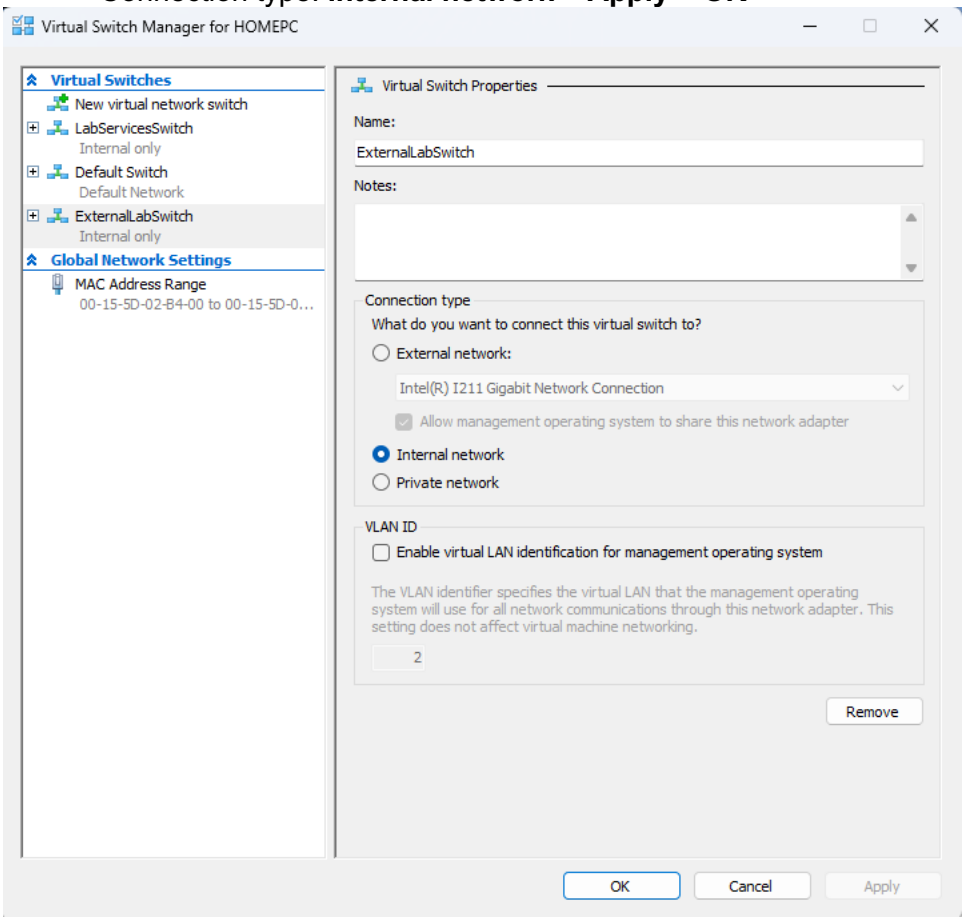
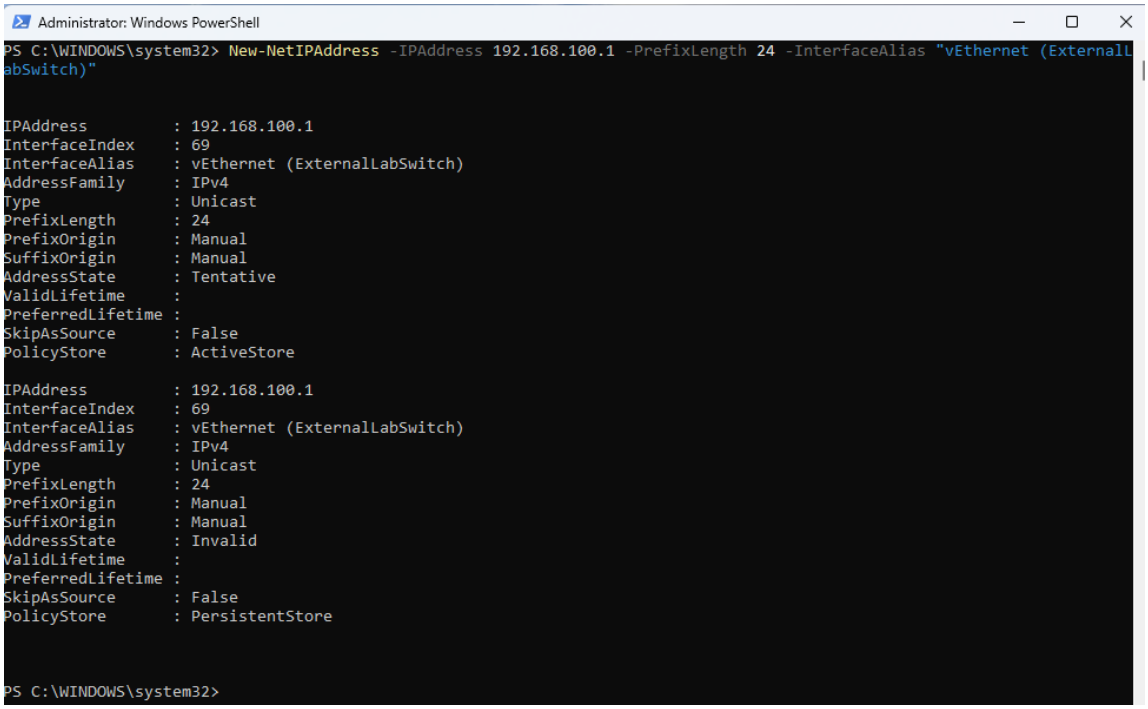
Installation and Configuration of VPN (OpenVPN) on pfSense and Testing by connecting remote Windows 10 to internal network

Prerequisites

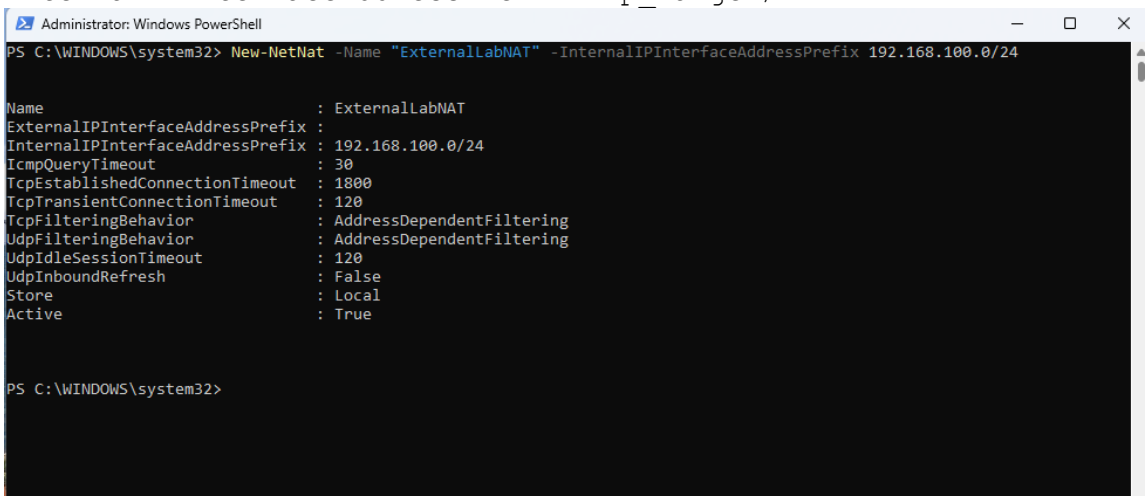
1. **Create an external virtual switch for pfSense WAN:**
    - On **Hyper-V**,
    - Right-click **pfSense VM > Settings > New virtual network switch**
    - Name: [newExternalSwitch]
    - Connection type: **Internal network > Apply > OK**



2. **Assign an IP address to the host's virtual adapter:**
   PowerShell (as administrator):
   `New-NetIPAddress -IPAdress <new_net_IP> -PrefixLength 24 -InterfaceAlias "vEthernet ([newExternalSwitch])"`

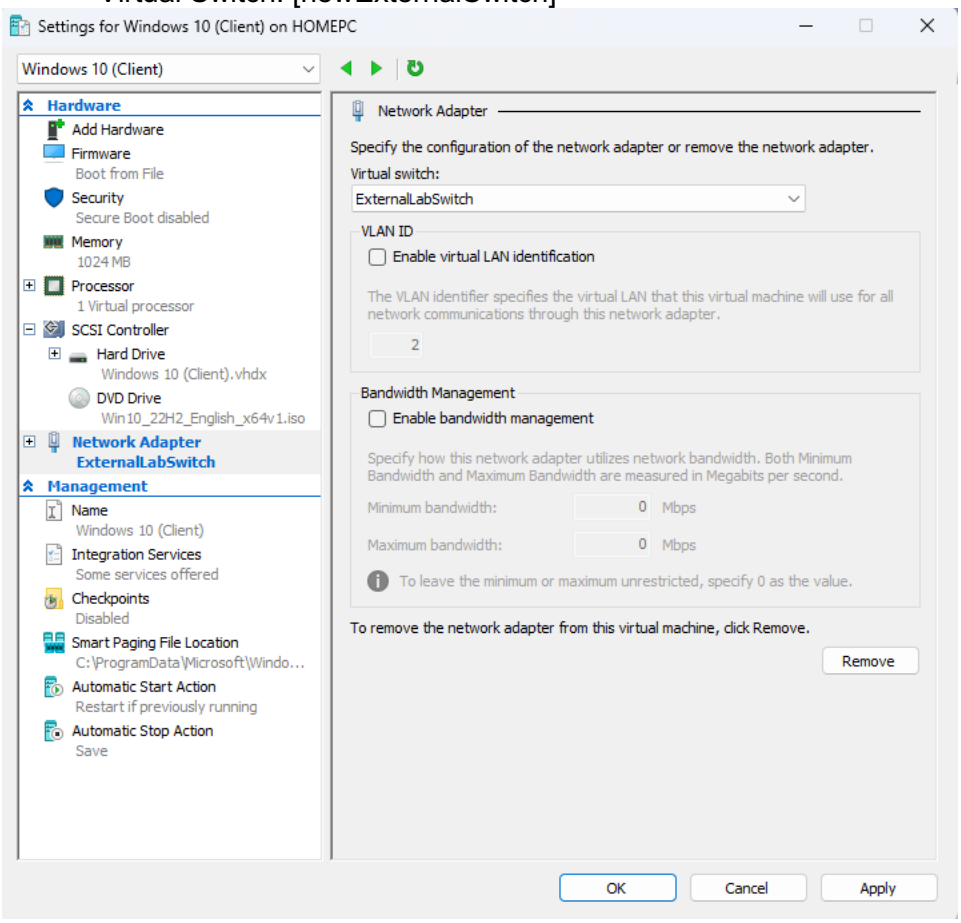


3. **Create a NAT network using this IP range:**
   PowerShell (as administrator):
   `New-NetNat -Name "[newNetNat]" -InternalIPInterfaceAddressPrefix <ip_range>/24`

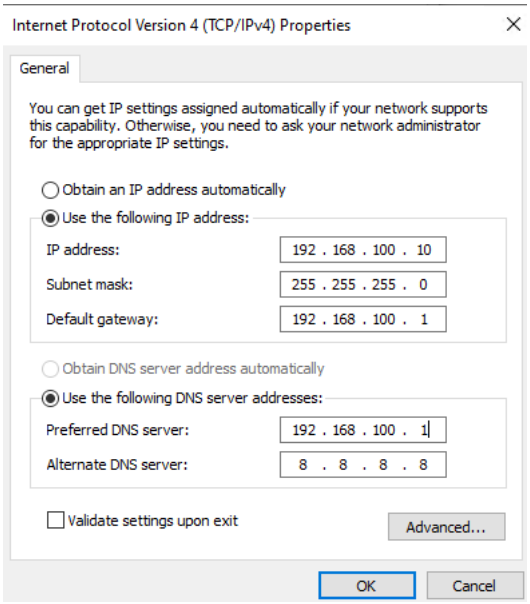


4. **Shutdown pfSense VM.**

5. **Change the network adapter settings of Windows 10 VM:**
    - On **Hyper-V**,
    - Right-click Windows 10 VM > Settings > Network Adapter
    - Virtual Switch: [newExternalSwitch]

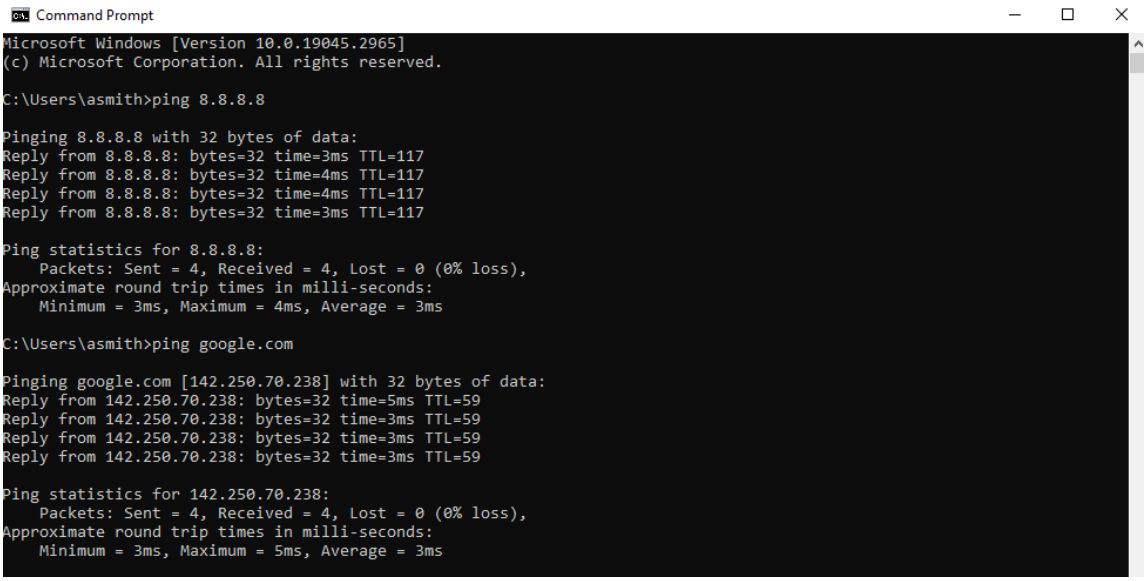


6. **Change the IP settings of the Windows 10 to connect to the NetIPAddress:**
    - Go to **Start > Control Panel > Network and Internet > Network and Sharing > Change adapter settings**
    - Right-click the **Ethernet > Properties > Select Internet Protocol Version 4 (TCP/IPv4) > Properties**
        - IP: <new_IP>
        - Subnet: 255.255.255.0
        - Gateway: <NetIPAddress>
        - DNS: 8.8.8.8 > OK > Close

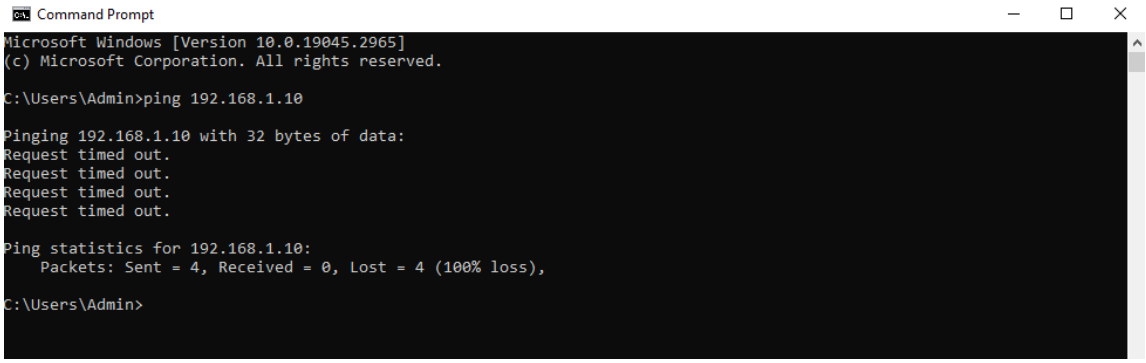


7. **Test Connectivity to internet:**

```
ping 8.8.8.8
ping google.com
```

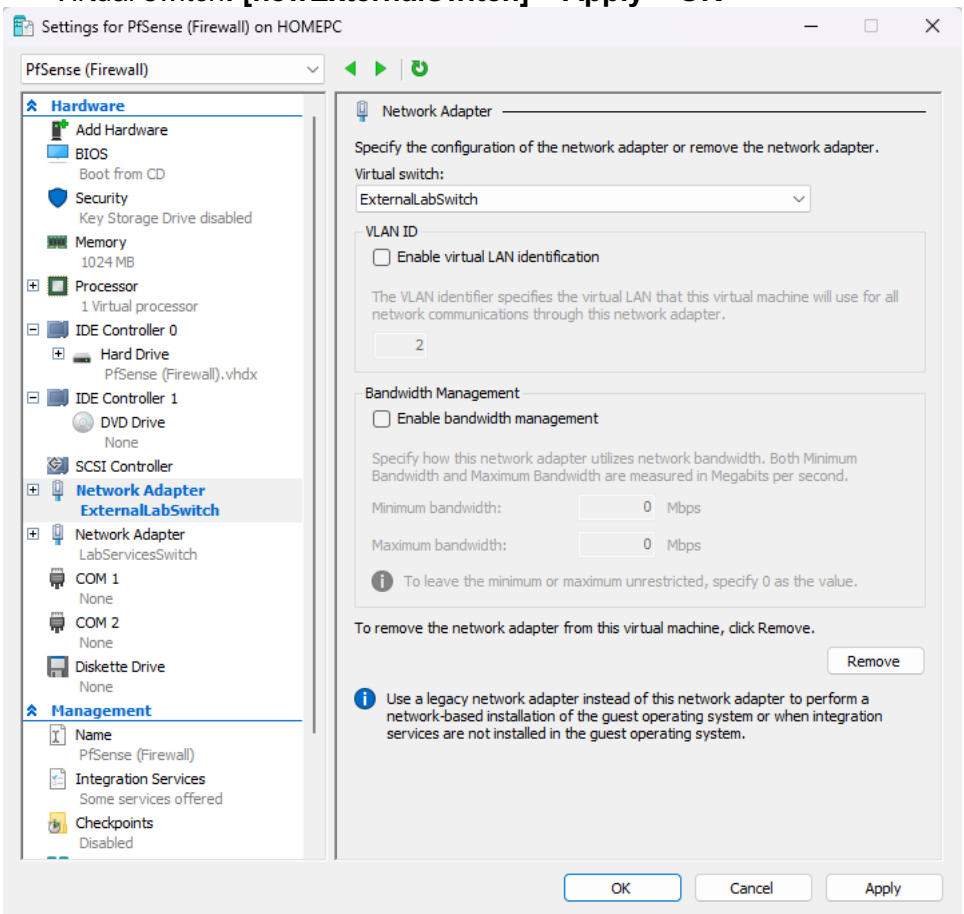


- **Test if you can connect to the Windows Server with the new IP Address:**
  It will not connect (request timed out) as they are in different subnet range.

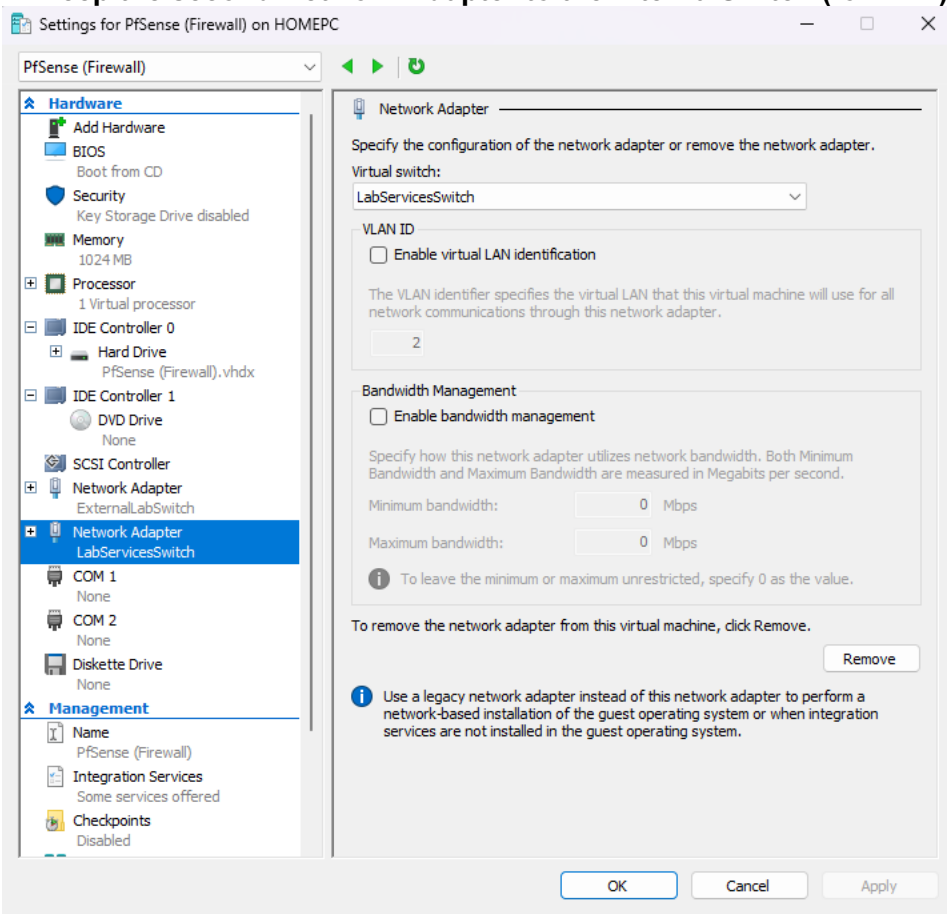


8. **Change the pfSense Network adapter Settings:**
   Keep pfSense connected to both:
   - **WAN interface** on [newExternalSwitch] (Internet)
   - **LAN interface** on LabServicesSwitch (Internal network)

- In **Hyper-V**,
- Right-**click pfSense VM > Settings > Network Adapter** (for WAN)
- Virtual switch**: [newExternalSwitch] > Apply > OK**

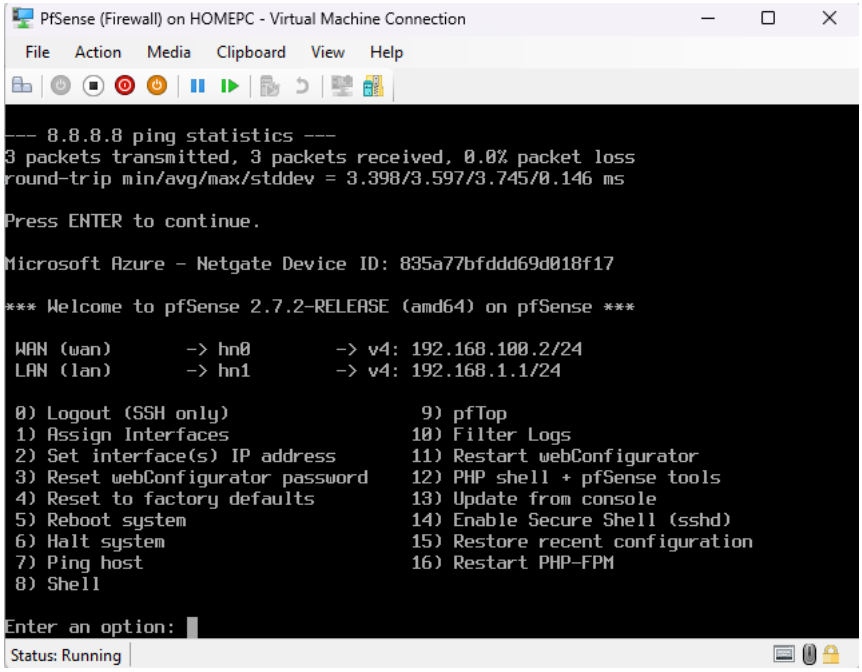


- **Keep the second Network Adapter to the internalSwitch (for LAN):**



9. **Connect to pfSense to make the changes:**
    - If not prompted, then Select option **1 (Assign interfaces)**
        - Do you want to configure VLANs now? [n]: n
        - Enter the WAN interface name: hn0 (hn0 hn1 a or ENTER)
        - Enter the LAN interface name: hn1 (hn0 hn1 a or ENTER)

    - Select option **2 (Set interface(s) IP address)**
    - Select **1 -> WAN**
        - Set **IPv4 address** when prompted to **<NetNatRange>**
        - When asked for subnet range: **24**
        - Gateway: **<NetIPAddress>**
        - Set it as default gateway: **y**
    - On the pfSense console, you'll see:
    - WAN -> v4: 192.168.100.X
    - LAN -> v4: 192.168.1.1

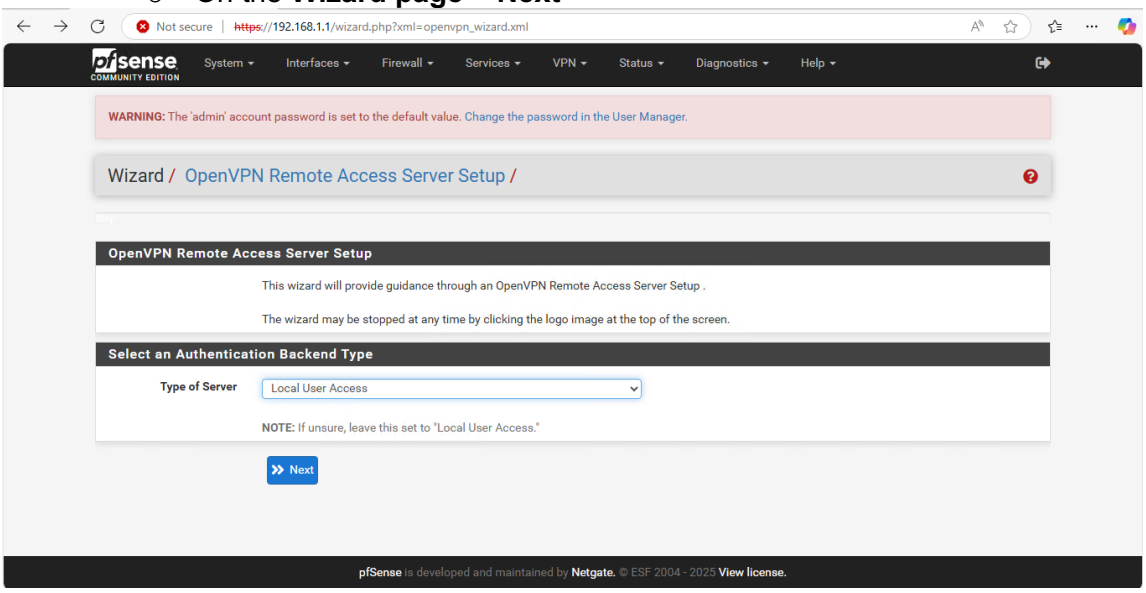


Setup VPN on pfSense (OpenVPN Server)

1. **Access pfSense Web UI via Windows Server**
    - In browser,
      http://<pfsense_ip>
    - Login using default credentials if not changed:
        - Username: admin
        - Password: pfsense

2. Launch the OpenVPN Wizard

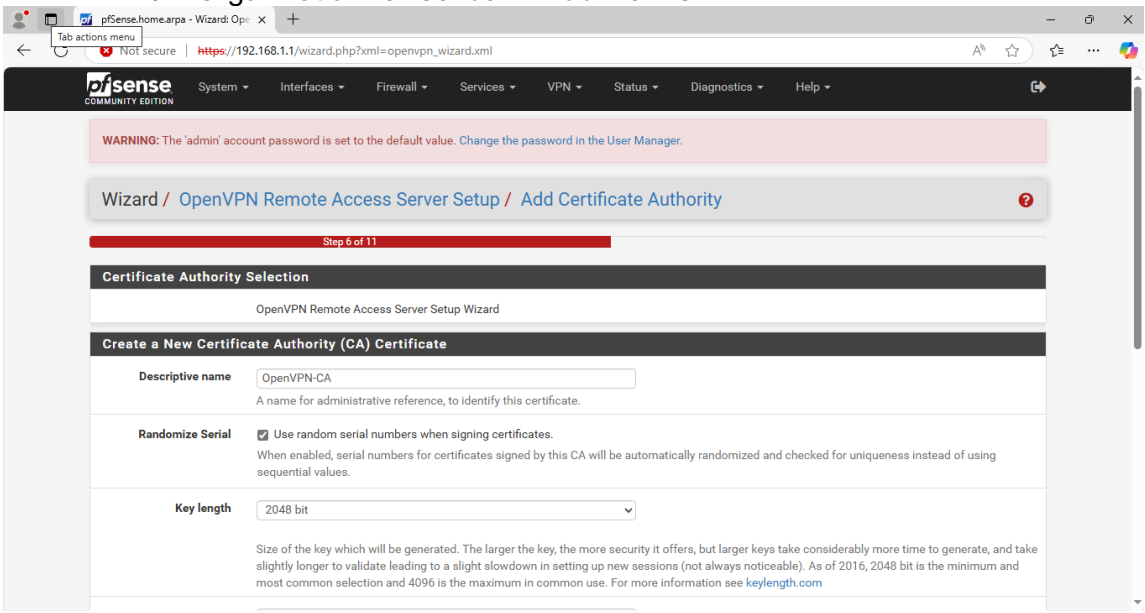
- Navigate to:
  VPN > OpenVPN > Wizards
  - On the **Wizard page > Next**

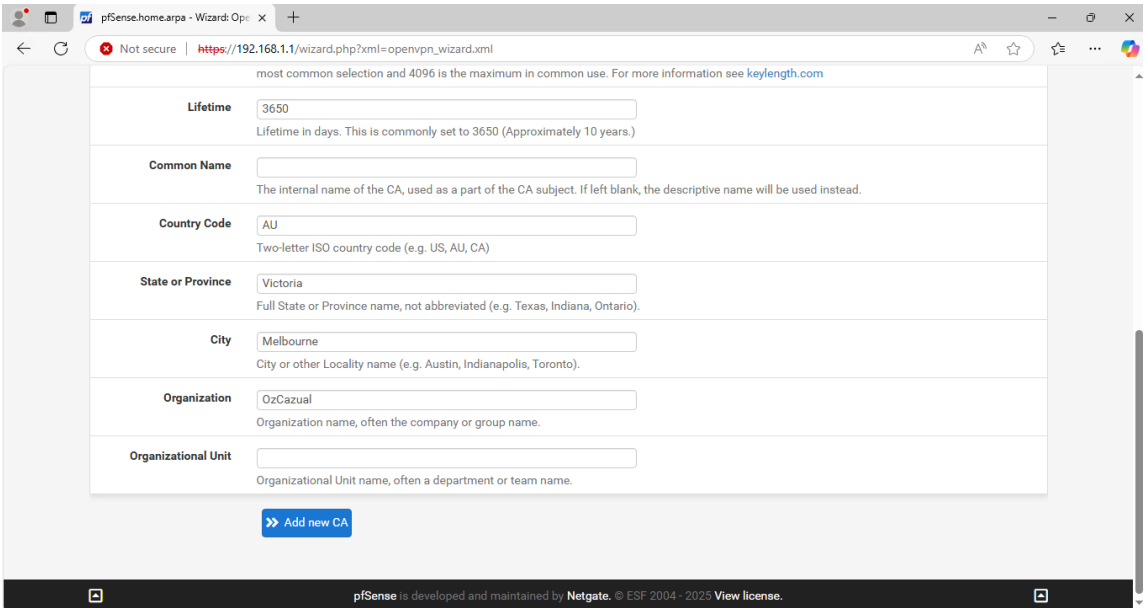


3. Create Certificate Authority (CA)

You'll first create a root CA for your VPN:

- **Descriptive Name**: OpenVPN-CA
- Fill in the fields (or leave defaults):
  - Country Code: AU
  - State: Victoria
  - City: Melbourne
  - Organization: OzCazual > **Add New CA**

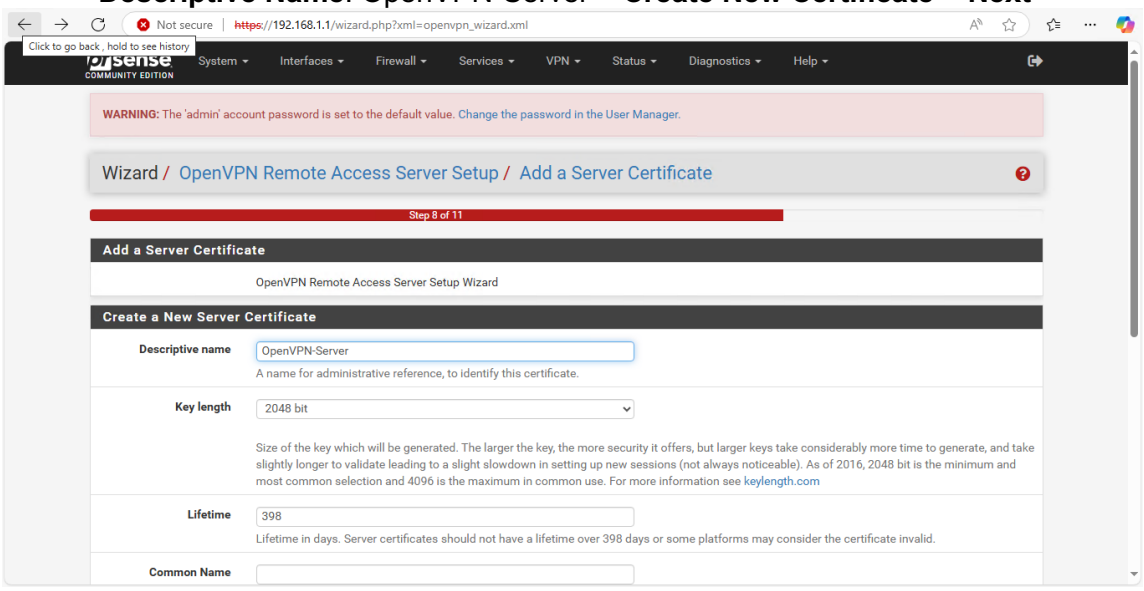




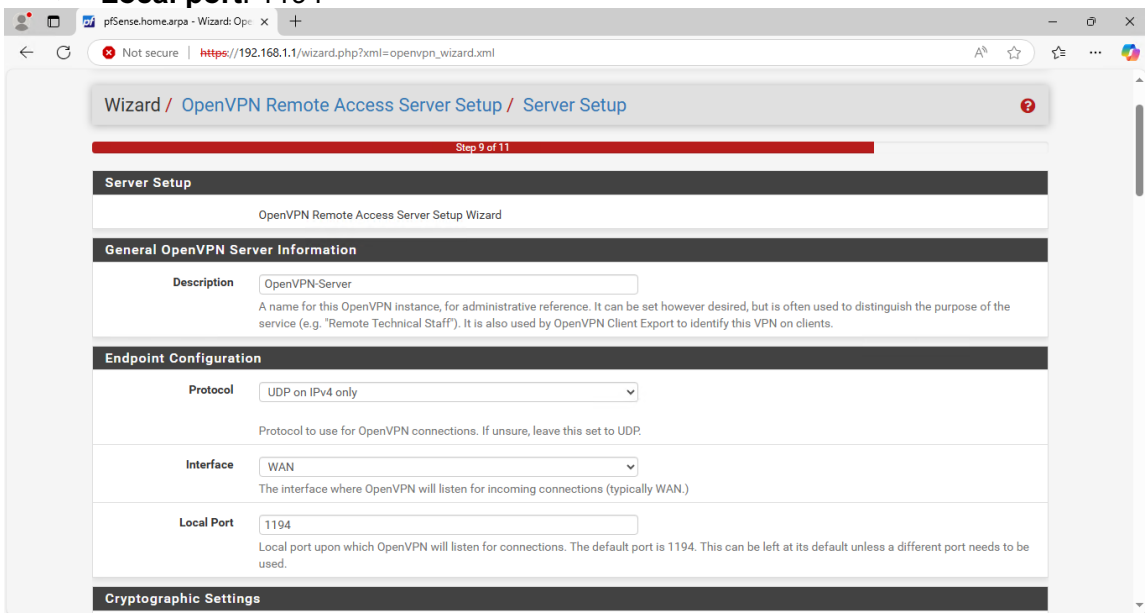
4. Create Server Certificate

Now generate a certificate that the VPN server will use:

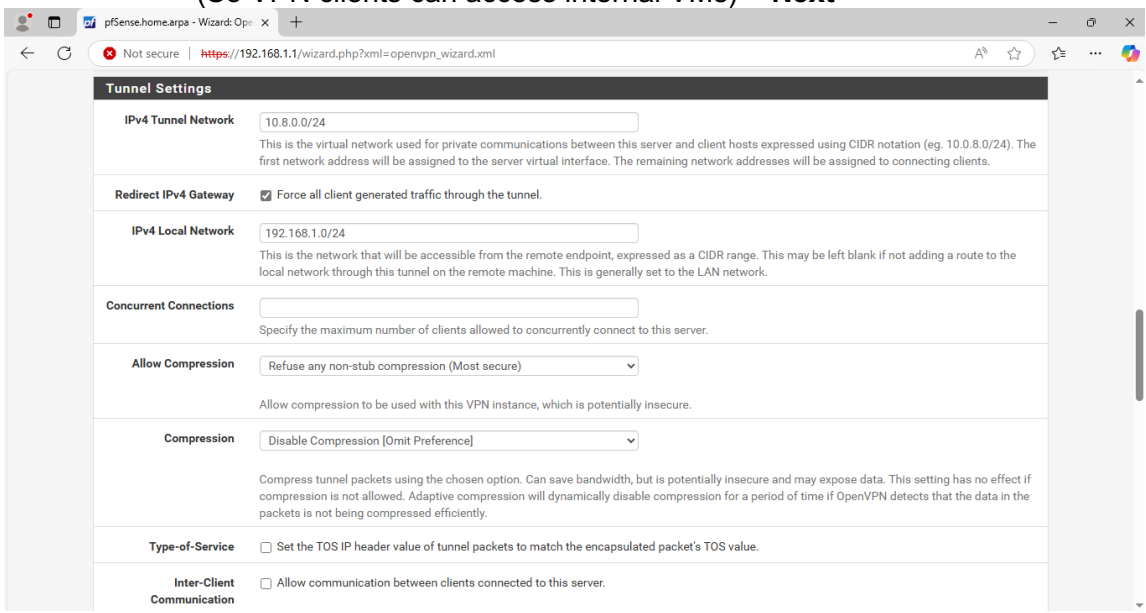
- **Descriptive Name**: OpenVPN-Server > **Create New Certificate** > **Next**



5. **Configure OpenVPN Server**
   - **Protocol**: UDP on IPv4 only
   - **Interface**: WAN
   - **Local port**: 1194

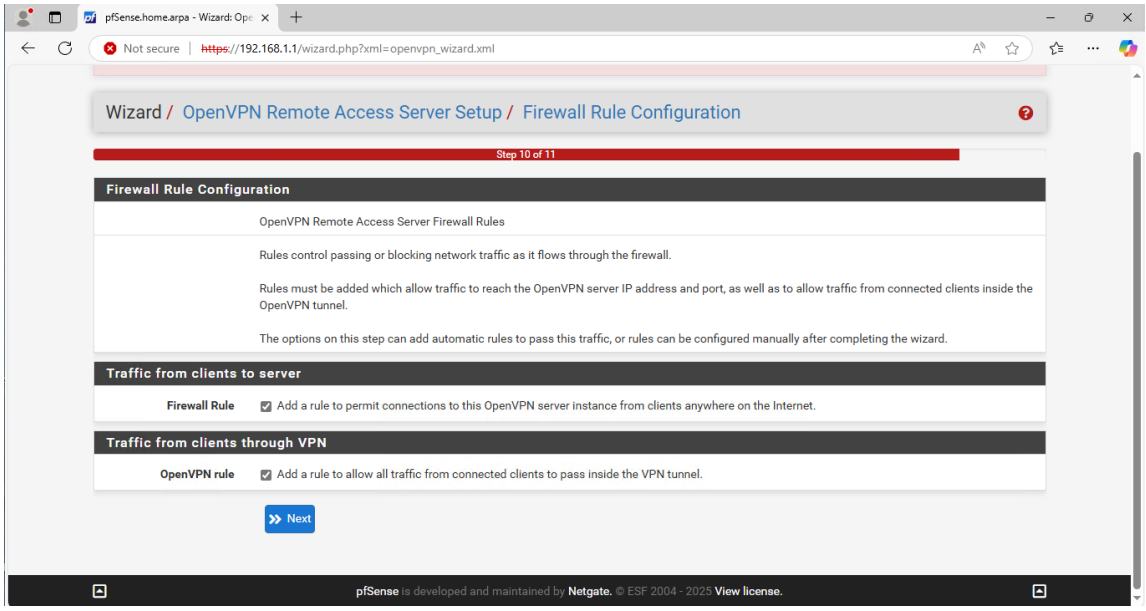


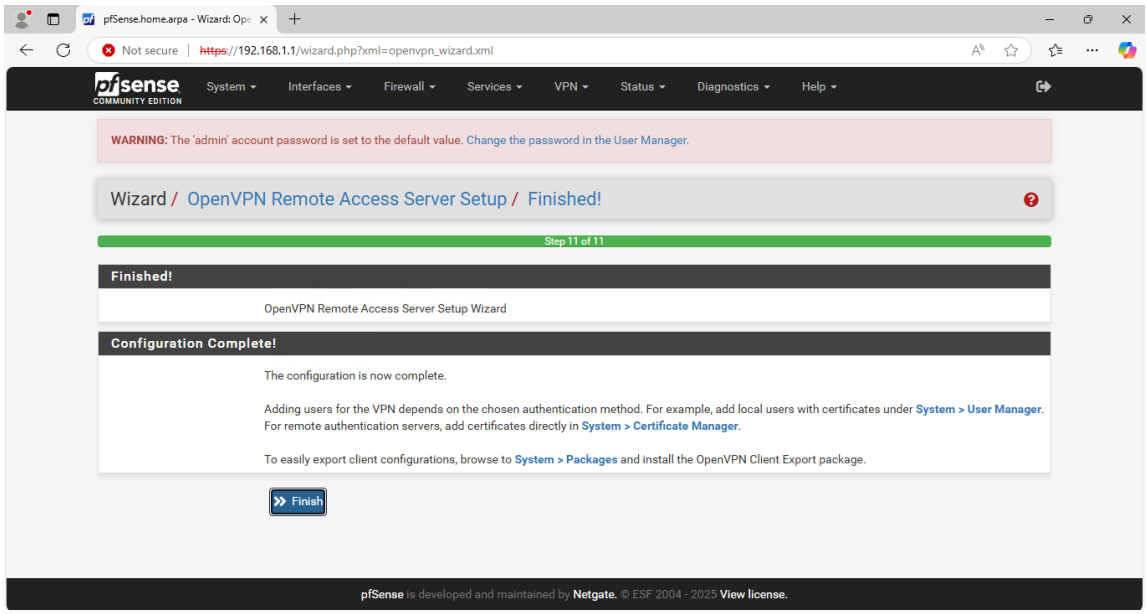
- **Tunnel Settings:**
  - **Tunnel Network**: 10.8.0.0/24
    (This is the virtual VPN subnet)
  - **Local Network**: 192.168.1.0/24
    (So VPN clients can access internal VMs) > **Next**



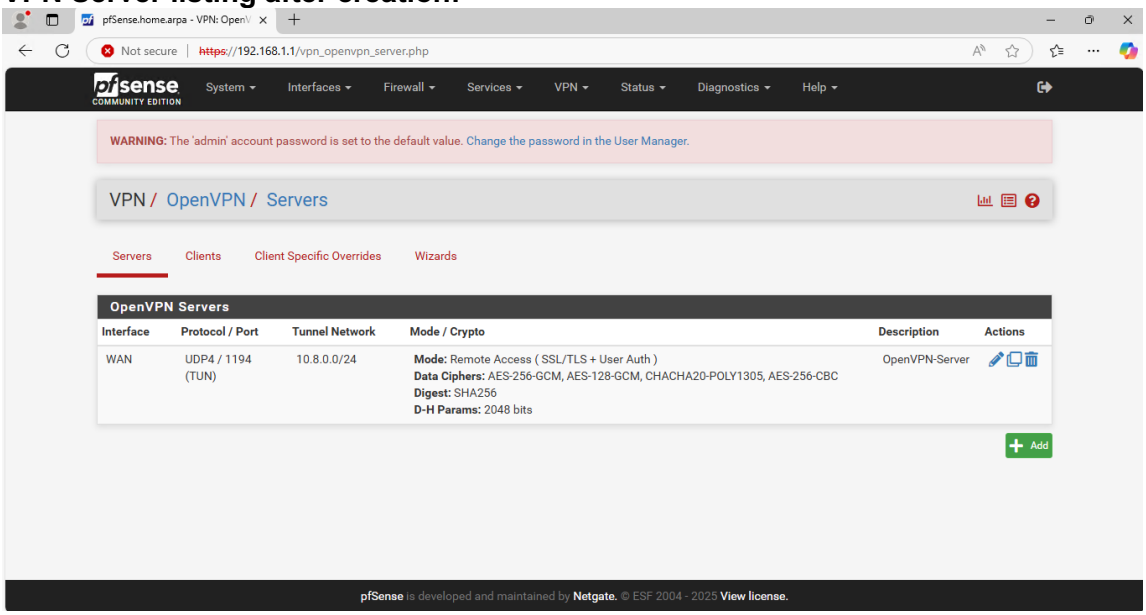
6. Firewall Rules

- pfSense will ask if you want to auto-create rules:
- Check:
  - **Firewall Rule** to allow traffic on WAN for OpenVPN
  - **OpenVPN Rule** to allow traffic from VPN clients to LAN
- Click **Next** > **Finish**

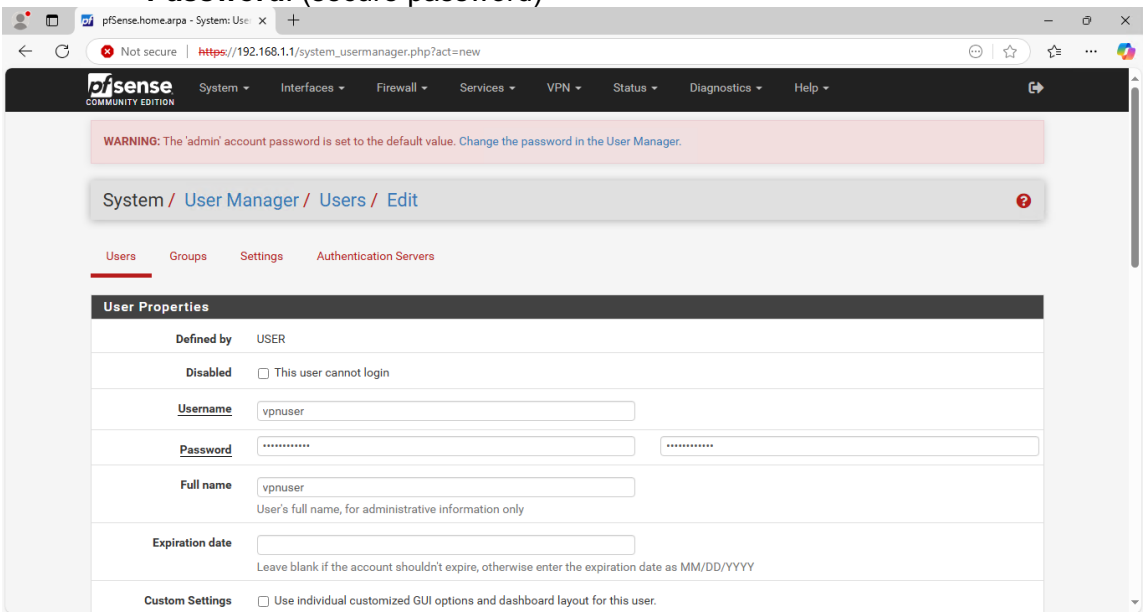




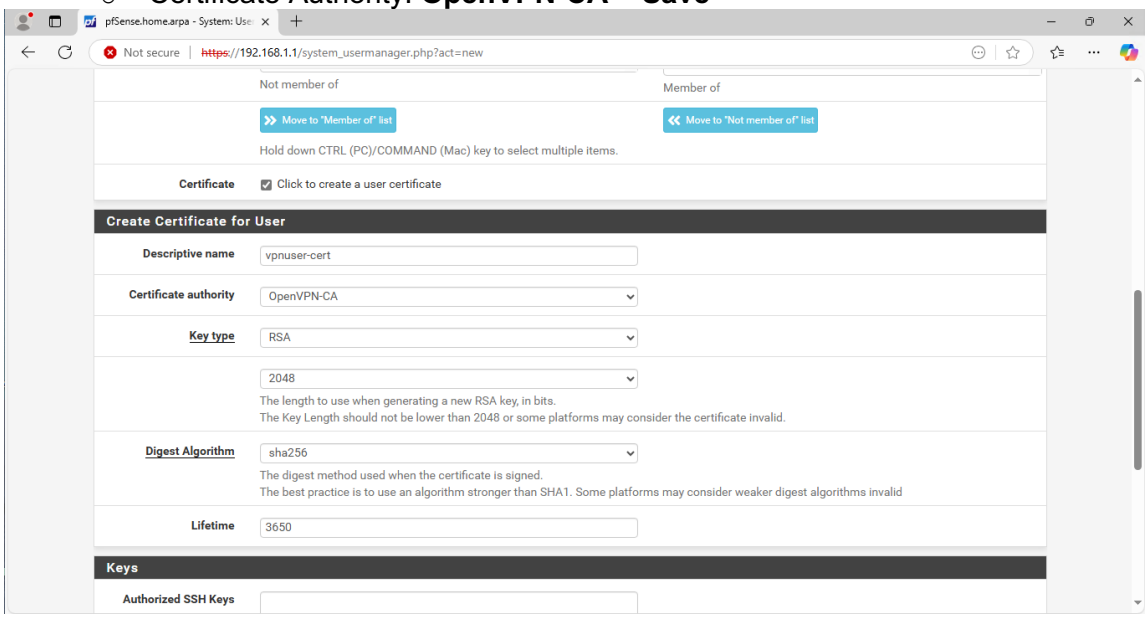
VPN Server listing after creation:



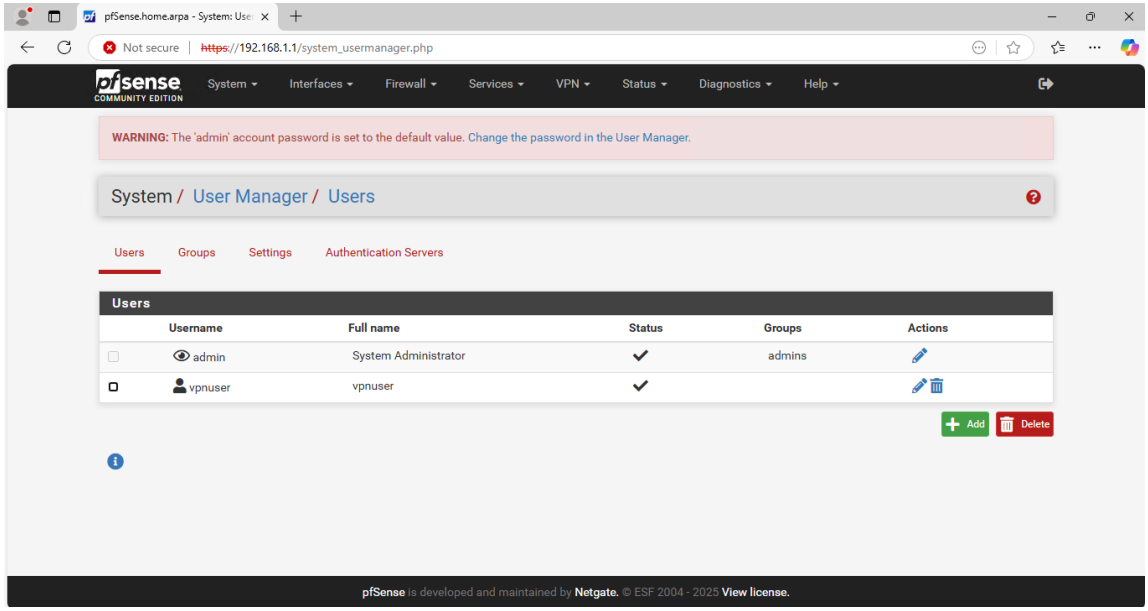
7. **Create a VPN User with Certificate**
   Go to **System > User Manager**
   Click **Add** to create a new user
   Fill in:
   - **Username**: vpnuser
   - **Password**: (secure password)



- **Check**: "Click to create a user certificate"
    - Descriptive Name: **vpnuser-cert**
    - Certificate Authority: **OpenVPN-CA** > **Save**

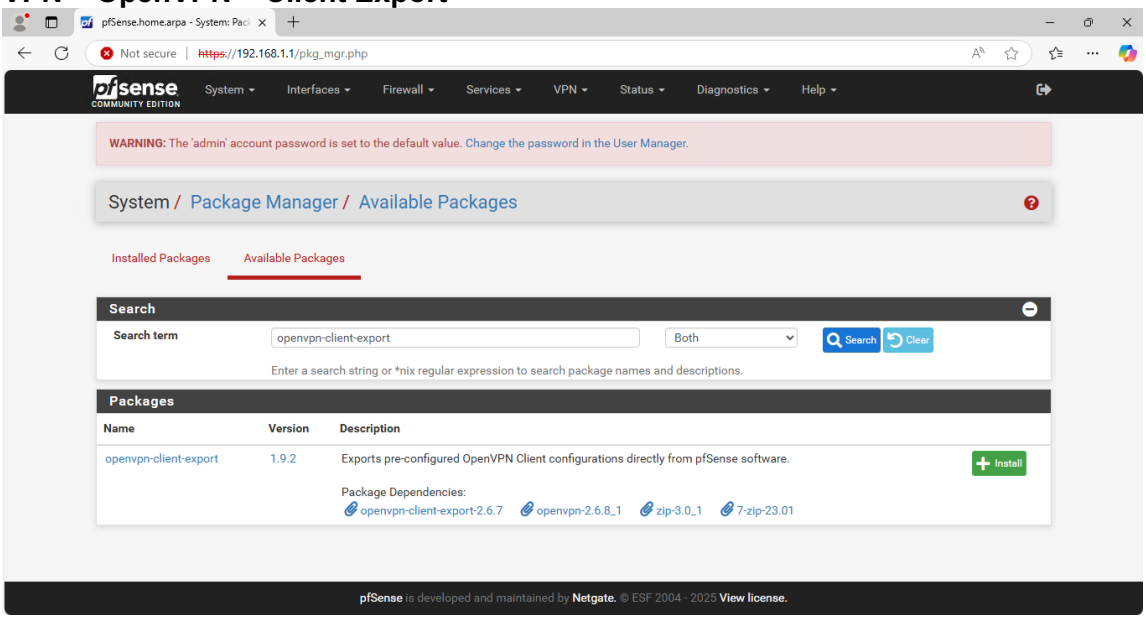


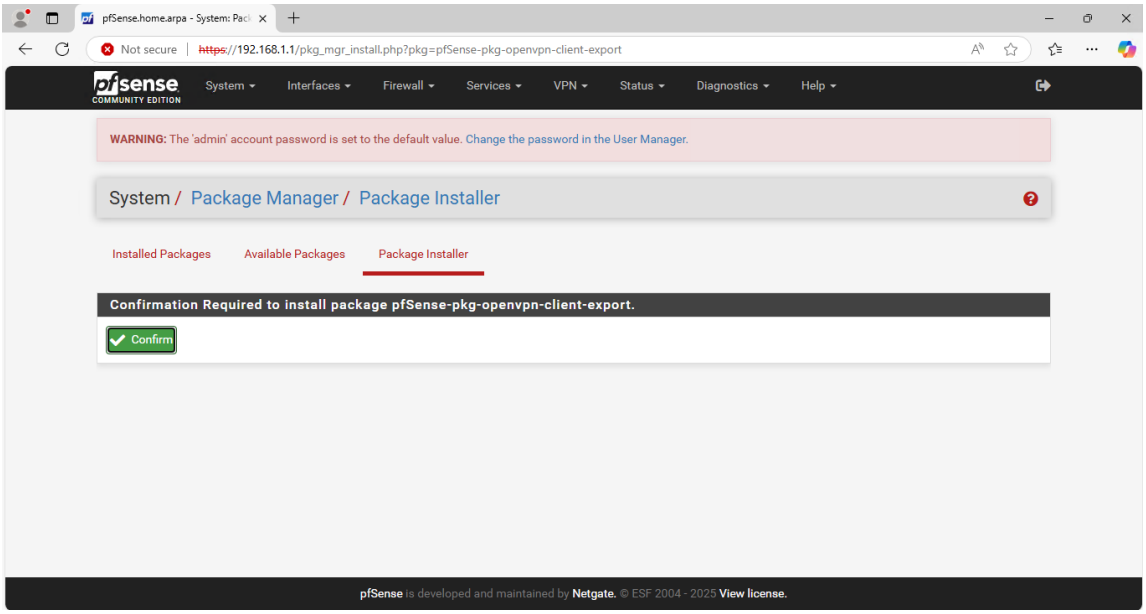
- **VPN user listed under Users after creation:**

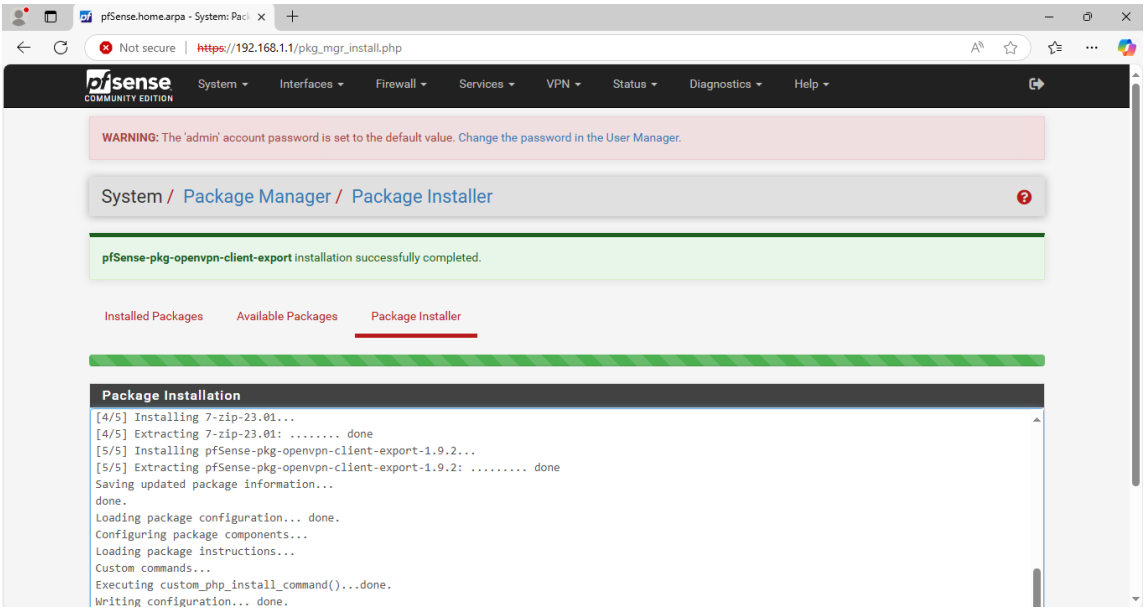


8. Install the Client Export Package

- Go to **System > Package Manager > Available Packages**
- Search for openvpn-client-export > **Install**
- Once installed, go to:
  VPN > OpenVPN > Client Export



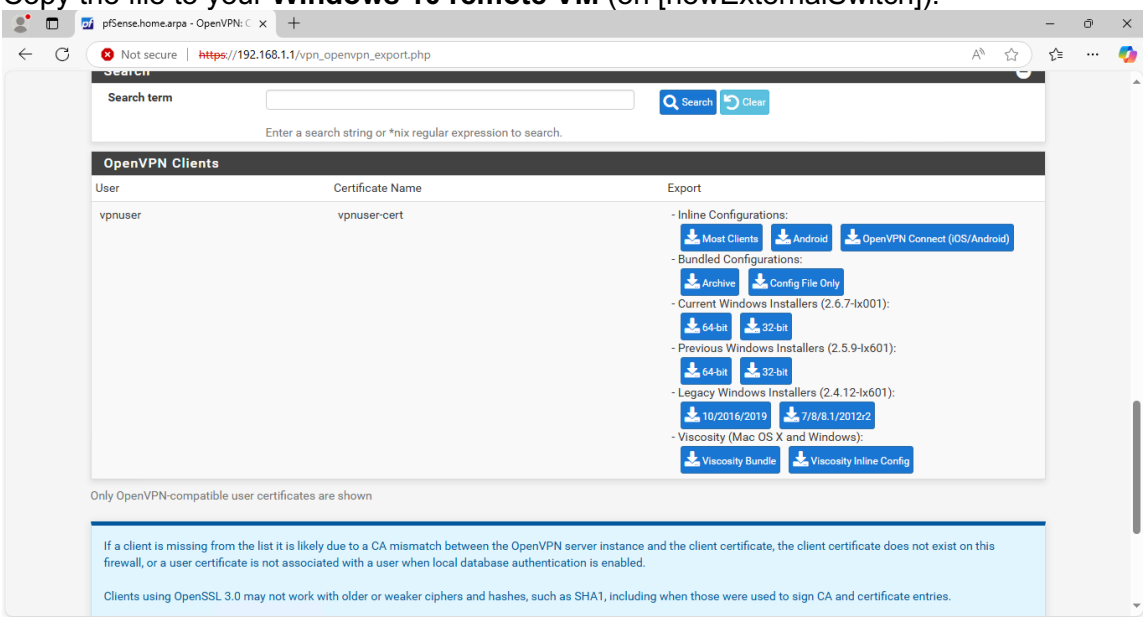




9. Download VPN Configuration for Windows 10

1. Scroll to **Client Export** section
2. Find the row for vpnuser
3. Download:
    - **Inline Configurations (Most Clients)** containing .ovpn config file if you want to use OpenVPN GUI

Copy the file to your **Windows 10 remote VM** (on [newExternalSwitch]).

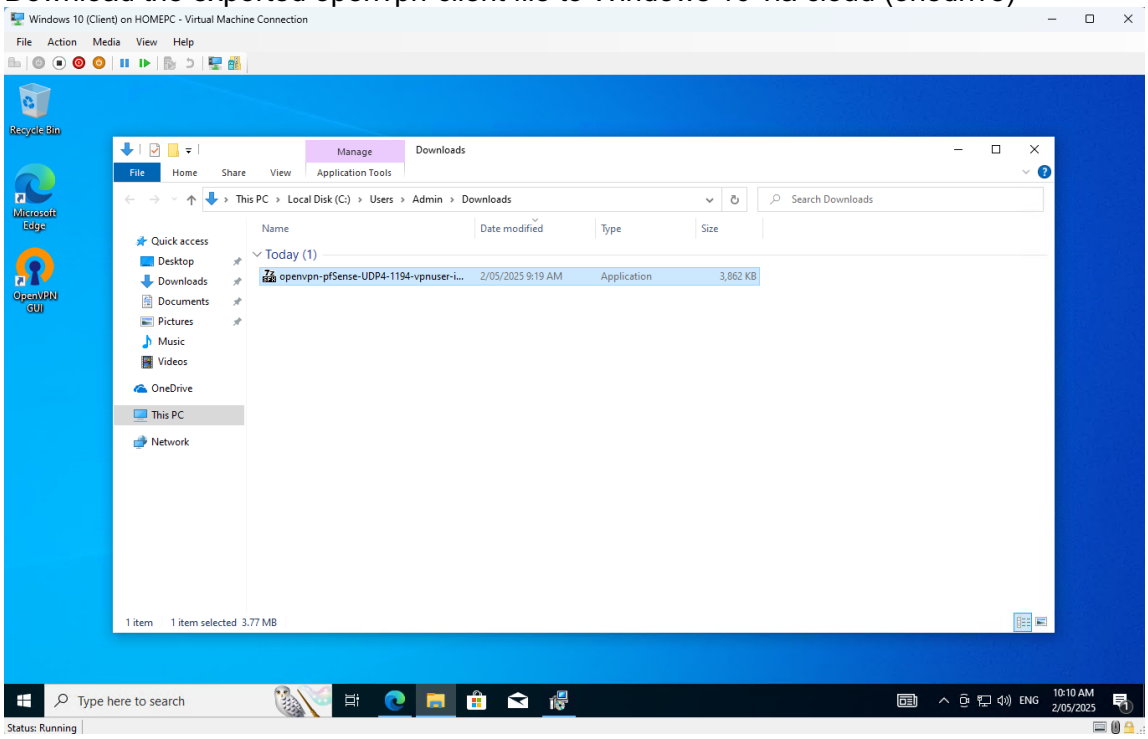


10. Download OpenVPN Client for Windows

1. Go to the official OpenVPN website: https://openvpn.net/community-downloads/
2. Under **Windows**, download the installer (e.g., OpenVPN-2.6.x-Ixxxx-win10.exe).

OR

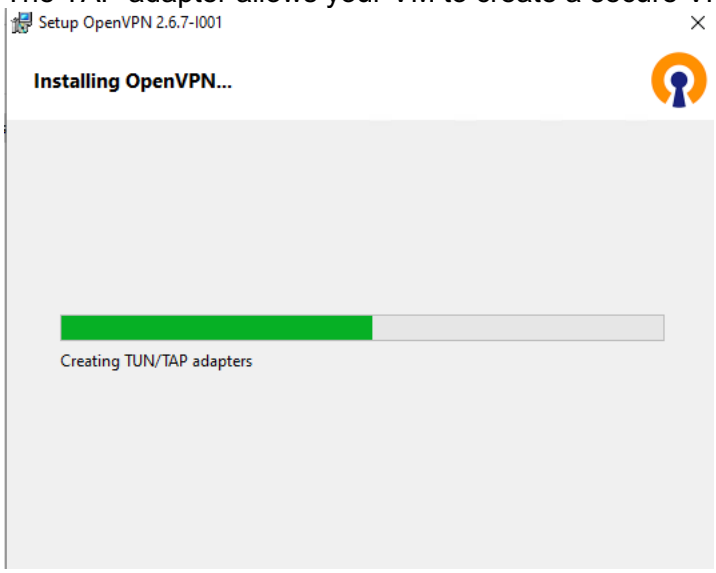
Download the exported openvpn-client file to Windows 10 via cloud (onedrive)

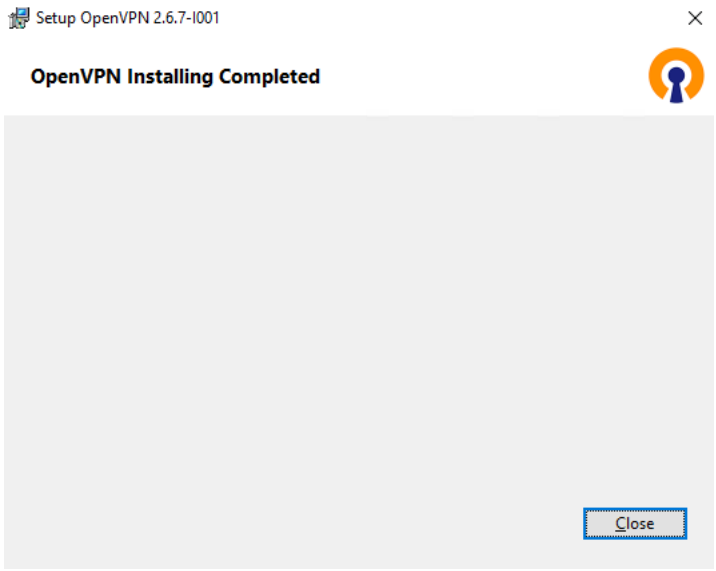


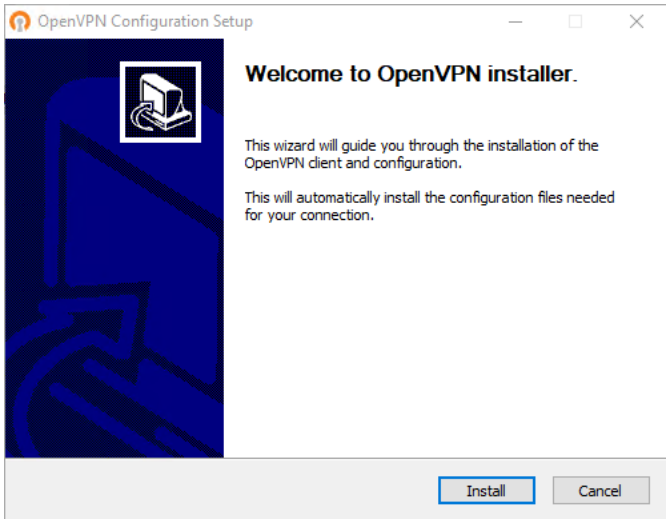
11. Install OpenVPN GUI

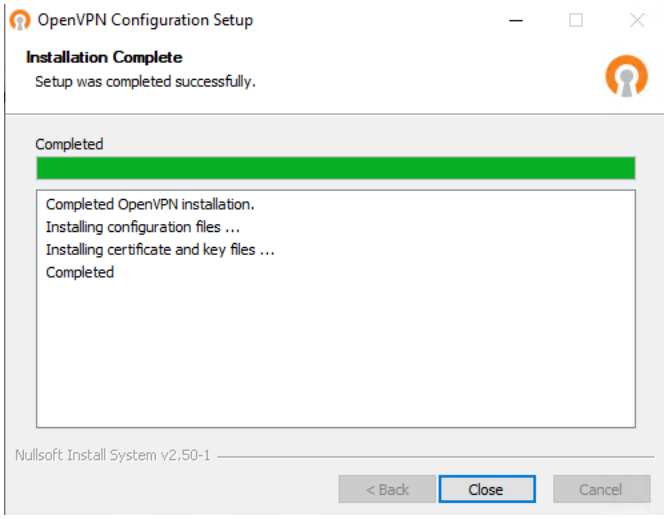
1. **Run the installer** as administrator.
2. Choose **"Next"** through the installation wizard and accept all defaults.
3. Allow it to install **OpenVPN GUI** and **TAP drivers** (virtual network adapter).
4. Finish the installation.

The TAP adapter allows your VM to create a secure VPN tunnel.

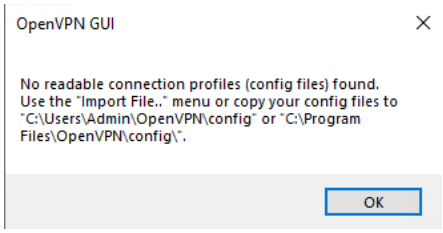



Setup OpenVPN 2.6.7-I001
OpenVPN Installing Completed
Close


OpenVPN Configuration Setup
Welcome to OpenVPN installer.
This wizard will guide you through the installation of the OpenVPN client and configuration.
This will automatically install the configuration files needed for your connection.
Install
Cancel


OpenVPN Configuration Setup
Installation Complete
Setup was completed successfully.
Completed
Completed OpenVPN installation.
Installing configuration files ...
Installing certificate and key files ...
Completed
Nullsoft Install System v2.50-1
< Back
Close
Cancel

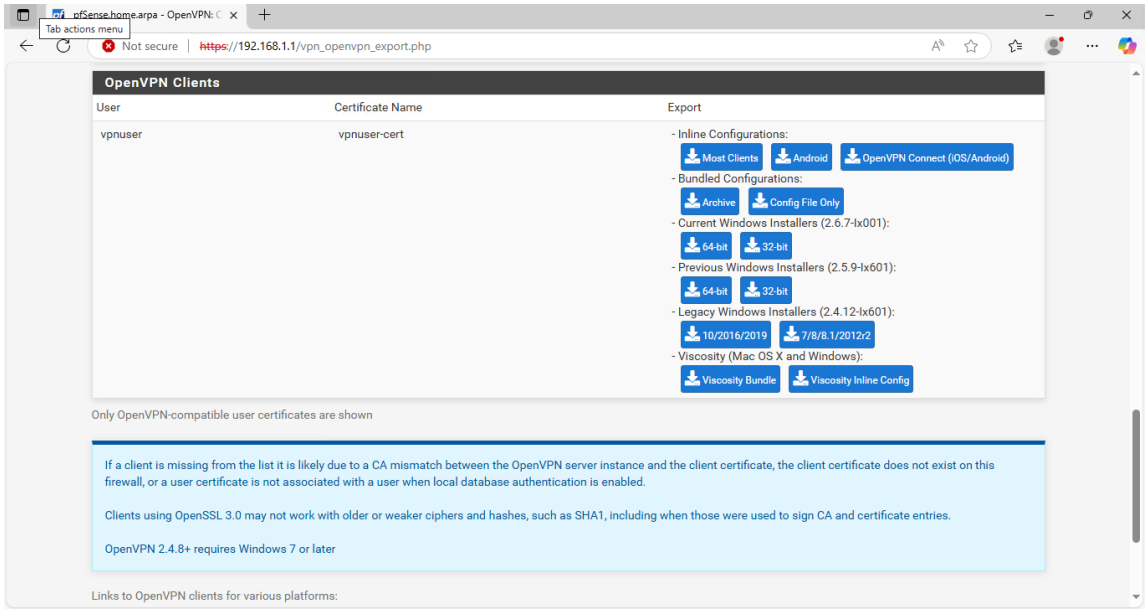
- **If this error occurs after installation of .exe file:**



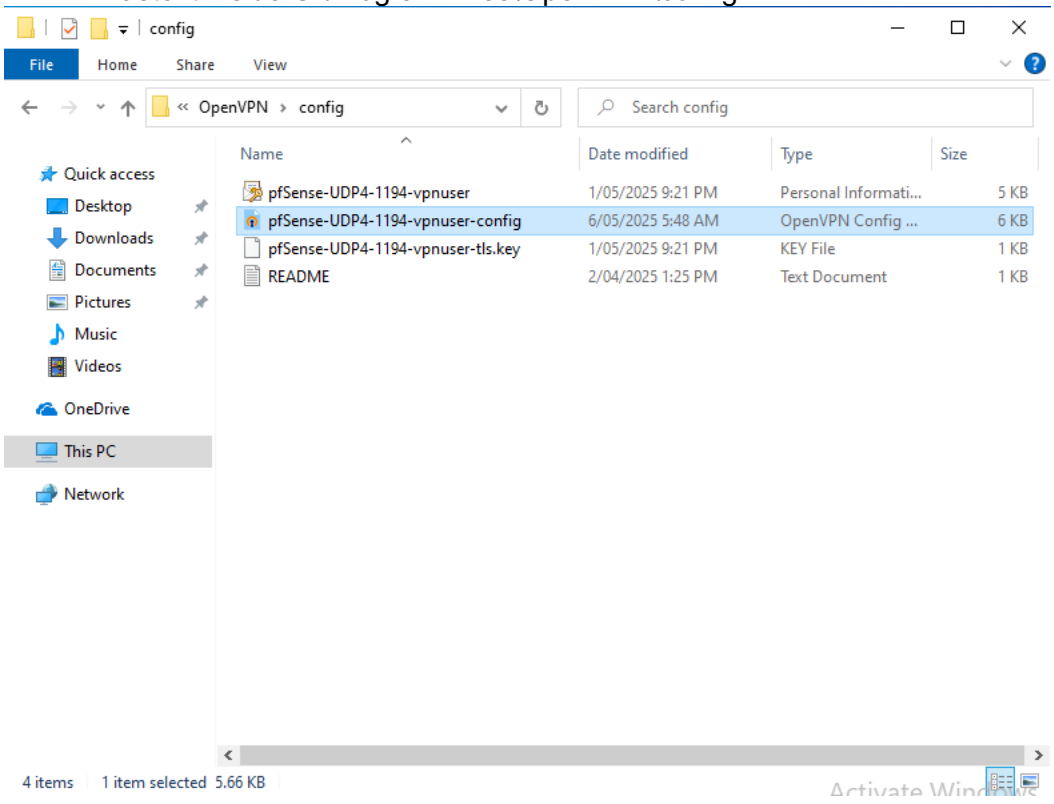
Open **pfSense Web UI**,

- Go to **VPN > OpenVPN > Client Export** tab
- **Scroll** to the **VPN user** you created then download **Inline Configurations: Most clients**

This will download a **.ovpn file** which has to be copied to the remote Windows 10.

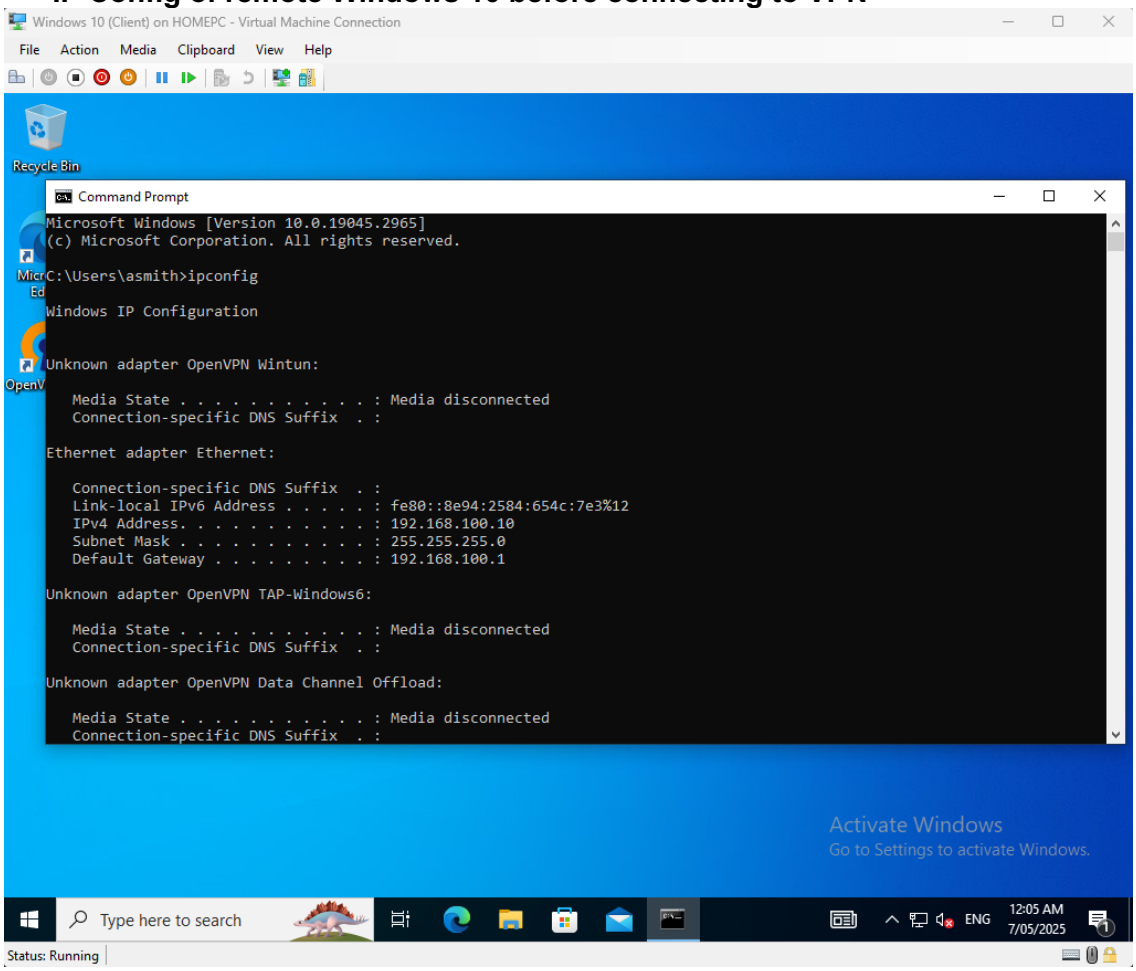


- **Copy the client export .ovpn file into the remote Win 10 VM:**
  Paste it inside C:\Program Files\OpenVPN\config

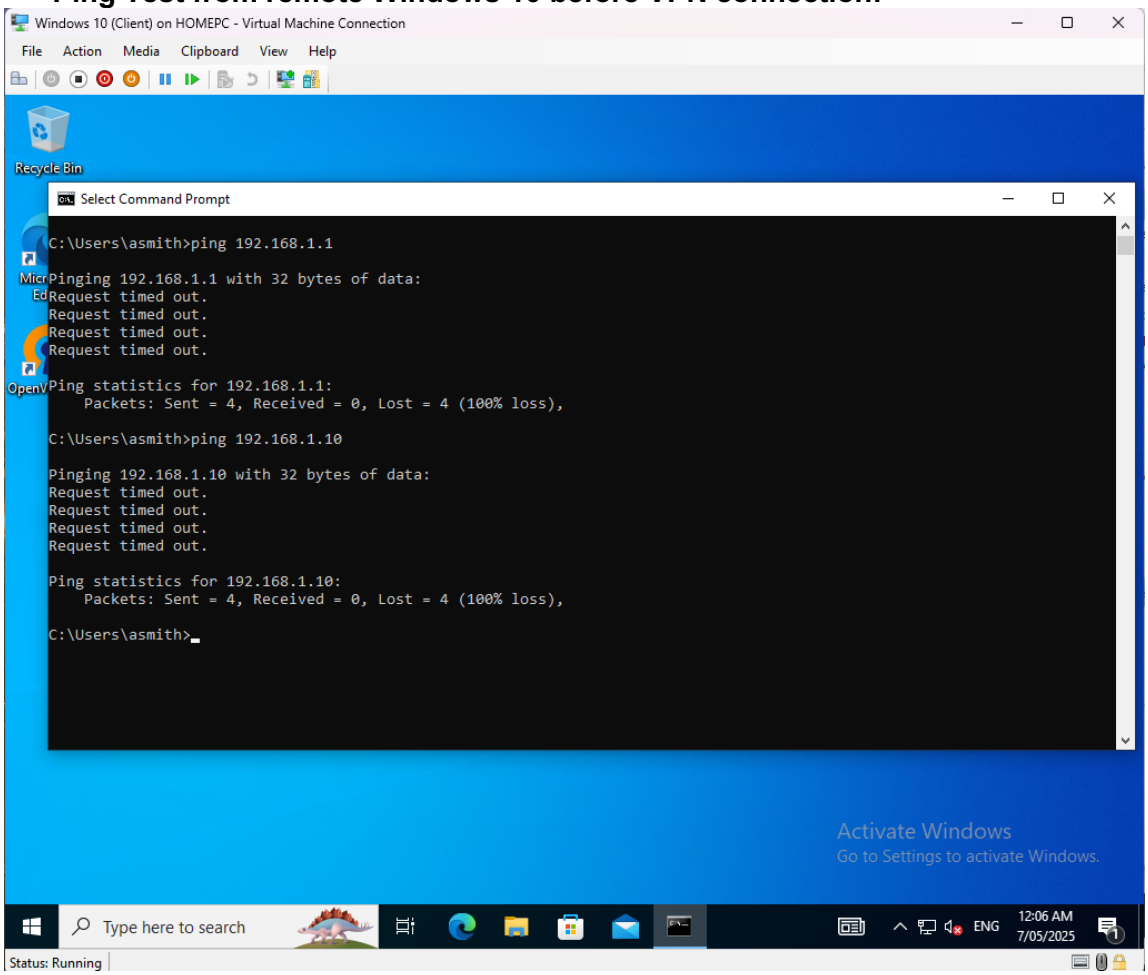


Tests done before connecting to VPN

- **IP Config of remote Windows 10 before connecting to VPN**

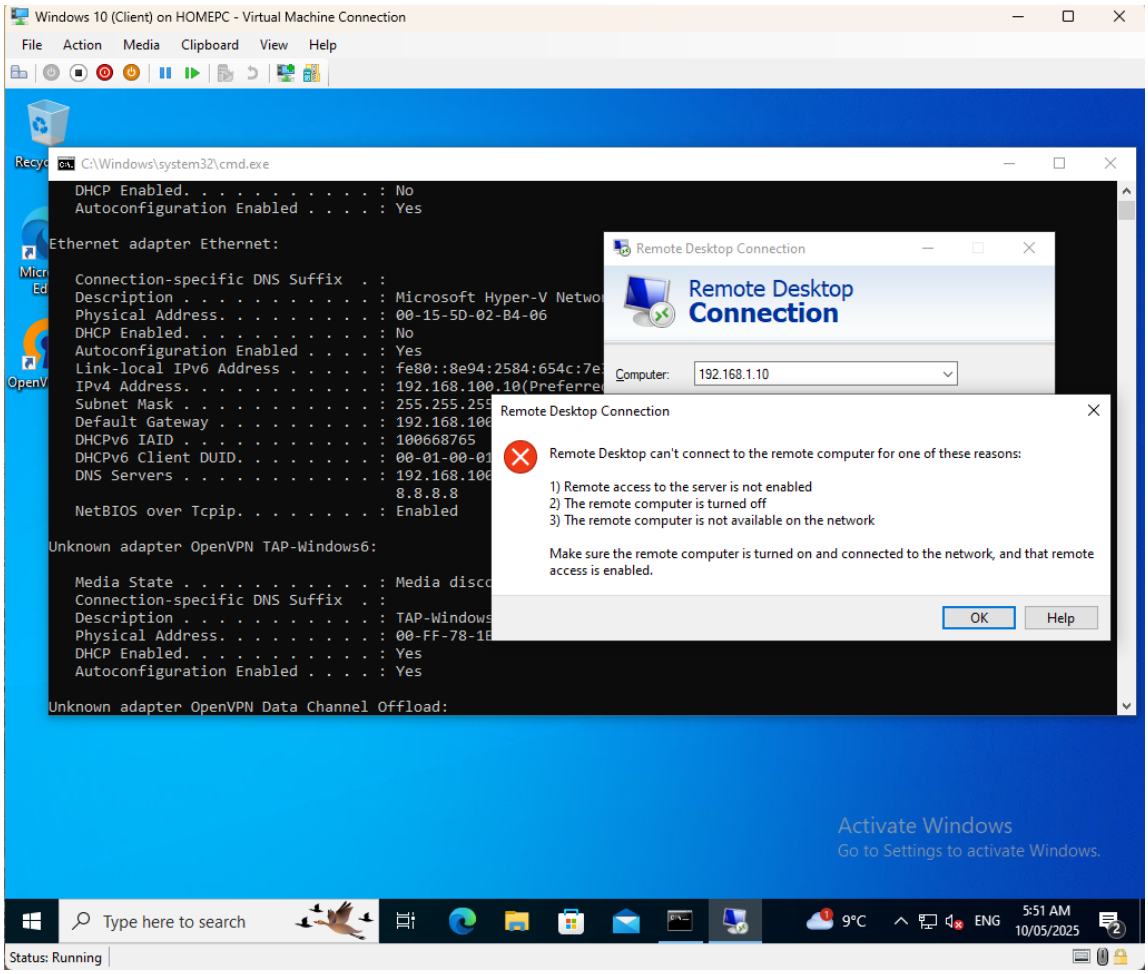


- **Ping Test from remote Windows 10 before VPN connection:**



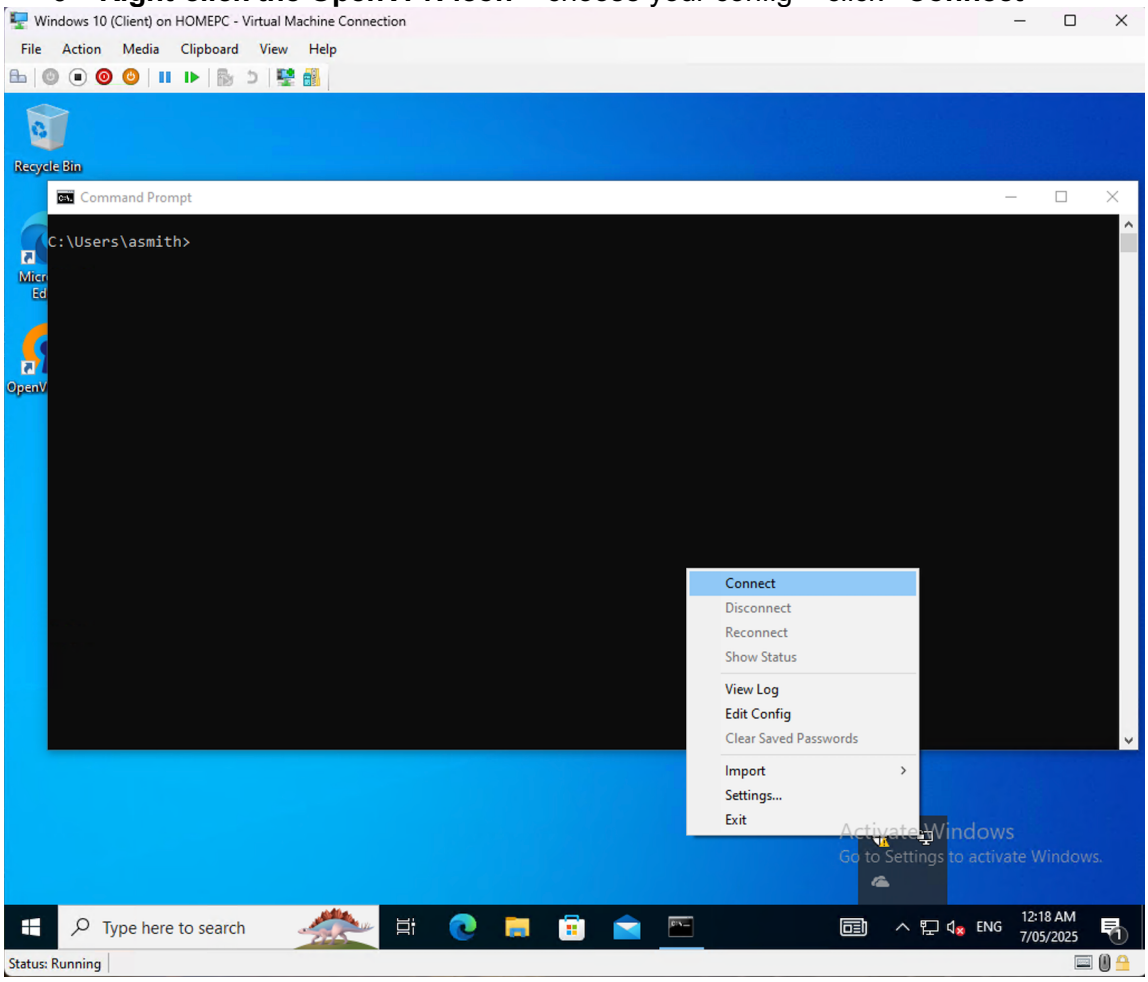
- **RDP access via mstsc to Windows Server before VPN connection:**
  - Press Win + R to open the **Run** dialog.
    mstsc
    and hit **Enter**.
  - You'll see the **Remote Desktop Connection** window.
  - In the **Computer** field, enter the **IP address** or **hostname** of the machine you want to connect to.

  It will not connect to the Windows Server as the Windows 10 is not connected to VPN.

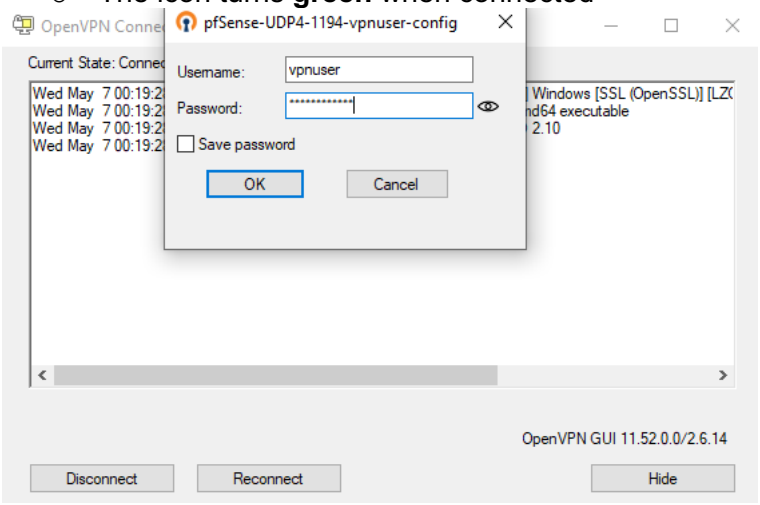


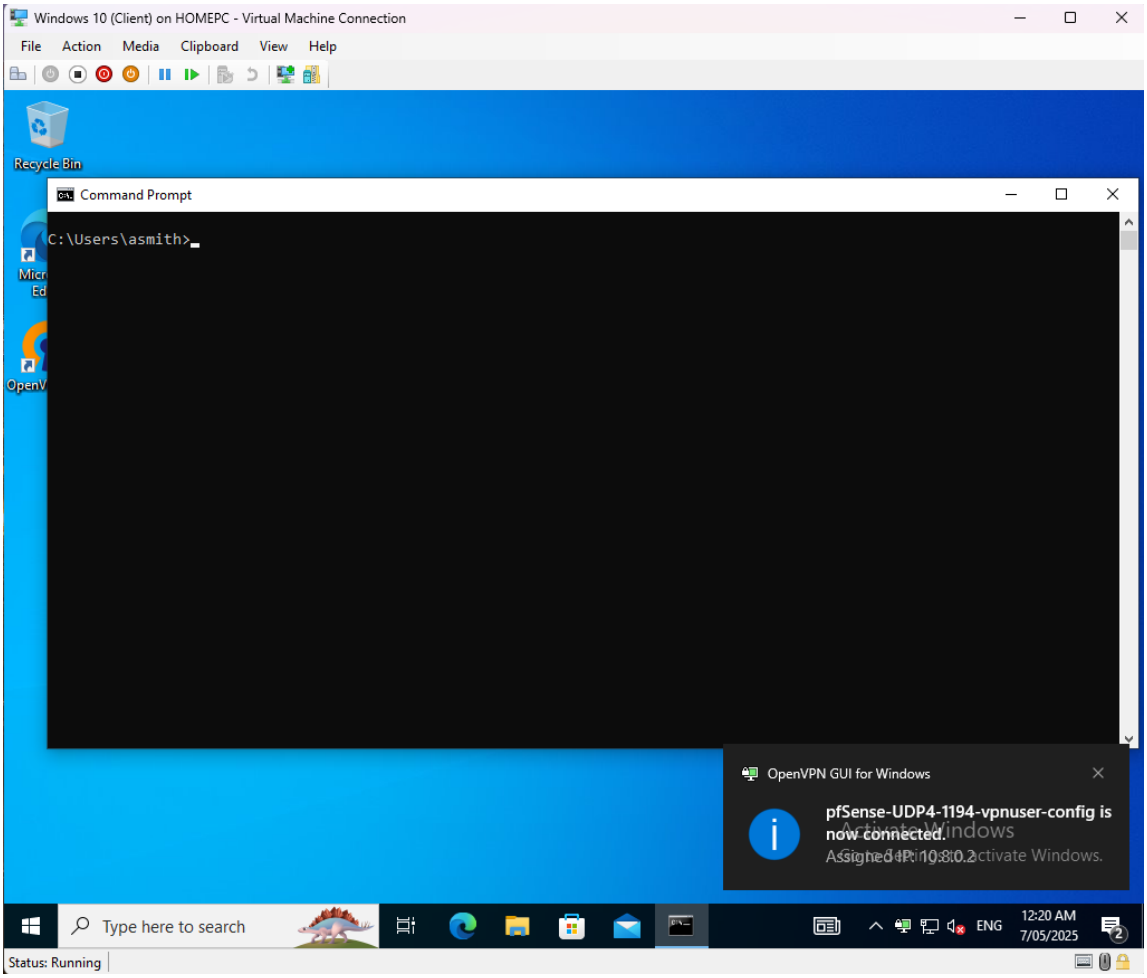
Connect and Test

1. **Connect to the VPN**
   On the **Windows 10 VM**,
   - **Right-click the OpenVPN GUI shortcut** on the desktop.
   - Choose **"Run as administrator"**
     This is necessary so the TAP adapter can be used
   - Look in the **system tray (bottom-right corner)** for the OpenVPN icon (monitor with a lock)
   - If it's hidden, click the **up arrow (^)** to reveal it
   - **Right-click the OpenVPN icon** > choose your config > click **"Connect"**

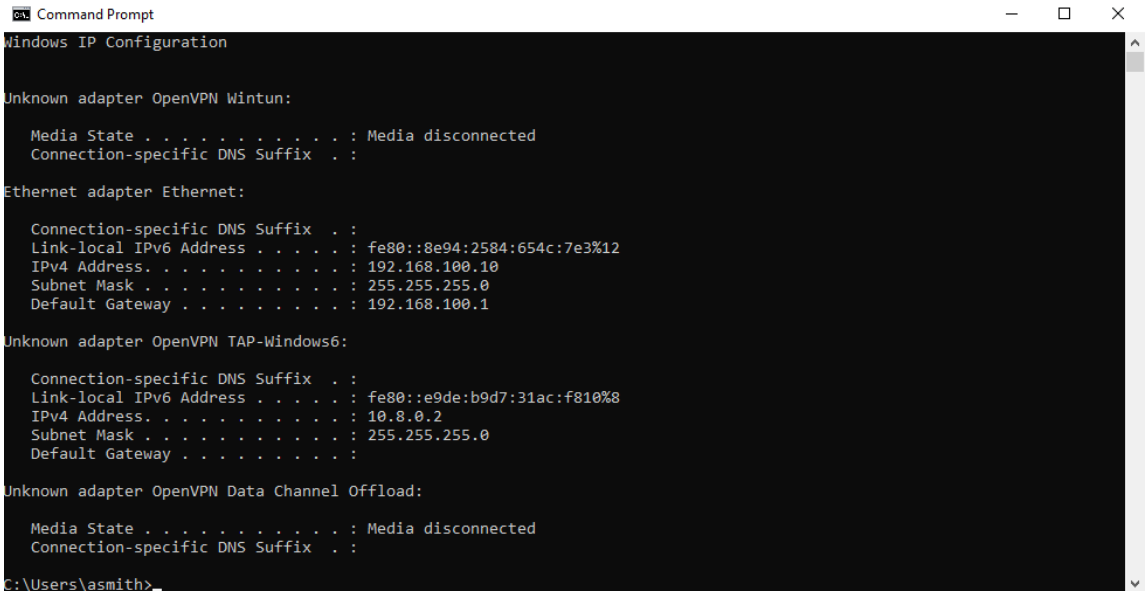


- **If everything is set up properly:**
  - You'll see a **log window** showing connection progress
  - Login using the user credentials created in pfsense for vpn user.
  - The icon turns **green** when connected

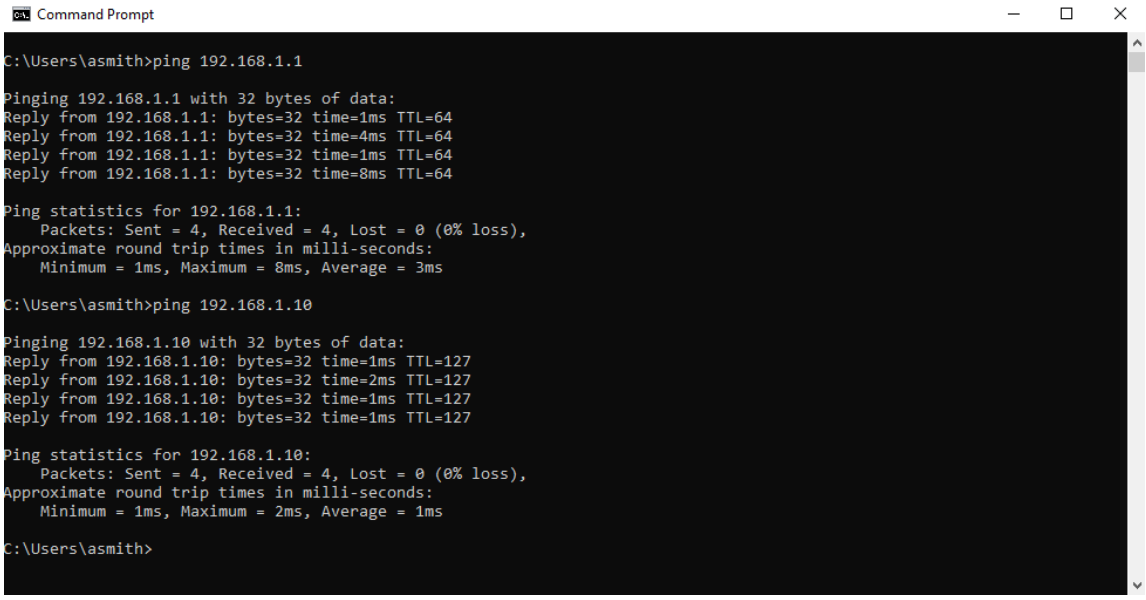




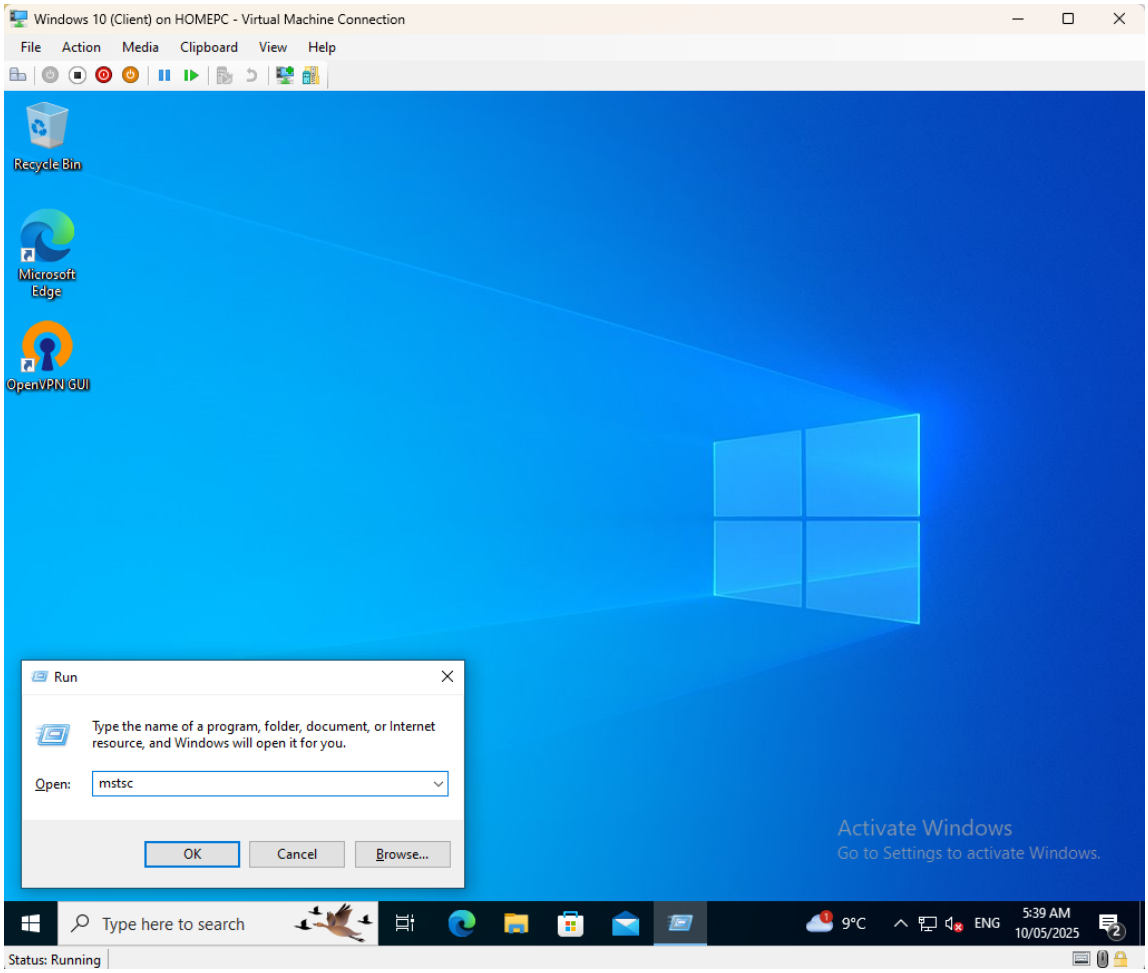
- **IP Config of Windows 10 post connection to VPN:**



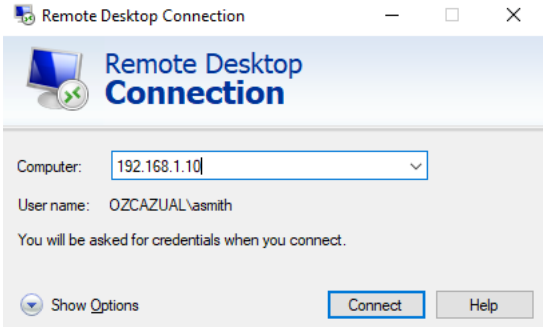
- **Testing Connection to pfSense and Windows Server from Windows 10:**
  ping 192.168.1.1 (pfSense)
  ping 192.168.1.10 (Windows Server)

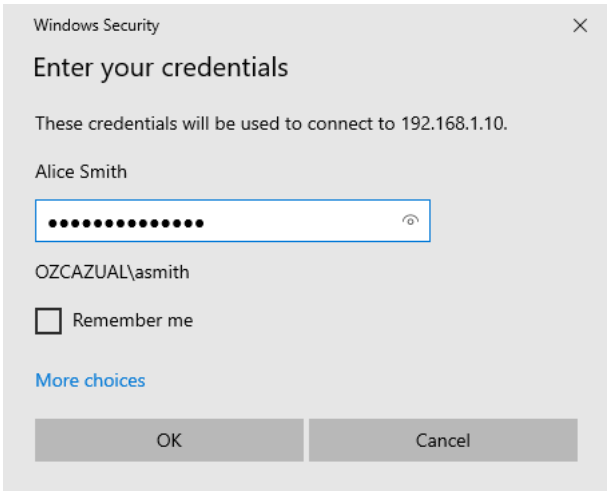


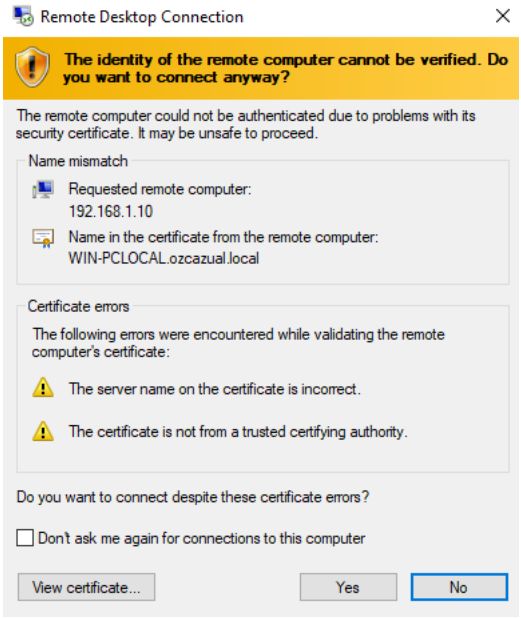
- **RDP via mstsc:**
  - Press Win + R to open the **Run** dialog.
    mstsc
  - and hit **Enter**.



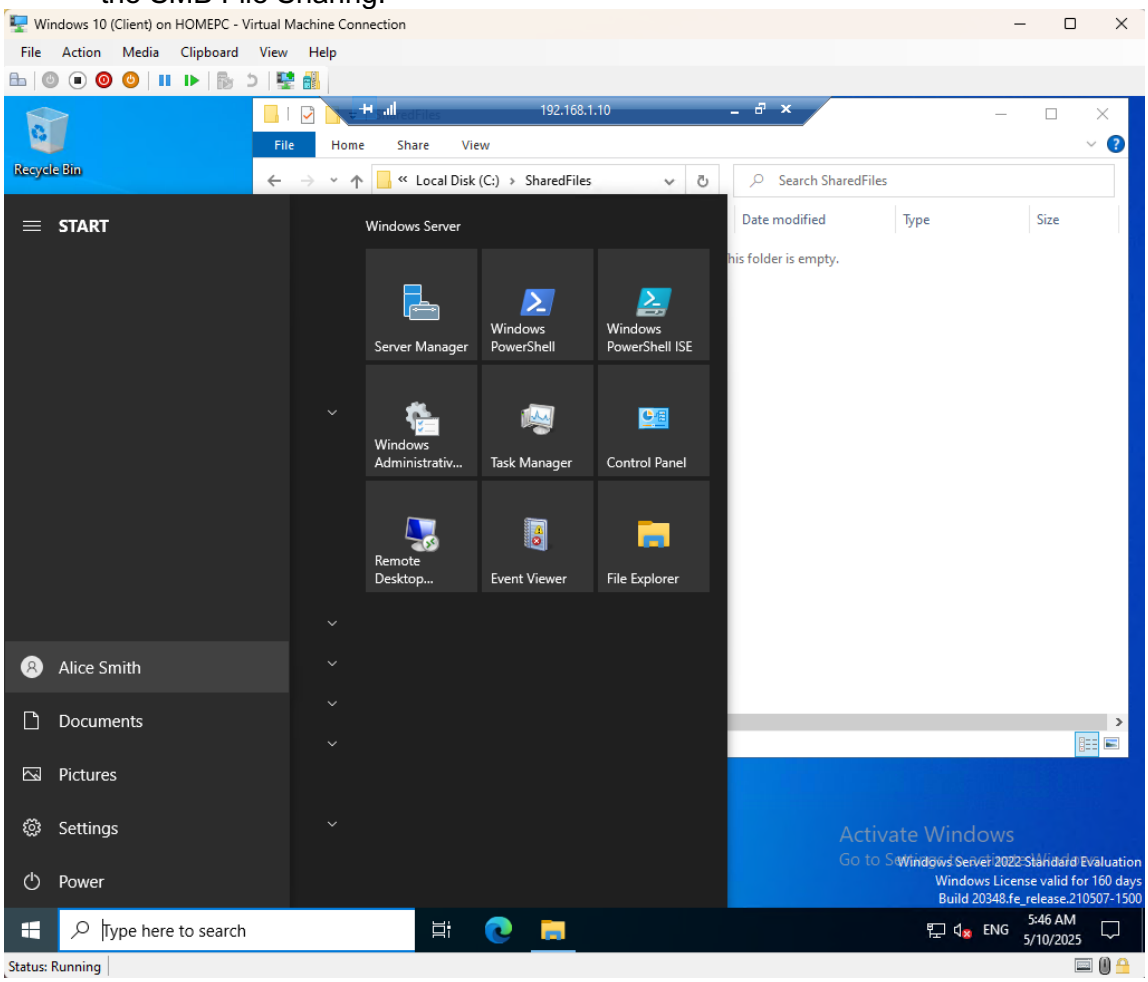
  - You'll see the **Remote Desktop Connection** window.
  - In the **Computer** field, enter the **IP address** or **hostname** of the machine you want to connect to.
  - Click **Connect**, and enter login credentials when prompted.




Windows Security
Enter your credentials
These credentials will be used to connect to 192.168.1.10.
Alice Smith
OZCAZUAL\asmith
Remember me
More choices
OK
Cancel


Remote Desktop Connection
The identity of the remote computer cannot be verified. Do you want to connect anyway?
The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed.
Name mismatch
Requested remote computer:
192.168.1.10
Name in the certificate from the remote computer:
WIN-PCLOCAL.ozcazual.local
Certificate errors
The following errors were encountered while validating the remote computer's certificate:
The server name on the certificate is incorrect.
The certificate is not from a trusted certifying authority.
Do you want to connect despite these certificate errors?
Don't ask me again for connections to this computer
View certificate...
Yes
No

- Logged in as remote employee into the Windows Server and can access the SMB File Sharing:



OpenVPN logs:

To view Logs,

Right-click on the taskbar OpenVPN tray image > View logs