

**PROJECT REPORT ON**  
**Blocking a Domain using**  
**pfSense**



**REPORTED BY:**

**VISHNU P V**

**TO INSTRUCTOR: ALAN SHERI**

**CICSA**



**RED TEAM HACKER ACADEMY**

# ACKNOWLEDGEMENT

We would like to express our sincere gratitude to everyone who supported us in the completion of this project.

We extend our heartfelt thanks to our supervisor, Alan Sheri for his guidance and invaluable feedback throughout this project.

We would also like to thank Red Team Hackers Academy for providing the necessary resources and a supportive environment that enabled us to complete this project successfully.

Thank you to everyone involved for your support and contributions. This project would not have been possible without the contributions of everyone mentioned, and I am truly appreciative of their efforts and dedication.

# ABSTRACT

Network security and traffic control are critical aspects of maintaining a secure and efficient organizational environment. pfSense, an open-source firewall and router solution, provides advanced capabilities for managing network traffic, enforcing policies, and protecting against unauthorized access. This project focuses on setting up and configuring pfSense to block access to a specific domain from within a virtual LAN network.

The project involves deploying pfSense in a virtualized environment, creating and configuring a virtual LAN, and implementing firewall rules to restrict access to unwanted domains. Through careful configuration of pfSense DNS Resolver/Forwarder and firewall policies, the project demonstrates how domain-based blocking can be effectively applied to control user activity and safeguard network resources.

The primary goal is to illustrate how pfSense can be used to enforce domain restrictions at the firewall level, thereby preventing access to potentially harmful or distracting websites from connected client systems. By implementing domain blocking, the project enhances security, improves productivity, and reduces the risks associated with malicious or suspicious domains.

This practical implementation highlights pfSense as a reliable, customizable, and cost-effective firewall solution for administrators aiming to strengthen network controls within virtualized test environments as well as real-world enterprise networks.

# TABLE OF CONTENT

<b>INTRODUCTION.....</b>	<b>1</b>
<b>OBJECTIVE.....</b>	<b>1</b>
<b>PREREQUISITE.....</b>	<b>2</b>
I.    HARDWARE .....	2
II.   SOFTWARE .....	2
<b>PROCEDURES .....</b>	<b>3</b>
I.    SETTING UP pfSENSE .....	3
II.   CREATING FIREWALL RULES TO BLOCK A SPECIFIC DOMAIN.....	5
<b>CONCLUSION.....</b>	<b>10</b>
<b>REFERENCES.....</b>	<b>10</b>
<b>CONTRIBUTIONS.....</b>	<b>11</b>

# INTRODUCTION

Network security plays a pivotal role in protecting organizational resources and ensuring operational efficiency. Firewalls serve as the first line of defense by controlling incoming and outgoing network traffic based on defined security policies. pfSense, an open-source firewall platform, offers robust routing and firewall capabilities suitable for enterprise and virtual environments. This project focuses on deploying pfSense as a firewall solution to block access to a specific domain within a virtual LAN (VLAN) setup, illustrating how network administrators can enforce domain-level restrictions to enhance security and productivity.

## OBJECTIVES

1. To set up pfSense firewall in a virtualized environment supporting VLANs.
2. To configure the virtual LAN network for client devices.
3. To implement firewall and DNS rules in pfSense that block access to a specified domain.
4. To validate and test the domain blocking functionality ensuring clients cannot reach the targeted domain.

By the end of this project, administrators will be able to configure pfSense to reliably block access to chosen domains from within a VLAN, establishing improved control over user web activity and safeguarding the network against risky or non-compliant resources.

## PREREQUISITE

### HARDWARE

A system with the following minimum configurations:

- **Processor:** 64-bit amd64 (x86-64) compatible CPU, 600 MHz or faster (modern Intel Core i5 processors or equivalent recommended for smooth performance).
- **RAM:** 1 GB or more (2 GB or more recommended for better virtualized pfSense performance).
- **Storage:** 8 GB or larger disk space (SSD recommended) allocated for pfSense virtual machine.
- **Network:** At least two network interfaces required; VirtualBox adapters configured as NAT for WAN and Host-only/Internal Network for LAN simulation. Stable internet connectivity on the host system.

### SOFTWARE

The following software are used for this project. Exact versions are not mandatory to complete the objective:

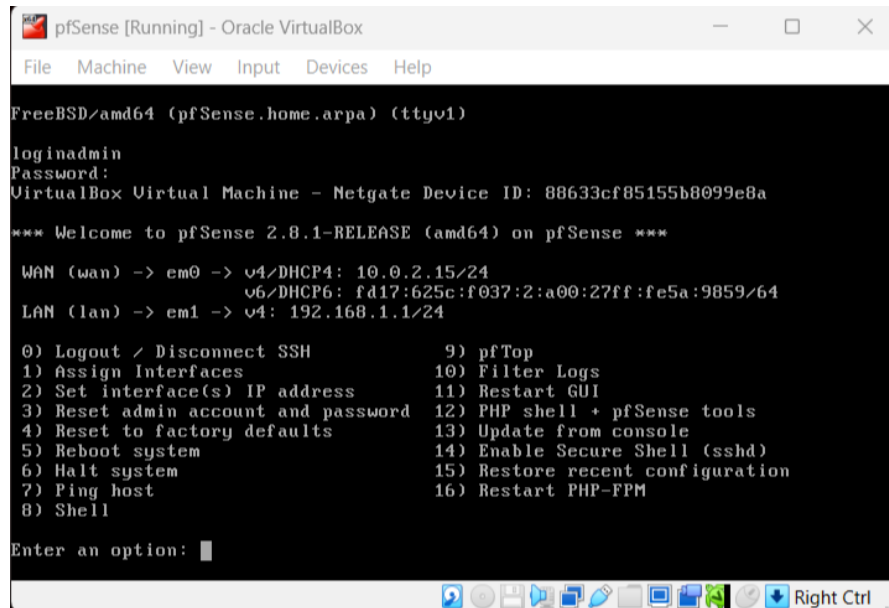
- **Windows 10:** Operating system running on the virtual machine that manages the virtualized lab environment.
- **Oracle VirtualBox:** Virtualization software used to create and manage a virtual machine hosting pfSense firewall/router.
- **pfSense:** Open-source firewall and routing platform installed as a virtual machine in VirtualBox, providing network security and routing functions within the lab setup.

# PROCEDURES

## SETTING UP pfSense

### Step 1:

Start pfSense machine on virtual Box:

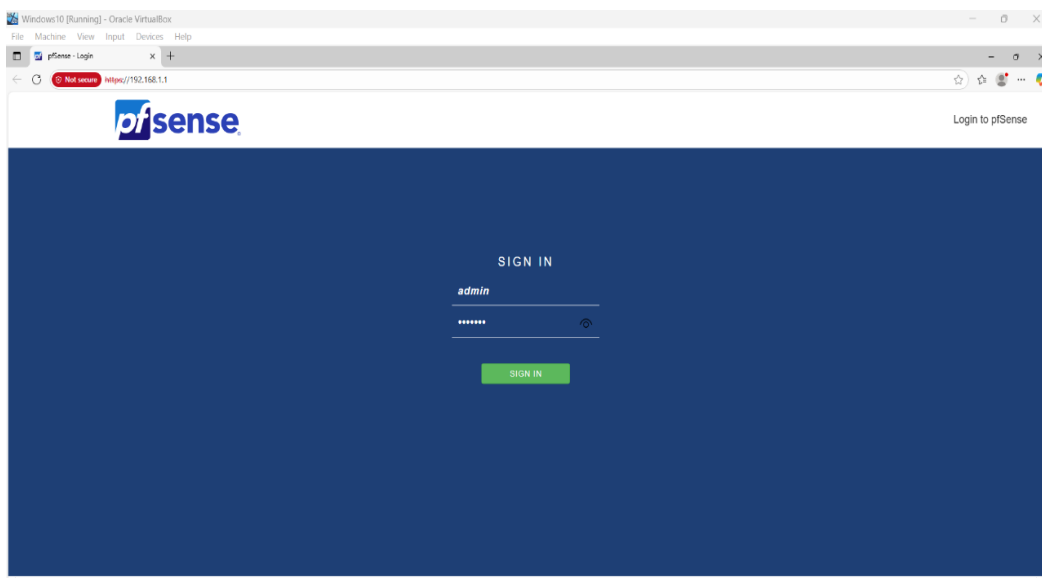
A screenshot of a terminal window titled 'pfSense [Running] - Oracle VirtualBox'. The window shows the pfSense login prompt 'loginadmin' and 'Password:'. Below the password prompt, it displays 'VirtualBox Virtual Machine - Netgate Device ID: 88633cf85155b8099e8a'. A welcome message '\*\*\* Welcome to pfSense 2.8.1-RELEASE (amd64) on pfSense \*\*\*' is shown. Network configuration is displayed: 'WAN (wan) -> em0 -> v4/DHCP4: 10.0.2.15/24' and 'v6/DHCP6: fd17:625c:f037:2:a00:27ff:fe5a:9859/64', and 'LAN (lan) -> em1 -> v4: 192.168.1.1/24'. A list of 16 options is shown, including 'Logout / Disconnect SSH', 'Assign Interfaces', 'Set interface(s) IP address', 'Reset admin account and password', 'Reset to factory defaults', 'Reboot system', 'Halt system', 'Ping host', 'Shell', 'pfTop', 'Filter Logs', 'Restart GUI', 'PHP shell + pfSense tools', 'Update from console', 'Enable Secure Shell (sshd)', 'Restore recent configuration', and 'Restart PHP-FPM'. The prompt 'Enter an option:' is at the bottom.

```
FreeBSD/amd64 (pfSense.home.arp) (ttyv1)
loginadmin
Password:
VirtualBox Virtual Machine - Netgate Device ID: 88633cf85155b8099e8a
*** Welcome to pfSense 2.8.1-RELEASE (amd64) on pfSense ***
WAN (wan) -> em0 -> v4/DHCP4: 10.0.2.15/24
v6/DHCP6: fd17:625c:f037:2:a00:27ff:fe5a:9859/64
LAN (lan) -> em1 -> v4: 192.168.1.1/24
0) Logout / Disconnect SSH          9) pfTop
1) Assign Interfaces                10) Filter Logs
2) Set interface(s) IP address      11) Restart GUI
3) Reset admin account and 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: █
```

### Step 2:

Access pfSense web interface on the test machine:

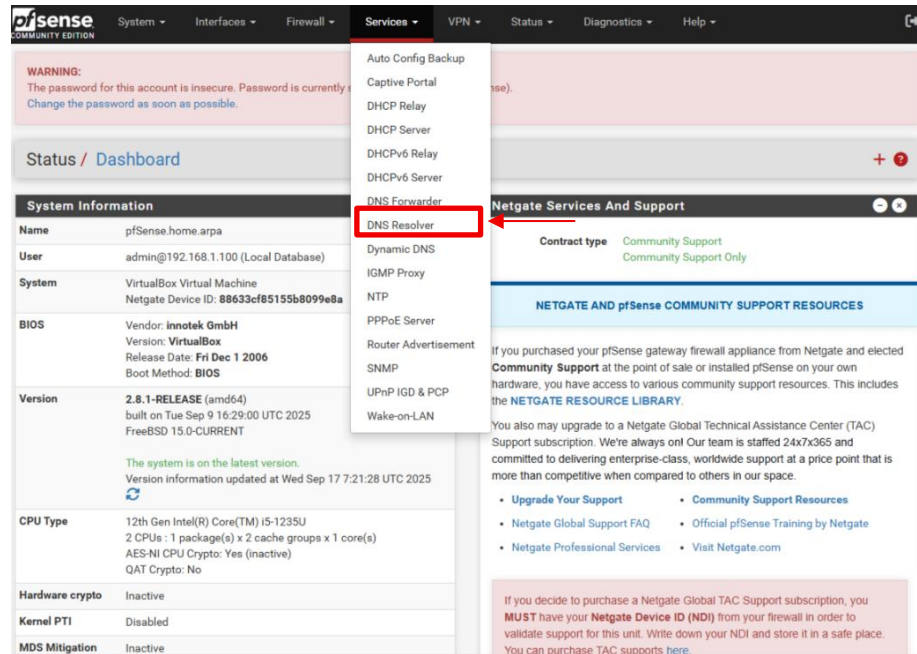
- Login with the credentials.



## Step 3:

### Access and configure DNS Resolver:

- Go to DNS Resolver from services dropdown list.



## Step 4:

### Configure General DNS Resolver Settings

#### Step 1:

- Enable DNS Resolver.



**pfSense** Community Edition

System - Interfaces - Firewall - Services - VPN - Status - Diagnostics - Help

**WARNING:**  
The password for this account is insecure. Password is currently set to the default value (pfSense).  
Change the password as soon as possible.

Services / DNS Resolver / General Settings

The DNS resolver configuration has been changed.  
The changes must be applied for them to take effect. [Apply Changes](#)

ISC DHCP has reached end-of-life and will be removed in a future version of pfSense. Visit [System > Advanced > Networking](#) to switch DHCP backend.

General Settings | Advanced Settings | Access Lists

**General DNS Resolver Options**

Enable ☒ **Enable DNS resolver**

Listen Port: 53  
The port used for responding to DNS queries. It should normally be left blank unless another service needs to bind to TCP/UDP port 53.

Enable SSL/TLS Service ☐ Respond to incoming SSL/TLS queries from local clients  
Configures the DNS Resolver to act as a DNS over SSL/TLS server which can answer queries from clients which also support DNS over TLS. Activating this option disables automatic interface response routing behavior, thus it works best with specific interface bindings.

SSL/TLS Certificate: GUI default (68c523e94854a)  
The server certificate to use for SSL/TLS service. The CA chain will be determined automatically.

SSL/TLS Listen Port: 853  
The port used for responding to SSL/TLS DNS queries. It should normally be left blank unless another service needs to bind to TCP/UDP port 853.

Network Interfaces: All, WAN, LAN

## Step 2:

- Scroll down and enable DHCP registration in DNS Resolver.
- Leave other options as of default.

System Domain Local Zone Type: Transparent  
The local-zone type used for the pfSense system domain (System > General Setup). Transparent is the default.

DNSSEC ☒ Enable DNSSEC Support

Python Module ☐ Enable Python Module  
Enable the Python Module.

DNS Query Forwarding ☐ Enable Forwarding Mode  
If this option is set, DNS queries will be forwarded to the upstream DNS servers defined under System > General Setup or those obtained via dynamic interfaces such as DHCP, PPP, or OpenVPN (if DNS Server Override is enabled there).

☐ Use SSL/TLS for outgoing DNS Queries to Forwarding Servers  
When set in conjunction with DNS Query Forwarding, queries to all upstream forwarding DNS servers will be sent using SSL/TLS on the default port of 853. Note that ALL configured forwarding servers MUST support SSL/TLS queries on port 853.

DHCP Registration ☒ **Register DHCP leases in the DNS Resolver**  
If this option is set, then machines that specify their hostname when requesting an IPv4 DHCP lease will be registered in the DNS Resolver so that their name can be resolved. Note that this will cause the Resolver to reload and flush its resolution cache whenever a DHCP lease is issued. The domain in System > General Setup should also be set to the proper value.

Static DHCP ☐ Register DHCP static mappings in the DNS Resolver  
If this option is set, then DHCP static mappings will be registered in the DNS Resolver, so that their name can be resolved. The domain in System > General Setup should also be set to the proper value.

OpenVPN Clients ☐ Register connected OpenVPN clients in the DNS Resolver  
If this option is set, then the common name (CN) of connected OpenVPN clients will be registered in the DNS Resolver, so that their name can be resolved. This only works for OpenVPN servers (Remote Access SSL/TLS or User Auth with Username as Common Name option) operating in "tun" mode. The domain in System > General Setup should also be set to the proper value.

Display Custom Options [Display Custom Options](#)

[Save](#)

### Step 3:

- Scroll down to the bottom of the DNS Resolver page until you see the **Domain Overrides** section.
- Click the green **+ Add** button in the **Domain Overrides** section.

The screenshot shows the DNS Resolver configuration page. At the top, there are sections for 'Static DHCP' and 'OpenVPN Clients', each with a checkbox to 'Register' in the DNS Resolver. Below these is a 'Display Custom Options' section with a '+ Display Custom Options' button. A 'Save' button is located below the 'Display Custom Options' section. The 'Host Overrides' section is visible, with a table that has columns: Host, Parent domain of host, IP to return for host, Description, and Actions. Below the table is a '+ Add' button. The 'Domain Overrides' section is also visible, with a table that has columns: Domain, Lookup Server IP Address, Description, and Actions. Below the table is a '+ Add' button, which is highlighted with a red box and a red arrow pointing to it from the right.

- Fill in the required fields for **Domain** and **Lookup Server IP Address** as necessary.
  - Enter **amazon.com** in the Domain field to specify that DNS lookups for this domain will use a custom server.
  - Fill in **127.0.0.1** as the **IP Address** for the authoritative DNS server for **amazon.com** lookups.
  - Optionally, tick the box for the **Use SSL/TLS for DNS Queries forwarded to this server** if you want DNS queries to be encrypted (leave unchecked in this example).
  - Leave the **TLS Hostname** field empty unless you need to specify a custom hostname for certificate verification (not required in this example).
  - Optionally, add any details in the **Description** field for reference.
  - Click **Save** at the bottom to apply your domain override settings.

**WARNING:**  
The password for this account is insecure. Password is currently set to the default value (pfSense).  
Change the password as soon as possible.

Services / DNS Resolver / General Settings / Edit Domain Override

**Domains to Override with Custom Lookup Servers**

<b>Domain</b>	amazon.com
<b>IP Address</b>	127.0.0.1
<b>TLS Queries</b>	<input type="checkbox"/> Use SSL/TLS for DNS Queries forwarded to this server When set, queries for all DNS servers for this domain will be sent using SSL/TLS on the default port of 853.
<b>TLS Hostname</b>	
<b>Description</b>	

**Save**

#### Step 4:

- After saving your changes, look for the yellow banner stating “The DNS resolver configuration has been changed.”
- Click the green **Apply Changes** button to activate your updated DNS resolver configuration.
- Wait for the confirmation that the settings have been successfully applied before proceeding with further configuration.

**WARNING:**  
The password for this account is insecure. Password is currently set to the default value (pfSense).  
Change the password as soon as possible.

Services / DNS Resolver / General Settings

The DNS resolver configuration has been changed.  
The changes must be applied for them to take effect.

**Apply Changes**

ISC DHCP has reached end-of-life and will be removed in a future version of pfSense. Visit [System > Advanced > Networking](#) to switch DHCP backend.

General Settings | Advanced Settings | Access Lists

**General DNS Resolver Options**

**Enable** ☒ Enable DNS resolver

**Listen Port** 53  
The port used for responding to DNS queries. It should normally be left blank unless another service needs to bind to TCP/UDP port 53.

**Enable SSL/TLS Service** ☐ Respond to incoming SSL/TLS queries from local clients  
Configures the DNS Resolver to act as a DNS over SSL/TLS server which can answer queries from clients which also support DNS over TLS. Activating this option disables automatic interface response routing behavior; thus it works best with specific interface bindings.

**SSL/TLS Certificate** GUI default (68c323e94854a)  
The server certificate to use for SSL/TLS service. The CA chain will be determined automatically.

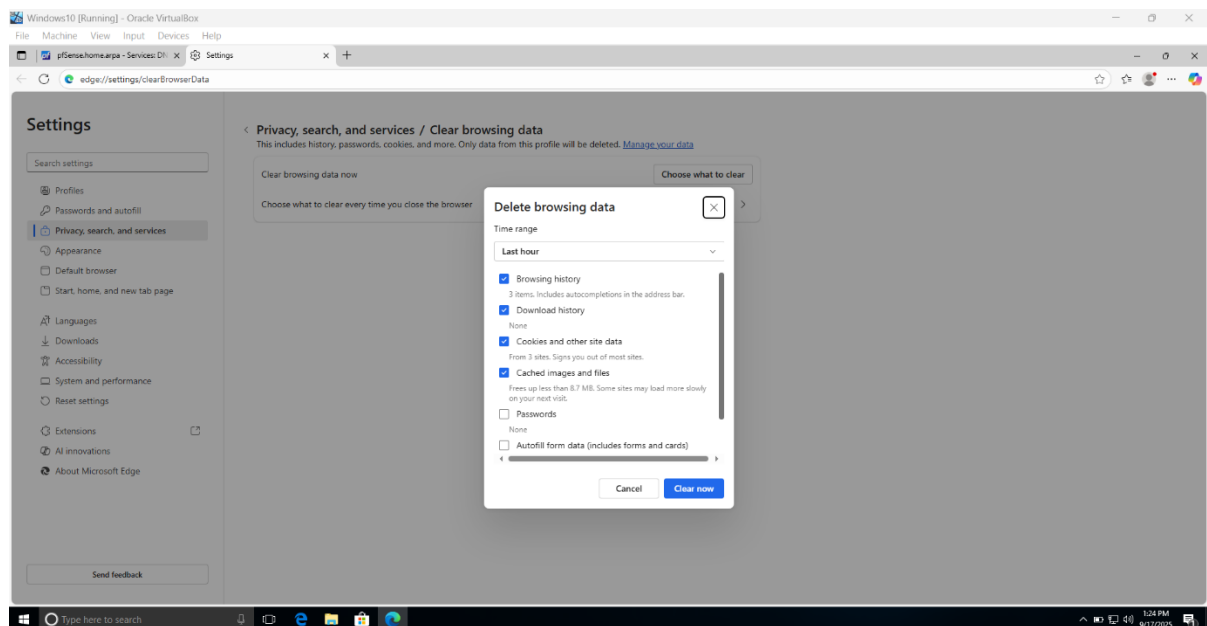
**SSL/TLS Listen Port** 853  
The port used for responding to SSL/TLS DNS queries. It should normally be left blank unless another service needs to bind to TCP/UDP port 853.

**Network Interfaces** WAN  
LAN

## Step 5:

- Navigate to browser settings and select the '**Privacy, search, and services**' section. Alternatively, use the shortcut **Ctrl + H** to directly access the browsing history.
- Click on Choose what to clear under "**Clear browsing data**" to open the data selection window.
- Select key items to delete:
  - **Browsing history** removes records of visited pages and autocompletions.
  - **Cookies and other site data** signs out of most sites and clears session info.
  - **Cached images and files** force the browser to reload all resources from the web, ensuring new DNS settings are respected.
- Optionally clear additional items like **Passwords** and **Autofill form data** if required.
- Set the desired **Time range** for deletion, such as "Last hour" or "All time" to ensure thorough cache refresh.
- Click **Clear now** to apply changes and confirm that the cache is deleted.

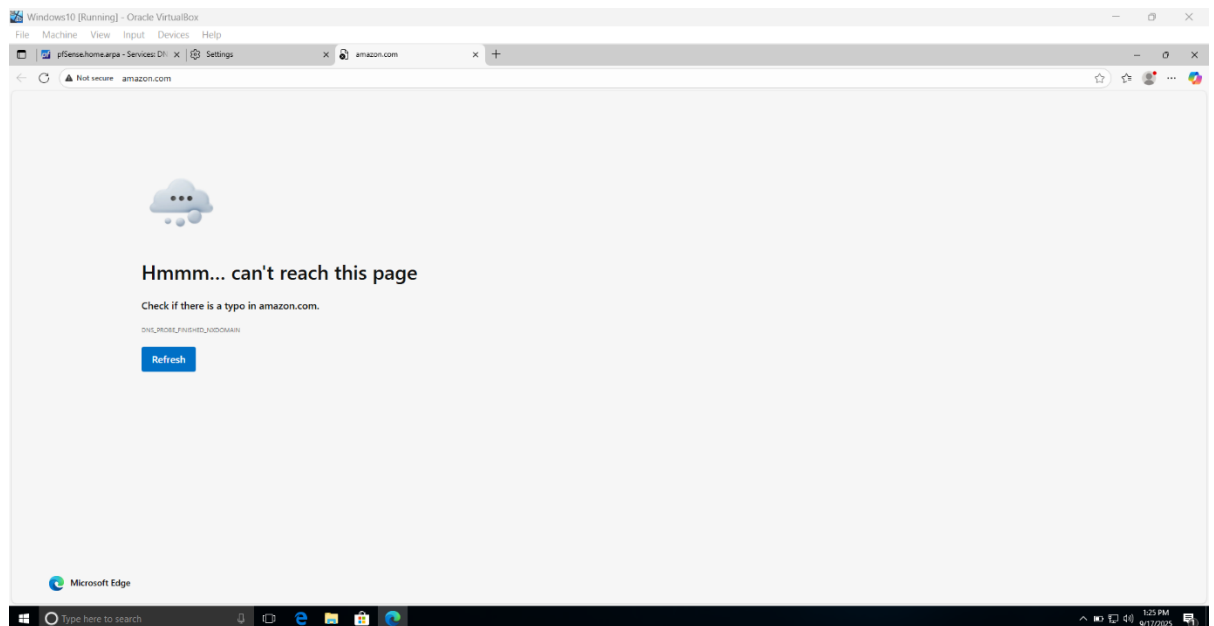
Clearing the cache ensures that recent DNS configuration changes are not masked by old browser data, helping troubleshoot and verify if domains resolve properly using the new DNS settings.



## Step 6:

### Verify Site Accessibility After DNS Changes

- Attempt to access the target website (e.g., amazon.com) using your browser to confirm the effect of your DNS override configuration.
- Observe the result; if the site does not load and displays an error (such as “can’t reach this page”), it indicates that pfSense DNS Resolver has successfully blocked or redirected traffic for this domain as intended.
- Use this outcome to confirm that DNS overrides are functioning correctly and the configured settings are being enforced by pfSense.



## CONCLUSION

This project successfully demonstrated the use of pfSense as a powerful and flexible firewall solution to block access to a specific domain within a virtual LAN environment. By deploying pfSense in a virtualized setup, configuring the DNS Resolver with domain overrides, and applying appropriate firewall rules, we effectively restricted client access to the targeted domain. The practical approach highlights pfSense's strong capabilities in managing network security and controlling user activity at the DNS level. This domain blocking solution enhances organizational productivity and security by preventing access to unauthorized or potentially harmful websites. Overall, pfSense proves to be a reliable, customizable, and cost-effective tool for network administrators seeking to enforce domain restrictions within both test and real-world environments.

## REFERENCES

1. pfSense Official Documentation:  
<https://docs.netgate.com/pfsense/en/latest/index.html>
2. pfSense DNS Resolver Guide:  
<https://docs.netgate.com/pfsense/en/latest/services/dns/resolver.html>
3. Netgate Forum - discussion on DNS Resolver domain overrides (see Netgate community for details).
4. Oracle VirtualBox Documentation:  
<https://www.virtualbox.org/manual/UserManual.html>
5. Microsoft Edge Browser Settings Help: <https://support.microsoft.com/en-us/microsoft-edge>

## CONTRIBUTIONS

### **Vishnu P V:**

pfSense setup, VLAN configuration, DNS resolver and firewall rule implementation, documentation, project reporting, configuration guides, and validation testing.