

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.

Welcome to VMware Workstation 16 Player

Create a New Virtual Machine

Create a new virtual machine, which will then be added to the top of your library.

Open a Virtual Machine

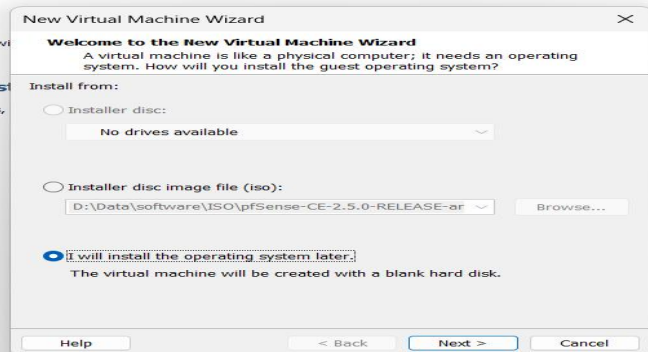
Open an existing virtual machine, which will be added to the top of your library.

Upgrade to VMware Workstation

Get advanced features such as snapshots, shared folders, and more.

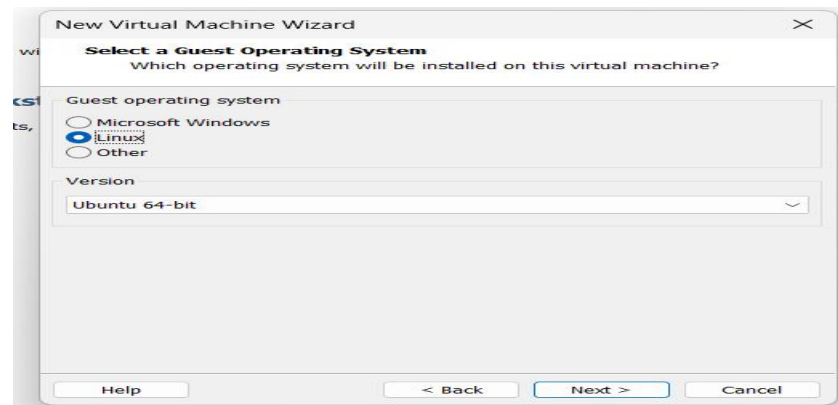
Help

View online help.

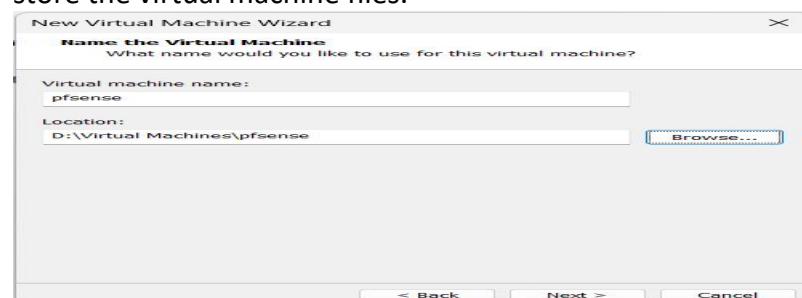


On the window that opens, select I will install the operating system later. Click Next.

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

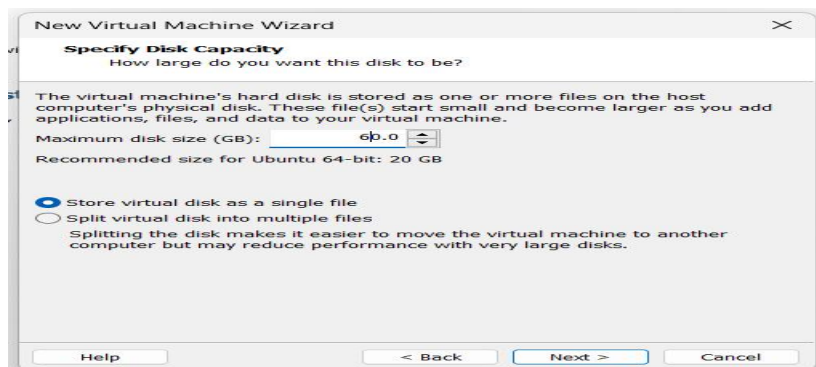


On the next window provide a name for the virtual machine. Also provide a path to store the virtual machine files.

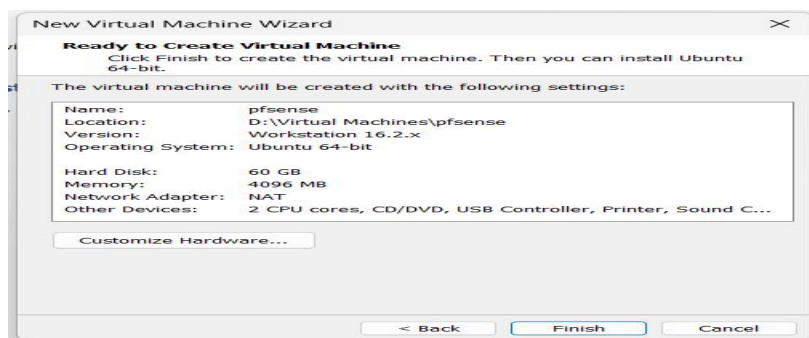


Click Next.

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.



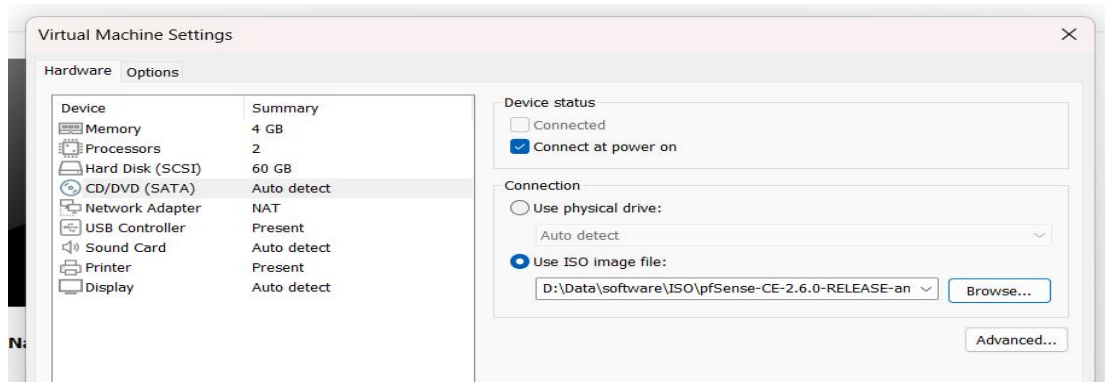
Click Finish to create the virtual machine. The virtual machine is shown as below.



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.

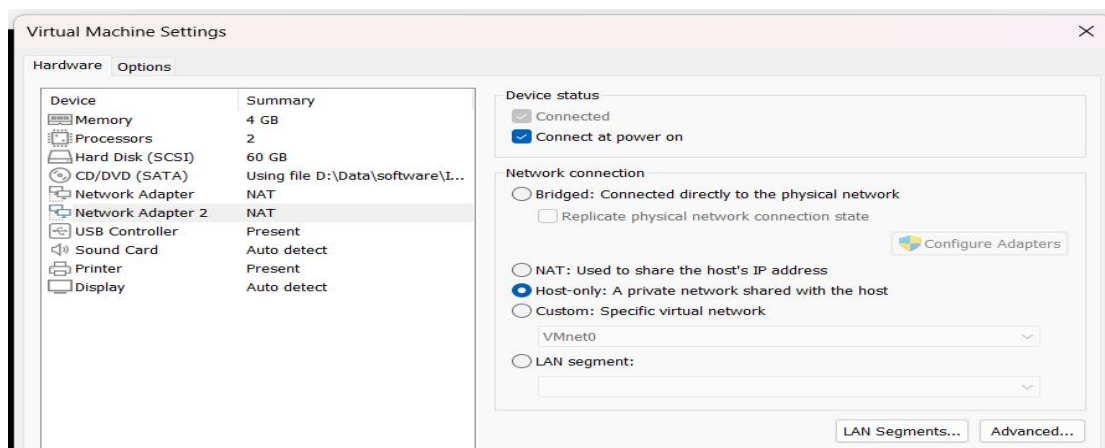
This is shown in the following image.



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.

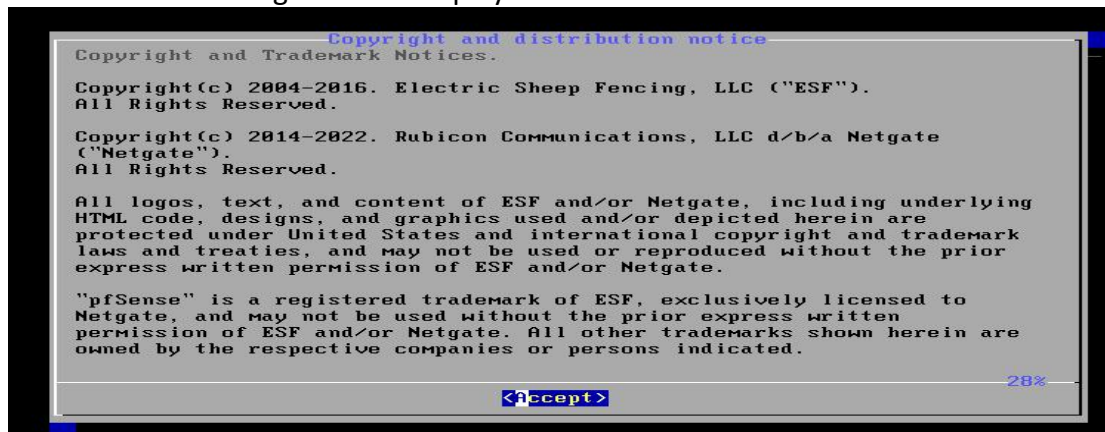


Click OK to close the settings window. Then Click the green arrow in the menu bar or click Play virtual machine option.

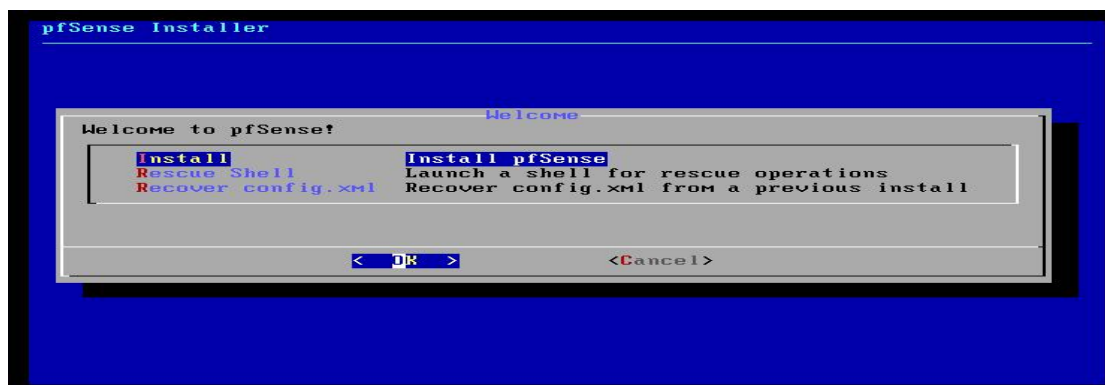


The Virtual machine will start and the pfSense installation begins.

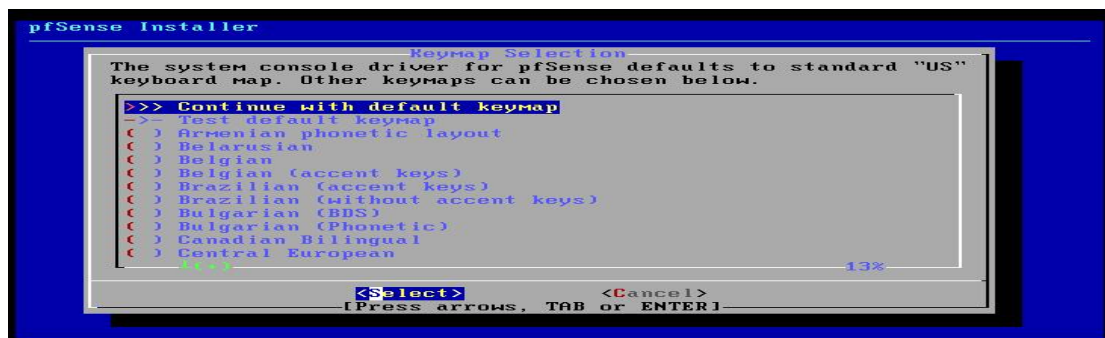
Wait till the following screen is displayed.



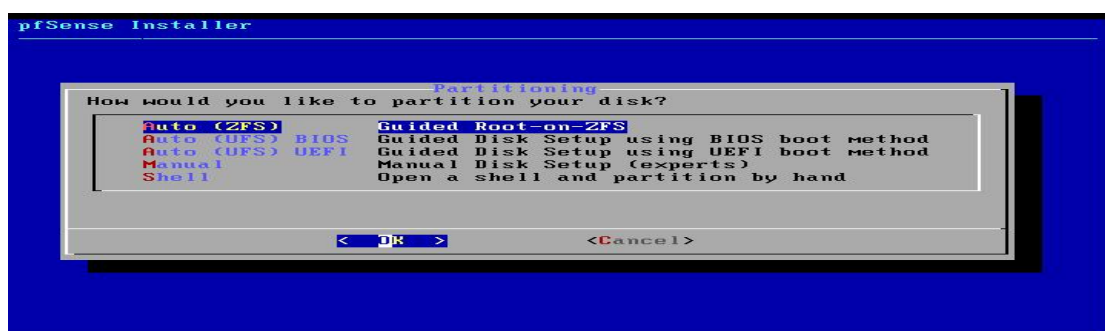
Press Enter to Accept to accept the Copyright and distribution notice.



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.

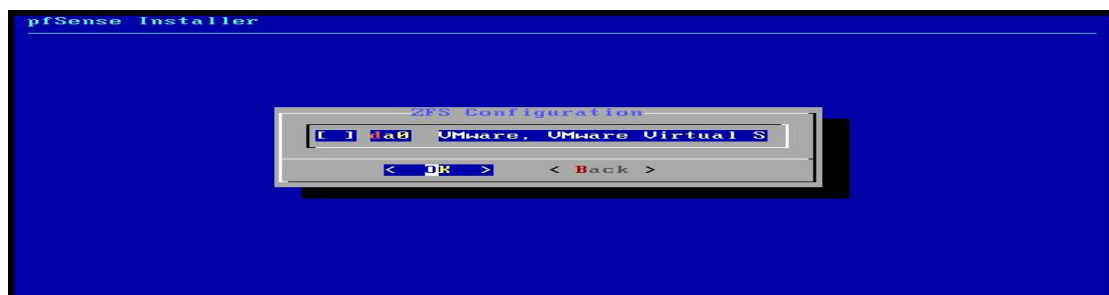
Press Enter on the following screen to proceed with the installation.



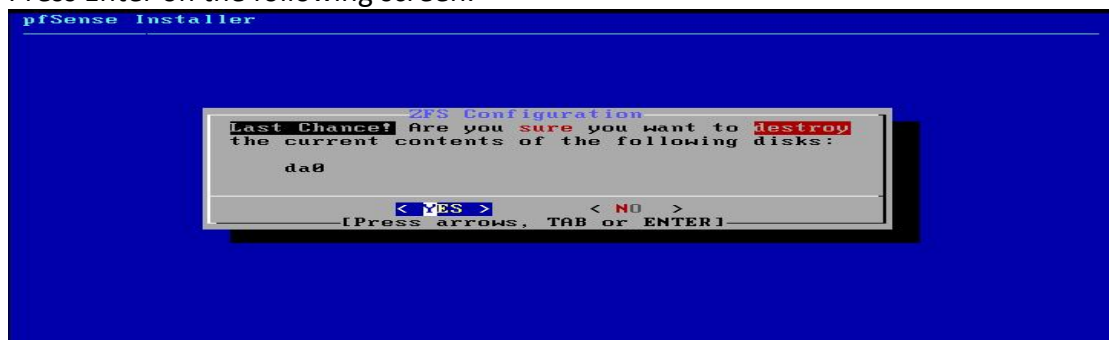
On the next screen again press Enter to continue with the default **stripe** option.



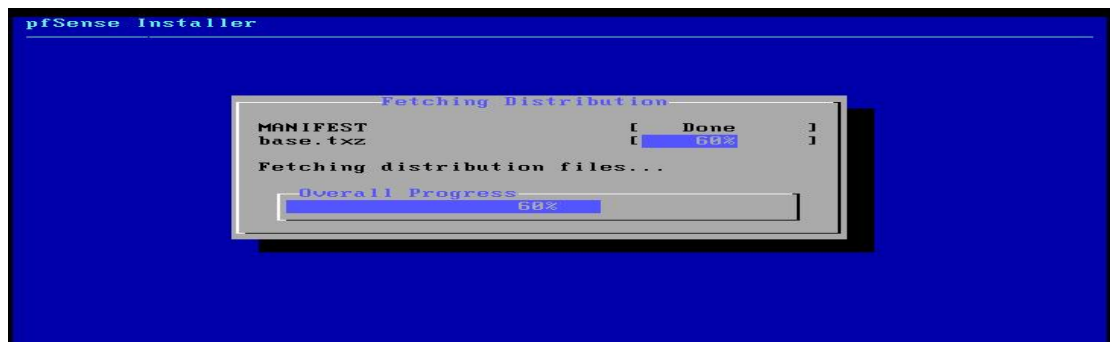
On the next screen displayed, press space bar to select the da0 square box. Then press Enter to continue.



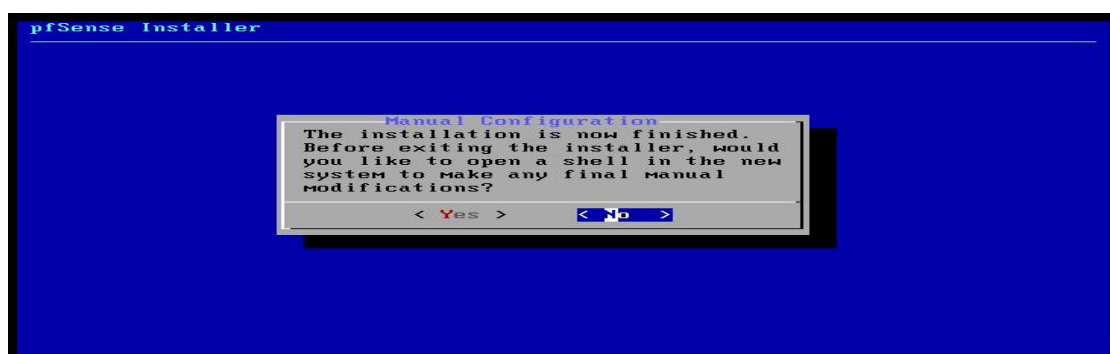
Press Enter on the following screen.



This will start the pfSense installation.



Once Installation is complete, following screen is displayed.



Press Enter to continue with the No option.

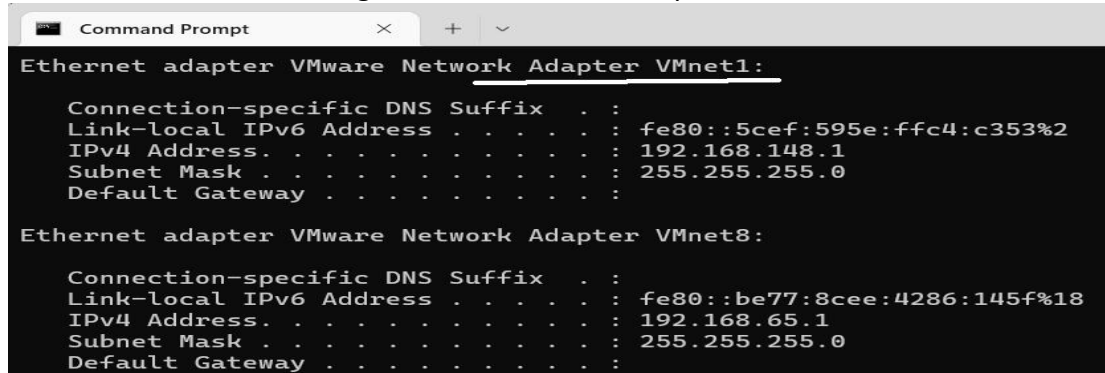


Press Enter to reboot the pfSense virtual machine. Once the pfSense starts following screen is displayed.



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

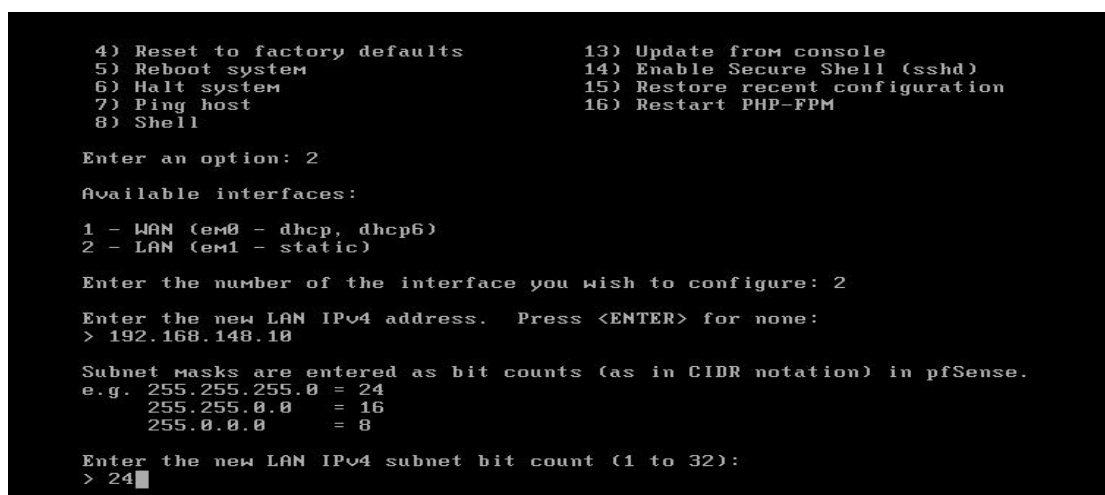
Ethernet adapter VMware Network Adapter VMnet1:

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

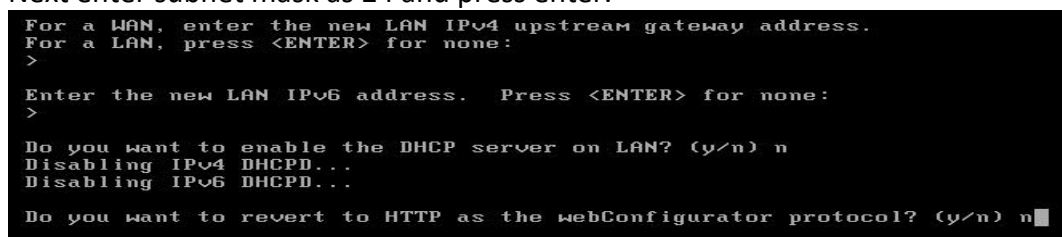
Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24
```

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...

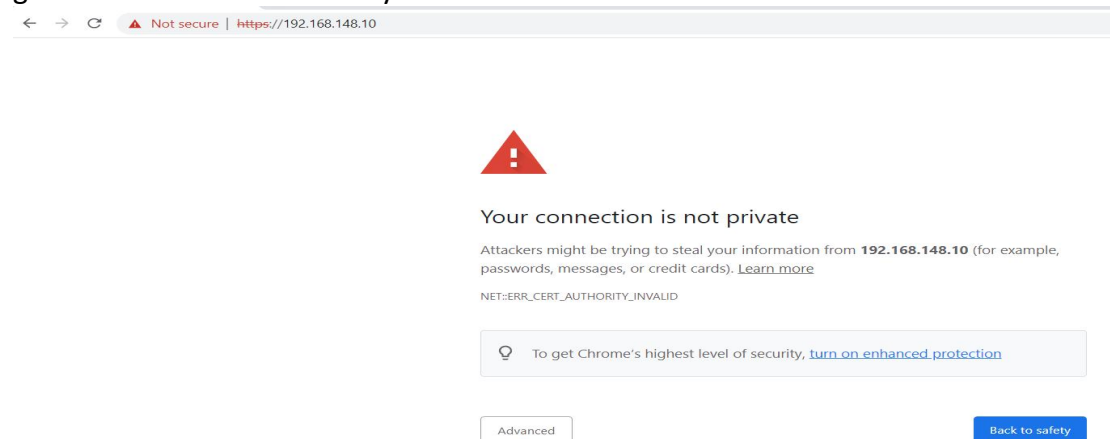
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n
```

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.

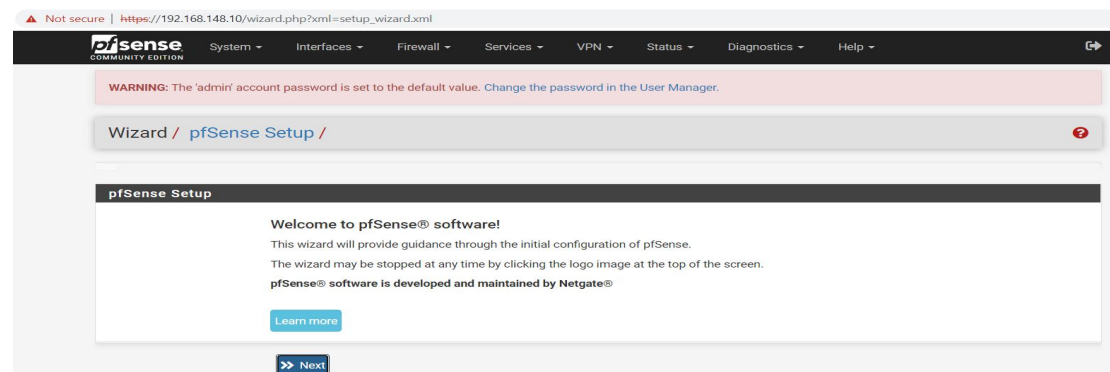
Now go to your second Virtual Machine (Either Windows or Linux) . Make sure the network adapter of this VM is in **host-only** mode.

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.

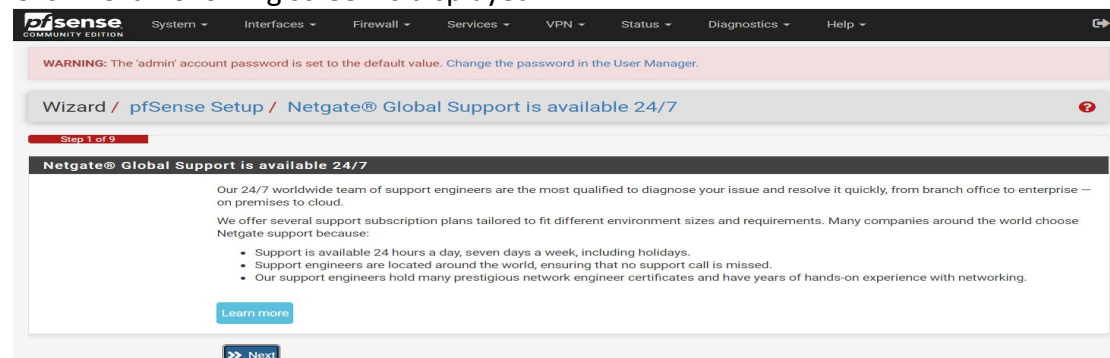


Click Advanced and proceed to the website. On the Login page login with username as **admin** and password as **pfSense**.

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.

This screenshot shows the 'General Information' step of the pfSense setup wizard. It includes fields for Hostname (HO-pfSense), Domain (demo.lab), Primary DNS Server (8.8.8.8), and Secondary DNS Server (8.8.4.4). There is also a checkbox for 'Override DNS' which is checked. A 'Next' button is at the bottom.

General Information	
On this screen the general pfSense parameters will be set.	
Hostname	HO-pfSense <small>EXAMPLE: myserver</small>
Domain	demo.lab <small>EXAMPLE: mydomain.com</small>
The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.	
Primary DNS Server	8.8.8.8
Secondary DNS Server	8.8.4.4
Override DNS	<input checked="" type="checkbox"/> <small>Allow DNS servers to be overridden by DHCP/PPP on WAN</small>
Next	

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

This screenshot shows the 'Time Server Information' step of the pfSense setup wizard. It includes fields for Time server hostname (2.pfsense.pool.ntp.org) and Timezone (Asia/Kolkata). A 'Next' button is at the bottom.

Time Server Information	
Please enter the time, date and time zone.	
Time server hostname	2.pfsense.pool.ntp.org <small>Enter the hostname (FQDN) of the time server.</small>
Timezone	Asia/Kolkata
Next	

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.

This screenshot shows the 'Configure WAN Interface' step of the pfSense setup wizard. It includes a dropdown for 'SelectedType' (DHCP) and a section for 'General configuration' with fields for MAC Address, MTU, and MSS. A 'Next' button is at the bottom.

Configure WAN Interface	
On this screen the Wide Area Network information will be configured.	
SelectedType	DHCP
General configuration	
MAC Address	<input type="text"/> <small>This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections). Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.</small>
MTU	<input type="text"/> <small>Set the MTU of the WAN interface. If this field is left blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.</small>
MSS	<input type="text"/> <small>If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If this field is left blank, an MSS of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed. This should match the above MTU value in most all cases.</small>
Next	

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.

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 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.

[Next](#)

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.

Not secure | https://192.168.148.10/wizard.php?xml=setup_wizard.xml

pfSense COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Wizard / pfSense Setup / Configure LAN Interface

Step 5 of 9

Configure LAN Interface

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

LAN IP Address: 192.168.148.10
Type dhcp if this interface uses DHCP to obtain its IP address.

Subnet Mask: 24

[Next](#)

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

Not secure | https://192.168.148.10/wizard.php?xml=setup_wizard.xml

pfSense COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Wizard / pfSense Setup / Set Admin WebGUI Password

Step 6 of 9

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: [password field]

Admin Password AGAIN: [password field]

[Next](#)

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

Not secure | https://192.168.148.10/wizard.php?xml=setup_wizard.xml

pfSense COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

Wizard / pfSense Setup / Reload configuration

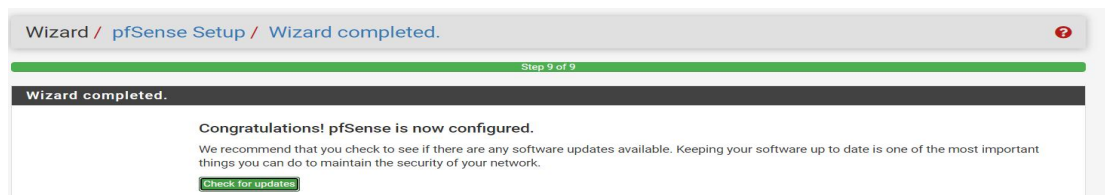
Step 7 of 9

Reload configuration

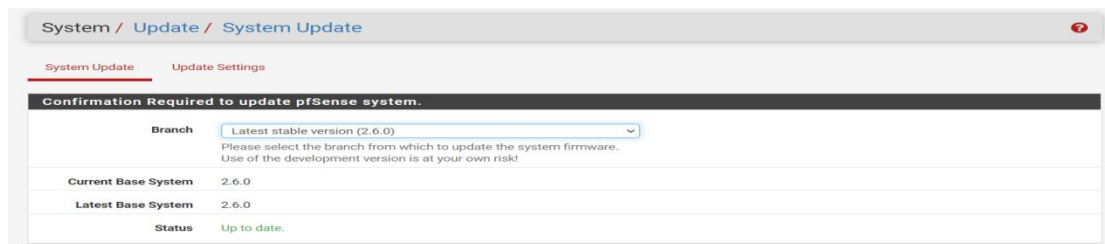
Click 'Reload' to reload pfSense with new changes.

[Reload](#)

On the next screen click check for updates.



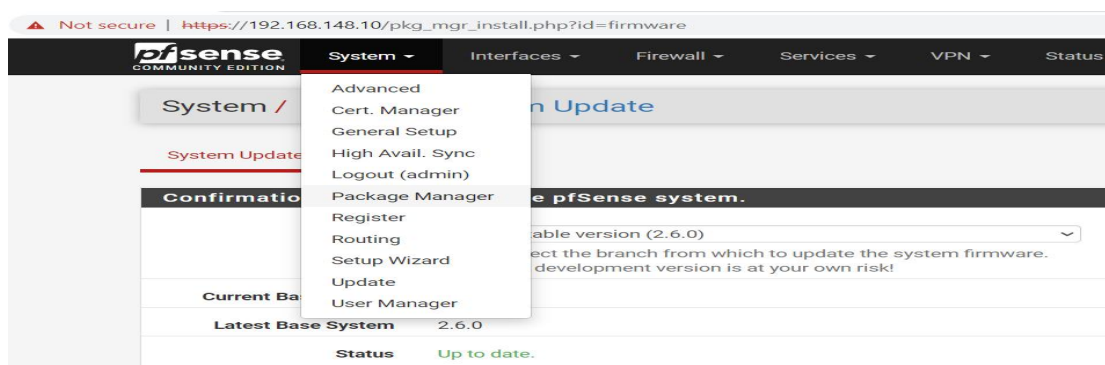
If any updates are present, then it will download the updates. It may take time based on update size and the internet speed.



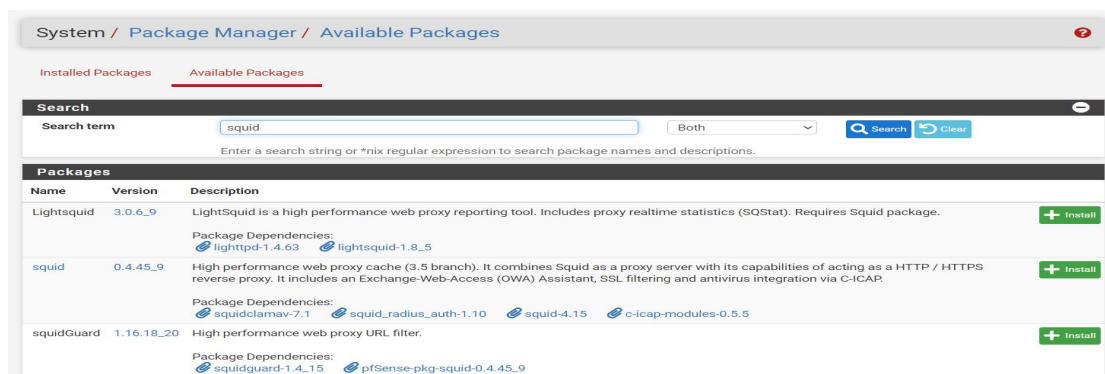
Finally once the update is over, above screen is displayed.

2. Install Squid on pfSense.

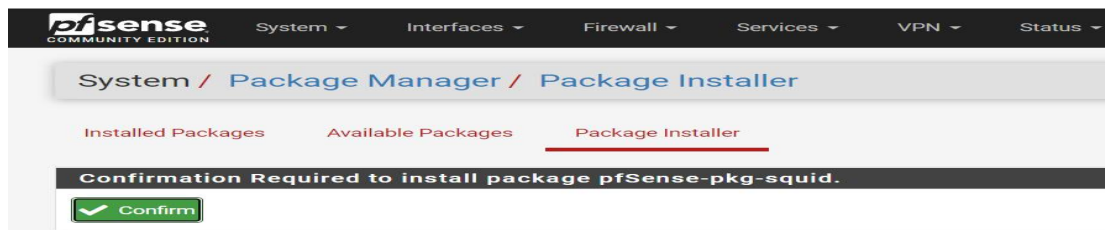
After initial setup, now we will install the Squid proxy on the pfSense. For this Click the **System** tab. In the list displayed click **Package Manager**.



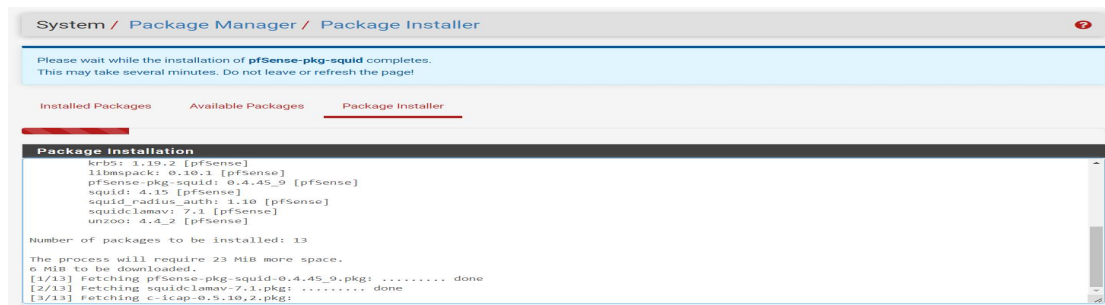
In the screen that is displayed, click available packages. In the search box type squid and press enter. This will display 3 packages. Click Install button in front of Squid package.



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



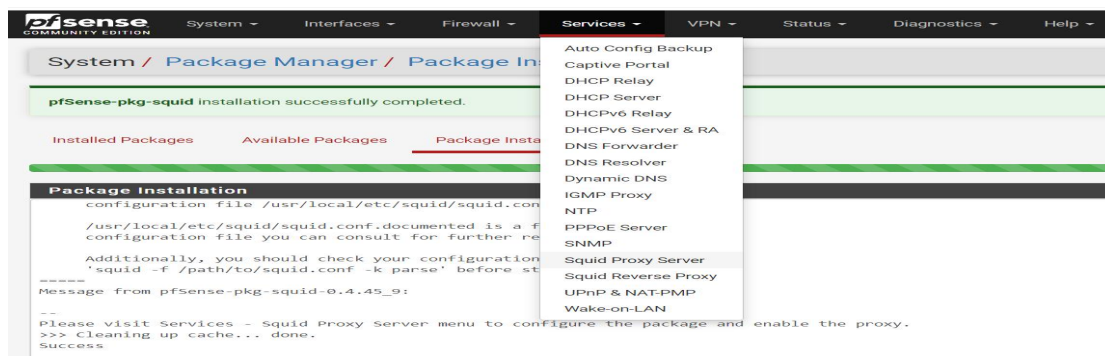
Click Confirm. The following screen will appear. It shows the Squid installation progress.



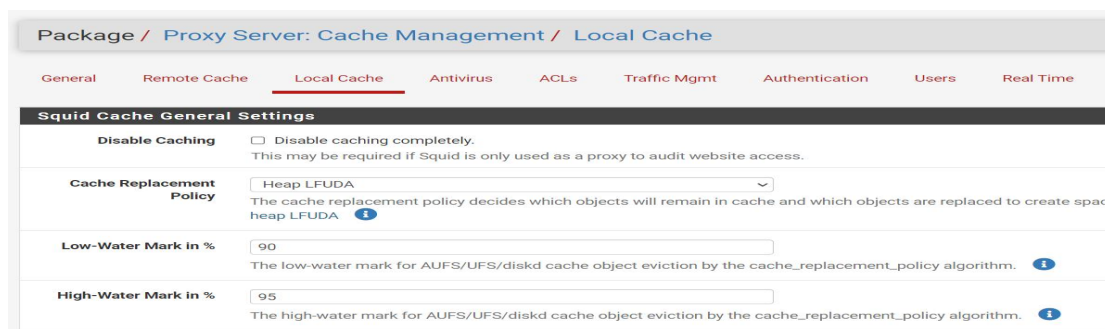
The installation may take time depending on the Internet speed.

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.

Package / Proxy Server: General Settings / General

General Remote Cache Local Cache Antivirus ACLs Traffic Mgmt Authentication Users Real Time Status Sync

Squid General Settings

Enable Squid Proxy	<input checked="" type="checkbox"/> Check to enable the Squid proxy. Important: If unchecked, ALL Squid services will be disabled and stopped.
Keep Settings/Data	<input checked="" type="checkbox"/> If enabled, the settings, logs, cache, AV defs and other data will be preserved across package reinstalls. Important: If disabled, all settings and data will be wiped on package uninstall/reinstall/upgrade.
Listen IP Version	IPv4 Select the IP version Squid will use to select addresses for accepting client connections.
CARP Status VIP	none Used to determine the HA MASTER/BACKUP status. Squid will be stopped when the chosen VIP is in BACKUP status, and started in MASTER status. Important: Don't forget to generate Local Cache on the secondary node and configure XMLRPC Sync for the settings synchronization.
Proxy Interface(s)	WAN LAN loopback The interface(s) the proxy server will bind to. Use CTRL + click to select multiple interfaces.
Outgoing Network Interface	Default (auto) The interface the proxy server will use for outgoing connections.
Proxy Port	3128

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

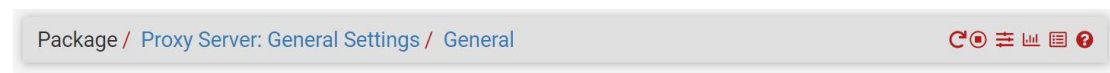
Enable Access Logging	<input checked="" type="checkbox"/> This will enable the access log. Warning: Do NOT enable if available disk space is low.
Log Store Directory	/var/squid/logs The directory where the logs will be stored; also used for logs other than the Access Log above. Default: /var/squid/logs Important: Do NOT include the trailing / when setting a custom location.
Rotate Logs	<input type="text"/> Defines how many days of logfiles will be kept. Rotation is disabled if left empty.
Log Pages Denied by SquidGuard	<input type="checkbox"/> Makes it possible for SquidGuard denied log to be included on Squid logs. Click Info for detailed instructions.

Headers Handling, Language and Other Customizations

Visible Hostname	proxy.demo.lab This is the hostname to be displayed in proxy server error messages.
Administrator's Email	admin@demo.lab This is the email address displayed in error messages to the users.
Error Language	en Select the language in which the proxy server will display error messages to users.
X-Forwarded Header Mode	(on) Choose how to handle X-Forwarded-For headers. Default: on
Disable VIA Header	<input type="checkbox"/> If not set, Squid will include a Via header in requests and replies as required by RFC2616.
URI Whitespace Characters Handling	strip Choose how to handle whitespace characters in URL. Default: strip

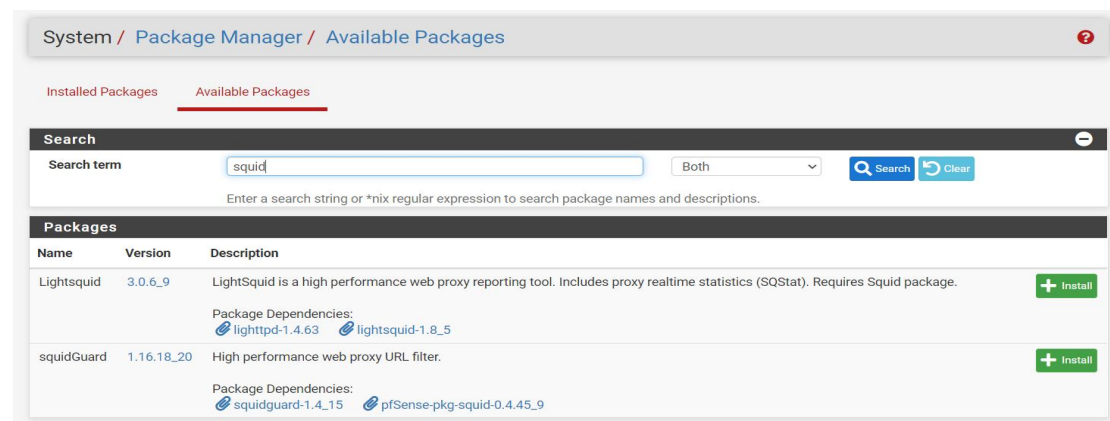
Scroll to the end. Click Save. This will start the squid proxy service.

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

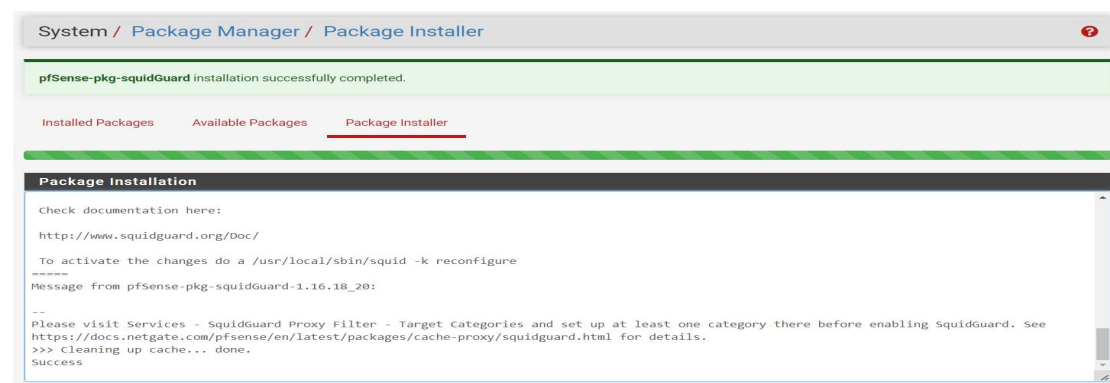


4. Install Squidguard

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.

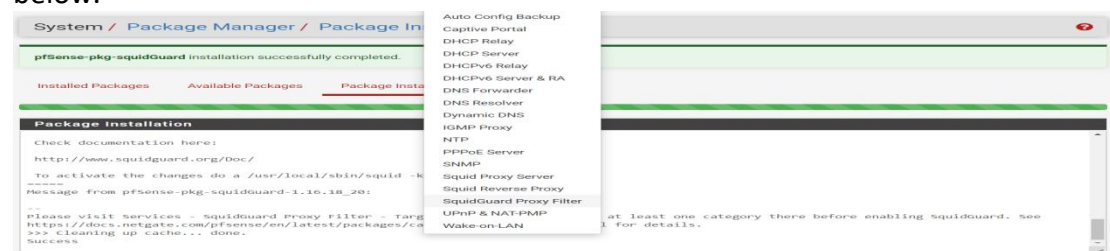


Click Confirm on the next screen . This will start Squidguard installation. Once the installation is complete following screen is displayed.



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.

The screenshot shows the 'General settings' tab for the 'Proxy filter SquidGuard' package. The 'General Options' section has an 'Enable' checkbox that is currently unchecked. Below it, there is an 'Important' note: 'Please set up at least one category on the 'Target Categories' tab before enabling. See this link for details. The Save button at the bottom of this page must be clicked to save configuration changes. To activate squidGuard configuration changes, the Apply button must be clicked.' There is a green 'Apply' button. At the bottom, the 'SquidGuard service state' is shown as 'STOPPED'.

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

The screenshot shows the 'Blacklist options' section. The 'Blacklist' checkbox is checked. Below it, there is a 'Blacklist proxy' field. The 'Blacklist URL' field contains the URL 'http://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfsense.tar.gz'. Below the URL field, there is a 'Save' button.

Click Save.

Then go to the Blacklist tab as shown below.

The screenshot shows the 'Blacklist Update' section. The 'Blacklist download progress' is shown as 51%. The 'Blacklist URL' field contains the same URL as before. Below the URL field, there are 'Download', 'Cancel', and 'Restore Default' buttons. Below these buttons, there is a 'Blacklist update Log' section showing the progress of the download.

Make sure the URL is displayed. Click Download.

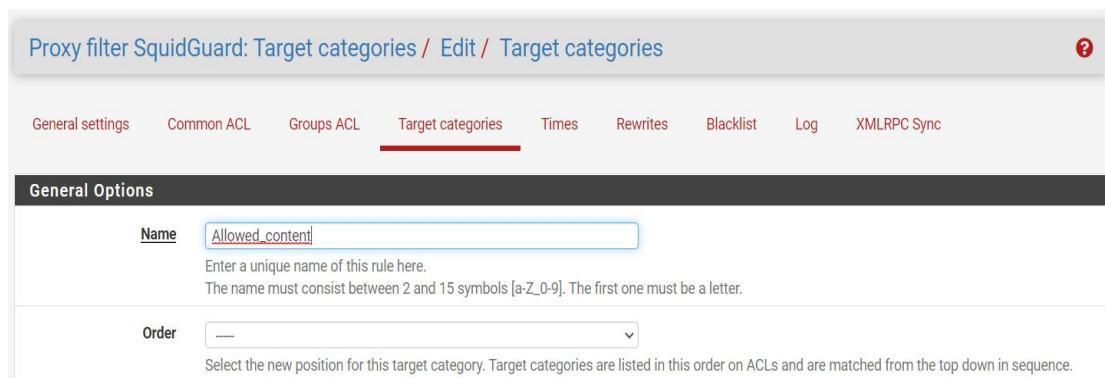
This will download the blacklist for URL filter.

Next go to Target categories.

The screenshot shows the 'Target categories' tab for the 'Proxy filter SquidGuard' package. The 'Target categories' section is empty, with columns for 'Name', 'Redirect', and 'Description'. There is a '+ Add' button and a 'Save' button.

Click Add.

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




Proxy filter SquidGuard: Target categories / Edit / Target categories

General settings Common ACL Groups ACL **Target categories** Times Rewrites Blacklist Log XMLRPC Sync

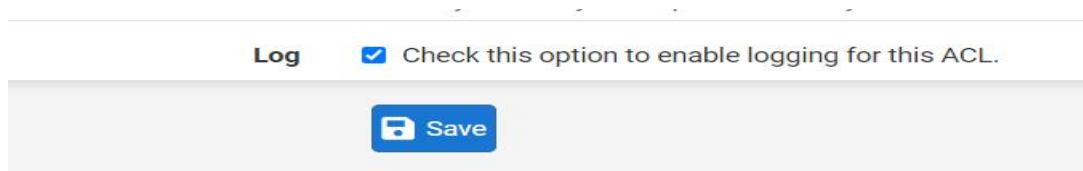
General Options

Name
Enter a unique name of this rule here.
The name must consist between 2 and 15 symbols [a-Z_0-9]. The first one must be a letter.


Order
Select the new position for this target category. Target categories are listed in this order on ACLs and are matched from the top down in sequence.



Click check box in front of Log.

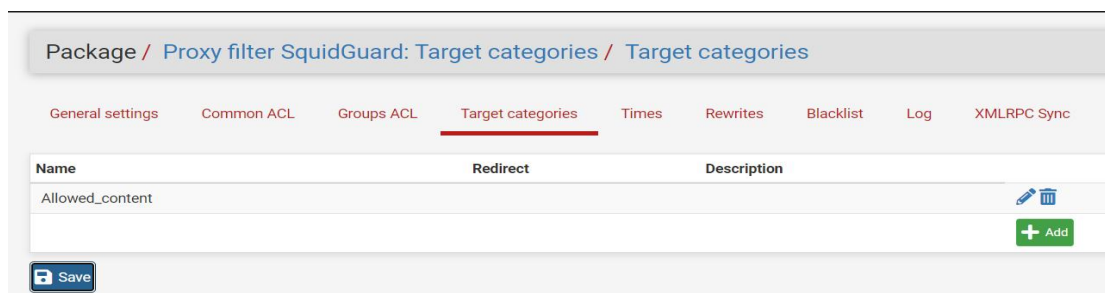


Log ☒ Check this option to enable logging for this ACL.



Click Save.



This will create the target category as shown below.



Package / Proxy filter SquidGuard: Target categories / Target categories

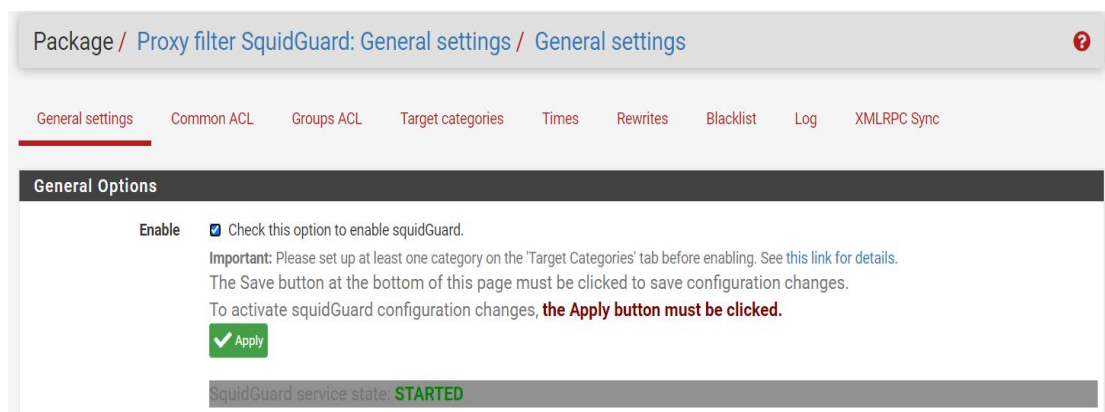
General settings Common ACL Groups ACL **Target categories** Times Rewrites Blacklist Log XMLRPC Sync

Name	Redirect	Description
Allowed_content		

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.




Package / Proxy filter SquidGuard: General settings / General settings

General settings **Common ACL** Groups ACL Target categories Times Rewrites Blacklist Log XMLRPC Sync

General Options

Enable ☒ Check this option to enable squidGuard.
Important: Please set up at least one category on the 'Target Categories' tab before enabling. See [this link for details](#).
The Save button at the bottom of this page must be clicked to save configuration changes.
To activate squidGuard configuration changes, **the Apply button must be clicked.**

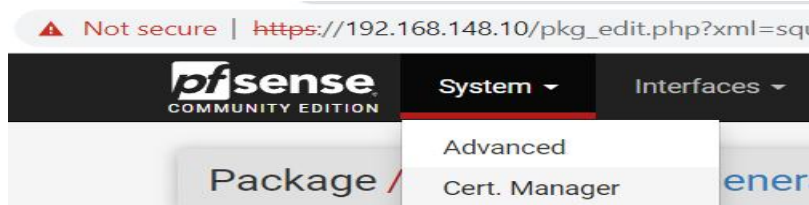


SquidGuard service state: **STARTED**

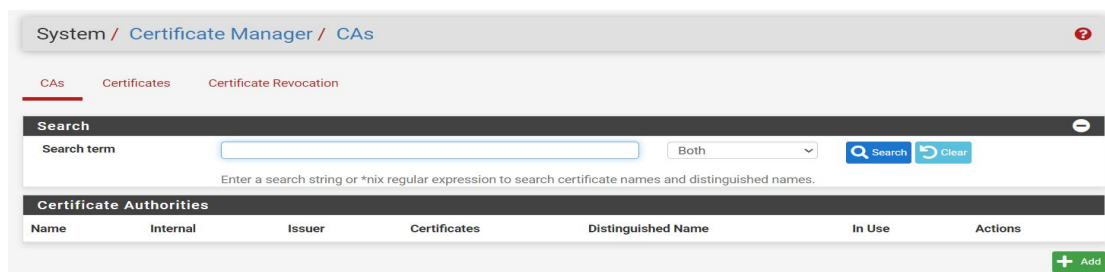
6. Configure SSL Man in the Middle.

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.

A screenshot of the pfSense web interface showing the 'Certificate Manager / CAs / Edit' page. The page has a 'Create / Edit CA' section with the following fields: 'Descriptive name' (demo-CA), 'Method' (Create an internal Certificate Authority), 'Trust Store' (checkbox), and 'Randomize Serial' (checkbox). Below this is the 'Internal Certificate Authority' section with the following fields: 'Key type' (RSA), 'Key length' (2048), and 'Digest Algorithm' (sha256). The page also has a 'System / Certificate Manager / CAs / Edit' breadcrumb and a red question mark icon.

Scroll Down.

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

Internal Certificate Authority

Key type: RSA

Key length: 2048
The length to use when generating a new RSA key, in bits.
The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.

Digest Algorithm: sha256
The digest method used when the CA is signed.
The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid.

Lifetime (days): 3650

Common Name: internal-ca

The following certificate authority subject components are optional and may be left blank.

Country Code: IN

State or Province: MH

City: PN

Organization: demo

Organizational Unit: labs

Save

Click Save.

System / Certificate Manager / CAs

CA's Certificates Certificate Revocation

Search

Search term: Both

Enter a search string or *nix regular expression to search certificate names and distinguished names.

Certificate Authorities						
Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
demo-CA	<input checked="" type="checkbox"/>	self-signed	0	ST=MH, OU=labs, O=demo, L=PN, CN=internal-ca, C=IN <small>Valid From: Mon, 14 Nov 2022 00:39:20 +0530 Valid Until: Thu, 11 Nov 2032 00:39:20 +0530</small>		

+ Add

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.

SSL Man in the Middle Filtering

HTTPS/SSL Interception ☒ Enable SSL filtering.

SSL/MITM Mode Splice Whitelist, Bump Otherwise
 The SSL/MITM mode determines how SSL interception is treated when 'SSL Man In the Middle Filtering' is enabled.
 Default: Splice Whitelist, Bump Otherwise. [Click Info for details.](#) ⓘ

SSL Intercept Interface(s) WAN
LAN
 The interface(s) the proxy server will intercept SSL requests on. Use CTRL + click to select multiple interfaces.

SSL Proxy Port
 This is the port the proxy server will listen on to intercept SSL while using transparent proxy. Default: 3129

SSL Proxy Compatibility Mode Modern
 The compatibility mode determines which cipher suites and TLS versions are supported. Default: Modern. [Click Info for details.](#) ⓘ

DHParams Key Size 2048 (default)
 DH parameters are used for temporary/ephemeral DH key exchanges and improve security by enabling the use of DHE ciphers.

CA demo-CA
 Select Certificate Authority to use when SSL interception is enabled. ⓘ

SSL Certificate Deamon Children
 This is the number of SSL certificate daemon children to start. May need to be increased in busy environments. Default: 5

Remote Cert Checks Accept remote server certificate with errors
Do not verify remote certificate
 Select remote SSL certificate checks to perform. Use CTRL + click to select multiple options.

Certificate Adapt Sets the "Not After" (setValidAfter)
Sets the "Not Before" (setValidBefore)
Sets CN property (setCommonName)
 See sslproxy_cert_adapt directive documentation and Mimic original SSL server certificate wiki article for details.

Logging Settings

Click Save.

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

Package / [Proxy Server: Authentication](#) / [Authentication](#)

[General](#) [Remote Cache](#) [Local Cache](#) [Antivirus](#) [ACLs](#) [Traffic Mgmt](#) [Authentication](#) [Users](#) [Real Time](#)

Squid Authentication General Settings

Authentication Method Local
 Select an authentication method. This will allow users to be authenticated by local or external services.

Click Save.

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

Package / [Proxy Server: Local Users](#) / [Users](#) ⓘ

[General](#) [Remote Cache](#) [Local Cache](#) [Antivirus](#) [ACLs](#) [Traffic Mgmt](#) [Authentication](#) [Users](#) [Real Time](#) [Status](#) [Sync](#)

Username	Description
+ Add	

[Save](#)

Click Add to add a new user.

[Proxy Server: Local Users](#) / [Edit](#) / [Users](#) ⓘ

[General](#) [Remote Cache](#) [Local Cache](#) [Antivirus](#) [ACLs](#) [Traffic Mgmt](#) [Authentication](#) [Users](#) [Real Time](#) [Status](#) [Sync](#)

Squid Local Users

Username
 Enter the username here.

Password
 Enter the password here.

Description
 You may enter a description here for your reference (not parsed).

[Save](#)

Provide Username , password , Description and Click Save.

