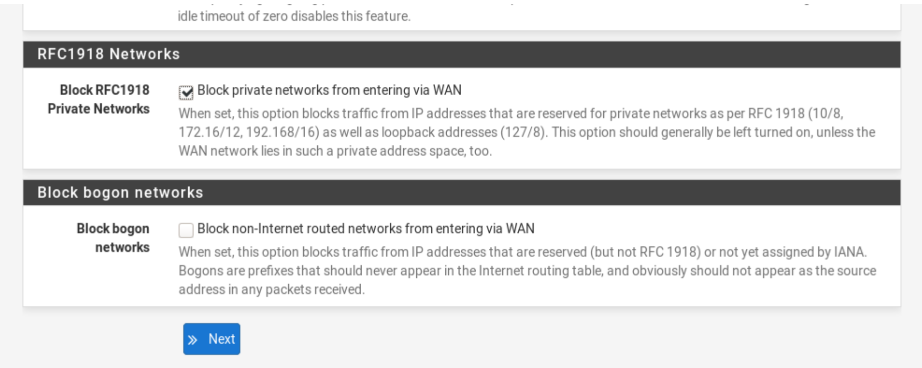
Time Server Information

Please enter the time, date and time zone.

Time server hostname	2.pfsense.pool.ntp.org Enter the hostname (FQDN) of the time server.
Timezone	Etc/UTC

Figure 19. Setting the time server

On the WAN configuration page, there is nothing to be changed, unless you are going to have pfSense behind a private IP address. If so, uncheck the blocking of RFC1918 and BOGON networks.



idle timeout of zero disables this feature.

RFC1918 Networks

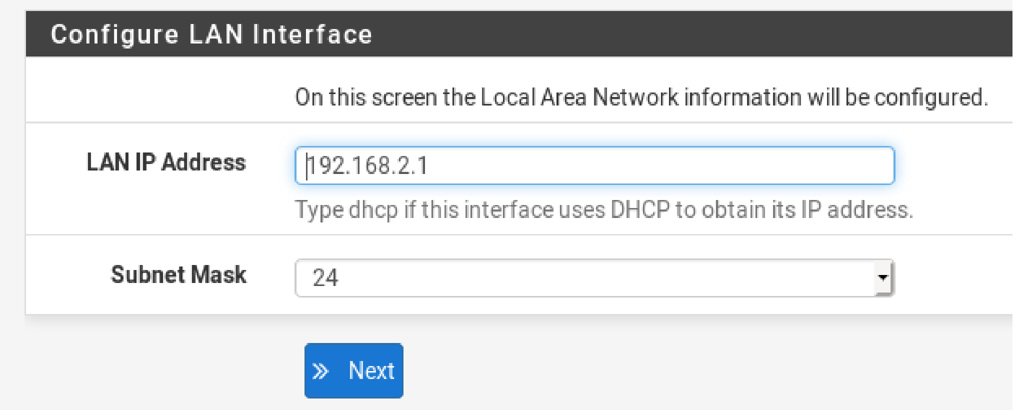
Block RFC1918 Private Networks	☑ Block private networks from entering via WAN When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). This option should generally be left turned on, unless the WAN network lies in such a private address space, too.

Block bogon networks

Block bogon networks	□ Block non-Internet routed networks from entering via WAN When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets received.

Figure 20. Allowing private range IP addresses

Then you configure your LAN interface.



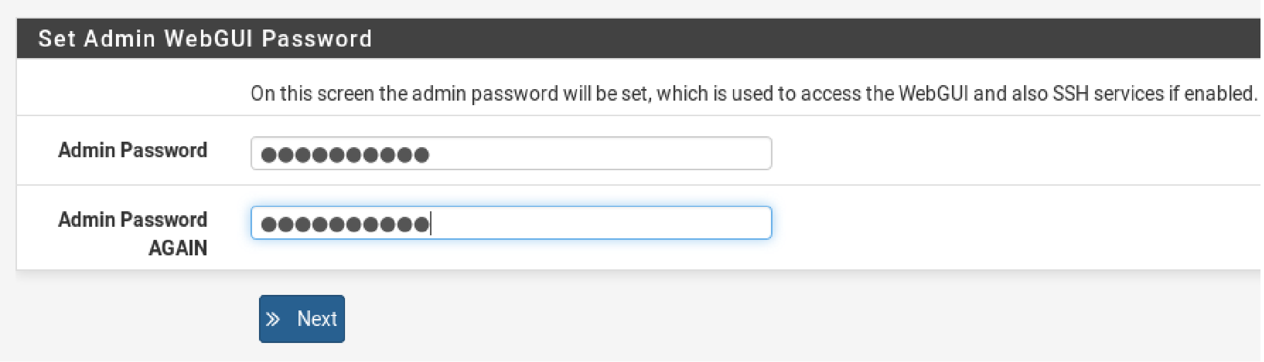
Configure LAN Interface

On this screen the Local Area Network information will be configured.

LAN IP Address	192.168.2.1 Type dhcp if this interface uses DHCP to obtain its IP address.
Subnet Mask	24

Figure 21. Configuring the LAN interface

Set the password for accessing the pfSense web interface



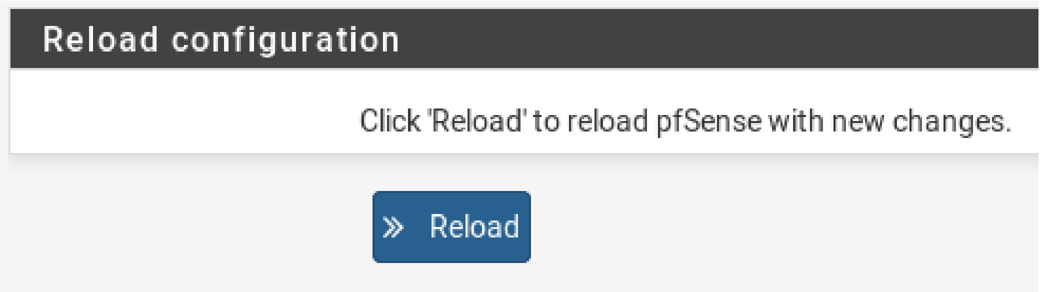
Set Admin WebGUI Password

On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled.

Admin Password	●●●●●●●●●●●
Admin Password AGAIN	●●●●●●●●●●●

Figure 22. Setting the Admin password for the web interface

And finally click ‘Reload’ to finish the wizard setup and reboot pfSense.

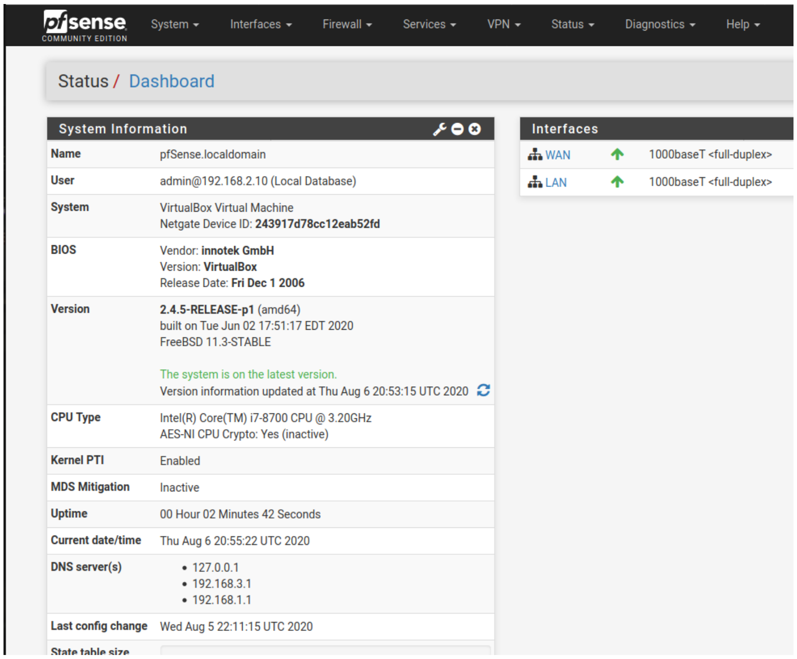


Reload configuration

Click 'Reload' to reload pfSense with new changes.

Figure 23. Reloading the configuration

After pfSense reboots, you are greeted with the basic install screen of pfSense. Congratulations your new firewall is ready to be setup with rules!!



Status / Dashboard

System Information

Name	pfSense.localdomain
User	admin@192.168.2.10 (Local Database)
System	VirtualBox Virtual Machine Netgate Device ID: **243917d78cc12eab52fd**
BIOS	Vendor: **innotek GmbH** Version: **VirtualBox** Release Date: **Fri Dec 1 2006**
Version	**2.4.5-RELEASE-p1** (amd64) built on Tue Jun 02 17:51:17 EDT 2020 FreeBSD 11.3-STABLE The system is on the latest version. Version information updated at Thu Aug 6 20:53:15 UTC 2020
CPU Type	Intel(R) Core(TM) i7-8700 CPU @ 3.20GHz AES-NI CPU Crypto: Yes (inactive)
Kernel PTI	Enabled
MDS Mitigation	Inactive
Uptime	00 Hour 02 Minutes 42 Seconds
Current date/time	Thu Aug 6 20:55:22 UTC 2020
DNS server(s)	• 127.0.0.1 • 192.168.3.1 • 192.168.1.1
Last config change	Wed Aug 5 22:11:15 UTC 2020
State table size	

Interfaces

WAN	↑	1000baseT <full-duplex>
LAN	↑	1000baseT <full-duplex>

Figure 24. The default status screen of pfSense

Firewall Rules

A PfSense out of the box feature is the firewall rules. The following will be for basic setup of routing all traffic from WAN to LAN interfaces.

First, you will need to navigate to the WAN rules page under Firewall > Rules > WAN.

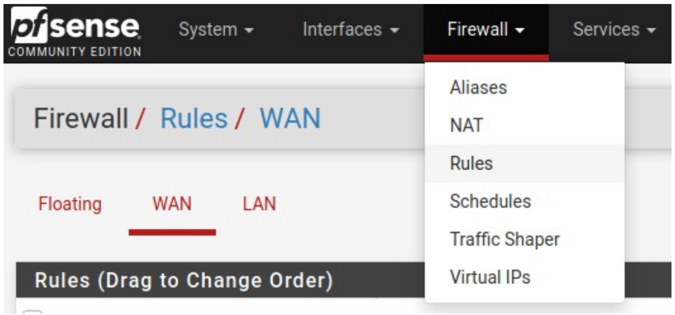
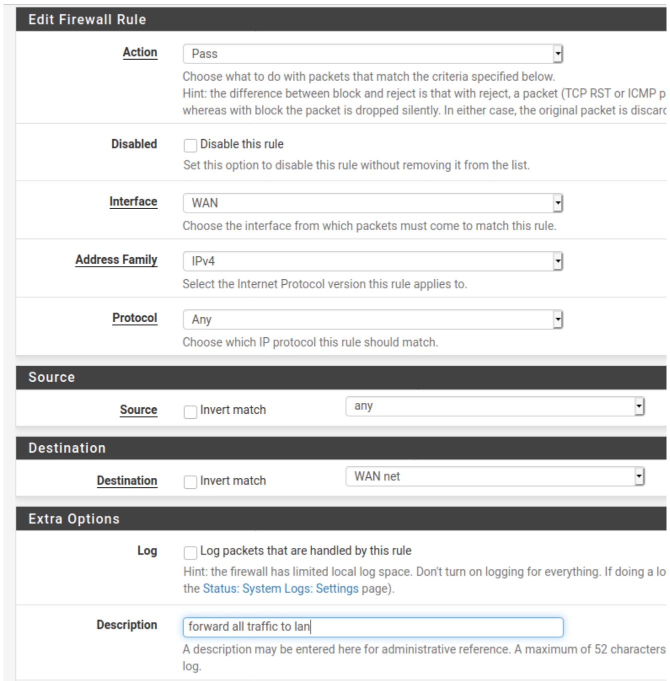


Figure 25. Navigating to the firewall rules

Then create a new rule on the WAN interface by clicking the ’↥ add’ button to create a new rule. Then you be taken to a ‘new rule’ page where you can configure a new rule. The following configuration below allows for all traffic to be routed from the WAN interface to the LAN interface and vice versa.



Edit Firewall Rule

Action: Pass
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP p
whereas with block the packet is dropped silently. In either case, the original packet is discarc

Disabled: □ Disable this rule
Set this option to disable this rule without removing it from the list.

Interface: WAN
Choose the interface from which packets must come to match this rule.

Address Family: IPv4
Select the Internet Protocol version this rule applies to.

Protocol: Any
Choose which IP protocol this rule should match.

Source

Source: □ Invert match any

Destination

Destination: □ Invert match WAN net

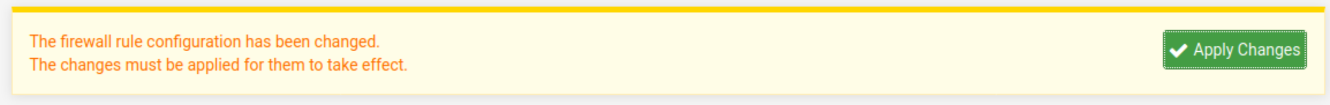
Extra Options

Log: □ Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lo
the Status: System Logs: Settings page).

Description: forward all traffic to lan
A description may be entered here for administrative reference. A maximum of 52 characters
log.

Figure 26. Creating rules for interfaces

Once done creating your rule, click ‘save’ at the bottom of the page and then click ‘apply changes’ to apply your newly created rule to your interface.



The firewall rule configuration has been changed.
The changes must be applied for them to take effect.

Figure 27. Applying changes to rules

VLANs

As previously mentioned with VLANs, you can create virtual LAN networks that allow you to create separate network segments that operate independently of each other.

To start with, navigate to Interfaces > Assignments > VLANs, then click the '+ Add' button to create a new VLAN.

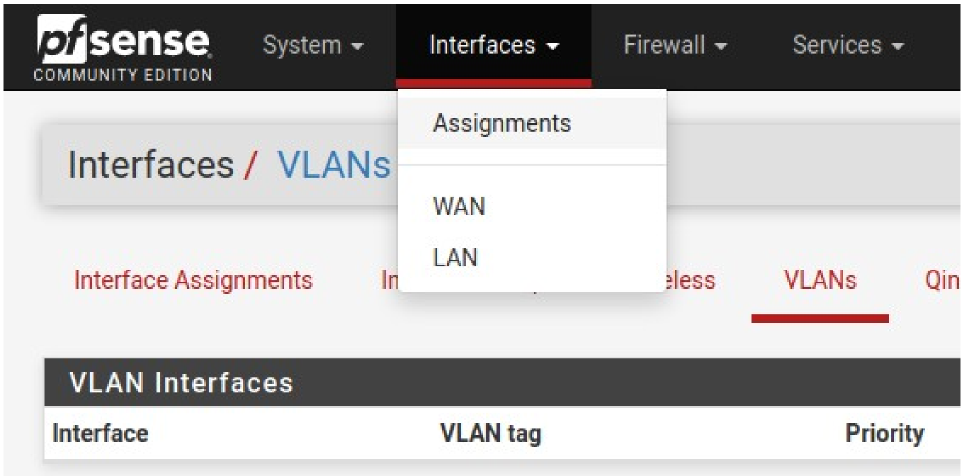
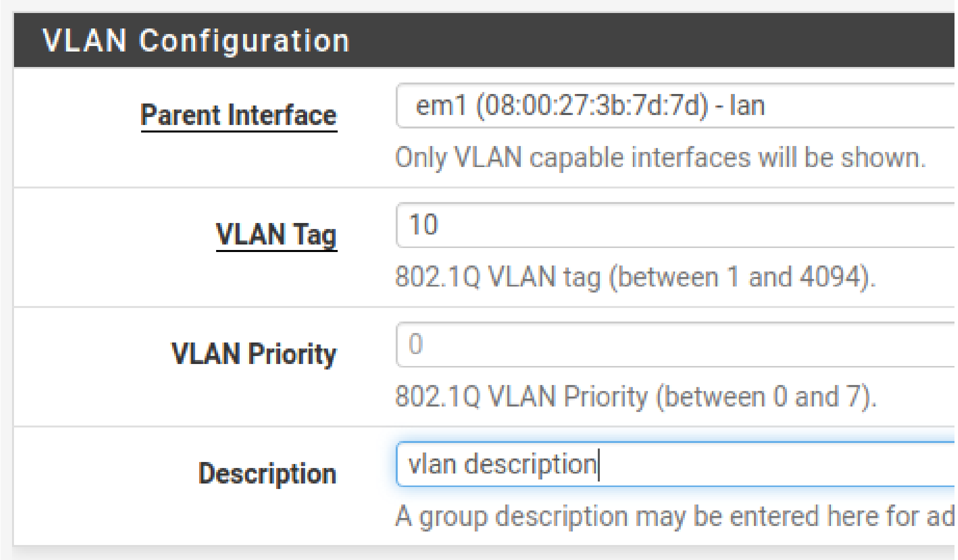


Figure 28. Navigating to VLAN creation

From the VLAN configuration page, we change define what the interface is that the VLAN will be using as well as the VLANs tag and description.



VLAN Configuration

Parent Interface	em1 (08:00:27:3b:7d:7d) - lan Only VLAN capable interfaces will be shown.
VLAN Tag	10 802.1Q VLAN tag (between 1 and 4094).
VLAN Priority	0 802.1Q VLAN Priority (between 0 and 7).
Description	vlan description A group description may be entered here for ad

Figure 29. Creating a VLAN

To finalize the configuration, hit 'save' and now you have a new VLAN to use on your network.

Section 6: IoT

What is IoT?

IoT or internet of things is the term used for any small non-personal computer device that can connect to your network either wired or wirelessly. Today, most of these devices can be a range of things like refrigerators, light switches, smart tv’s, etc. The majority of these have minimal security in place and can become a pivot point or entry point for an attacker to enter your network. A way to combat this is to have all of your IoT devices on the same VLAN with its own rules blocking the majority of unused ports to prevent the creation of connections outbound to the internet. Doing so will not only help mitigate security risks but also help you track the worst offenders for suspicious traffic on that VLAN.

Summary

Originally, household networks were primarily comprised of cable tv and maybe a couple of laptops using WiFi. People have been adding more and more onto their networks and ‘lag’ has become a household word. When COVID happened, families were thrust into depending upon their networks heavily with a high volume of traffic. This scenario will not go away even if COVID does. People have realized that they ‘can’ work from home if they have the right tools. People are no longer looking to buy ‘open floor plan’ homes, but rather homes that have individual rooms that can be used for video conferencing. College students can live at home and take courses online. All this leads to one necessity and that is a secure and robust household network.