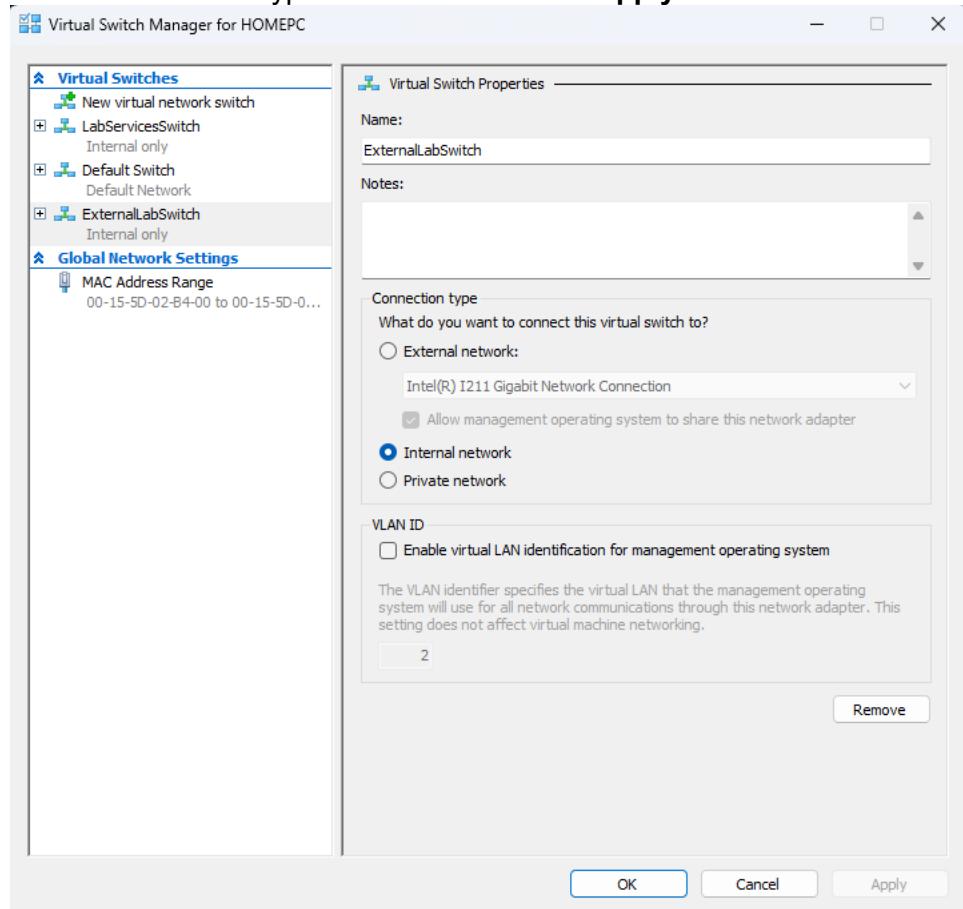


Installation and Configuration of VPN (OpenVPN) on pfSense and Testing by connecting remote Windows 10 to internal network

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 -IPAddress <new_net_IP> -PrefixLength 24 -  
InterfaceAlias "vEthernet ([newExternalSwitch])"
```

```
Administrator: Windows PowerShell  
PS C:\WINDOWS\system32> New-NetIPAddress -IPAddress 192.168.100.1 -PrefixLength 24 -InterfaceAlias "vEthernet (ExternalLabSwitch)"  
  
IPAddress : 192.168.100.1  
InterfaceIndex : 69  
InterfaceAlias : vEthernet (ExternalLabSwitch)  
AddressFamily : IPv4  
Type : Unicast  
PrefixLength : 24  
PrefixOrigin : Manual  
SuffixOrigin : Manual  
AddressState : Tentative  
ValidLifetime :  
PreferredLifetime :  
SkipAsSource : False  
PolicyStore : ActiveStore  
  
IPAddress : 192.168.100.1  
InterfaceIndex : 69  
InterfaceAlias : vEthernet (ExternalLabSwitch)  
AddressFamily : IPv4  
Type : Unicast  
PrefixLength : 24  
PrefixOrigin : Manual  
SuffixOrigin : Manual  
AddressState : Invalid  
ValidLifetime :  
PreferredLifetime :  
SkipAsSource : False  
PolicyStore : PersistentStore  
  
PS C:\WINDOWS\system32>
```

3. Create a NAT network using this IP range:

PowerShell (as administrator):

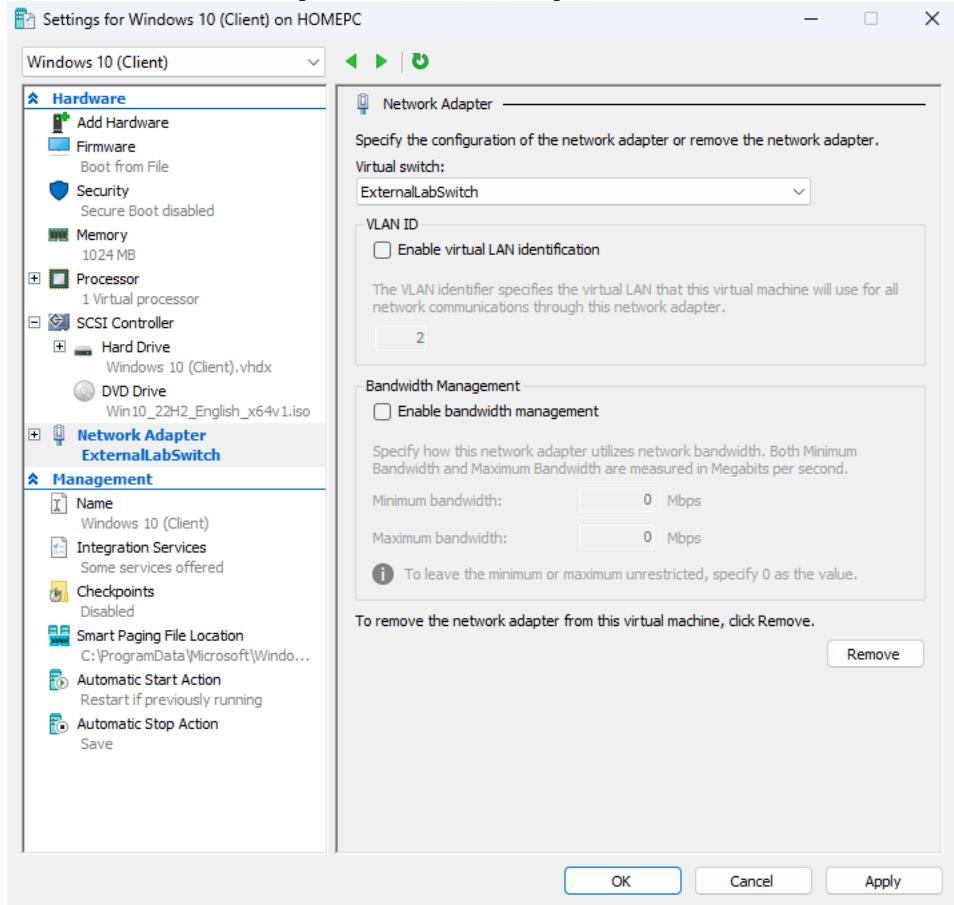
```
New-NetNat -Name "[newNetNat]" -  
InternalIPInterfaceAddressPrefix <ip_range>/24
```

```
Administrator: Windows PowerShell  
PS C:\WINDOWS\system32> New-NetNat -Name "ExternalLabNAT" -InternalIPInterfaceAddressPrefix 192.168.100.0/24  
  
Name : ExternalLabNAT  
ExternalIPInterfaceAddressPrefix :  
InternalIPInterfaceAddressPrefix : 192.168.100.0/24  
IcmpQueryTimeout : 30  
TcpEstablishedConnectionTimeout : 1800  
TcpTransientConnectionTimeout : 120  
TcpFilteringBehavior : AddressDependentFiltering  
UdpFilteringBehavior : AddressDependentFiltering  
UdpIdleSessionTimeout : 120  
UdpInboundRefresh : False  
Store : Local  
Active : True  
  
PS C:\WINDOWS\system32>
```

4. Shutdown pfSense VM.

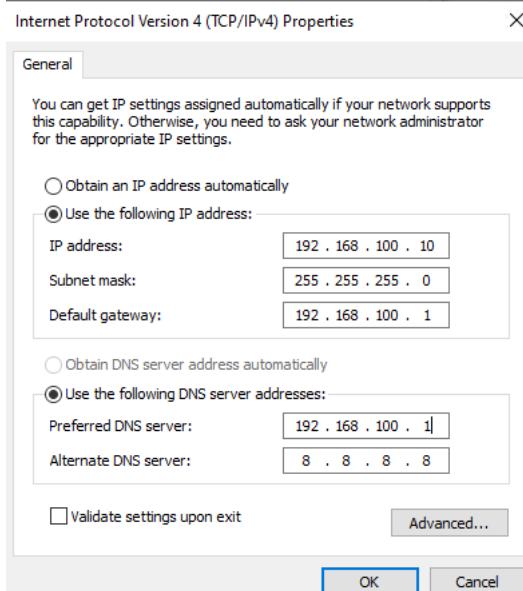
5. Change the network adapter settings of Windows 10 VM:

- 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



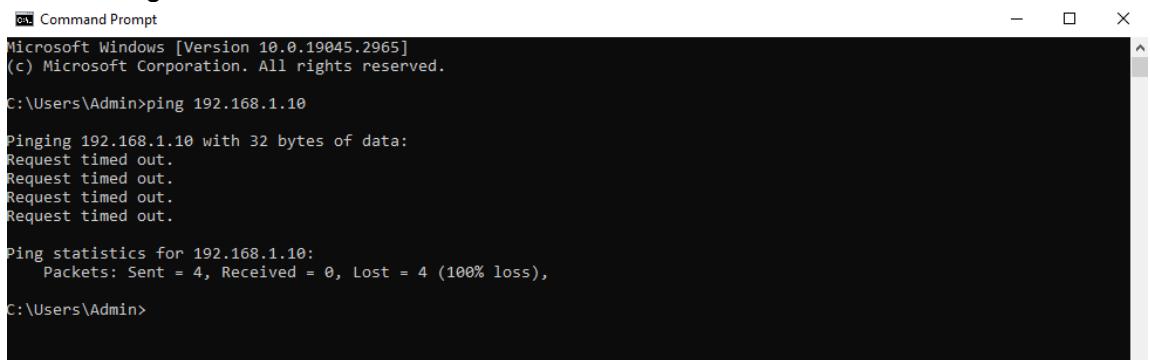
7. Test Connectivity to internet:

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

```
C:\> ping 8.8.8.8  
Pinging 8.8.8.8 with 32 bytes of data:  
Reply from 8.8.8.8: bytes=32 time=3ms TTL=117  
Reply from 8.8.8.8: bytes=32 time=4ms TTL=117  
Reply from 8.8.8.8: bytes=32 time=4ms TTL=117  
Reply from 8.8.8.8: bytes=32 time=3ms TTL=117  
  
Ping statistics for 8.8.8.8:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 3ms, Maximum = 4ms, Average = 3ms  
  
C:\> ping google.com  
Pinging google.com [142.250.70.238] with 32 bytes of data:  
Reply from 142.250.70.238: bytes=32 time=5ms TTL=59  
Reply from 142.250.70.238: bytes=32 time=3ms TTL=59  
Reply from 142.250.70.238: bytes=32 time=3ms TTL=59  
Reply from 142.250.70.238: bytes=32 time=3ms TTL=59  
  
Ping statistics for 142.250.70.238:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 3ms, Maximum = 5ms, Average = 3ms
```

- **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.



```
Command Prompt
Microsoft Windows [Version 10.0.19045.2965]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin>ping 192.168.1.10

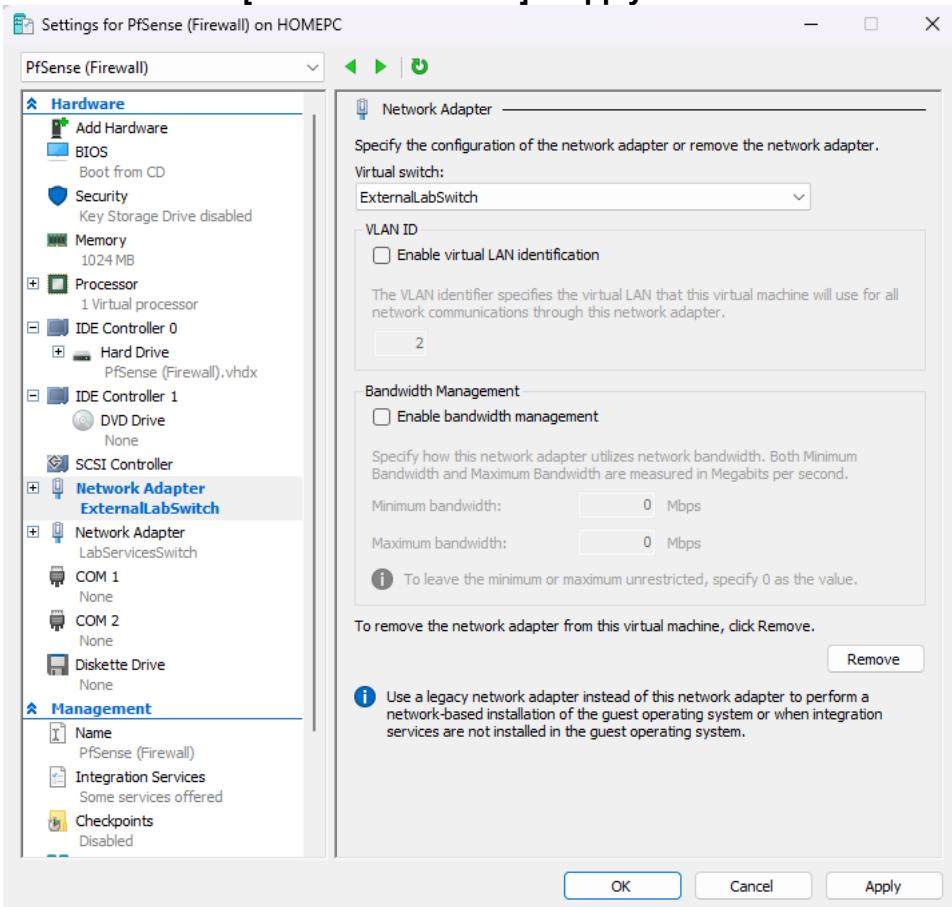
Pinging 192.168.1.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\Admin>
```

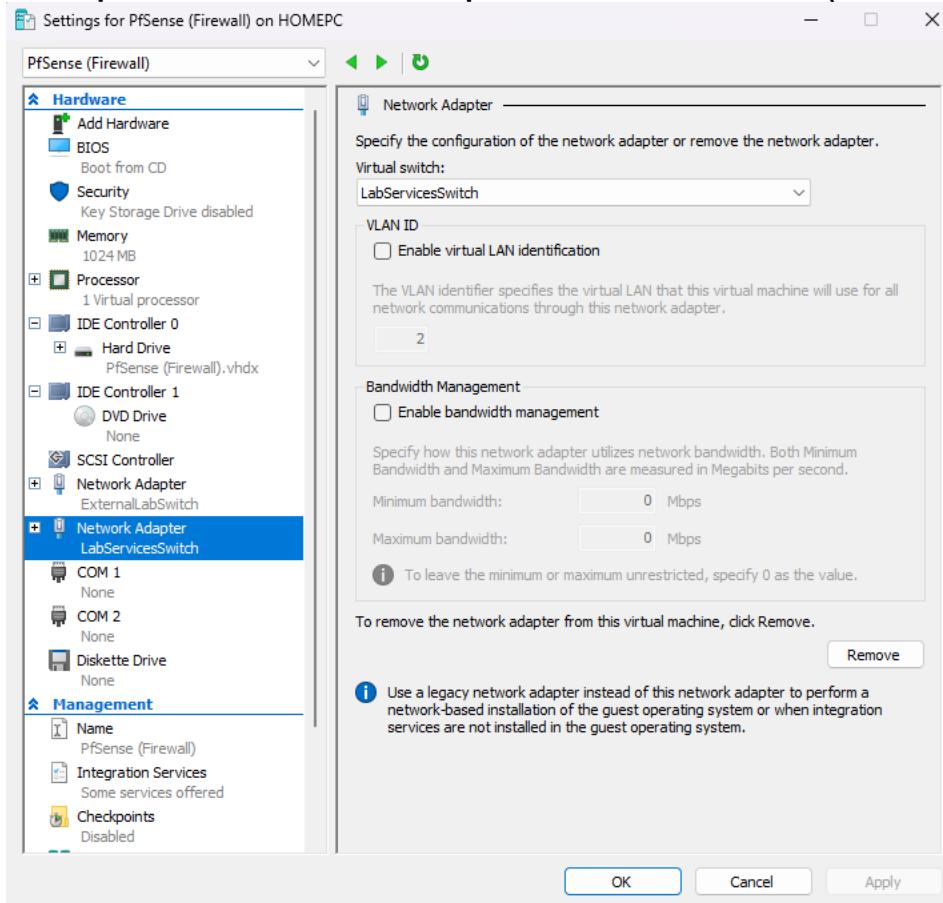
8. Change the pfSense Network adapter Settings:

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

The screenshot shows a terminal window titled "PFSense (Firewall) on HOMEPC - Virtual Machine Connection". The window includes a toolbar with icons for file operations and system status. The terminal output displays ping statistics, Microsoft Azure device information, and a welcome message for pfSense 2.7.2-RELEASE. It then lists network interfaces (WAN and LAN) and a menu of 16 options ranging from Logout to Shell. The status bar at the bottom indicates "Status: Running".

```
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 3.398/3.597/3.745/0.146 ms

Press ENTER to continue.

Microsoft Azure - Netgate Device ID: 835a77bfddd69d018f17

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> hn0      -> v4: 192.168.100.2/24
LAN (lan)      -> hn1      -> v4: 192.168.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces           10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system               14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM

Enter an option: [ ]
```

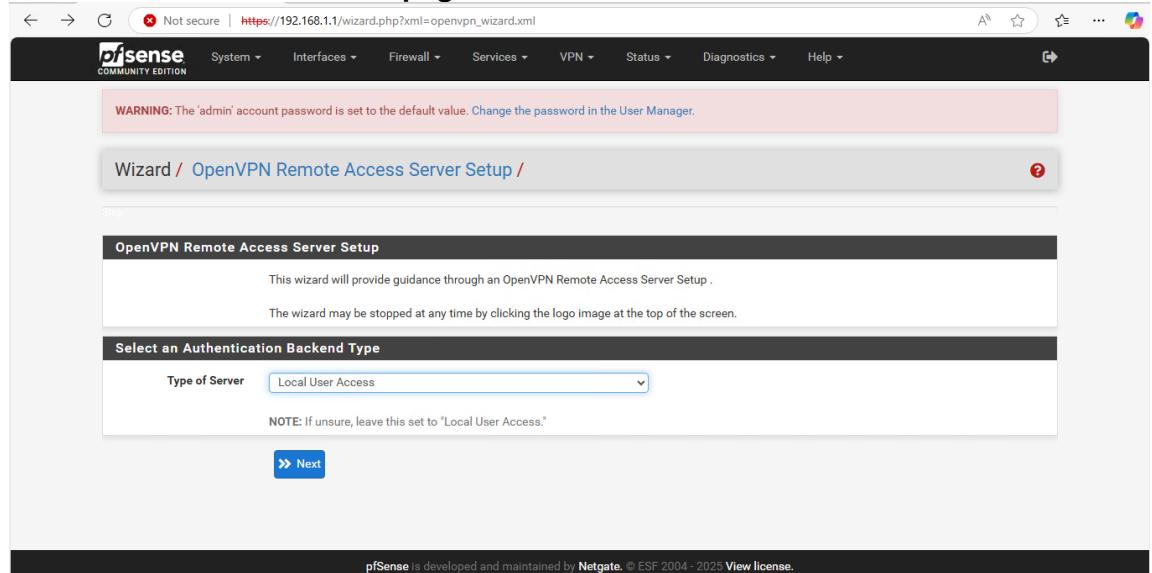
Setup VPN on pfSense (OpenVPN Server)

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**

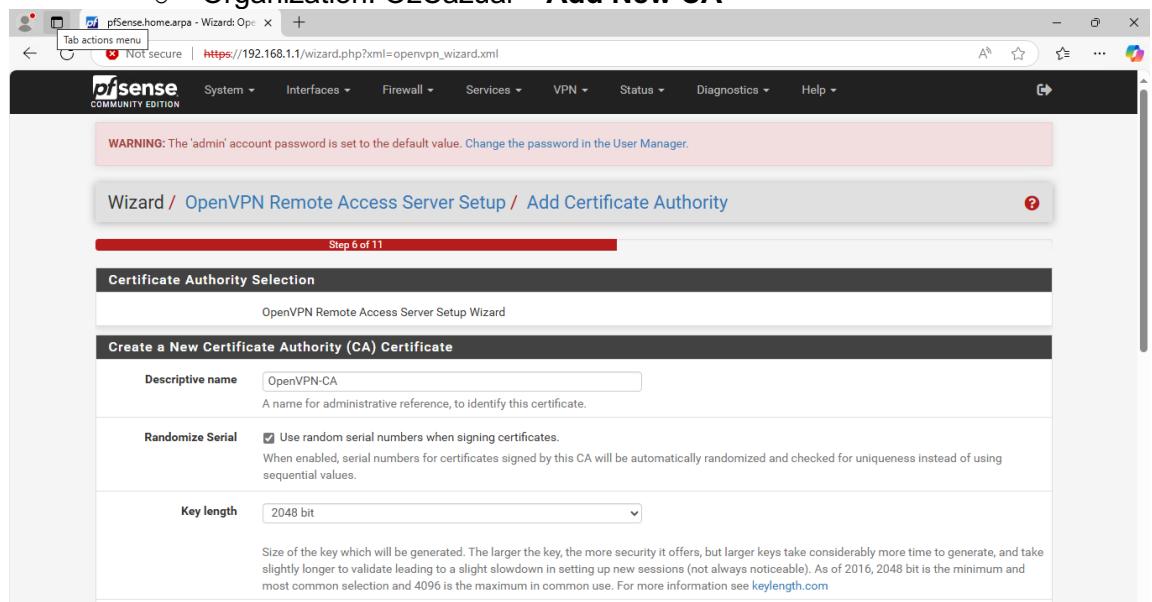


The screenshot shows the 'OpenVPN Remote Access Server Setup' wizard page. At the top, there is a warning message: 'WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.' Below this, the title is 'Wizard / OpenVPN Remote Access Server Setup /'. The main content area is titled 'OpenVPN Remote Access Server Setup' and contains the following text: 'This wizard will provide guidance through an OpenVPN Remote Access Server Setup.' and 'The wizard may be stopped at any time by clicking the logo image at the top of the screen.' A dropdown menu labeled 'Type of Server' is set to 'Local User Access'. A note below it says: 'NOTE: If unsure, leave this set to "Local User Access."'. At the bottom right of the content area is a blue '» Next' button. The footer of the browser window displays the pfSense logo and copyright information: 'pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 View license.'

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**



The screenshot shows the 'Add Certificate Authority' step of the wizard. The title is 'Wizard / OpenVPN Remote Access Server Setup / Add Certificate Authority'. It indicates 'Step 5 of 11'. The main content area is titled 'Certificate Authority Selection' and shows the 'OpenVPN Remote Access Server Setup Wizard'. Below this, there is a section titled 'Create a New Certificate Authority (CA) Certificate' with the following fields:

- Descriptive name:** OpenVPN-CA (A name for administrative reference, to identify this certificate.)
- Randomize Serial:** Use random serial numbers when signing certificates. (When enabled, serial numbers for certificates signed by this CA will be automatically randomized and checked for uniqueness instead of using sequential values.)
- Key length:** 2048 bit (Size of the key which will be generated. The larger the key, the more security it offers, but larger keys take considerably more time to generate, and take slightly longer to validate leading to a slight slowdown in setting up new sessions (not always noticeable). As of 2016, 2048 bit is the minimum and most common selection and 4096 is the maximum in common use. For more information see [keylength.com](#))

pfSense.home.apa - Wizard: OpenVPN Remote Access Server Setup

Not secure | https://192.168.1.1/wizard.php?xml=openvpn_wizard.xml

most common selection and 4096 is the maximum in common use. For more information see [keylength.com](#)

Lifetime	3650
Lifetime in days. This is commonly set to 3650 (Approximately 10 years.)	
Common Name	
The internal name of the CA, used as a part of the CA subject. If left blank, the descriptive name will be used instead.	
Country Code	AU
Two-letter ISO country code (e.g. US, AU, CA)	
State or Province	Victoria
Full State or Province name, not abbreviated (e.g. Texas, Indiana, Ontario).	
City	Melbourne
City or other Locality name (e.g. Austin, Indianapolis, Toronto).	
Organization	OzCasual
Organization name, often the company or group name.	
Organizational Unit	
Organizational Unit name, often a department or team name.	

» Add new CA

pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 [View license](#).

4. Create Server Certificate

Now generate a certificate that the VPN server will use:

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

Click to go back, hold to see history | https://192.168.1.1/wizard.php?xml=openvpn_wizard.xml

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Wizard / OpenVPN Remote Access Server Setup / Add a Server Certificate

Step 8 of 11

Add a Server Certificate

OpenVPN Remote Access Server Setup Wizard

Create a New Server Certificate

Descriptive name	OpenVPN-Server
A name for administrative reference, to identify this certificate.	
Key length	2048 bit
Size of the key which will be generated. The larger the key, the more security it offers, but larger keys take considerably more time to generate, and take slightly longer to validate leading to a slight slowdown in setting up new sessions (not always noticeable). As of 2016, 2048 bit is the minimum and most common selection and 4096 is the maximum in common use. For more information see keylength.com	
Lifetime	398
Lifetime in days. Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate invalid.	
Common Name	

5. Configure OpenVPN Server

- **Protocol:** UDP on IPv4 only
- **Interface:** WAN
- **Local port:** 1194

The screenshot shows the "Server Setup" step of the OpenVPN wizard. It includes fields for the server's name ("OpenVPN-Server"), protocol ("UDP on IPv4 only"), interface ("WAN"), and local port ("1194"). The "Cryptographic Settings" section is also visible.

- **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**

The screenshot shows the "Tunnel Settings" step of the wizard. It includes fields for the tunnel network ("10.8.0.0/24"), redirect gateway ("Force all client generated traffic through the tunnel" checked), local network ("192.168.1.0/24"), concurrent connections, allow compression (set to "Refuse any non-stub compression (Most secure)"), compression (set to "Disable Compression [Omit Preference]"), type-of-service (unchecked), and inter-client communication (unchecked).

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**

The screenshot shows the 'Firewall Rule Configuration' step of the OpenVPN Remote Access Server Setup wizard. It is Step 10 of 11. The page title is 'Wizard / OpenVPN Remote Access Server Setup / Firewall Rule Configuration'. The main content area is titled 'Firewall Rule Configuration' and contains the following text:

OpenVPN Remote Access Server Firewall Rules
Rules control passing or blocking network traffic as it flows through the firewall.
Rules must be added which allow traffic to reach the OpenVPN server IP address and port, as well as to allow traffic from connected clients inside the OpenVPN tunnel.
The options on this step can add automatic rules to pass this traffic, or rules can be configured manually after completing the wizard.

Below this, there are two sections: 'Traffic from clients to server' and 'Traffic from clients through VPN'. Under 'Traffic from clients to server', there is a 'Firewall Rule' section with a checkbox 'Add a rule to permit connections to this OpenVPN server instance from clients anywhere on the Internet.' Under 'Traffic from clients through VPN', there is an 'OpenVPN rule' section with a checkbox 'Add a rule to allow all traffic from connected clients to pass inside the VPN tunnel.' At the bottom of the page is a blue 'Next' button.

The screenshot shows the 'Finished!' step of the OpenVPN Remote Access Server Setup wizard. It is Step 11 of 11. The page title is 'Wizard / OpenVPN Remote Access Server Setup / Finished!'. The main content area is titled 'Finished!' and contains the following text:

OpenVPN Remote Access Server Setup Wizard

Configuration Complete!
The configuration is now complete.
Adding users for the VPN depends on the chosen authentication method. For example, add local users with certificates under [System > User Manager](#). For remote authentication servers, add certificates directly in [System > Certificate Manager](#).
To easily export client configurations, browse to [System > Packages](#) and install the OpenVPN Client Export package.

At the bottom of the page is a blue 'Finish' button.

VPN Server listing after creation:

The screenshot shows the pfSense web interface under the 'VPN / OpenVPN / Servers' section. 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.' Below this, a table lists an 'OpenVPN Server' entry:

Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
WAN	UDPA / 1194 (TUN)	10.8.0.0/24	Mode: Remote Access (SSL/TLS + User Auth) Data Ciphers: AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC Digest: SHA256 D-H Params: 2048 bits	OpenVPN-Server	

A green '+' button labeled 'Add' is located in the bottom right corner of the table.

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)

The screenshot shows the pfSense web interface under the 'System / User Manager / Users' section. 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.' Below this, a form titled 'User Properties' is displayed:

Defined by	USER
Disabled	<input type="checkbox"/> This user cannot login
Username	vpnuser
Password	*****
Full name	vpnuser <small>User's full name, for administrative information only</small>
Expiration date	<input type="text"/> <small>Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY</small>
Custom Settings	<input type="checkbox"/> Use individual customized GUI options and dashboard layout for this user.

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

The screenshot shows the 'Create Certificate for User' page in the pfSense User Manager. The 'Descriptive name' field contains 'vpnuser-cert'. The 'Certificate authority' dropdown is set to 'OpenVPN-CA'. The 'Key type' dropdown is set to 'RSA'. The 'Key Length' dropdown is set to '2048'. The 'Digest Algorithm' dropdown is set to 'sha256'. The 'Lifetime' input field contains '3650'.

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

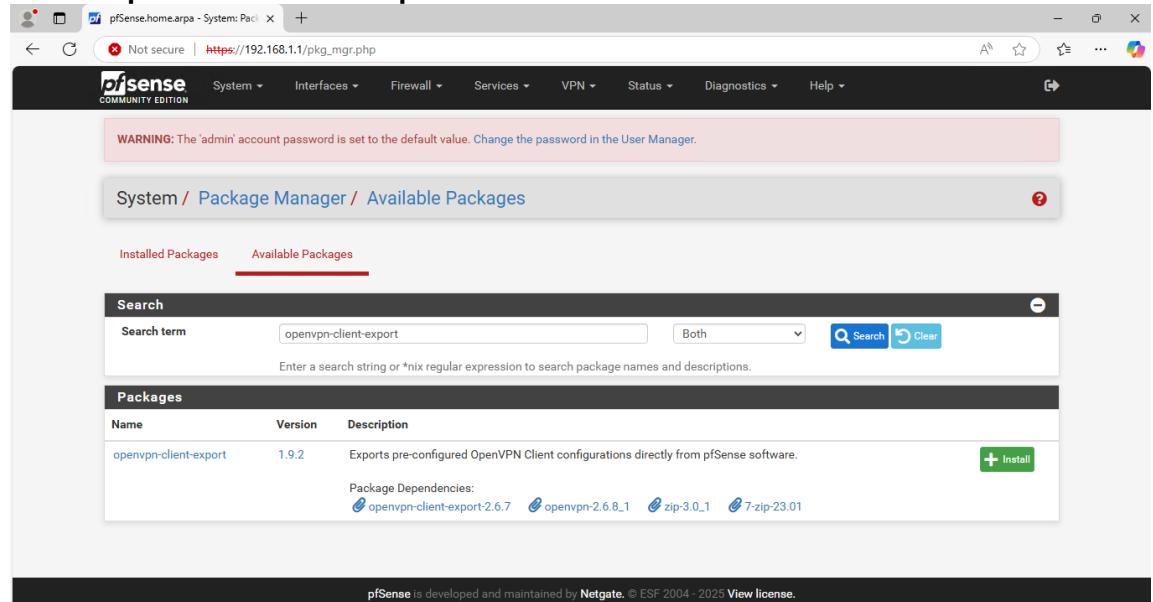
The screenshot shows the 'Users' list page in the pfSense User Manager. There are two entries in the table:

Username	Full name	Status	Groups	Actions
admin	System Administrator	✓	admins	
vpnuser	vpnuser	✓		

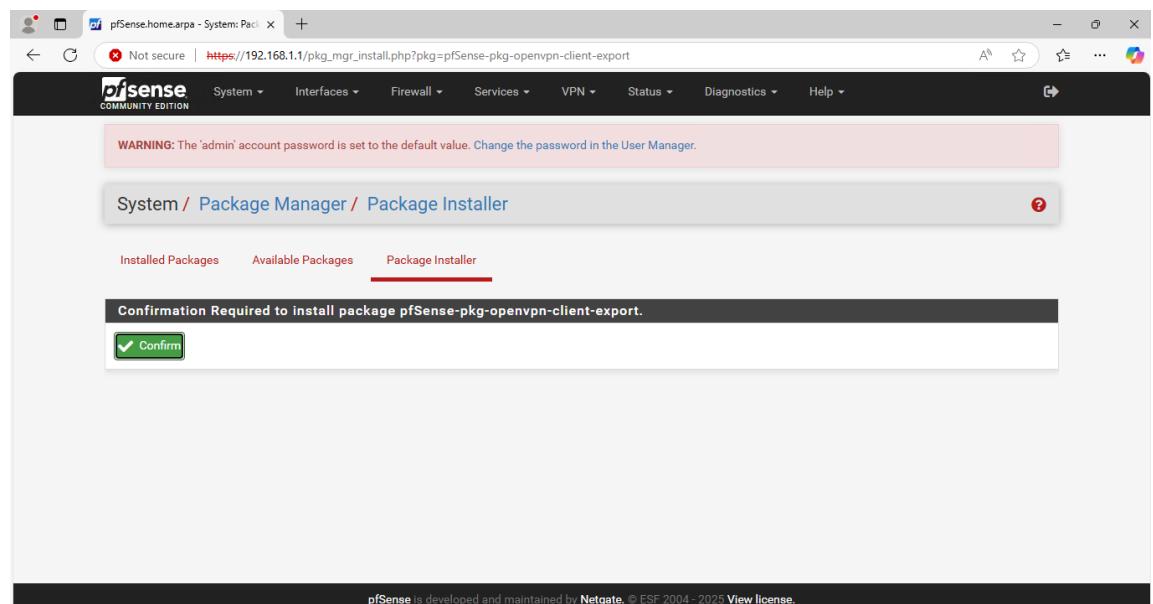
At the bottom of the page, there is a footer note: 'pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 [View license](#)'.

8. Install the Client Export Package

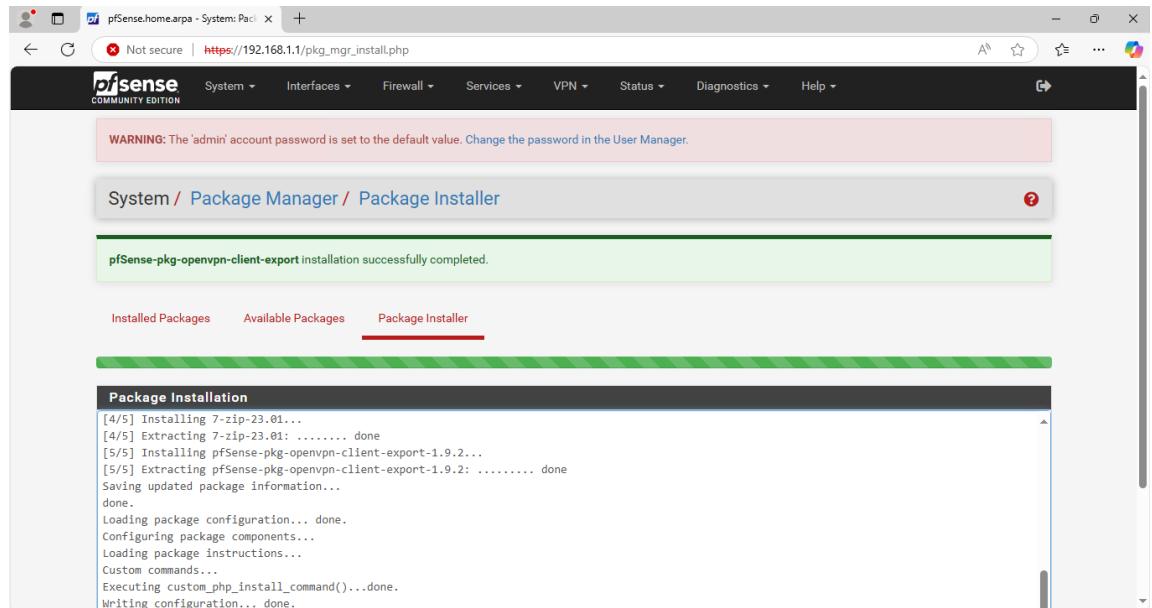
- Go to **System > Package Manager > Available Packages**
- Search for **openvpn-client-export** > **Install**
- Once installed, go to:
VPN > OpenVPN > Client Export



The screenshot shows the pfSense Package Manager interface. The title bar says "pfSense.home.arpa - System: Pac...". The address bar shows "Not secure | https://192.168.1.1/pkg_mgr.php". The menu bar includes System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. A red banner at the top states: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below the banner, the page title is "System / Package Manager / Available Packages". There are two tabs: "Installed Packages" and "Available Packages", with "Available Packages" being active. A search bar at the top has "openvpn-client-export" in the "Search term" field and "Both" in the dropdown. A "Search" button and a "Clear" button are next to it. Below the search bar is a "Packages" table with columns: Name, Version, and Description. One row is shown: "openvpn-client-export" version 1.9.2, which "Exports pre-configured OpenVPN Client configurations directly from pfSense software." To the right of this row is a green "Install" button. Below the table, under "Package Dependencies", are links to "openvpn-client-export-2.6.7", "openvpn-2.6.8_1", "zip-3.0_1", and "7-zip-23.01". At the bottom of the page, a black footer bar says "pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 View license."



The screenshot shows the pfSense Package Manager interface. The title bar says "pfSense.home.arpa - System: Pac...". The address bar shows "Not secure | https://192.168.1.1/pkg_mgr_install.php?pkg=pfSense-pkg-openvpn-client-export". The menu bar includes System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. A red banner at the top states: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below the banner, the page title is "System / Package Manager / Package Installer". There are three tabs: "Installed Packages", "Available Packages", and "Package Installer", with "Package Installer" being active. A black header bar at the top of the main content area says "Confirmation Required to install package pfSense-pkg-openvpn-client-export.". Below this, there is a green "Confirm" button. At the bottom of the page, a black footer bar says "pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 View license."



9. Download VPN Configuration for Windows 10

1. Scroll to **Client Export** section
2. Find the row for vpnuser
3. Download:
 - o **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]).

A screenshot of a web browser window titled "pfSense.home.arpa - OpenVPN: C". The URL is https://192.168.1.1/vpn_openvpn_export.php. The page lists "OpenVPN Clients" with one entry: "User" vpnuser and "Certificate Name" vpnuser-cert. To the right, there is a "Export" section with several download buttons:

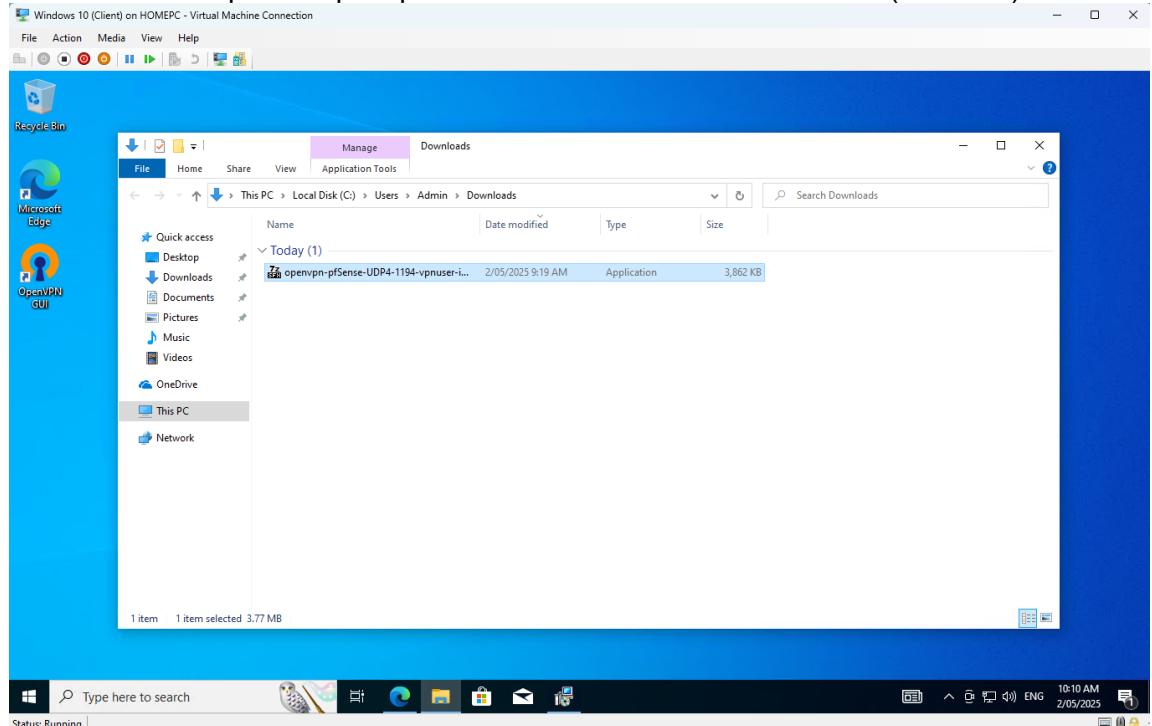
- Inline Configurations:
 - [Download] Most Clients
 - [Download] Android
 - [Download] OpenVPN Connect (iOS/Android)
- Bundled Configurations:
 - [Download] Archive
 - [Download] Config File Only
- Current Windows Installers (2.6.7-ix001):
 - [Download] 64-bit
 - [Download] 32-bit
- Previous Windows Installers (2.5.9-ix601):
 - [Download] 64-bit
 - [Download] 32-bit
- Legacy Windows Installers (2.4.12-ix601):
 - [Download] 10/2016/2019
 - [Download] 7/8/8.1/2012
- Viscosity (Mac OS X and Windows):
 - [Download] Viscosity Bundle
 - [Download] Viscosity Inline Config

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-lxxxx-win10.exe).

OR

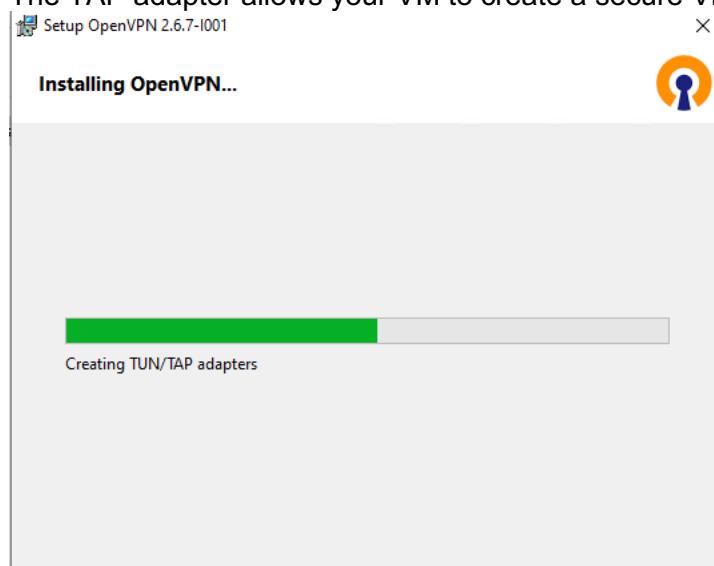
Download the exported openvpn-client file to Windows 10 via cloud (onedrive)

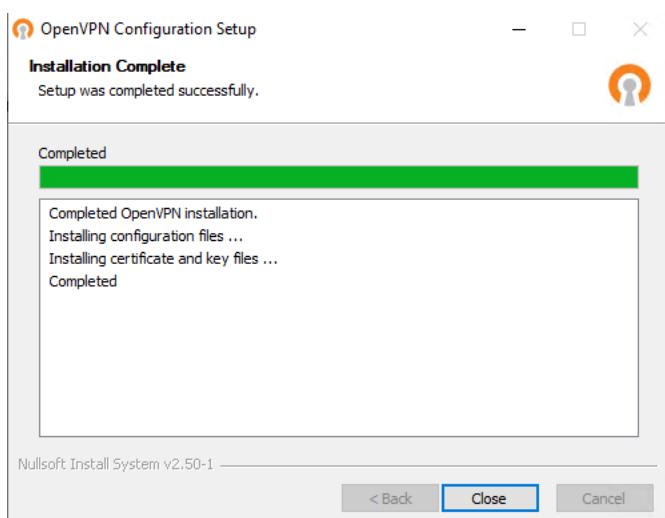
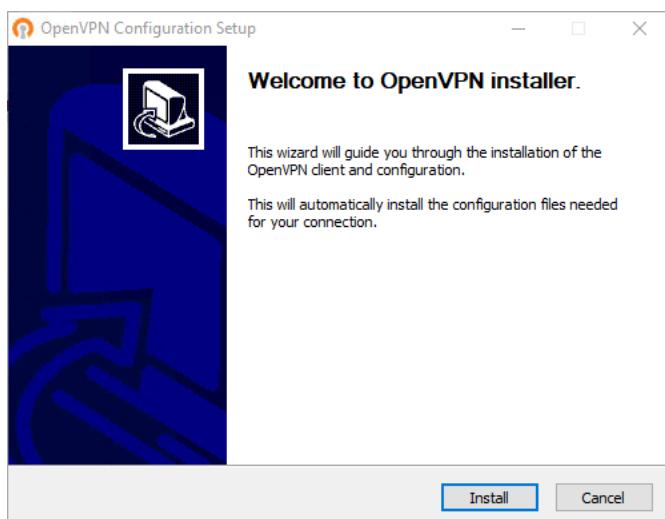
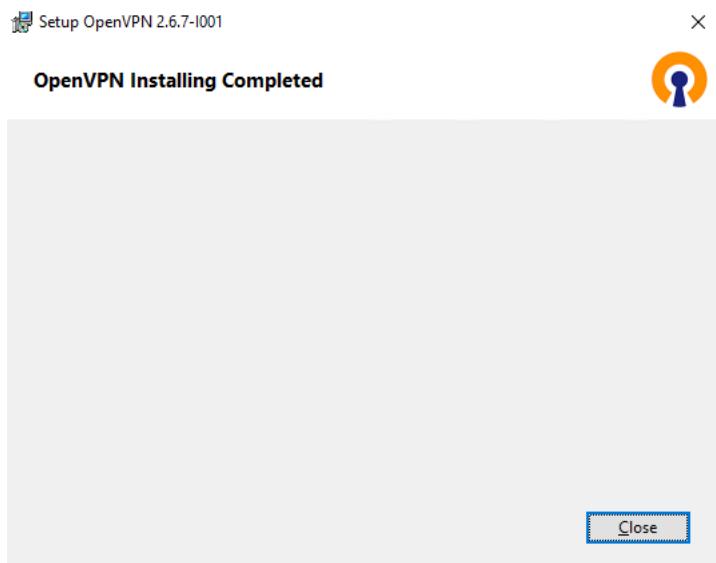


11. Install OpenVPN GUI

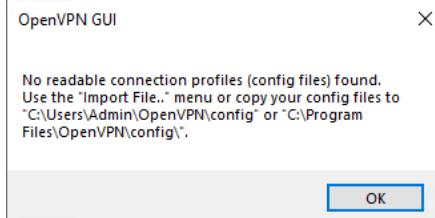
1. Run the installer as administrator.
2. Choose “Next” through the installation wizard and accept all defaults.
3. Allow it to install **OpenVPN GUI** and **TAP drivers** (virtual network adapter).
4. Finish the installation.

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





- 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.

OpenVPN Clients

User	Certificate Name	Export
vpnuser	vpnuser-cert	<ul style="list-style-type: none"> - Inline Configurations: <ul style="list-style-type: none"> Most Clients Android OpenVPN Connect (iOS/Android) - Bundled Configurations: <ul style="list-style-type: none"> Archive Config File Only - Current Windows Installers (2.6.7-1x001): <ul style="list-style-type: none"> 64-bit 32-bit - Previous Windows Installers (2.5.9-1x601): <ul style="list-style-type: none"> 64-bit 32-bit - Legacy Windows Installers (2.4.12-1x601): <ul style="list-style-type: none"> 10/2016/2019 7/8/8.1/2012/2 - Viscosity (Mac OS X and Windows): <ul style="list-style-type: none"> Viscosity Bundle Viscosity Inline Config

Only OpenVPN-compatible user certificates are shown

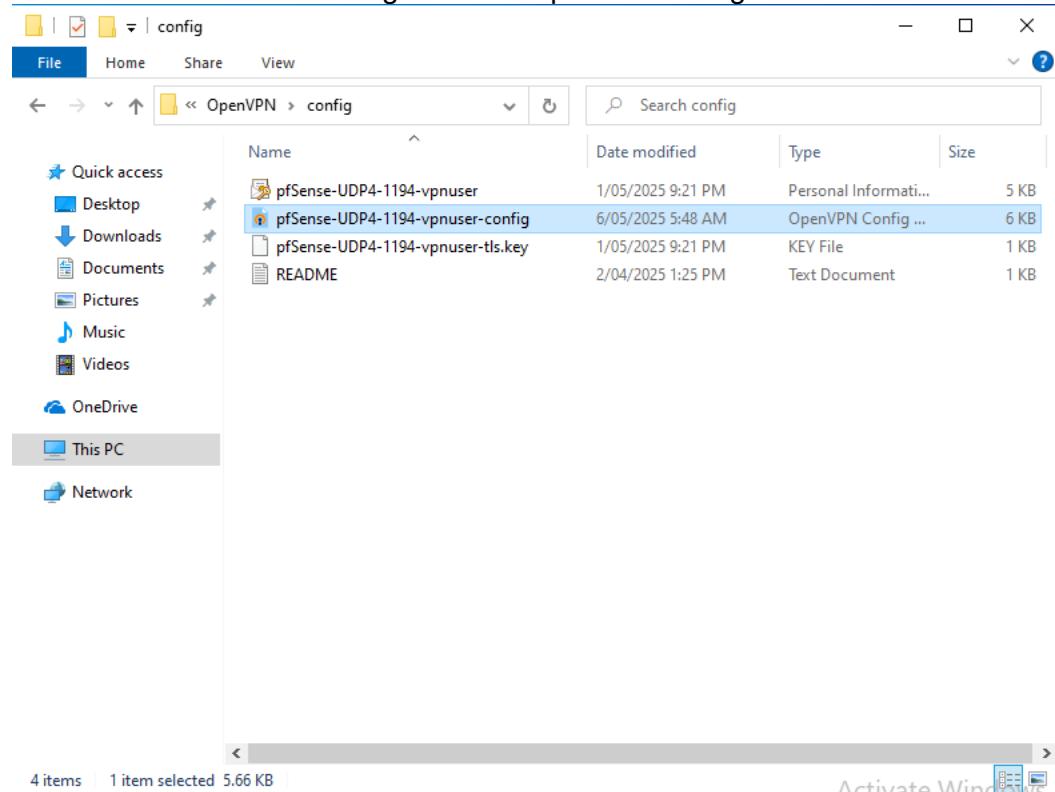
If a client is missing from the list it is likely due to a CA mismatch between the OpenVPN server instance and the client certificate, the client certificate does not exist on this firewall, or a user certificate is not associated with a user when local database authentication is enabled.

Clients using OpenSSL 3.0 may not work with older or weaker ciphers and hashes, such as SHA1, including when those were used to sign CA and certificate entries.

OpenVPN 2.4.8+ requires Windows 7 or later

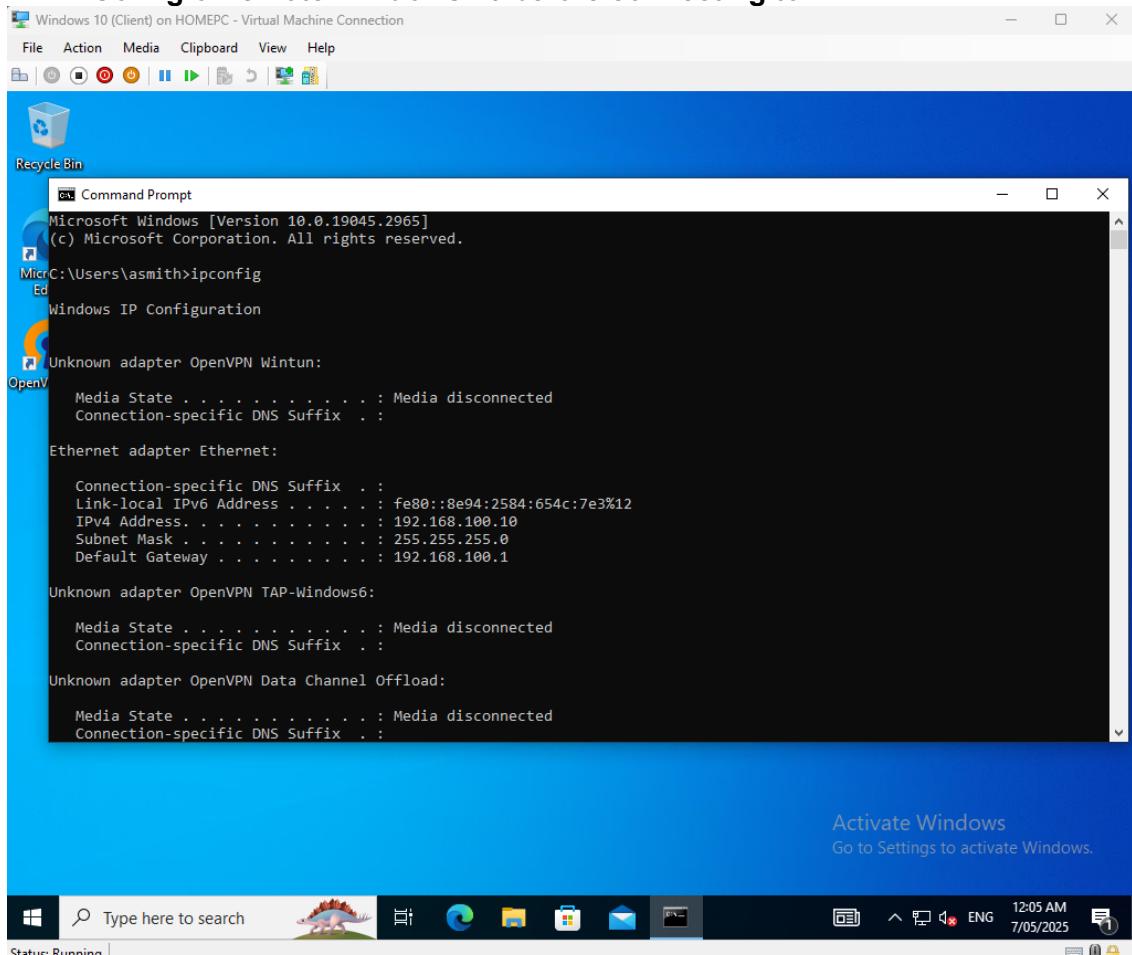
Links to OpenVPN clients for various platforms:

- **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:

The screenshot shows a Windows 10 desktop environment. A Command Prompt window titled "Select Command Prompt" is open, displaying ping test results. The desktop background is blue, and the taskbar at the bottom includes icons for File Explorer, Edge, File Explorer, Mail, and Task View, along with system status indicators like battery level and network connection. A watermark for "Activate Windows Go to Settings to activate Windows." is visible in the center of the screen.

```
C:\Users\asmith>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

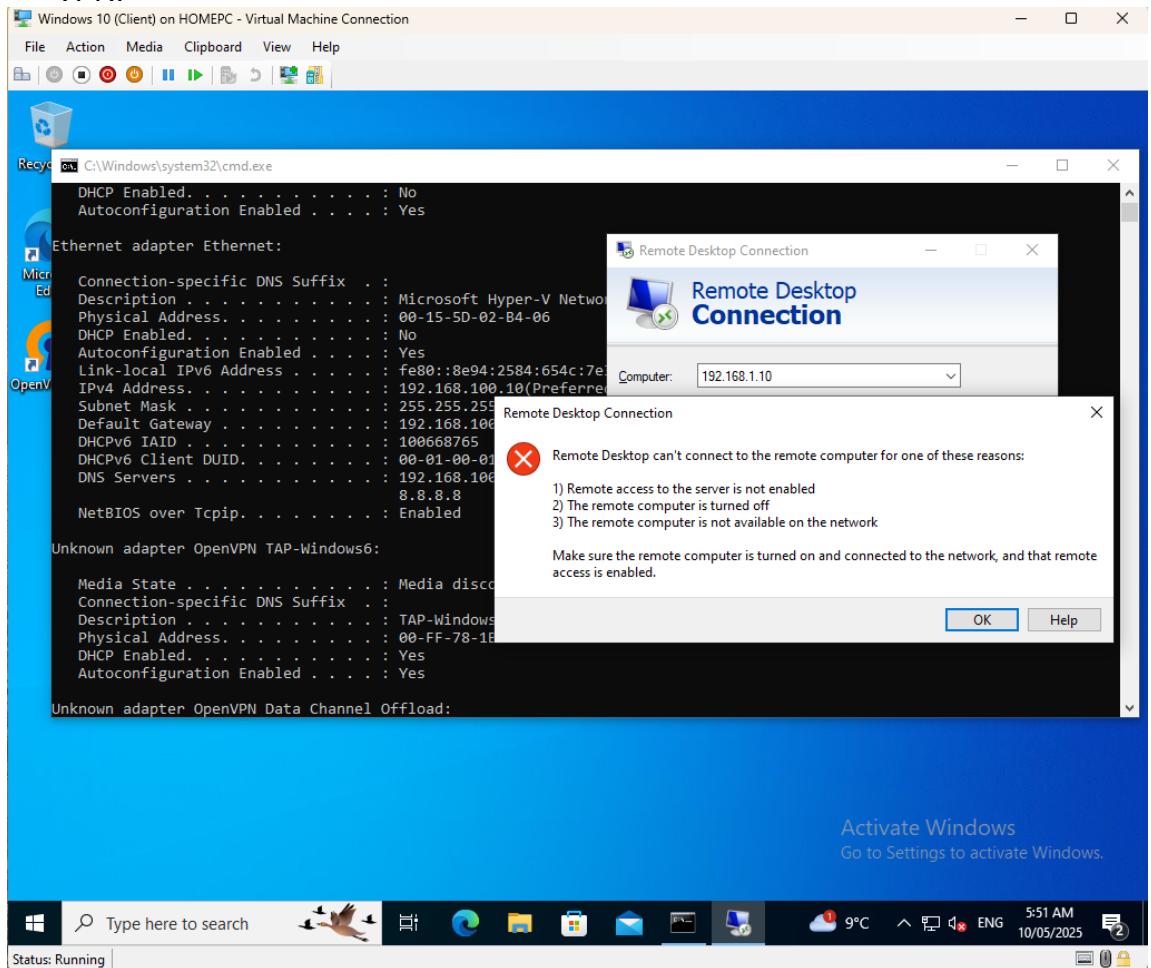
Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\asmith>ping 192.168.1.10
Pinging 192.168.1.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\asmith>
```

- **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.

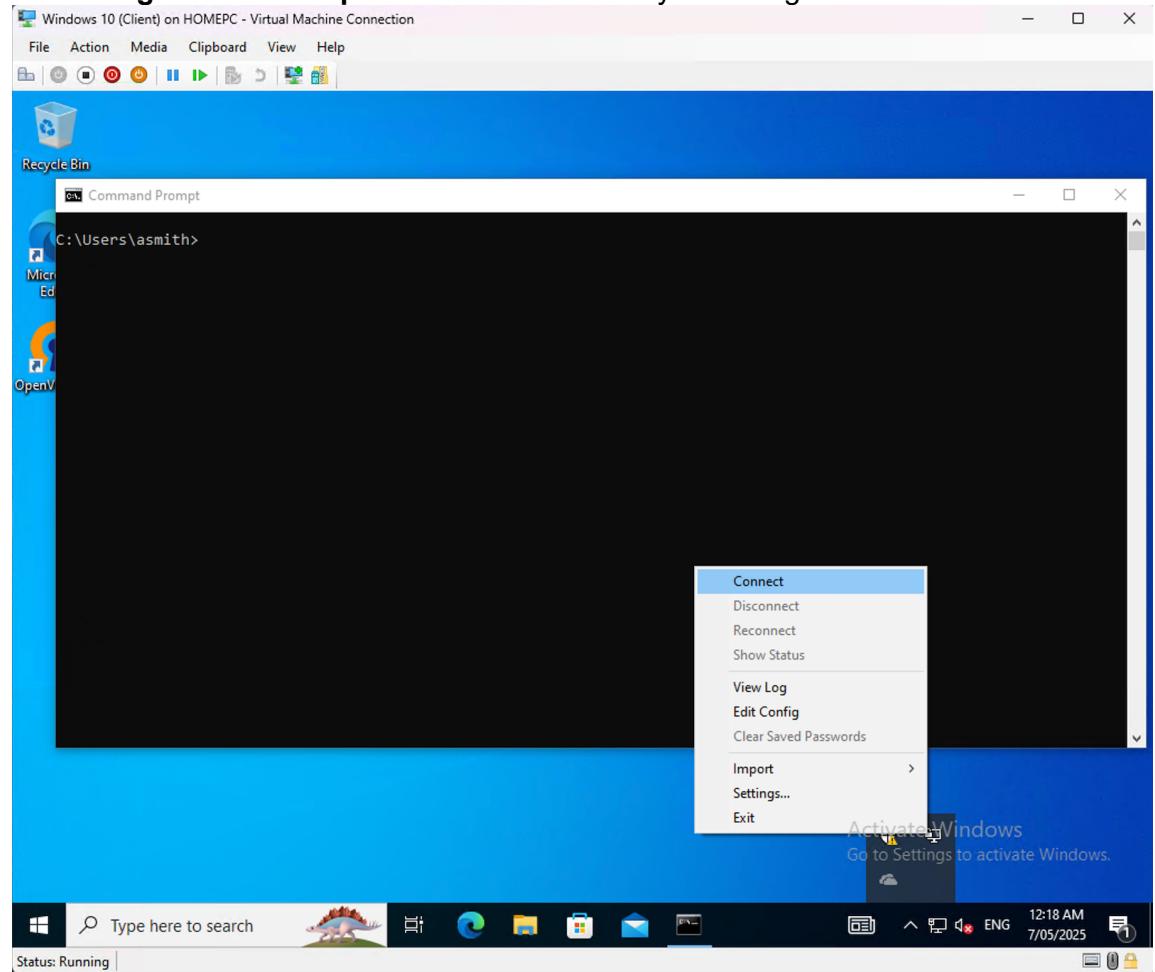


Connect and Test

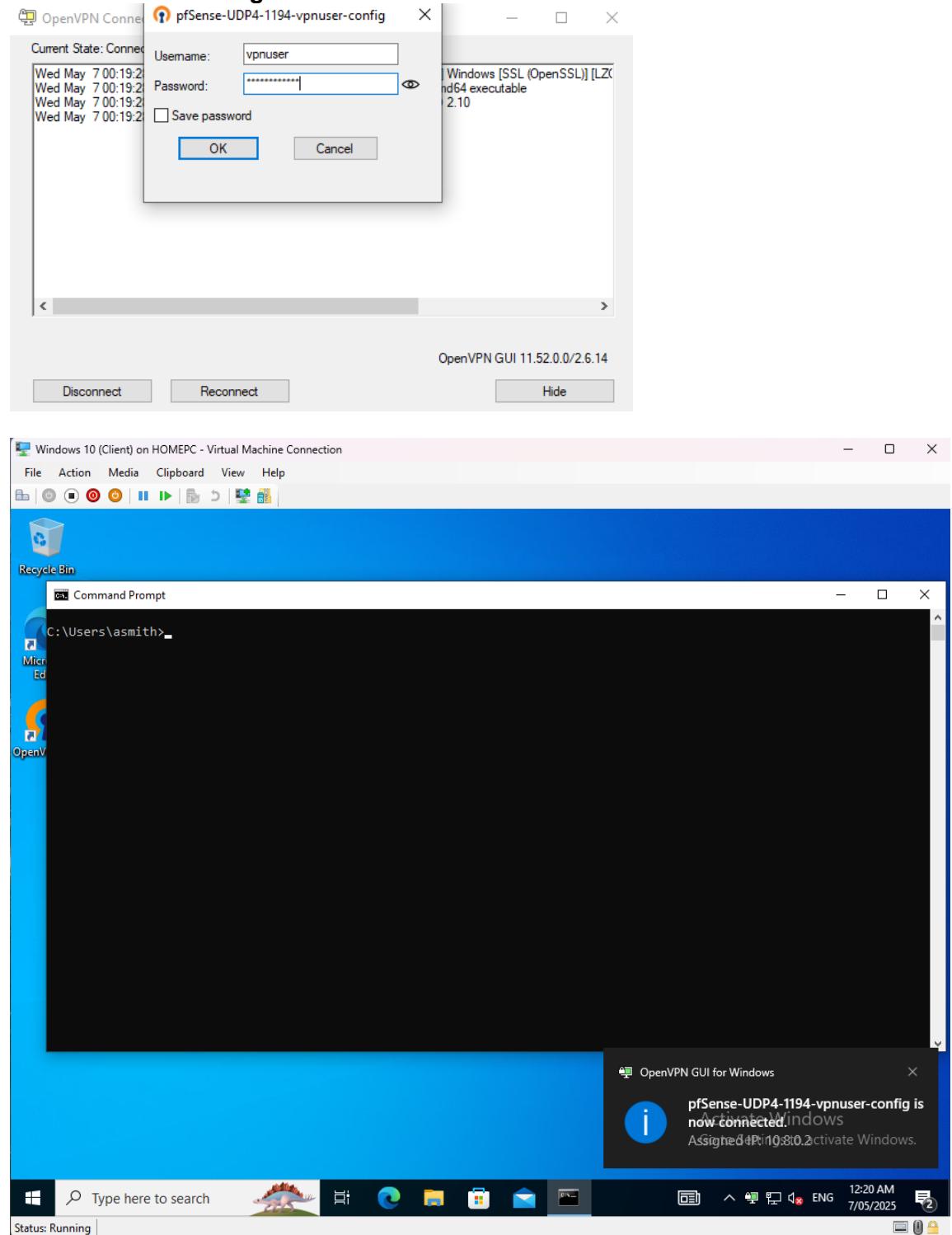
1. Connect to the VPN

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:**

```
Windows IP Configuration

Unknown adapter OpenVPN Wintun:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . :

Ethernet adapter Ethernet:
  Connection-specific DNS Suffix . :
  Link-local IPv6 Address . . . . . : fe80::8e94:2584:654c:7e3%12
  IPv4 Address. . . . . : 192.168.100.10
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.100.1

Unknown adapter OpenVPN TAP-Windows6:
  Connection-specific DNS Suffix . :
  Link-local IPv6 Address . . . . . : fe80::e9de:b9d7:31ac:f810%8
  IPv4 Address. . . . . : 10.8.0.2
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . :

Unknown adapter OpenVPN Data Channel Offload:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . :

C:\Users\asmith>
```

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

```
C:\Users\asmith>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=4ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=8ms TTL=64

Ping statistics for 192.168.1.1:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 8ms, Average = 3ms

C:\Users\asmith>ping 192.168.1.10

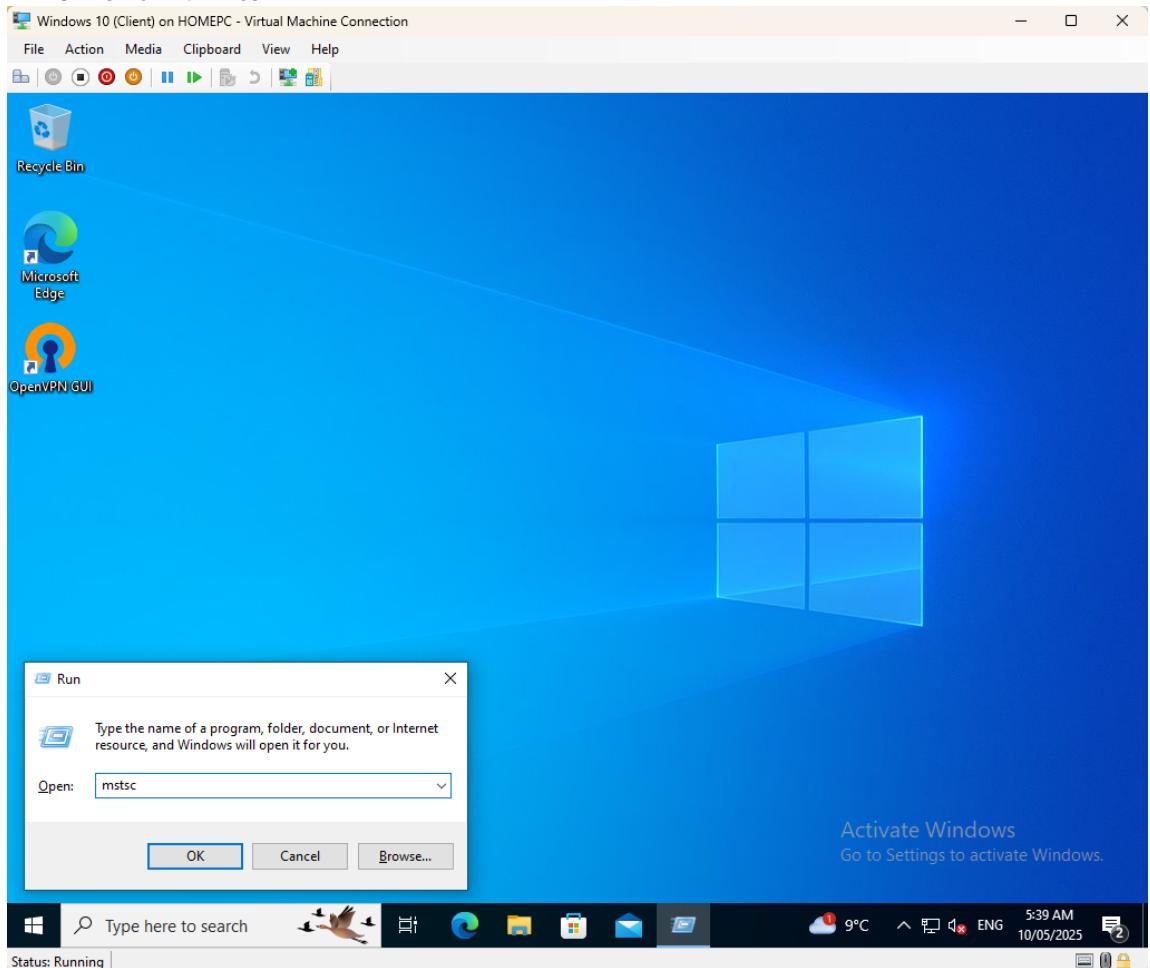
Pinging 192.168.1.10 with 32 bytes of data:
Reply from 192.168.1.10: bytes=32 time=1ms TTL=127
Reply from 192.168.1.10: bytes=32 time=2ms TTL=127
Reply from 192.168.1.10: bytes=32 time=1ms TTL=127
Reply from 192.168.1.10: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.1.10:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

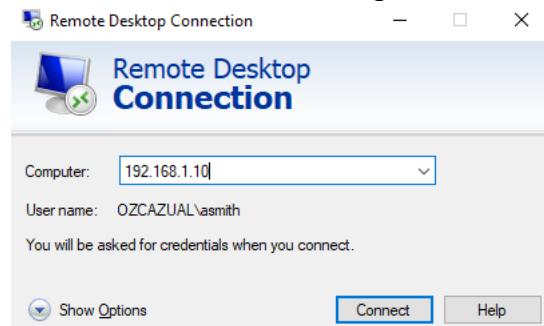
C:\Users\asmith>
```

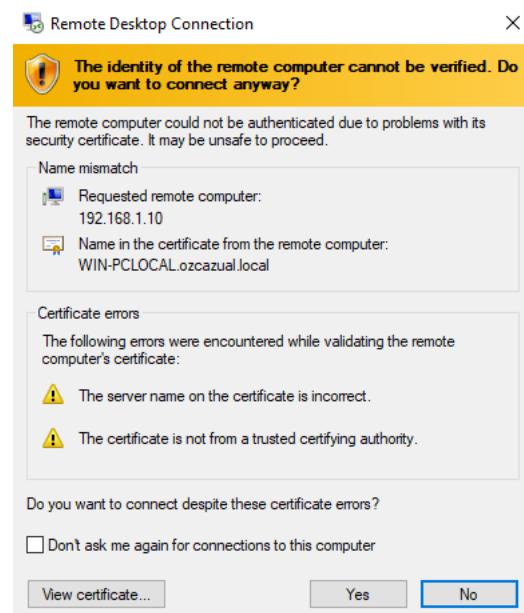
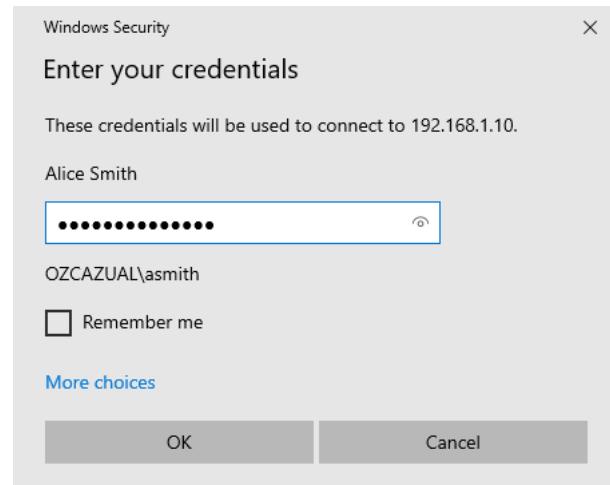
- **RDP via mstsc:**

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

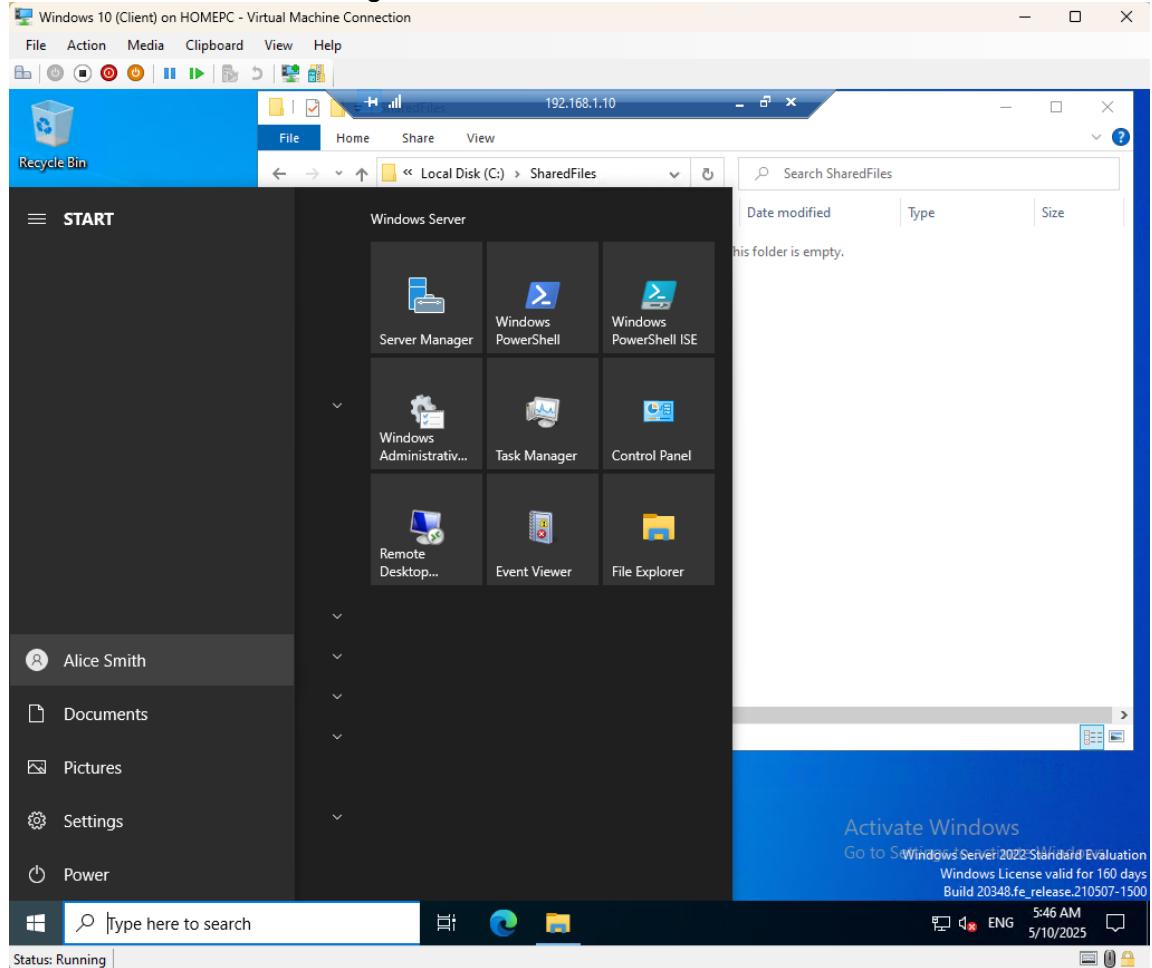


- You'll see the **Remote Desktop Connection** window.
- In the **Computer** field, enter the **IP address or hostname** of the machine you want to connect to.
- Click **Connect**, and enter login credentials when prompted.





- 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 toolbar OpenVPN tray image > View logs

```
pfSense-UDP4-1194-vpnuser-config - Notepad
File Edit Format View Help
2025-05-10 05:33:25 OpenVPN 2.6.14 [git:v2.6.14/f588592ee6c6323b] Windows [SSL (OpenSSL)] []
2025-05-10 05:33:25 Windows version 10.0 (Windows 10 or greater), amd64 executable
2025-05-10 05:33:25 library versions: OpenSSL 3.4.1 11 Feb 2025, LZO 2.10
2025-05-10 05:33:25 DCO version: 1.2.1
2025-05-10 05:33:32 TCP/UDP: Preserving recently used remote address: [AF_INET]192.168.100.
2025-05-10 05:33:32 UDPv4 link local: (not bound)
2025-05-10 05:33:32 UDPv4 link remote: [AF_INET]192.168.100.2:1194
2025-05-10 05:33:32 WARNING: this configuration may cache passwords in memory -- use the au
2025-05-10 05:33:32 [OpenVPN-Server] Peer Connection Initiated with [AF_INET]192.168.100.2:
2025-05-10 05:33:33 open_tun
2025-05-10 05:33:33 tap-windows6 device [OpenVPN TAP-Windows6] opened
2025-05-10 05:33:33 Set TAP-Windows TUN subnet mode network/local/netmask = 10.8.0.0/10.8.0
2025-05-10 05:33:33 Notified TAP-Windows driver to set a DHCP IP/netmask of 10.8.0.2/255.25
2025-05-10 05:33:33 Successful ARP Flush on interface [8] {781BAE5B-7EF2-4234-9A2C-4393B3A6
2025-05-10 05:33:33 IPv4 MTU set to 1500 on interface 8 using service
2025-05-10 05:33:38 Initialization Sequence Completed
2025-05-10 05:48:53 SIGTERM received, sending exit notification to peer
2025-05-10 05:49:07 SIGTERM[soft,exit-with-notification] received, process exiting
```