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.

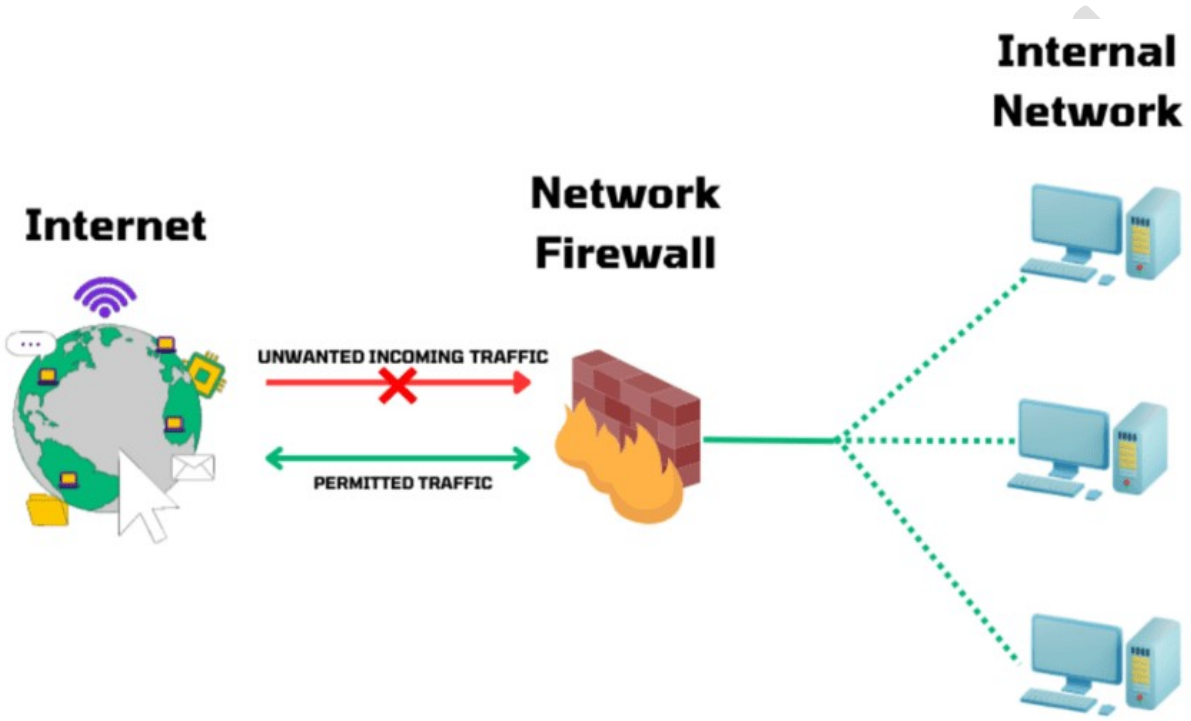
Firewall Policies:

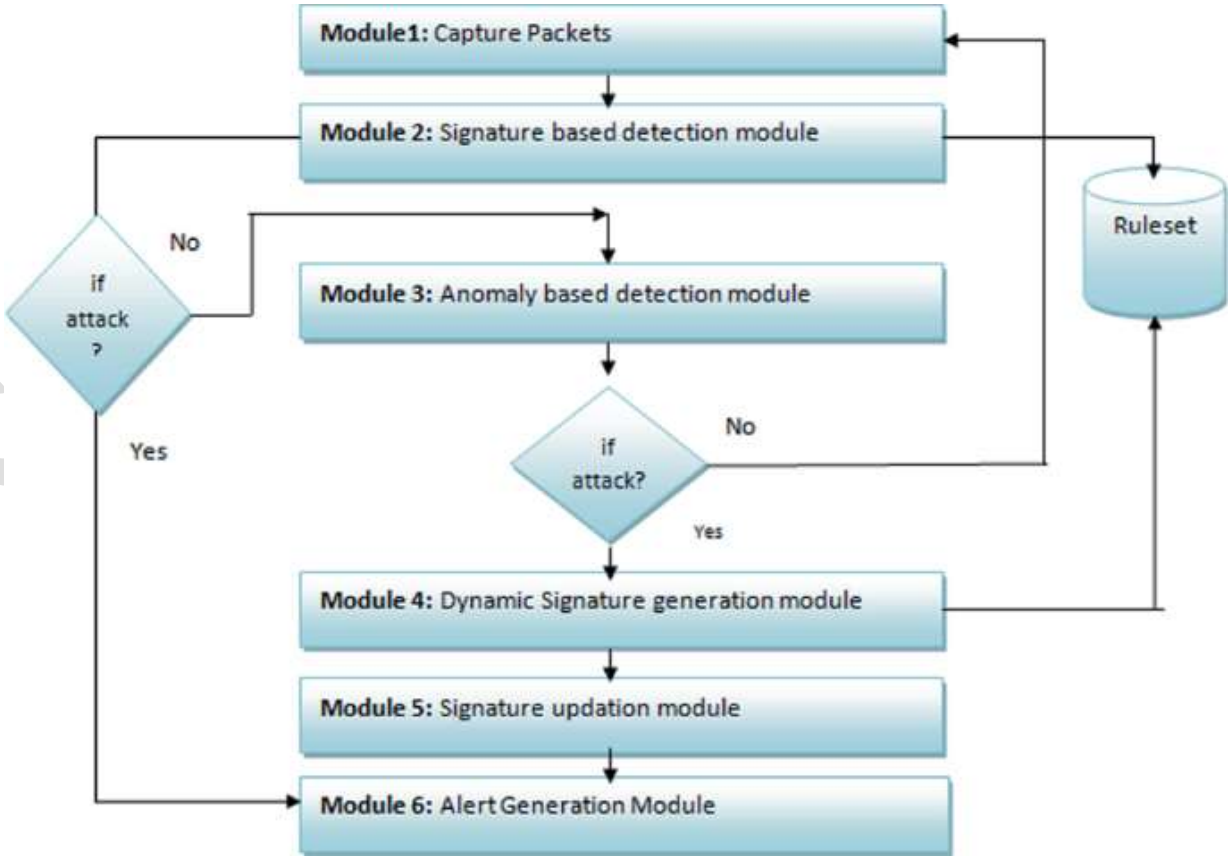
Ingress and Egress Rules:

Ingress rules control incoming traffic.
Egress rules control outgoing traffic.

Default Deny vs. Default Allow:

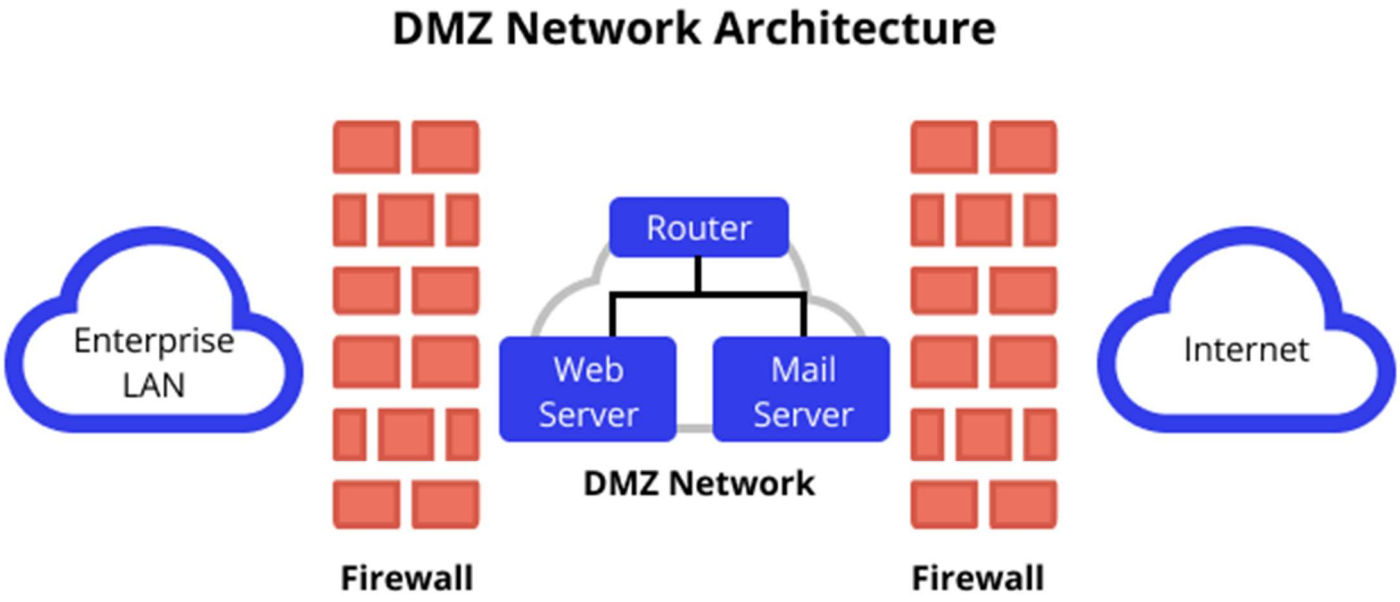
Default deny blocks all traffic unless explicitly allowed.
Default allow allows all traffic unless explicitly blocked.





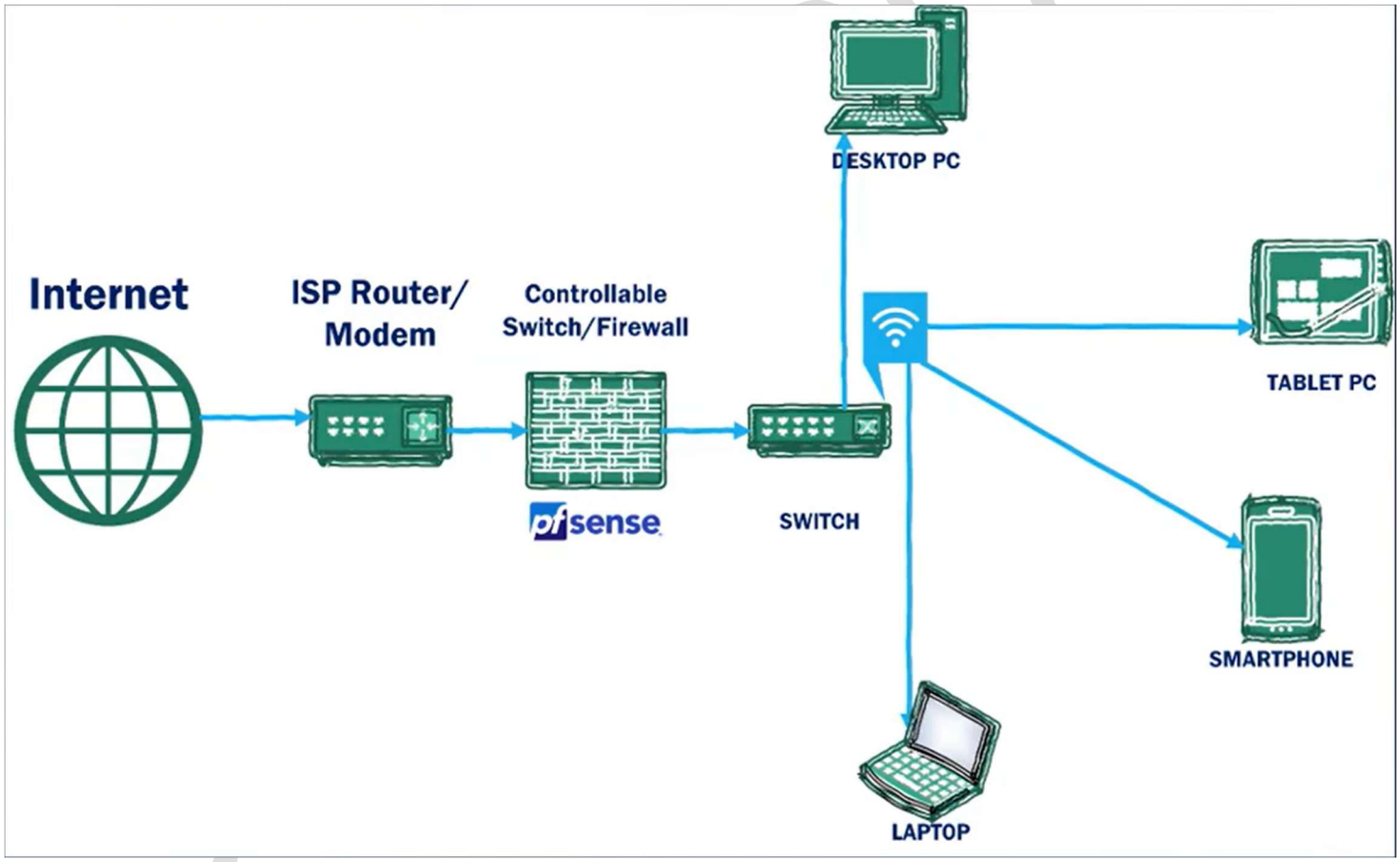
Demilitarized Zone:

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.



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.

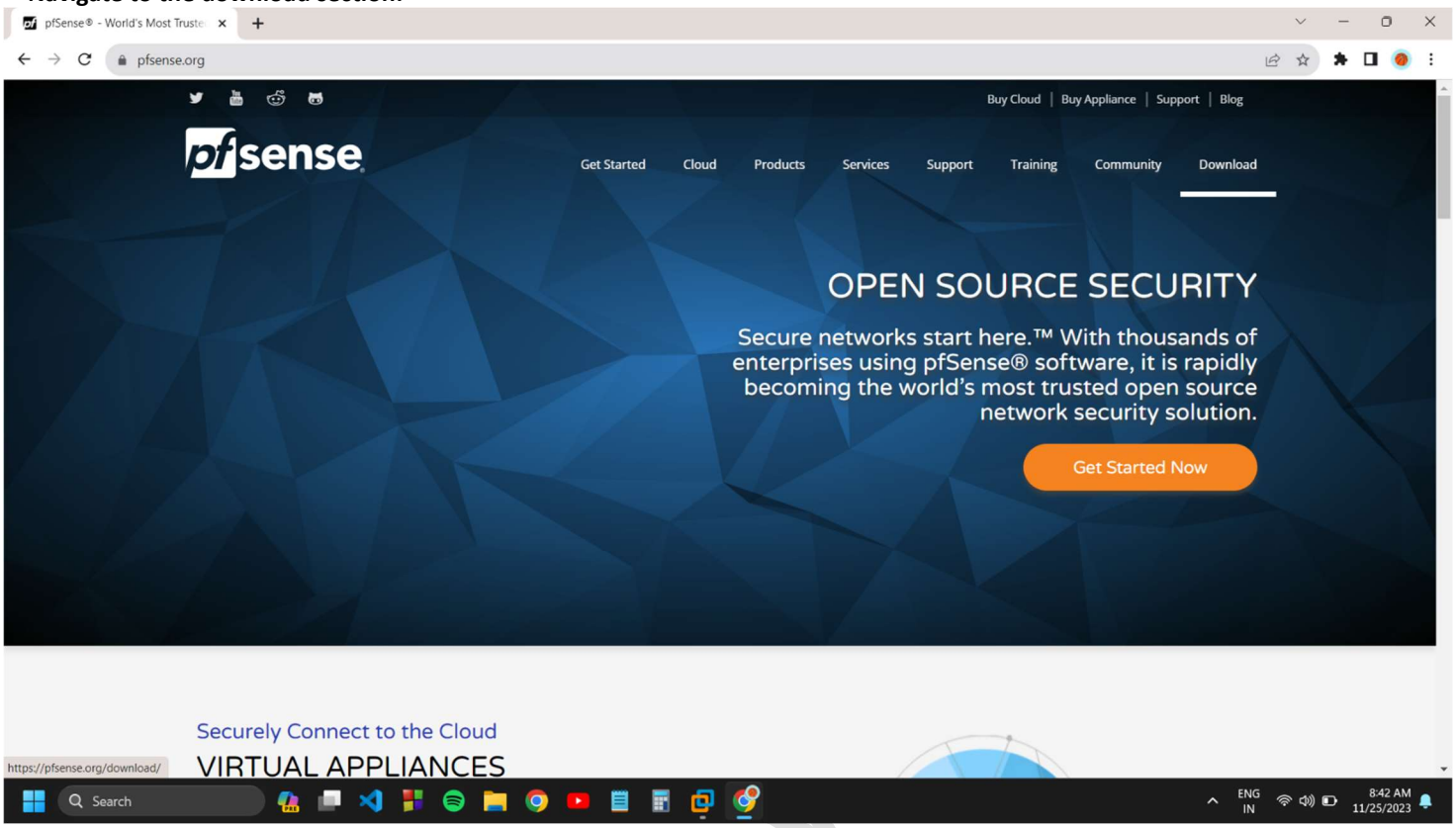
Pfsense Architecture:



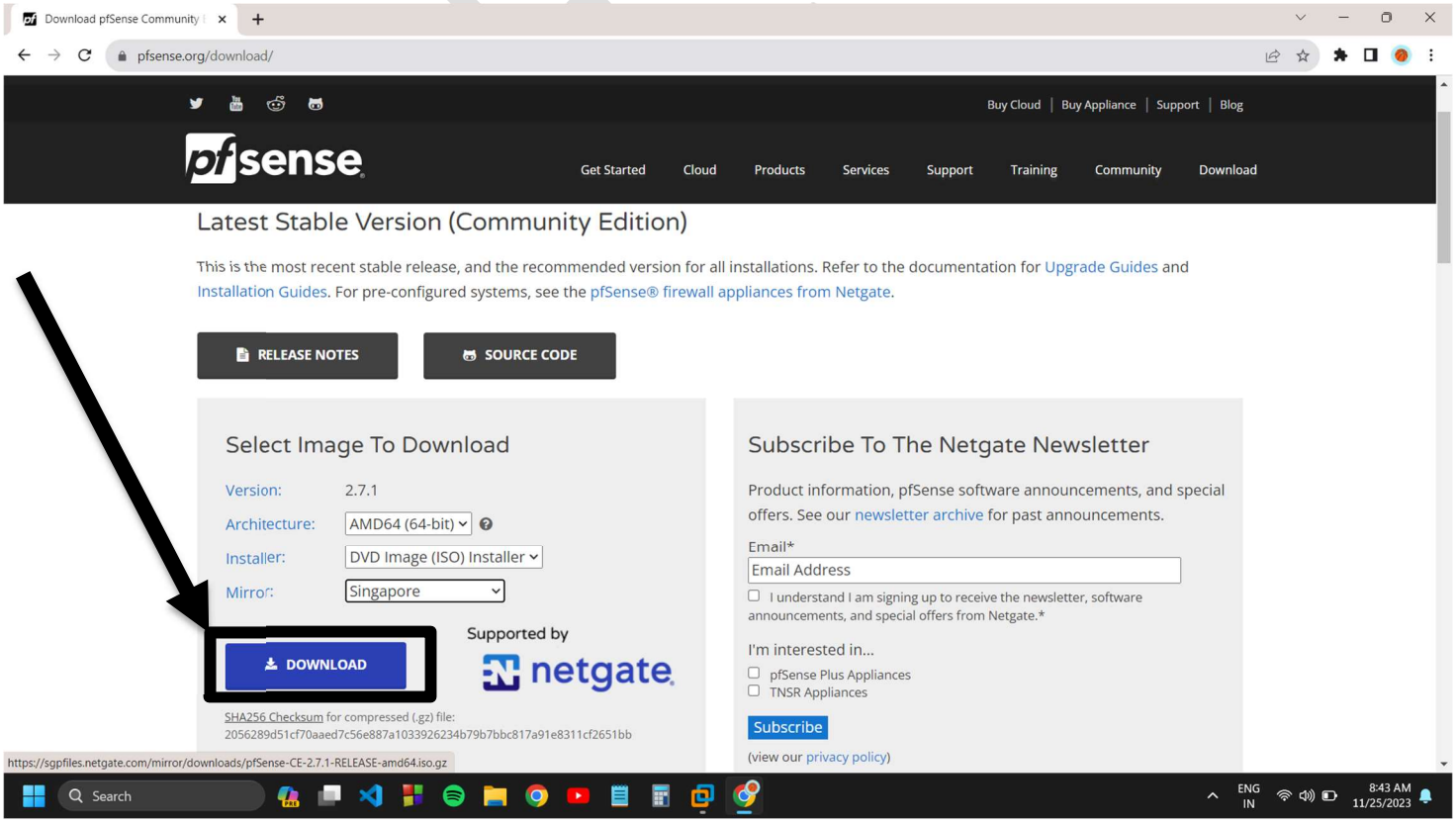
Installation & Configuration Of Pfsense:

Download pfSense ISO:

- **Visit pfsense.org.**
- **Navigate to the download section.**

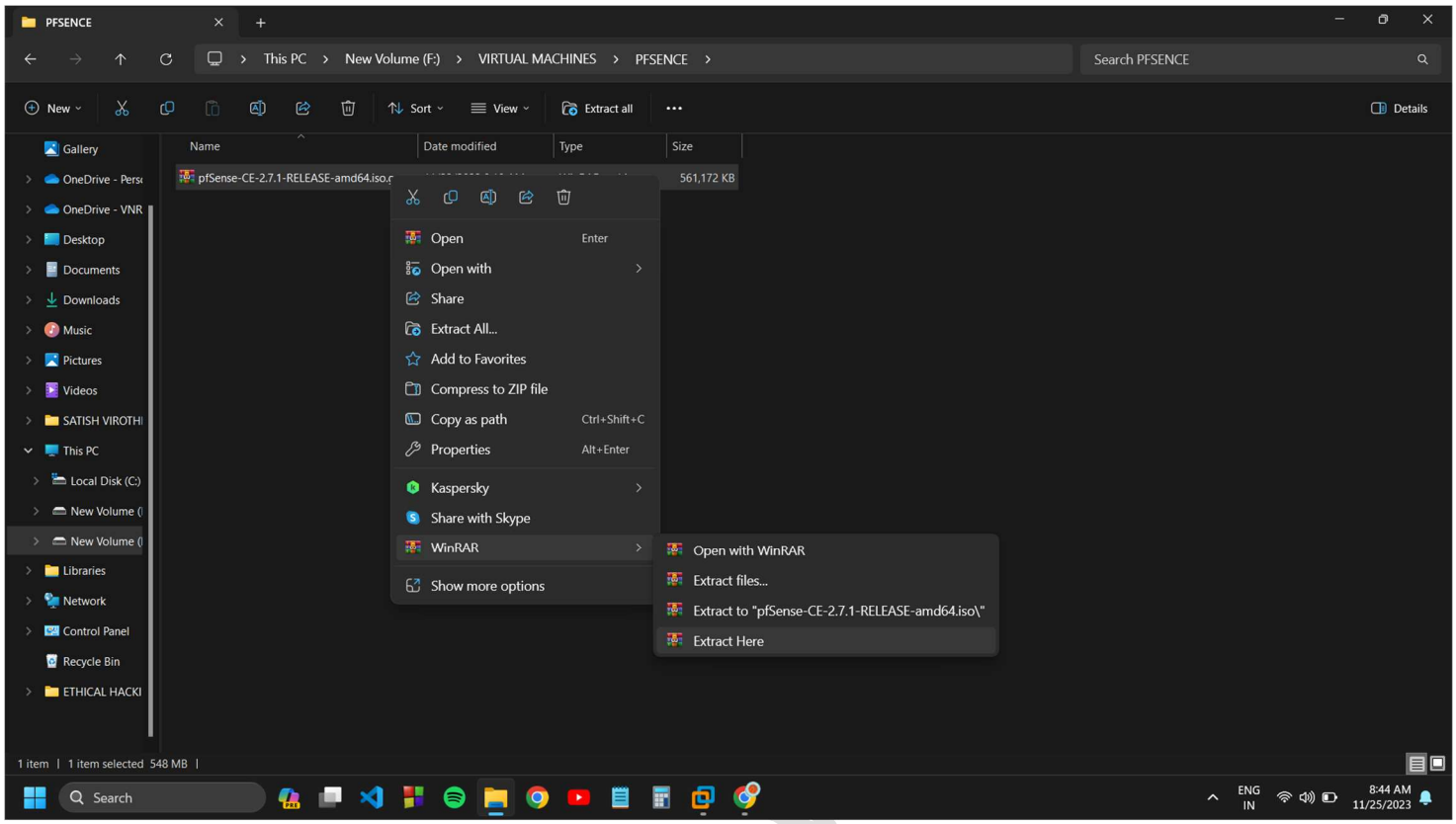


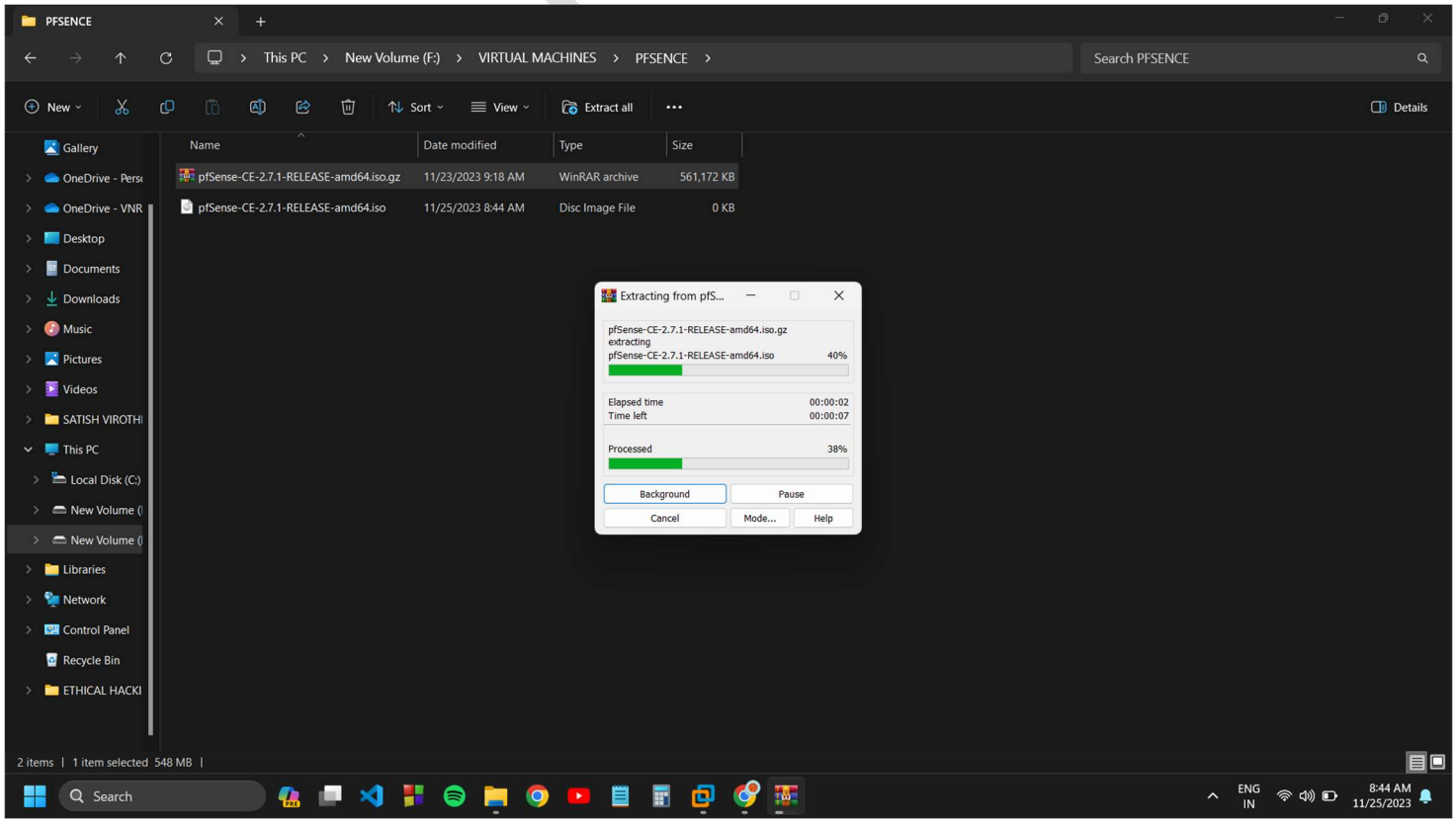
- **Download the pfSense ISO image file.**



Unzip Downloaded File:

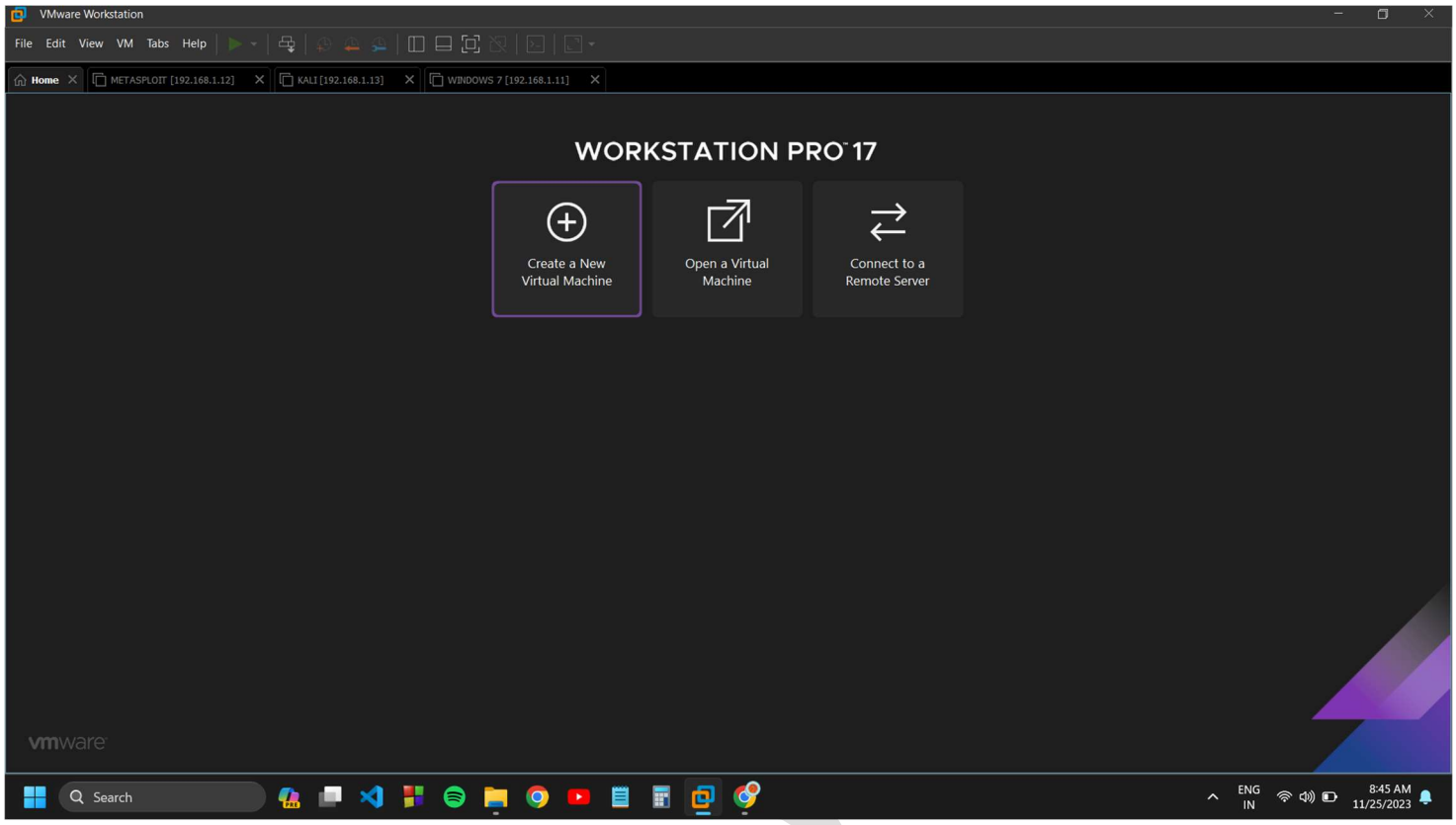
- **Locate the downloaded file in your designated folder.**
- **Unzip the folder to access the pfSense ISO file.**

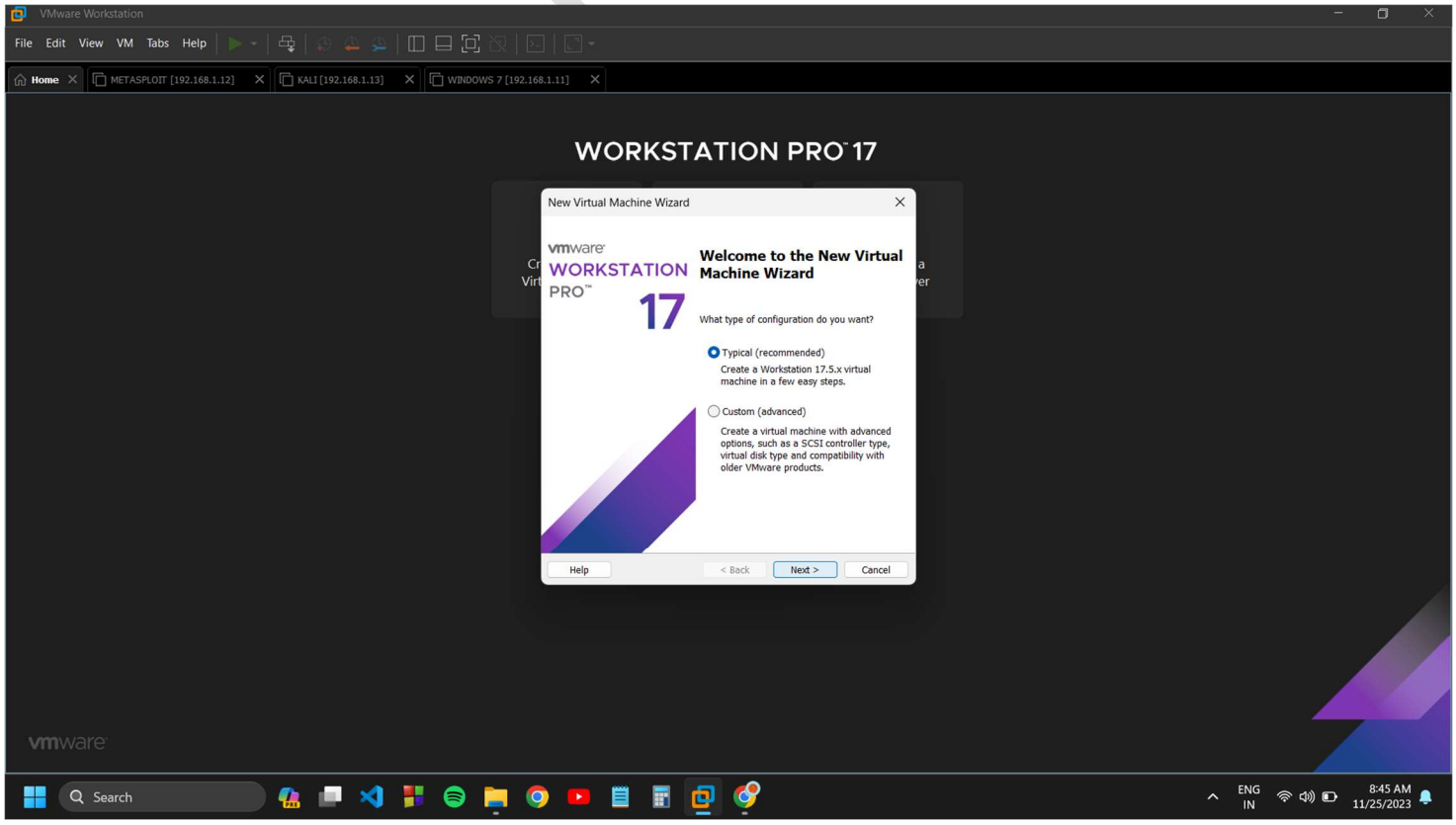




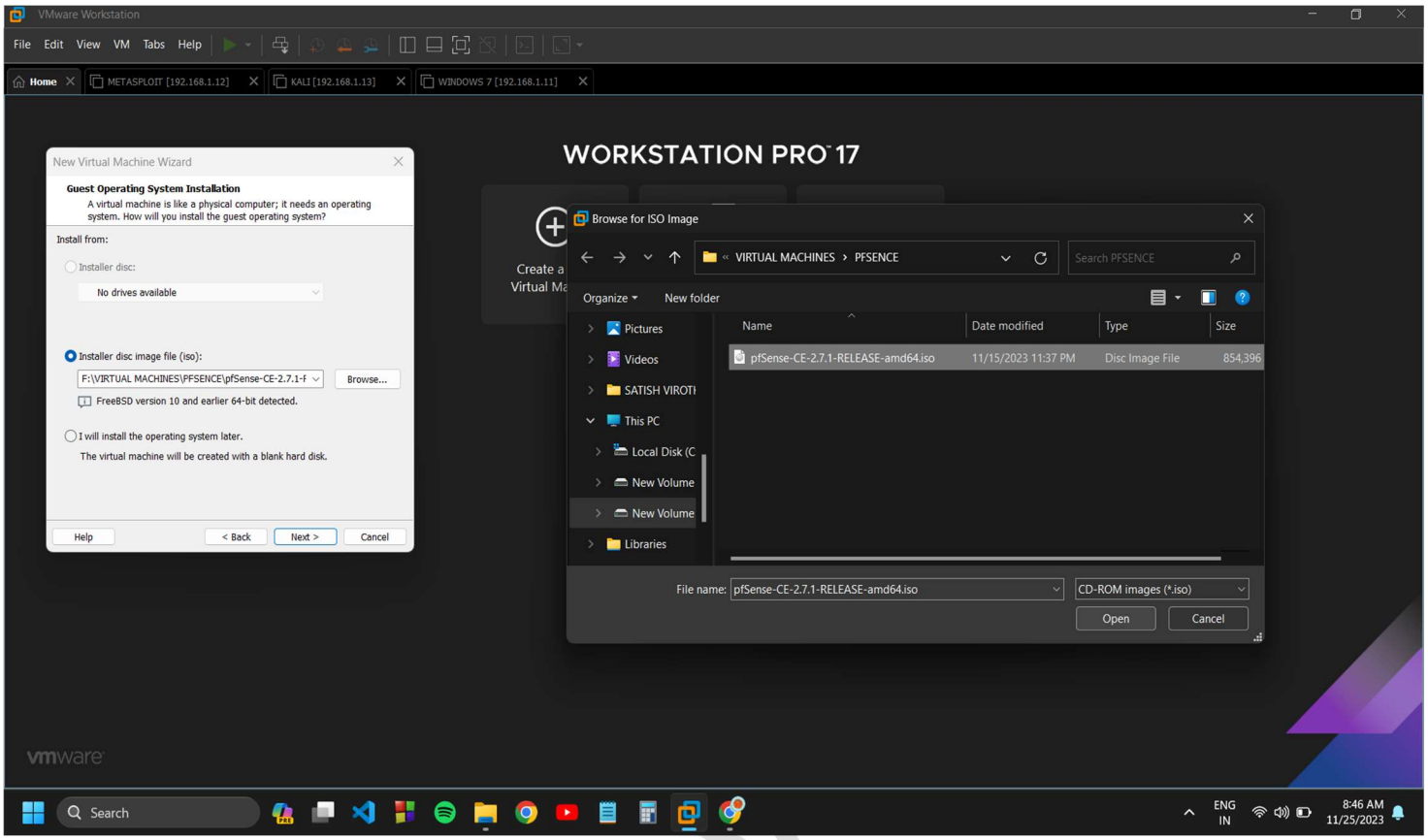
Create a Virtual Machine (VM) in VMware:

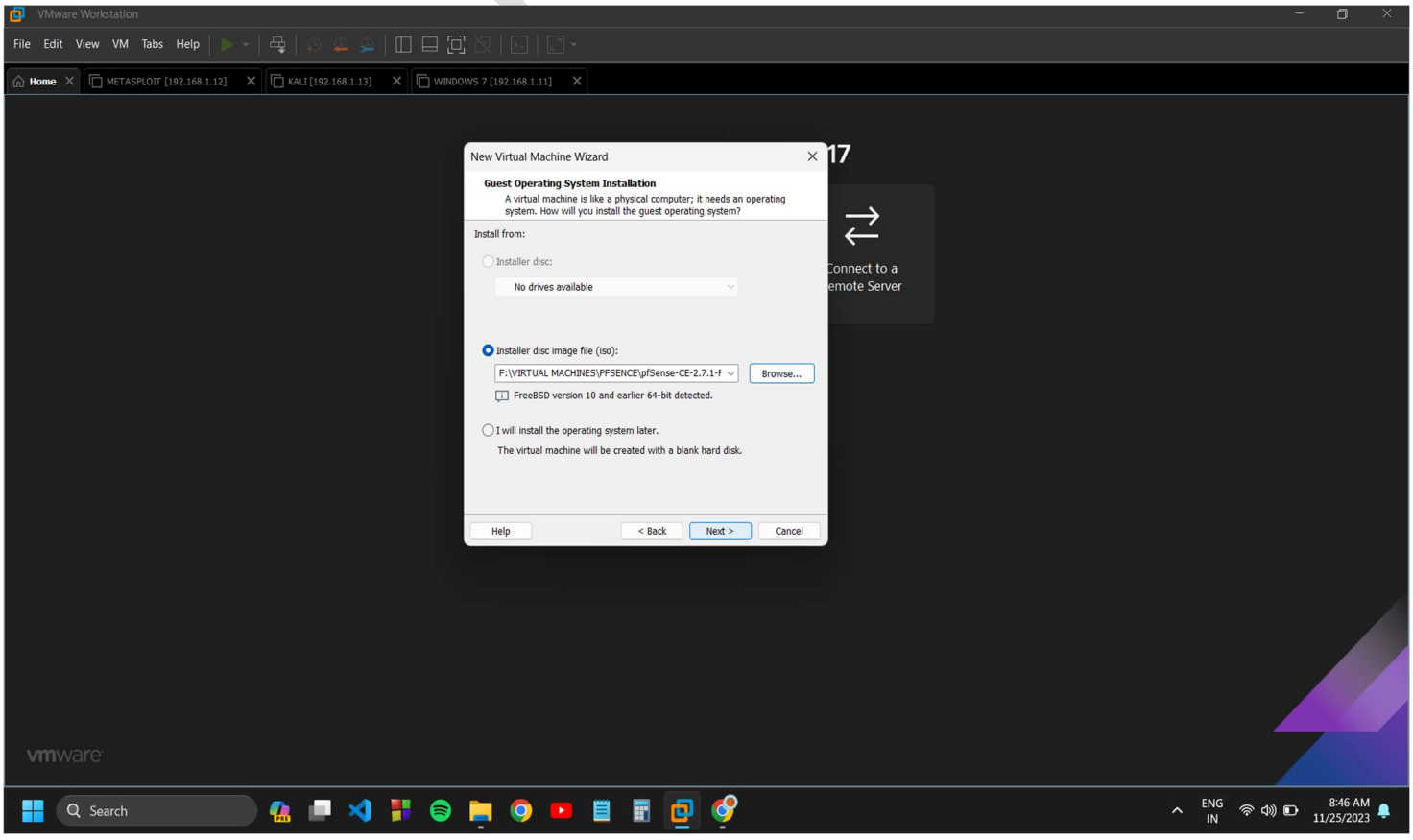
- **Open VMware and create a new virtual machine.**



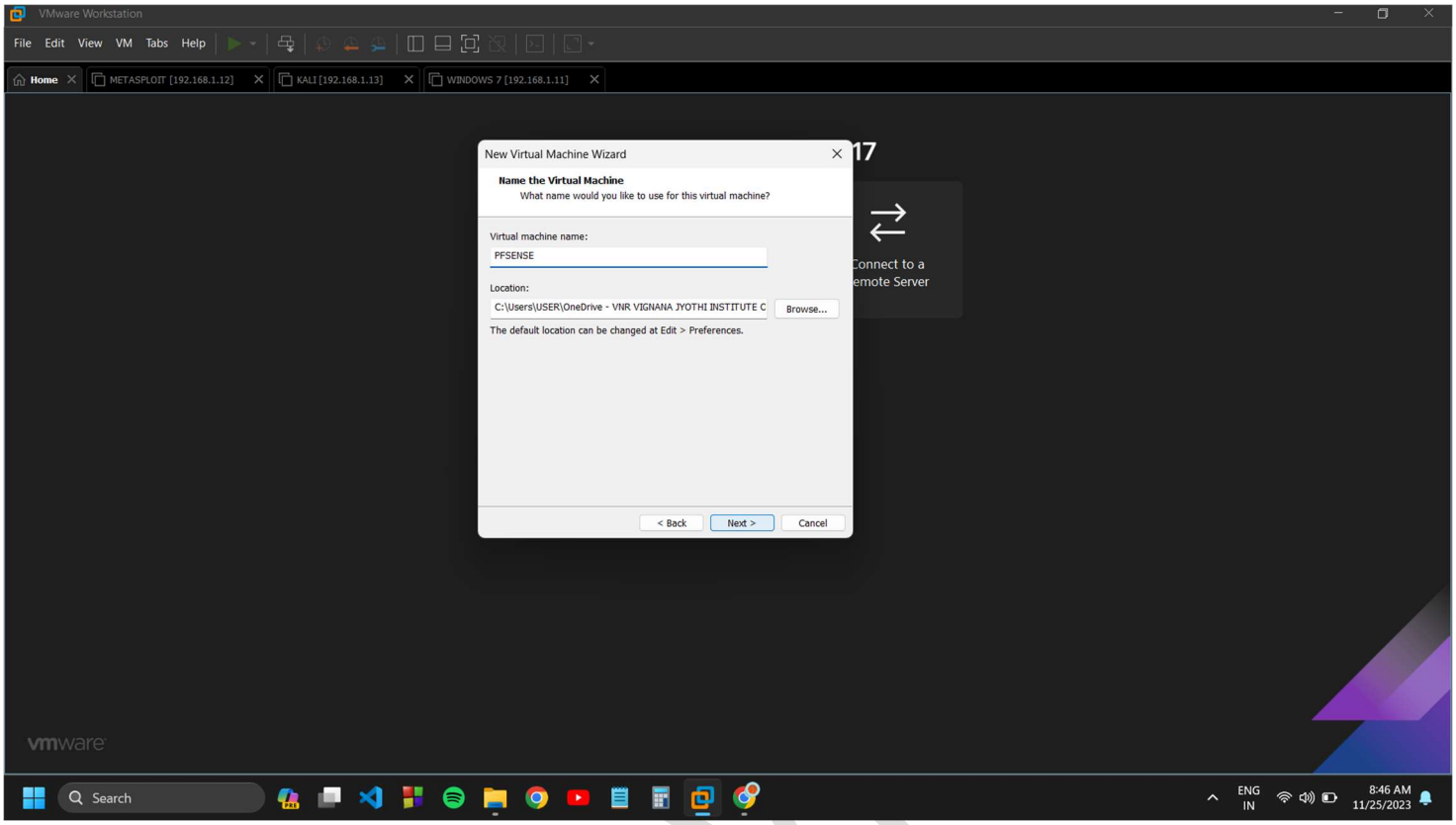


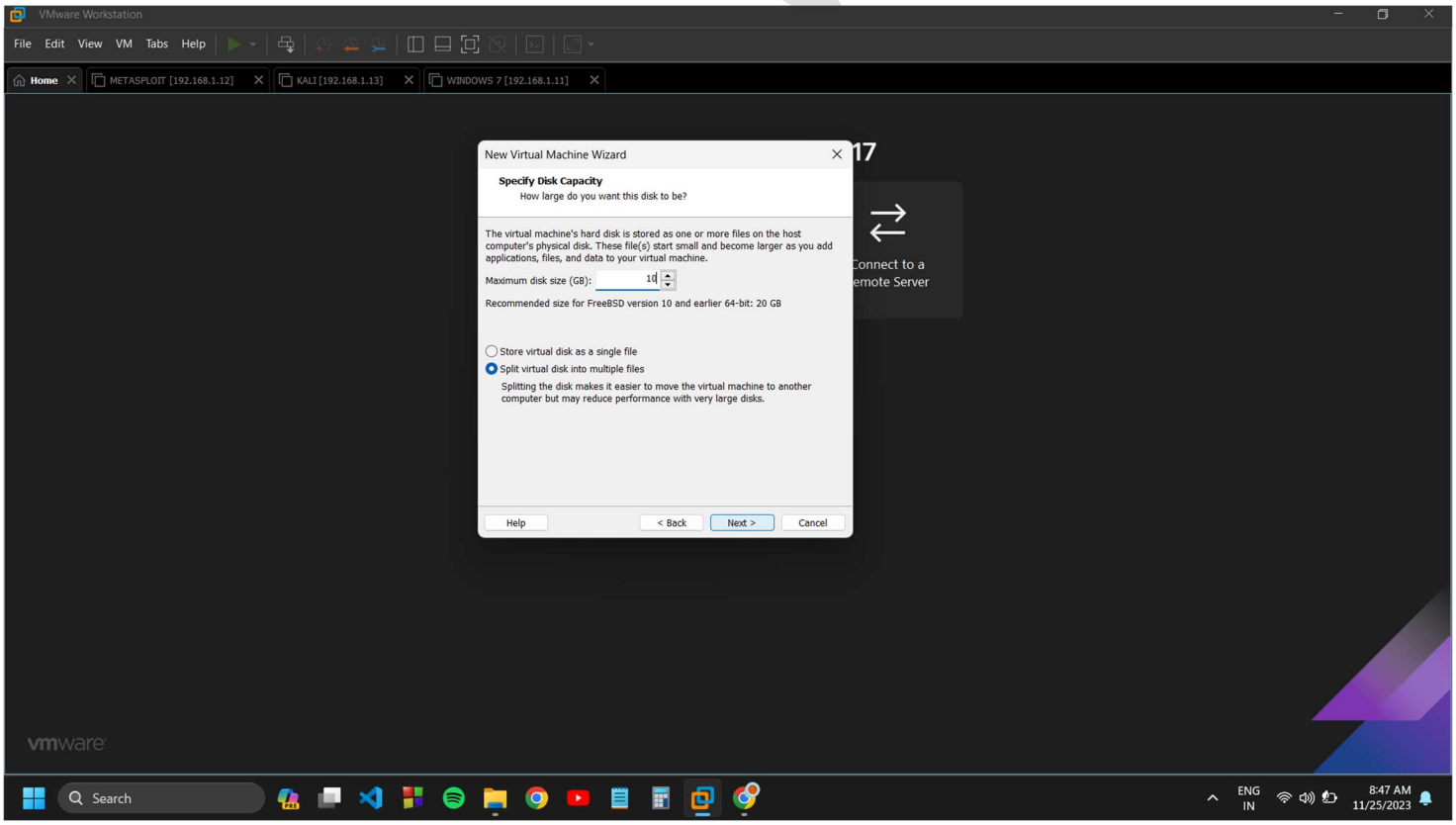
- **Choose "Installer disc image file" and browse to the pfSense ISO.**

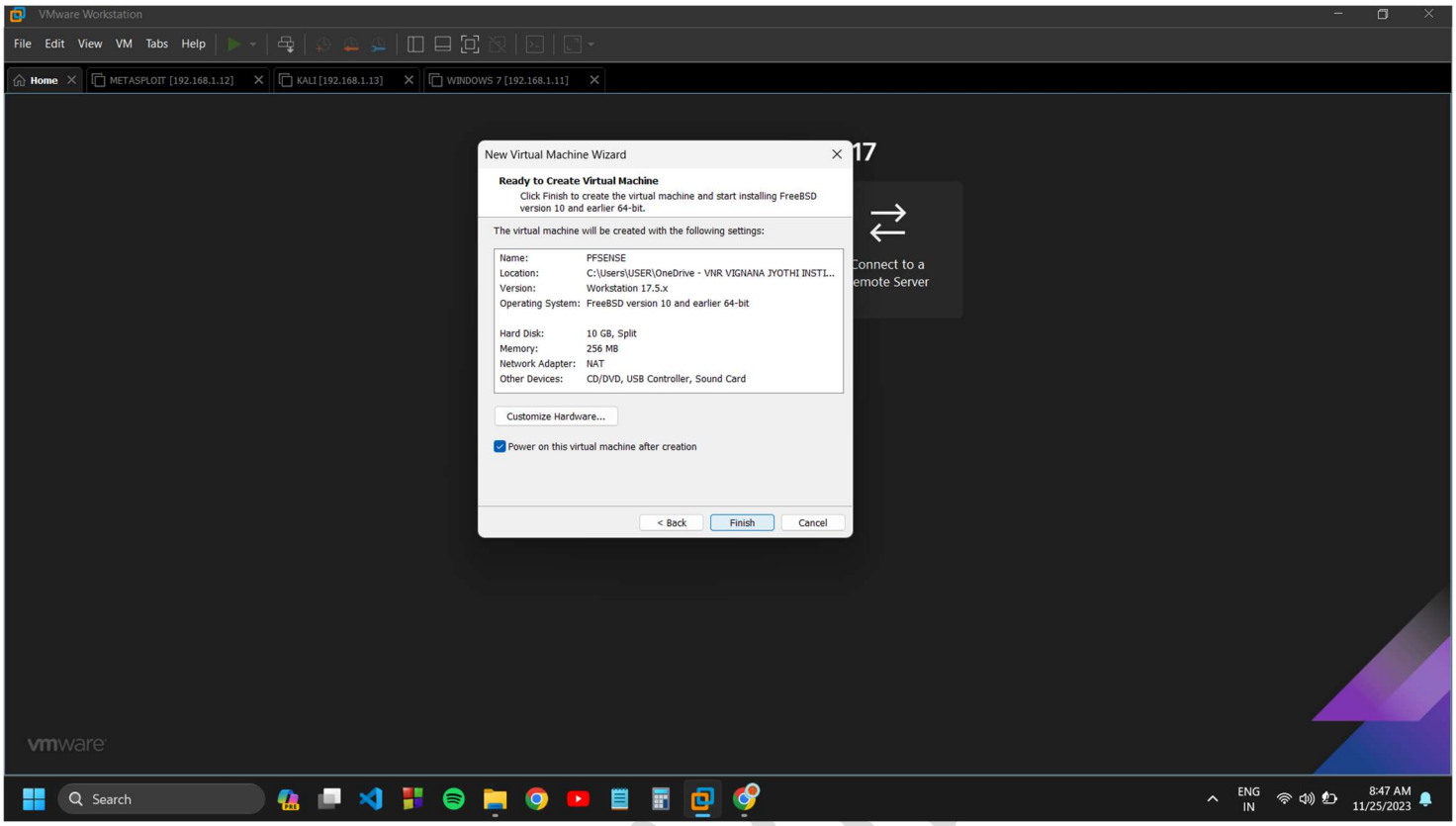




- **Specify settings: name, location, disk size, etc.**

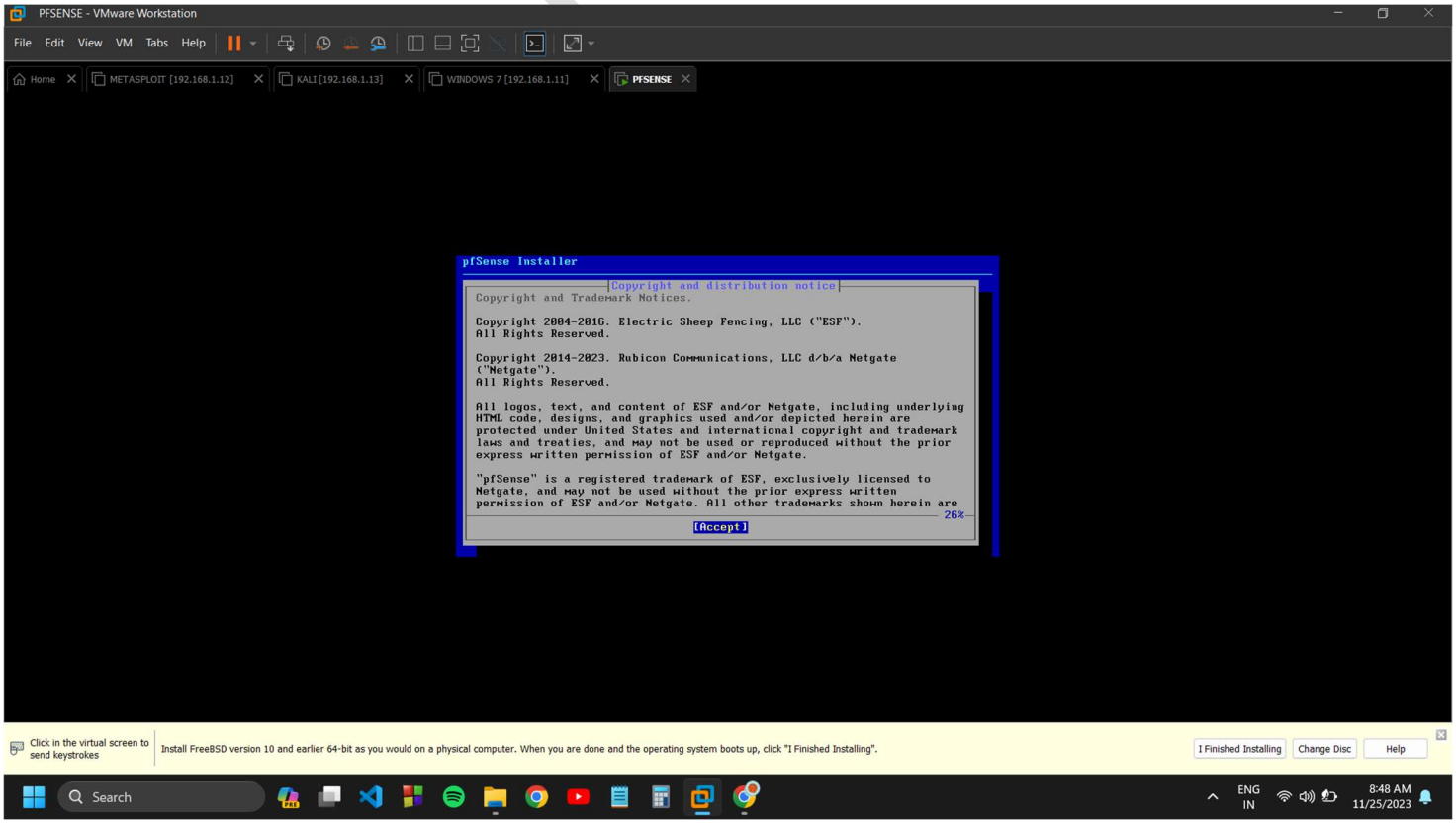


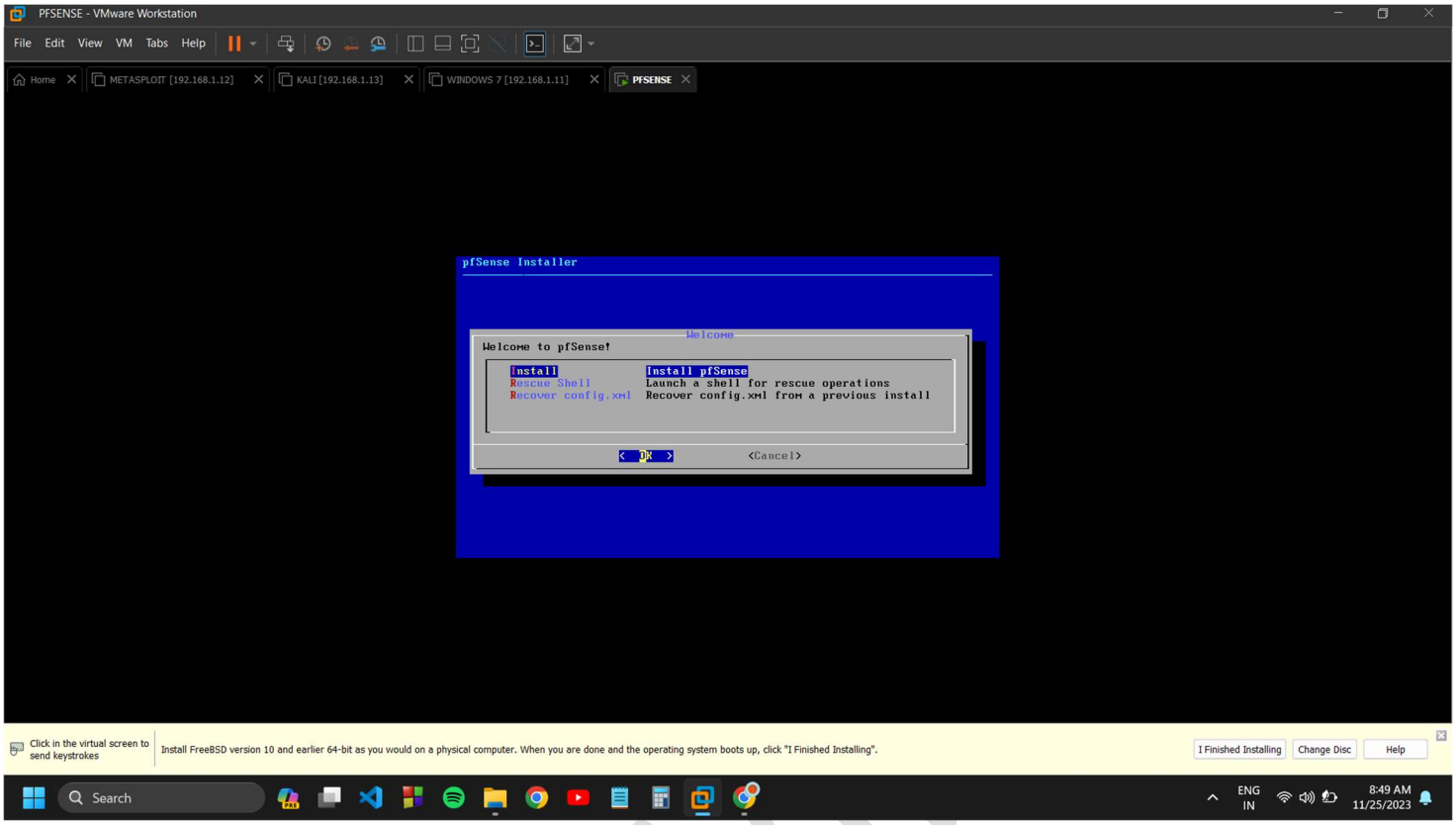


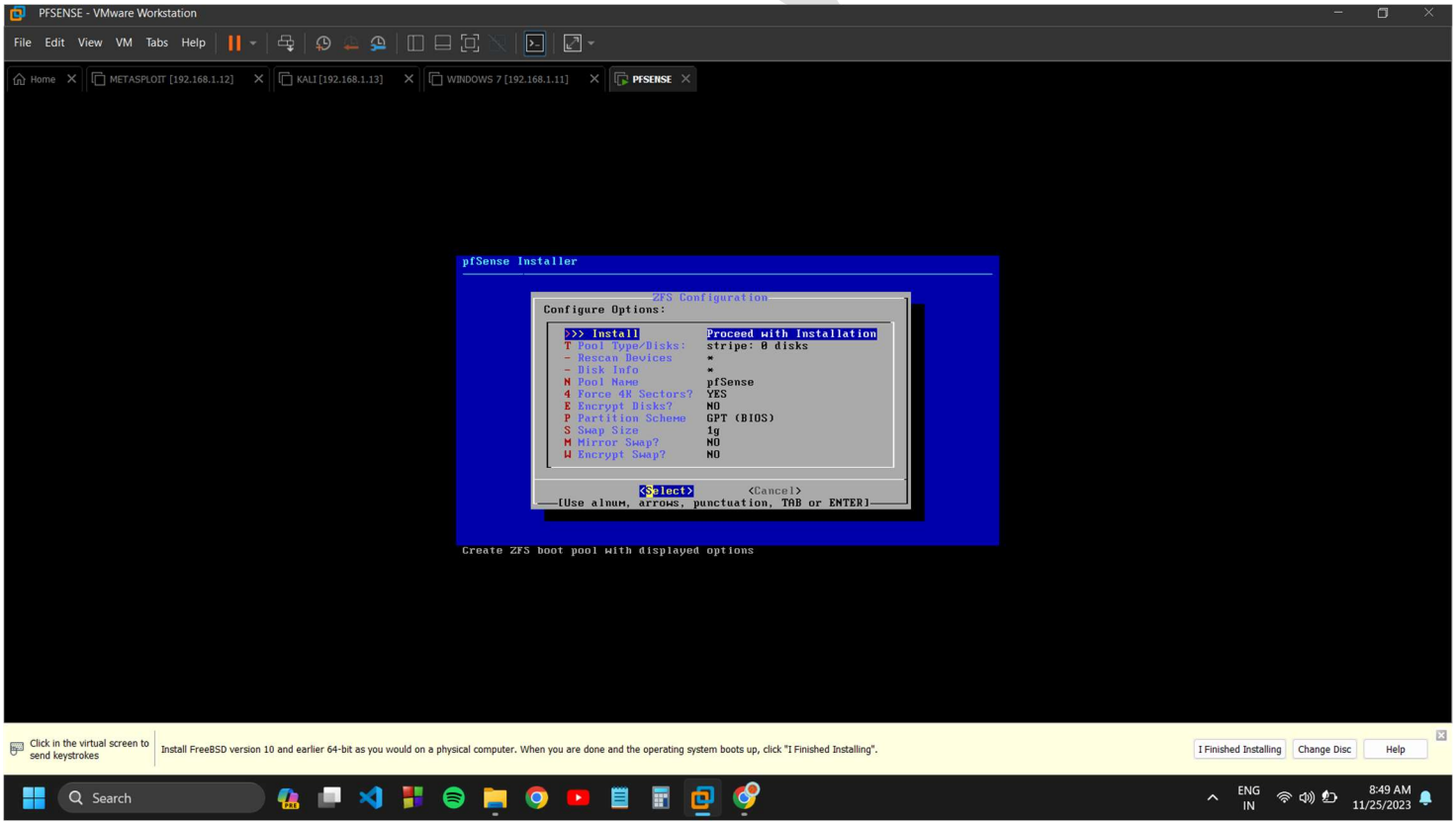


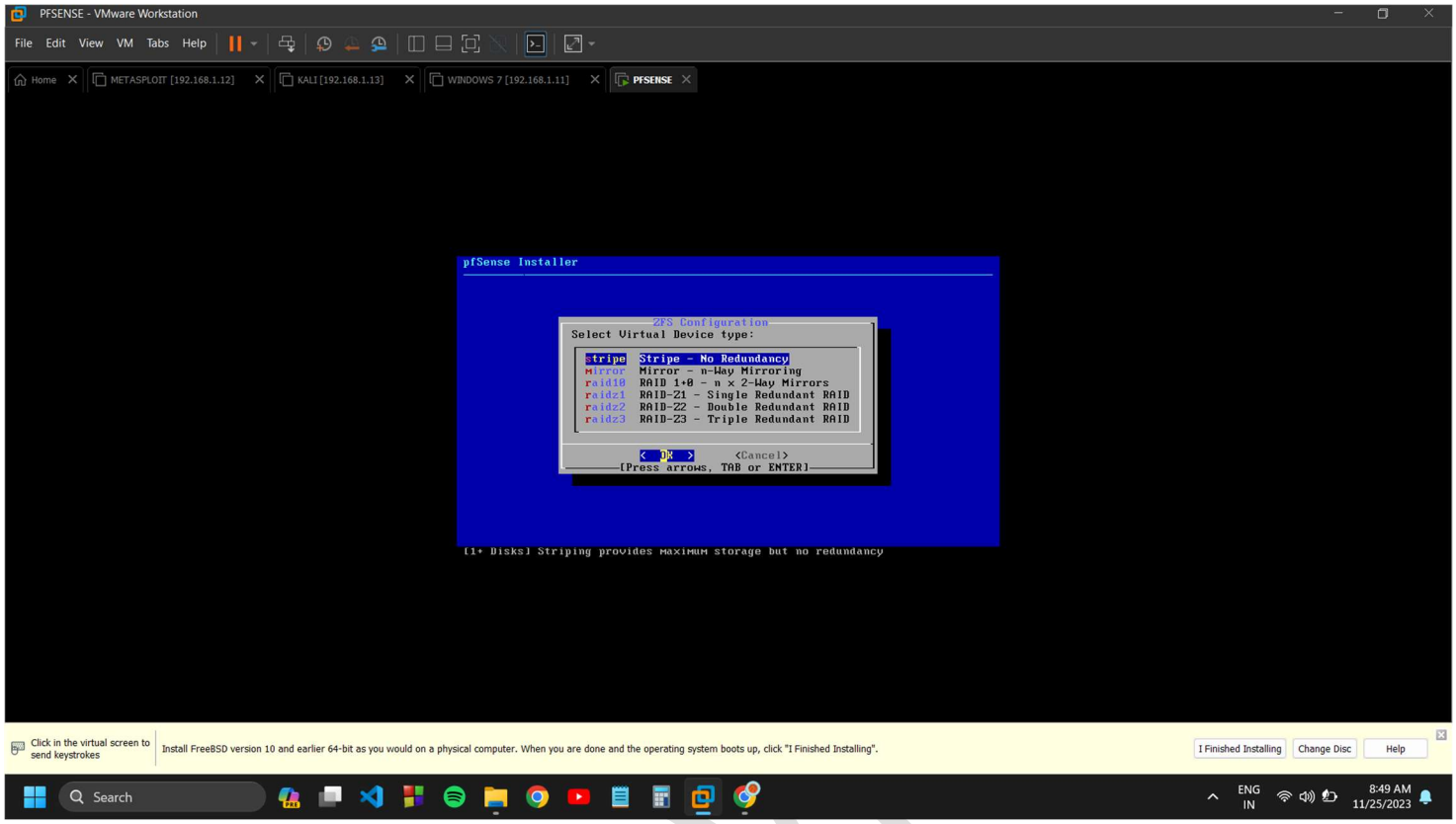
Install pfSense:

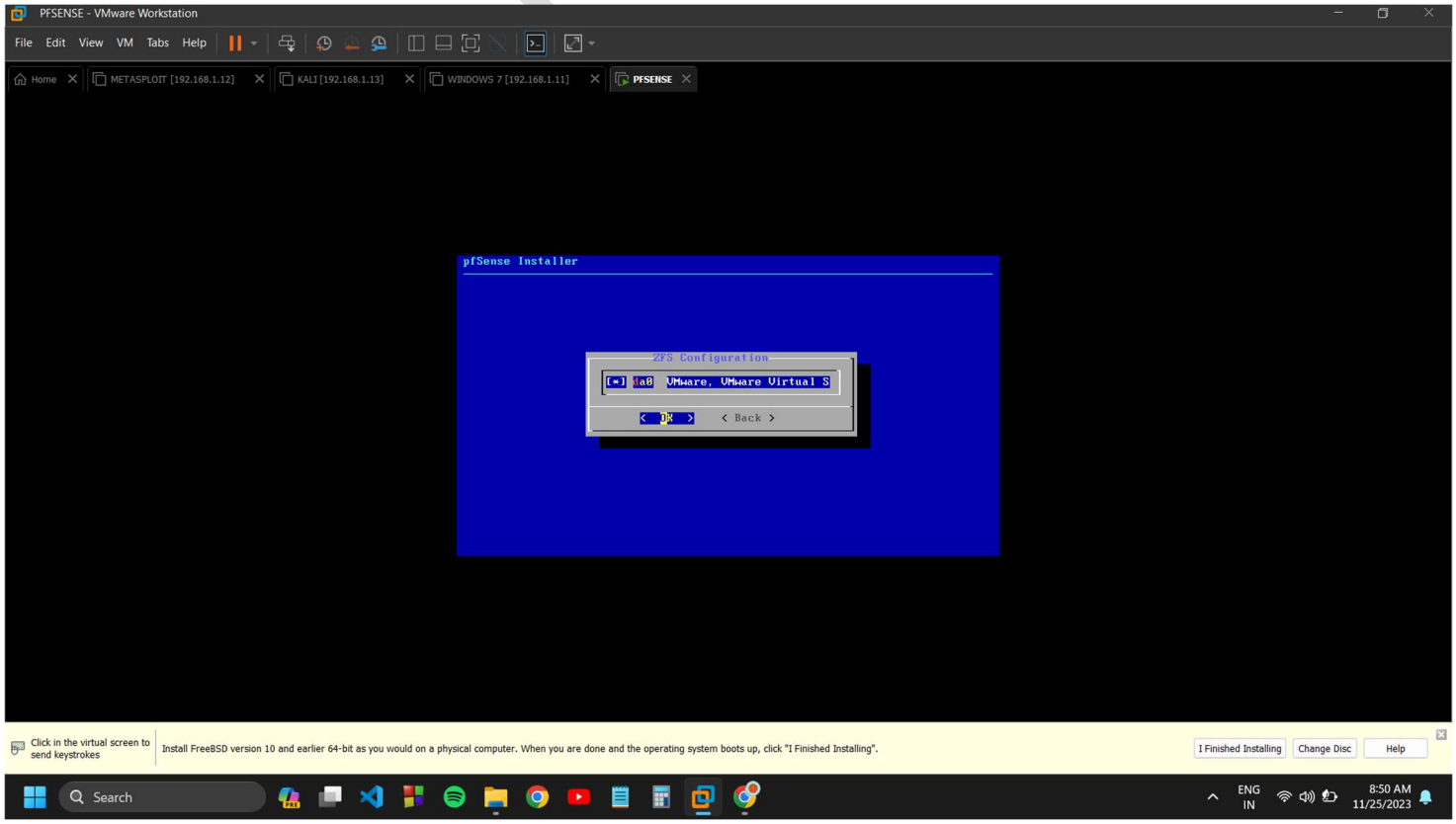
- **Start the virtual machine.**
- **Follow on-screen instructions to install pfSense.**

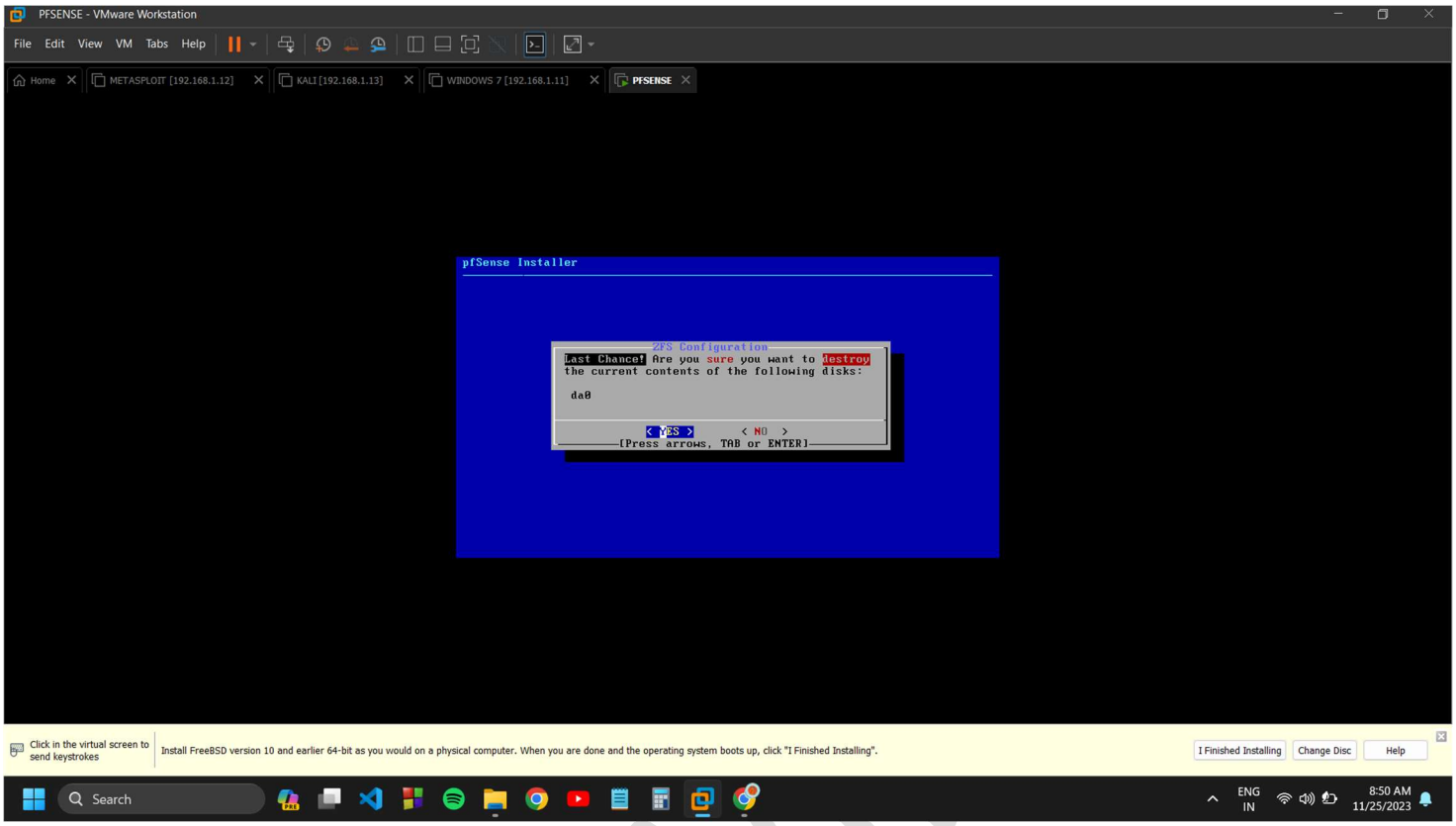


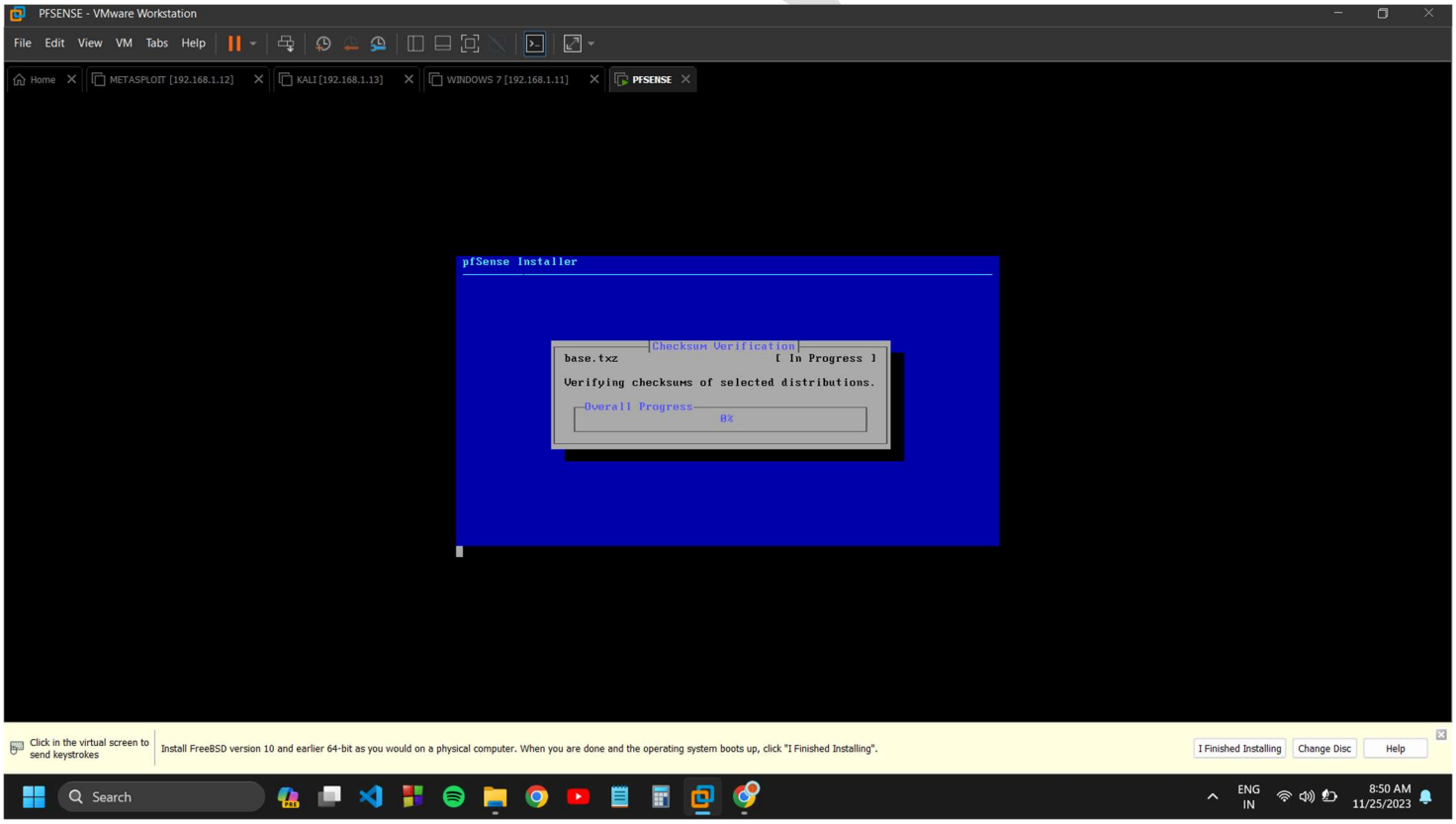

PFSENSE - VMware Workstation
File Edit View VM Tabs Help
Home
METASPLOIT [192.168.1.12]
KALI [192.168.1.13]
WINDOWS 7 [192.168.1.11]
PFSENSE
pfSense Installer
Welcome
Welcome to pfSense!
Install Install pfSense
Rescue Shell Launch a shell for rescue operations
Recover config.xml Recover config.xml from a previous install
<OK>
<Cancel>
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
ENG IN
8:49 AM 11/25/2023

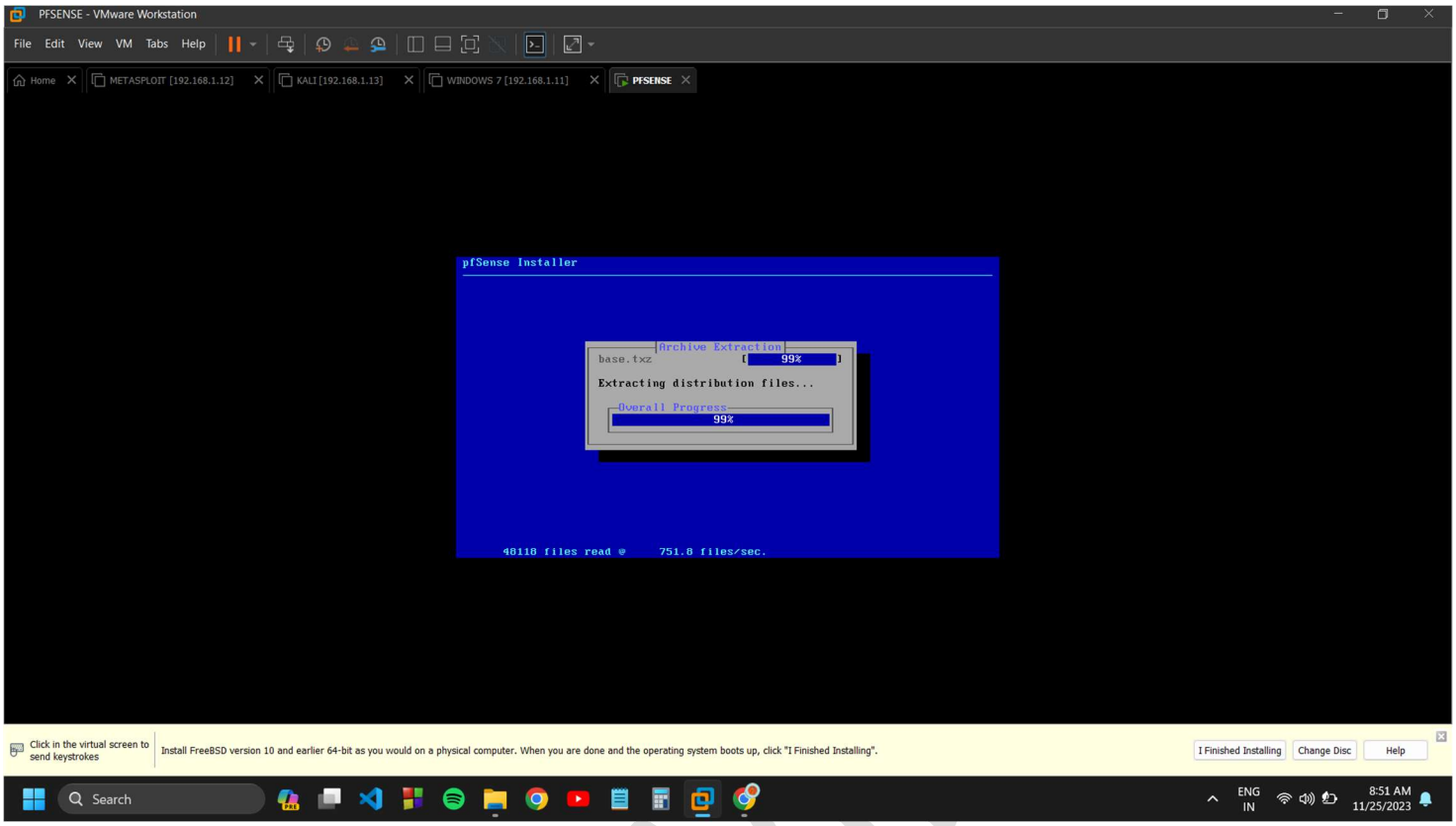

PFSENSE - VMware Workstation
File Edit View VM Tabs Help
Home
METASPLOIT [192.168.1.12]
KALI [192.168.1.13]
WINDOWS 7 [192.168.1.11]
PFSENSE
pfSense Installer
ZFS Configuration
Configure Options:
>>> Install Proceed with Installation
T Pool Type/Disks: stripe: 0 disks
- Rescan Devices *
- Disk Info *
N Pool Name pfSense
4 Force 4K Sectors? YES
E Encrypt Disks? NO
P Partition Scheme GPT (BIOS)
S Swap Size 1g
M Mirror Swap? NO
W Encrypt Swap? NO
<Select>
<Cancel>
[Use alnum, arrows, punctuation, TAB or ENTER]
Create ZFS boot pool with displayed options
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
ENG IN
8:49 AM 11/25/2023

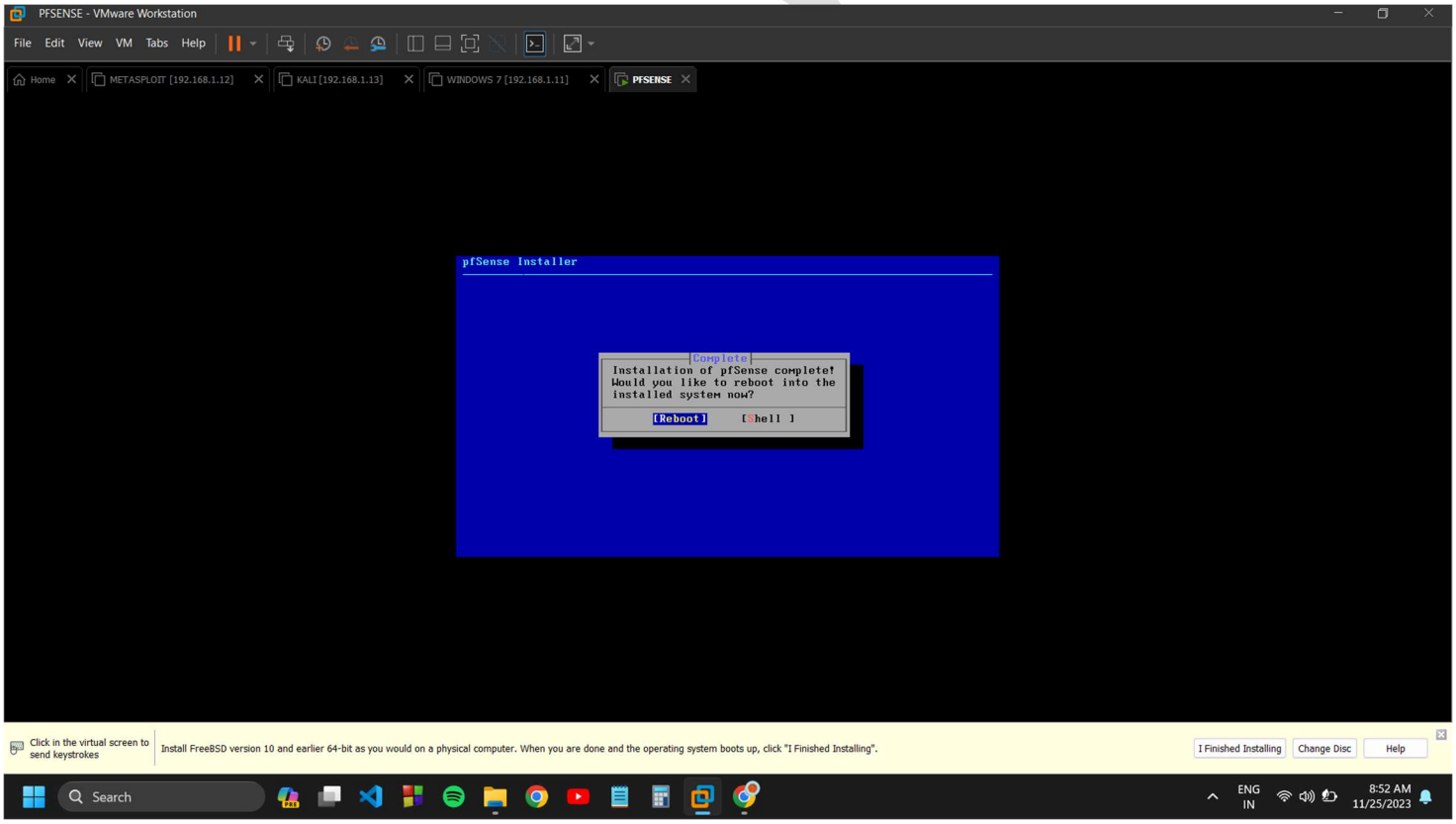

PFSENSE - VMware Workstation
File Edit View VM Tabs Help
Home
METASPLOIT [192.168.1.12]
KALI [192.168.1.13]
WINDOWS 7 [192.168.1.11]
PFSENSE
pfSense Installer
ZFS Configuration
Select Virtual Device type:
stripe Stripe - No Redundancy
mirror Mirror - n-Way Mirroring
raid10 RAID 1+0 - n x 2-Way Mirrors
raidz1 RAID-Z1 - Single Redundant RAID
raidz2 RAID-Z2 - Double Redundant RAID
raidz3 RAID-Z3 - Triple Redundant RAID
< OK >
<Cancel>
[Press arrows, TAB or ENTER]
[1+ Disks] Striping provides maximum storage but no redundancy
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
ENG IN
8:49 AM 11/25/2023


PFSENSE - VMware Workstation
File Edit View VM Tabs Help
Home
METASPLOIT [192.168.1.12]
KALI [192.168.1.13]
WINDOWS 7 [192.168.1.11]
PFSENSE
pfSense Installer
ZFS Configuration
[*] da0 VMware, VMware Virtual S
< OK >
< Back >
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
ENG IN
8:50 AM 11/25/2023


PFSENSE - VMware Workstation
File Edit View VM Tabs Help
Home
METASPLOIT [192.168.1.12]
KALI [192.168.1.13]
WINDOWS 7 [192.168.1.11]
PFSENSE
pfSense Installer
ZFS Configuration
Last Chance! Are you sure you want to destroy
the current contents of the following disks:
da0
< YES >
< NO >
[Press arrows, TAB or ENTER]
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
ENG
IN
8:50 AM
11/25/2023

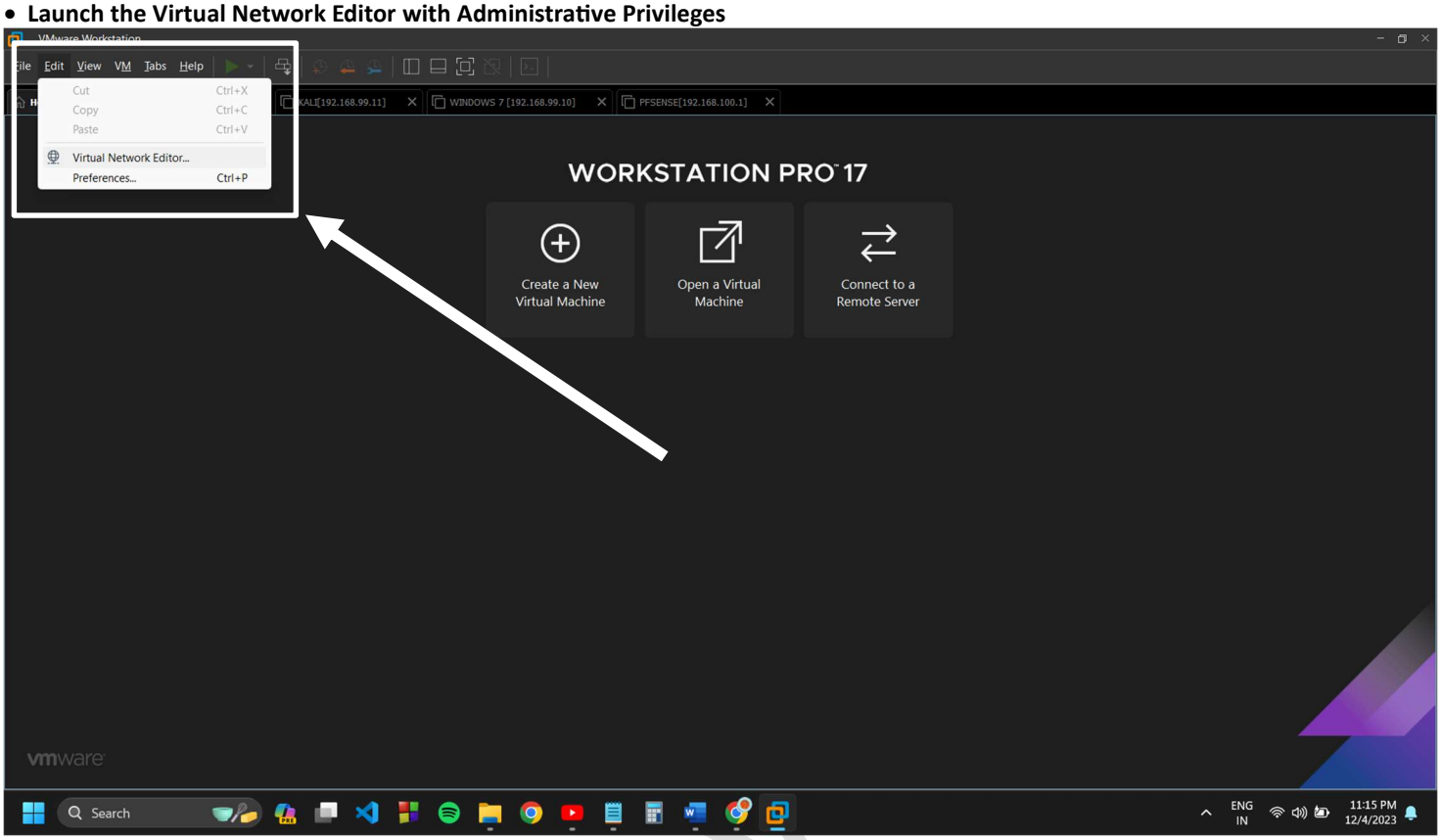

PFSENSE - VMware Workstation
File Edit View VM Tabs Help
Home
METASPLOIT [192.168.1.12]
KALI [192.168.1.13]
WINDOWS 7 [192.168.1.11]
PFSENSE
pfSense Installer
Checksum Verification
base.txz [In Progress]
Verifying checksums of selected distributions.
Overall Progress
0%
Click in the virtual screen to 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
ENG
IN
8:50 AM
11/25/2023


PFSENSE - VMware Workstation
File Edit View VM Tabs Help
Home
METASPLOIT [192.168.1.12]
KALI [192.168.1.13]
WINDOWS 7 [192.168.1.11]
PFSENSE
pfSense Installer
Archive Extraction
base.txz
99%
Extracting distribution files...
Overall Progress
99%
48118 files read @ 751.8 files/sec.
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
ENG
IN
8:51 AM
11/25/2023


PFSENSE - VMware Workstation
File Edit View VM Tabs Help
Home
METASPLOIT [192.168.1.12]
KALI [192.168.1.13]
WINDOWS 7 [192.168.1.11]
PFSENSE
pfSense Installer
Complete
Installation of pfSense complete! Would you like to reboot into the installed system now?
[Reboot]
[Shell]
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
ENG
IN
8:52 AM
11/25/2023

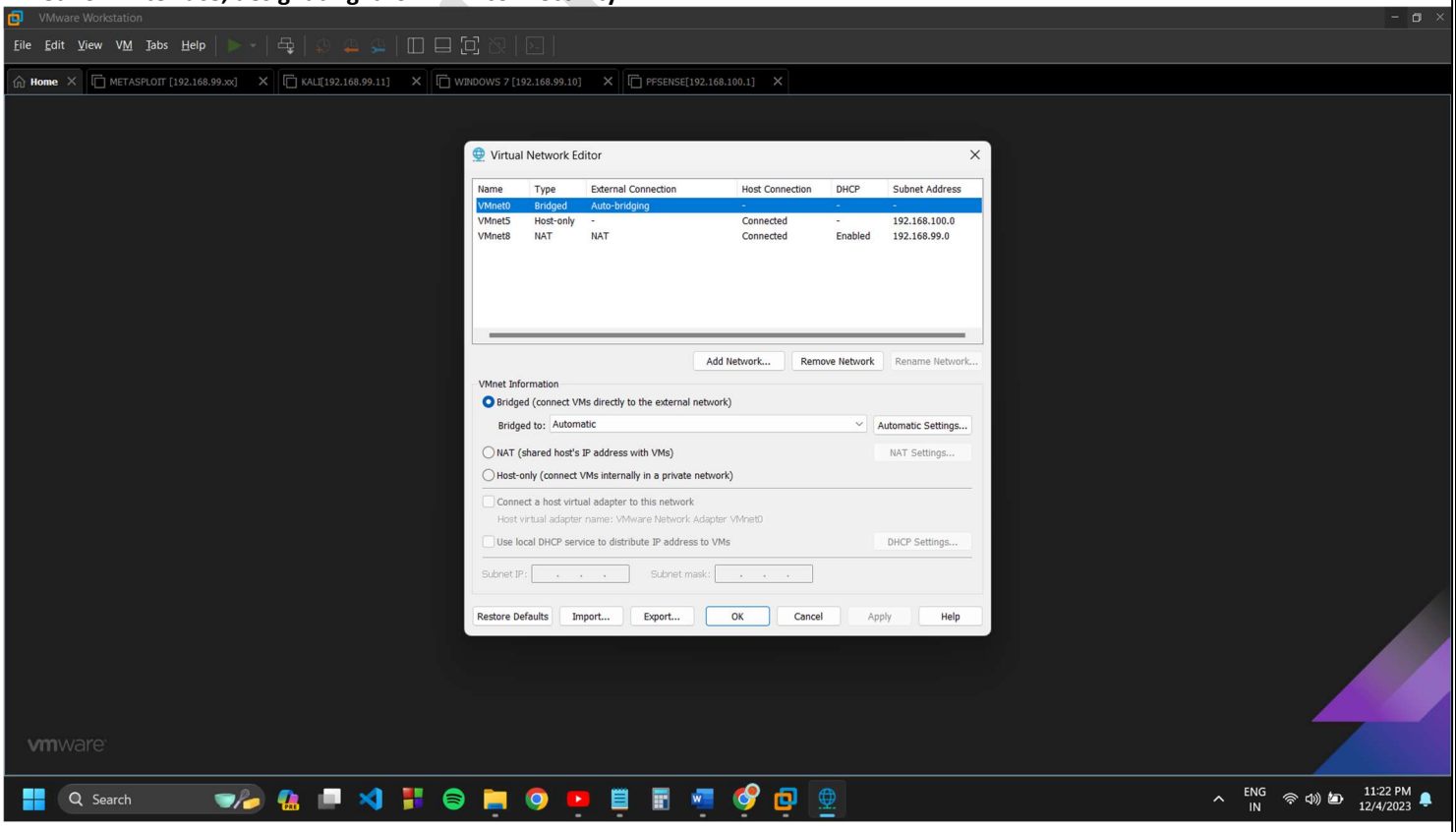
Adjust Virtual Machine Settings in VMware:

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



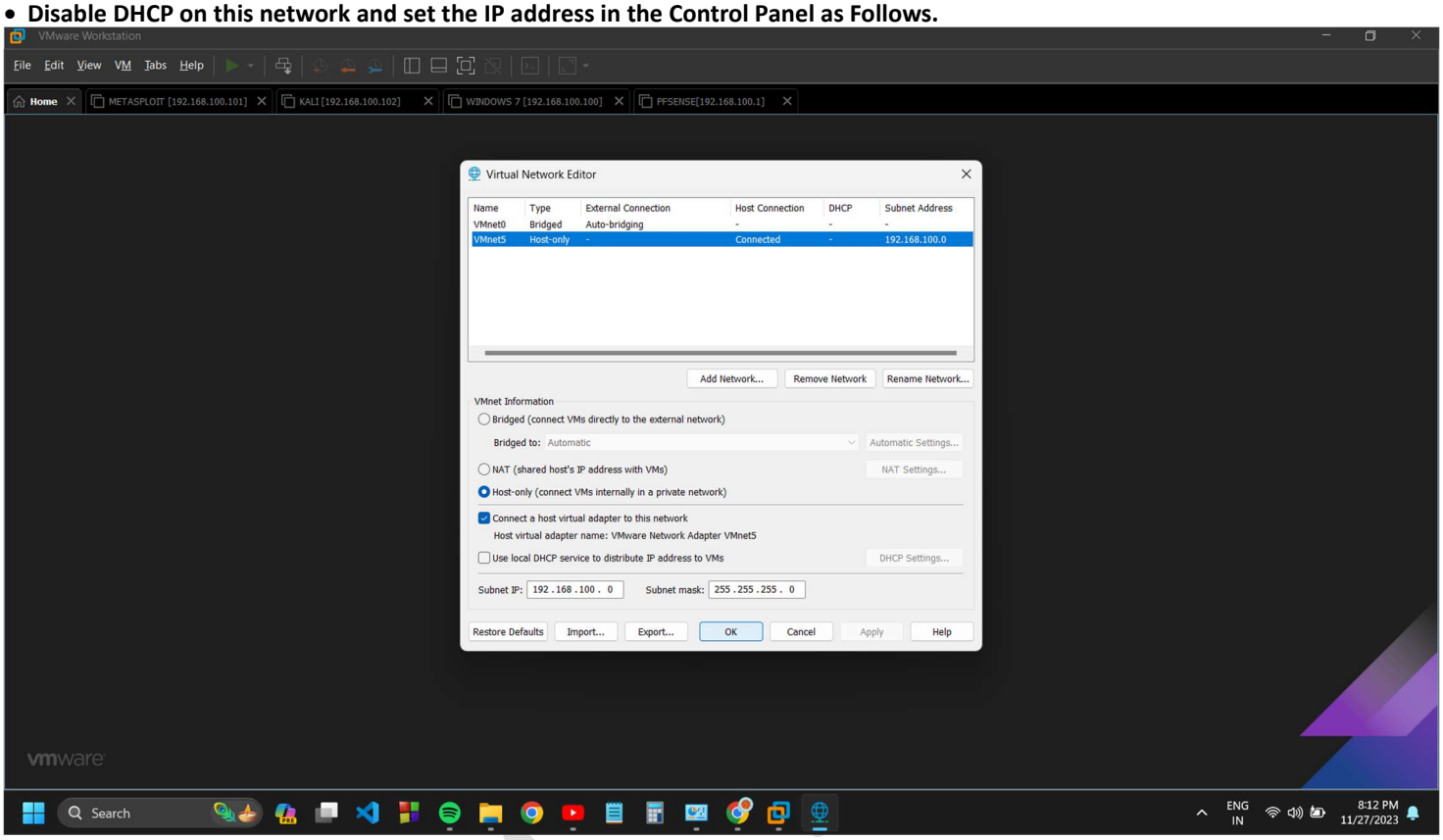
Create a Network (e.g., vmnet0) for Autobridging (WAN):

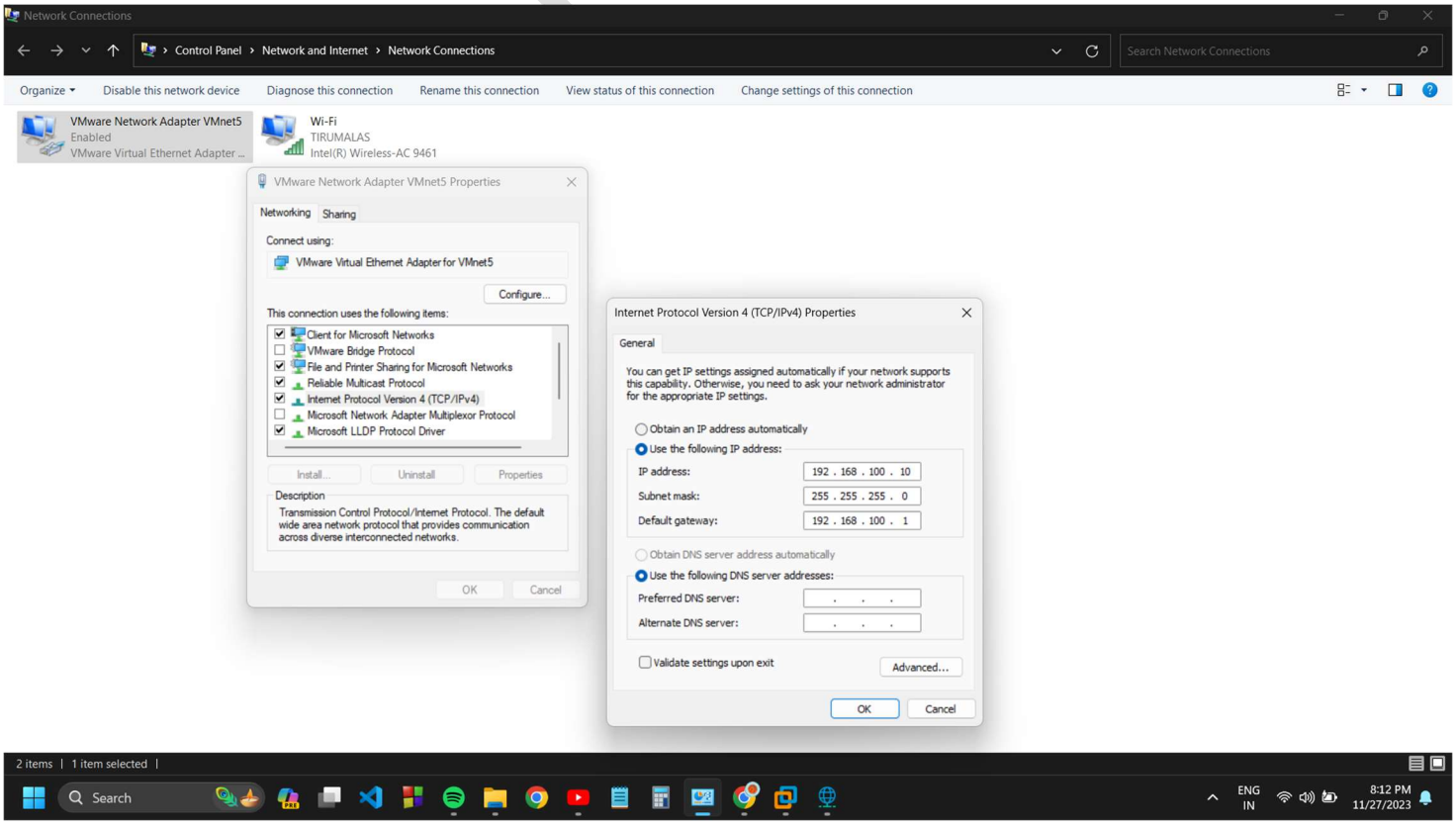
- In the Virtual Network Editor, create a new network and assign it a specific identifier (e.g., vmnet0).
- Set the network type to "Autobridging." This configuration enables the virtual network to automatically bridge with a physical network interface, designating it for WAN connectivity.



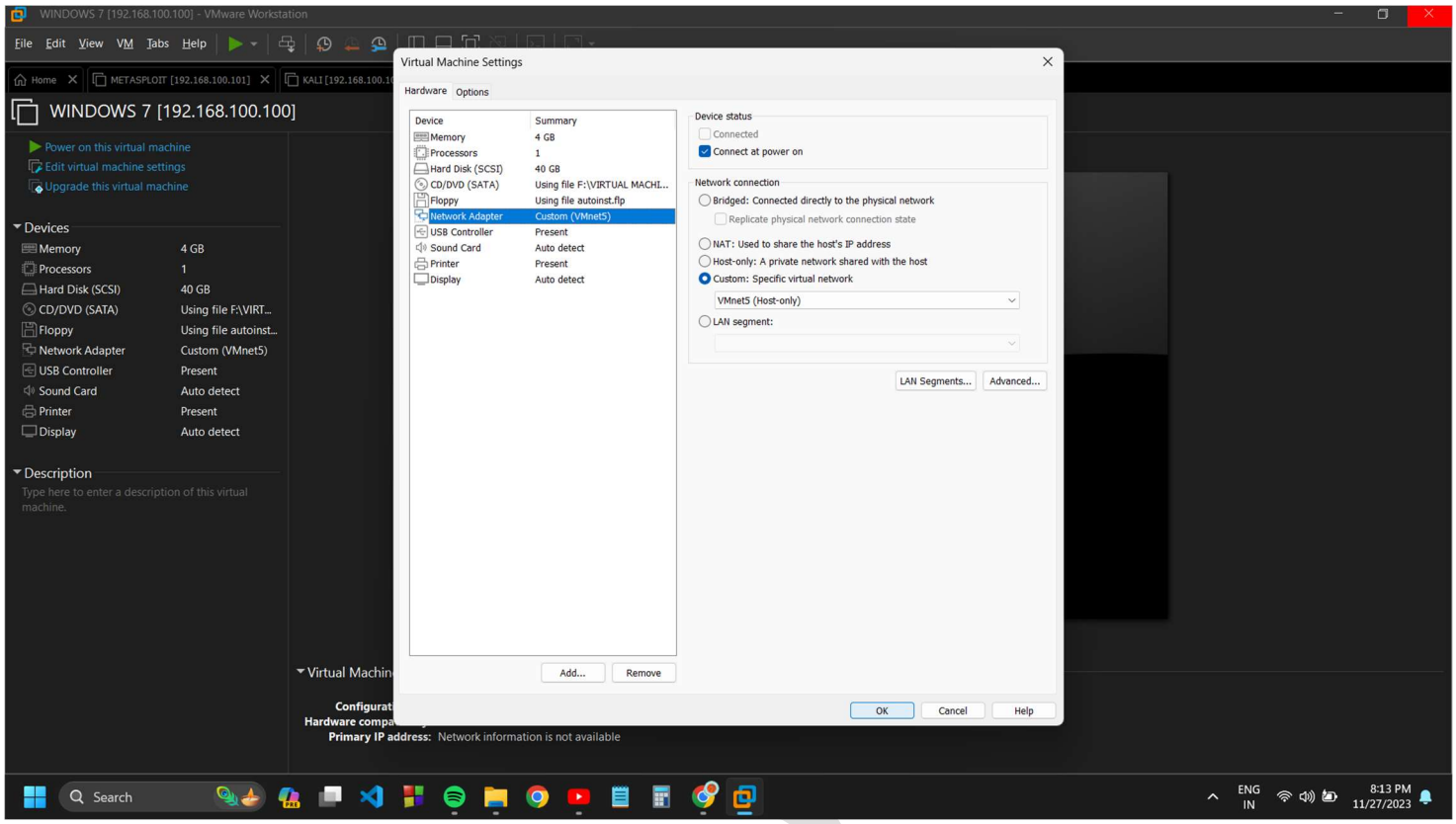
Establish Another Network (e.g., vmnet5) as Host-Only (LAN):

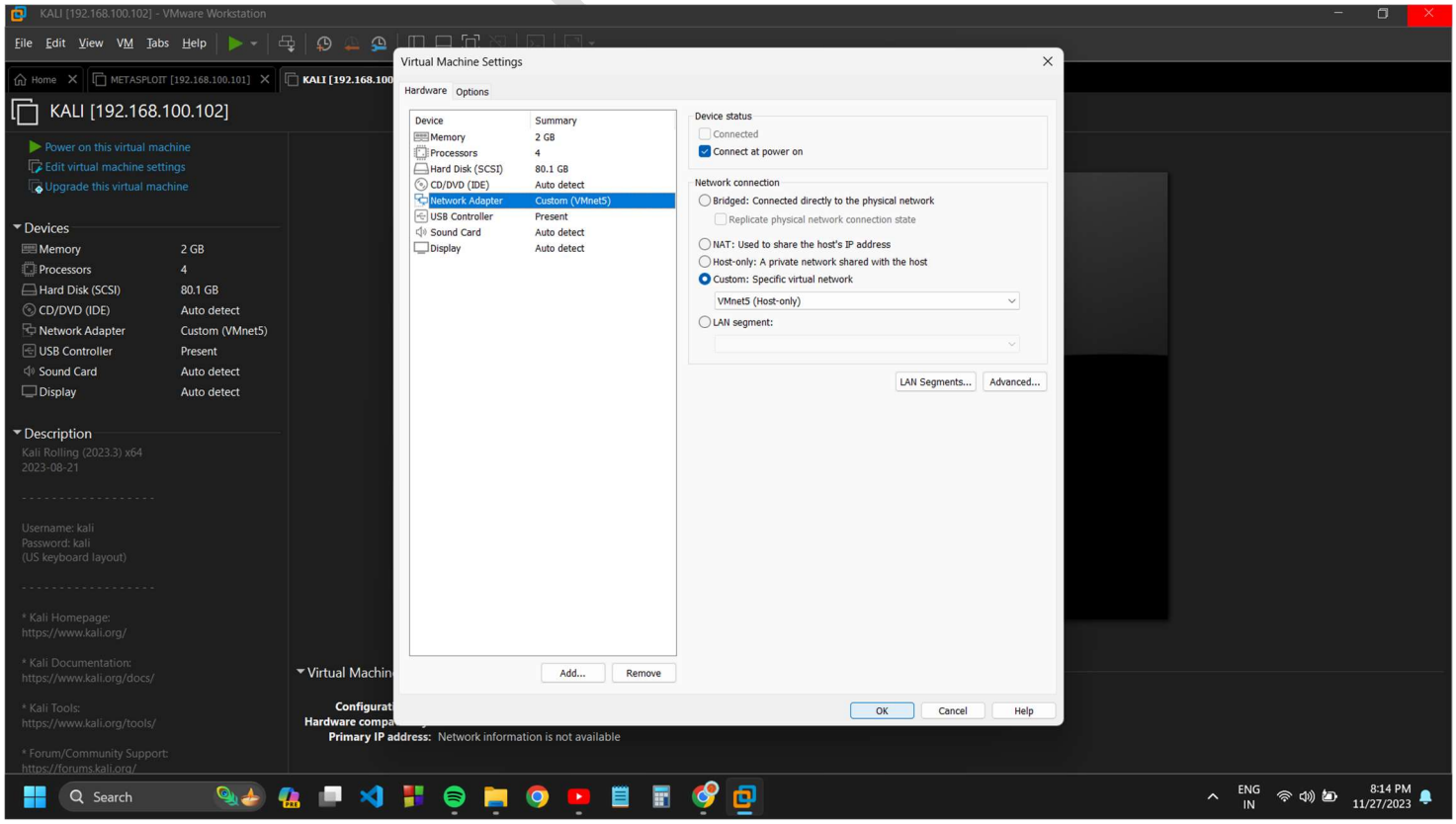
- Create an additional network in the Virtual Network Editor, using a different identifier (e.g., vmnet5).
- Set the network type to "Host-Only." This setting ensures isolation, allowing communication solely between virtual machines connected to this network.
- Disable DHCP on this network and set the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





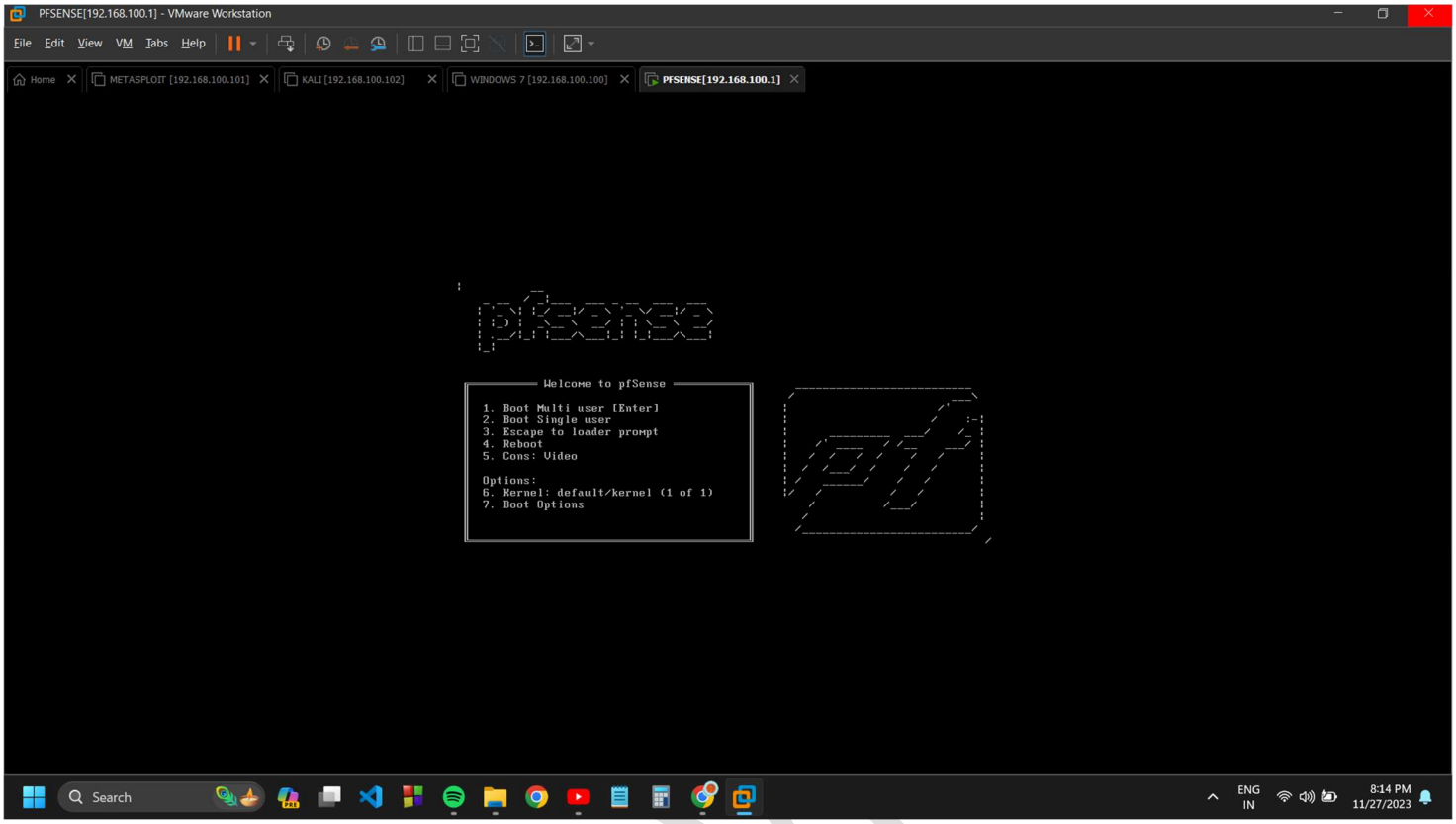
- **Change Kali Linux's and Windows 7's network adapter to the Host-Only network vmnet5 in VMware**





Configure pfSense Network:

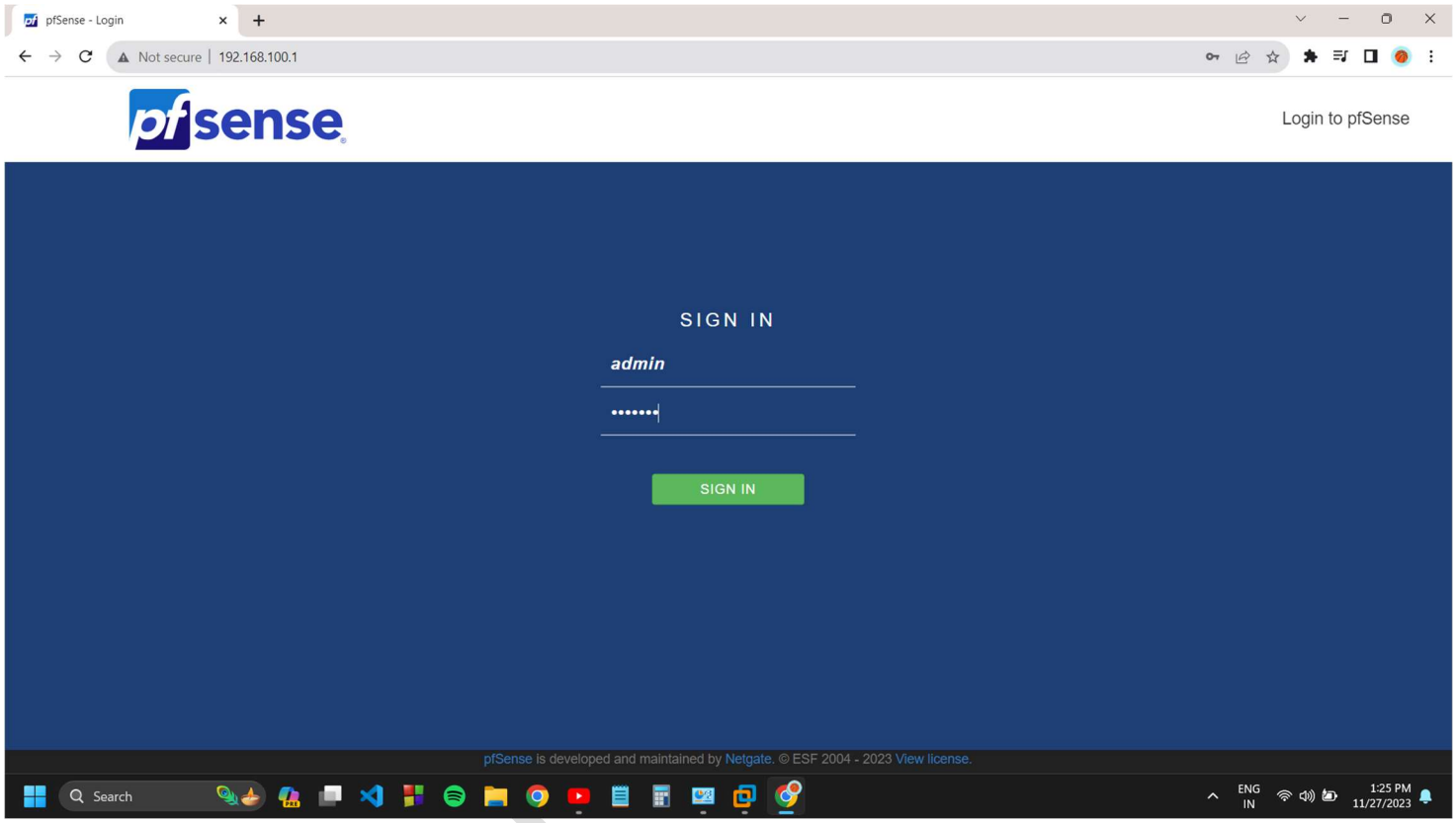
- **Observe and note the IP addresses for WAN and LAN.**

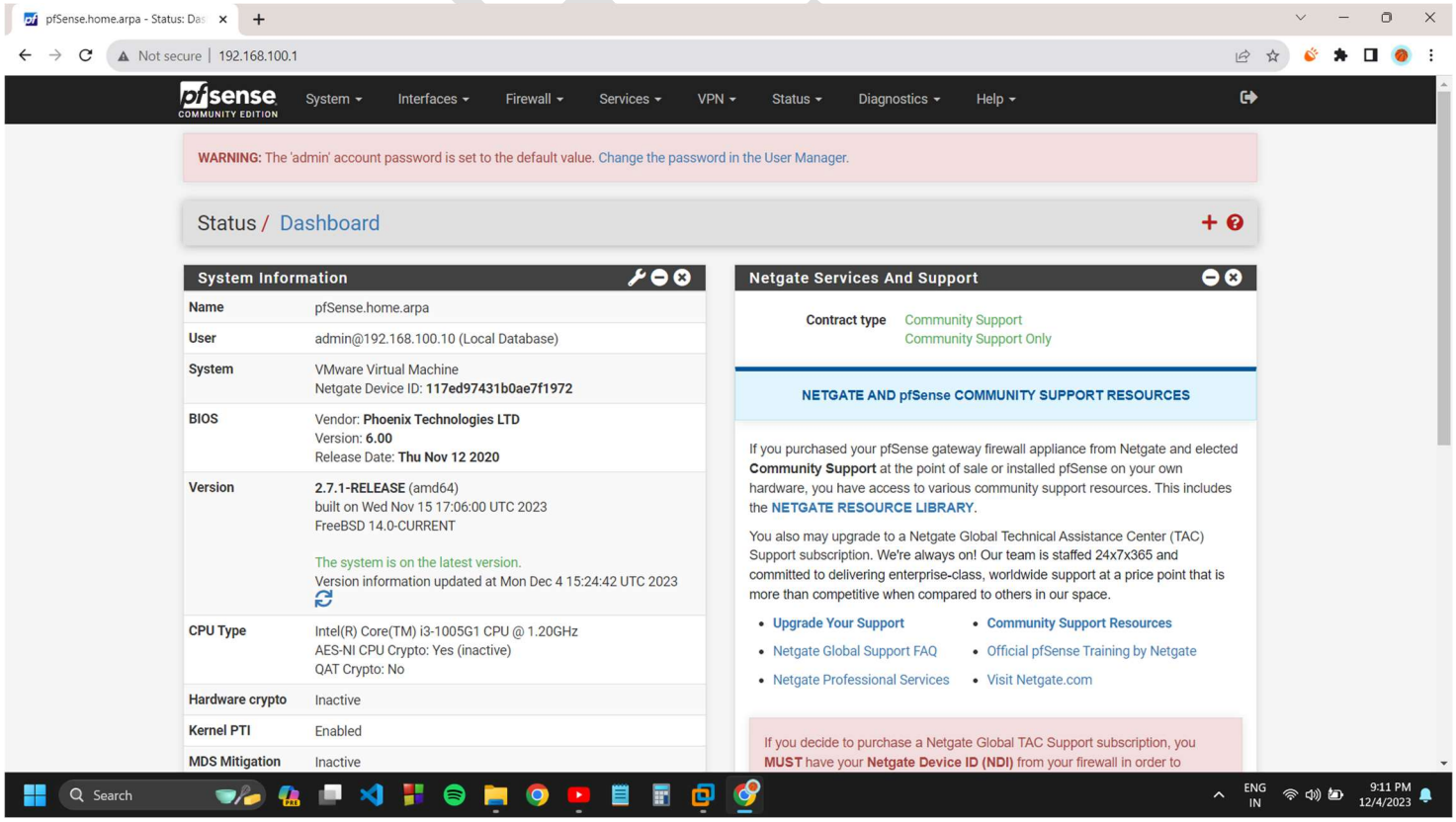



```
FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

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:dda1/64
 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.'

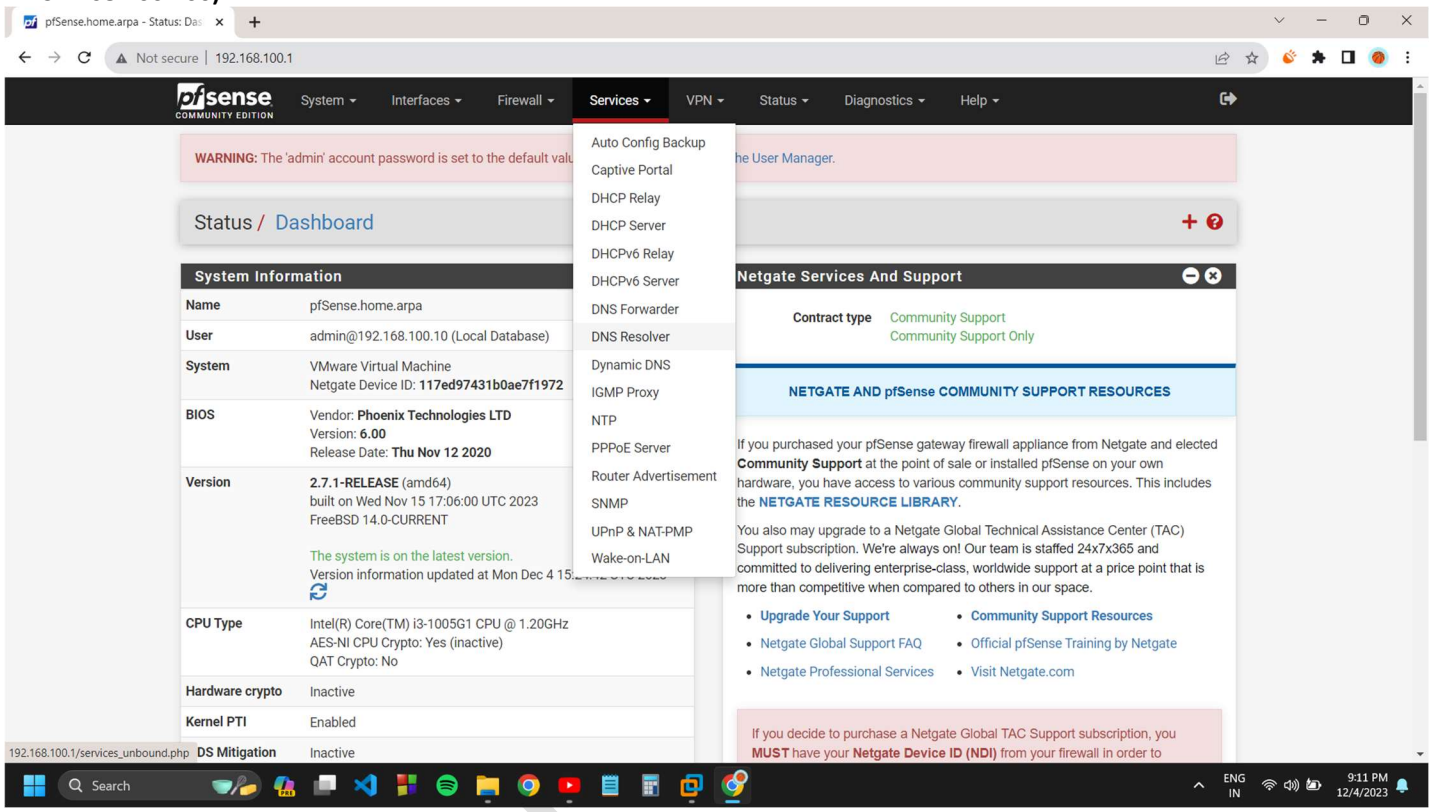


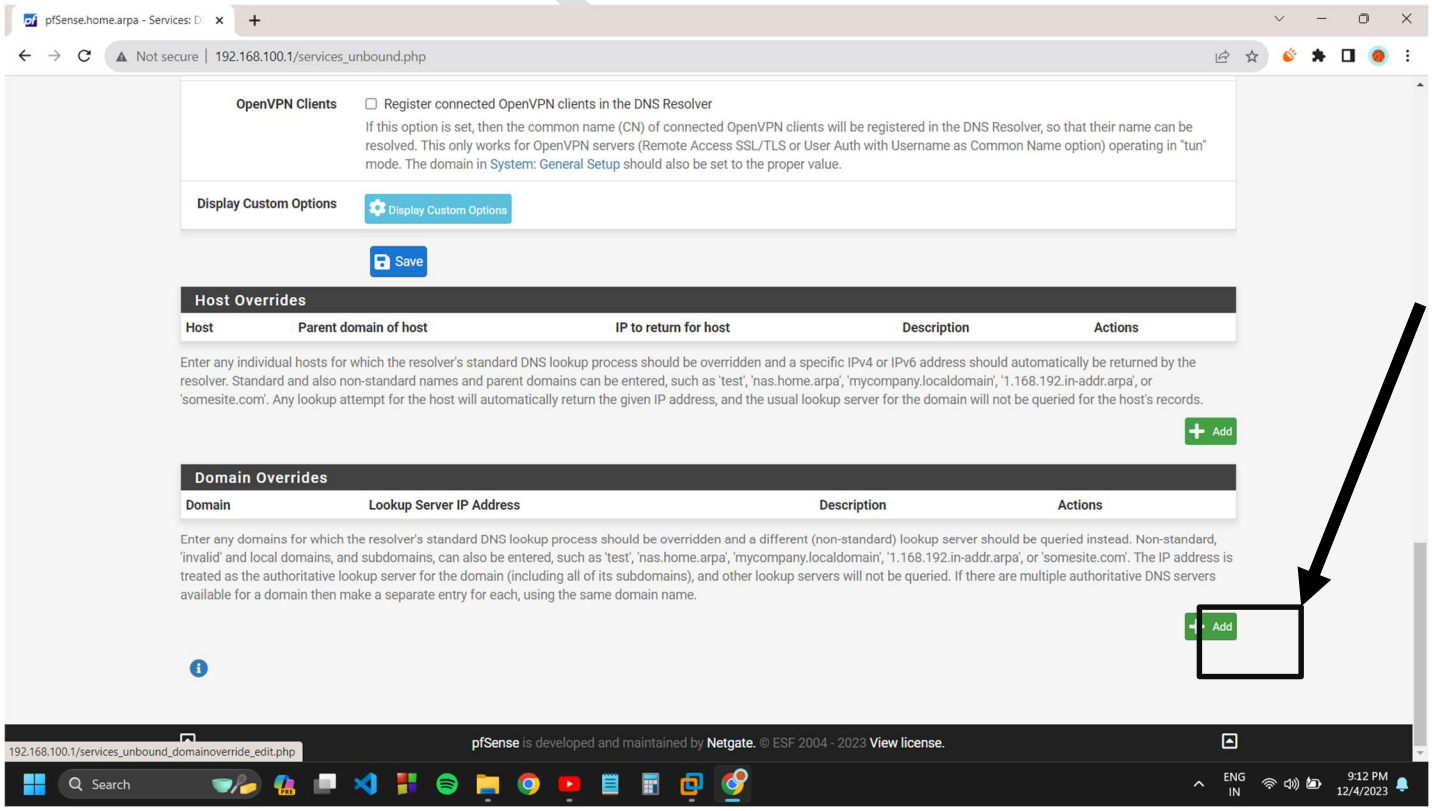


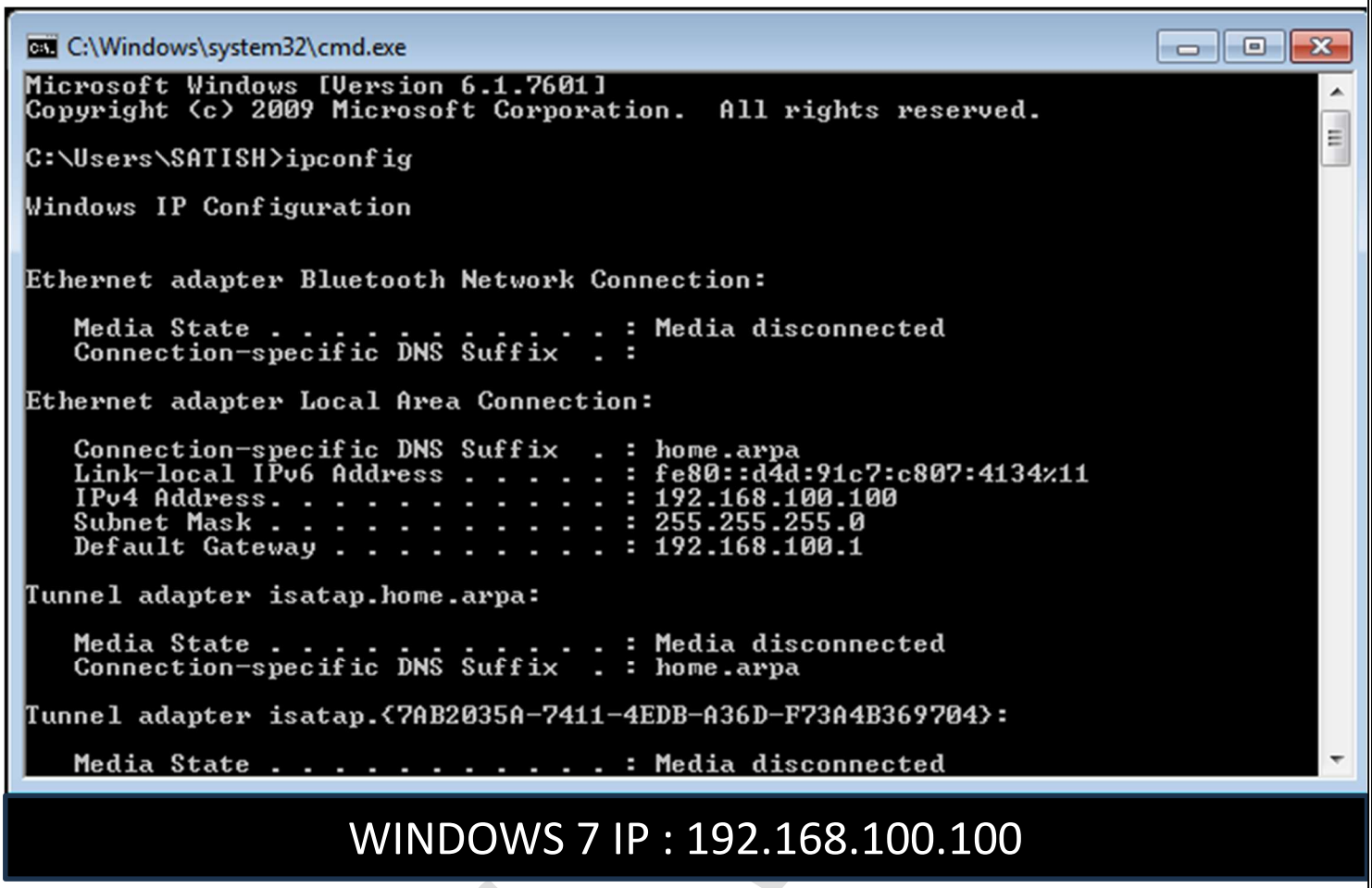
CONFIGURING THE FIREWALL TO RESTRICT ACCESS TO CERTAIN WEBSITES

Configure DNS Resolver:

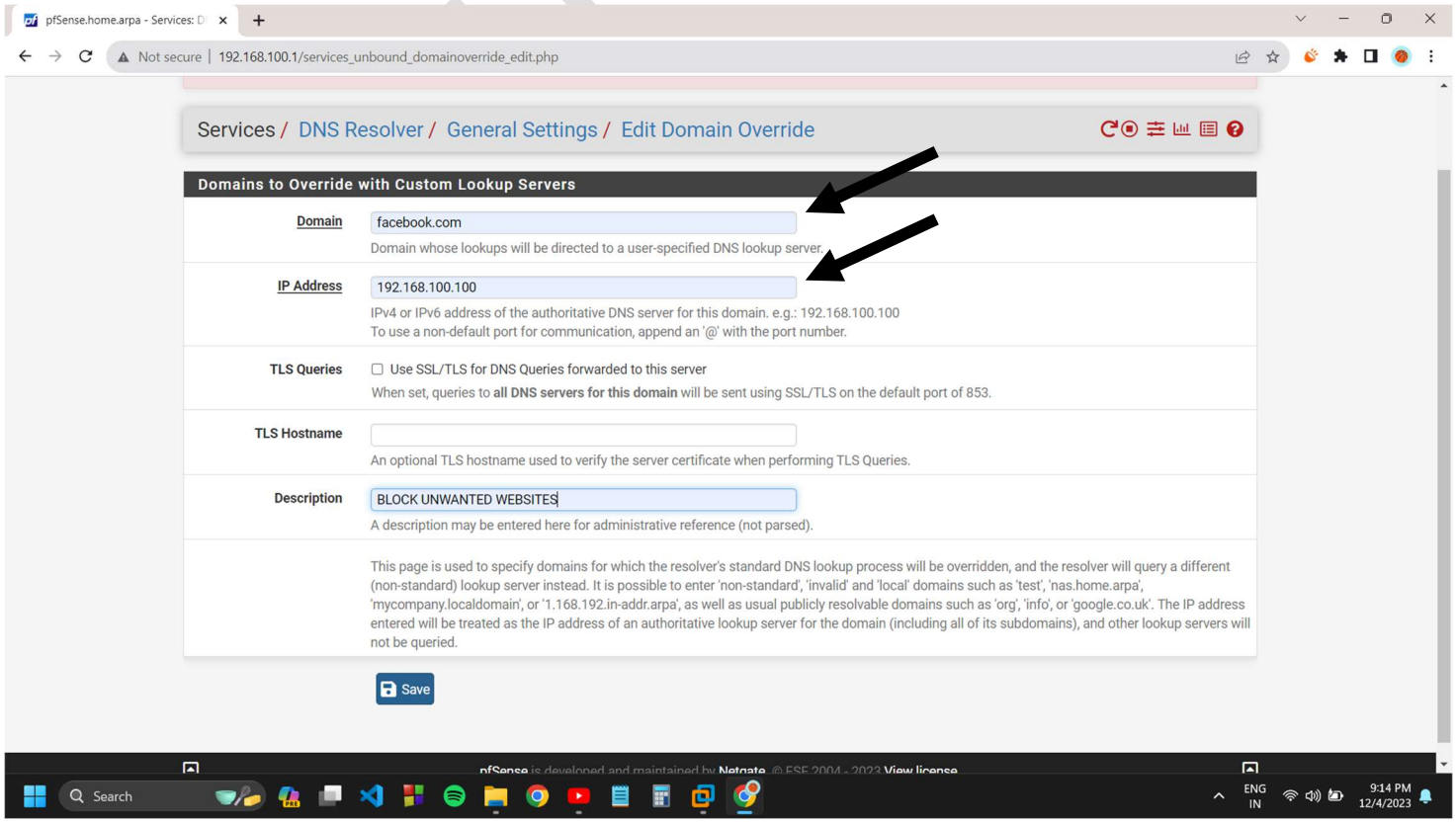
- **In pfSense, navigate to Services/DNS Resolver/.**
- **Edit the domain override.**
- **Specify the domain to block (e.g., facebook.com) and the IP address of the host in which the website has to block (e.g., 192.168.100.100).**



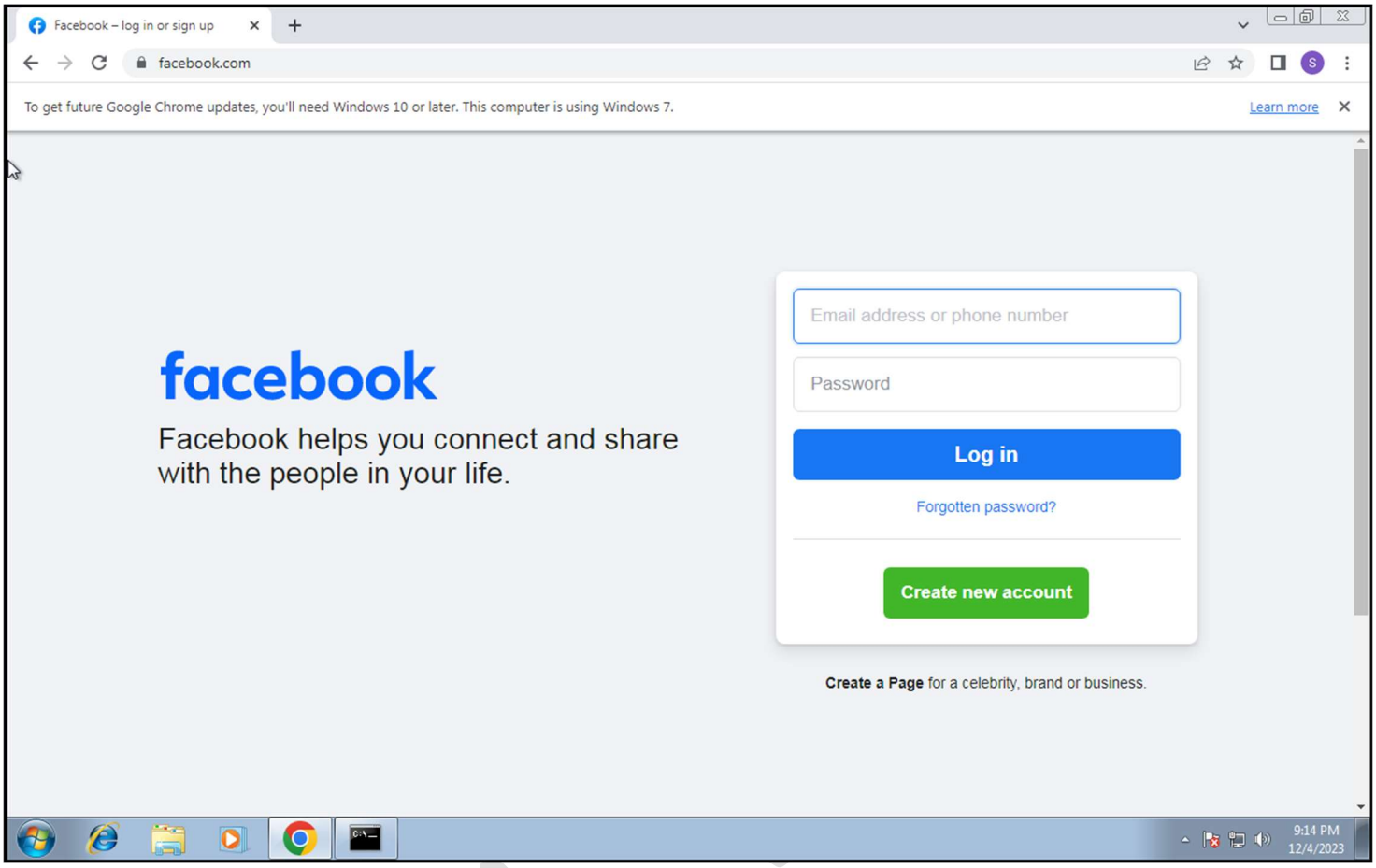




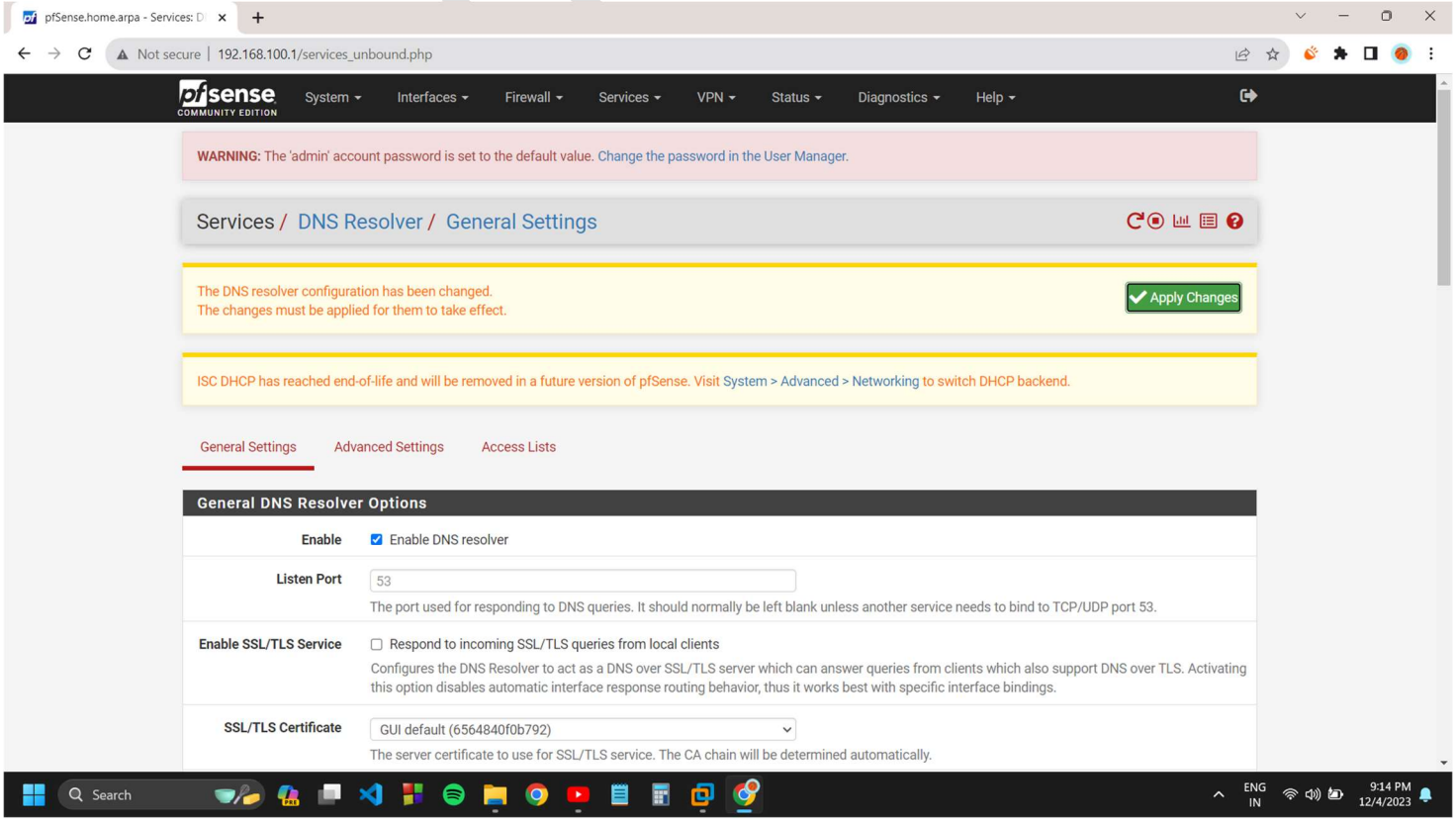
WINDOWS 7 IP : 192.168.100.100

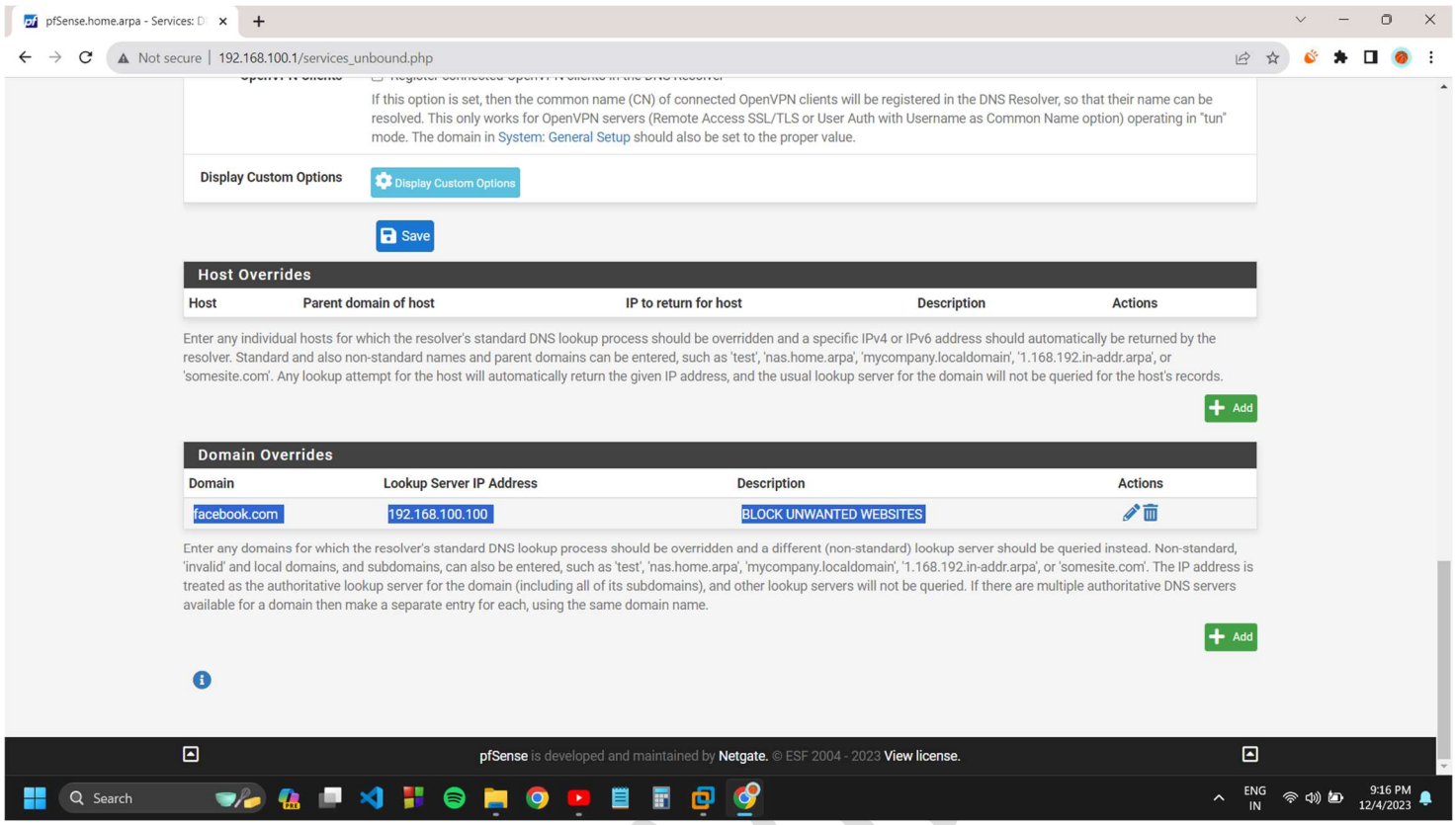


- **Before blocking a domain,check its availability.**

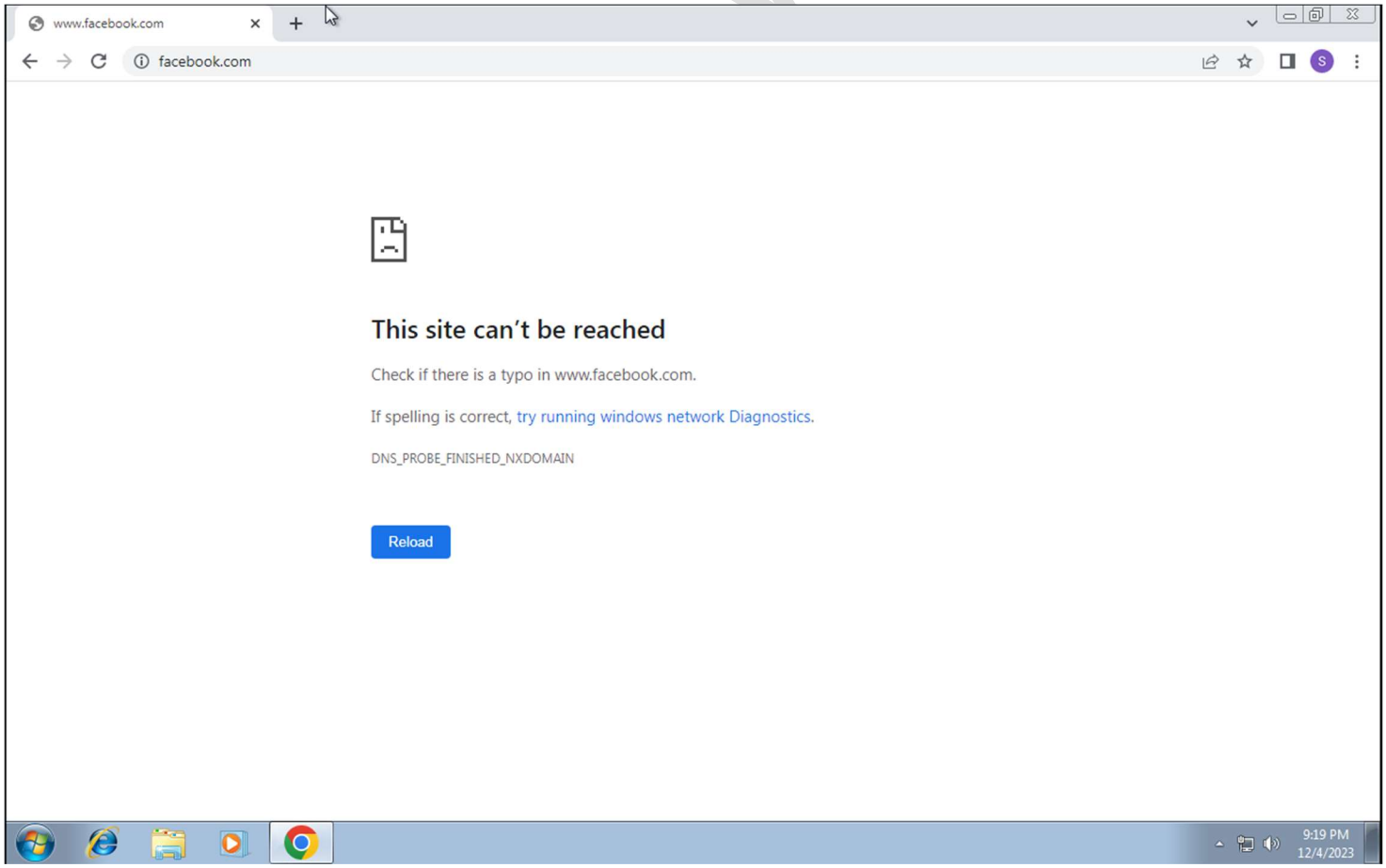


- **Now return to the pfsense web interface and click on apply changes.**

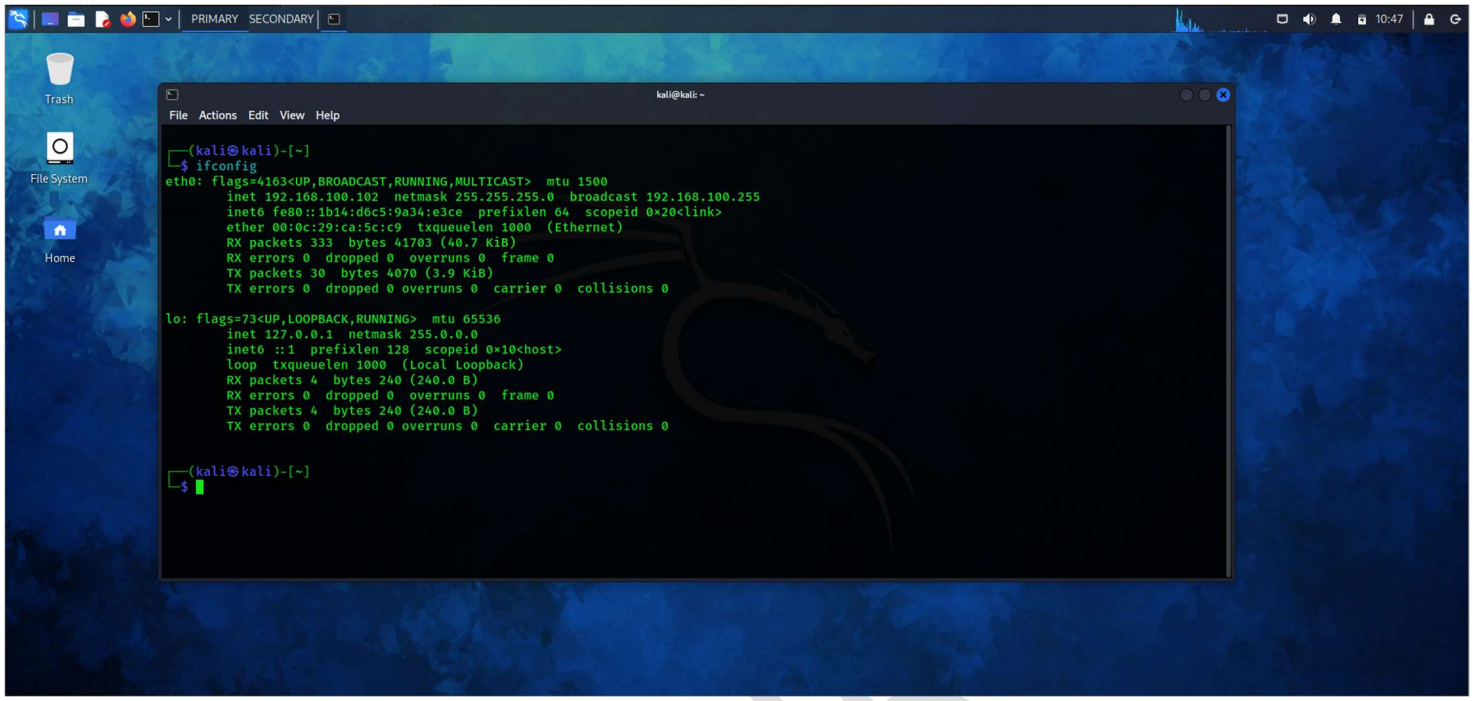


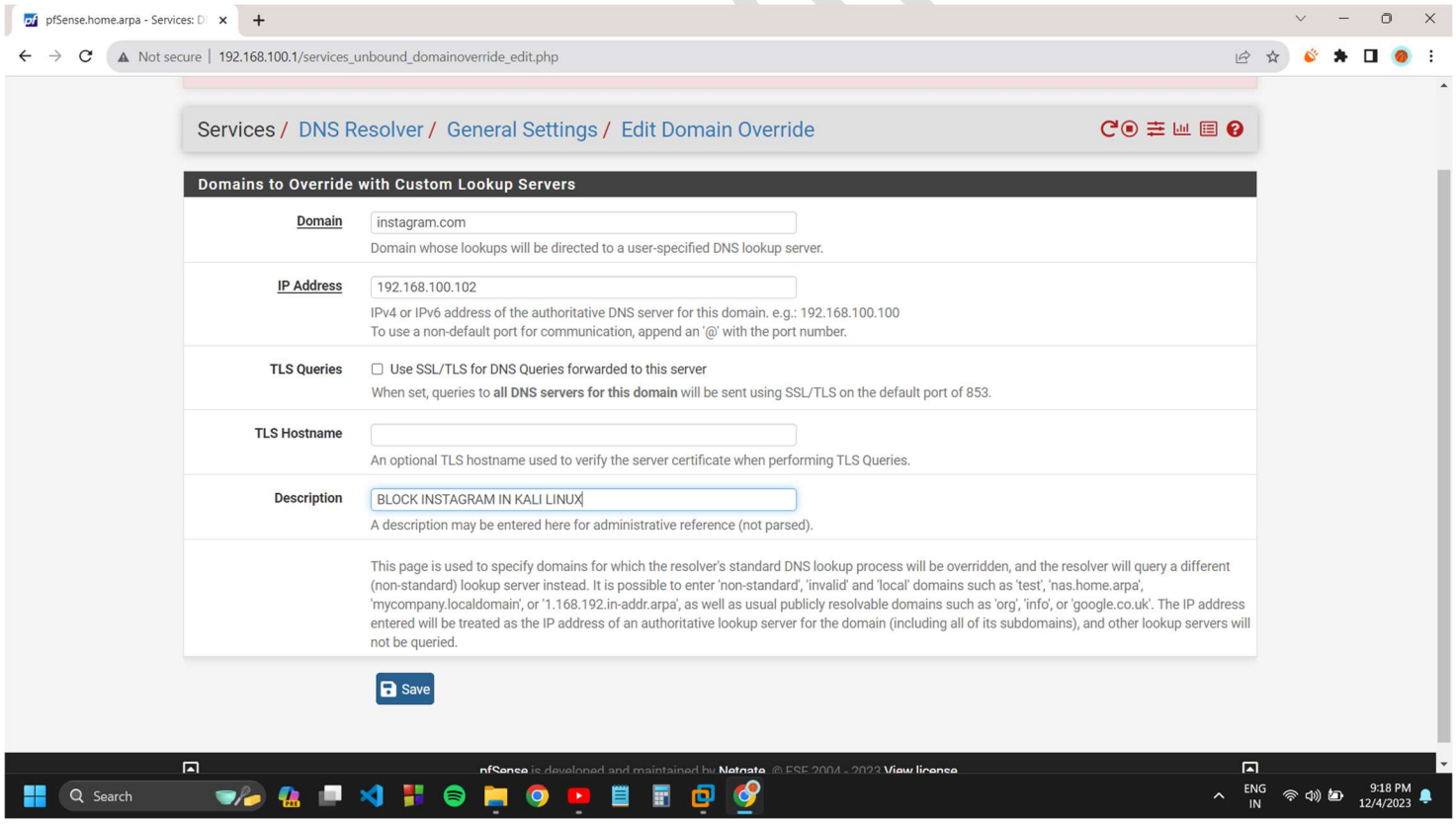


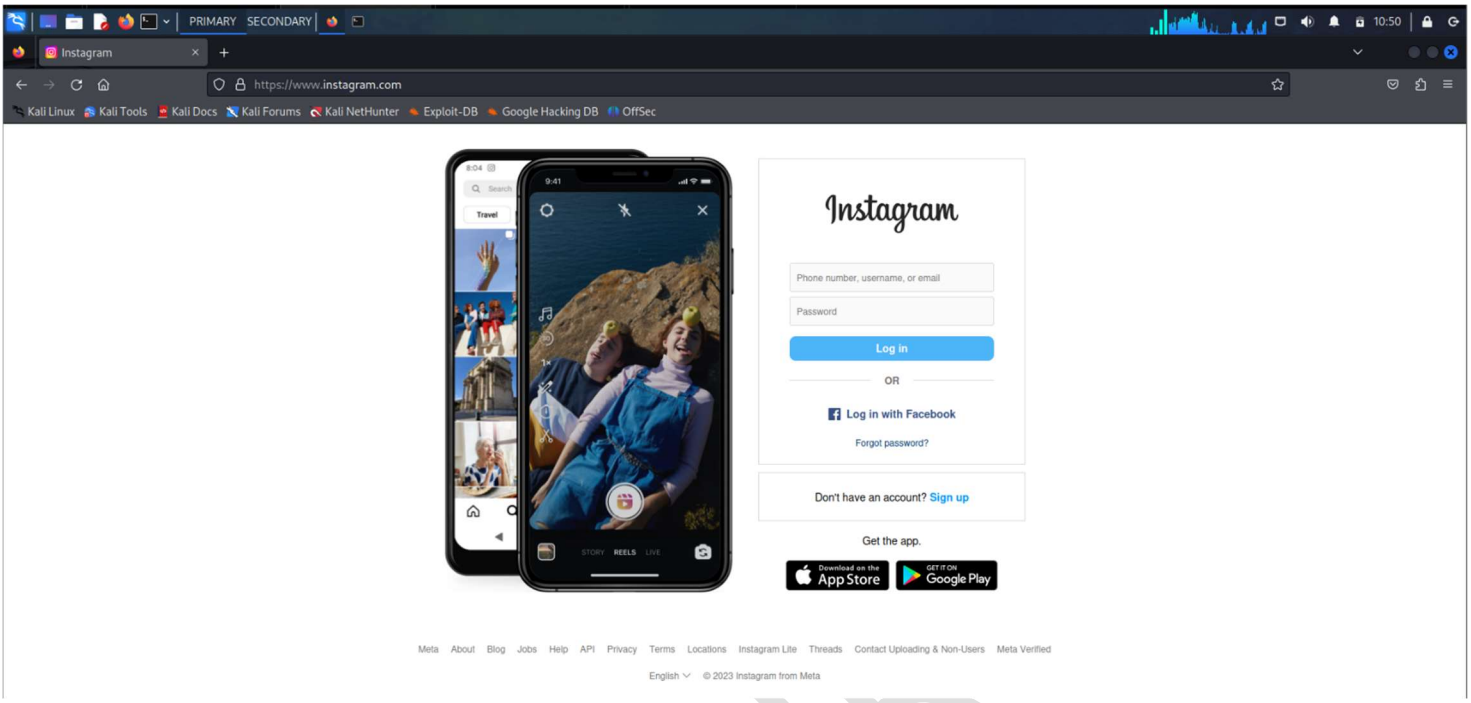
- **Availability of domain after blocking the domain.**

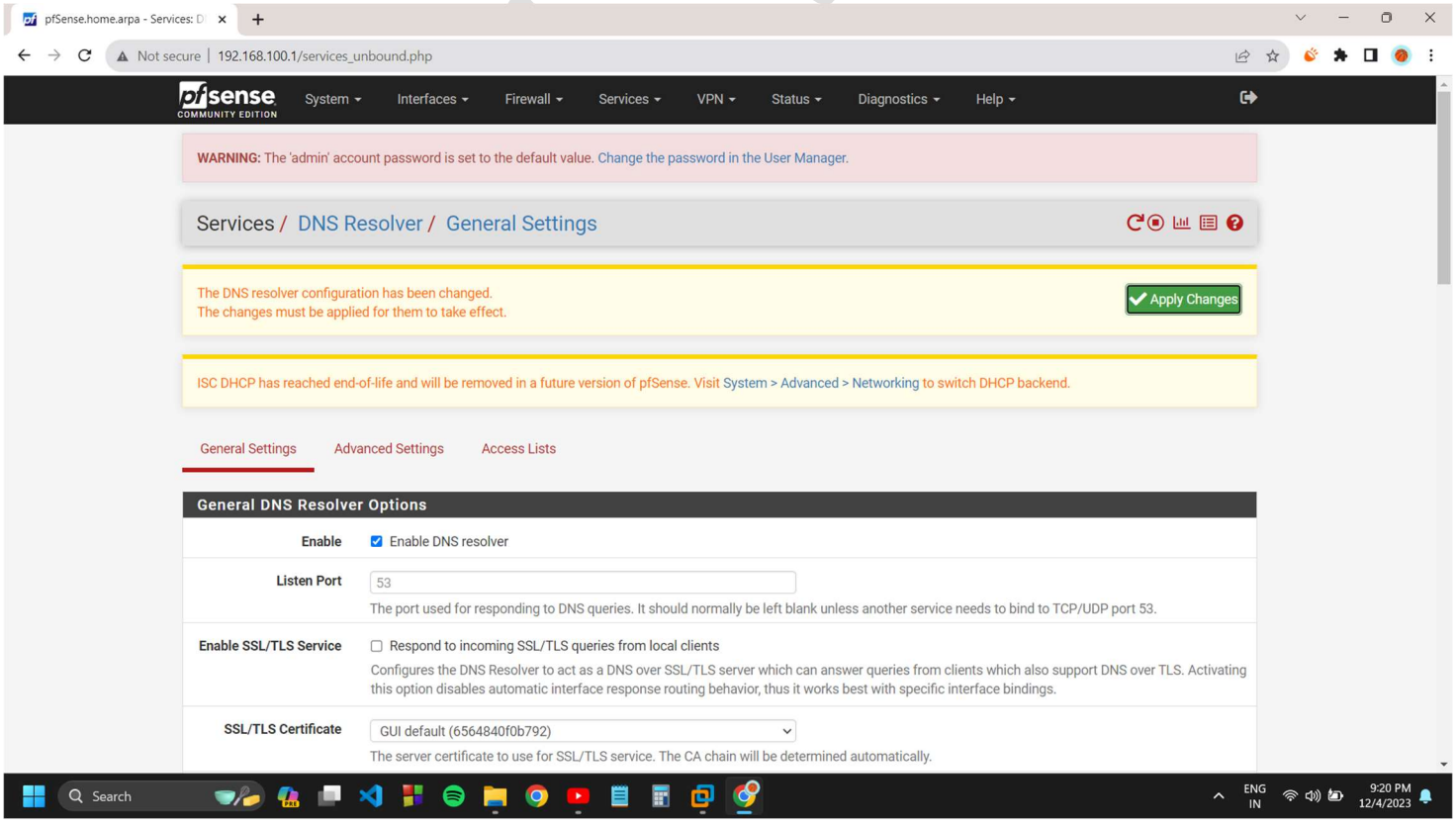


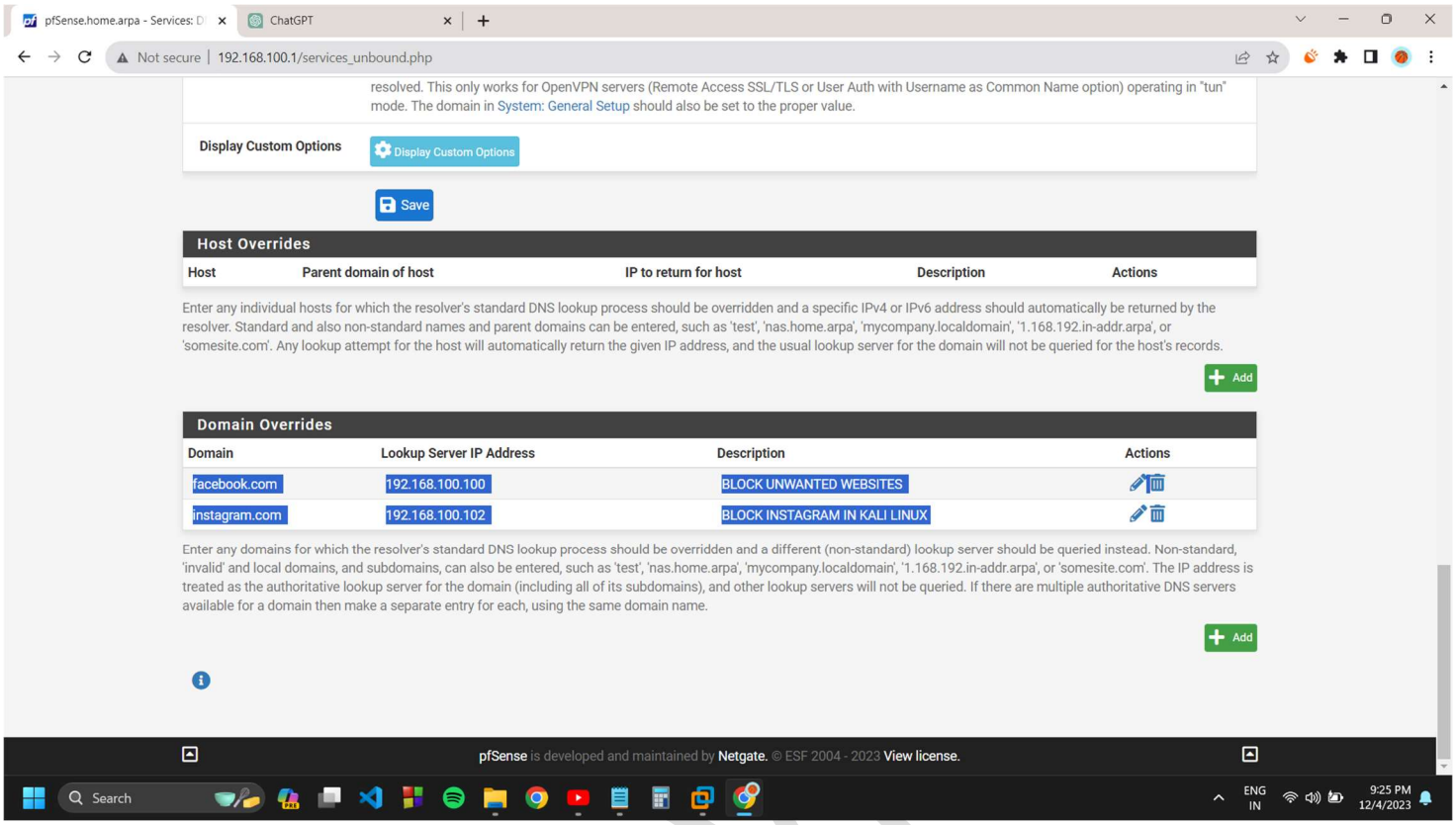
- **Now follow the same procedure and block Instagram.com from the Kali Linux virtual machine.**

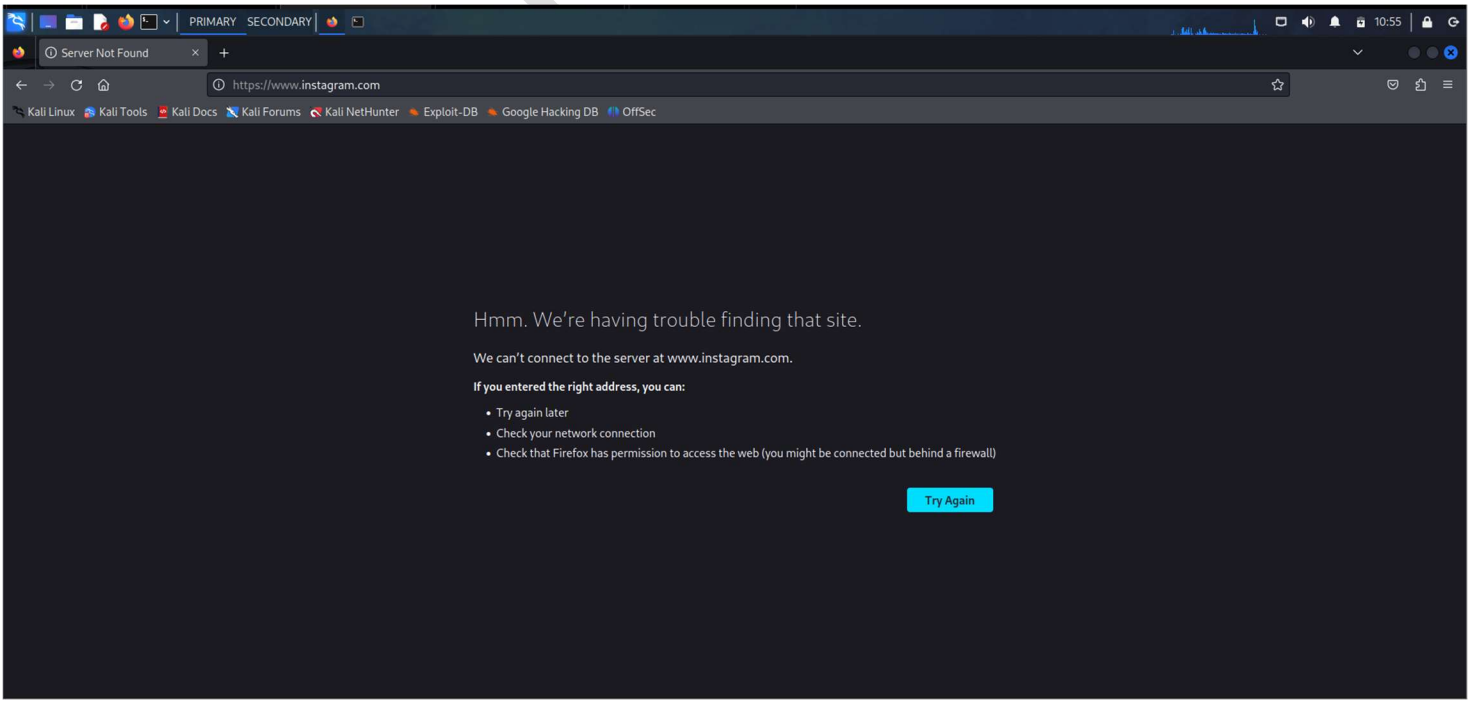





PRIMARY SECONDARY
10:50
Instagram
https://www.instagram.com
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Instagram
Phone number, username, or email
Password
Log in
OR
Log in with Facebook
Forgot password?
Don't have an account? Sign up
Get the app.
Download on the App Store
GET IT ON Google Play
Meta About Blog Jobs Help API Privacy Terms Locations Instagram Lite Threads Contact Uploading & Non-Users Meta Verified
English © 2023 Instagram from Meta


pfSense.home.arpa - Services: D
Not secure | 192.168.100.1/services_unbound.php
pfsense COMMUNITY EDITION
System Interfaces Firewall Services VPN Status Diagnostics Help
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.
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 (6564840f0b792)
The server certificate to use for SSL/TLS service. The CA chain will be determined automatically.
Search
ENG IN
9:20 PM 12/4/2023


pfSense.home.arpa - Services: D
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
instagram.com
192.168.100.102
BLOCK INSTAGRAM IN KALI LINUX
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
ENG IN
9:25 PM 12/4/2023


PRIMARY SECONDARY
10:55
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