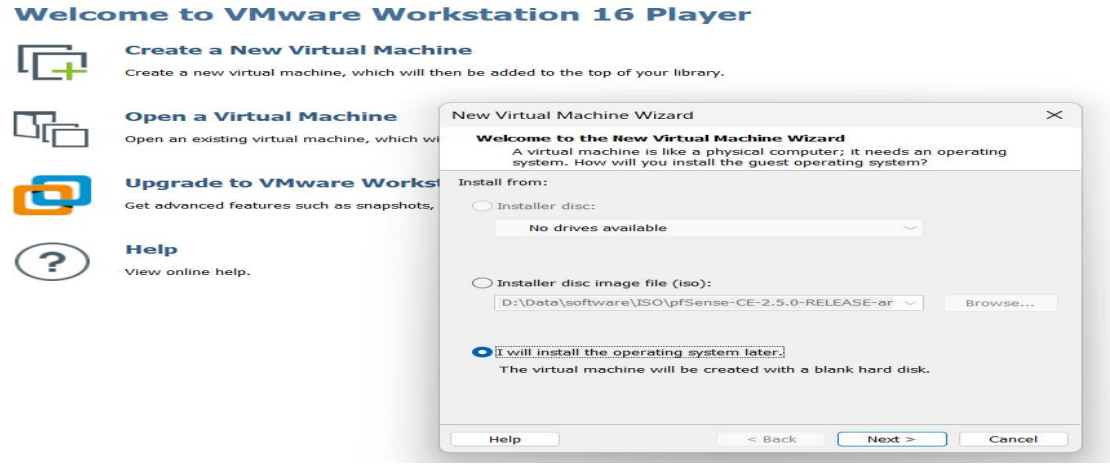
pfSense Firewall Installation and Configuration

This lab demonstrates installation of pfSense firewall. Installing Squid proxy on it. Then configuring Squidguard on it for URL filtering. Configuring user based access to internet.

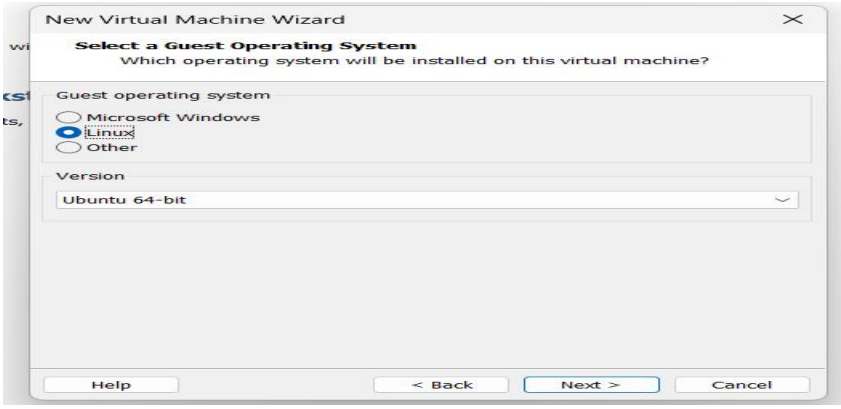
1. Creating a virtual machine in VMWare player and install pfSense.

Open VMWare player. Click Create a NEW Virtual Machine.

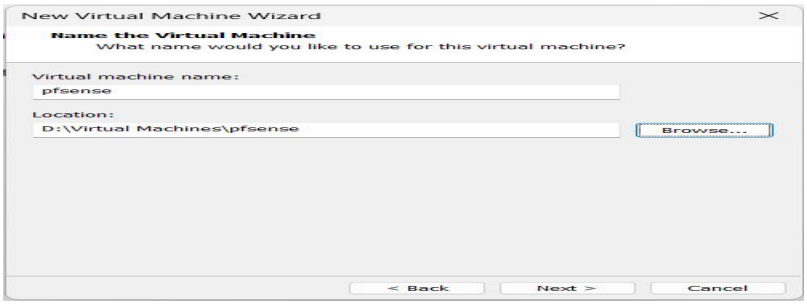


On the window that opens, select I will install the operating system later. Click Next.

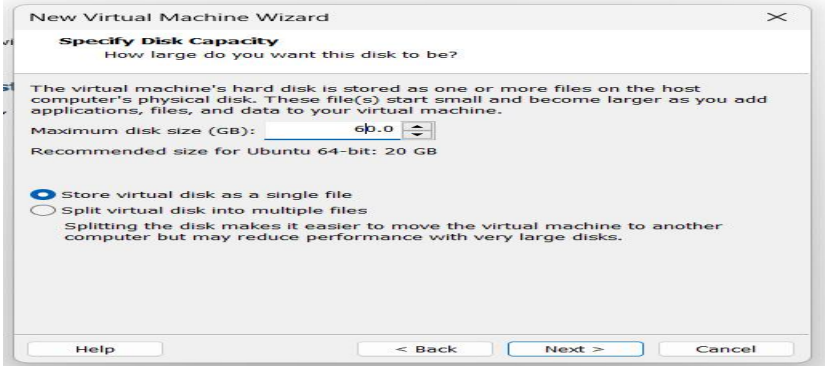
On the following window that opens, select **Linux** in the Guest Operating System. In the version select **Ubuntu 64 bit**. Click Next.



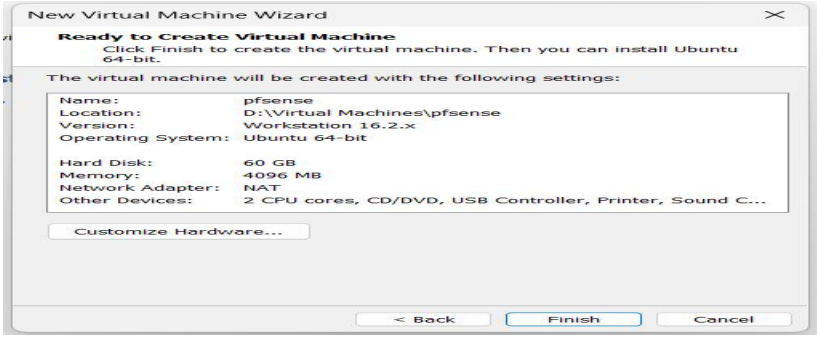
On the next window provide a name for the virtual machine. Also provide a path to store the virtual machine files.



Click Next.
On the following window specify the hard disk size as 60 GB. Also click store virtual disk as a single file. Click Next.



The next window displays the summary page. Check the configuration.

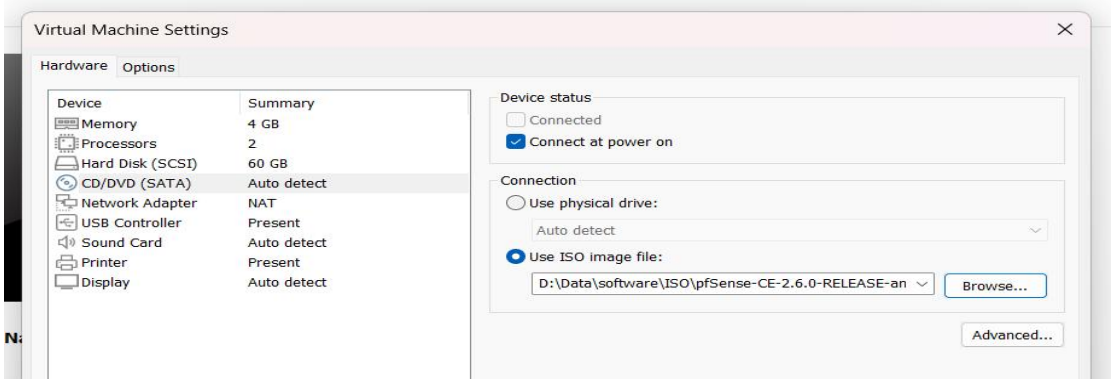


Click Finish to create the virtual machine. The virtual machine is shown as below.

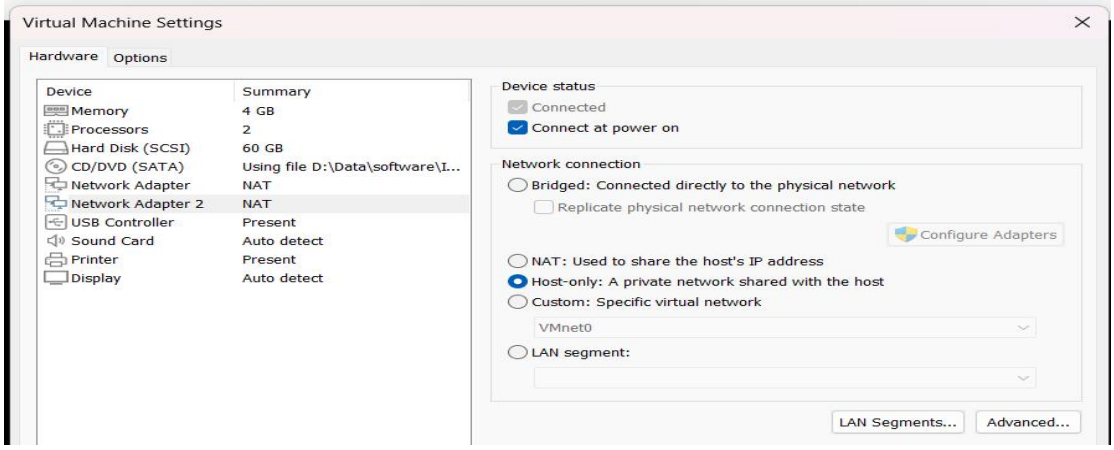
Select the machine and click **Edit virtual machine settings**. The option is displayed on the right side.

On the settings window that opens, click CD/DVD. Click **use ISO image file** option. Click Browse button and select the pfSense iso image downloaded from the pfSense web site.

This is shown in the following image.



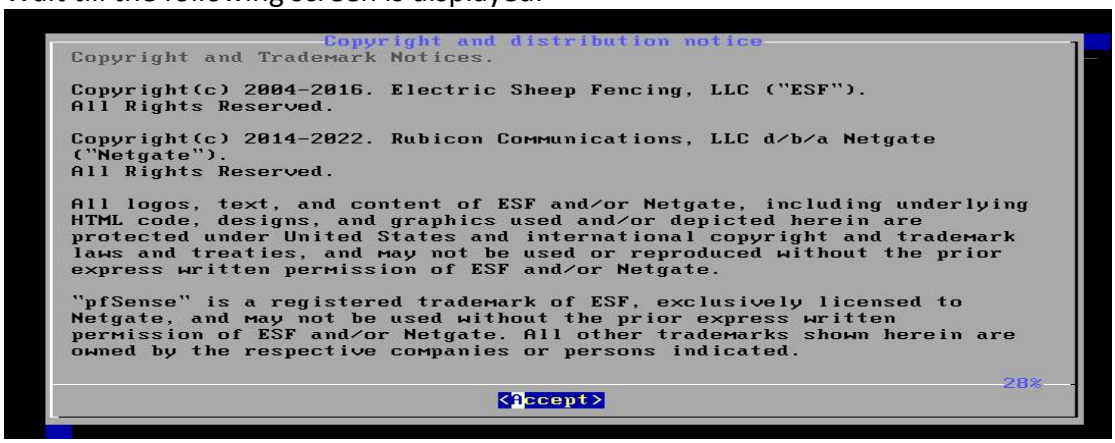
Then click Add button at the bottom. Select Network Adapter. This will add the second network adapter to the virtual machine.
pfSense requires 2 network cards. One is used as WAN adapter. This adapter is connected to the Internet. Second LAN adapter. It is connected to the internal network switch.
Thus keep the **first** network adapter in **NAT** mode. **Second** network adapter in **Host-only** mode. This is shown below.



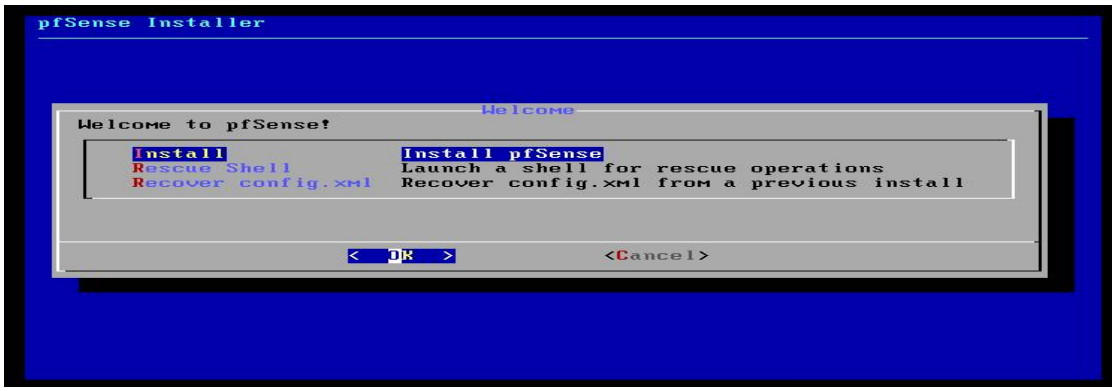
Click OK to close the settings window. Then Click the green arrow in the menu bar or click Play virtual machine option.

The Virtual machine will start and the pfSense installation begins.

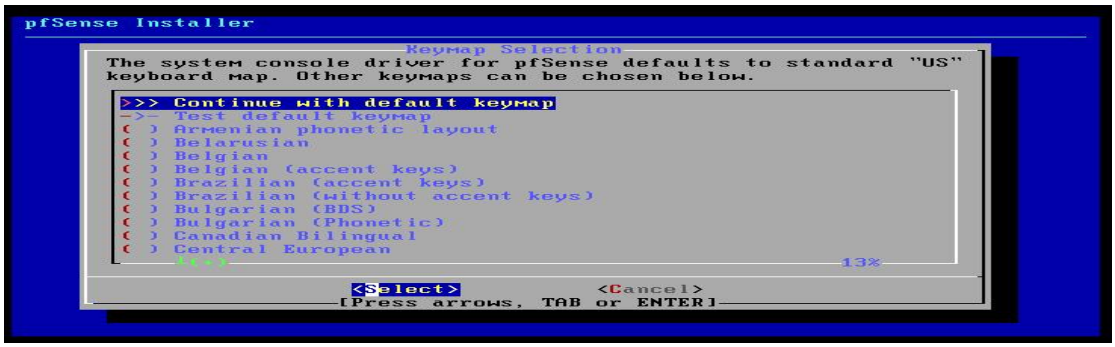
Wait till the following screen is displayed.



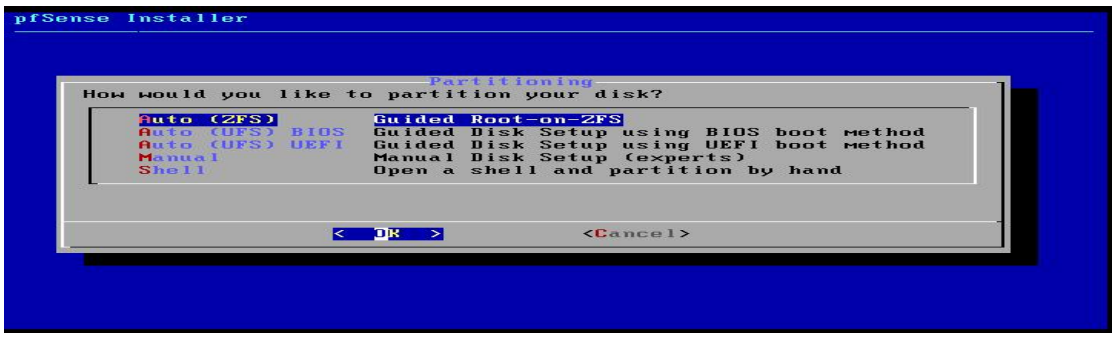
Press Enter to Accept to accept the Copyright and distribution notice.



Press Enter to select OK to install pfSense on the above screen.

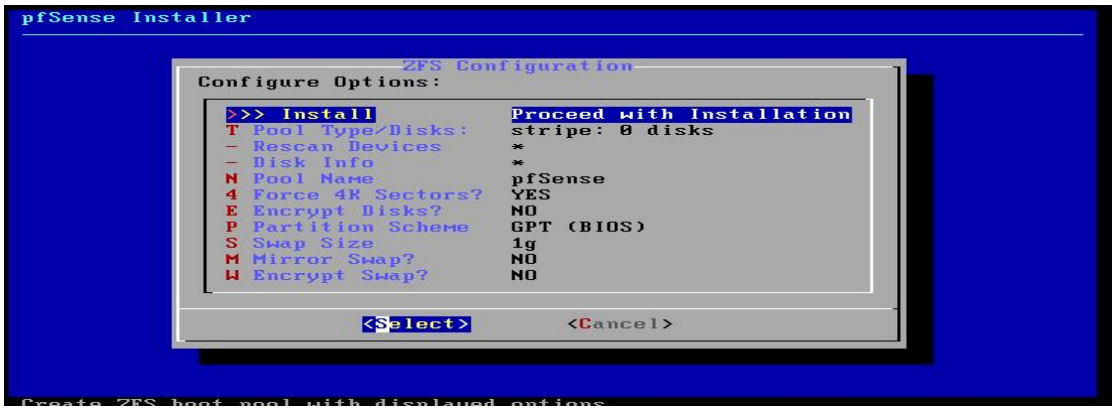


When the above screen is displayed, press Enter to select the Default Keymap.

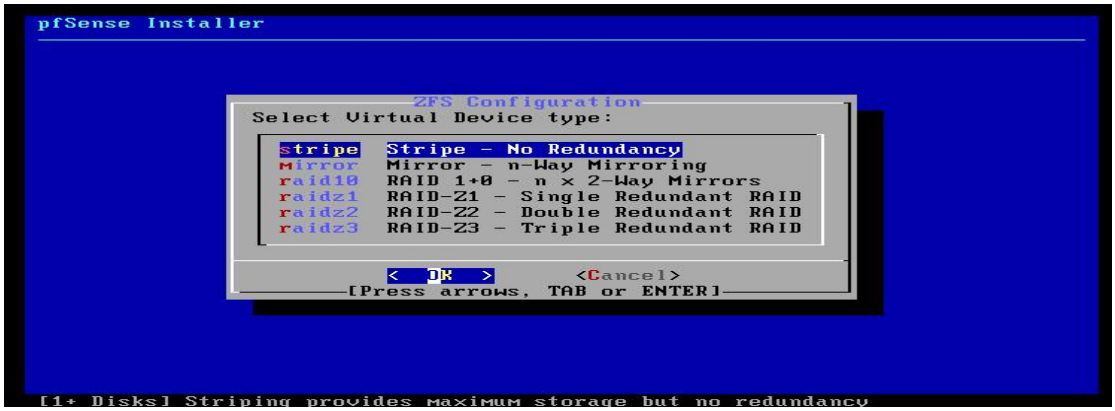


Press Enter to select OK to continue with the default option.

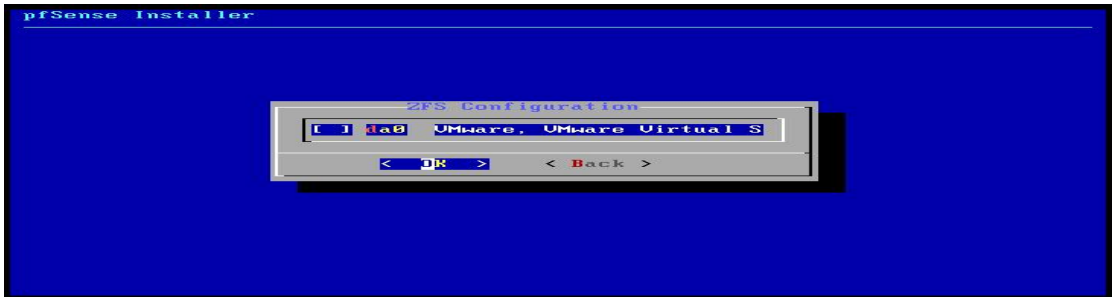
Press Enter on the following screen to proceed with the installation.



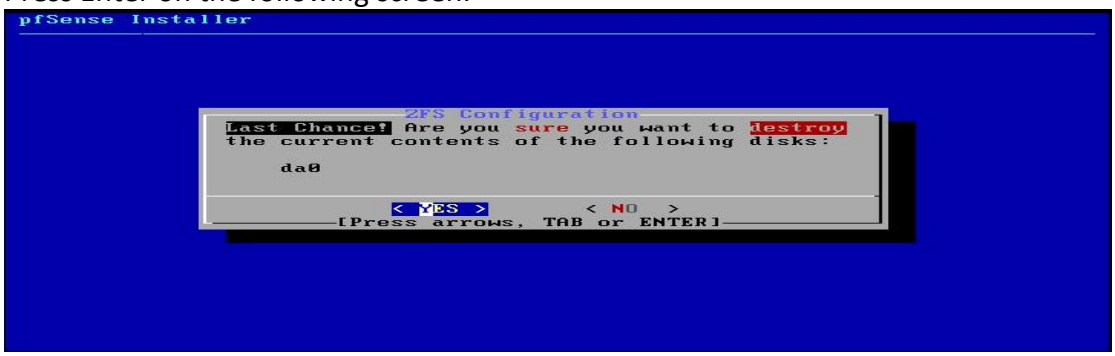
On the next screen again press Enter to continue with the default **stripe** option.



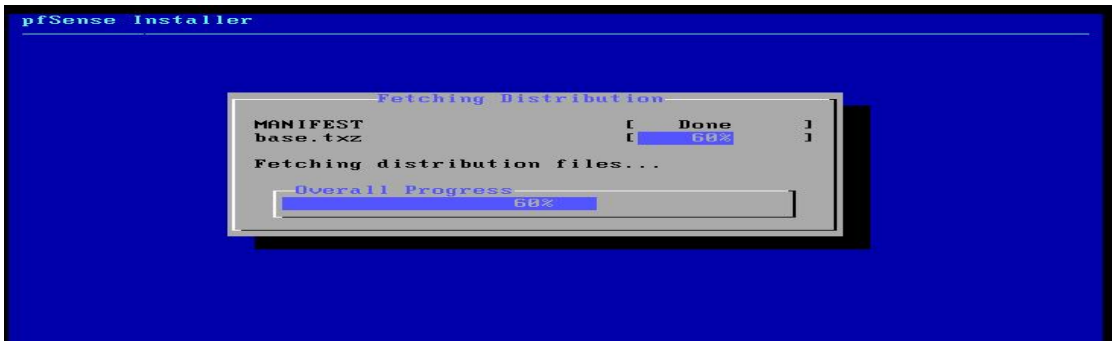
On the next screen displayed, press space bar to select the da0 square box. Then press Enter to continue.



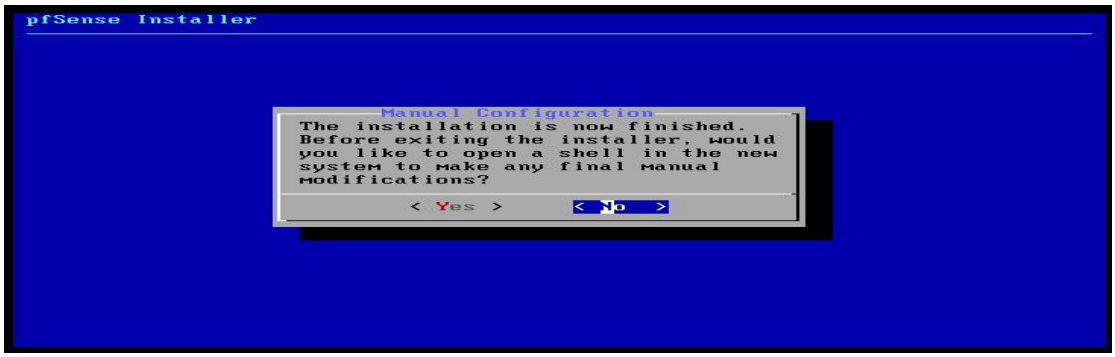
Press Enter on the following screen.



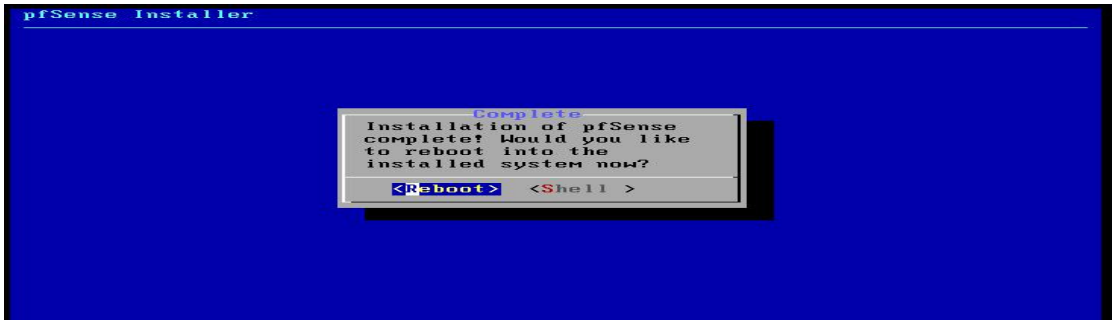
This will start the pfSense installation.



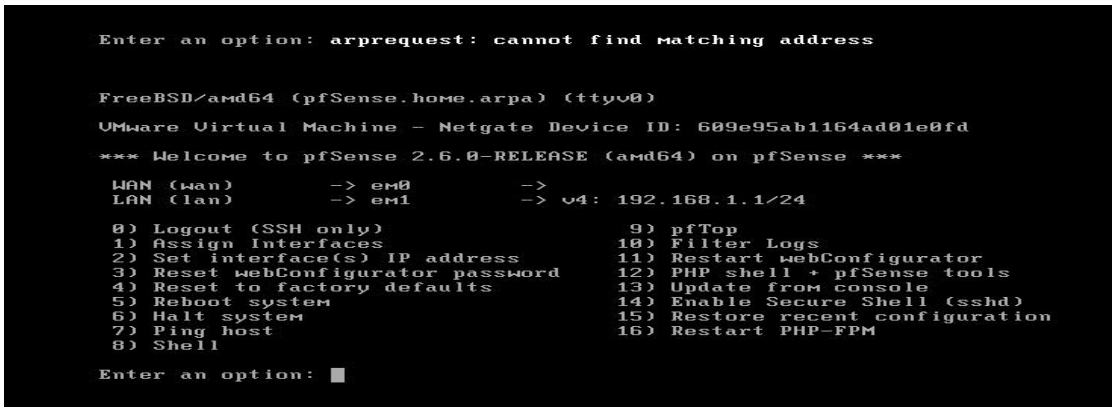
Once Installation is complete, following screen is displayed.



Press Enter to continue with the No option.



Press Enter to reboot the pfSense virtual machine. Once the pfSense starts following screen is displayed.



After installation pfSense by default assigns 192.168.1.1/24 IP address to the LAN interface. However we need to change it to match the vmnet1 adapter in our Windows.
First go to the main Windows. Open command prompt. Use ipconfig command and find out the IP address assigned to the VMnet1 adapter. This is as shown below.

```
Command Prompt

Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::5cef:595e:ffc4:c353%2
   IPv4 Address. . . . . . . . . . . : 192.168.148.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::be77:8cee:4286:145f%18
   IPv4 Address. . . . . . . . . . . : 192.168.65.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
```

We will assign a new IP address to the pfSense LAN adapter which is in the range of vMnet1 adapter.

```
 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: 2

Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 192.168.148.10

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24
```

On the pfSense console press 2 Set Interface(s) IP Address. As shown in the above image.
Select 2 again to change the LAN interface IP address.
Next Enter the IP address to be assigned to the LAN adapter. Make sure it is in the range of VMnet1 adapter. Here the IP address assigned is 192.168.148.10. But in your case the IP address may be different. Press Enter.

Next enter subnet mask as 24 and press enter.

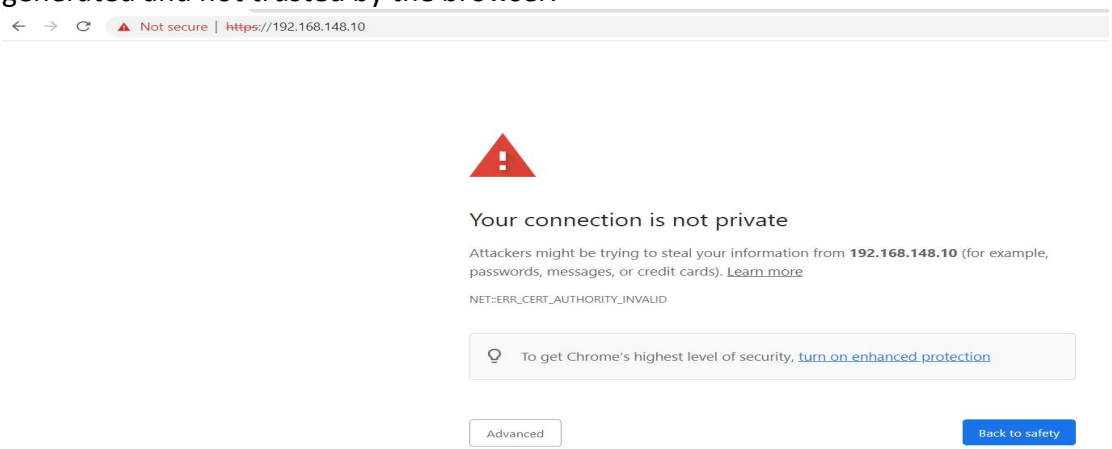
```
For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Enter the new LAN IPv6 address.  Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) n
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n
```

Then press Enter. Next type n as we do not want to start DHCP server on LAN network. However in production environment you may want to enable DHCP server.

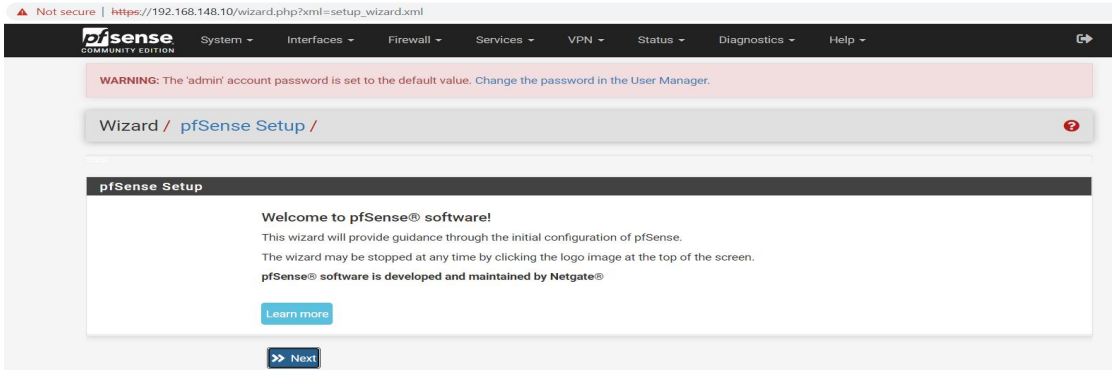
Type n on the next prompt. This will not revert the webConfigurator to HTTP. Thus we can access the pfSense web console using HTTPS.
Thus the LAN IP address is configured.

Now go to your second Virtual Machine (Either Windows or Linux) . Make sure the network adapter of this VM is in **host-only** mode.

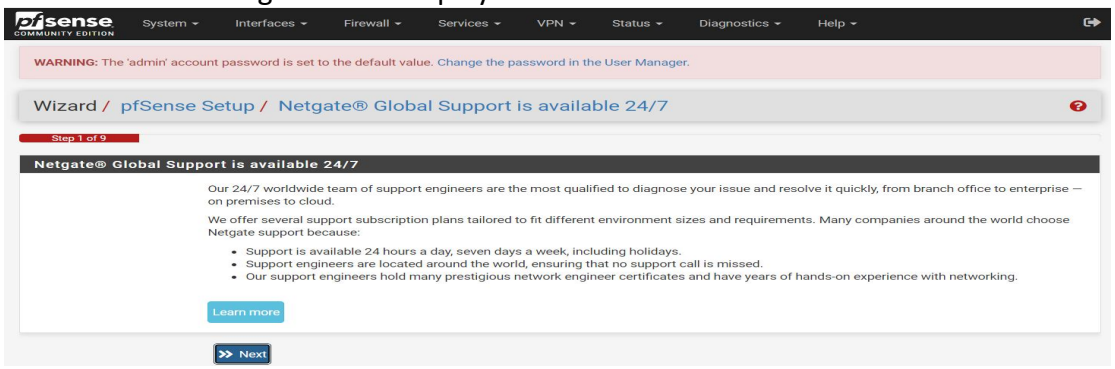
On this VM open the browser and type https://IP-of-pfSense-LAN . Following warning will be displayed. This is because the certificate issued by pfSense is self generated and not trusted by the browser.



Click Advanced and proceed to the website. On the Login page login with username as **admin** and password as **pfsense**.
The pfSense initial setup will start as shown below.

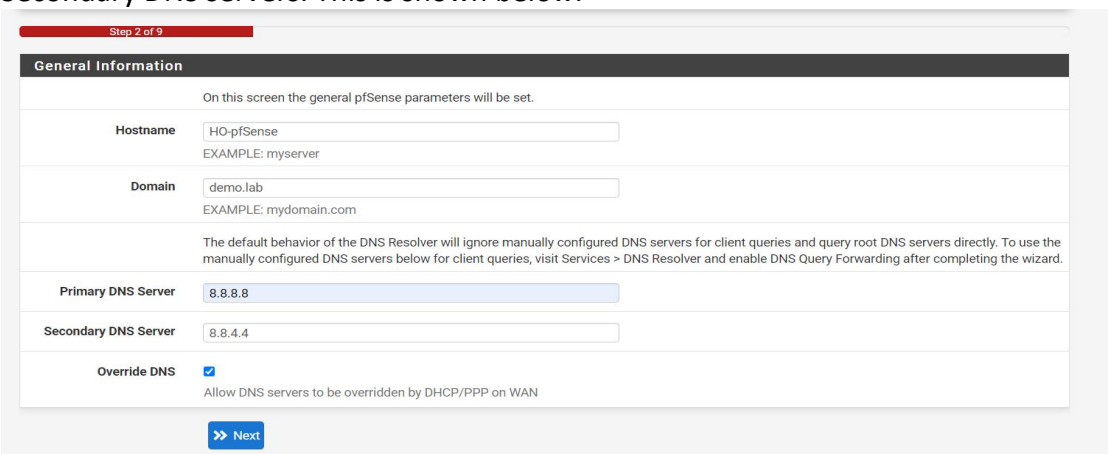


Click Next. Following screen is displayed.

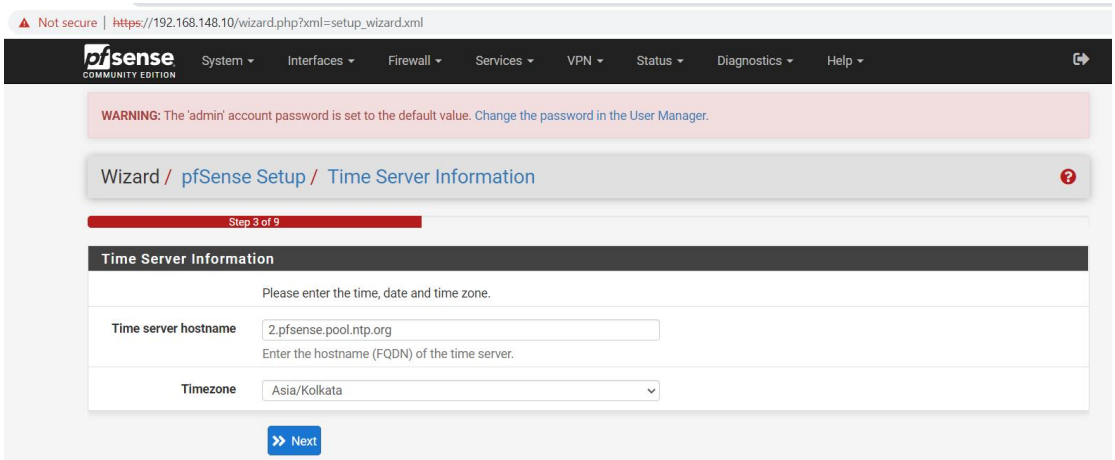


Click Next.

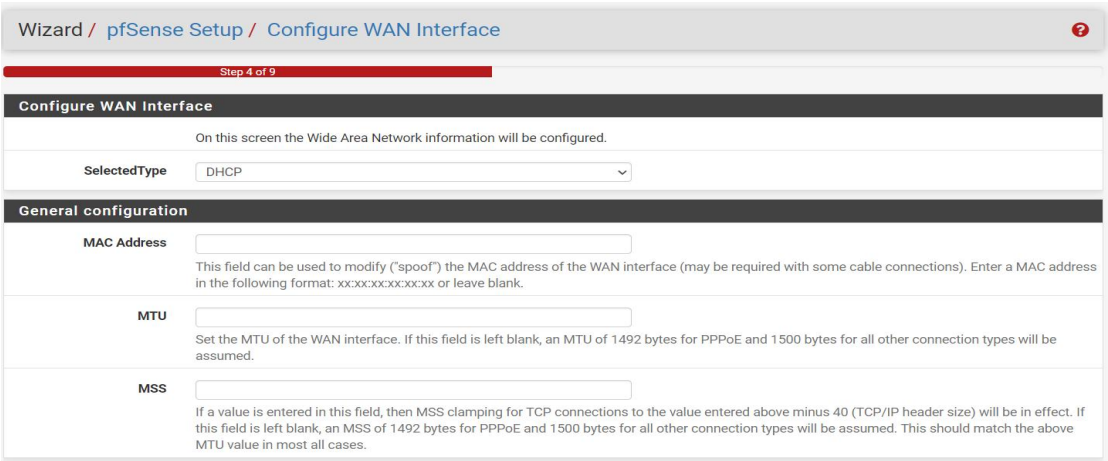
On the next screen enter a Hostname . Enter some domain name. Enter primary and Secondary DNS servers. This is shown below.



Click Next. The next Screen requires time server information. Keep it default.

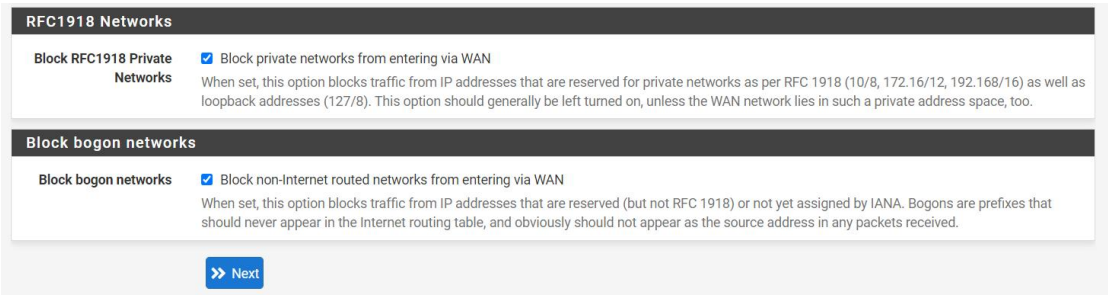


Click Next. The following screen requires setup for WAN interface. In production environment you may have to select PPPoE option as you may need to enter username and password provided by ISP to connect to Internet.
However for this LAB, we will keep the default option to DHCP.

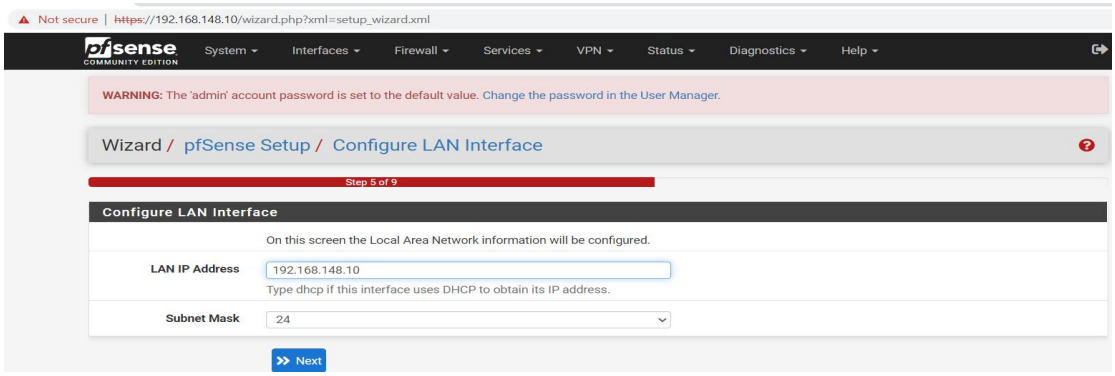


At the bottom of the page following 2 rules are present.

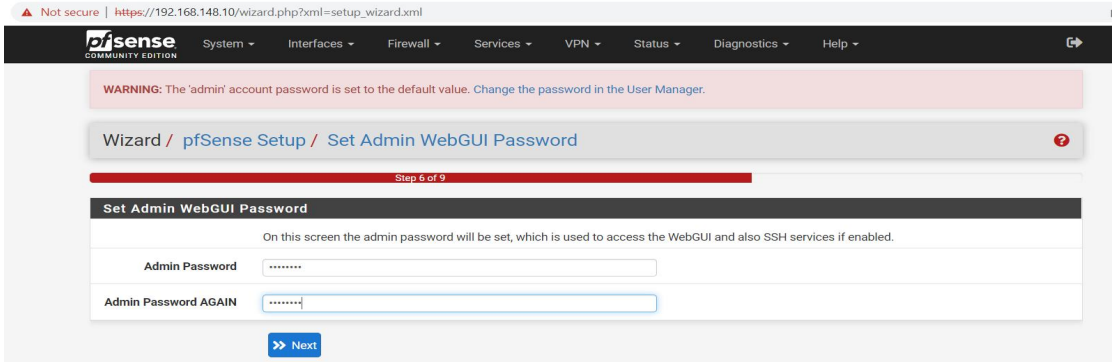
The first rule blocks any packet on WAN interface with the source IP from any IPv4 private address range.
The second rule blocks the reserved IP range or addresses not assigned by IANA on the WAN interface.



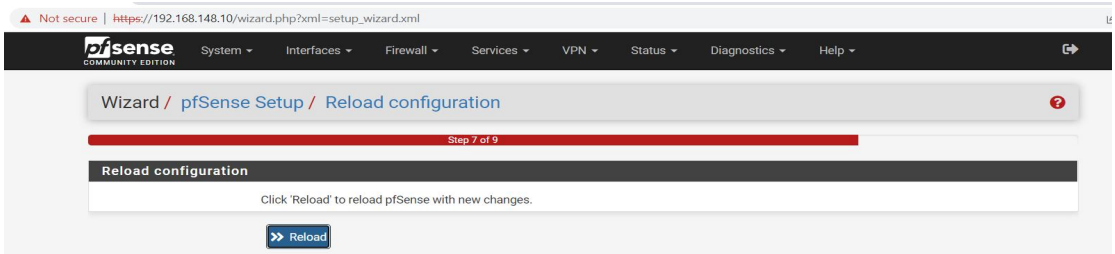
The rules are selected by default. Click Next. The next screen allows you to define the LAN IP address. However we have set the LAN IP already from the pfSense console.



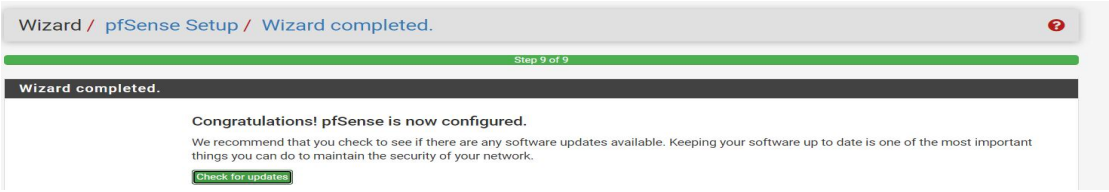
Keep settings as it is. Click Next. The next screen will ask you to enter a new password for the Admin user.



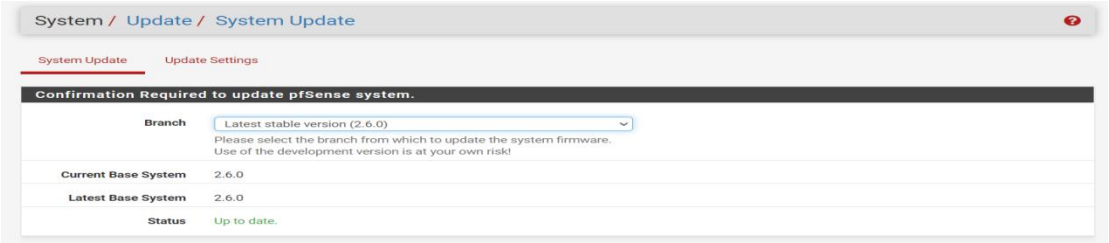
Enter a new password in both the fields and click Next. Click Reload on the next screen.



On the next screen click check for updates.



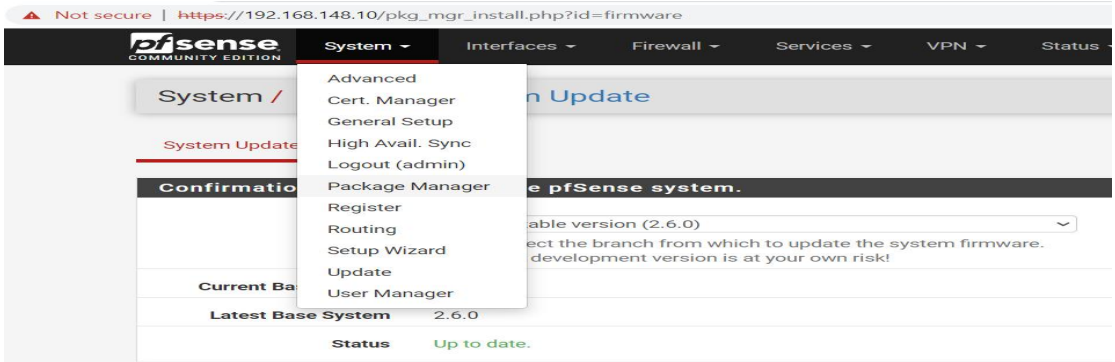
If any updates are present, then it will download the updates. It may take time based on update size and the internet speed.



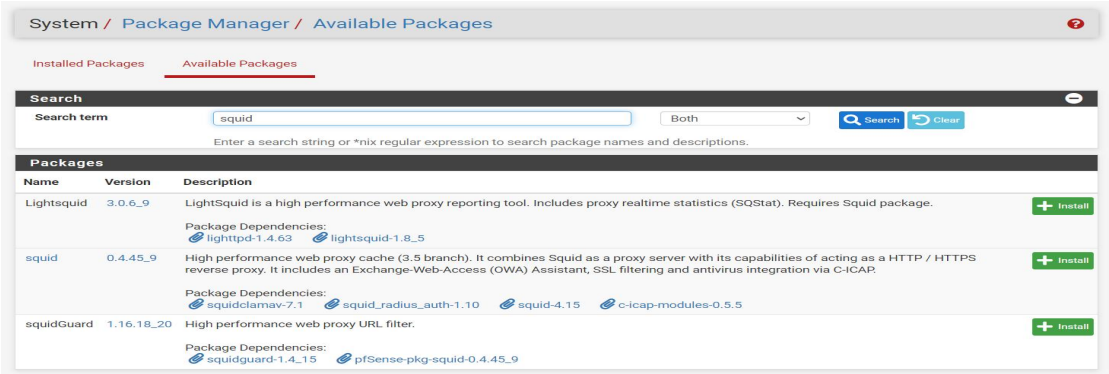
Finally once the update is over, above screen is displayed.

2. **Install Squid on pfSense**.

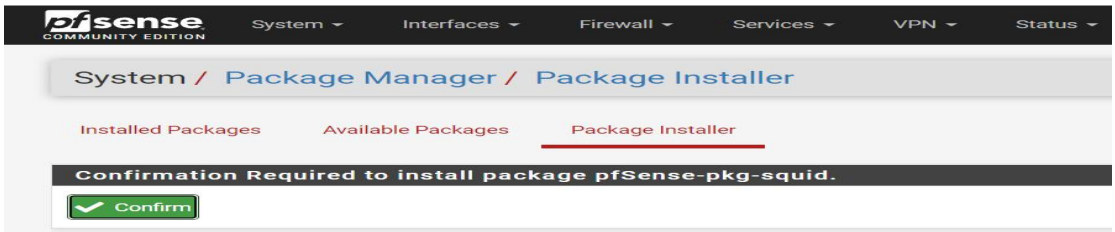
After initial setup, now we will install the Squid proxy on the pfSense. For this Click the **System** tab. In the list displayed click **Package Manager**.



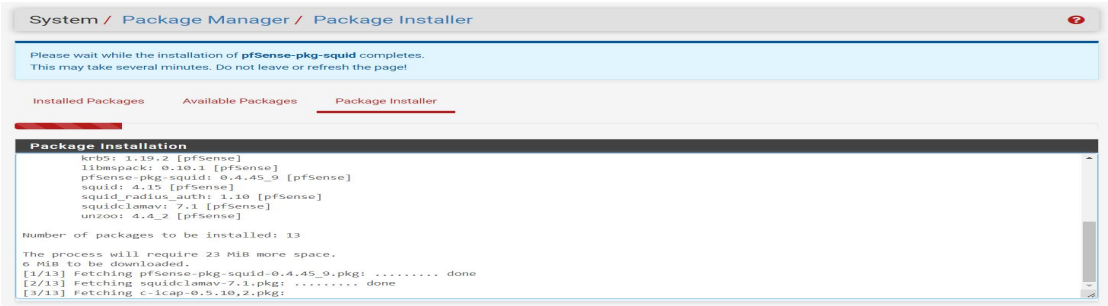
In the screen that is displayed, click available packages. In the search box type squid and press enter. This will display 3 packages. Click Install button in front of Squid package.



The following screen will appear asking confirmation to install the Squid package.



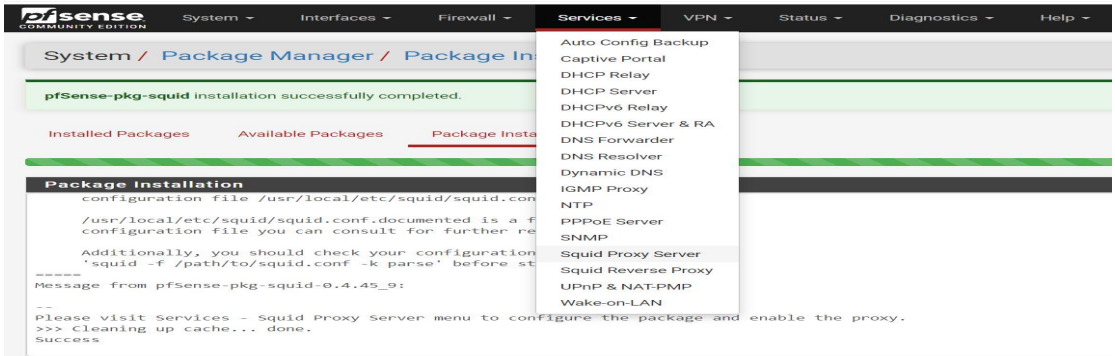
Click Confirm. The following screen will appear. It shows the Squid installation progress.



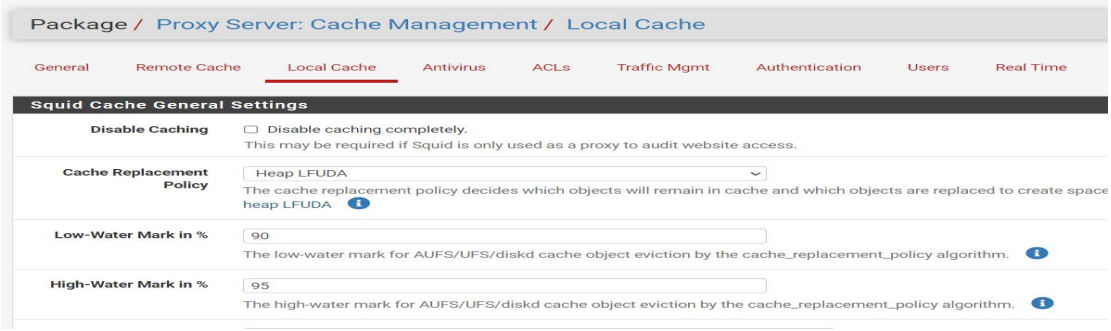
The installation may take time depending on the Internet speed.

3. **Configure Squid**.

Now to configure squid proxy, Click Services tab. In the list displayed click Squid Proxy Server.

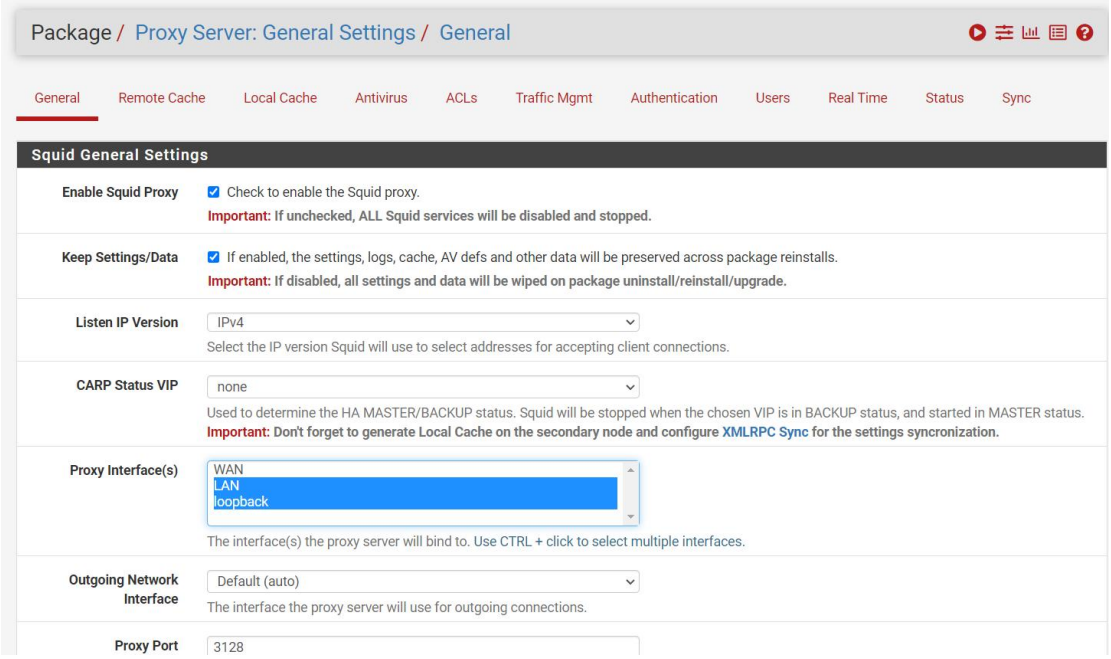


On the Squid proxy configuration page, first go to Local Cache tab as shown below.

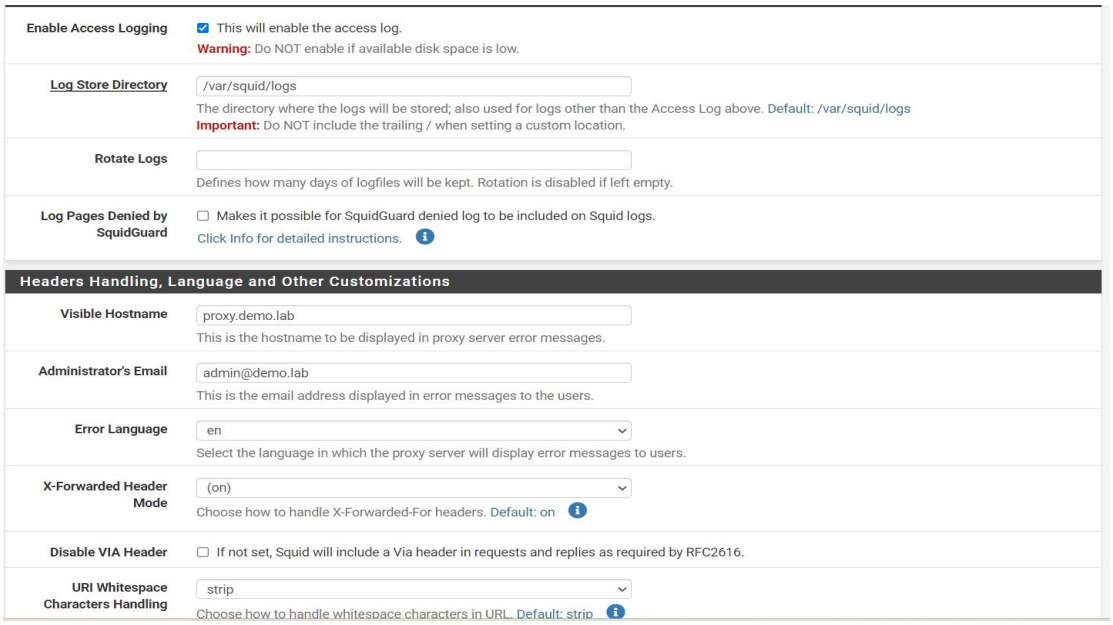


On this page you can configure Hard Disk Cache size, Hard Disk Cache Location, Memory Cache size etc.
However for this lab purpose we keep all values to their default. **Click Save**.

Then go to the General tab as shown below.
On this page select the check box to Enable Squid Proxy. In the Proxy Interfaces Select LAN and Loopback both. The default port used by Squid is 3128.

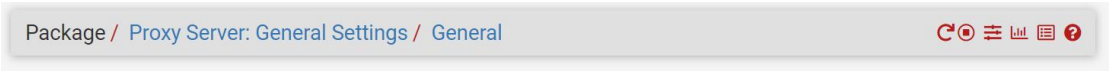


Scroll down. Click check box to Enable Access Logging. Set Visible Hostname. Set Administrator's Email.



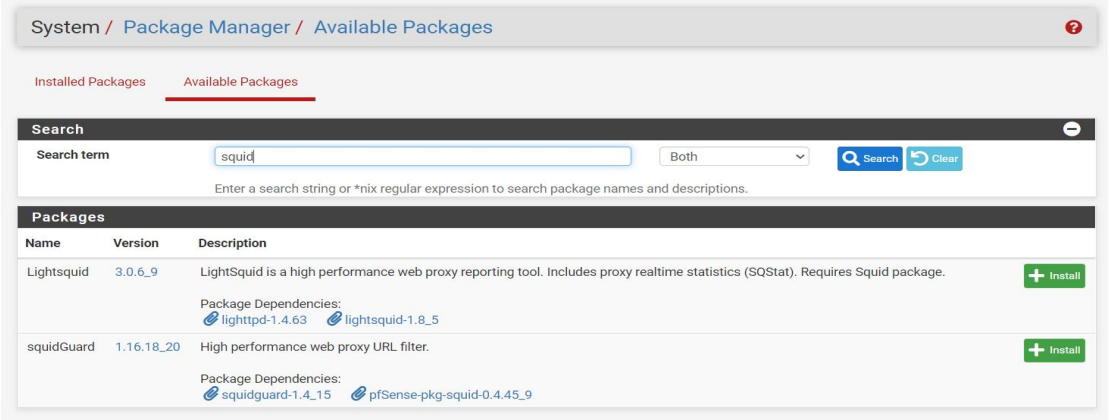
Scroll to the end. Click Save. This will start the squid proxy service.

At the top of Squid proxy server page buttons to restart, stop squid service will appear as shown below.

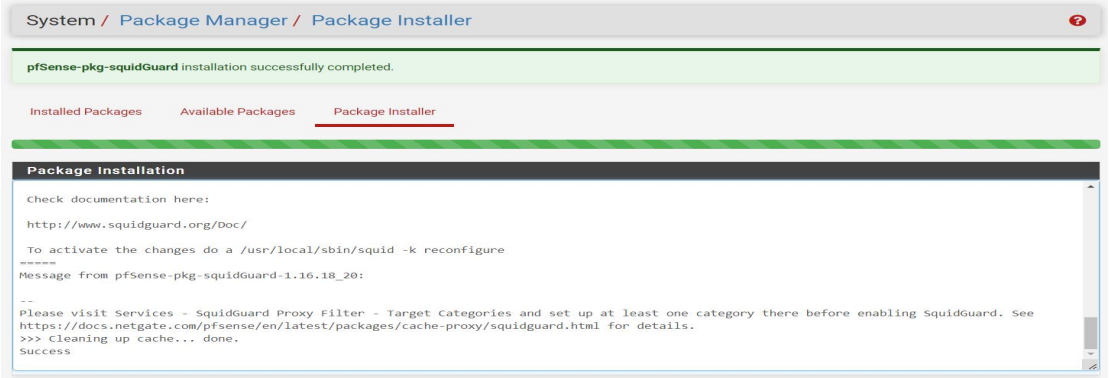


4. **Install Squidguard**

Again go to the Systems tab. Click Package Manager. Click Available Packages. In the search field type squid. Now 2 squid packages will be displayed.
Click Install button in front of Squidguard to install it.

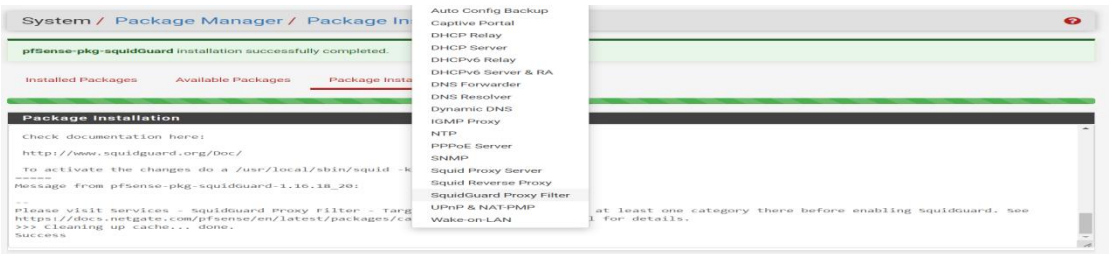


Click Confirm on the next screen . This will start Squidguard installation. Once the installation is complete following screen is displayed.

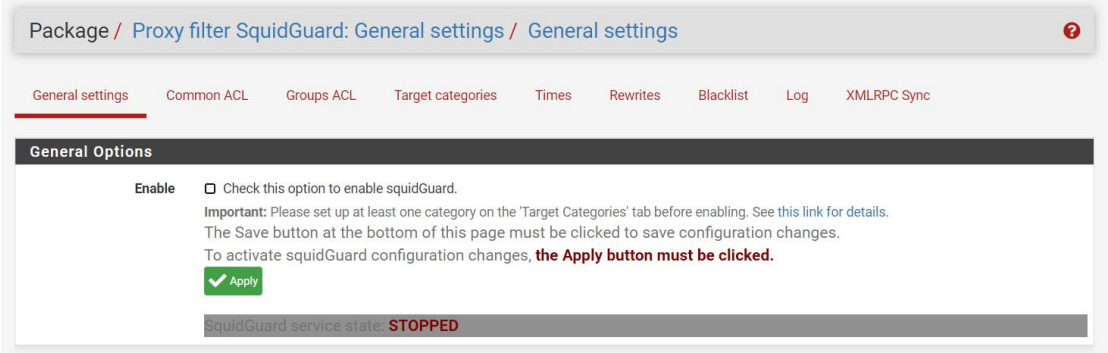


5. Configure Squidguard

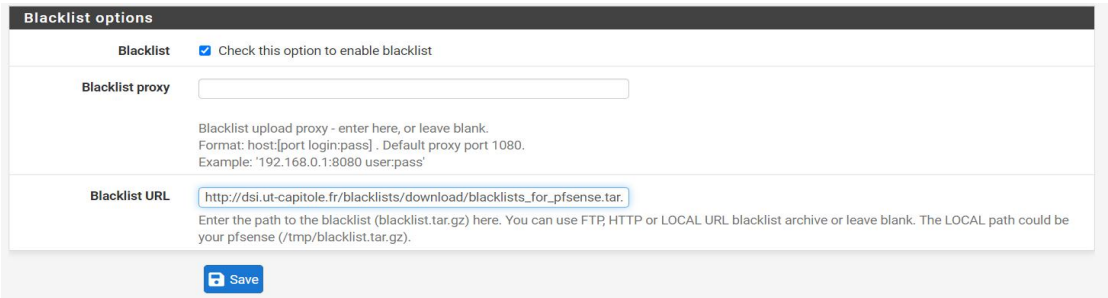
Go to Services tab. In the list displayed click Squidguard Proxy Filter option as shown below.



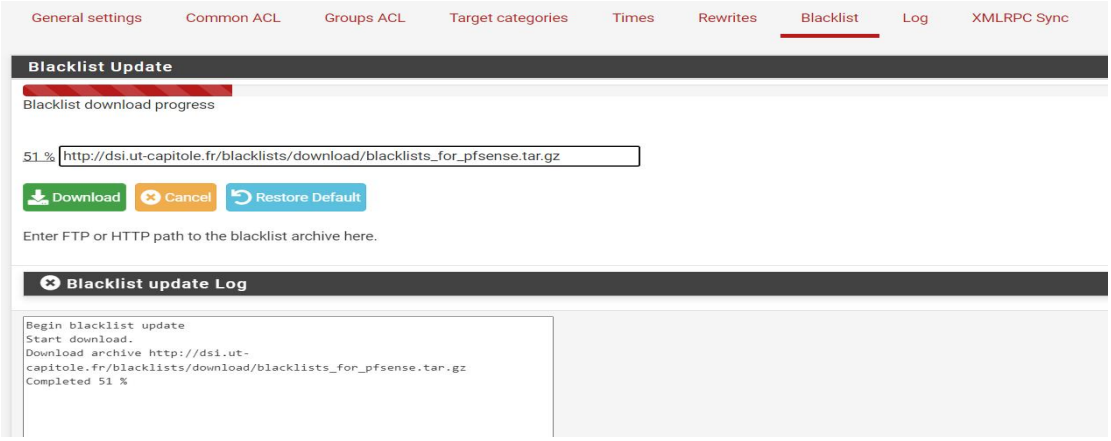
Click General Settings . Do not click the Check box to Enable Squidguard.



Scroll down to the Blacklist option. Click Blacklist checkbox. In the Blacklist URL type following URL.
https://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfsense.tar.gz

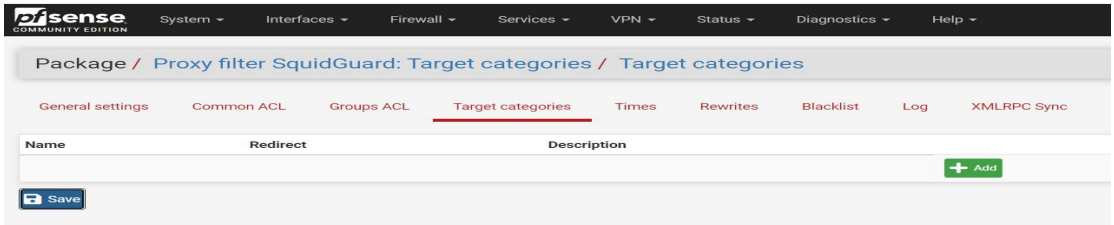


Click Save.
Then go to the Blacklist tab as shown below.

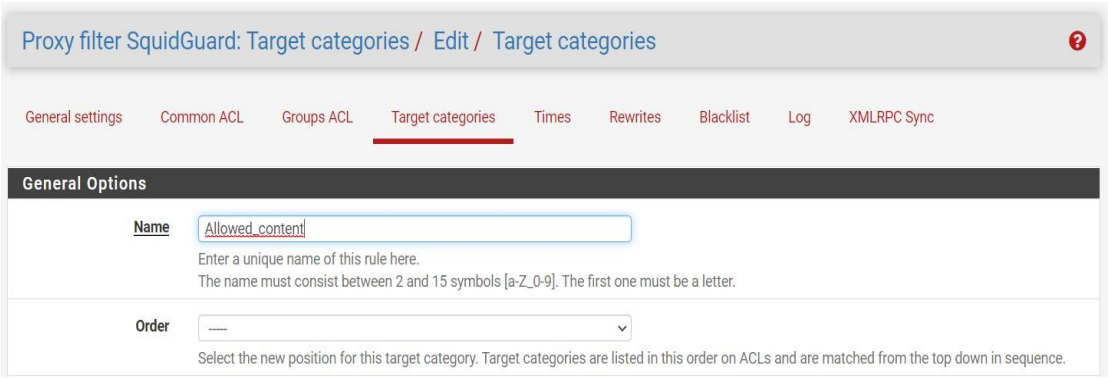


Make sure the URL is displayed. Click Download.
This will download the blacklist for URL filter.

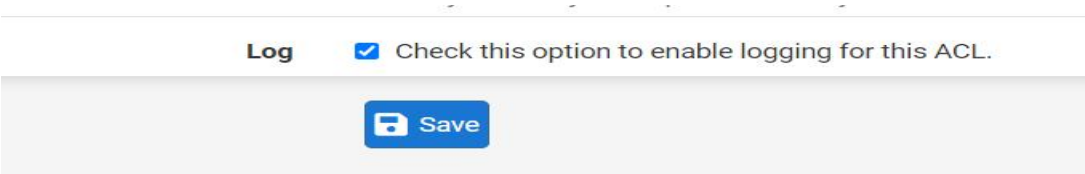
Next go to Target categories.



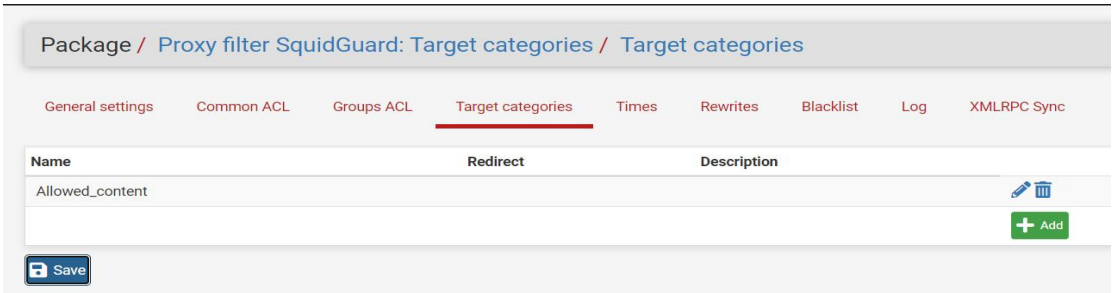
Click Add.
On the screen that is displayed, first provide a Name to the target category.



Click check box in front of Log.

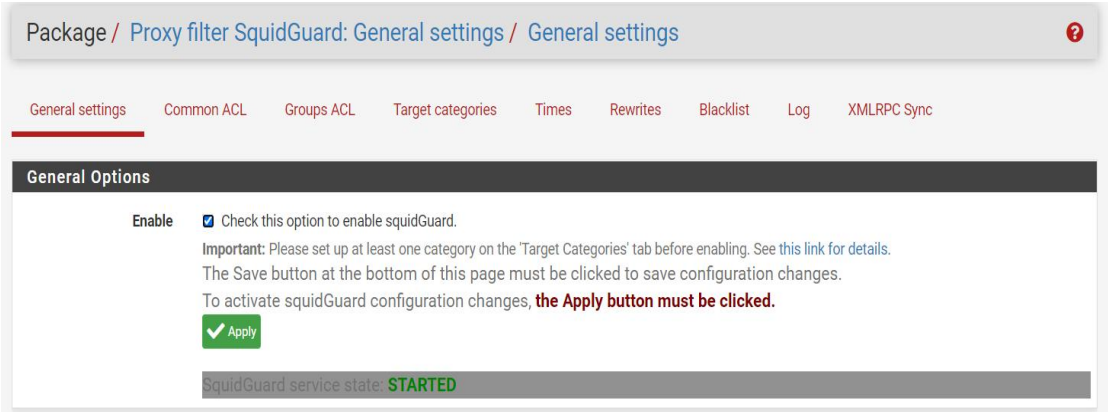


Click Save.
This will create the target category as shown below.



Click Save.

Then go to the General Settings. Click the check box to Enable Squidguard. Click Apply. Then the Squidguard service will start as shown below.

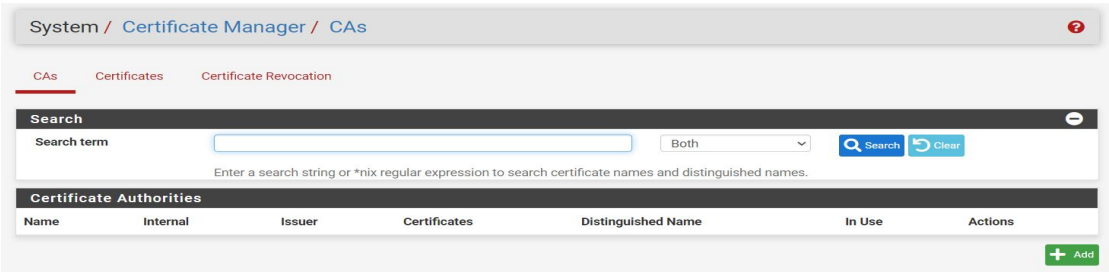


6. Configure SSL Man in the Middle.

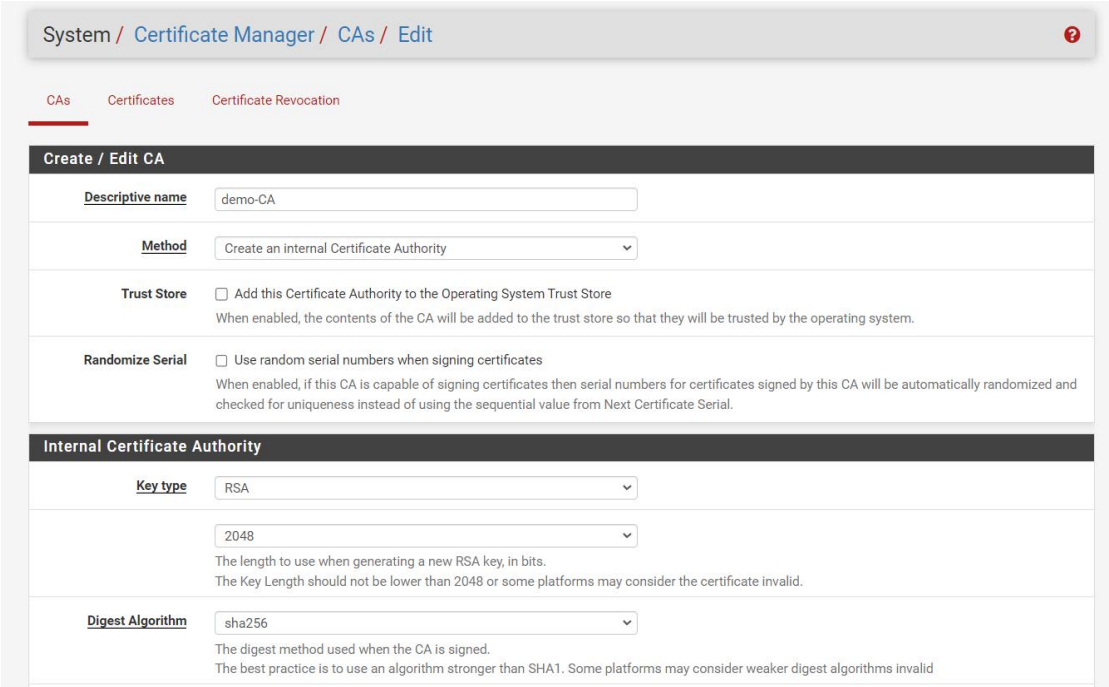
Now we will configure the SSL Man in the Middle for Squid proxy server. This will help Squid to perform more accurate filtering based on URL contents.

Click the System tab. In the list displayed click Cert. Manager.

Go to the CAs tab. By default there is no Certification Authority created.

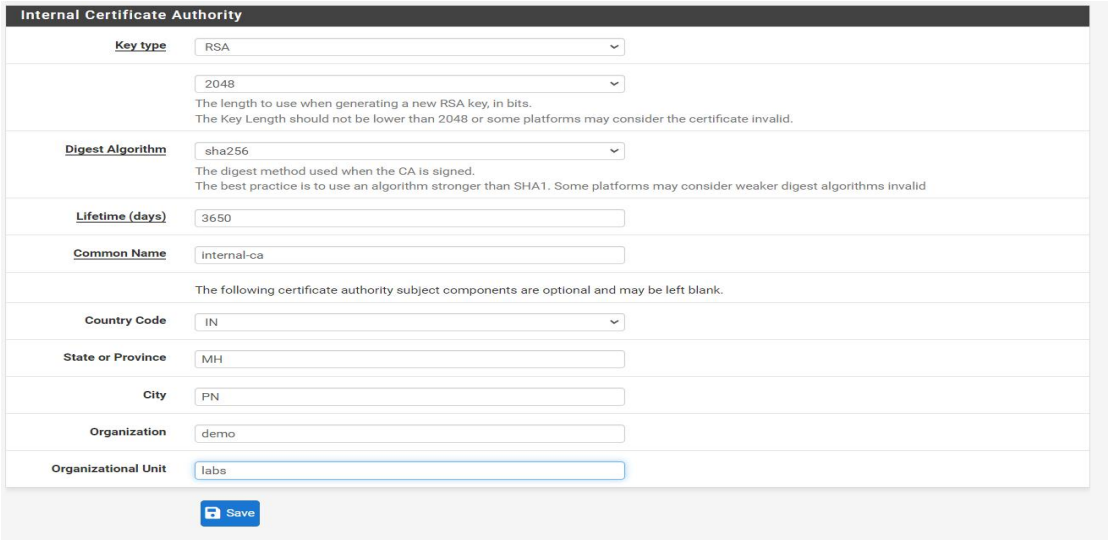


Click Add button. Following page will be displayed. This will create a new certification authority.
Provide a distinguished name. In method select Create an Internal Certificate Authority. Keep all other options to their default value.

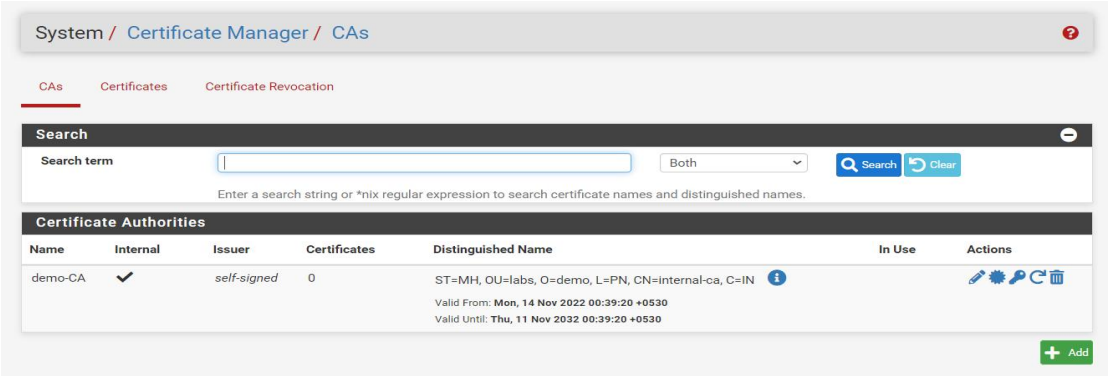


Scroll Down.

Provide a Common name. Enter details like Country Code, State or Province, City, Organization, Organizational Unit etc.



Click Save.



The above screen displays the new CA created.

Now configure the Squid proxy server to perform the SSL Man in the Middle. Click the Services tab. Select Squid Proxy Server. Click the general tab . Scroll down to the following section.

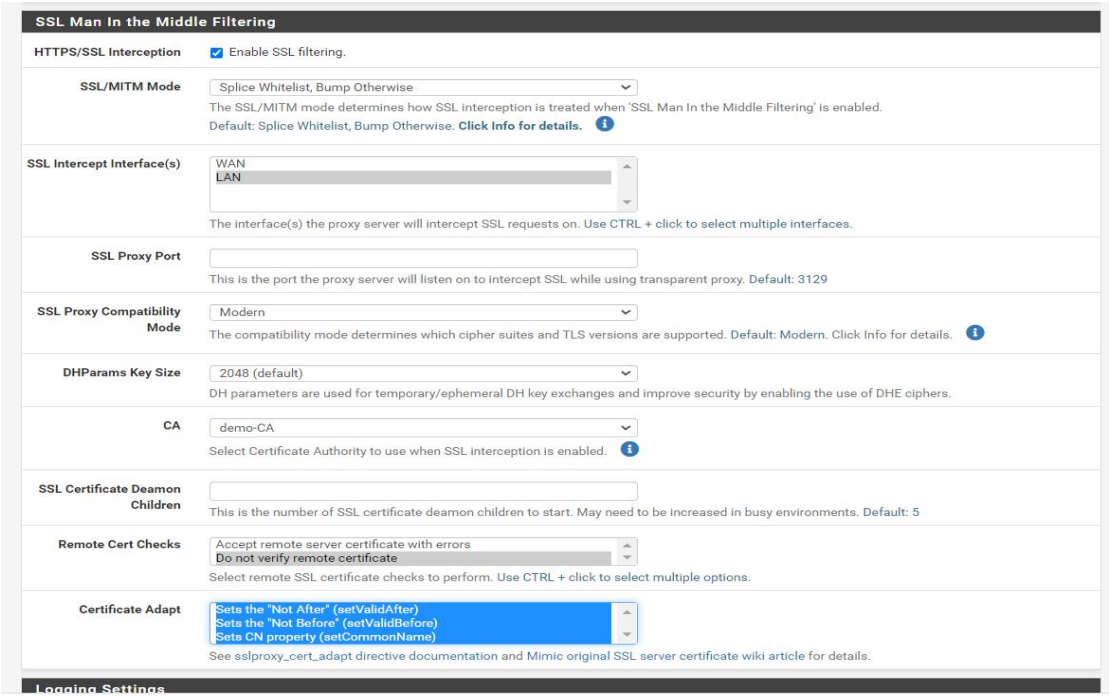
Click the check box in front of HTTPS/SSL Interception.

Select LAN in the SSL Intercept Interface.

In the CA field click the drop down list to select the CA that we created above.

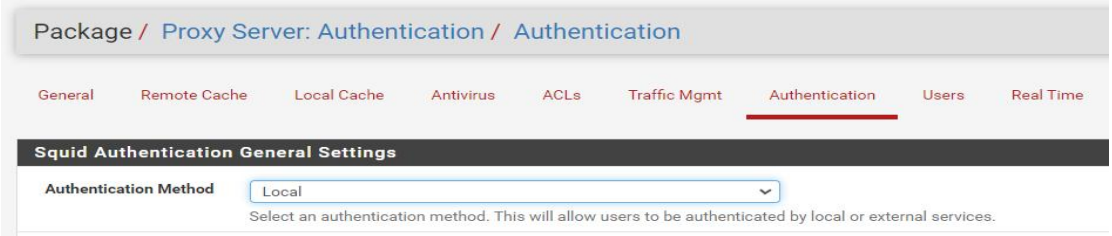
In the Remote cert. Checks, click Do not Verify remote Certificate option.

Select all options in the Certificate Adopt section.



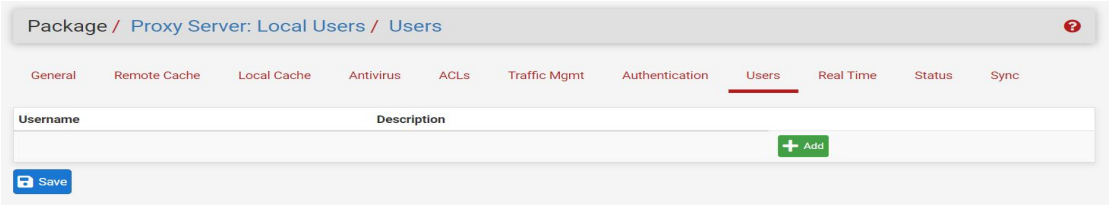
Click Save.

Now we enable user based access control. Go to the Authentication tab.
In the Authentication Method use drop down and select Local .

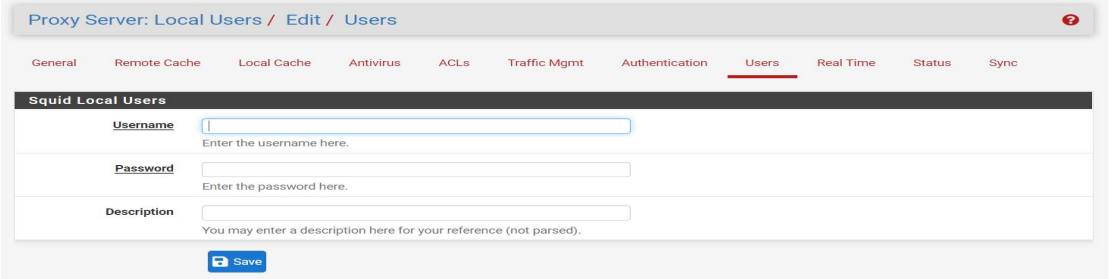


Click Save.

To create Squid proxy users. Go to the Users tab.



Click Add to add a new user.



Provide Username , password , Description and Click Save.