

## **FIREWALLS**

A firewall is a network security device or software that monitors and controls incoming and outgoing network traffic based on predetermined security rules. The primary purpose of a firewall is to establish a barrier between a secure internal network and untrusted external networks, such as the Internet. Firewalls are a crucial component in safeguarding computer systems and networks from unauthorized access, cyberattacks, and other security threats.

### **Here are key aspects to understand about firewalls:**

#### **Types of Firewalls:**

##### **Packet Filtering Firewalls:**

Examines packets (small units of data) based on predefined rules.

Filters packets based on criteria such as source and destination IP addresses, port numbers, and the protocol used.

##### **Stateful Inspection Firewalls:**

Keeps track of the state of active connections and makes decisions based on the context of the traffic.

Monitors the state of the connection and allows only legitimate traffic that is part of an established connection.

##### **Proxy Firewalls (Application Layer Firewalls):**

Acts as an intermediary between internal and external systems.

Inspects and filters traffic at the application layer, providing a higher level of security.

Can cache content, making it a useful tool for optimizing network performance.

##### **Next-Generation Firewalls (NGFW):**

Combines traditional firewall features with additional capabilities such as intrusion prevention, antivirus filtering, and deep packet inspection.

Offers more advanced threat detection and prevention capabilities.

#### **Firewall Components:**

##### **Rule Base:**

Defines the criteria for allowing or blocking traffic.

Rules are typically based on IP addresses, port numbers, protocols, and other factors.

##### **Logging and Monitoring:**

Keeps track of network activity, providing information for analysis and auditing.

Logs can be used to identify security incidents and troubleshoot network issues.

##### **Network Address Translation (NAT):**

Modifies network address information in packet headers while in transit.

It helps conceal internal network structures and conserves public IP addresses.

#### **Firewall Deployment:**

##### **Hardware Firewalls:**

Dedicated physical devices are designed to protect a network.

Often used to protect entire networks or segments of a network.

##### **Software Firewalls:**

Installed on individual computers or servers.

Commonly used for personal computer security.

##### **Cloud Firewalls:**

Deployed in cloud environments to protect virtual networks and resources.

Can be managed centrally and scaled based on demand.

**Firewall Policies:****Ingress and Egress Rules:**

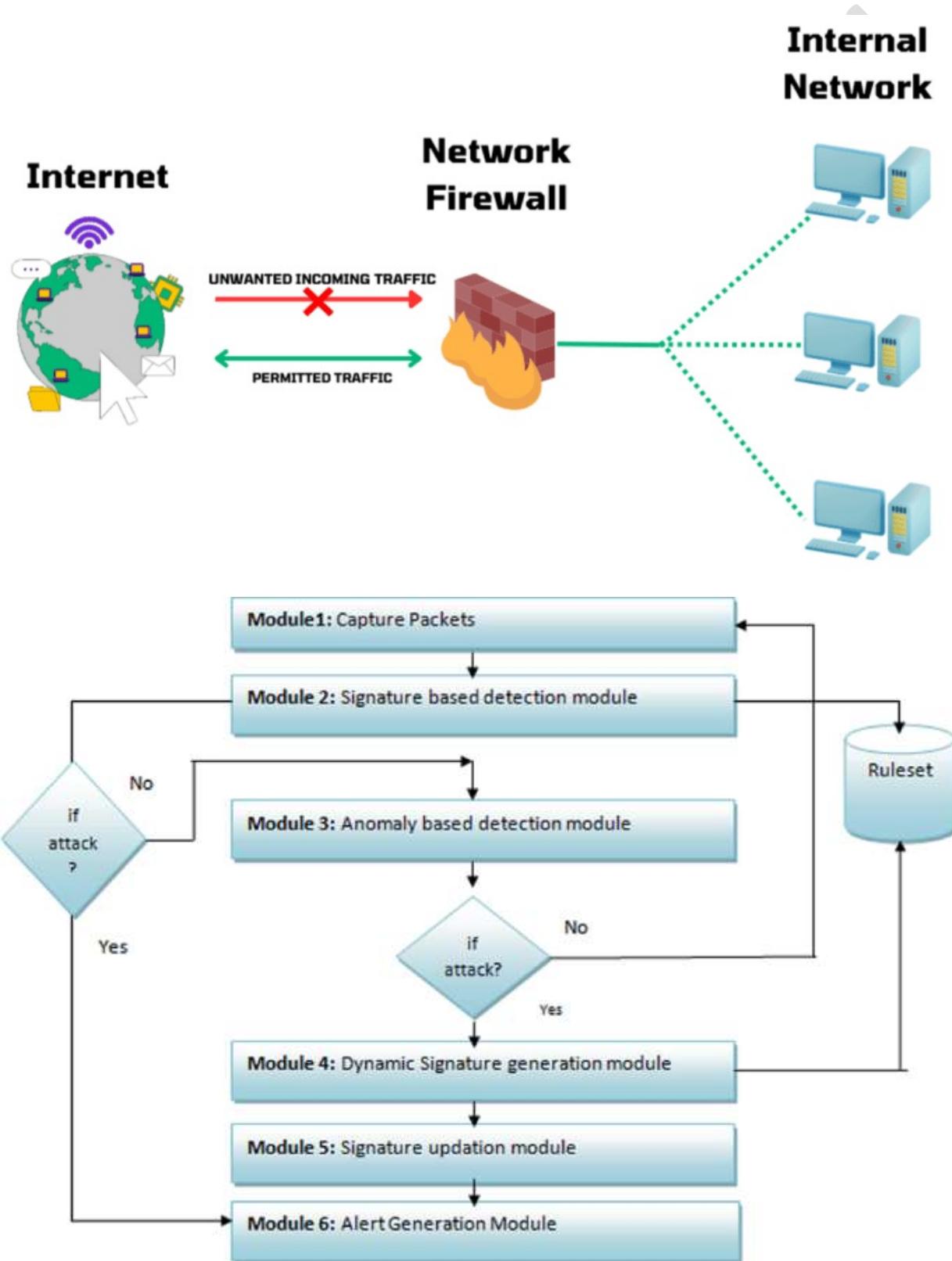
Ingress rules control incoming traffic.

Egress rules control outgoing traffic.

**Default Deny vs. Default Allow:**

Default deny blocks all traffic unless explicitly allowed.

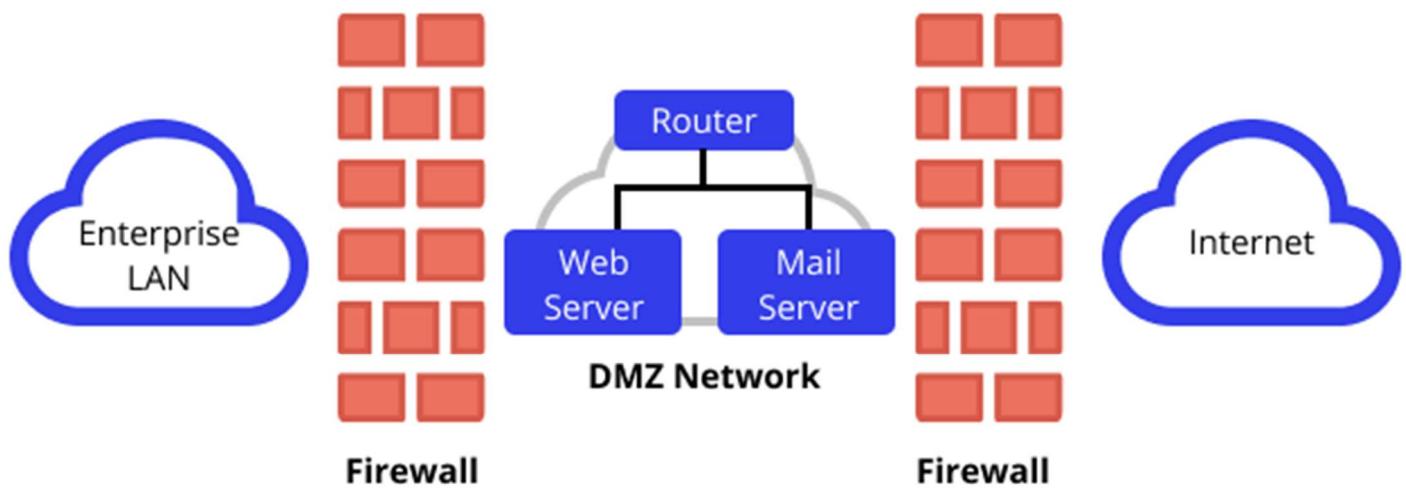
Default allow allows all traffic unless explicitly blocked.



**Demilitarized Zone:**

DMZ (Demilitarized Zone) is a network segment positioned between an internal network and the external internet. It serves as a buffer zone, isolating services that require internet accessibility, such as web servers or email servers. By placing these services in the DMZ, organizations enhance security, preventing direct access to the internal network. The firewall governing the DMZ enforces specific rules, allowing external traffic to reach services in the DMZ while restricting access to the internal network. This architecture adds an extra layer of protection, shielding critical internal systems from potential security threats originating from the internet.

## DMZ Network Architecture

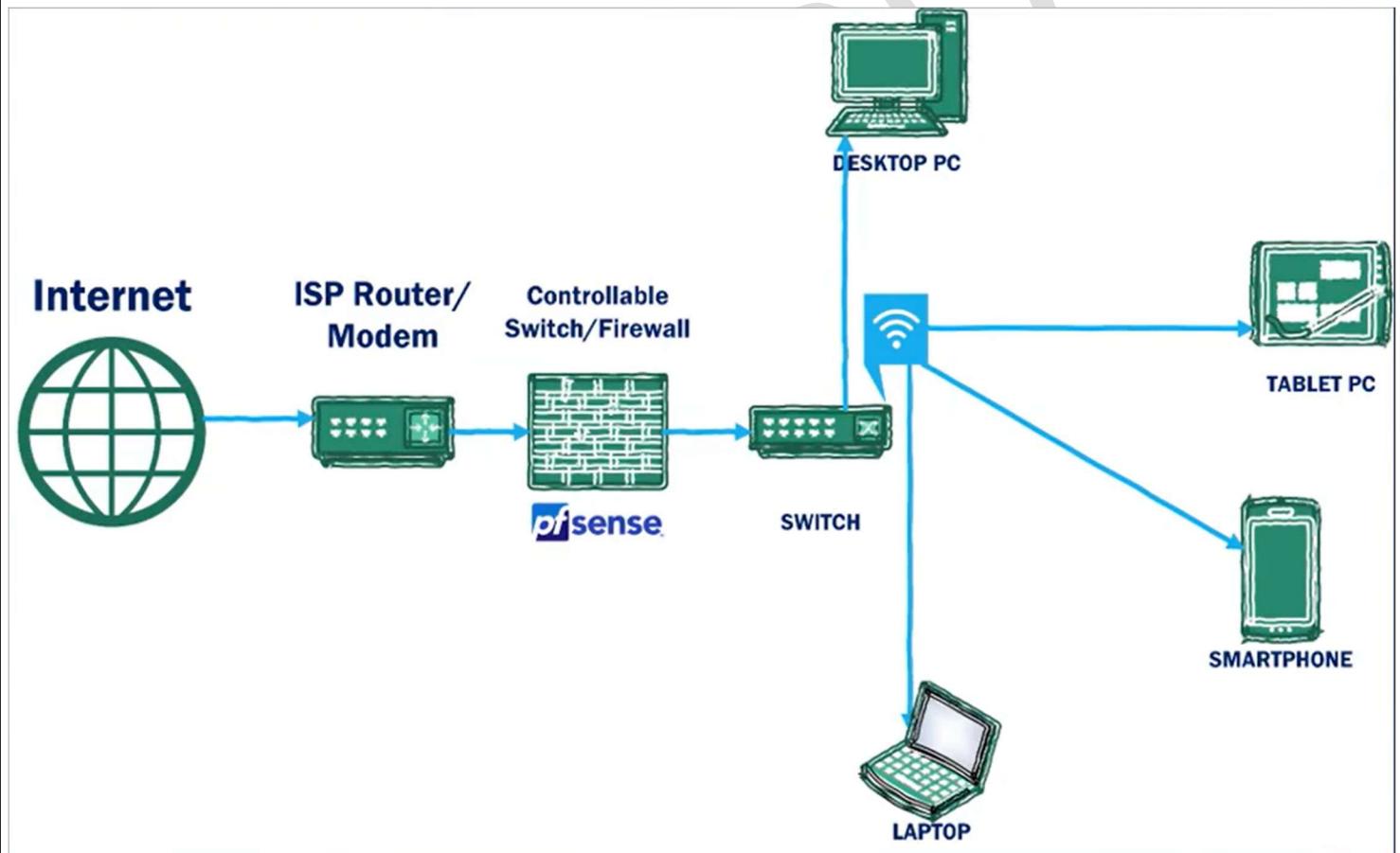


SATISH -



pfSense is a powerful and versatile open-source firewall and routing software distribution built on the FreeBSD operating system. Designed to convert standard hardware into a robust security appliance, pfSense provides a comprehensive suite of features for network security, management, and customization. With a user-friendly web interface, pfSense offers ease of configuration, making it accessible to users with varying levels of technical expertise. Known for its flexibility and scalability, pfSense is suitable for a wide range of network environments, including home networks, small businesses, and large enterprises. The active and engaged open-source community contributes to its continuous development, ensuring that pfSense remains at the forefront of network security technology. Whether protecting against external threats, setting up VPNs, or managing network traffic, pfSense stands as a reliable and customizable solution for safeguarding and optimizing network environments.

### Pfsense Architecture:



## Installation & Configuration Of Pfsense:

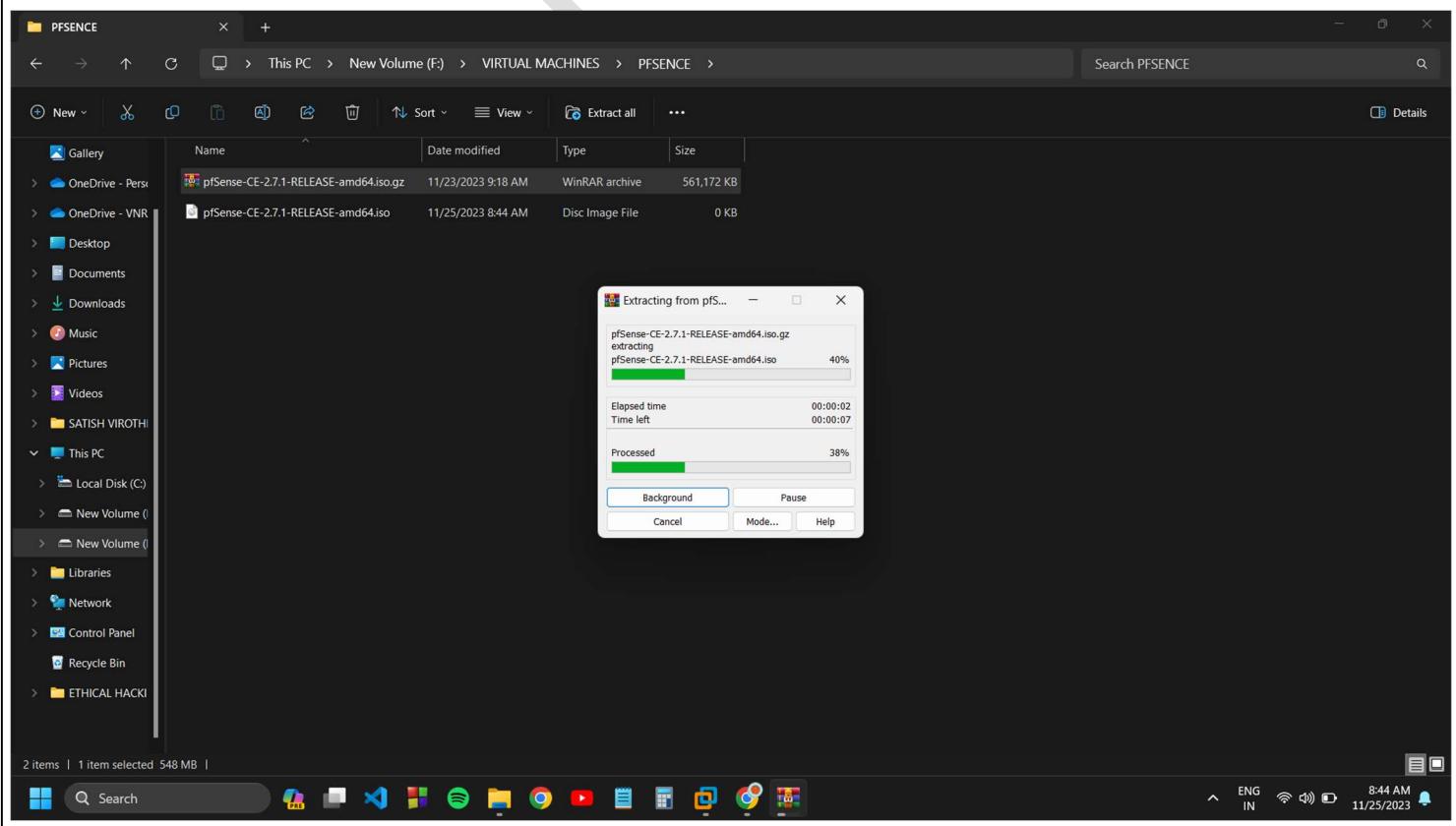
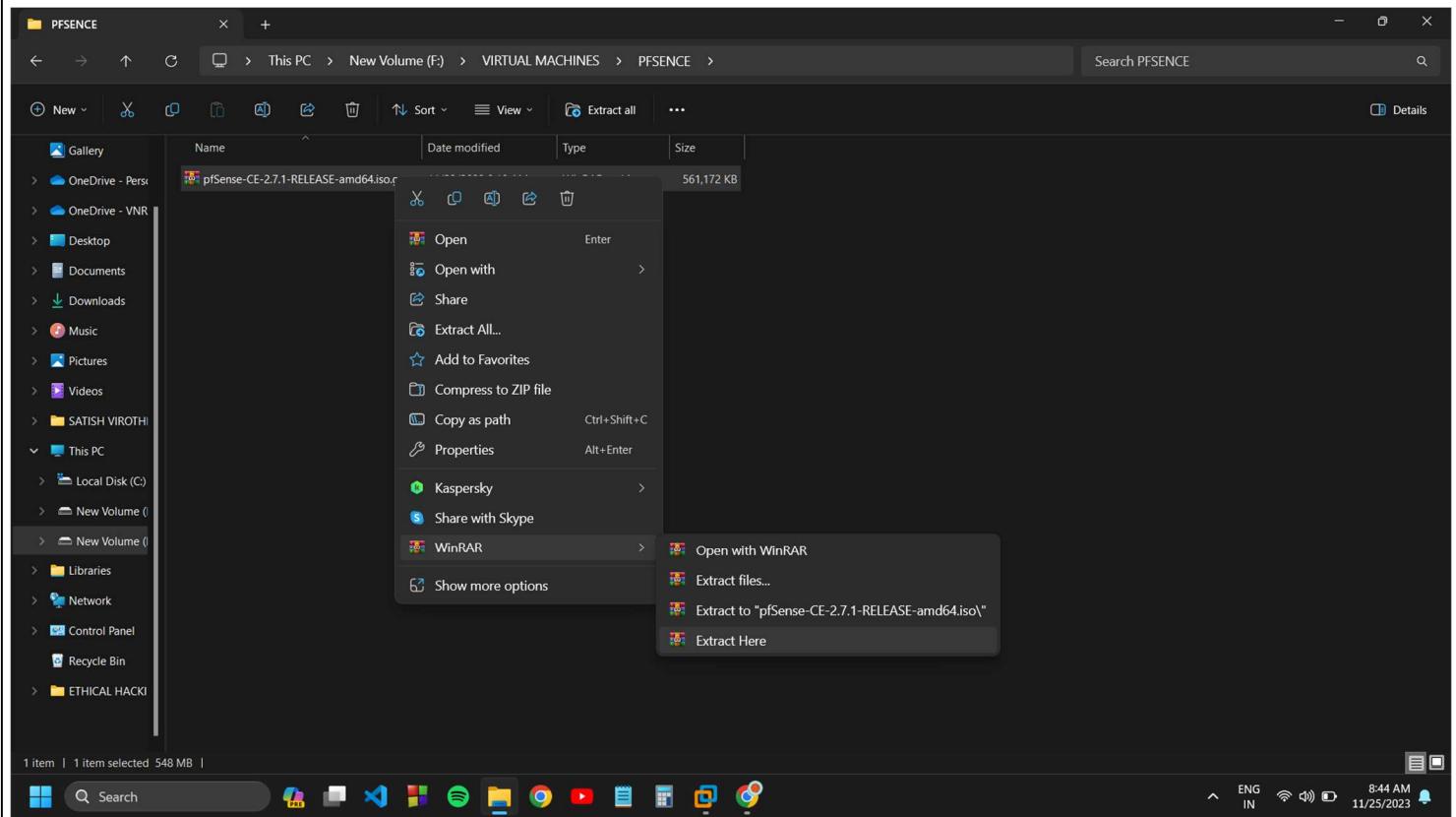
### Download pfSense ISO:

- Visit [pfsense.org](https://www.pfsense.org).
- Navigate to the download section.

- Download the pfSense ISO image file.

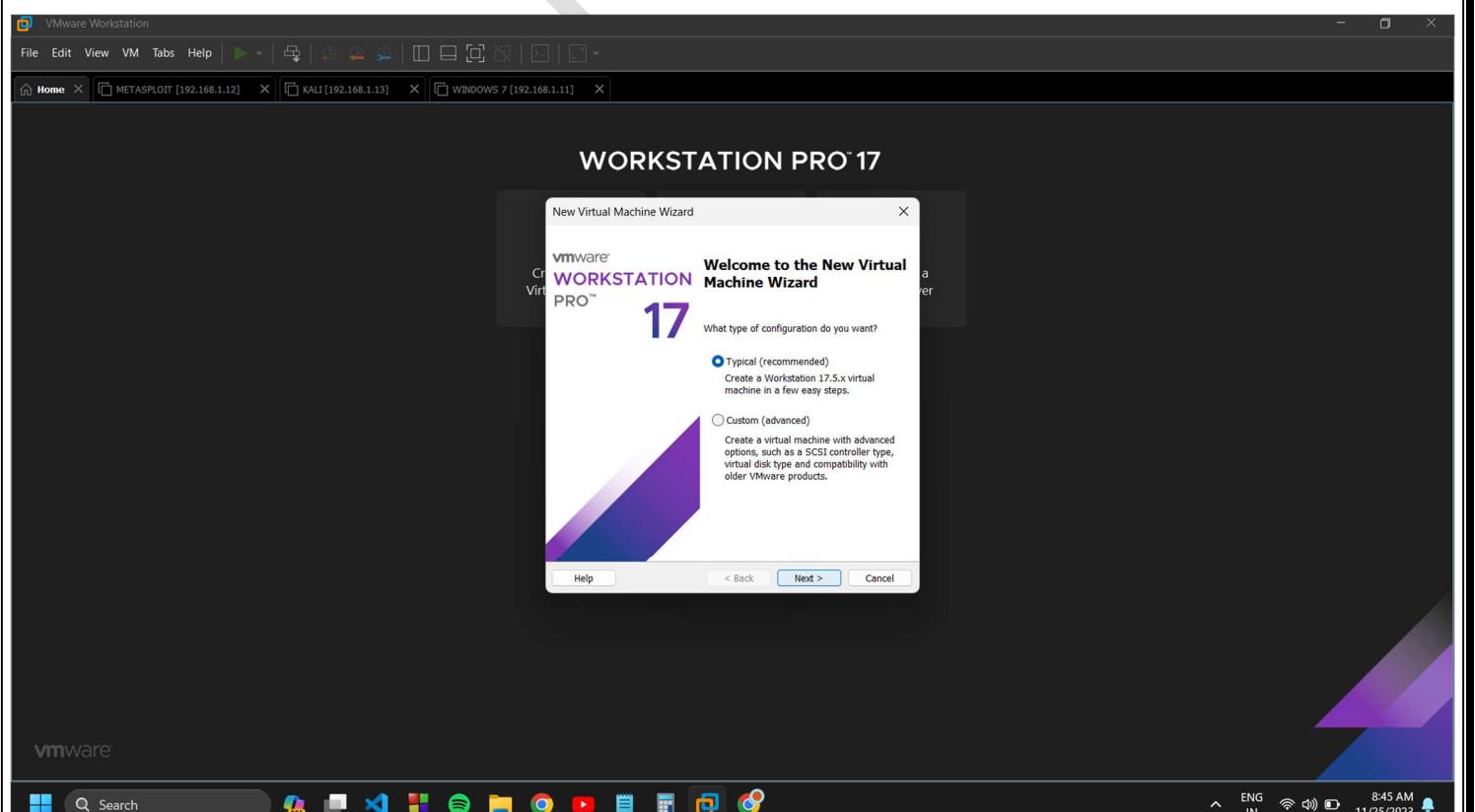
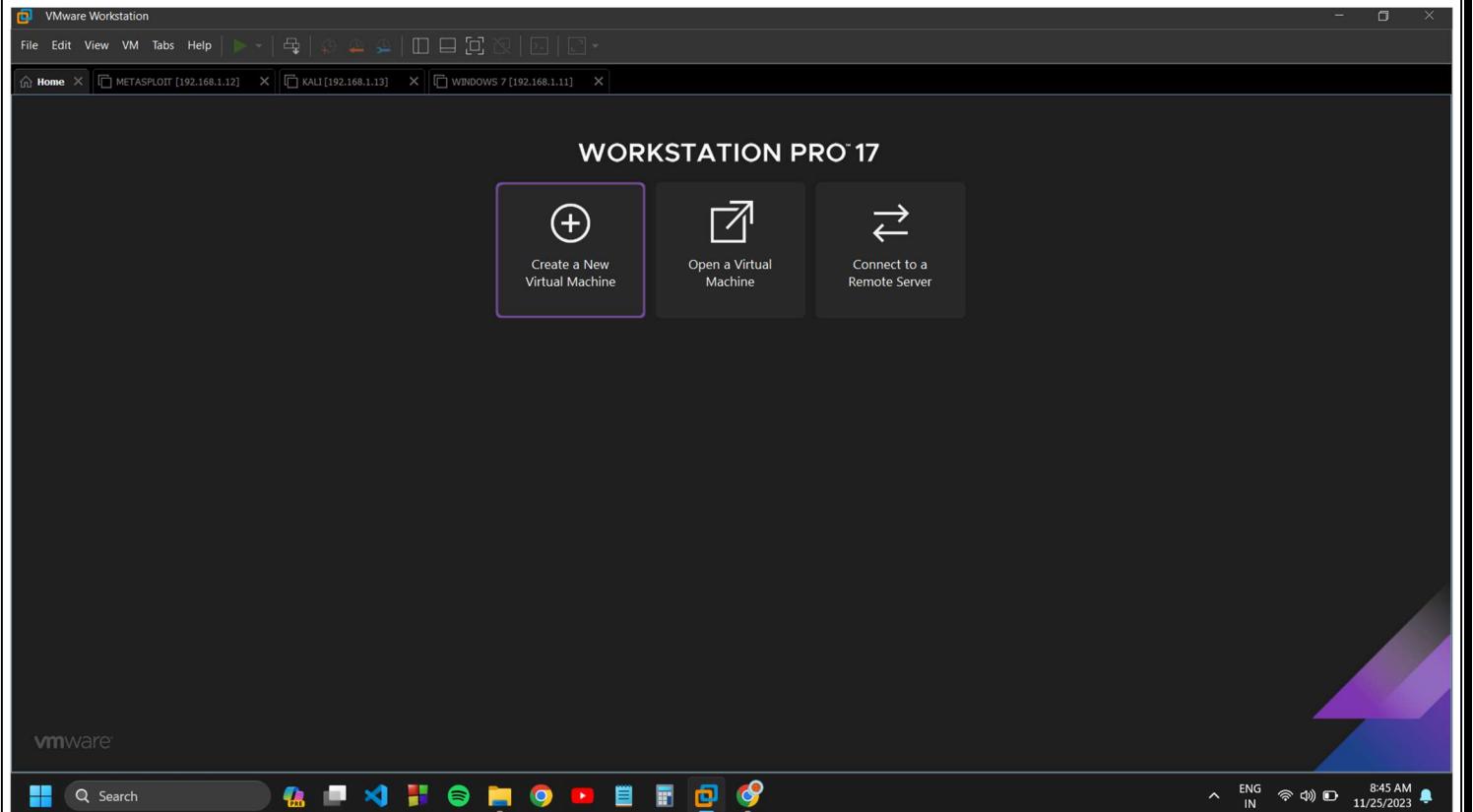
### Unzip Downloaded File:

- Locate the downloaded file in your designated folder.
- Unzip the folder to access the pfSense ISO file.

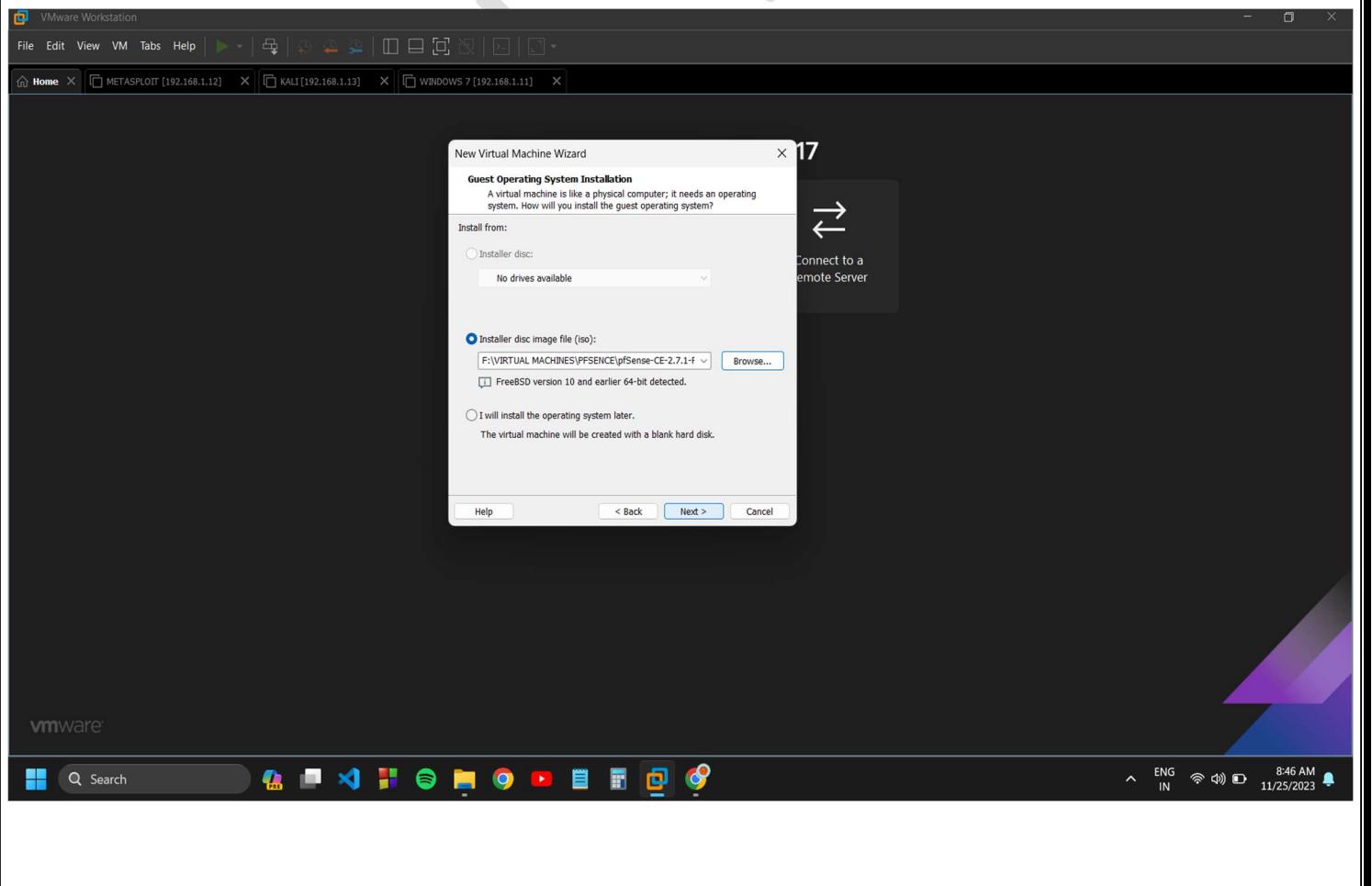
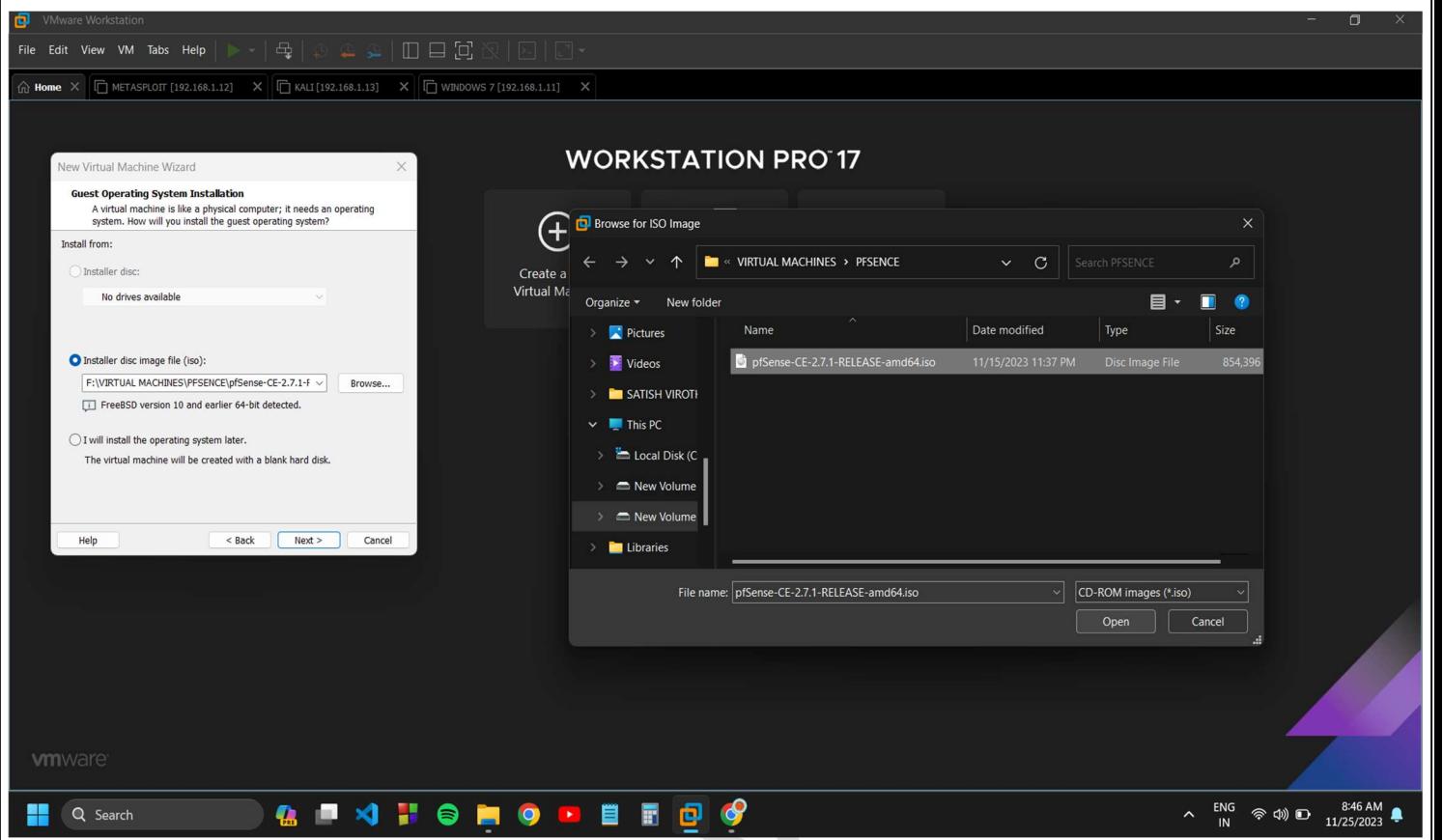


**Create a Virtual Machine (VM) in VMware:**

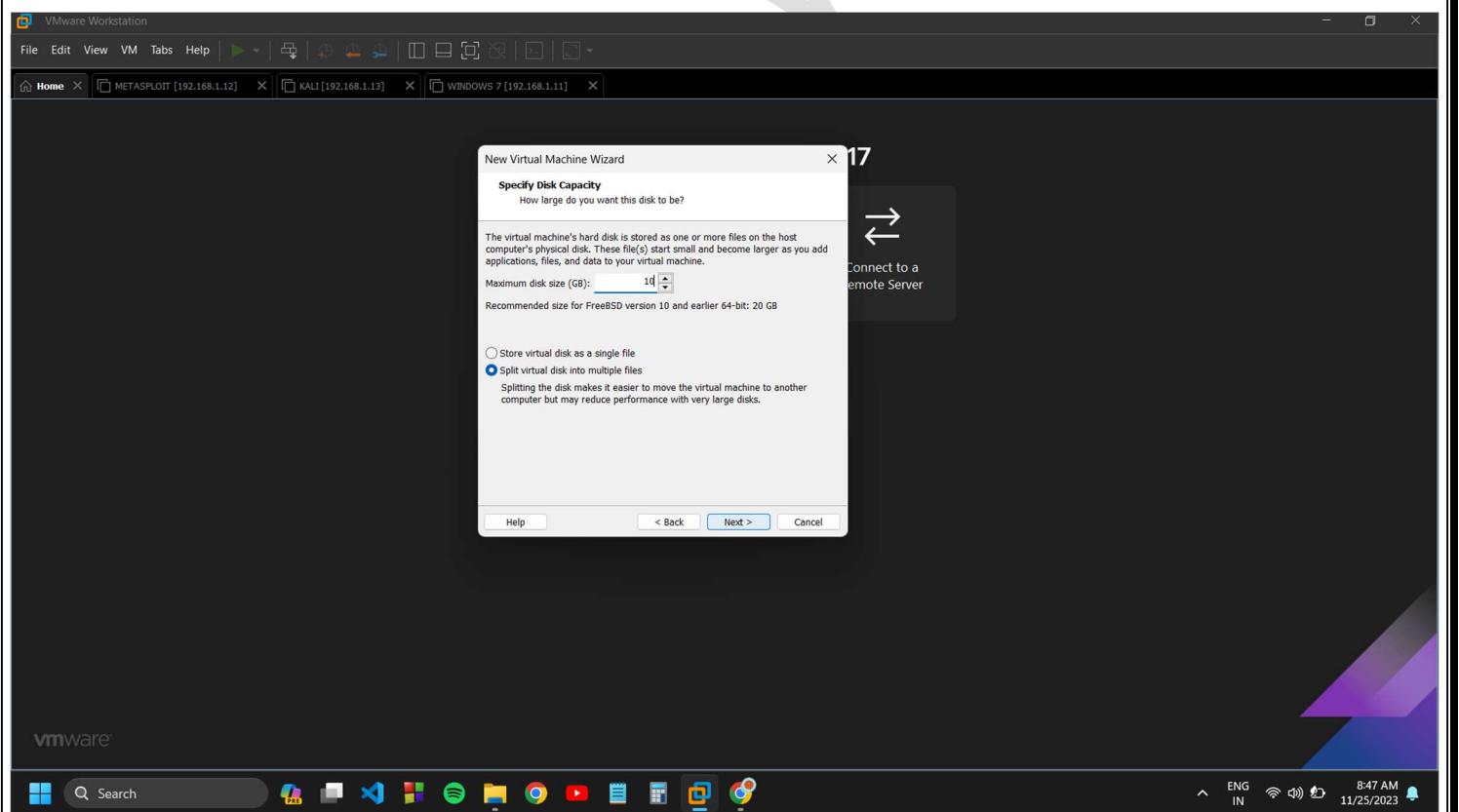
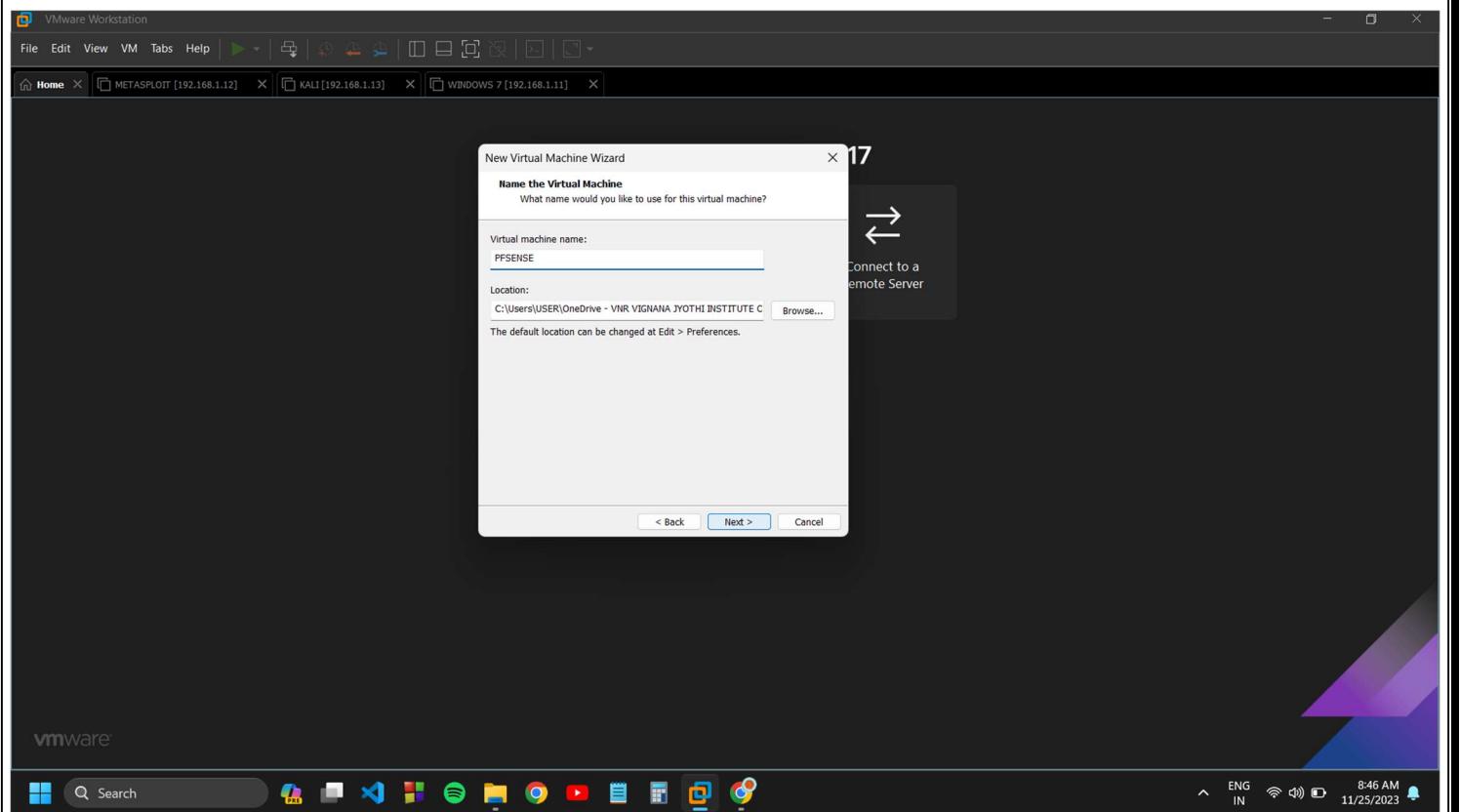
- Open VMware and create a new virtual machine.

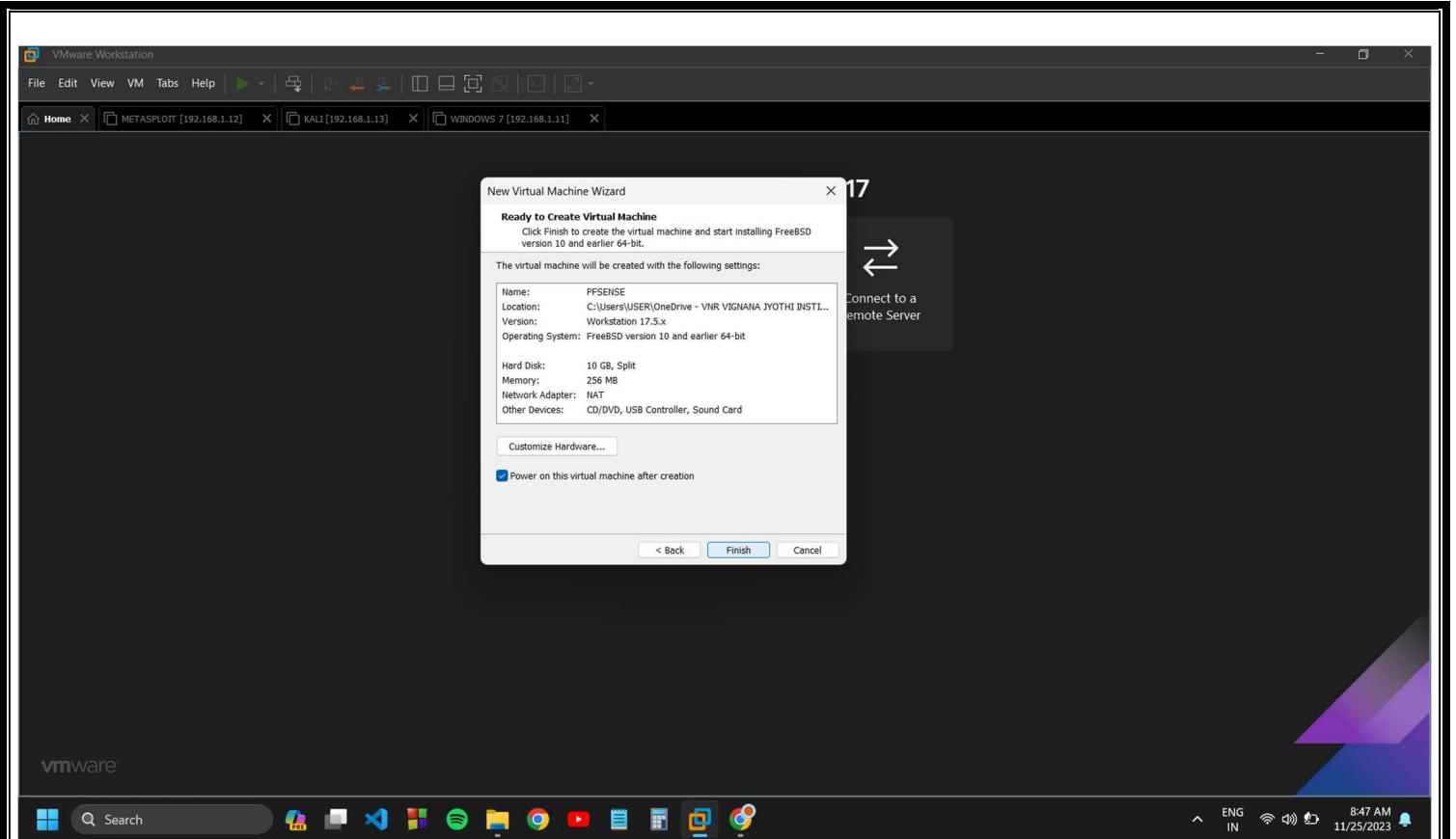


- Choose "Installer disc image file" and browse to the pfSense ISO.



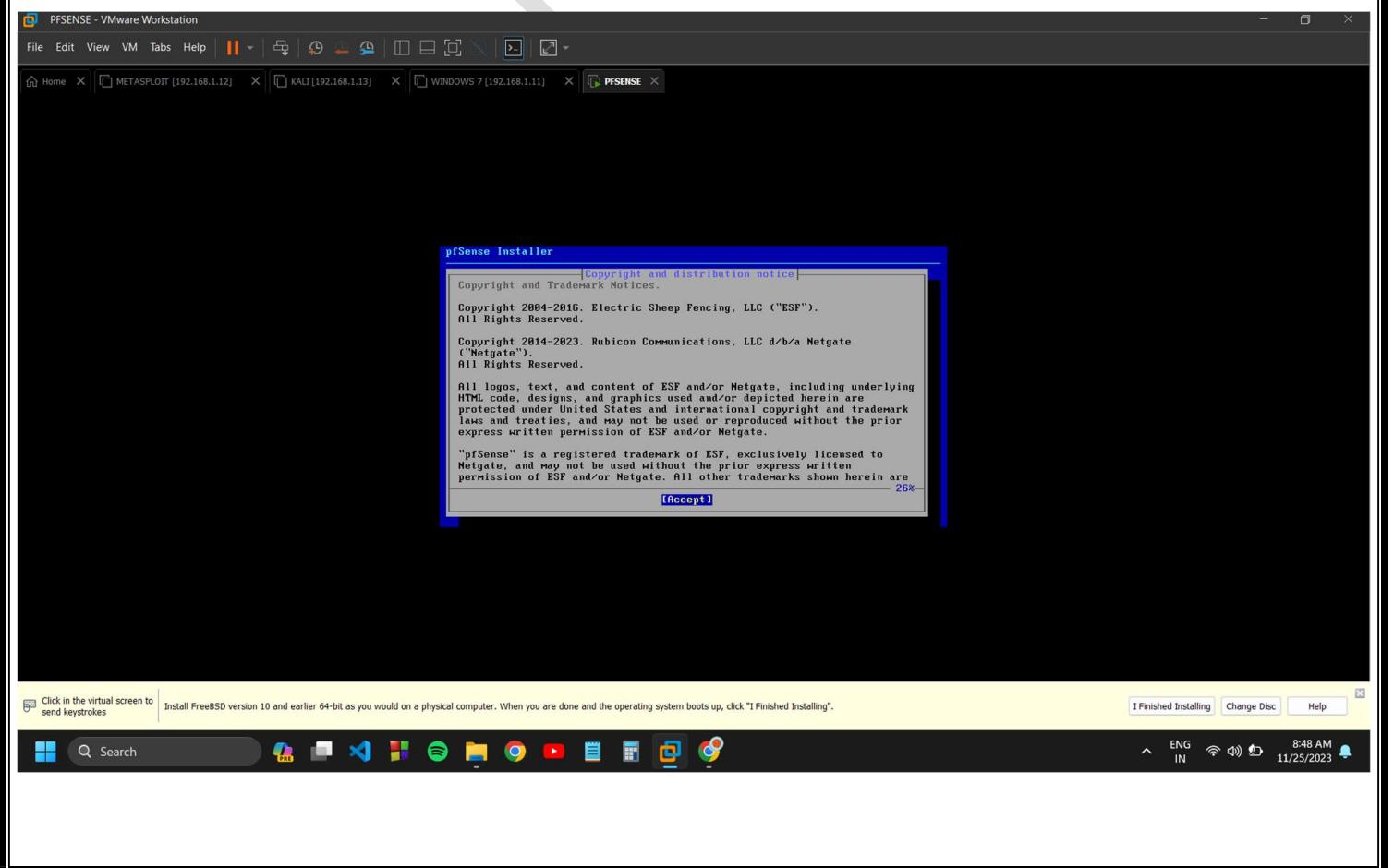
- Specify settings: name, location, disk size, etc.

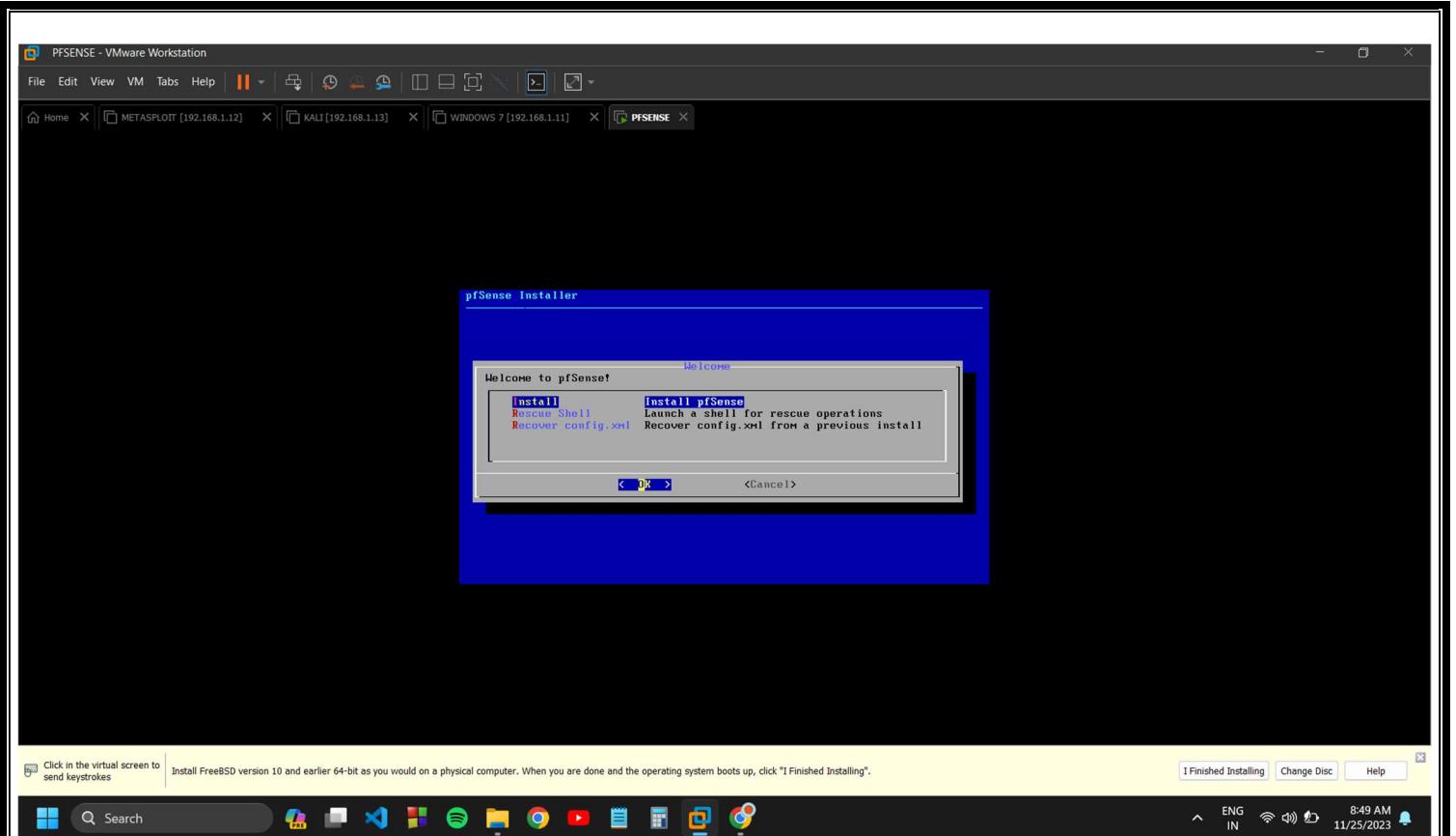




## Install pfSense:

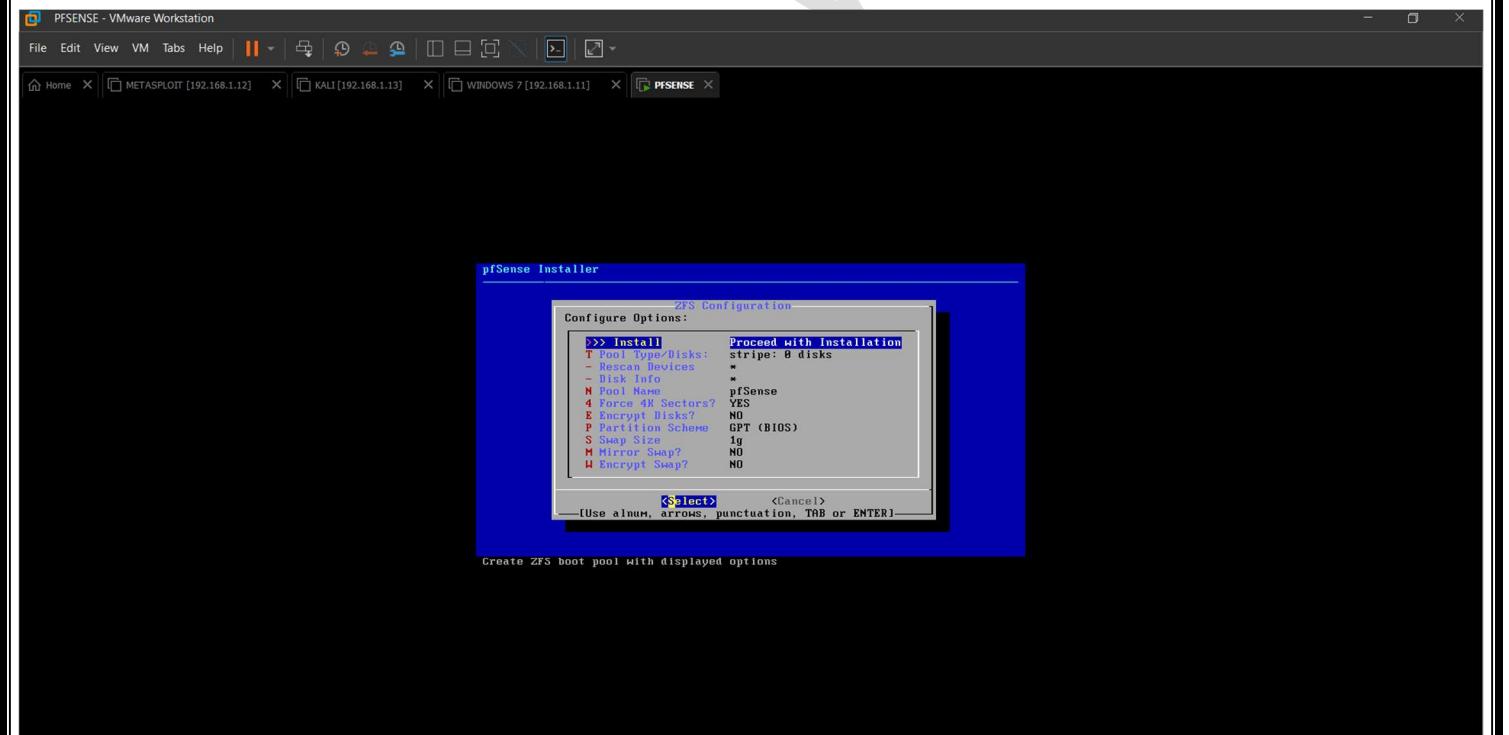
- Start the virtual machine.
- Follow on-screen instructions to install pfSense.





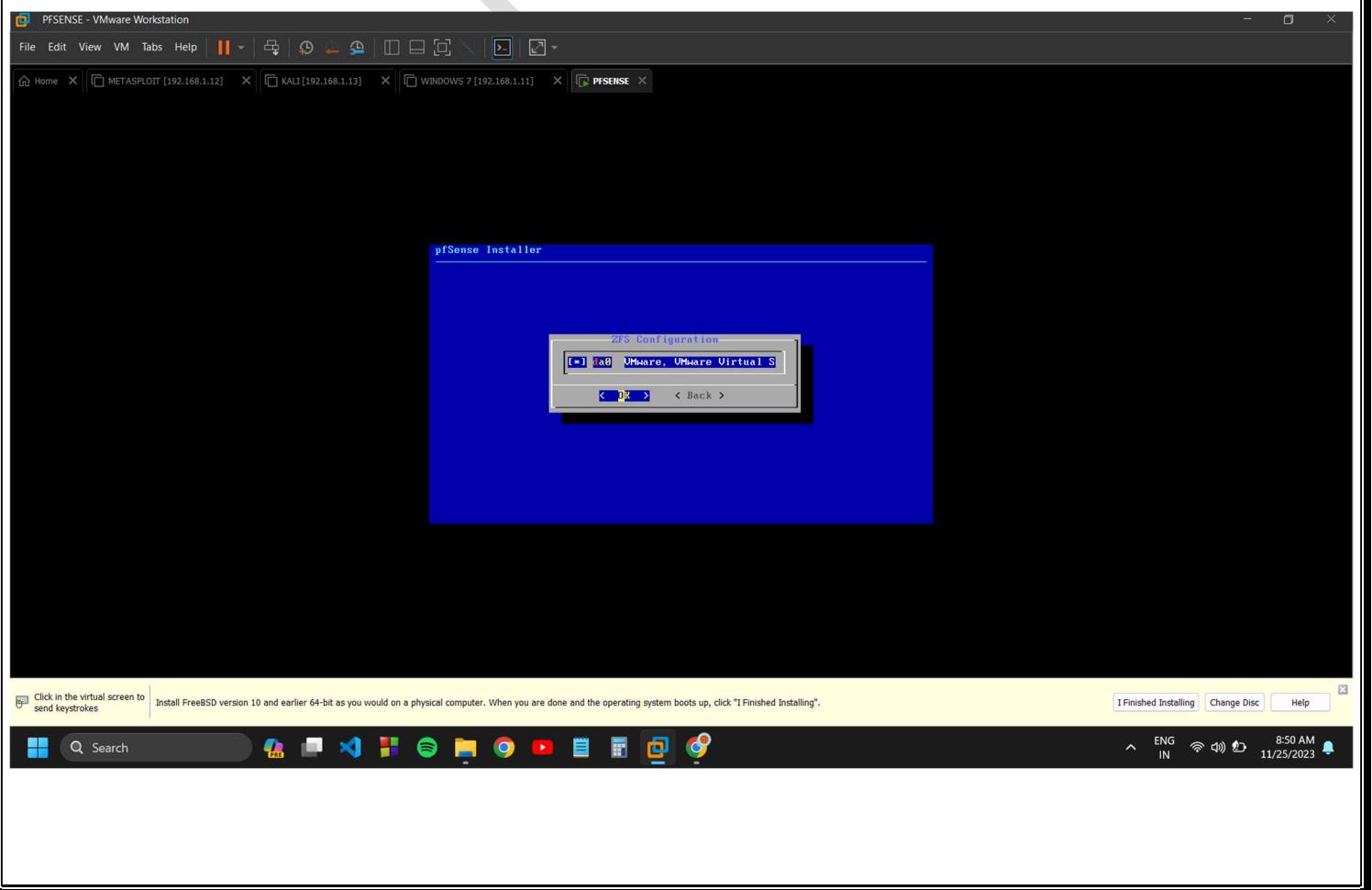
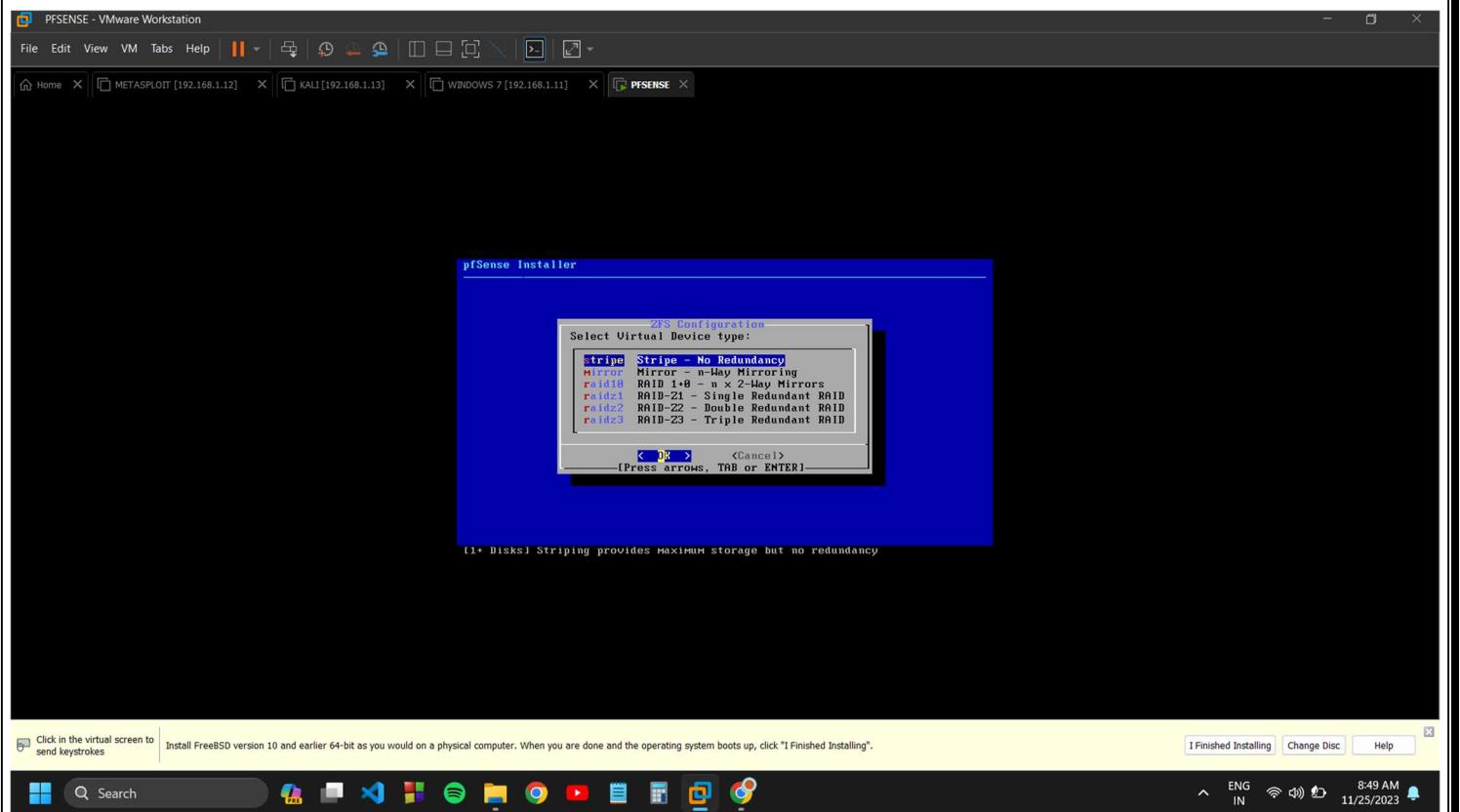
Click in the virtual screen to send keystrokes. Install FreeBSD version 10 and earlier 64-bit as you would on a physical computer. When you are done and the operating system boots up, click "I Finished Installing". I Finished Installing Change Disc Help

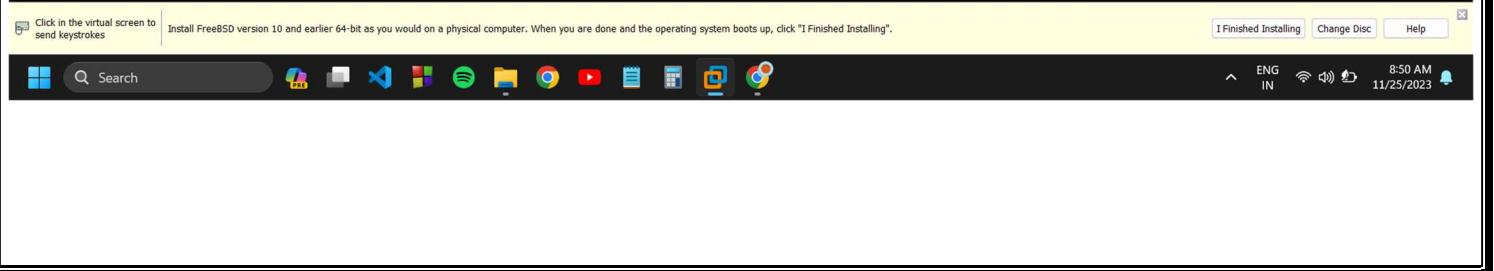
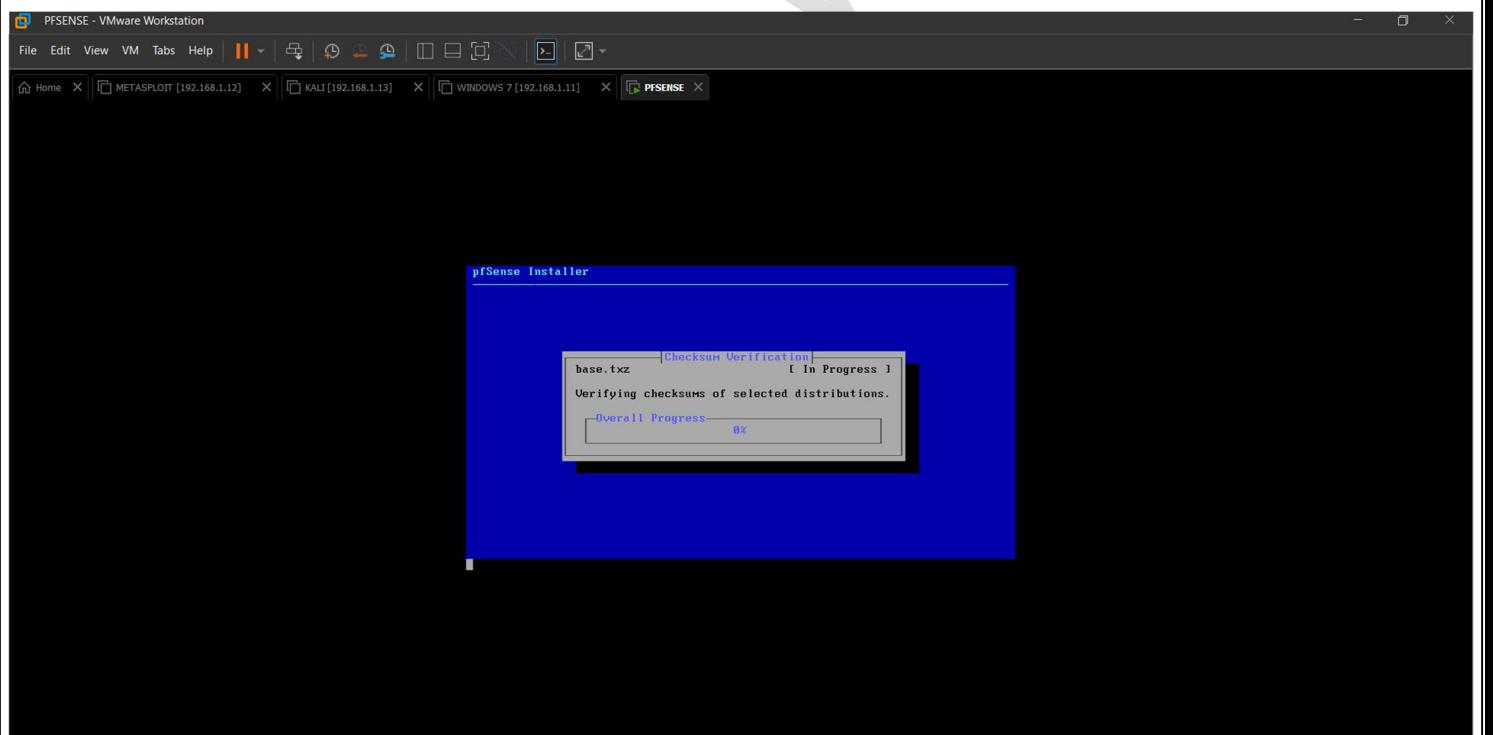
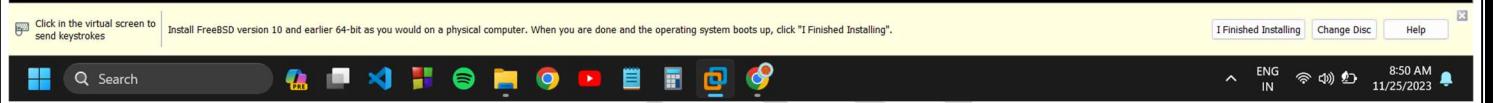
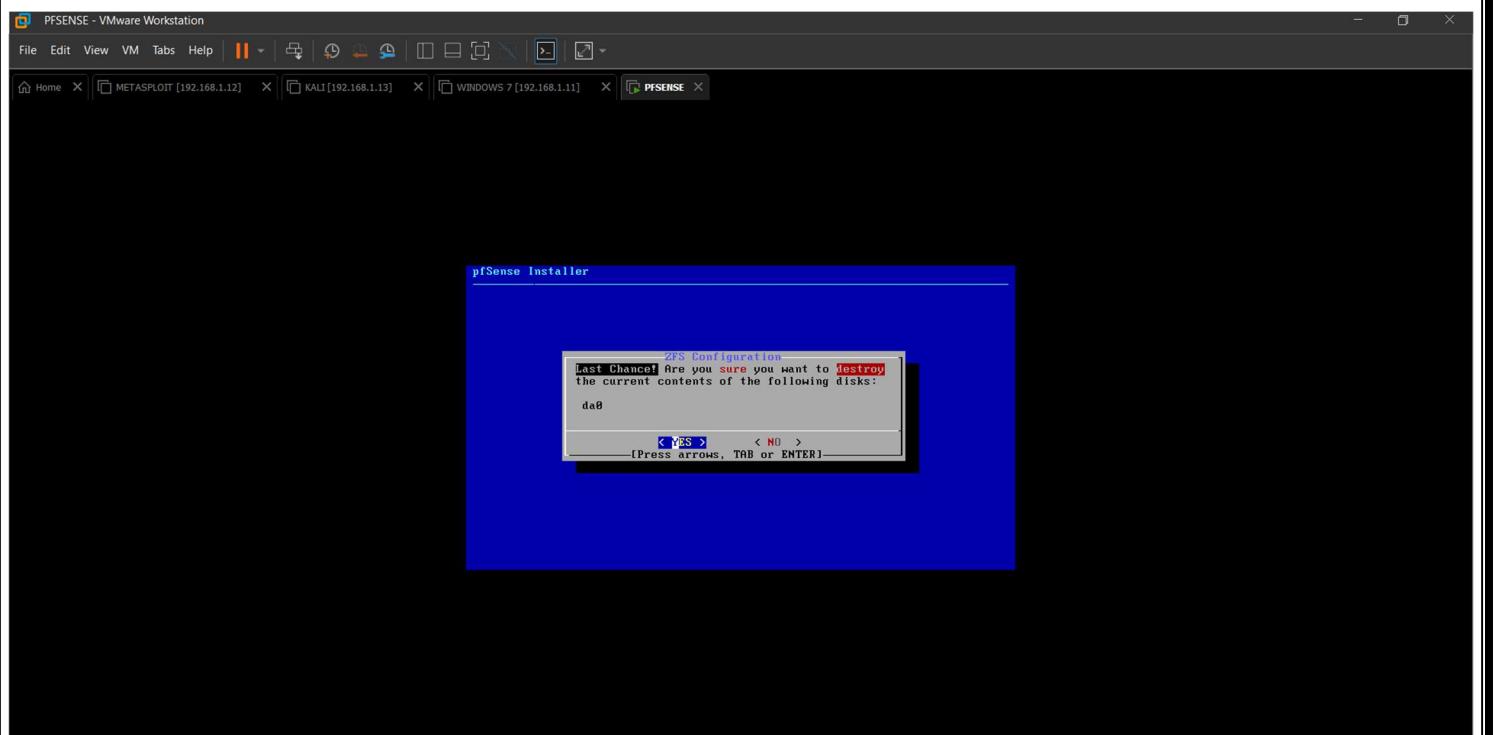
Search Search ENG IN 8:49 AM 11/25/2023

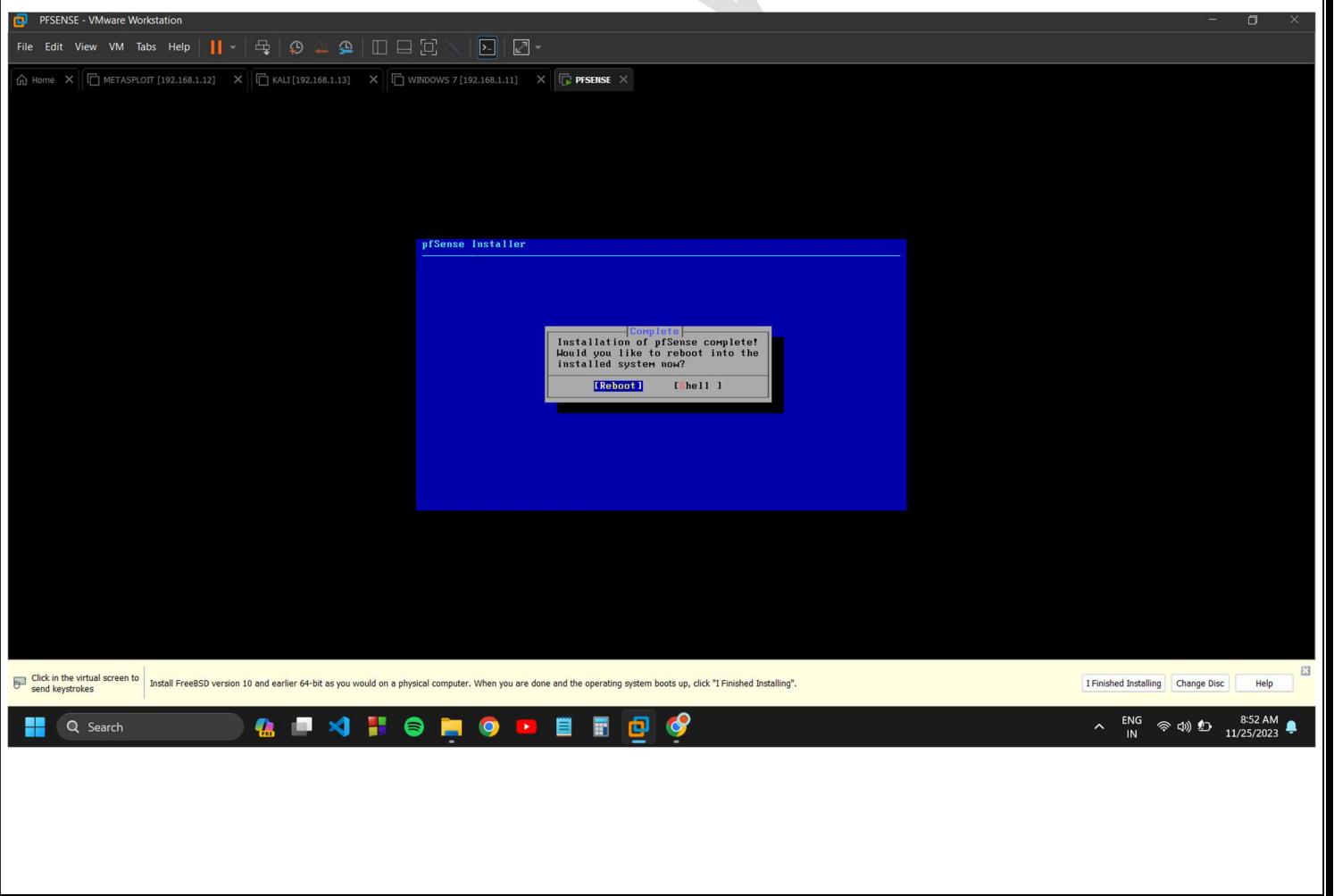
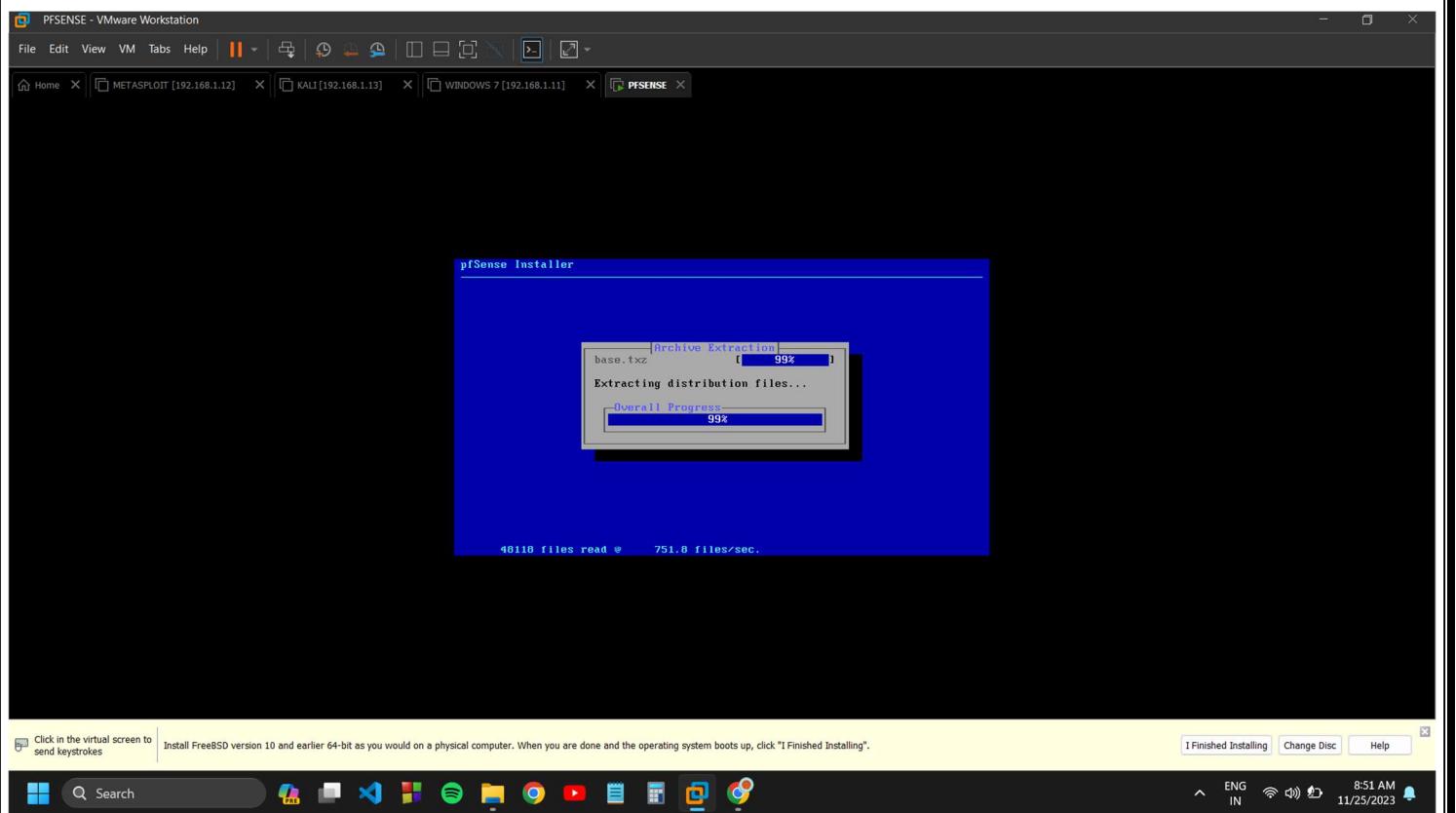


Click in the virtual screen to send keystrokes. Install FreeBSD version 10 and earlier 64-bit as you would on a physical computer. When you are done and the operating system boots up, click "I Finished Installing". I Finished Installing Change Disc Help

Search Search ENG IN 8:49 AM 11/25/2023

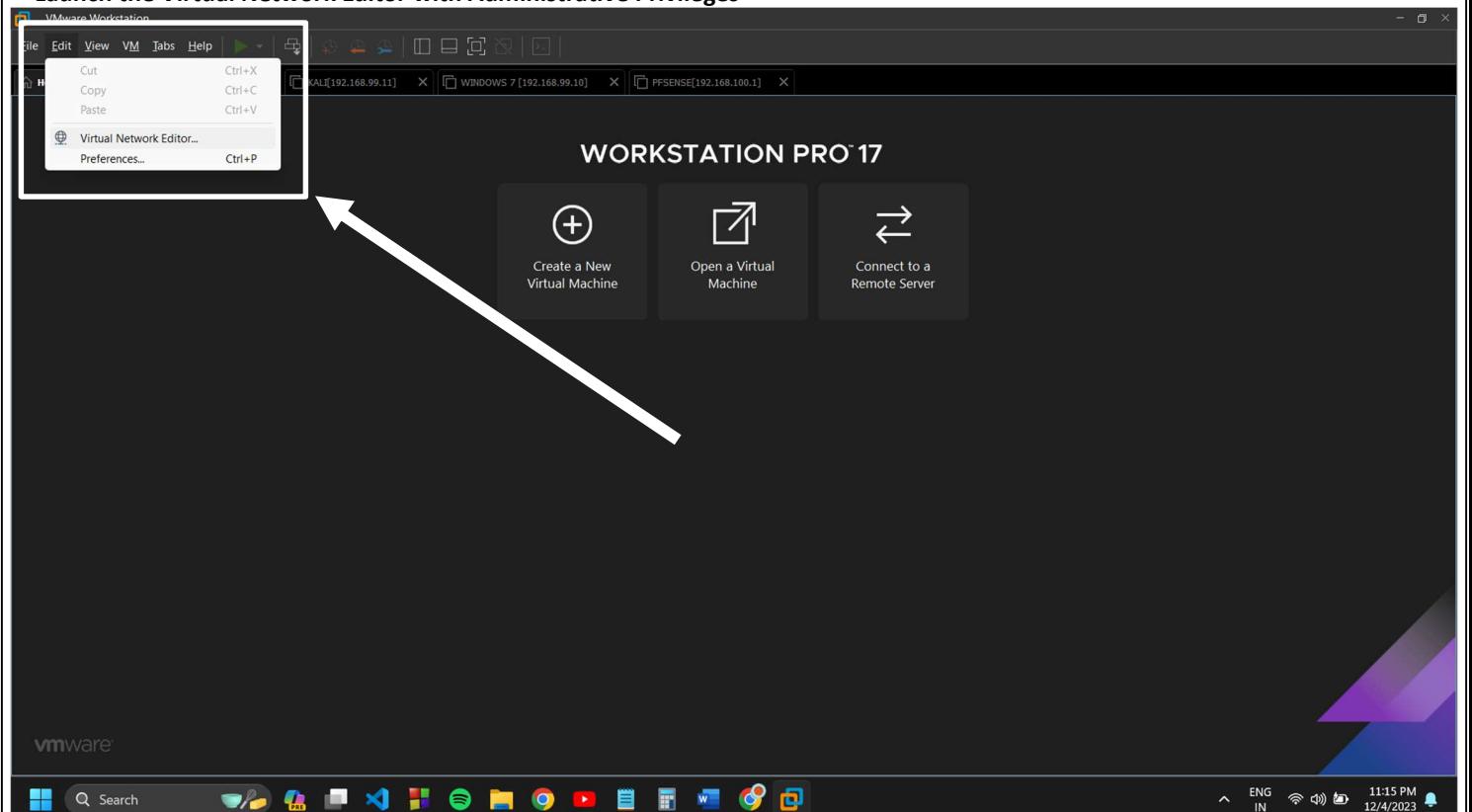






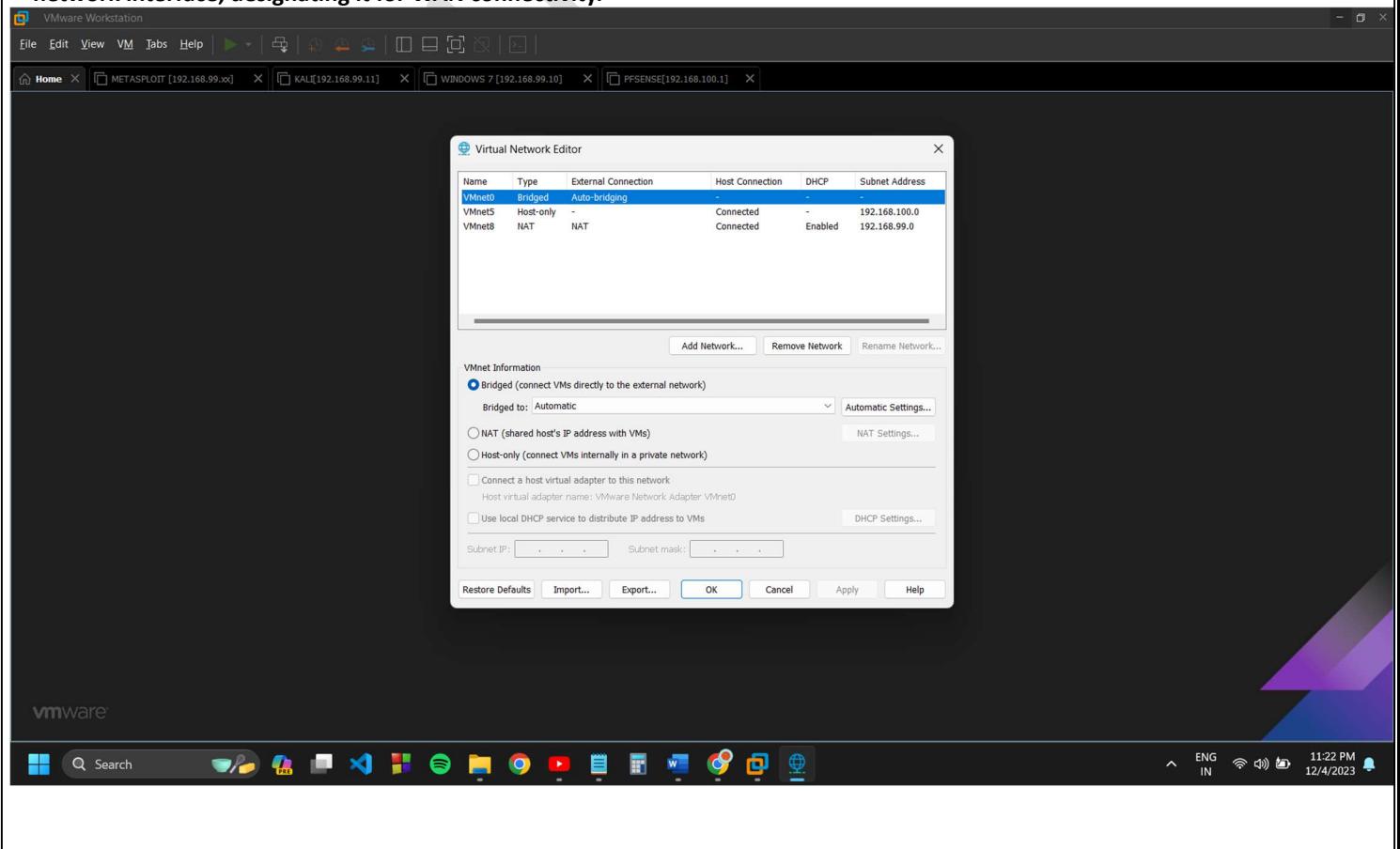
## Adjust Virtual Machine Settings in VMware:

- Access the virtual machine settings in VMware.
- Launch the Virtual Network Editor with Administrative Privileges



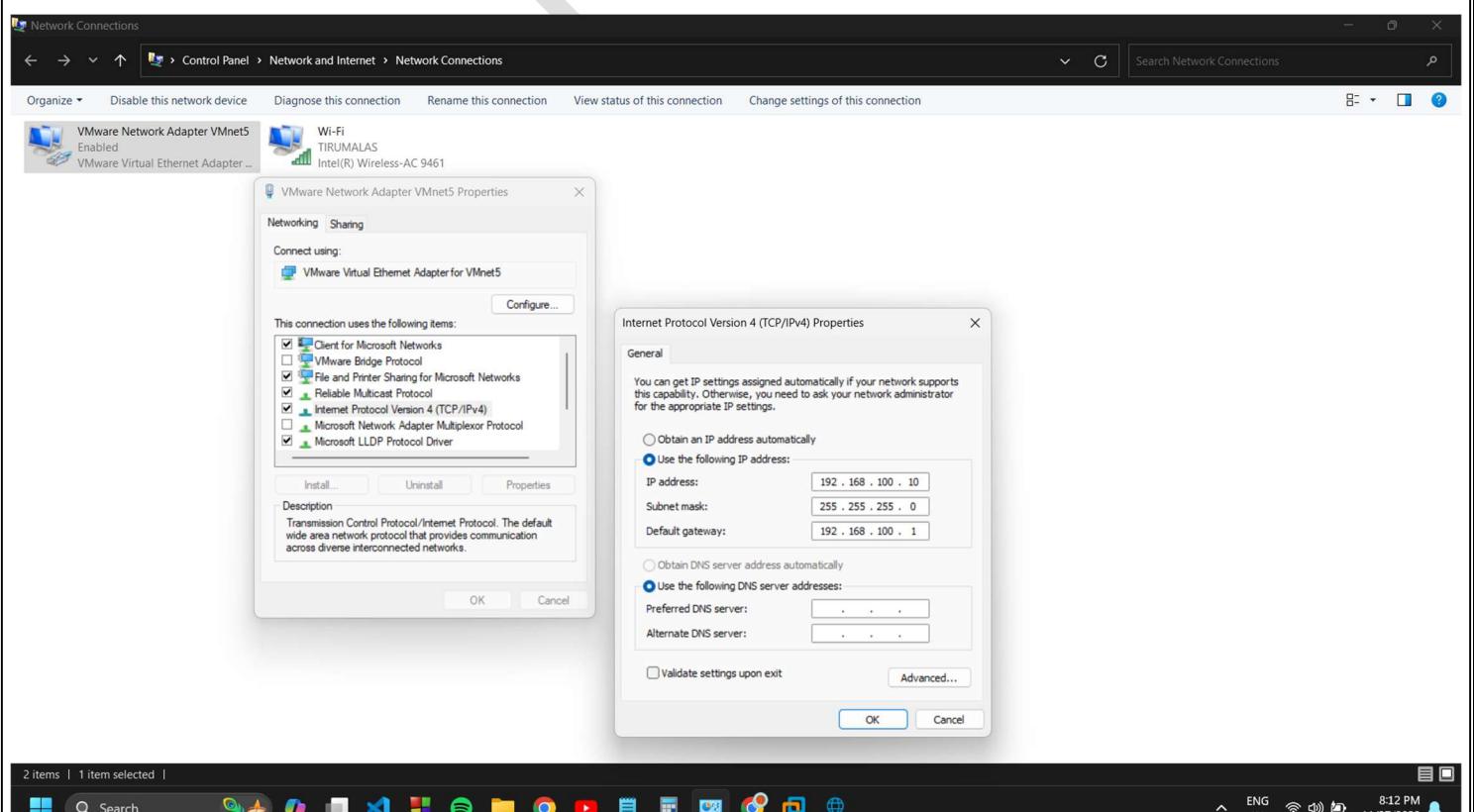
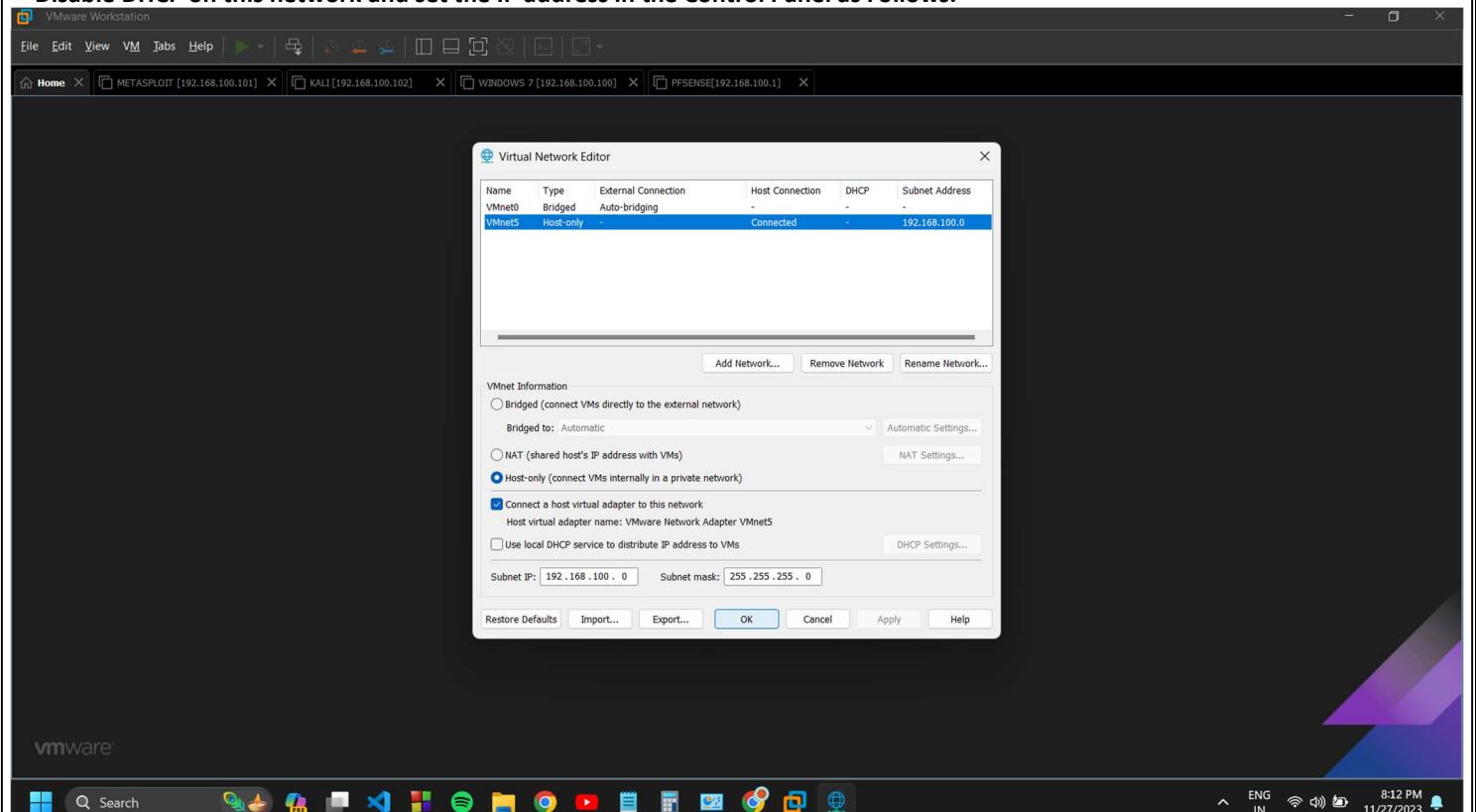
## Create a Network (e.g., vmnet0) for Autobridging (WAN):

- In the Virtual Network Editor, create a new network and assign it a specific identifier (e.g., vmnet0).
- Set the network type to "Autobridging." This configuration enables the virtual network to automatically bridge with a physical network interface, designating it for WAN connectivity.

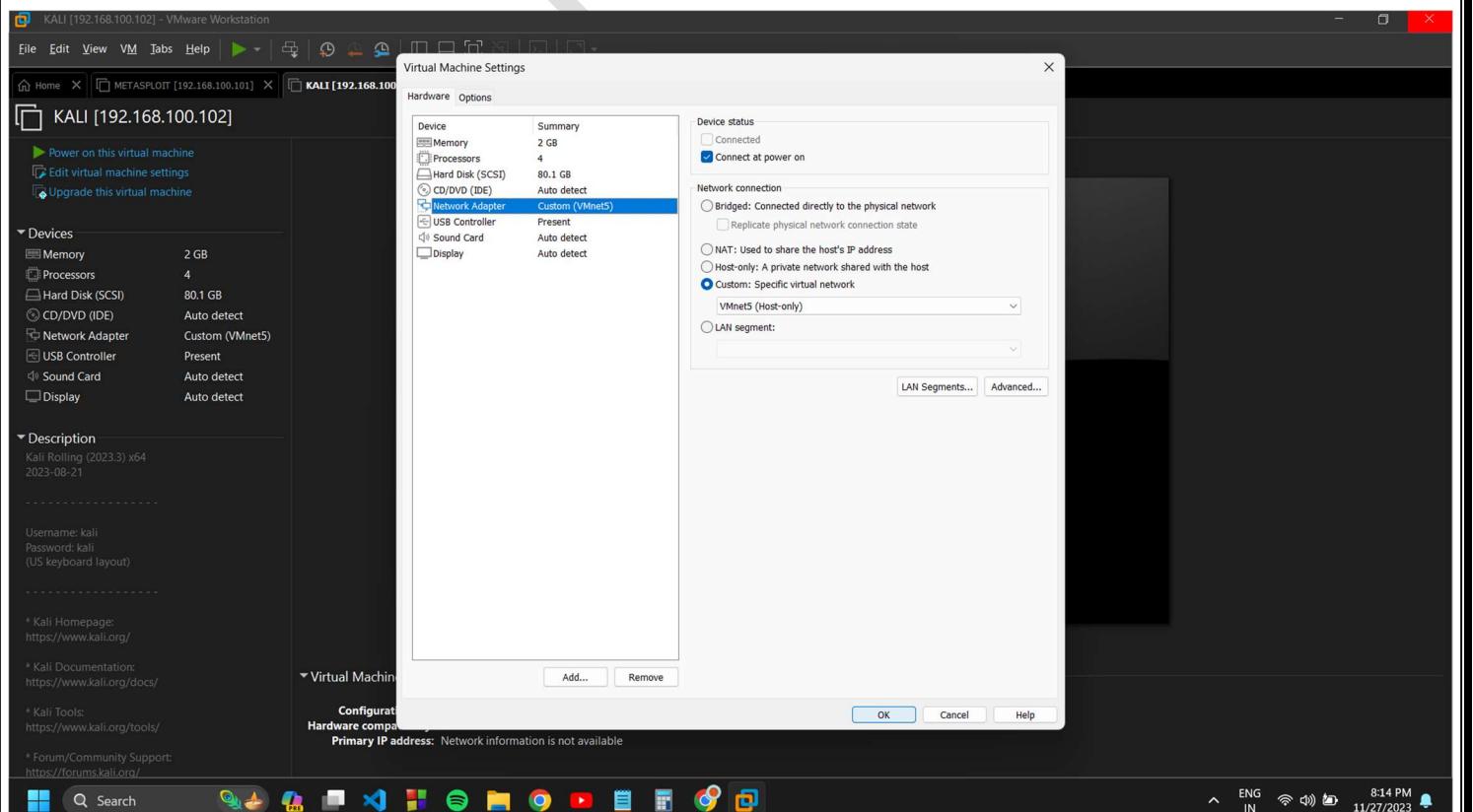
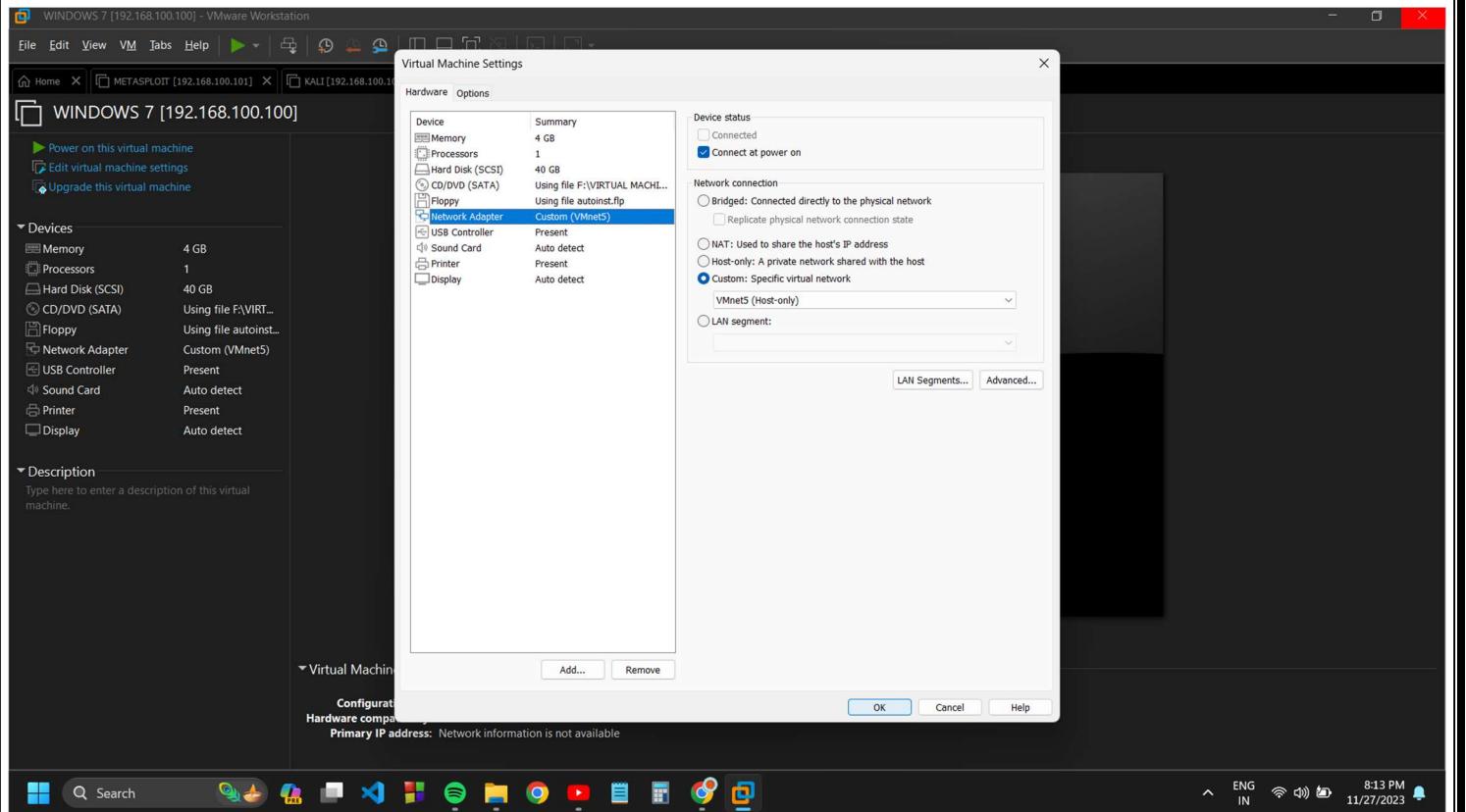


### Establish Another Network (e.g., vmnet5) as Host-Only (LAN):

- Create an additional network in the Virtual Network Editor, using a different identifier (e.g., vmnet5).
- Set the network type to "Host-Only." This setting ensures isolation, allowing communication solely between virtual machines connected to this network.
- Disable DHCP on this network and set the IP address in the Control Panel as Follows.

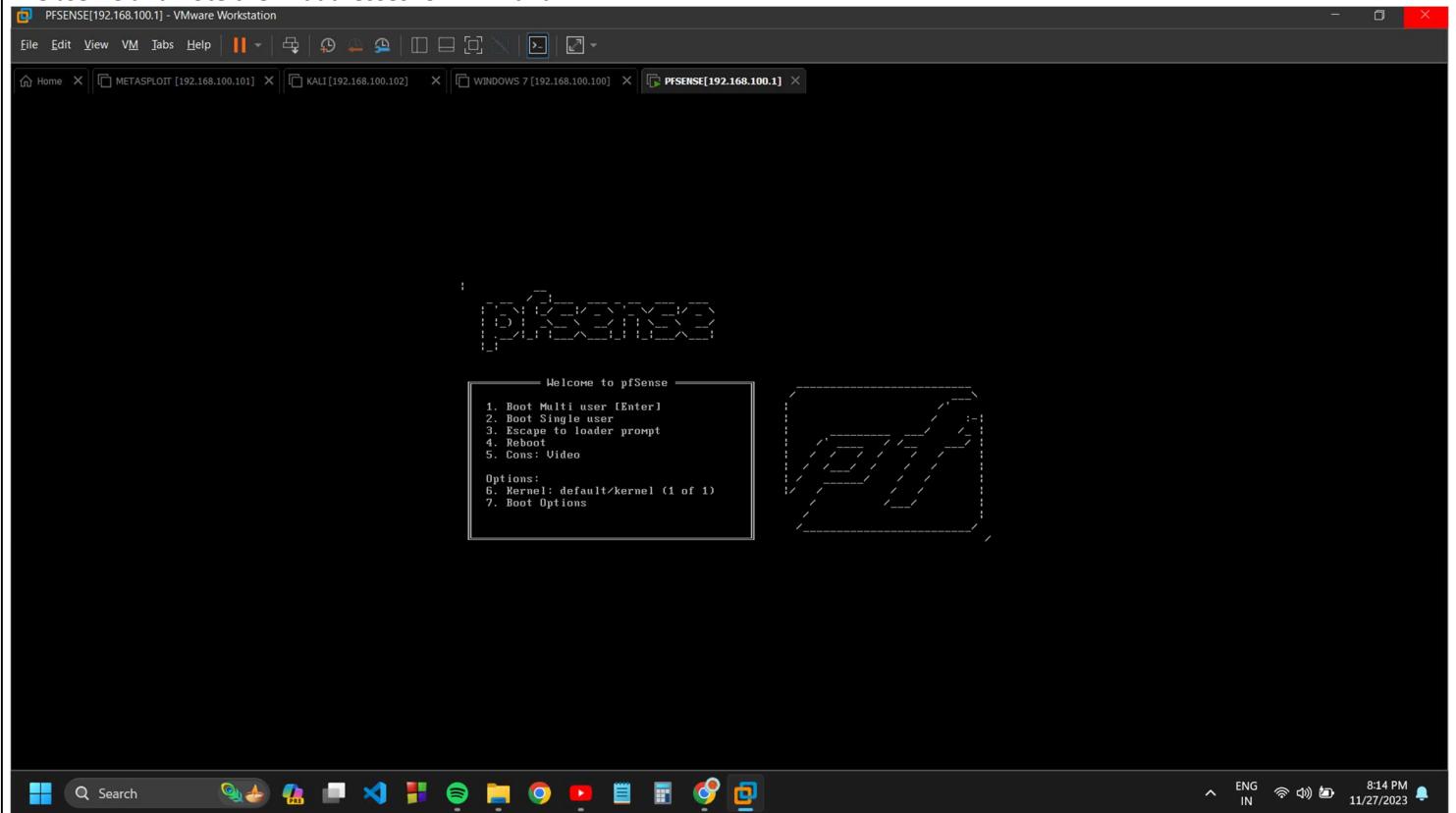


- Change Kali Linux's and Windows 7's network adapter to the Host-Only network vmnet5 in VMware



**Configure pfSense Network:**

- Observe and note the IP addresses for WAN and LAN.



```
FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)
```

```
VMware Virtual Machine - Netgate Device ID: 117ed97431b0ae7f1972
```

```
*** Welcome to pfSense 2.7.1-RELEASE (amd64) on pfSense ***
```

WAN (wan)	-> em0	-> v4/DHCP4: 192.168.0.150/24
		v6/DHCP6: fd01::20c:29ff:fed3:dd1/64
LAN (lan)	-> em1	-> v4: 192.168.100.1/24

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:
```

```
Message from syslogd@pfSense at Dec 4 15:26:21 ...
php-fpm[74111]: /index.php: Successful login for user 'admin' from: 192.168.100.
10 (Local Database)
```

## Access pfSense Web Interface:

- Open a web browser from another operating system.
- Enter the pfSense IP address.
- Login with username 'admin' and password 'pfsense.'

The screenshot shows a web browser window for the pfSense Login page. The URL is 192.168.100.1. The page has a dark blue header with the pfSense logo. Below it, the word "SIGN IN" is centered. There are two input fields: one for "admin" and one for a password (represented by a series of dots). A green "SIGN IN" button is at the bottom. At the very bottom of the page, there is a footer note: "pfSense is developed and maintained by Netgate. © ESF 2004 - 2023 [View license](#)". The browser's taskbar at the bottom shows various pinned icons and the date/time as 11/27/2023.

The screenshot shows the pfSense Status / Dashboard page. The URL is 192.168.100.1. The page features a navigation bar with links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. A red warning message at the top states: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." The main content area is divided into sections: "System Information" (listing Name: pfSense.home.arpa, User: admin@192.168.100.10, System: VMware Virtual Machine, BIOS: Phoenix Technologies LTD, Version: 6.00, Release Date: Thu Nov 12 2020, Version: 2.7.1-RELEASE (amd64), CPU Type: Intel(R) Core(TM) i3-1005G1 CPU @ 1.20GHz, AES-NI CPU Crypto: Yes (inactive), QAT Crypto: No, Hardware crypto: Inactive, Kernel PTI: Enabled, MDS Mitigation: Inactive), "Netgate Services And Support" (Contract type: Community Support, Community Support Only), and "NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES". The support section includes a note about Netgate Device ID (NDI) and a list of upgrade options. The browser's taskbar at the bottom shows various pinned icons and the date/time as 12/4/2023.

## CONFIGURING THE FIREWALL TO RESTRICT ACCESS TO CERTAIN WEBSITES

### Configure DNS Resolver:

- In pfSense, navigate to Services/DNS Resolver/.
- Edit the domain override.
- Specify the domain to block (e.g., facebook.com) and the IP address of the host in which the website has to block (e.g., 192.168.100.100).

The screenshot shows the pfSense web interface. On the left, the 'System Information' page displays various system details such as Name (pfSense.home.arpa), User (admin@192.168.100.10), System (VMware Virtual Machine), BIOS (Phoenix Technologies LTD), Version (2.7.1-RELEASE), CPU Type (Intel(R) Core(TM) i3-1005G1), Hardware crypto (Inactive), Kernel PTI (Enabled), and DS Mitigation (Inactive). A message at the top states: "WARNING: The 'admin' account password is set to the default value". On the right, there is a sidebar titled "Netgate Services And Support" with sections for "Contract type" (Community Support, Community Support Only), "NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES", and a link to "NETGATE RESOURCE LIBRARY". Below this, there is a message about purchasing pfSense from Netgate and access to community support resources. At the bottom of the sidebar, there are links for "Upgrade Your Support", "Community Support Resources", "Netgate Global Support FAQ", "Official pfSense Training by Netgate", and "Netgate Professional Services".

The screenshot shows two pages of the pfSense web interface. The top part shows the 'Host Overrides' section of the 'Services/DNS Resolver/' page. It includes a table with columns: Host, Parent domain of host, IP to return for host, Description, and Actions. A note below the table says: "Enter any individual hosts for which the resolver's standard DNS lookup process should be overridden and a specific IPv4 or IPv6 address should automatically be returned by the resolver. Standard and also non-standard names and parent domains can be entered, such as 'test', 'nas.home.arpa', 'mycompany.localdomain', '1.168.192.in-addr.arpa', or 'somesite.com'. Any lookup attempt for the host will automatically return the given IP address, and the usual lookup server for the domain will not be queried for the host's records." A 'Save' button is visible. The bottom part shows the 'Domain Overrides' section of the 'Services/DNS Resolver/' page. It includes a table with columns: Domain, Lookup Server IP Address, Description, and Actions. A note below the table says: "Enter any domains for which the resolver's standard DNS lookup process should be overridden and a different (non-standard) lookup server should be queried instead. Non-standard, 'invalid' and local domains, and subdomains, can also be entered, such as 'test', 'nas.home.arpa', 'mycompany.localdomain', '1.168.192.in-addr.arpa', or 'somesite.com'. The IP address is treated as the authoritative lookup server for the domain (including all of its subdomains), and other lookup servers will not be queried. If there are multiple authoritative DNS servers available for a domain then make a separate entry for each, using the same domain name." A 'Save' button is also visible.

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\SATISH>ipconfig

Windows IP Configuration

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . . . . : 

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . . . . . : home.arpa
    Link-local IPv6 Address . . . . . : fe80::d4d:91c7:c807:4134%11
    IPv4 Address . . . . . : 192.168.100.100
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.100.1

Tunnel adapter isatap.home.arpa:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . . . . : home.arpa

Tunnel adapter isatap.{7AB2035A-7411-4EDB-A36D-F73A4B369704}:

    Media State . . . . . . . . . : Media disconnected
```

WINDOWS 7 IP : 192.168.100.100

The screenshot shows the pfSense web interface for managing DNS resolver settings. A specific configuration for the domain `facebook.com` is highlighted. Two arrows point to the `Domain` field (containing `facebook.com`) and the `IP Address` field (containing `192.168.100.100`). The interface includes sections for `TLS Queries`, `TLS Hostname`, and `Description` (set to `BLOCK UNWANTED WEBSITES`). A note at the bottom explains the purpose of this configuration.

**Services / DNS Resolver / General Settings / Edit Domain Override**

**Domains to Override with Custom Lookup Servers**

<b>Domain</b>	<code>facebook.com</code>
Domain whose lookups will be directed to a user-specified DNS lookup server.	
<b>IP Address</b>	<code>192.168.100.100</code>
IPv4 or IPv6 address of the authoritative DNS server for this domain. e.g.: 192.168.100.100 To use a non-default port for communication, append an '@' with the port number.	
<b>TLS Queries</b>	<input type="checkbox"/> Use SSL/TLS for DNS Queries forwarded to this server When set, queries to all DNS servers for this domain will be sent using SSL/TLS on the default port of 853.
<b>TLS Hostname</b>	<input type="text"/>
An optional TLS hostname used to verify the server certificate when performing TLS Queries.	
<b>Description</b>	<code>BLOCK UNWANTED WEBSITES</code>
A description may be entered here for administrative reference (not parsed).	

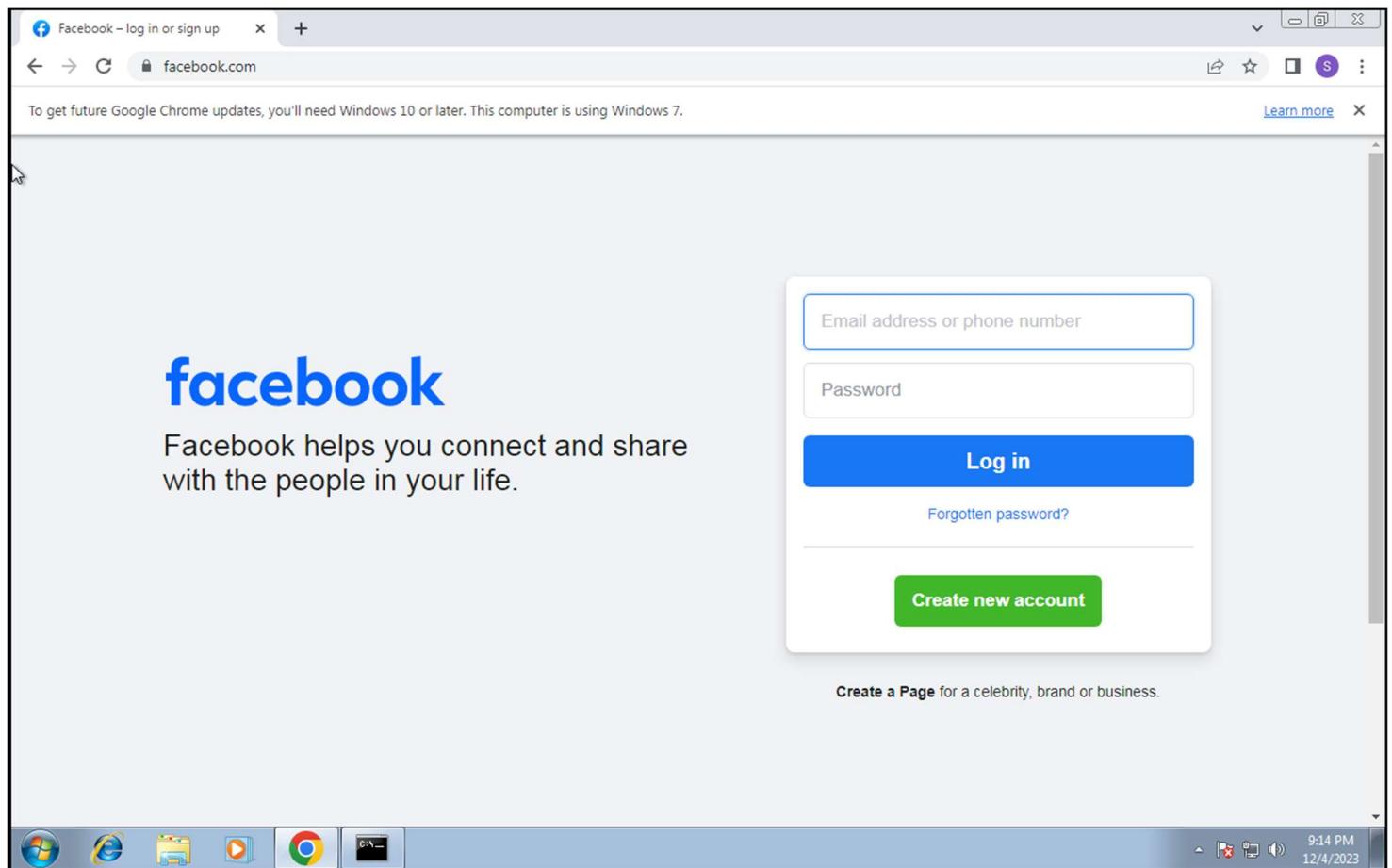
This page is used to specify domains for which the resolver's standard DNS lookup process will be overridden, and the resolver will query a different (non-standard) lookup server instead. It is possible to enter 'non-standard', 'invalid' and 'local' domains such as 'test', 'nas.home.arpa', 'mycompany.localdomain', or '1.168.192.in-addr.arpa', as well as usual publicly resolvable domains such as 'org', 'info', or 'google.co.uk'. The IP address entered will be treated as the IP address of an authoritative lookup server for the domain (including all of its subdomains), and other lookup servers will not be queried.

**Save**

pfSense is developed and maintained by Netgate © ESE 2004 - 2023 [View license](#)

Search ENG IN 9:14 PM 12/4/2023

- Before blocking a domain, check its availability.



- Now return to the pfSense web interface and click on apply changes.

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**

**Host Overrides**

Host	Parent domain of host	IP to return for host	Description	Actions
				<a href="#">Add</a>

Enter any individual hosts for which the resolver's standard DNS lookup process should be overridden and a specific IPv4 or IPv6 address should automatically be returned by the resolver. Standard and also non-standard names and parent domains can be entered, such as 'test', 'nas.home.arpá', 'mycompany.localdomain', '1.168.192.in-addr.arpá', or 'somesite.com'. Any lookup attempt for the host will automatically return the given IP address, and the usual lookup server for the domain will not be queried for the host's records.

**Domain Overrides**

Domain	Lookup Server IP Address	Description	Actions
facebook.com	192.168.100.100	BLOCK UNWANTED WEBSITES	<a href="#">Edit</a> <a href="#">Delete</a>

Enter any domains for which the resolver's standard DNS lookup process should be overridden and a different (non-standard) lookup server should be queried instead. Non-standard, 'invalid' and local domains, and subdomains, can also be entered, such as 'test', 'nas.home.arpá', 'mycompany.localdomain', '1.168.192.in-addr.arpá', or 'somesite.com'. The IP address is treated as the authoritative lookup server for the domain (including all of its subdomains), and other lookup servers will not be queried. If there are multiple authoritative DNS servers available for a domain then make a separate entry for each, using the same domain name.

[Add](#)

[Info](#)

pfSense is developed and maintained by Netgate. © ESF 2004 - 2023 [View license](#).

- Availability of domain after blocking the domain.

www.facebook.com

facebook.com

This site can't be reached

Check if there is a typo in www.facebook.com.

If spelling is correct, [try running windows network Diagnostics](#).

DNS\_PROBE\_FINISHED\_NXDOMAIN

[Reload](#)

9:19 PM 12/4/2023

- Now follow the same procedure and block Instagram.com from the Kali Linux virtual machine.

```
(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.100.102  netmask 255.255.255.0  broadcast 192.168.100.255
              inet6 fe80::1b14:d6c5:9a34:e3ce  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:ca:5c:c9  txqueuelen 1000  (Ethernet)
          RX packets 333  bytes 41703 (40.7 KiB)
          RX errors 0  dropped 0  overruns 0  frame 0
          TX packets 30  bytes 4070 (3.9 KiB)
          TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
              inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
          RX packets 4  bytes 240 (240.0 B)
          RX errors 0  dropped 0  overruns 0  frame 0
          TX packets 4  bytes 240 (240.0 B)
          TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

(kali㉿kali)-[~]
$
```

pfSense.home.arpd - Services: D +

Not secure | 192.168.100.1/services\_unbound\_domainoverride\_edit.php

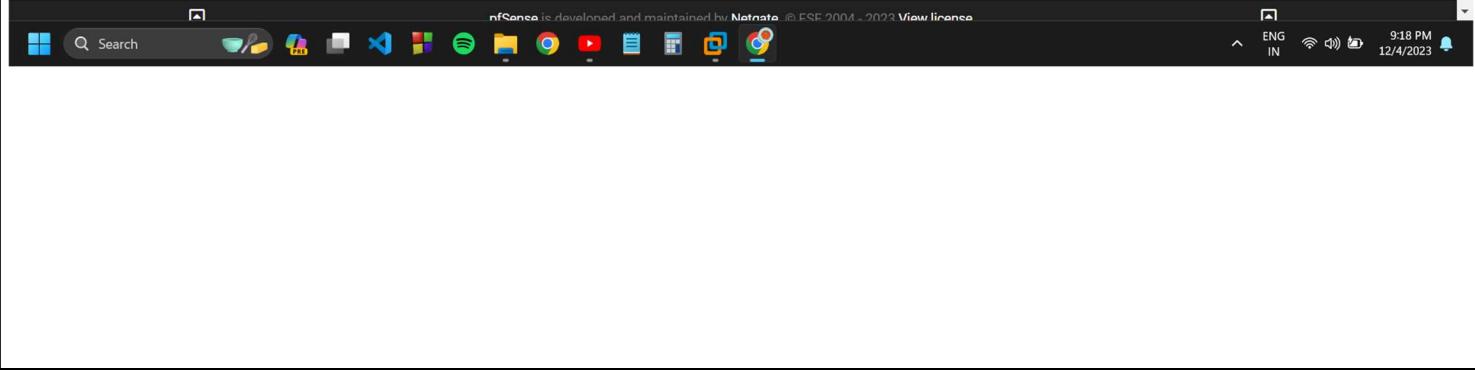
Services / DNS Resolver / General Settings / Edit Domain Override

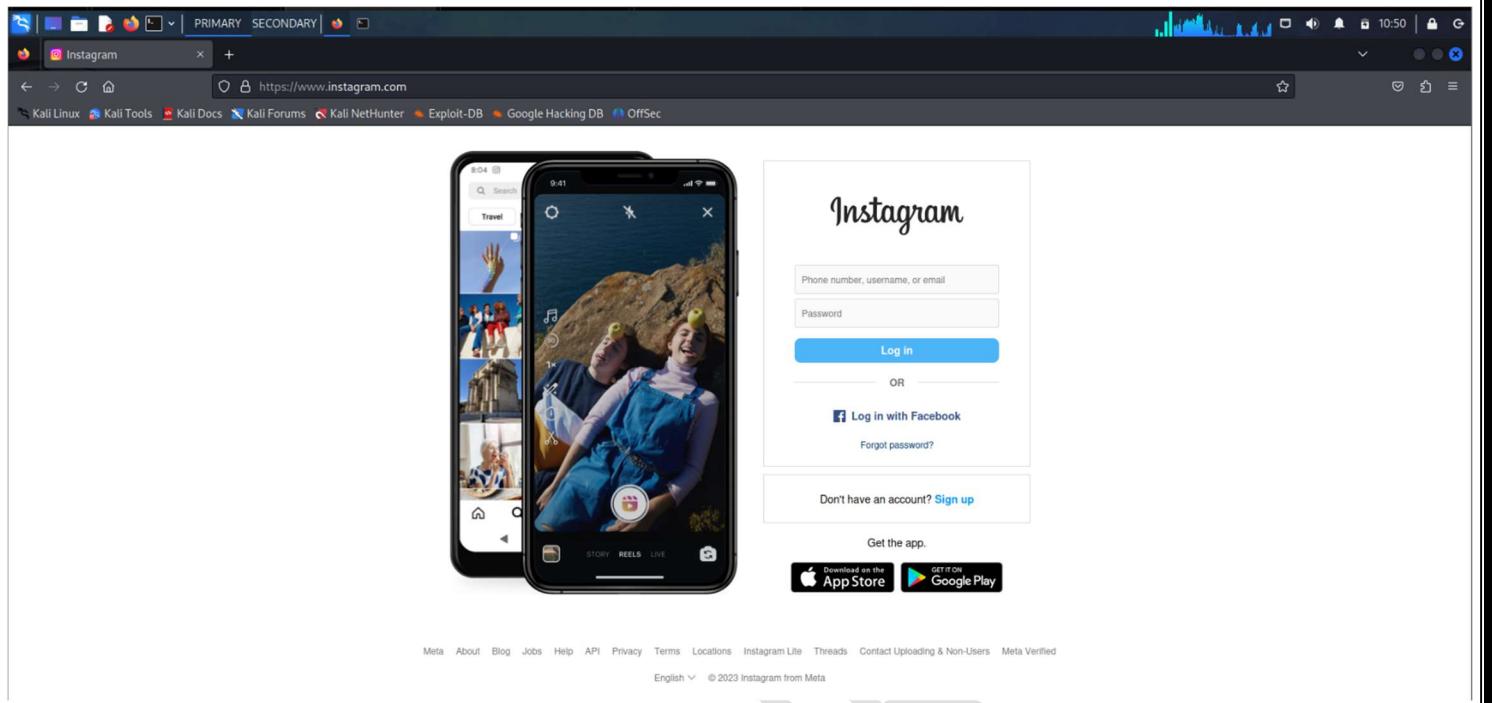
**Domains to Override with Custom Lookup Servers**

<b>Domain</b>	<input type="text" value="instagram.com"/>	Domain whose lookups will be directed to a user-specified DNS lookup server.
<b>IP Address</b>	<input type="text" value="192.168.100.102"/>	IPv4 or IPv6 address of the authoritative DNS server for this domain. e.g.: 192.168.100.100 To use a non-default port for communication, append an '@' with the port number.
<b>TLS Queries</b>	<input checked="" type="checkbox"/> Use SSL/TLS for DNS Queries forwarded to this server	When set, queries to all DNS servers for this domain will be sent using SSL/TLS on the default port of 853.
<b>TLS Hostname</b>	<input type="text"/>	An optional TLS hostname used to verify the server certificate when performing TLS Queries.
<b>Description</b>	<input type="text" value="BLOCK INSTAGRAM IN KALI LINUX"/>	A description may be entered here for administrative reference (not parsed).

This page is used to specify domains for which the resolver's standard DNS lookup process will be overridden, and the resolver will query a different (non-standard) lookup server instead. It is possible to enter 'non-standard', 'invalid' and 'local' domains such as 'test', 'nas.home.arpd', 'mycompany.localdomain', or '1.168.192.in-addr.arpd', as well as usual publicly resolvable domains such as 'org', 'info', or 'google.co.uk'. The IP address entered will be treated as the IP address of an authoritative lookup server for the domain (including all of its subdomains), and other lookup servers will not be queried.

**Save**





A screenshot of a pfSense web interface. The top navigation bar includes links for Meta, About, Blog, Jobs, Help, API, Privacy, Terms, Locations, Instagram Lite, Threads, Contact, Uploading & Non-Users, Meta Verified, English, and © 2023 Instagram from Meta. The main content area shows a warning message: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this is a section titled "Services / DNS Resolver / General Settings". A message states: "The DNS resolver configuration has been changed. The changes must be applied for them to take effect." A green "Apply Changes" button is visible. Another message at the bottom of the page says: "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." At the bottom of the page are tabs for General Settings, Advanced Settings, and Access Lists. Under General Settings, there is a "General DNS Resolver Options" section with the following configuration:

- Enable:**  Enable DNS resolver
- Listen Port:** 53
- Enable SSL/TLS Service:**  Respond to incoming SSL/TLS queries from local clients
- SSL/TLS Certificate:** GUI default (6564840f0b792)

The status bar at the bottom of the screen shows various icons and the date/time: 9:50 PM, ENG IN, 12/4/2023.

pfSense.home.arpa - Services: 0 | ChatGPT

Not secure | 192.168.100.1/services\_unbound.php

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](#)

### Host Overrides

Host	Parent domain of host	IP to return for host	Description	Actions
Enter any individual hosts for which the resolver's standard DNS lookup process should be overridden and a specific IPv4 or IPv6 address should automatically be returned by the resolver. Standard and also non-standard names and parent domains can be entered, such as 'test', 'nas.home.arpa', 'mycompany.localdomain', '1.168.192.in-addr.arpa', or 'somesite.com'. Any lookup attempt for the host will automatically return the given IP address, and the usual lookup server for the domain will not be queried for the host's records.				

[+ Add](#)

### Domain Overrides

Domain	Lookup Server IP Address	Description	Actions
facebook.com	192.168.100.100	BLOCK UNWANTED WEBSITES	<a href="#"></a> <a href="#"></a>
instagram.com	192.168.100.102	BLOCK INSTAGRAM IN KALI LINUX	<a href="#"></a> <a href="#"></a>

Enter any domains for which the resolver's standard DNS lookup process should be overridden and a different (non-standard) lookup server should be queried instead. Non-standard, 'invalid' and local domains, and subdomains, can also be entered, such as 'test', 'nas.home.arpa', 'mycompany.localdomain', '1.168.192.in-addr.arpa', or 'somesite.com'. The IP address is treated as the authoritative lookup server for the domain (including all of its subdomains), and other lookup servers will not be queried. If there are multiple authoritative DNS servers available for a domain then make a separate entry for each, using the same domain name.

[+ Add](#)

pfSense is developed and maintained by Netgate. © ESF 2004 - 2023 [View license](#).

Search, Taskbar icons, Network status, Date/Time: 9:25 PM 12/4/2023

PRIMARY SECONDARY

Server Not Found

https://www.instagram.com

Kali Linux Kali Tools Kali Docs Kali Forums Kali Nethunter Exploit-DB Google Hacking DB OffSec

Hmm. We're having trouble finding that site.

We can't connect to the server at www.instagram.com.

If you entered the right address, you can:

- Try again later
- Check your network connection
- Check that Firefox has permission to access the web (you might be connected but behind a firewall)

[Try Again](#)