## Contents

GitHub: isiah-emmanuel
Email: techisiahtto@gmail.com
CompTIA career ID: COMP001021724464 (CompTIA Linux+ xk0 – 004 Linux Administrator)
Contact: 1868 380-2647

Follow this link to obtain some scripts that will do some of the configurations for you: https://github.com/isiah-emmanuel/emmanuel-linux-open-source-environment-2020

# Guide to setting up an open source Environment / low resource client server environment

This environment provides the following:

1. Firewall
2. Content filtering
3. Secure VPN access
4. Remote access and control to all network clients
5. Print server and management
6. DHCP services
7. DNS services

plus additional applications can be integrated on request

## Choosing server version:

You can choose to run a headless server; however, I advise that you download an Ubuntu server image with a GUI. The server image of choice if different from Ubuntu should be a systemd system. I strongly recommend the use of Ubuntu 16.04 upward. From my testing with the environment I implemented at the Carenage ICT Access Centre, Ubuntu 18.04 was the most stable.

If you download a server image it does not have a GUI by default, run the following command to install a GUI: `sudo apt-get install Ubuntu-desktop`

## Creating bootable device and configuring file system correctly

- https://releases.ubuntu.com/18.04/ the following link will take you to the official Ubuntu release page where you can download an .iso for Ubuntu 18.04 LTS (long term support).
- After downloading the image, insert an empty flash drive with a minimum of 8gbs of space.
- https://rufus.ie/ this link will direct you to the Rufus site which is a program best suiting for making Linux bootable images.
- After installing Rufus open the application, locate and select the image you just downloaded, select the correct USB device connected to your machine and hit start, when the process is complete, the status field of Rufus will say ready.

At this point you are ready to install the image on the server.

## Installing software

- Insert USB into the server appliance
- Access the boot menu and choose to boot from USB
- The Ubuntu wizard will begin, and walk you through the installation process, read and follow carefully.
- Upon reaching the file system section, you can adjust the settings based on what level of security you want etc. and also based on how you want to divide the available resources. The default should work fine.

## Post installation configuration

- Give your server a static IP address:
  depending on the image you have installed, this command may produce different results:

  ```
  sudo apt-get install netman/network-manager
  ```

  if network manager is not installed the command will prompt you with a yes or no question asking you if you want to install the application, if it is already installed you will not be prompted, and you should proceed to run the following:

  ```
  sudo vim /etc/network/interfaces
  ```

  **results will look similar to this:-**

  ```
  # This file describes the network interfaces available on your system
  # and how to activate them. For more information, see interfaces(5).

  # The loopback network interface
  auto lo
  iface lo inet loopback

  # The primary network interface
  auto eth0
  iface eth0 inet dhcp
  ```

  **the "#" means that the following line is commented out, we need to edit the last 2 lines.**

  **hit 'i' to enter insert mode on the vim editor**

  The settings you will use is directly dependant on your own network environment here is an example:

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
#auto eth0
#iface eth0 inet dhcp
auto eth0
iface eth0 inet static
        address 192.168.1.2
        netmask 255.255.255.0
        network 192.168.1.0
        broadcast 192.168.1.255
        gateway 192.168.1.1
        dns-nameservers 192.168.1.3
        dns-search home
```

when you are done editing the file, hit [esc] :wq and hit enter, this will write the changes and quit.

Install LTSP:

this step can be bypassed if you are aiming strictly for a client-server environment where the client machines are not Thin Clients.[working with minor bugs]

1. **sudo apt-get install ltsp-server-standalone**

**Edit the dhcpd.conf file to suit your environment**

2. **sudo vim /etc/ltsp/dhcpd.conf**

**this file is very important for getting the clients to boot from the server as a thin client, if complications are met, do contact me via email for assistance/ consulting.**

```
# Default LTSP dhcpd.conf config file.
#

authoritative;

subnet 192.168.0.0 netmask 255.255.255.0 {
       range 192.168.0.20 192.168.0.250;
       option domain-name "example.com";
       option domain-name-servers 192.168.0.1;
       option broadcast-address 192.168.0.255;
       option routers 192.168.0.1;
#      next-server 192.168.0.1;
#      get-lease-hostnames true;
       option subnet-mask 255.255.255.0;
       option root-path "/opt/ltsp/i386";
       if substring( option vendor-class-identifier, 0, 9 ) = "PXEClient"
{
              filename "/ltsp/i386/pxelinux.0";
       } else {
              filename "/ltsp/i386/nbi.img";
       }
}
```

above, you should edit the highlighted text to suit your current network configurations.

when you are done editing the file, hit [esc]: wq and hit enter, this will write the changes and quit.

### Restart the DHCP server on the host

**sudo /etc/init.d/dhcp3-server restart or sudo systemctl restart dhcpd**

### Build the LTSP environment and the client image(optional)

**sudo ltsp-build-client --arch i386 the build can vary based on the hardware you possess most modern hardware use x64, however, you can leave it as default as the highlighted build is the most stable and tested to be working well at the Carenage Centre.**

## Boot the client via the network(optional)

At this point you can connect to a client device and set in the bios the client to boot via the network, the client, once connected to the server, should pull an IP address. Once the client is fully booted, you can sign in with an account created on the server. This will not install an OS on the client and the majority of processing will be done on the server, the server will also have full control of all connected clients.

# Important changes and environment optimization [stable 100% uptime]

There is a bit of a downside of booting over the network, that being bandwidth, which directly affects boot time, I strongly recommend to proceed with the following. Once the server is configured correctly:

1. repeat the installation process with a client image on the client machines https://releases.ubuntu.com/20.04/
2. make the first account on the client machine an administrator
3. make another account on the same client device for regular users

   secondary accounts can be created using the GUI or through the command line using the command [ useradd –m {username}]

   then set the password using the command: [passwd username]

## configure server to control laptops and micro PCs

```
on the server run the following commands:

apt-get install --install-recommends epoptes

gpasswd -a username epoptes
```

## configure all client machines to be monitored and controlled by server

```
apt-get install --install-recommends epoptes-client

by default, the application will try to connect to the server via DNS, in order for this
connection to be made you must run these commands:

sudo vim /etc/hosts

hit ‘i’ to enter insert mode on the editor

then enter the line> 192.168.1.2 server
replacing the IP address with the IP of your server

once these configurations are done; run the following command: epoptes-client –c

these commands will successfully connect clients and server.
```

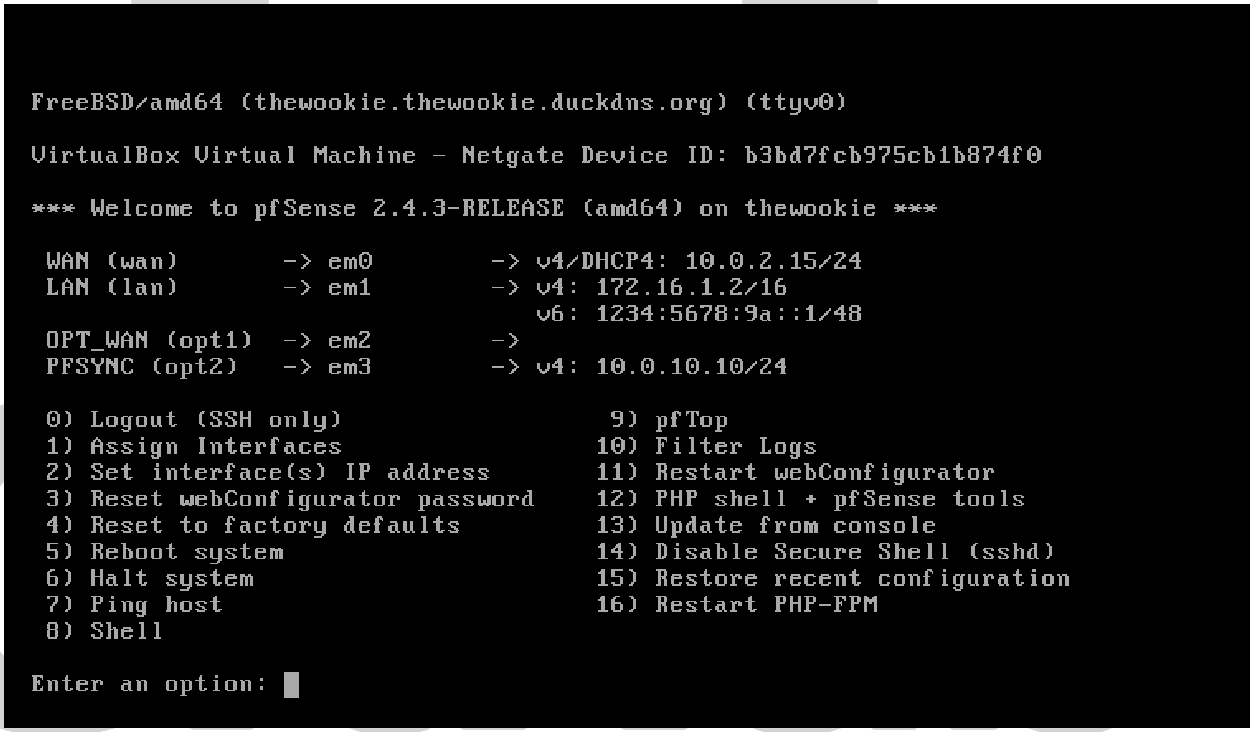
# Install and configure Pfsense Firewall Appliance, secure OpenVPN connection, and Content filtering [stable 100% uptime]

Download the Pfsense iso from the following link:
https://nyifiles.netgate.com/mirror/downloads/pfSense-CE-2.5.0-RELEASE-amd64.iso.gz

1. you will need to create another installation media with the following iso, following the same method as above where you created the server installation media. Enter the boot menu on the device and select boot from usb, follow through with the installation wizard adjusting settings accordingly.

   Pfsense is strictly command line interface, not to worry, it takes the form of a wizard type environment when its installed.

2. once the OS is properly installed on the hardware you may need to configure the interfaces for the LAN/WAN network, given that you may not have done so on the initial setup.

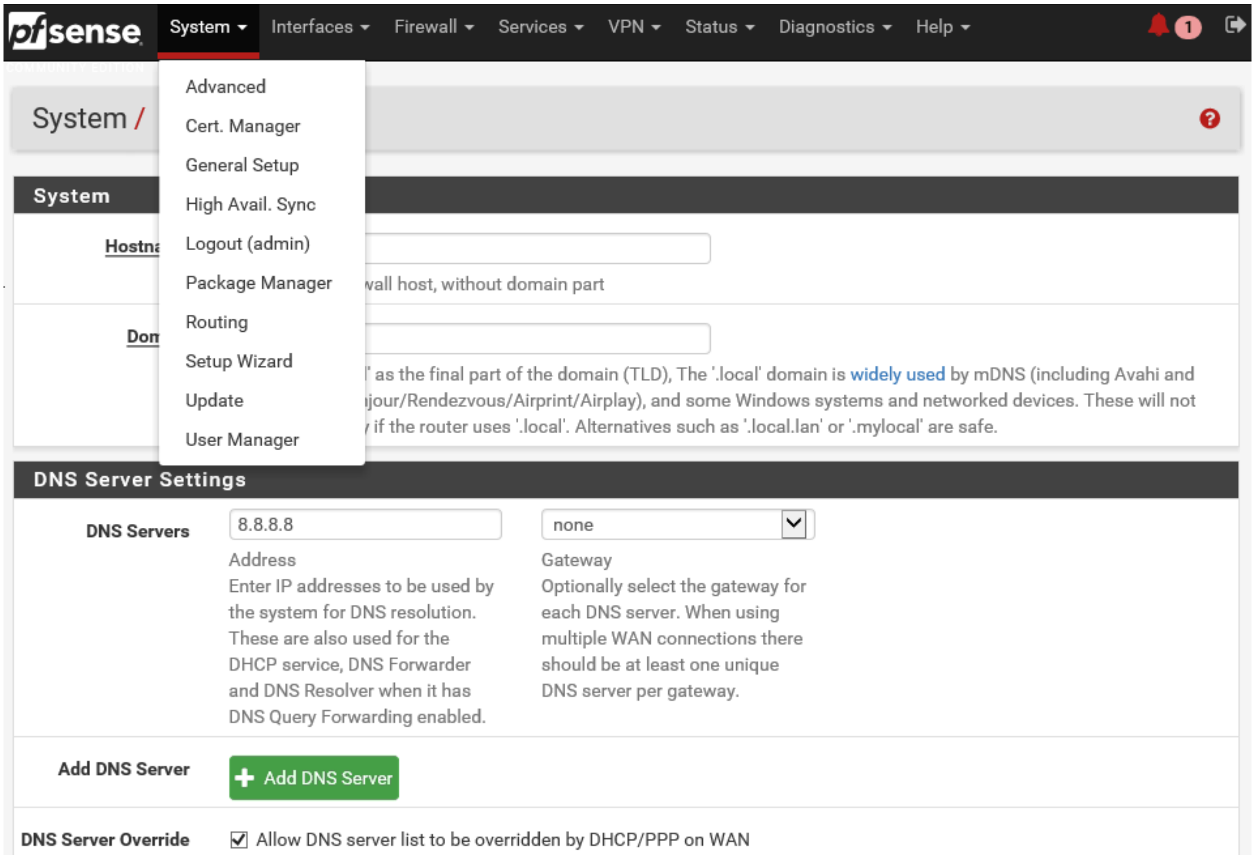


```
FreeBSD/amd64 (thewookie.thewookie.duckdns.org) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: b3bd7fcb975cb1b874f0

*** Welcome to pfSense 2.4.3-RELEASE (amd64) on thewookie ***

 WAN (wan)       -> em0        -> v4/DHCP4: 10.0.2.15/24
 LAN (lan)       -> em1        -> v4: 172.16.1.2/16
                                  v6: 1234:5678:9a::1/48
 OPT_WAN (opt1)  -> em2        ->
 PFSYNC (opt2)   -> em3        -> v4: 10.0.10.10/24

 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) Disable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option: 
```

this will be the interface you see while configuring the device. The only options we are concerned with at this point is option 1 and option 2.

3. Once you have configured both network interfaces on the device correctly, you will now be able to access the firewall from a much nicer, and user friendly interface, the configurations is directly dependent on how your Pfsense device if connected to the network, and well as IP addressing schemes.

4. You will now have a firewall device between the internet and the internal network, this device will run DHCP, DNS if required, Content filtering, and VPN. The VPN can be set up on this device or another device based on your preference.



wall host, without domain part

' as the final part of the domain (TLD), The '.local' domain is widely used by mDNS (including Avahi and jour/Rendezvous/Airprint/Airplay), and some Windows systems and networked devices. These will not if the router uses '.local'. Alternatives such as '.local.lan' or '.mylocal' are safe.

DNS Servers: 8.8.8.8 | none

Address
Enter IP addresses to be used by the system for DNS resolution. These are also used for the DHCP service, DNS Forwarder and DNS Resolver when it has DNS Query Forwarding enabled.

Gateway
Optionally select the gateway for each DNS server. When using multiple WAN connections there should be at least one unique DNS server per gateway.

DNS Server Override: ☑ Allow DNS server list to be overridden by DHCP/PPP on WAN

5. Squid and SquidGuard is the content filtering packages needed to control site access, they can be installed using the Pfsense package manager. To access the package manager, click on packages in the system menu. Select the available packages tab and scroll down until you find SquidGuard, then click the plus symbol next to the description to begin the installation. Once the installation is complete, you will have a new menu item under services called proxy filter.

## Enabling a Blacklist

To configure the blacklist feature, open the general settings page (Services \ Proxy Filter). Click on the checkbox to enable the blacklist feature.

find a list of several blacklists at http://www.squidguard.org/blacklists.html. Once you determine which blacklist you are going to use, enter the URL of the blacklist into the blacklist URL box on Pfsense.

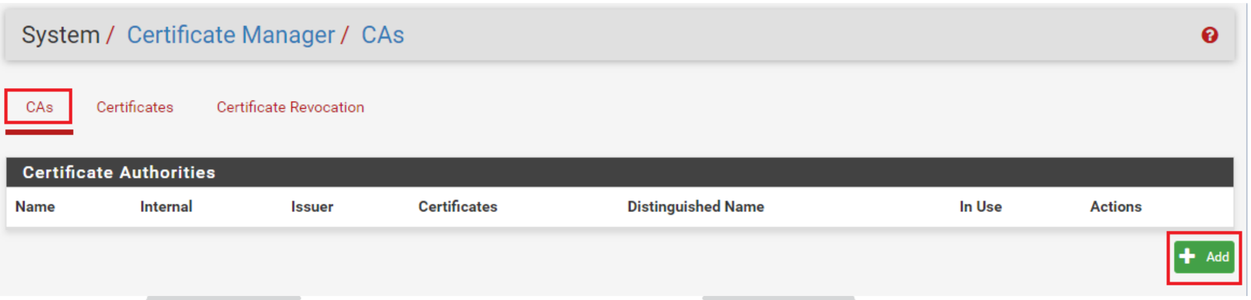
Click save, then click on the blacklist tab and click on download. It can take several minutes for the list to download and process. Once it is finished, it will display "Blacklist update complete" in the status box below.

At this point you will now have a blacklist enabled you will need to browse the different categories and select what you want to allow or den on your internal network.

Content filtering is a very broad subject area, here is a thread that should help you do more customization if you want it, https://turbofuture.com/internet/URL-Filtering-How-To-Configure-SquidGuard-in-pfSense

## VPN configuration

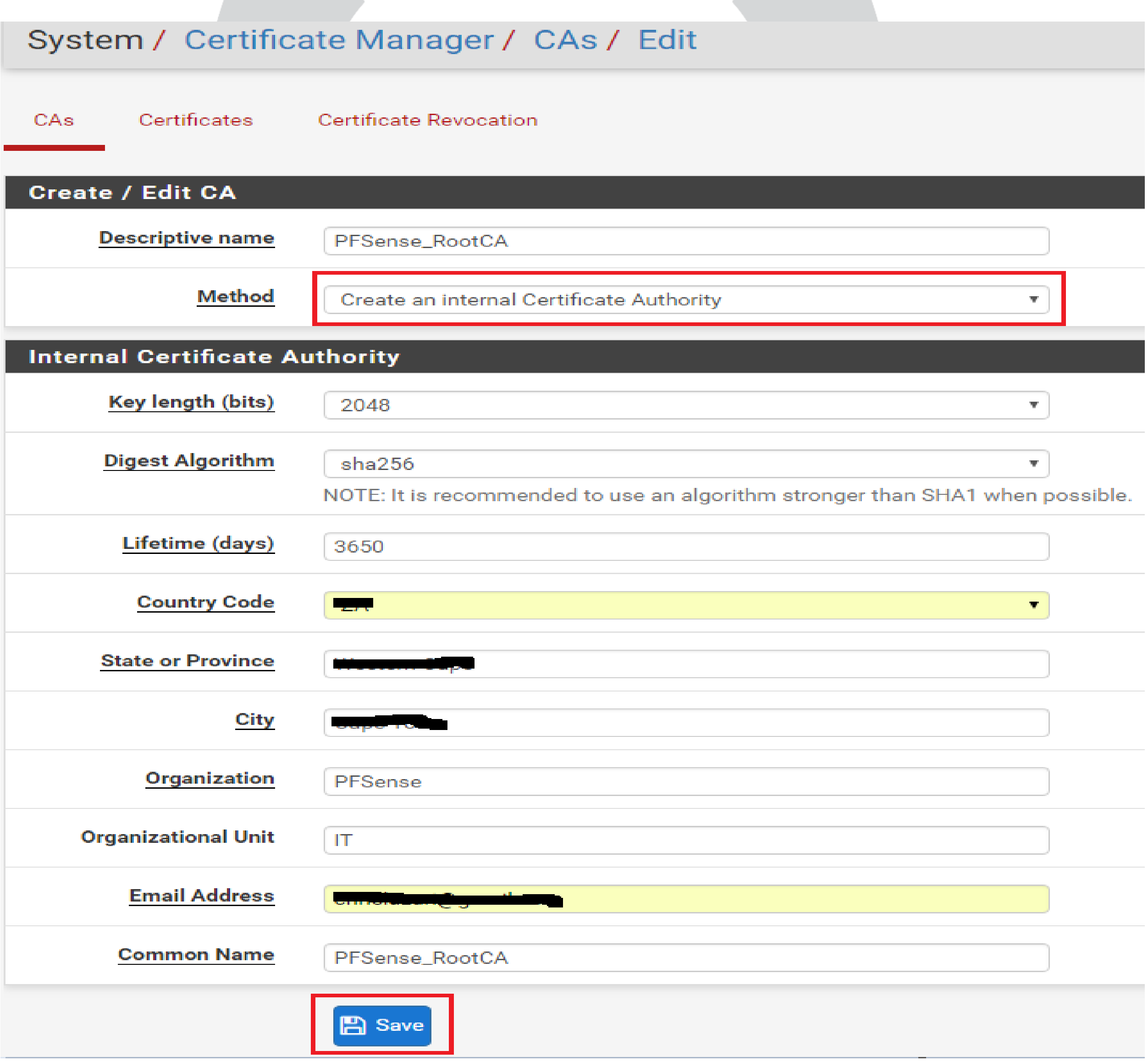
1. Again head into the package manager on Pfsense and search for OpenVPN and install it.
2. Next you will need to create a CA cert.



System / Certificate Manager / CAs

**Certificate Authorities**

| Name | Internal | Issuer | Certificates | Distinguished Name | In Use | Actions |
|---|---|---|---|---|---|---|



System / Certificate Manager / CAs / Edit

**Create / Edit CA**

| | |
|---|---|
| Descriptive name | PFSense_RootCA |
| Method | Create an internal Certificate Authority |

**Internal Certificate Authority**

| | |
|---|---|
| Key length (bits) | 2048 |
| Digest Algorithm | sha256<br>NOTE: It is recommended to use an algorithm stronger than SHA1 when possible. |
| Lifetime (days) | 3650 |
| Country Code | [redacted] |
| State or Province | [redacted] |
| City | [redacted] |
| Organization | PFSense |
| Organizational Unit | IT |
| Email Address | [redacted] |
| Common Name | PFSense_RootCA |

3. Head over to the VPN section, select OpenVPN, select the wizard and follow through adjusting the settings based on your existing network.

## Print server and Print management

1. On the server open the command line
2. Enter the command: sudo apt-get install cups –y
3. Enter the command: sudo systemctl start cups
4. Enter the command: sudo systemctl enable cups
5. You can now access the CUPS interface which is very user friendly on the server, by heading to a preferred browser and entering localhost:631
6. In this interface you can add printers and set up permissions etc.

The steps above will cover how the existing environment at the Carenage ICT Access center is currently set up where there is 100% up time and no report of any technical issues. For further assistance in configuring or setting up of network feel free to email.