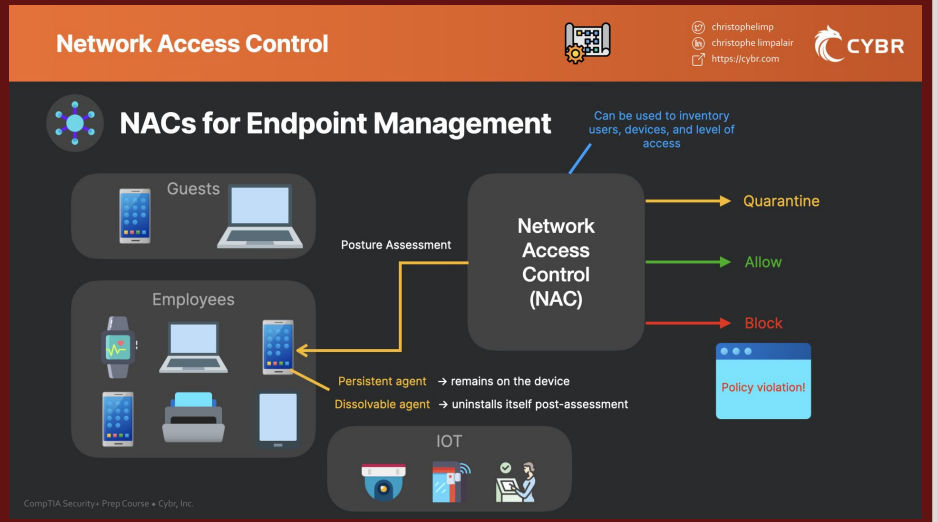
OpenVPN

Trey Atwood

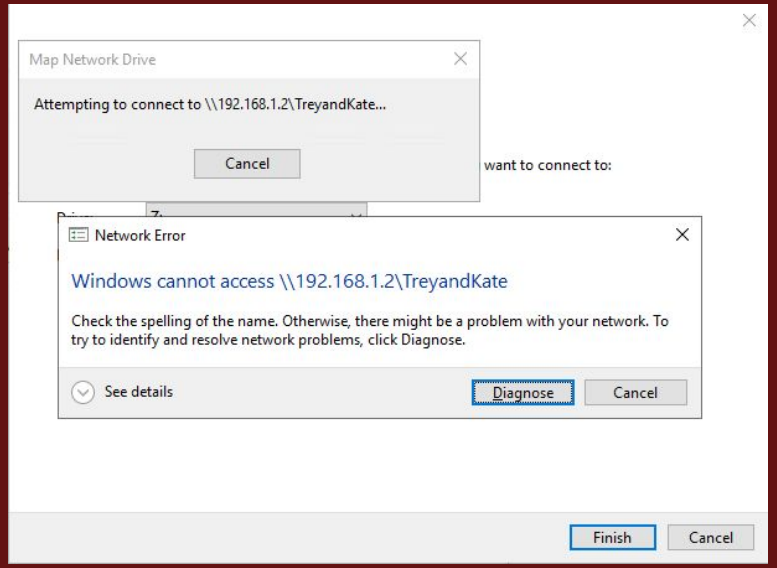
Network Access Control (Internal and External)

Network Access Control or NAC, is all about controlling who can get onto our network, and what they can do once they're in. External NAC that protects the network side from the internet into our closed network environment. For this activity we setup OpenVPN as our only entry point or External NAC into our network. PFSense only exposes the VPN to the internet, and the users must authenticate with their username and password that we setup in the local users in PFSense. As for the Internal NAC, this is everything that controls what a connected user to reach inside our network. In our OpenVPN settings in this lab we have a separate VPN subnet for the users connected. VPN clients get IPs in the 192.168.0.0/24 range, while our LAN is 192.168.1.0. This separation allows us to add rules that only allow users from the range 192.168.0.0/24 to reach our file server 192.168.1.2 over SMB.



Network Policy (Development and Enforcement)

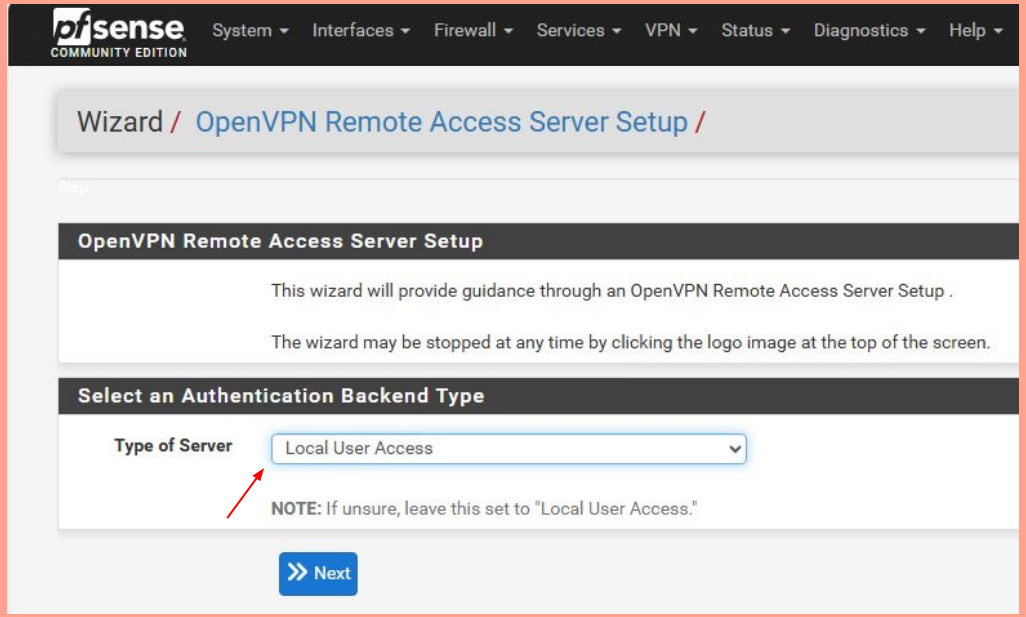
Network policy is the set of rules that says who can do what within the network, under what conditions, and how it's going to be monitored. The development side is where you are "writing the rules" here you define the goals of what you want the network policy to do. For this exercise we want to protect access to our file sharing with a VPN, so that is our goal. As for our lab we want to create a certain user who gets access to the file sharing which is another step in the development process. As for the enforcement, this is where you make the rules work. In the lab we tunneled network traffic through "192.168.0.0/24" and the local network "192.168.1.0/24" to enforce users to be separate from the LAN and they must cross through the firewall. On the WAN, only OpenVPN ports 1194 are allowed in, and in the WAN rules we disable SMB from the internet by disabling port 445 which forces users to use the VPN.



To start setting up OpenVPN, we first need to decide where our users are going to be authenticated. For this we want our users to be authenticated from our own PFSense, so for this we choose “Local User Access”.

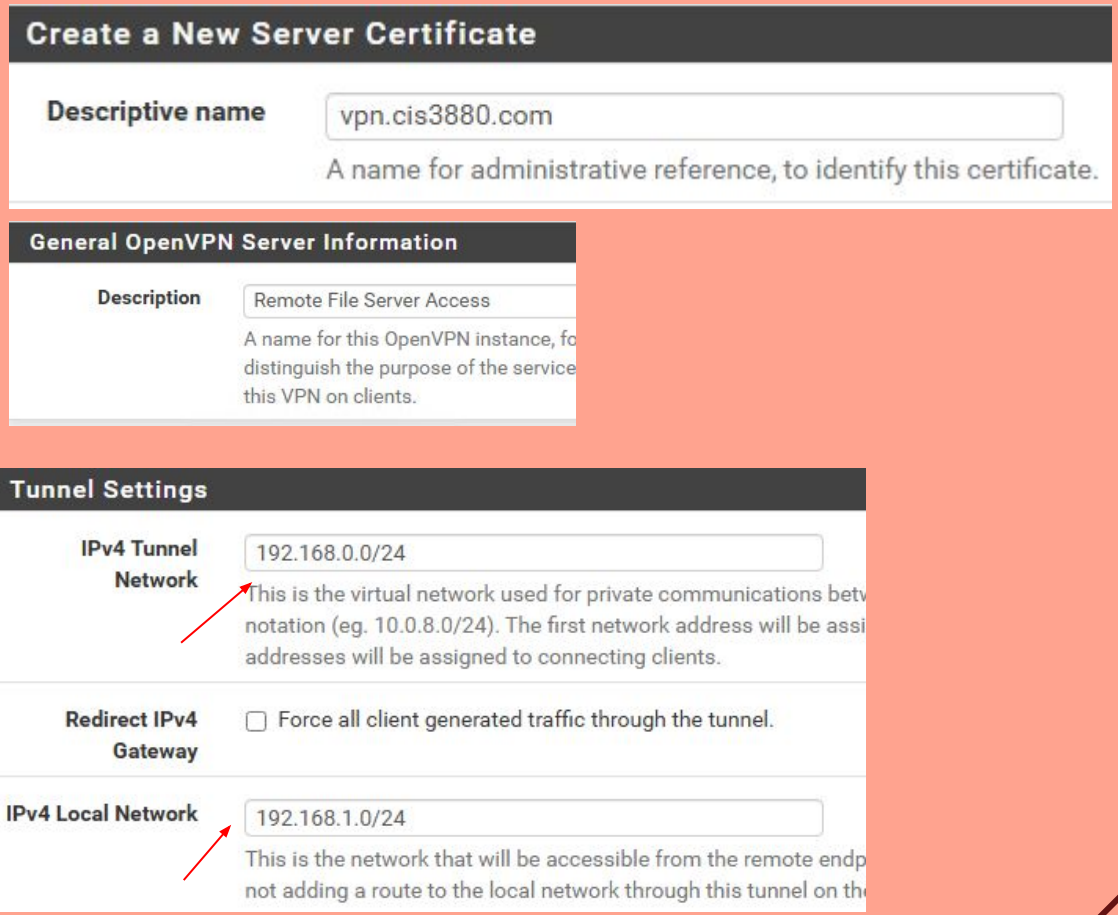
Next we’ll need to set up a Certificate Authority. This is necessary because all of the users who are using the VPN locally are going to need a certificate, and in order to have a certificate given to the users we need to properly setup a working Certificate Authority.

For the name for the CA I named it “Local User Access CA (OpenVPN)”



Next we will configure a Host Name for our VPN. For this I used the name of our class CIS 3880. Normally for the host name you would use the domain name of the company would be using the VPN.

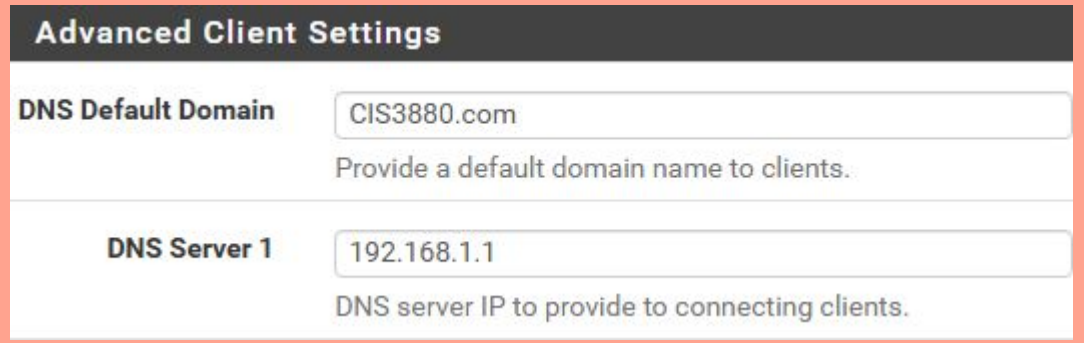
Next, we will need to setup the server information. Since we are going to be using the VPN to access file sharing I'll name the server "Remote File Server Access", keeping it specific as to what it's going to be used for. Next we will configure the IPv4 tunnel network, which we will set as "192.168.0.0/24", and set the IPv4 Local Network to "192.168.1.0/24". Our local network is the network that we are attaching the VPN to.

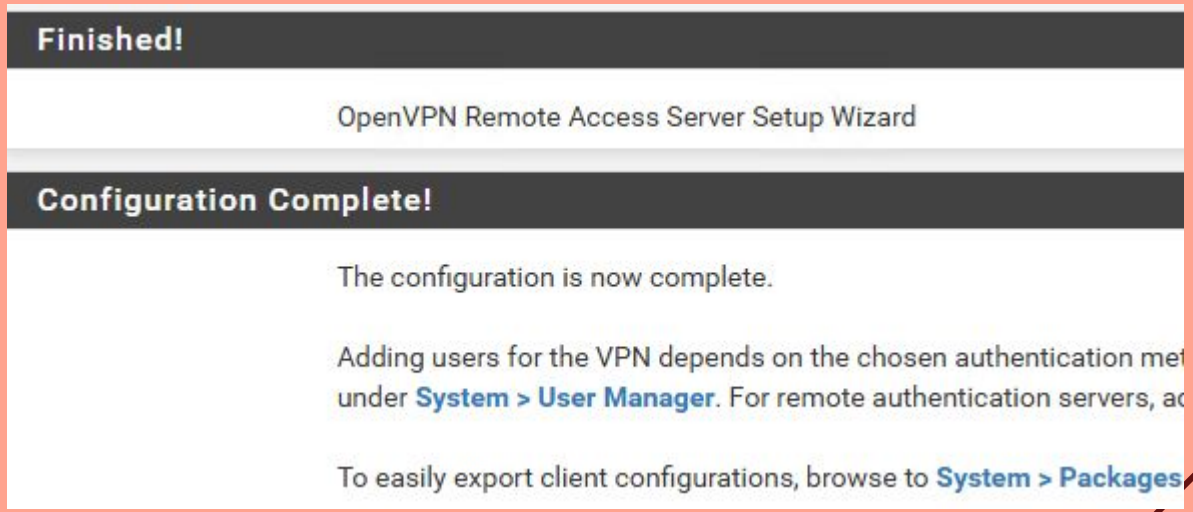


Finishing out the server setup, we will need to configure the DNS default domain, and the IP for our DNS server. For this I just used the name of our class once again "CIS3880.com" as the domain name, and set the DNS server to "192.168.1.1" which is the IP address for PFSense. If someone connects to the VPN they are going to use PFSense as the DNS for the VPN.

After we finish configuring all of these steps we are complete with the setup of the VPN!

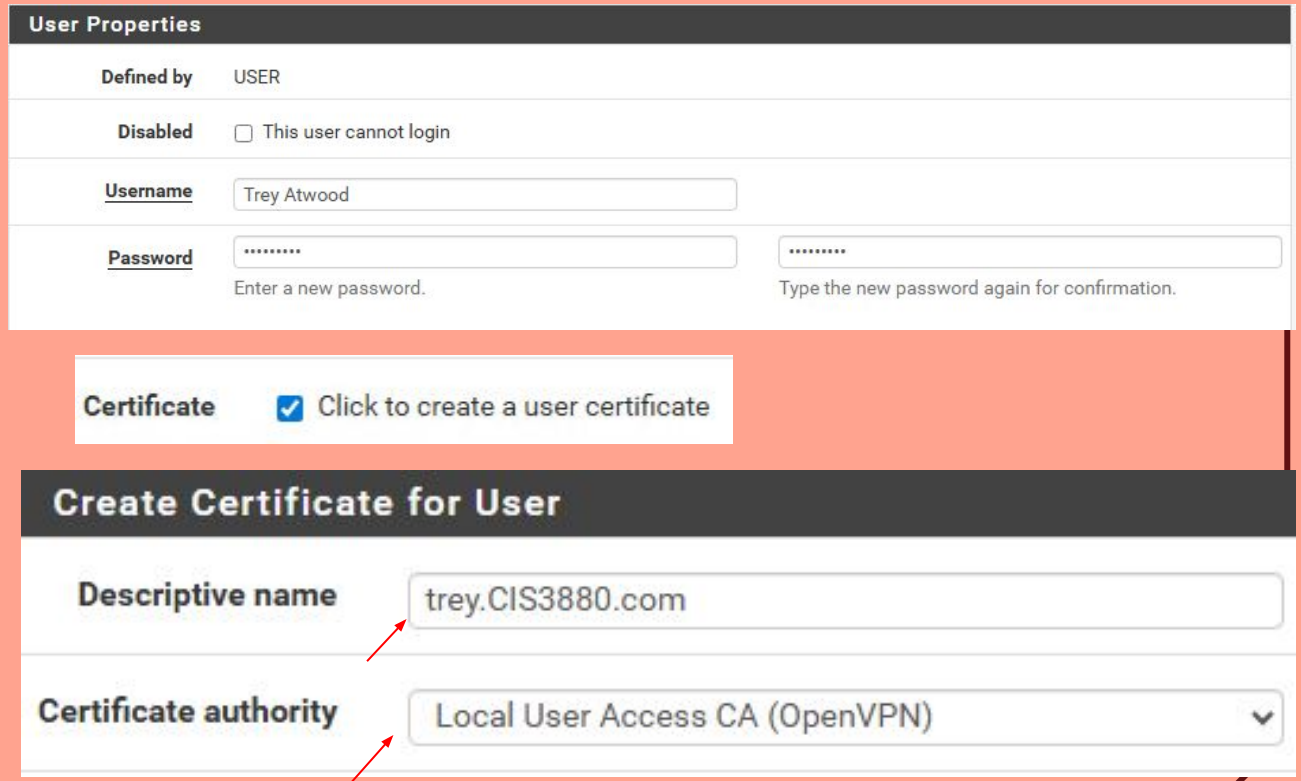
Next we need to set up a new User.





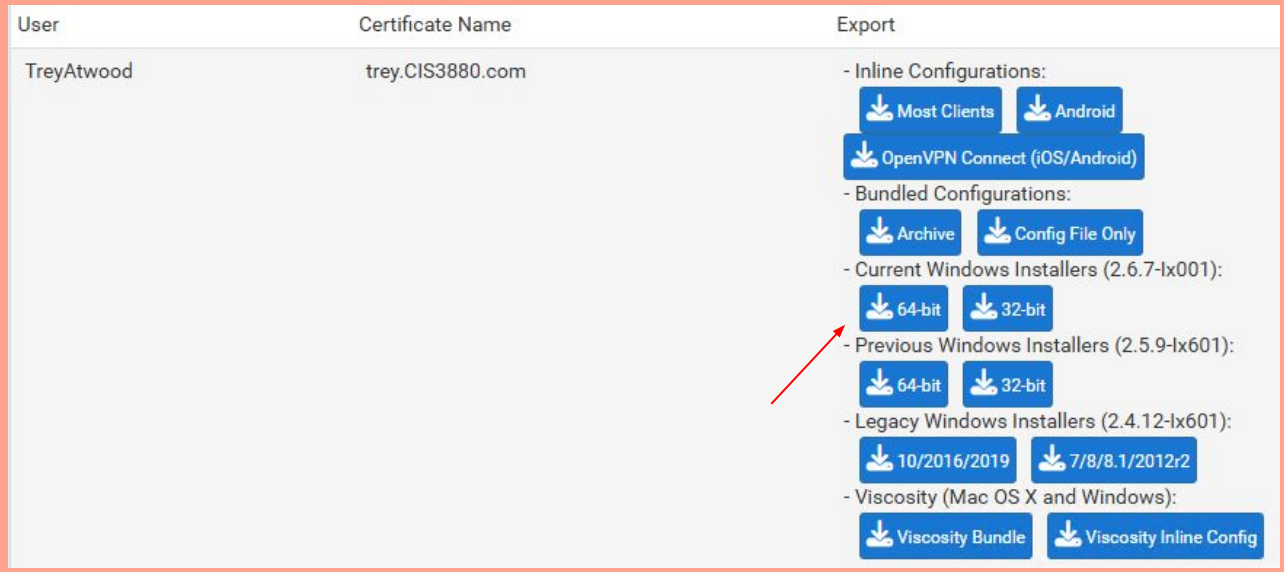
For the new user I used my own name “Trey Atwood” and set a password for my new user account. After setting up the username and password check the box that creates a new user certificate for the user.

When creating the new certificate for the user, I named it with my first name followed by the domain name that we are using for the VPN. And make sure you select the CA that we just created in the last steps as the CA for the user.

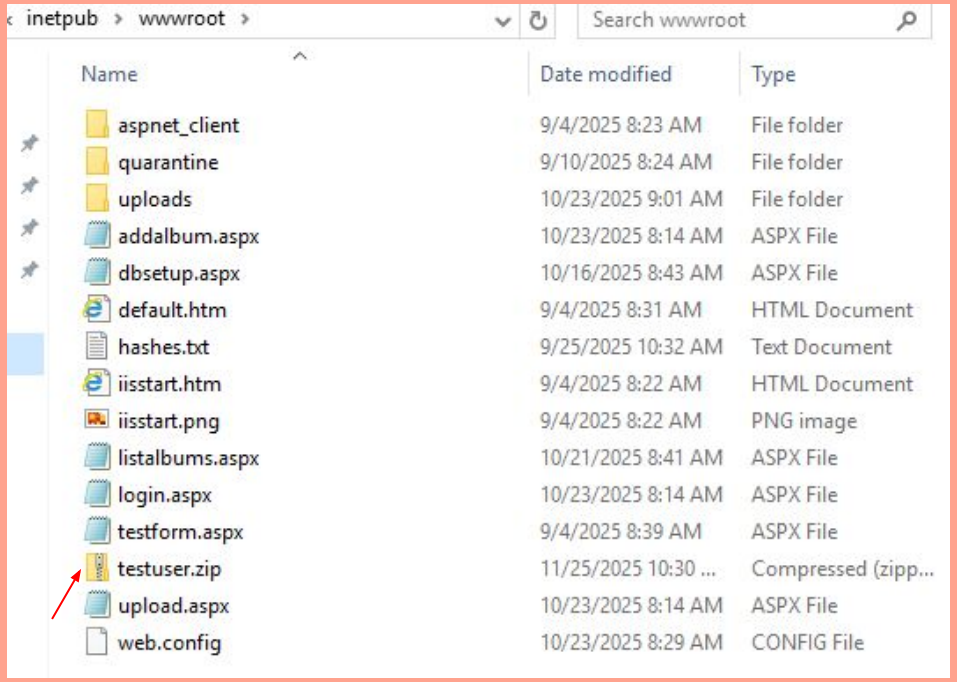


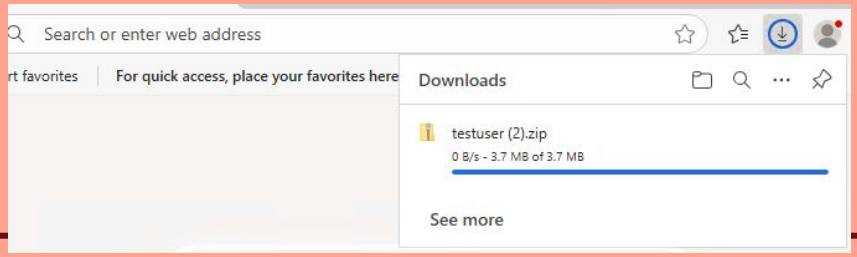
To export our client to our user through PFSense, we will navigate to our OpenVPN client list and download the current windows installed x64.

Once we download this we will need to move it over to our Azure machine so we can download and set up OpenVPN there. To do this I'll all the downloaded client file to my web server to make it easy to download on my Azure machine.



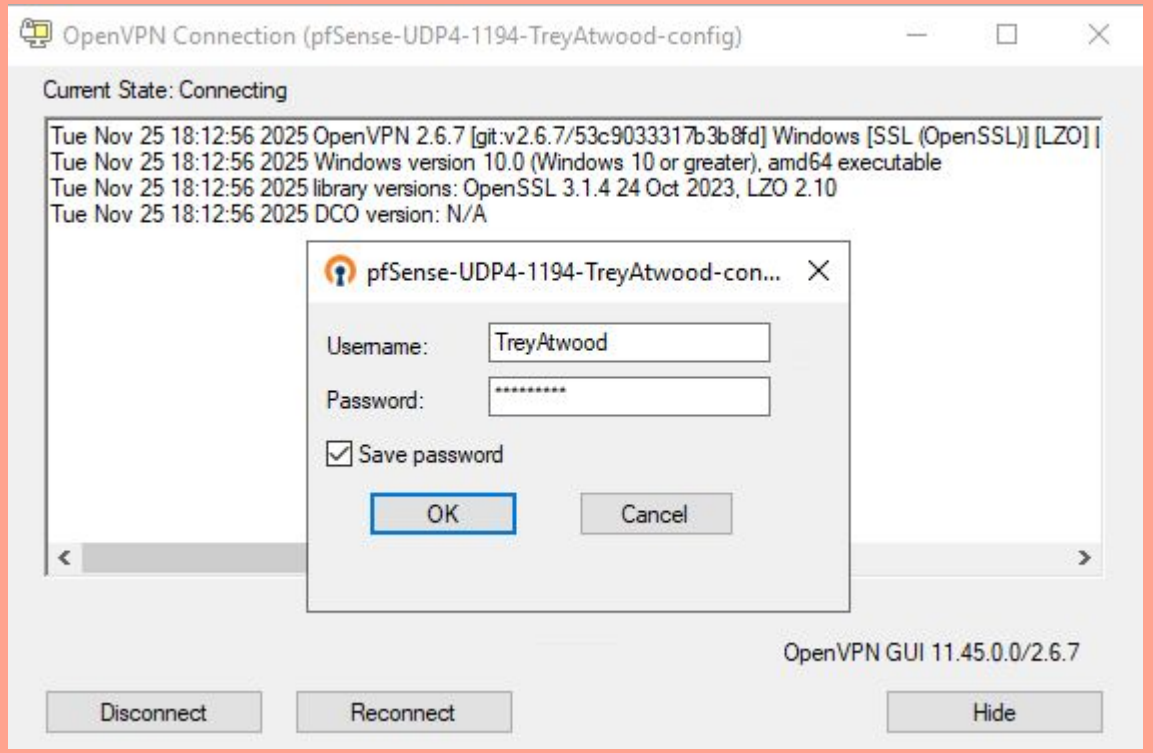
Here in my wwwroot folder I added the file test.user.zip which has the file we need to configure OpenVPN on the Azure machine.

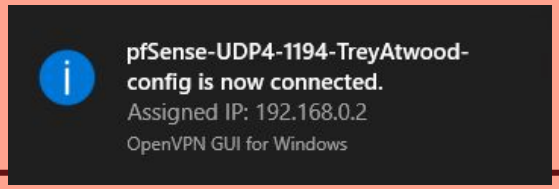




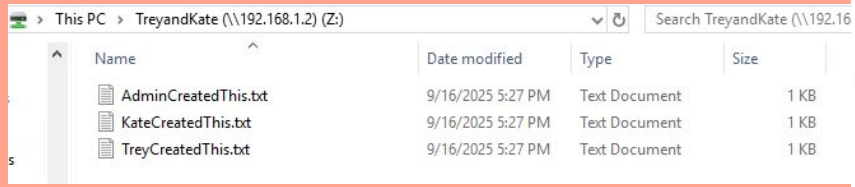
Now we need to install the VPN onto our Azure Machine to test to make sure that it works for our file sharing. Follow the setup wizards that come with the installation for OpenVPN and login with the user credentials.

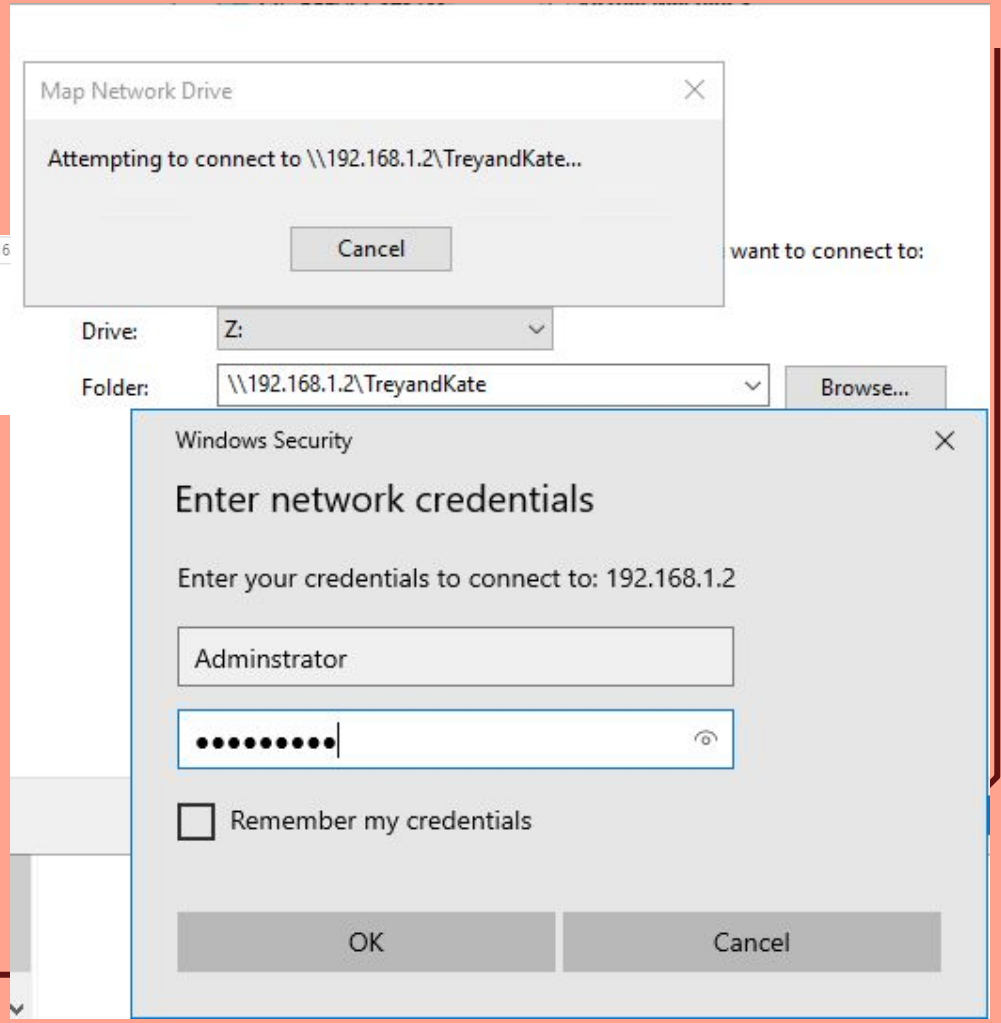
Here we login with the username “TreyAtwood” and the password I created.





To make sure that connection works, I'll connect to the shared folder that we created in a previous exercise.





To make sure that we can't access the file share without the connection of the VPN I'll disable the VPN and try to connect to the file share.

As you can see here windows isn't able to access the file share without an active connection to the VPN that we just set up!