



INSTITUTE FOR ADVANCED COMPUTING
AND
SOFTWARE DEVELOPMENT
AKURDI, PUNE

DOCUMENTATION ON

**“Securing Networks with PfSense: A Comprehensive
Firewall Implementation ”**

PG-DITISS SEPT-2023

SUBMITTED BY

Group No: 05

Birajdar Mahesh Basappa (239409)

Kulkarni Pushpak Milind (239430)

MR. ROHIT PURANIK

CENTRE CO-ORDINATOR

MRS. SUSHMA HATTARKI

PROJECT GUIDE

ABSTRACT

This project aims to enhance the security and manageability of a network infrastructure through the implementation of various open-source technologies, namely pfSense, Captive Portal, Squid, SquidGuard, and DHCP service. The primary focus is to create a robust defense mechanism against unauthorized access, malicious activities, and content filtering within the network. The deployment of pfSense, an open-source firewall and router platform, forms the backbone of the security architecture. Through its intuitive interface and extensive feature set, pfSense offers granular control over network traffic, enabling administrators to define and enforce security policies effectively. The integration of Captive Portal functionality further fortifies the network by requiring users to authenticate before accessing the internet. This authentication mechanism enhances accountability and allows for the implementation of user-specific policies, ensuring compliance with organizational security standards. Squid, a caching proxy server, coupled with SquidGuard, a content filtering plugin, provides additional layers of security by inspecting and filtering web traffic based on predefined rulesets. This capability empowers administrators to mitigate threats posed by malicious websites, inappropriate content, and malware, thereby safeguarding the network integrity and protecting end-users from potential risks. Furthermore, the implementation of a DHCP service streamlines network management by automating the assignment of IP addresses and network configuration parameters to connected devices. This ensures seamless connectivity while facilitating efficient resource utilization and minimizing administrative overhead. Overall, this project demonstrates the efficacy of leveraging open-source technologies to establish a secure and well-managed network environment. By incorporating robust security measures and efficient network management practices, organizations can mitigate security risks, enhance productivity, and uphold the integrity of their network infrastructure effectively.

INDEX

1. INTRODUCTION	1
1.1 PROBLEM STATEMENT	2
1.2 ADVANTAGES	2
2. LITERATURE SURVEY	3
3. SURVEY OF TECHNOLOGY	4
4. REQUIREMENT & ANALYSIS	5
5. METHODOLOGY	6
5.1 PROPOSED SYSTEM	7
6. SYSTEM DESIGN	8
6.1 PROJECT SETUP	8
7. IMPLEMENTATION	10
8. FUTURE SCOPE	38
9. CONCLUSION	39
10. REFERENCES	40

1. INTRODUCTION

In today's interconnected world, web security is paramount for organizations to safeguard data and prevent cyber attacks. pfSense, an open-source firewall software, offers features like Snort, captive portal, DHCP service, Squid, and SquidGuard to detect and block threats, control user internet access, filter web content, and improve network performance. This project explores pfSense's practical implementation as a cost-effective and robust web traffic security solution, addressing challenges like budget constraints and evolving cyber threats. With Snort for intrusion detection, Captive Portal for authentication, DHCP for network management, and Squid/SquidGuard for content filtering, pfSense enhances defense, visibility, and control over web traffic. By creating a safer web environment, pfSense empowers organizations to protect data, maintain reputation, and ensure business continuity. This report delves into deployment steps, best practices, challenges, and impact on network performance and security posture, providing insights for organizations seeking to bolster web security with pfSense.

1.1 PROBLEM STATEMENT

Many IT employees , and peoples don't know about which sites are authorized and which are not , some peoples opens harmful sites in companys pc , laptops due to only this reason it is possible the malware were enter into the systems , through download for harmful sites and unauthorised sites , this project will overcome those issues and prevent comapanys sensitive info and data , this is very helpful for companies as well as day to day life users who uses internet ,

This is will detect attack from unauthorised users , or attackers , it will detect it and provide

the attackers ip address and block attacks form that ip address.

ADVANTAGES :

1. Robust firewall protection for network security.
2. SquidGuard powerful content filtering to enforce policies.
3. Real-time intrusion detection and prevention.
4. Bandwidth Management Efficient allocation and prioritization.
5. Captive Portal using user authentication for controlled access.
6. Centralized Management & Simplified administration from one interface.
7. Logging and Reporting using valuable insights into network activity

2. LITERATURE SERVERY

A literature server employing pfSense, SquidGuard, Snort, and Captive Portal ensures robust network security. pfSense acts as a firewall, safeguarding against unauthorized access. SquidGuard enables content filtering, restricting access to inappropriate websites. Snort provides real-time intrusion detection and prevention, enhancing threat detection capabilities. Captive Portal enforces user authentication, allowing controlled access to resources. This setup offers centralized management, streamlined administration, and logging/reporting functionalities for network activity analysis. With customizable configurations and community support, it ensures high availability and reliability, crucial for maintaining a secure literature server environment.

Furthermore, bandwidth management features optimize resource allocation, ensuring smooth server operation even during peak usage. The integration of these tools not only fortifies network defenses but also enhances performance and user accountability. This comprehensive solution aligns with industry best practices, providing a solid foundation for protecting sensitive literary assets and maintaining a secure and efficient literature server infrastructure.

3. SURVEY OF TECHNOLOGY

1. SNORT

Securing web traffic at the WAN interface 192.168.80.128 is crucial for organizations to prevent cyber attacks and protect sensitive data. One way to achieve this is by configuring snort using pfSense, an open-source firewall software. Snort is an intrusion detection system that monitors network traffic for potential security threats and alerts system administrators in real-time. By configuring snort on the WAN interface, organizations can detect and block potential security threats at the network perimeter, enhancing their overall security posture. In this way, pfSense provides a powerful and effective solution for securing web traffic at the WAN interface and protecting organizations against cyber threats.

2. Squid

Squid is designed to improve the speed and efficiency of web browsing by caching frequently accessed web pages and serving them from memory instead of fetching them from the internet every time a user requests them.

3. Squid Guard

Squid-Guard is highly configurable, enabling administrators to define policies based on a wide range of criteria, including website URLs, domains, IP addresses, and keywords. In addition to content filtering, Squid-Guard can also be used to authenticate users and restrict access to certain parts of the internet based on their identity, location, or device. This makes it a powerful tool for protecting the organization's network from external threats and enforcing internal policies.

4. REQUIREMENT ANALYSIS

Hardware:

- ▶ Machine With Minimum Requirement:
 - ▶ Processor: Intel Core i3 or equivalent processor with at least 2 cores
 - ▶ Memory: At least 4GB RAM for small to medium-sized organizations, and 8GB or more for larger organizations.
 - ▶ Storage: At least 20GB of free disk space on the hard drive or SSD.
 - ▶ Network Interface Cards (NICs): At least two NICs, one for the WAN and one for the LAN.
 - ▶ Virtualization Platform: VMware vSphere or VMware Workstation, with the appropriate licenses for the number of virtual machines required.

Software :

- VM-ware Workstation
- pfSense OS
- Windows OS 10 or Latest
- 7-zip File Extractor

5. METHEDODOLOGY

The methodology leveraging pfSense, SquidGuard, Snort, and Captive Portal involves a systematic approach to network security and access control. Initially, pfSense is deployed as the primary firewall solution, establishing perimeter defense and regulating traffic flow. SquidGuard is then integrated to enforce content filtering policies, restricting access to undesirable websites based on predefined rules. Subsequently, Snort is implemented to provide intrusion detection and prevention capabilities, monitoring network traffic for suspicious activity and blocking potential threats in real-time. Captive Portal is employed to enforce user authentication, requiring individuals to authenticate before accessing network resources, thereby ensuring controlled access and accountability.

This methodology emphasizes customization to align security measures with specific organizational requirements and risk profiles. Administrators configure rulesets within each component to address the unique security needs of the environment, such as blocking malicious URLs, detecting unauthorized access attempts, and enforcing user access policies. Continuous monitoring and analysis of network logs and reports generated by these integrated solutions facilitate proactive threat mitigation and performance optimization. Regular updates and community support ensure the ongoing effectiveness and resilience of the security infrastructure, ultimately safeguarding the network against evolving cyber threats while maintaining operational efficiency.

5.1 Proposed Systems

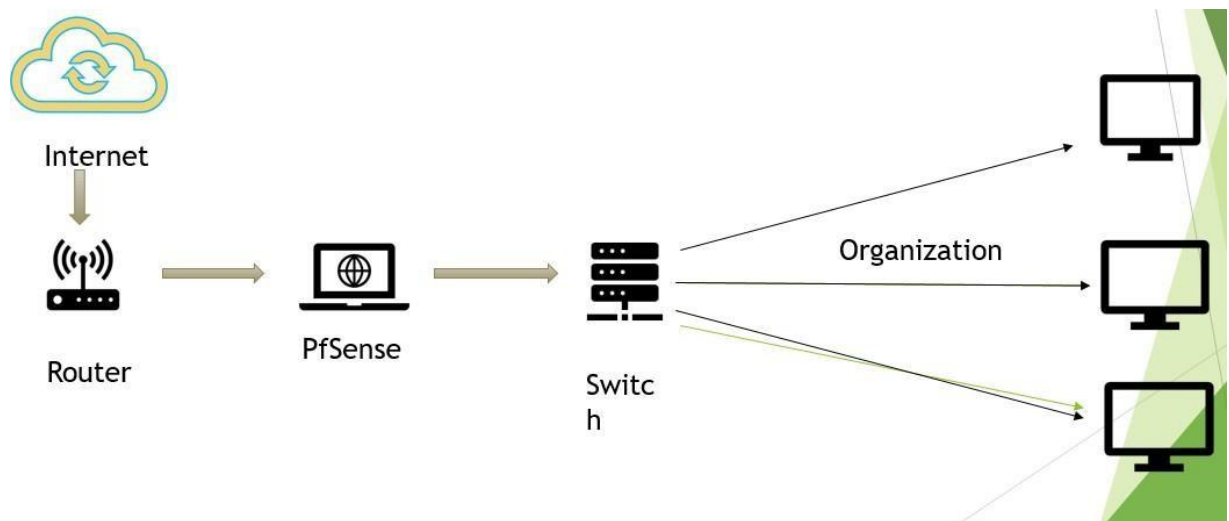
The proposed system integrates pfSense, SquidGuard, Snort, and Captive Portal to establish a robust and comprehensive network security infrastructure. pfSense serves as the core firewall solution, providing perimeter defense and traffic management capabilities. SquidGuard enhances security by implementing content filtering policies, restricting access to inappropriate or harmful websites.

Snort, an intrusion detection and prevention system, monitors network traffic for suspicious activity and blocks potential threats in real-time. Captive Portal ensures controlled access to network resources by enforcing user authentication, thereby enhancing accountability and preventing unauthorized access.

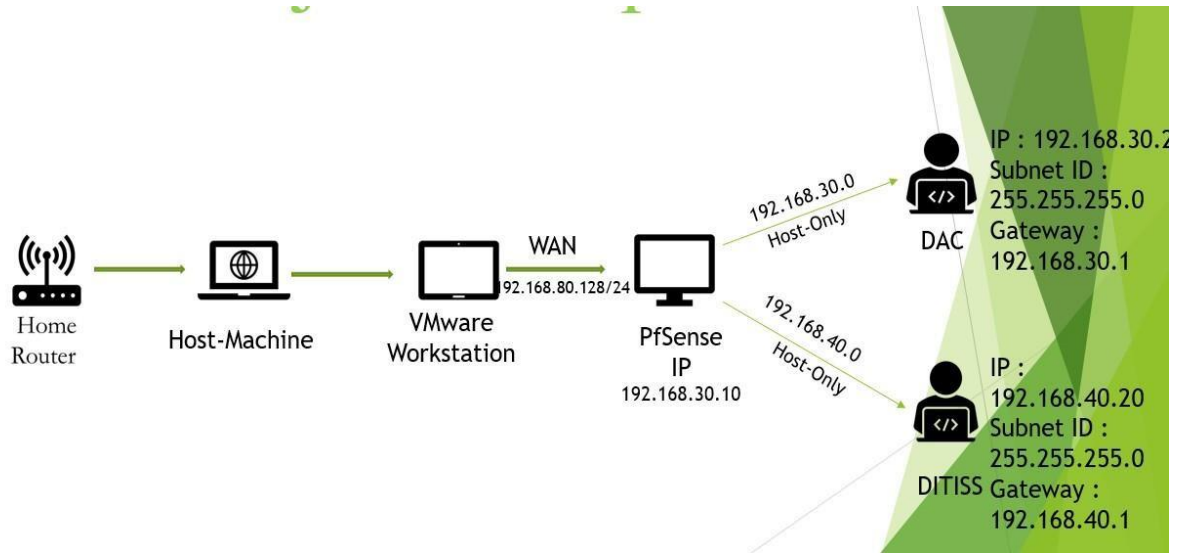
This system offers centralized management and configuration, simplifying administration tasks and providing a unified interface for monitoring and reporting network activities. Customization options allow organizations to tailor security measures to their specific needs, while continuous updates and community support ensure the ongoing effectiveness and adaptability of the security infrastructure. Overall, the proposed system provides comprehensive protection against a wide range of cyber threats while maintaining network performance and integrity.

6. SYSTEM DESIGN

1. BLOCK DIAGRAM



6.1 PROJECT SETUP



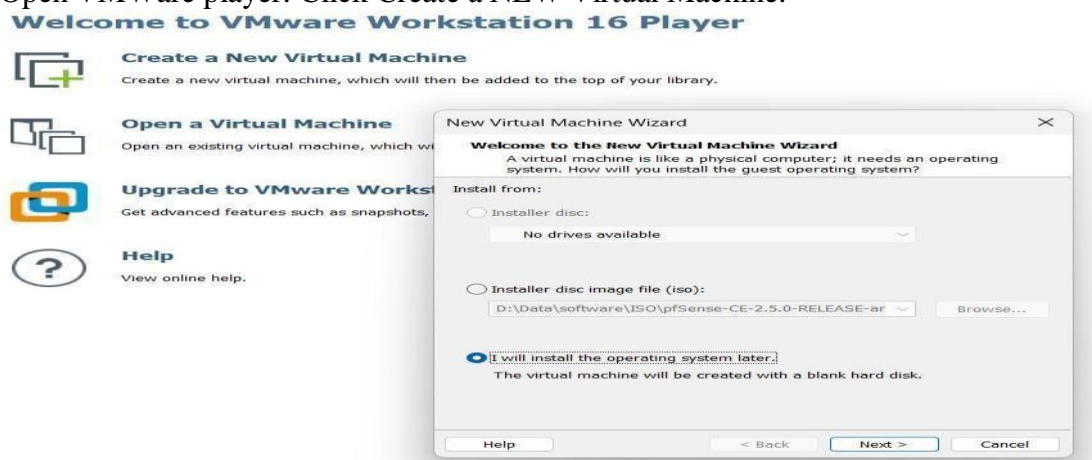
7. IMPLEMENTATION

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.

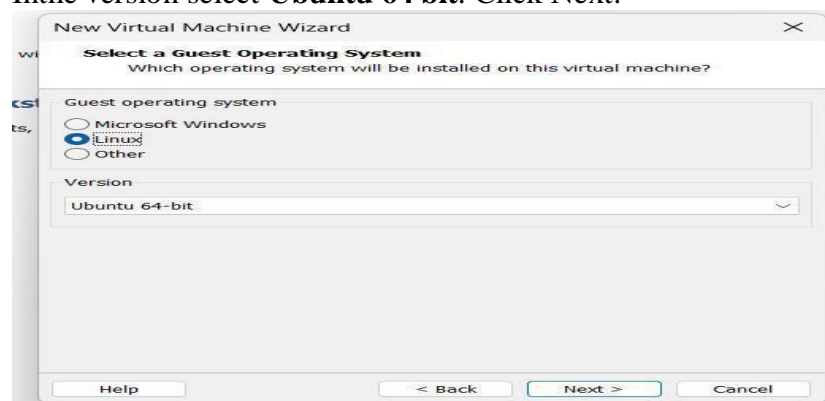
1. Creating a virtual machine in VMWare player and install pfSense.

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.

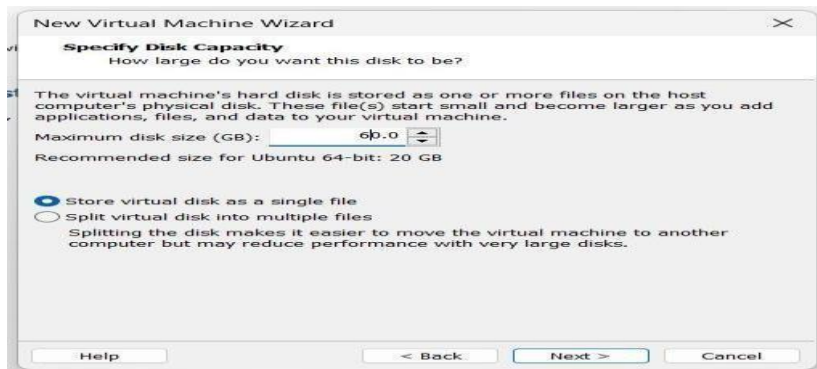


On the next window provide a name for the virtual machine. Also provide a path to store the virtual machine files.

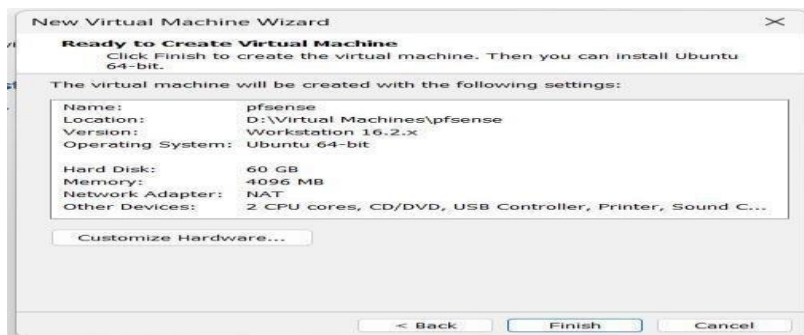


Click Next.

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



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



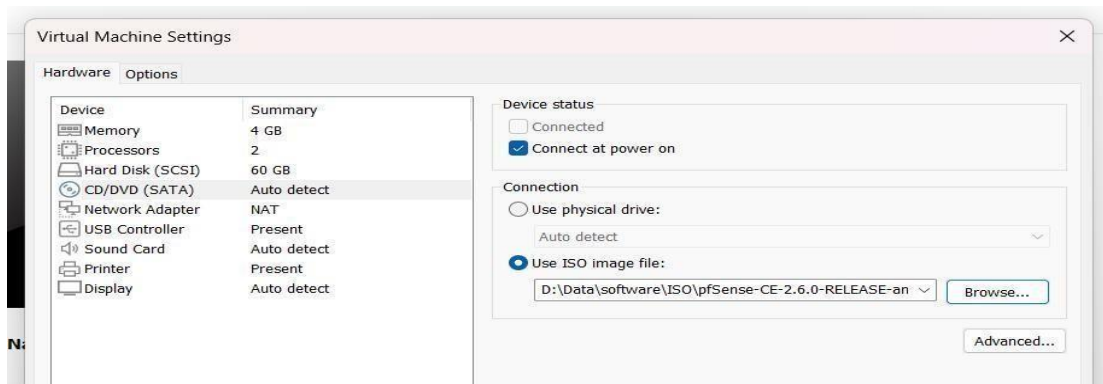
Click Finish to create the virtual machine. The virtual machine is shown as below.



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.

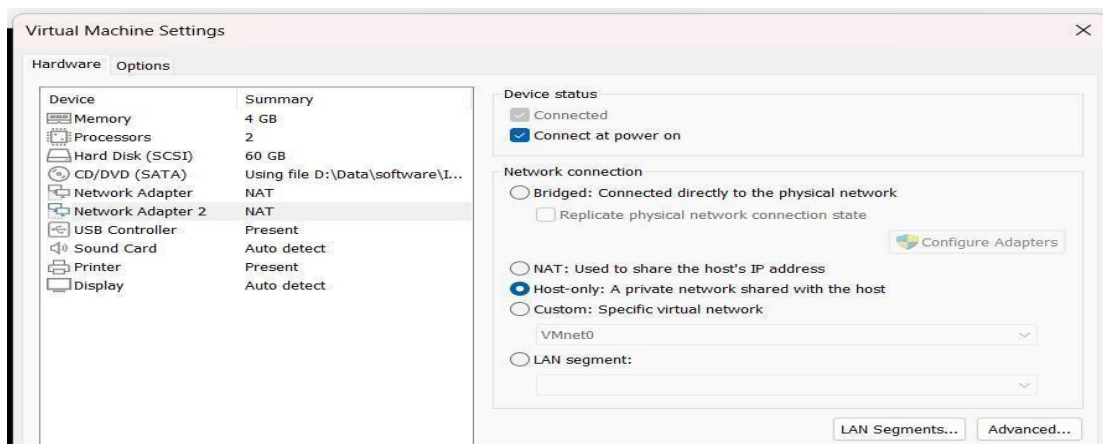
This is shown in the following image.



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.

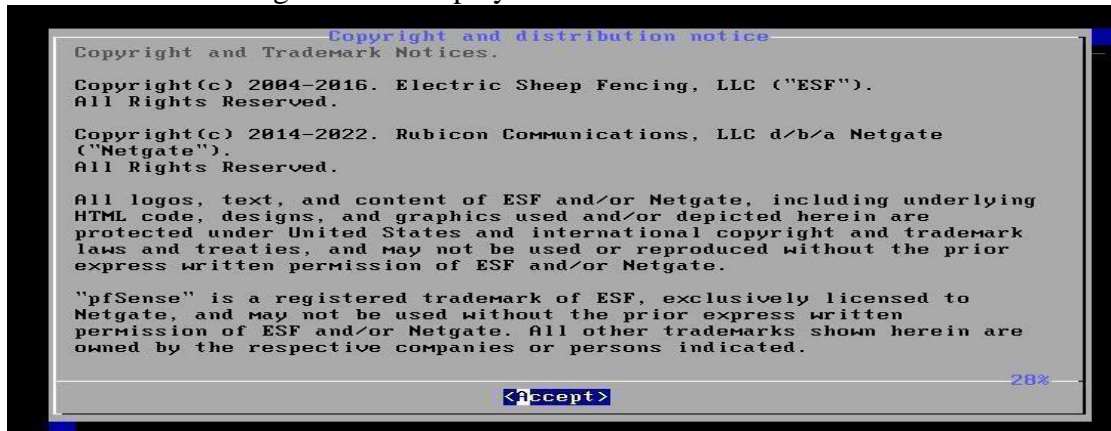


Click OK to close the settings window. Then Click the green arrow in the menu bar or click Play virtual machine option.



The Virtual machine will start and the pfSense installation begins.

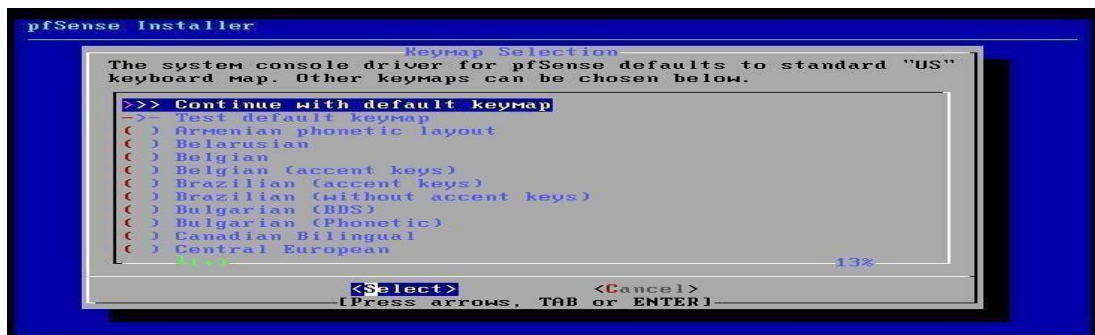
Wait till the following screen is displayed.



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.



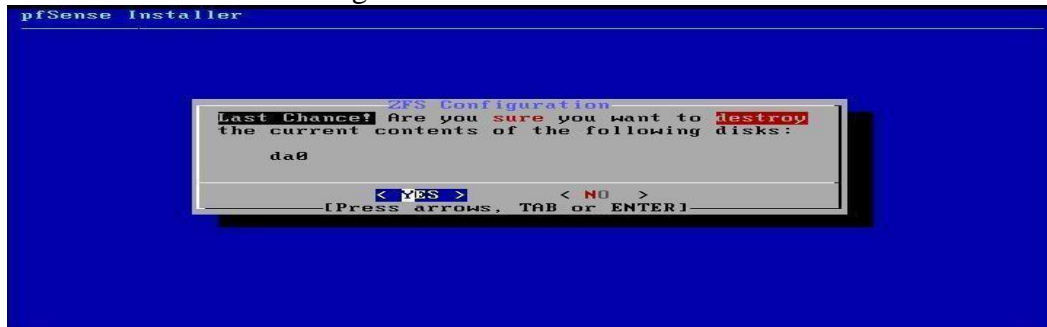
On the next screen again press Enter to continue with the default **stripe** option.



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.

```
Enter an option: arprequest: cannot find matching address

FreeBSD/amd64 (pfSense.home.arp) (ttyv0)
VMware Virtual Machine - Netgate Device ID: 609e95ab1164ad01e0fd
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

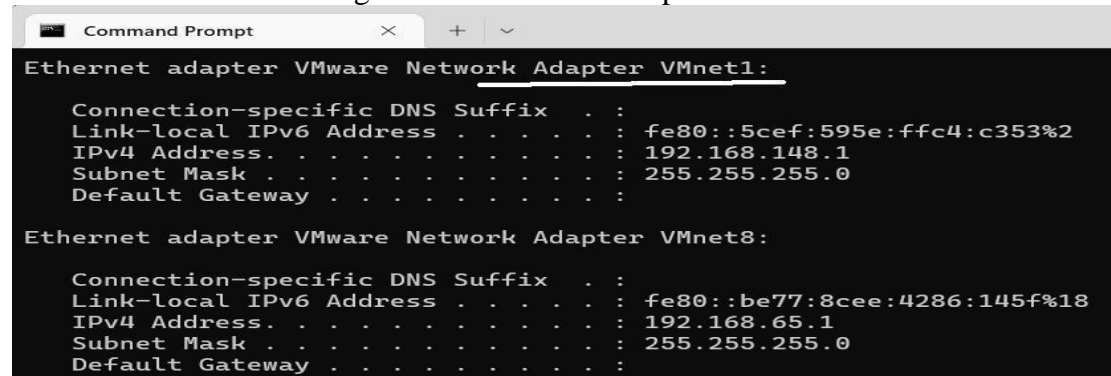
WAN (wan)      -> em0      ->
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

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: █
```

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:

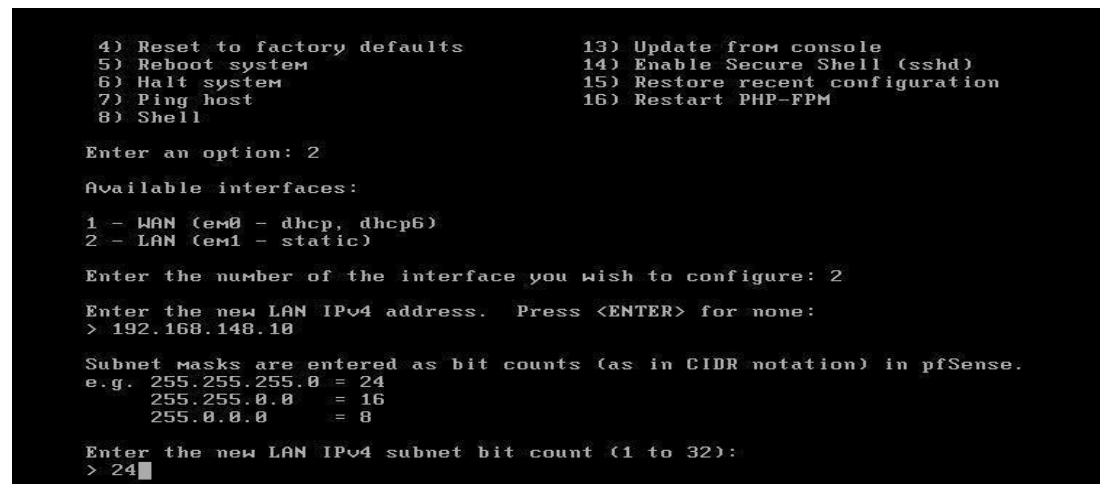
Connection-specific DNS Suffix . : 
Link-local IPv6 Address . . . . . : fe80::5cef:595e:ffc4:c353%2
IPv4 Address. . . . . : 192.168.148.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 

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

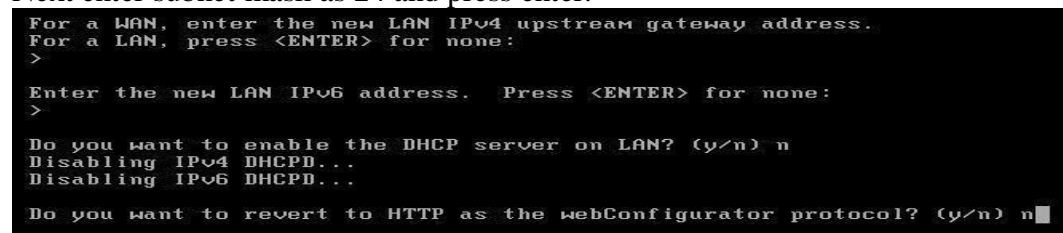
```

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

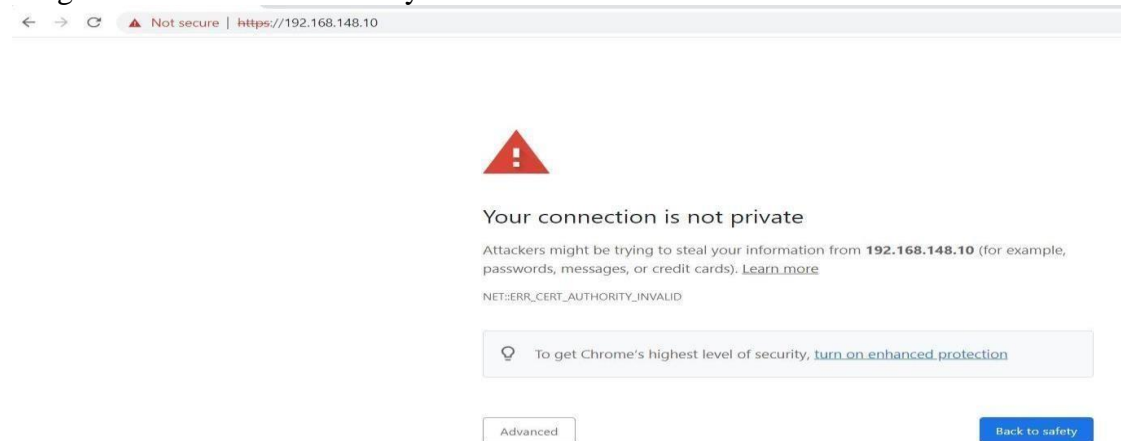
```

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.

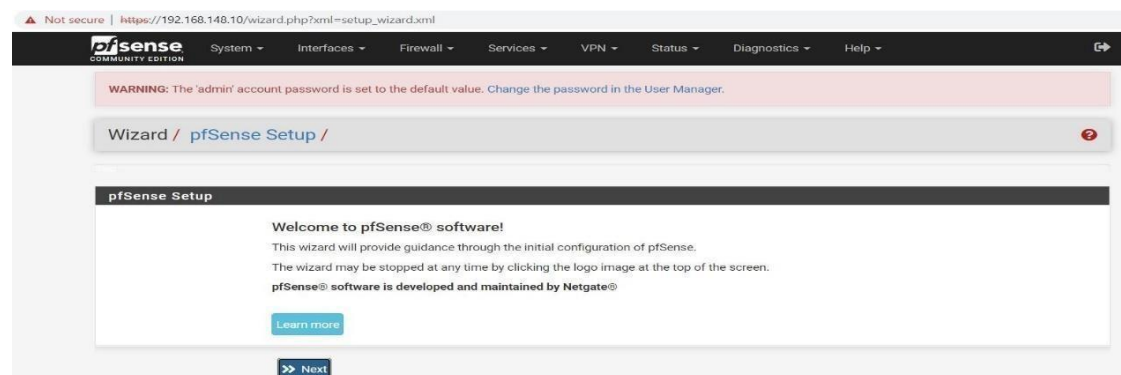
Type n on the next prompt. This will not revert the webConfigurator to HTTP. Thus we can access the pfSense web console using HTTPS. Thus the LAN IP address is configured.

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

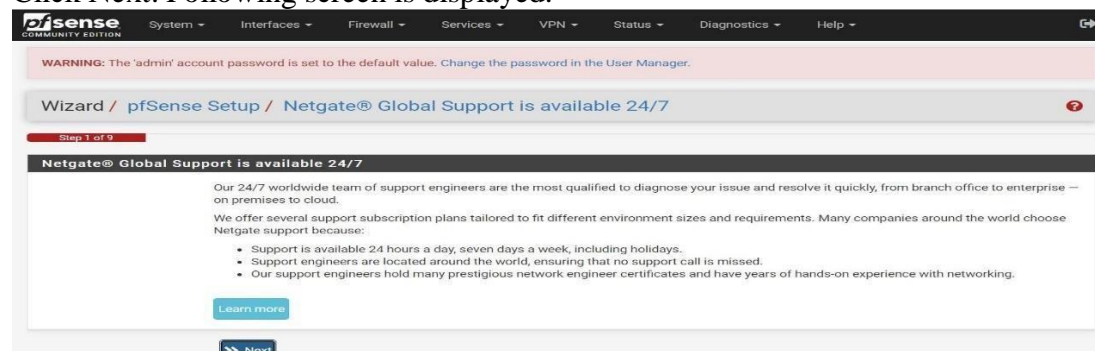
On this VM open the browser and type <https://IP-of-pfSense-LAN> . Following warning will be displayed. This is because the certificate issued by pfSense is selfgenerated and not trusted by the browser.



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.

Step 2 of 9

General Information

On this screen the general pfSense parameters will be set.

Hostname:
EXAMPLE: myserver

Domain:
EXAMPLE: mydomain.com

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:

Secondary DNS Server:

Override DNS: ☒
Allow DNS servers to be overridden by DHCP/PPP on WAN

[Next](#)

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

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

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:
Enter the hostname (FQDN) of the time server.

Timezone:

[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.

Wizard / pfSense Setup / Configure WAN Interface

Step 4 of 9

Configure WAN Interface

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

SelectedType:

General configuration

MAC Address:
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.

MTU:
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.

MSS:
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.

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

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

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

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

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 nextscreen.

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

Wizard / pfSense Setup / Reload configuration

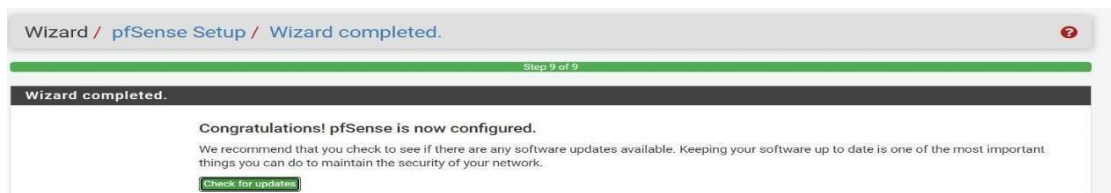
Step 7 of 9

Reload configuration

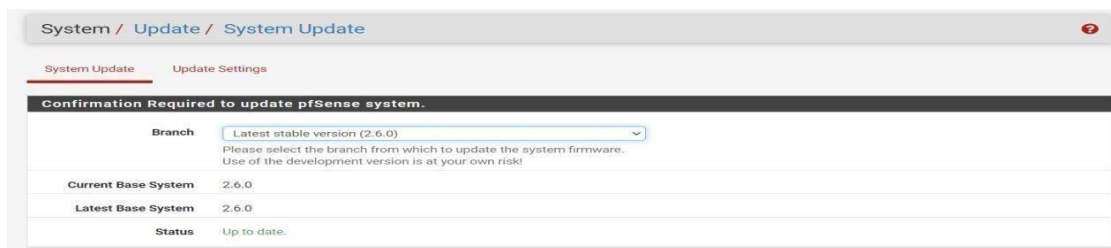
Click 'Reload' to reload pfSense with new changes.

[Reload](#)

On the next screen click check for updates.



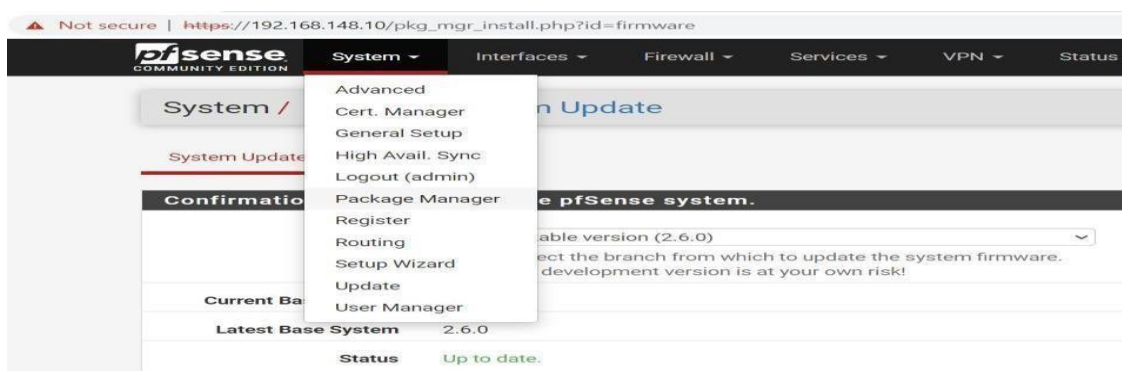
If any updates are present, then it will download the updates. It may take time based on update size and the internet speed.



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.

System / Package Manager / Available Packages

Installed Packages Available Packages

Search

Search term: squid Both Search Clear

Enter a search string or *nix regular expression to search package names and descriptions.

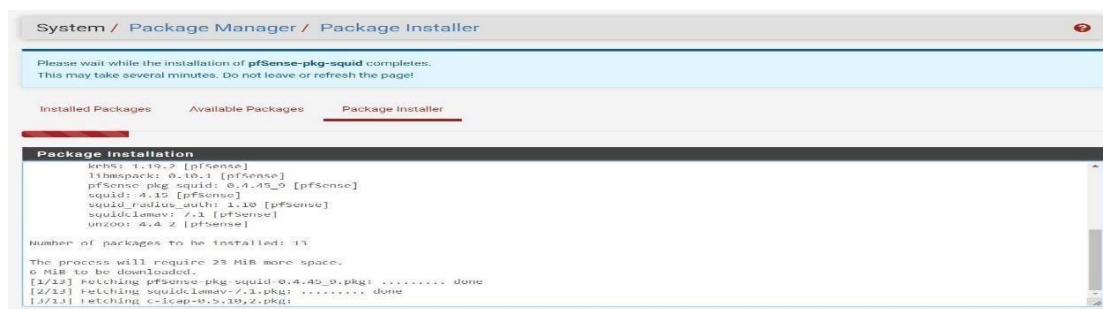
Packages

Name	Version	Description	
LightSquid	3.0.6_9	LightSquid is a high performance web proxy reporting tool. Includes proxy realtime statistics (SQStat). Requires Squid package.	+ Install
		Package Dependencies: lighttpd-1.4.63 lightsquid-1.8_5	
squid	0.4.45_9	High performance web proxy cache (3.5 branch). It combines Squid as a proxy server with its capabilities of acting as a HTTP / HTTPS reverse proxy. It includes an Exchange-Web Access (OWA) Assistant, SSL filtering and antivirus integration via C-ICAP.	+ Install
		Package Dependencies: squidclamav-7.1 squid_radius_auth-1.10 squid-4.15 c-icap-modules-0.5.5	
squidGuard	1.16.18_20	High performance web proxy URL filter.	+ Install
		Package Dependencies: squidguard-1.4_15 pfSense-pkg-squid-0.4.45_9	

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



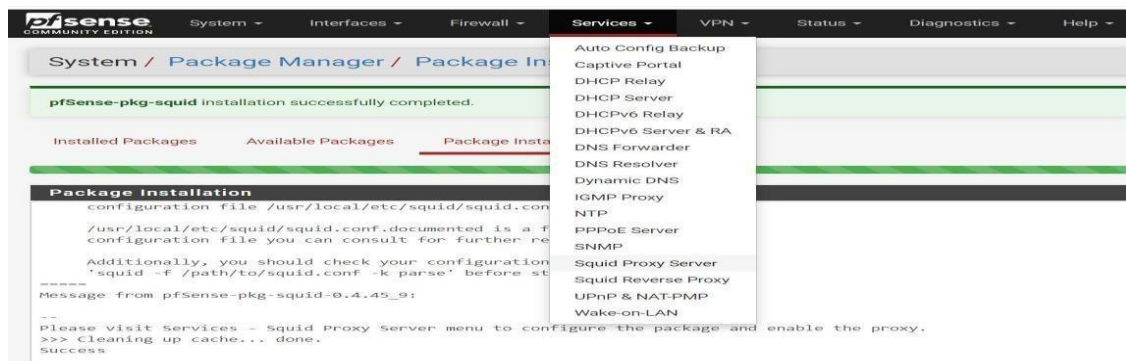
Click Confirm. The following screen will appear. It shows the Squid installation progress.



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 SquidProxy Server.



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

Package / Proxy Server: Cache Management / Local Cache

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

Squid Cache General Settings

Disable Caching	<input type="checkbox"/> Disable caching completely. This may be required if Squid is only used as a proxy to audit website access.
Cache Replacement Policy	<div>Heap LFUDA</div> <div>The cache replacement policy decides which objects will remain in cache and which objects are replaced to create space heap LFUDA ⓘ</div>
Low-Water Mark in %	<div>90</div> <div>The low-water mark for AUFS/UFS/diskd cache object eviction by the cache_replacement_policy algorithm. ⓘ</div>
High-Water Mark in %	<div>95</div> <div>The high-water mark for AUFS/UFS/diskd cache object eviction by the cache_replacement_policy algorithm. ⓘ</div>

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 ☒ Check to enable the Squid proxy.
Important: If unchecked, ALL Squid services will be disabled and stopped.

Keep Settings/Data ☒ 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 ☒ 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
Defines how many days of logfiles will be kept. Rotation is disabled if left empty.

Log Pages Denied by SquidGuard ☐ Makes it possible for SquidGuard denied log to be included on Squid logs.
Click Info for detailed instructions. [i](#)

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.

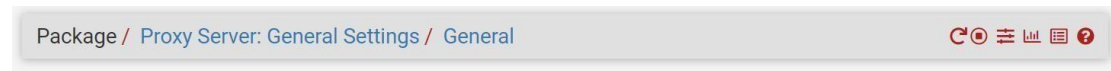
X-Forwarded Header Mode (on)
Choose how to handle X-Forwarded-For headers. Default: on [i](#)

Disable VIA Header ☐ 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 [i](#)

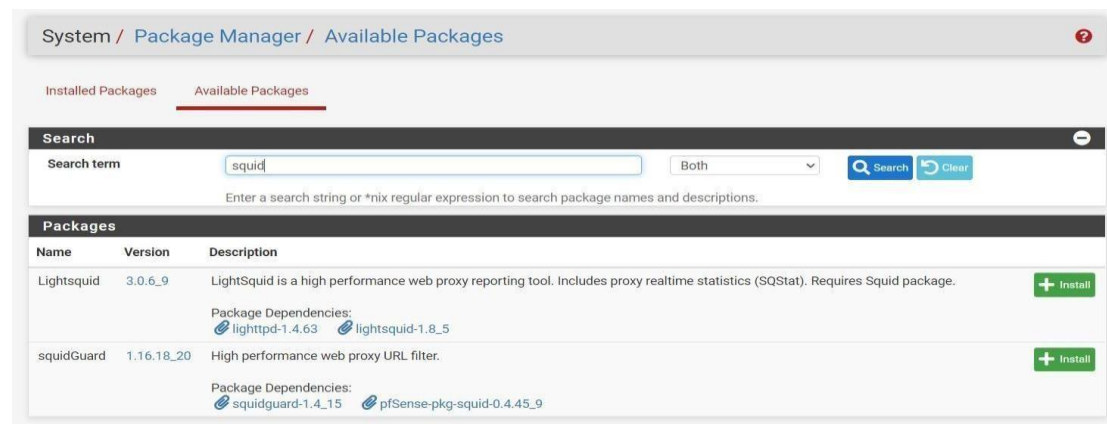
Scroll to the end. Click Save. This will start the squid proxy service.

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

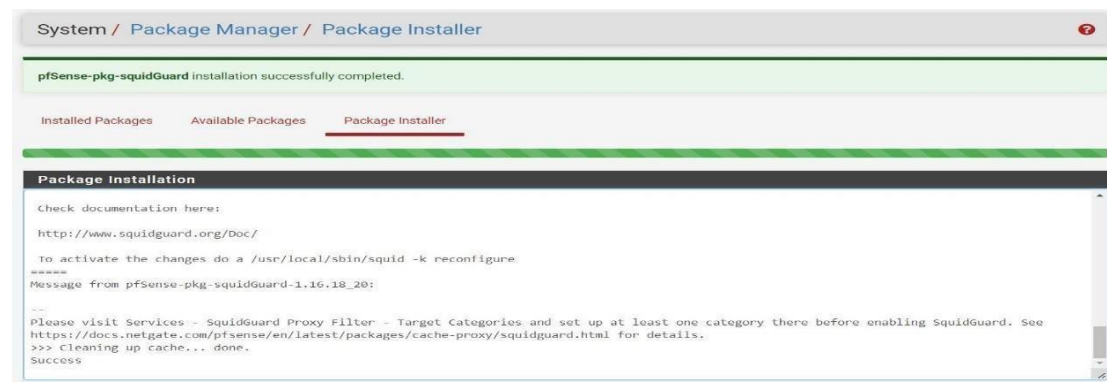


4. Install Squidguard

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.

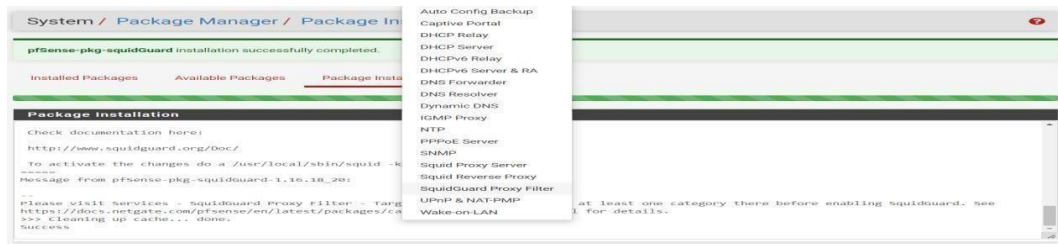


Click Confirm on the next screen . This will start Squidguard installation. Once the installation is complete following screen is displayed.



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.

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: **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

Blacklist options

Blacklist ☒ Check this option to enable blacklist

Blacklist proxy

Blacklist upload proxy - enter here, or leave blank.
 Format: host[:port login:pass] . Default proxy port 1080.
 Example: '192.168.0.1:8080 user:pass'

Blacklist URL
 Enter the path to the blacklist (blacklist.tar.gz) here. You can use FTP, HTTP or LOCAL URL blacklist archive or leave blank. The LOCAL path could be your pfsense (/tmp/blacklist.tar.gz).

Click Save.

Then go to the Blacklist tab as shown below.

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

Blacklist Update

Blacklist download progress

51 %

Enter FTP or HTTP path to the blacklist archive here.

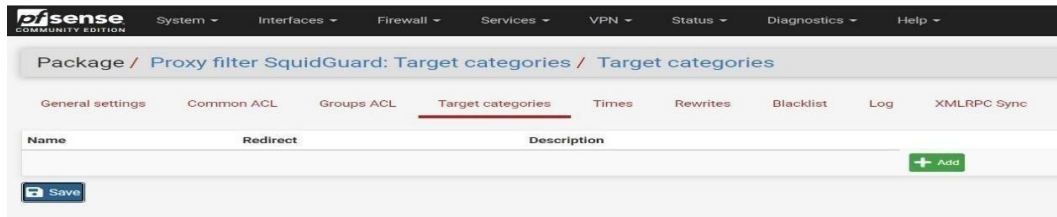
Blacklist update Log

```

Begin blacklist update
Start download.
Download archive http://dsi.ut-
capitole.fr/blacklists/download/blacklists_for_pfsense.tar.gz
Completed 51 %
  
```

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.

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.**

☒ Apply

SquidGuard service state:

STARTED

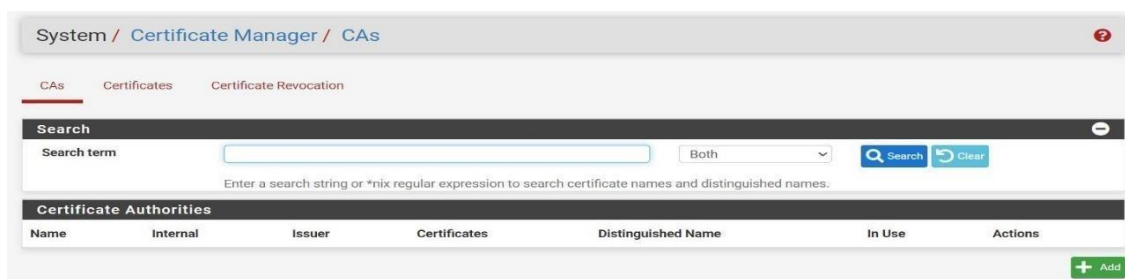
6. Configure SSL Man in the Middle.

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, specifically the 'Certificate Manager / CAs / Edit' page. The page has a breadcrumb trail 'System / Certificate Manager / CAs / Edit'. Below the breadcrumb, there are tabs for 'CAs', 'Certificates', and 'Certificate Revocation'. The 'CAs' tab is selected. The main content area is titled 'Create / Edit CA'. It contains several form fields: 'Descriptive name' (set to 'demo-CA'), 'Method' (set to 'Create an internal Certificate Authority'), 'Trust Store' (checkbox 'Add this Certificate Authority to the Operating System Trust Store' is unchecked), and 'Randomize Serial' (checkbox 'Use random serial numbers when signing certificates' is unchecked). Below these fields, there is a section titled 'Internal Certificate Authority' with 'Key type' (set to 'RSA'), 'Key length' (set to '2048'), and 'Digest Algorithm' (set to 'sha256').

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.

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 Valid From: Mon, 14 Nov 2022 00:39:20 +0530 Valid Until: Thu, 11 Nov 2032 00:39:20 +0530	<input type="checkbox"/>	Edit Refresh Reset Delete

+ 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 Daemon 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

8. FUTURE SCOPE

The future scope of pfSense, SquidGuard, Snort, and Captive Portal lies in their continued evolution to address emerging cybersecurity challenges. Advancements in artificial intelligence and machine learning will enable these integrated solutions to enhance threat detection capabilities, enabling more proactive and adaptive responses to evolving cyber threats. Additionally, there will be a greater focus on integrating these tools with cloud-native architectures, enabling seamless deployment and management of security policies across distributed and hybrid cloud environments. This will facilitate scalability and agility in adapting to changing network infrastructures. Furthermore, with the increasing adoption of Internet of Things (IoT) devices and the proliferation of remote work, there will be a need for enhanced network visibility and control. Future developments may include features for IoT device management, advanced user behavior analytics, and seamless integration with identity and access management solutions.

Overall, the future of pfSense, SquidGuard, Snort, and Captive Portal holds promise for delivering robust, scalable, and adaptive cybersecurity solutions to meet the evolving needs of modern networks.

9. CONCLUSION

The integration of pfSense, SquidGuard, Snort, and Captive Portal offers a comprehensive approach to network security, content filtering, intrusion detection, and user authentication. With customizable configurations, centralized management, and future-ready adaptability, this unified solution ensures robust protection, optimal performance, and streamlined administration in modern network environments.

10. REFERENCES

- <https://docs.netgate.com/pfsense/en/latest/>
- <https://www.snort.org/>
- <https://docs.netgate.com/pfsense/en/latest/packages/cache-proxy/squidguard.html>
- <https://docs.netgate.com/pfsense/en/latest/packages/snort/setup.html>
- https://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfsense.tar.gz