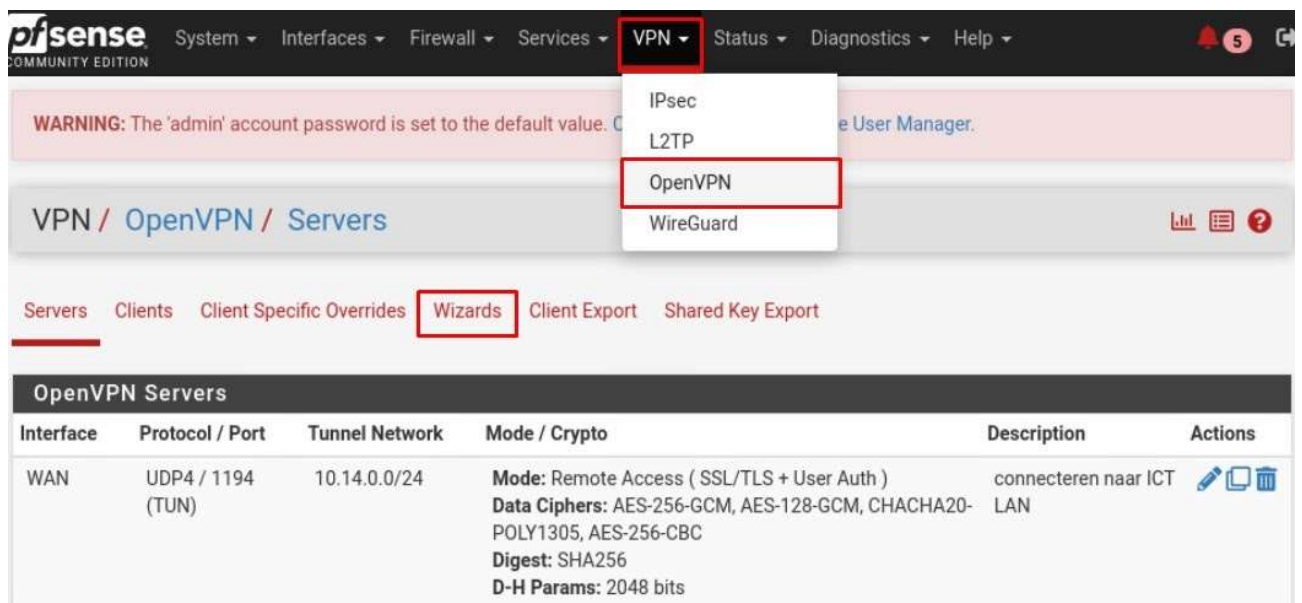
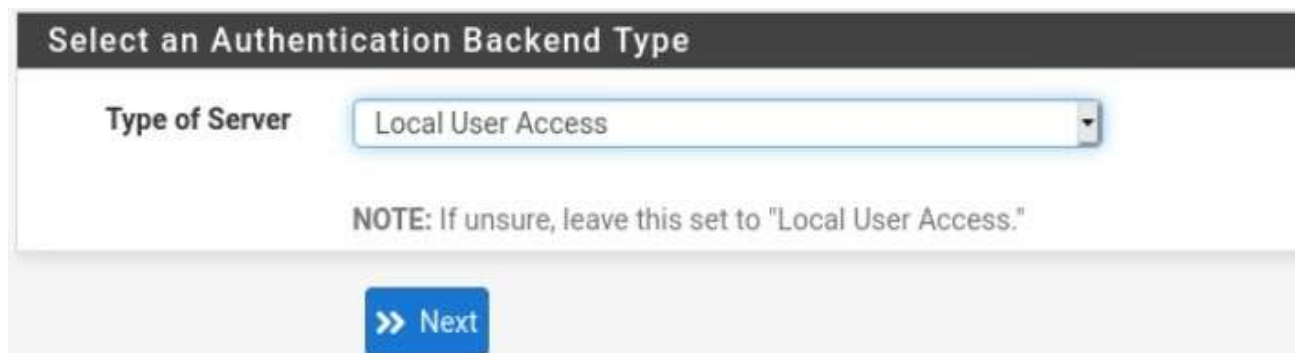


Documentatie VPN opzetten

We gaan een VPN opzetten zodat we van externe locatie ook kunnen connecteren naar het netwerk. Hiervoor gaan we naar de WEB GUI van pfSense. En gaan naar de tab 'VPN'



We openen de Wizards tab.



We selecteren bij 'type of server' voor Local user access en klikken op next.

=> 'add new CA' . Hier maken we een Nieuw Certificate Authority aan.

=> geef een naam op bij descriptive name: ik heb gekozen voor private_VPN_CA

=> key length laten we op 2048 bit staan

=> lifetime laten we ook op 10 jaar staan, (hier geef je dus in hoe lang je CA geldig blijft)

=> countrycode vullen we 'BE' voor België

=> state of province : Limburg

=> City : Hasselt

=> Organizatin: SSOL

Klik vervolgens op Add new CA

Descriptive name
A name for administrative reference, to identify this certificate. This is the same for all Certificates.

Key length
Size of the key which will be generated. The larger the key, the more security it provides (but it takes more time to generate, and take slightly longer to validate leading to a slight slowdown noticeable). As of 2016, 2048 bit is the minimum and most common selection. For more information see keylength.com

Lifetime
Lifetime in days. This is commonly set to 3650 (Approximately 10 years.)

Country Code
Two-letter ISO country code (e.g. US, AU, CA)

State or Province
Full State or Province name, not abbreviated (e.g. Kentucky, Indiana, Ontario).

City
City or other Locality name (e.g. Louisville, Indianapolis, Toronto).

Organization
Organization name, often the Company or Group name.

[» Add new CA](#)

Choose a Server Certificate

Certificate

[» Add new Certificate](#) [» Next](#)

Klik op Add new certificate

Vul deze Certificate in hetzelfde in gelijk de vorig allen geef je deze een andere naam en laat je de lifetime op 398 staan

Descriptive name	<input type="text" value="Server_CA"/>	A name for administrative reference, to identify this certificate. This is also known as the certificate's
Key length	<input type="text" value="2048 bit"/>	Size of the key which will be generated. The larger the key, the more security it offers, but larger keys take time to generate, and take slightly longer to validate leading to a slight slowdown in setting up new certificates (noticeable). As of 2016, 2048 bit is the minimum and most common selection and 4096 is the maximum. For more information see keylength.com
Lifetime	<input type="text" value="398"/>	Lifetime in days. Server certificates should not have a lifetime over 398 days or some platforms may consider them invalid.
Country Code	<input type="text" value="BE"/>	Two-letter ISO country code (e.g. US, AU, CA)
State or Province	<input type="text" value="LIMBURG"/>	Full State or Province name, not abbreviated (e.g. Kentucky, Indiana, Ontario).
City	<input type="text" value="HASSELT"/>	City or other Locality name (e.g. Louisville, Indianapolis, Toronto).
Organization	<input type="text" value="SSOL"/>	Organization name, often the Company or Group name.

[» Create new Certificate](#)

En klik op create new certificate.

Interface	<input type="text" value="WAN"/>	The interface where OpenVPN will listen for incoming connections (typically WAN.)
Protocol	<input type="text" value="UDP on IPv4 only"/>	Protocol to use for OpenVPN connections. If unsure, leave this set to UDP.
Local Port	<input type="text" value="1194"/>	Local port upon which OpenVPN will listen for connections. The default port is 1194. This can be left at its default unless a different port needs to be used.
Description	<input type="text" value="connecteren naar ICT LAN"/>	A name for this OpenVPN instance, for administrative reference. It can be set however desired, but is often used to distinguish the purpose of the service (e.g. "Remote Technical Staff"). It is also used by OpenVPN Client Export to identify this VPN on clients.

Nu gaan we de OpenVpn server informatie invullen

Interface => WAN : hier komt de connectie binnen.

Protocol => UDP on IPv4 only : UDP is sneller dan TCP maar is niet zo foutgevoelig, we kiezen UDP voor een snelle werking

Local port => 1194 : dit is de standaard OpenVPN port en laten we staan

Description => geef een toepasselijke beschrijving.

Nu gaan we de Encryptie instellen.

TLS Authentication	<input checked="" type="checkbox"/>	Enable authentication of TLS packets.
Generate TLS Key	<input checked="" type="checkbox"/>	Automatically generate a shared TLS authentication key.
TLS Shared Key	<div></div> <p>Paste in a shared TLS key if one has already been generated.</p>	
DH Parameters Length	2048 bit	Length of Diffie-Hellman (DH) key exchange parameters, used for establishing a secure communications channel. The DH parameters are different from key sizes, but as with other such settings, the larger the key, the more security it offers, but larger keys take considerably more time to generate. As of 2016, 2048 bit is a common and typical selection.
Data Encryption Negotiation	<input checked="" type="checkbox"/>	Enable negotiation of Data Encryption Algorithms between client and server. The best practice is keep this setting enabled.
Data Encryption Algorithms	AES-256-GCM AES-128-GCM CHACHA20-POLY1305	
Fallback Data Encryption Algorithm	AES-256-CBC (256 bit key, 128 bit block)	The algorithm used to encrypt traffic between endpoints when data encryption negotiation is disabled or fails.
Auth Digest Algorithm	SHA256 (256-bit)	The method used to authenticate traffic between endpoints. This setting must match on the client and server side, but is otherwise set however desired.
Hardware Crypto	No Hardware Crypto Acceleration	The hardware cryptographic accelerator to use for this VPN connection, if any.

Laat TLS auth. & Gen TLS Key Aangevinkt staan

DH Parmas Length laten we ook op 2048 staan.

Laat data encryption aangevinkt staan

Selecteer de 3 Encryption Algoritmes.

Selecteer AES-256-CBC (256b Key, 128b Block)

Selecteer SHA256 (256b)

En geen hardware crypto.

Tunnel Settings	
Tunnel Network	<input type="text" value="10.14.0.0/24"/> <small>This is the virtual network used for private communications between this server and client hosts expressed using CIDR notation (eg. 10.0.8.0/24). The first network address will be assigned to the server virtual interface. The remaining network addresses will be assigned to connecting clients.</small>
Redirect Gateway	<input checked="" type="checkbox"/> <small>Force all client generated traffic through the tunnel.</small>
Local Network	<input type="text" value="10.14.3.0/29"/> <small>This is the network that will be accessible from the remote endpoint, expressed as a CIDR range. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.</small>
Concurrent Connections	<input type="text" value="1"/> <small>Specify the maximum number of clients allowed to concurrently connect to this server.</small>

Nu gaan we de tunnel settings instellen.

We kiezen een virtueel netwerk, meestal word hier gekozen voor 10.0.8.0/24 zoals in de beschrijving te lezen staat. We hebben gekozen voor 10.14.0.0/24

Vink redirect Gateway aan. Zo wordt al de traffic door de firewall gehaald, dit is gemakkelijker om te monitoren.

Bij local network kiezen we het netwerk waar hij tot kan verbinden in ons geval ons ICT (lan net)

10.14.3.0/29

Concurrent connections: hier kun je aangeven hoeveel clients er gelijktijdig kunnen connecteren. We kiezen 1.

Laat de rest van de tunnel settings op default staan.

Dynamic IP	<input checked="" type="checkbox"/>	Allow connected clients to retain their connections if their IP address changes.
Topology	Subnet – One IP address per client in a common subnet ▾	Specifies the method used to supply a virtual adapter IP address to clients when using OpenVPN. Some clients may require this be set to "subnet" even for IPv6, such as OpenVPN Connect. Older versions of OpenVPN (before 2.0.9) or clients such as Yealink phones may require "static" instead.
DNS Default Domain	10.14.3.1	Provide a default domain name to clients.
DNS Server 1	8.8.8.8	DNS server IP to provide to connecting clients.
DNS Server 2	8.8.4.4	DNS server IP to provide to connecting clients.
DNS Server 3		DNS server IP to provide to connecting clients.
DNS Server 4		DNS server IP to provide to connecting clients.
NTP Server		Network Time Protocol server to provide to connecting clients.
NTP Server 2		Network Time Protocol server to provide to connecting clients.
NetBIOS Options	<input checked="" type="checkbox"/>	Enable NetBIOS over TCP/IP

Onder de client settings:

Vink Dynamic IP aan.

Topology: Subnet - One IP address per client in common subnet

DNS default geeft de GW op in ons geval 10.14.3.1

DNS1: 8.8.8.8

DNS2: 8.8.4.4

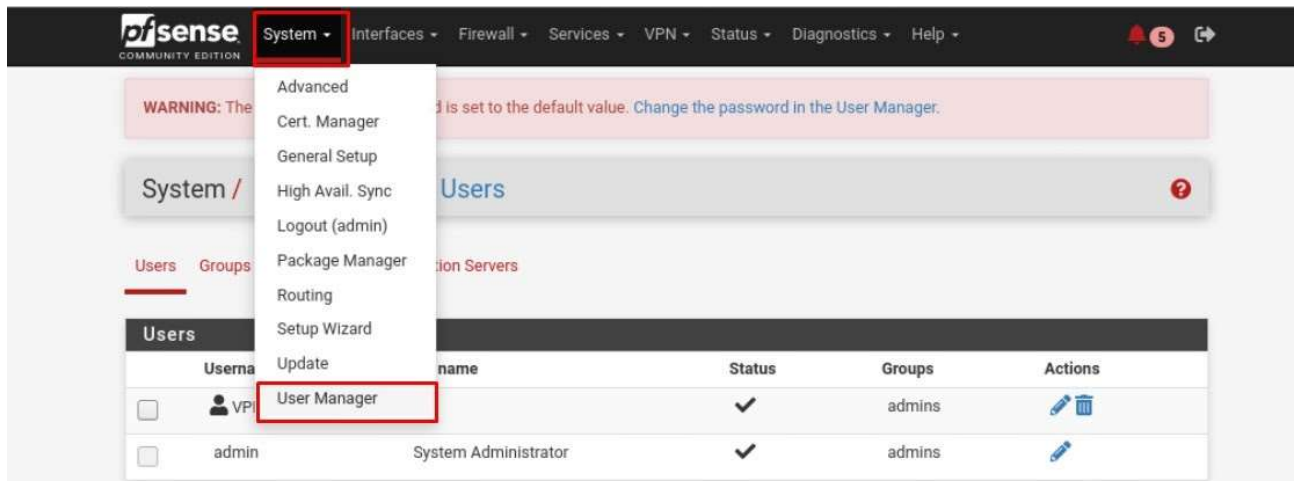
Vink netbios aan

Klik Next

Vink Firewall rule & Open VPN rule aan

Klik next en finish!

Nu gaan we een VPN User toevoegen.



Navigeer naar usermanager en klik op 'add'

Kies een naam voor de VPN user bv. VPNuser en kies hier een wachtwoord voor. Ons geval vpn123

Fullname hoeft je niet in te vullen

Je je user tijdelijk maken door een vervaldatum mee te geven onze is 12/31/2021

We plaatsen de user in de groep admins.

Vink certificate aan.

Descriptive name : naam geven bv. Certificate VPNuser

Bij certificate authority kies je je eerst aangemaakte CA.

Rsa lengte 2048

Digest algorithm sha256

Lifetime 3650

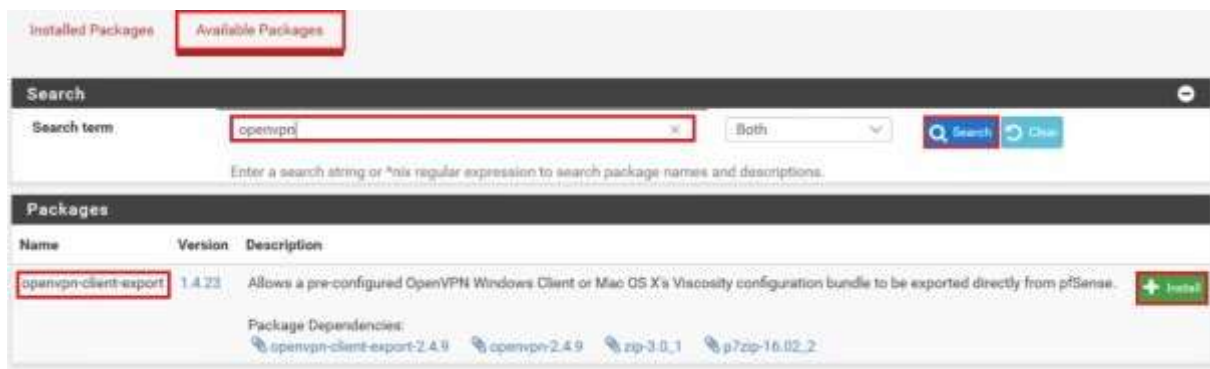
En klik op save!

Exporteren van .ovpn bestand

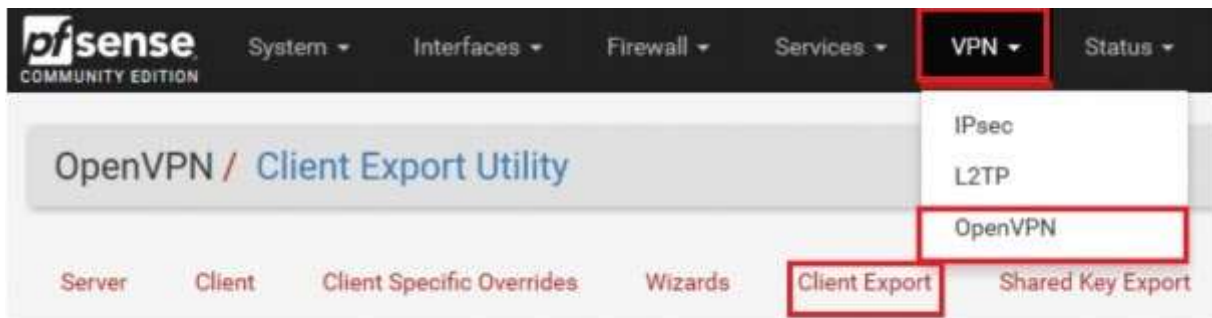
We navigeren ons naar de Package Manager:



Zoek tussen available packages naar openvpn en installeer 'openvpn-client-export'



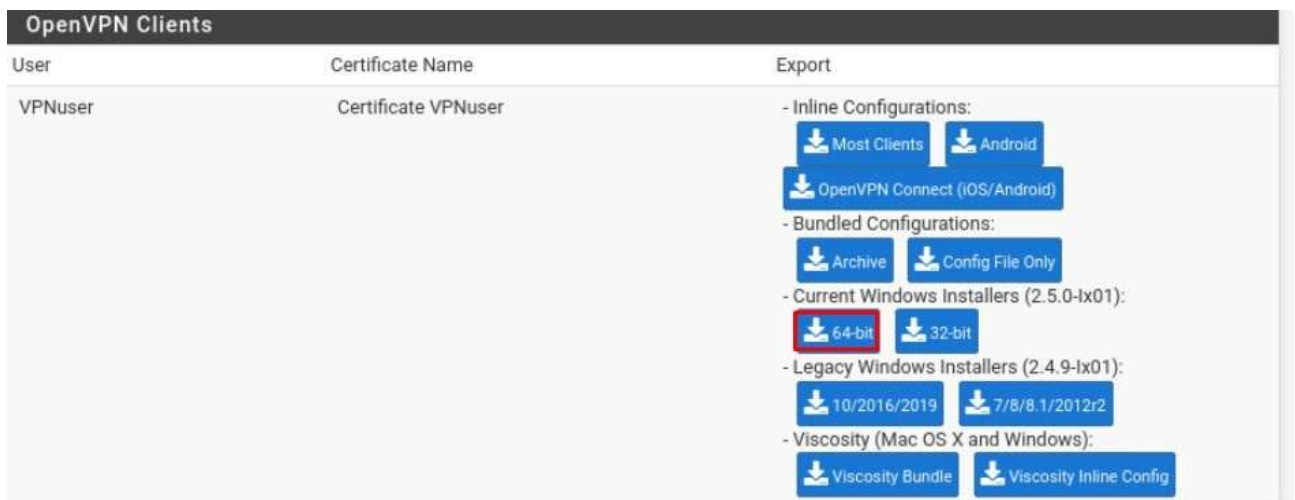
Nu moeten we .ovpn file downloaden zodat we dit bestand kunnen overbrengen naar de computer die VPN access krijgt. Navigeer daarvoor naar client export.



Selecteer je aangemaakte configuratie.

En laat al de default settings staan.

Dan scrollen we naar onder en klikken op 64-bit bij 'Current Windows installers'



Nu wordt het .ovpn bestand gedownload. Nu moeten we dit bestand nog op de betreffende computer krijgen.

Installatie openVPN op desktop

We starten de de desktop op. Kijk wel dat deze voorlopig in het netwerk zit. => ipconfig

```

Command Prompt
C:\Users\VPN USER>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : home.arpa
    Link-local IPv6 Address . . . . . : fe80::9cc6:a677:a57b:5643%12
    IPv4 Address. . . . . : 10.14.1.12
    Subnet Mask . . . . . : 255.255.255.128
    Default Gateway . . . . . : 10.14.1.1

C:\Users\VPN USER>

```

Nu gaan we een sftp connectie opzetten naar de computer die zonet het bestand gedownload had.
>sftp root@10.14.1.5

```
C:\Users\VPN USER>sftp root@10.14.1.5
The authenticity of host '10.14.1.5 (10.14.1.5)' can't be established.
ECDSA key fingerprint is SHA256:3fNd9Ypx9BgbZmYZFhu31VjDm3NdL2ieAWoEgvuasII.
Are you sure you want to continue connecting (yes/no)?
```

```
C:\Users\VPN USER>sftp root@10.14.1.5
The authenticity of host '10.14.1.5 (10.14.1.5)' can't be established.
ECDSA key fingerprint is SHA256:3fNd9Ypx9BgbZmYZFhu31VjDm3NdL2ieAWoEgvuasII.
Are you sure you want to continue connecting (yes/no)?
Warning: Permanently added '10.14.1.5' (ECDSA) to the list of known hosts.
root@10.14.1.5's password:
```

Typ yes & geef het wachtwoord op.

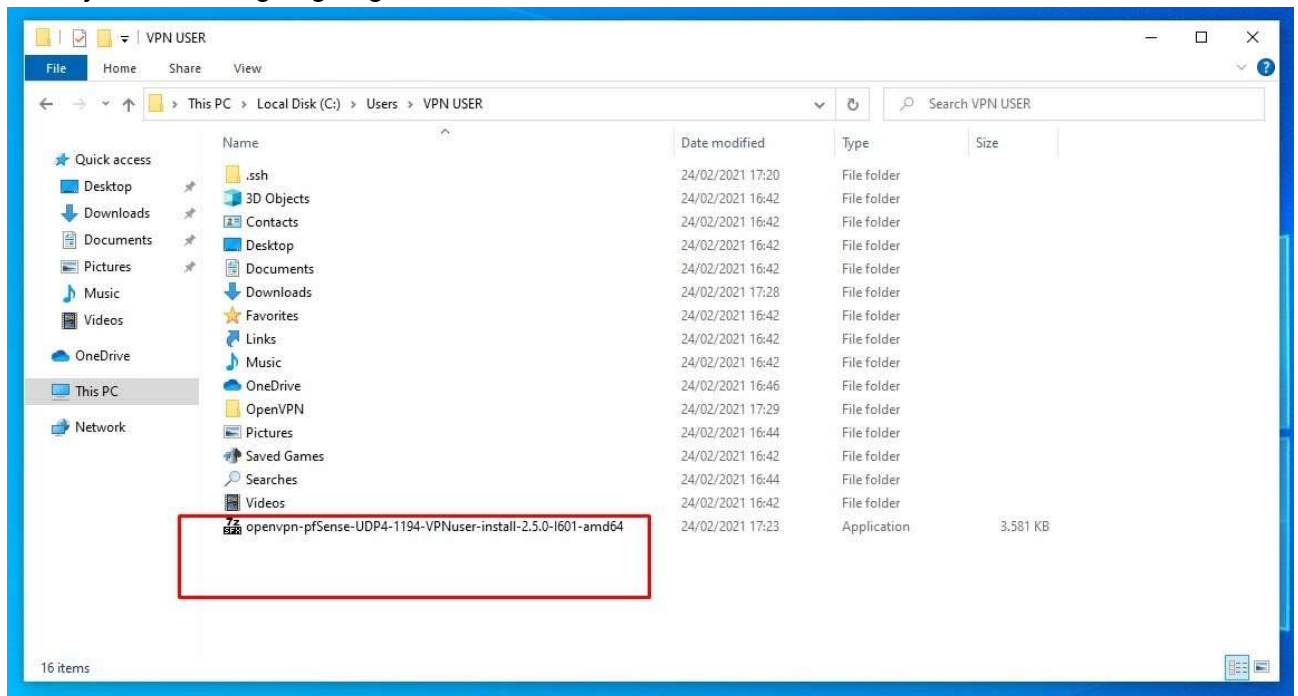
```
sftp> ls
Desktop                Documents              Downloads              Music                 Pictures
Public                Templates             Videos               anaconda-ks.cfg      initial-setup-ks.cfg
sftp> cd Downloads
sftp> ls
openvpn-pfSense-UDP4-1194-VPNuser-install-2.5.0-I601-amd64.exe
sftp> get openvpn-pfSense-UDP4-1194-VPNuser-install-2.5.0-I601-amd64.exe
```

Doe cd naar de map waar het bestand is gedownload. > cd Downloads & doe ls om te kijken of het bestand daar staat.

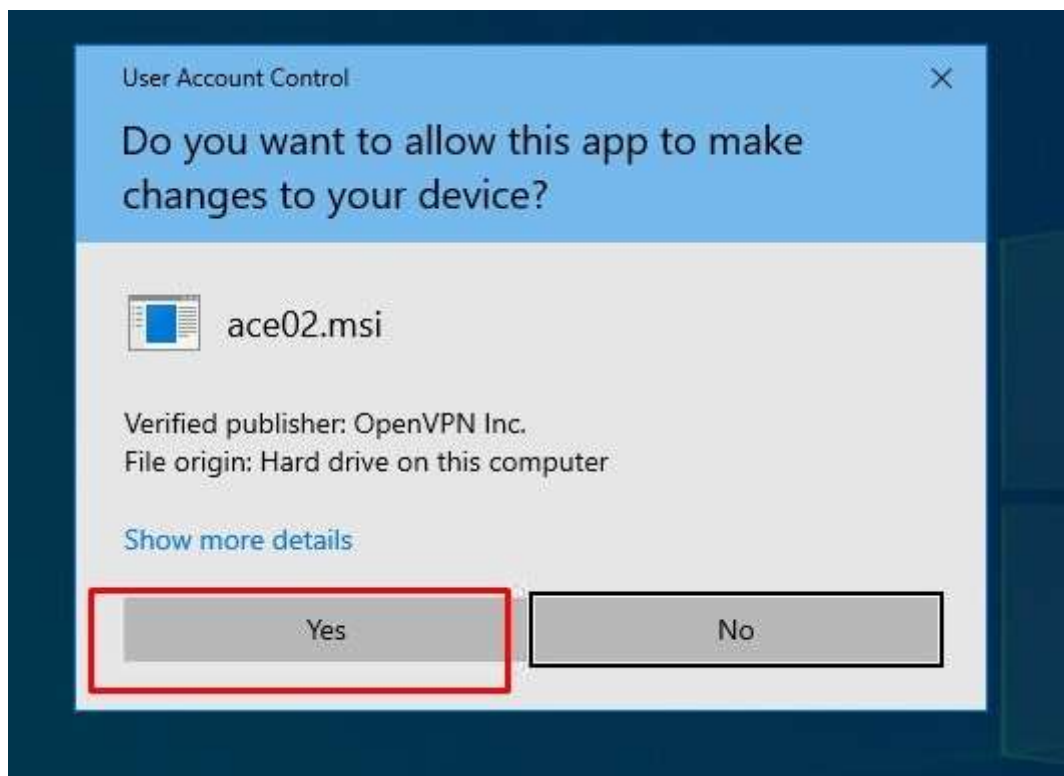
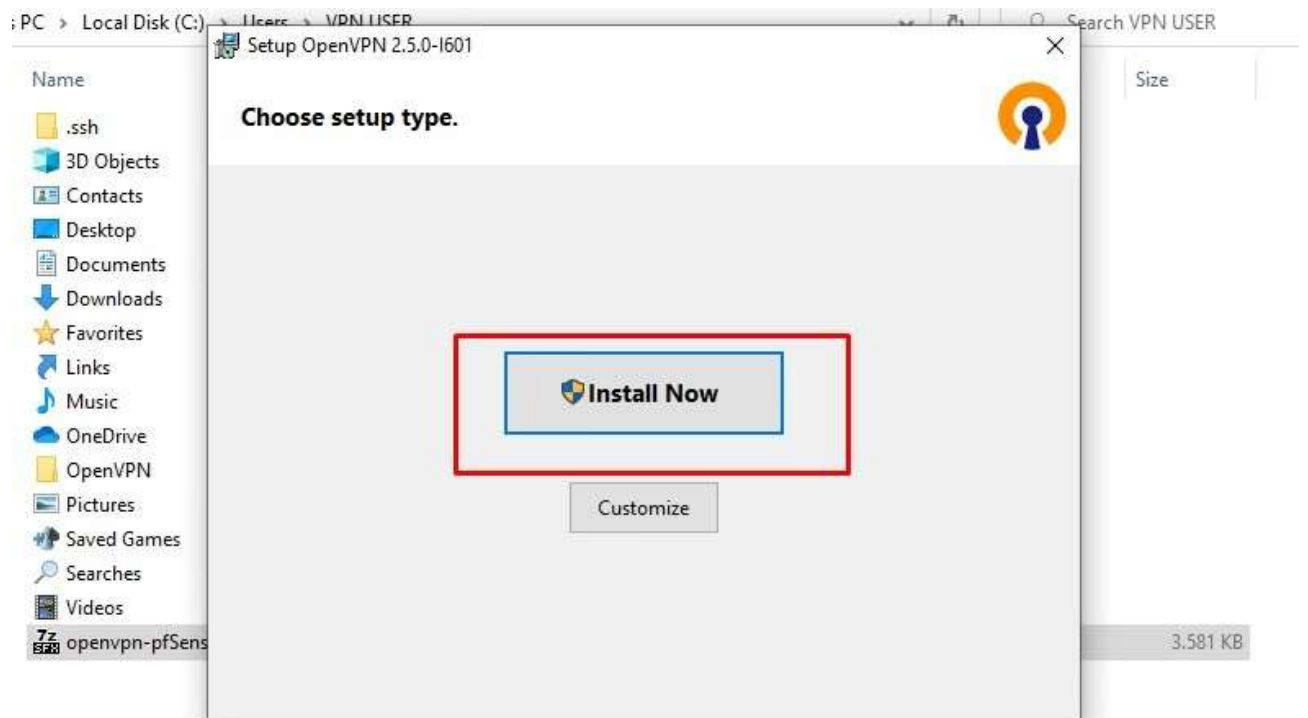
Als het bestand er staat typ dan

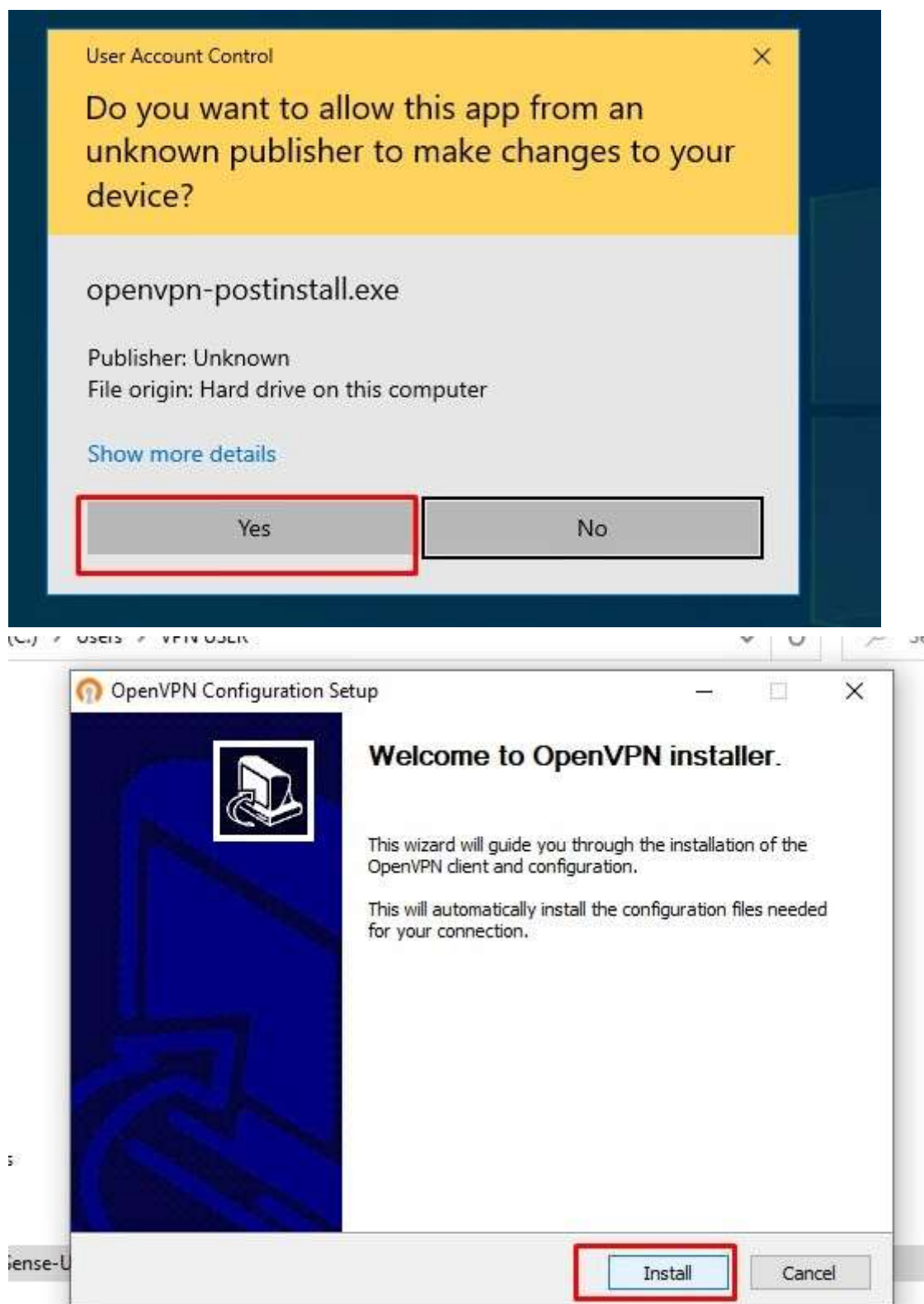
>get openvpn-pfSense-UDP4-1194-VPNuser-install-2.5.0-I601-amd64.exe (de filename dus)

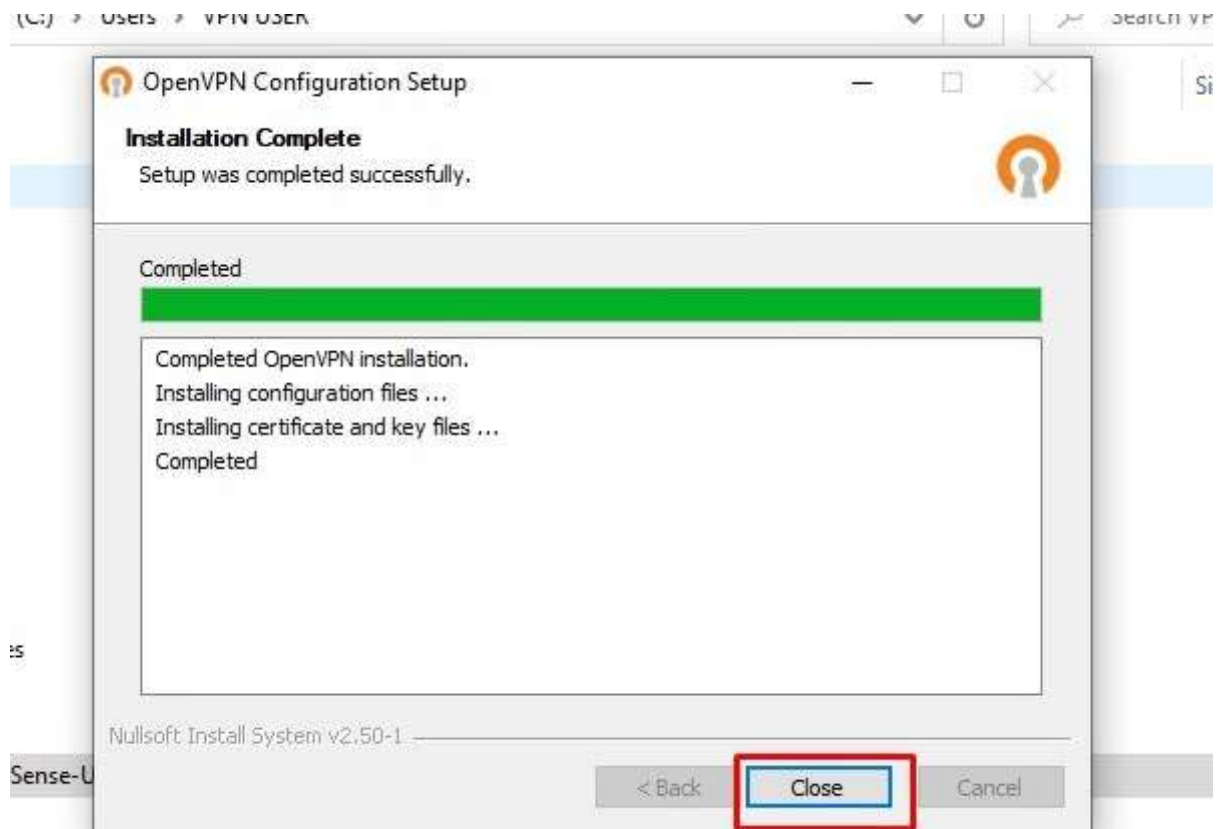
Dit bestand zal nu gedownload worden naar de computer. Dit bestand zal zich bevinden onder de C schijf onder de ingelogde gebruiker.



Voer dit bestand uit. Zie volgende stappen



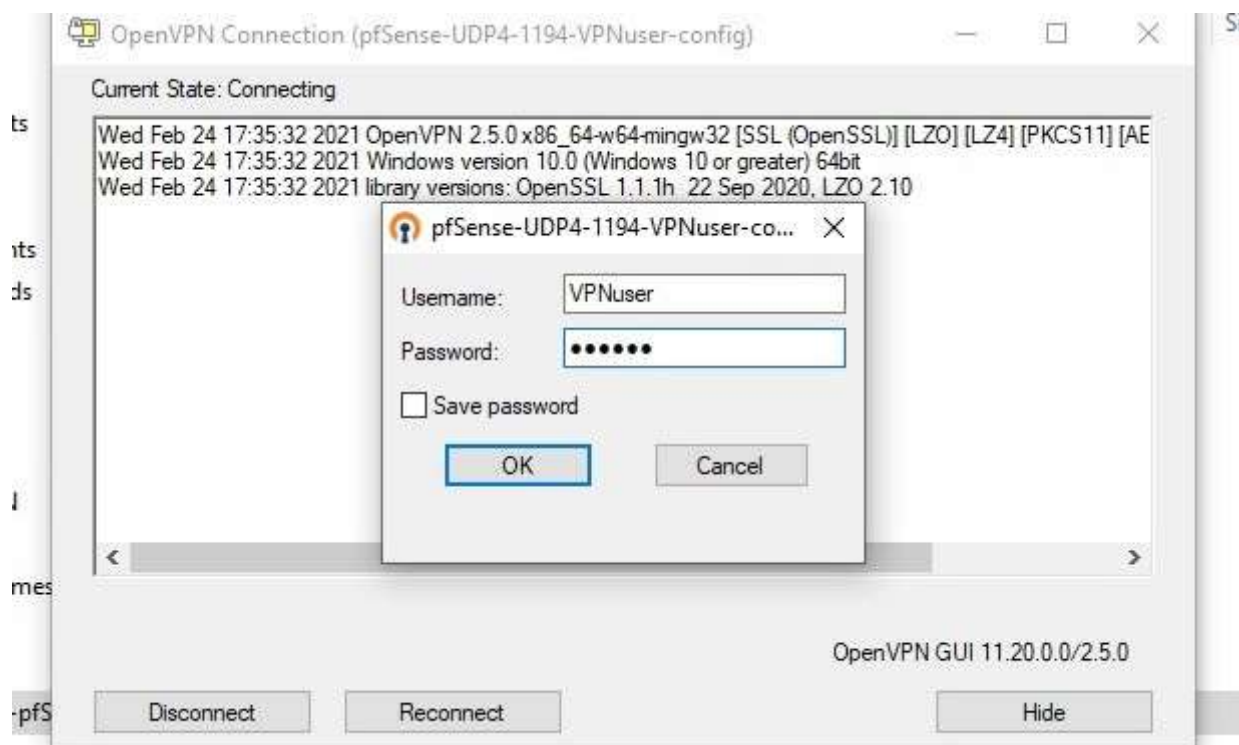
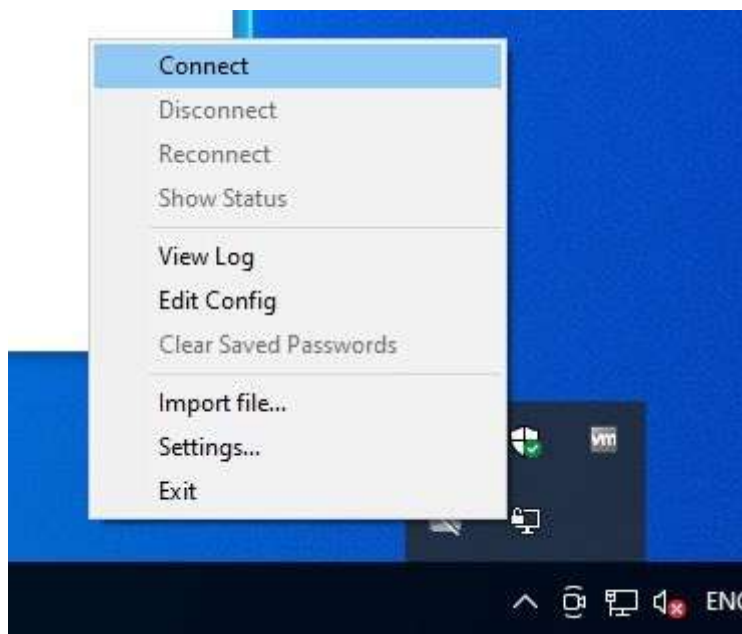




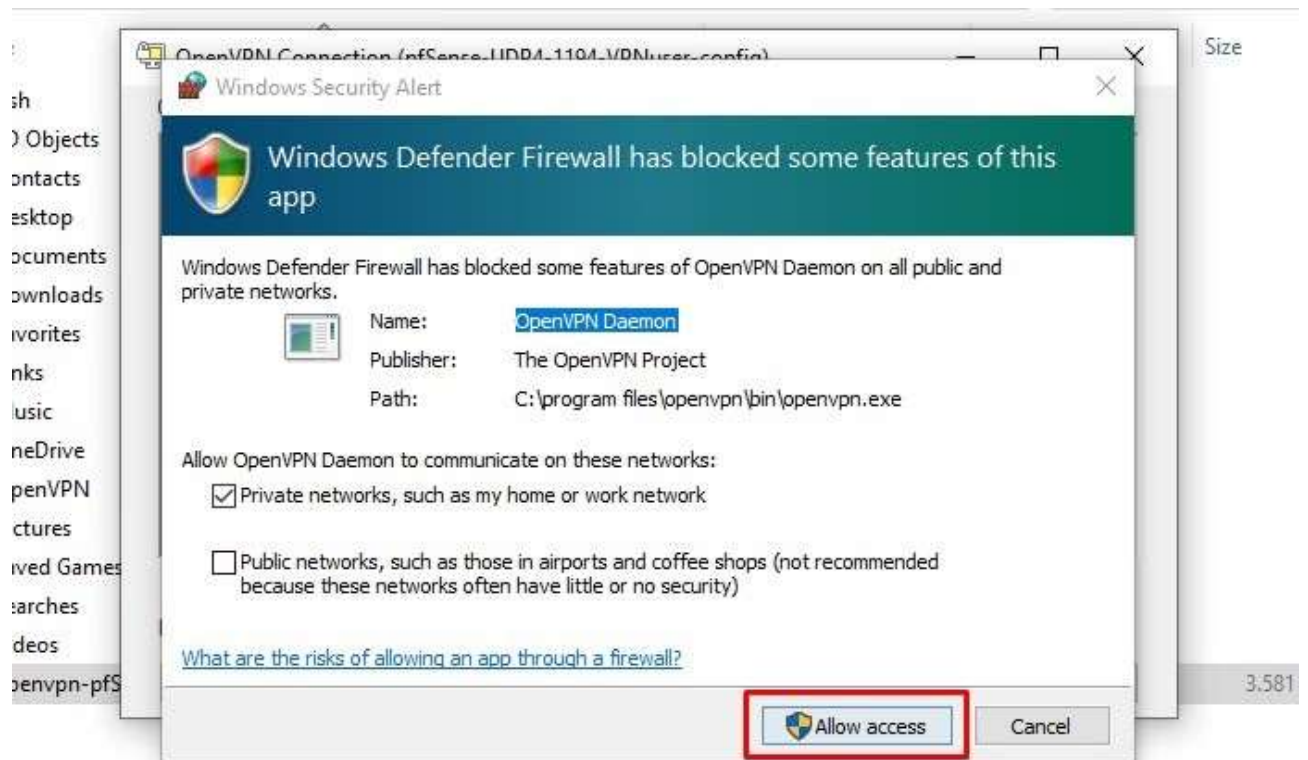
Nu gaan we connectie maken met het remote netwerk. Open de openVPN GUI.



=> Klik op Connect



Nu wordt er gevraagd om in te loggen. Doe dit met de aangemaakte user. VPNuser/vpn123 en druk op OK.



Allow access voor de Firewall

```
CA Command Prompt

C:\Users\VPN USER>ipconfig

Windows IP Configuration

Unknown adapter OpenVPN Wintun:

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

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : home.arpa
    Link-local IPv6 Address . . . . . : fe80::9cc6:a677:a57b:5643%12
    IPv4 Address. . . . . : 10.14.1.12
    Subnet Mask . . . . . : 255.255.255.128
    Default Gateway . . . . . : 10.14.1.1

Unknown adapter OpenVPN TAP-Windows6:

    Connection-specific DNS Suffix  . : 10.14.3.1
    Link-local IPv6 Address . . . . . : fe80::5c62:21c5:77e3:f0fc%25
    IPv4 Address. . . . . : 10.14.0.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

C:\Users\VPN USER>
```

En check of je in het remote netwerk zit. Als dit zo is heb je succesvol een VPN opgezet.