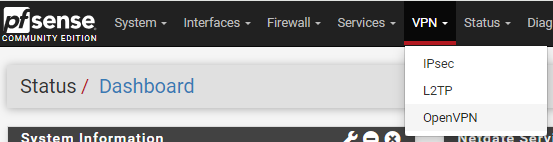
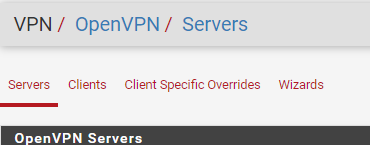
**VPN Server Configuration** – Complete on the Workstation that hosts your pfSense virtual machine.

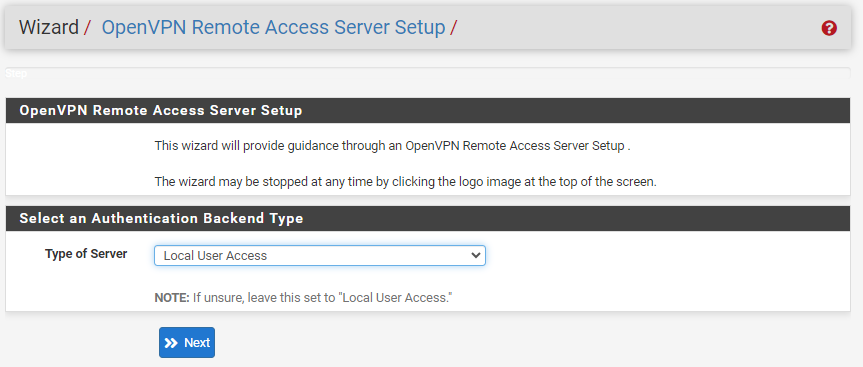
Open the VPN>OpenVPN menu item



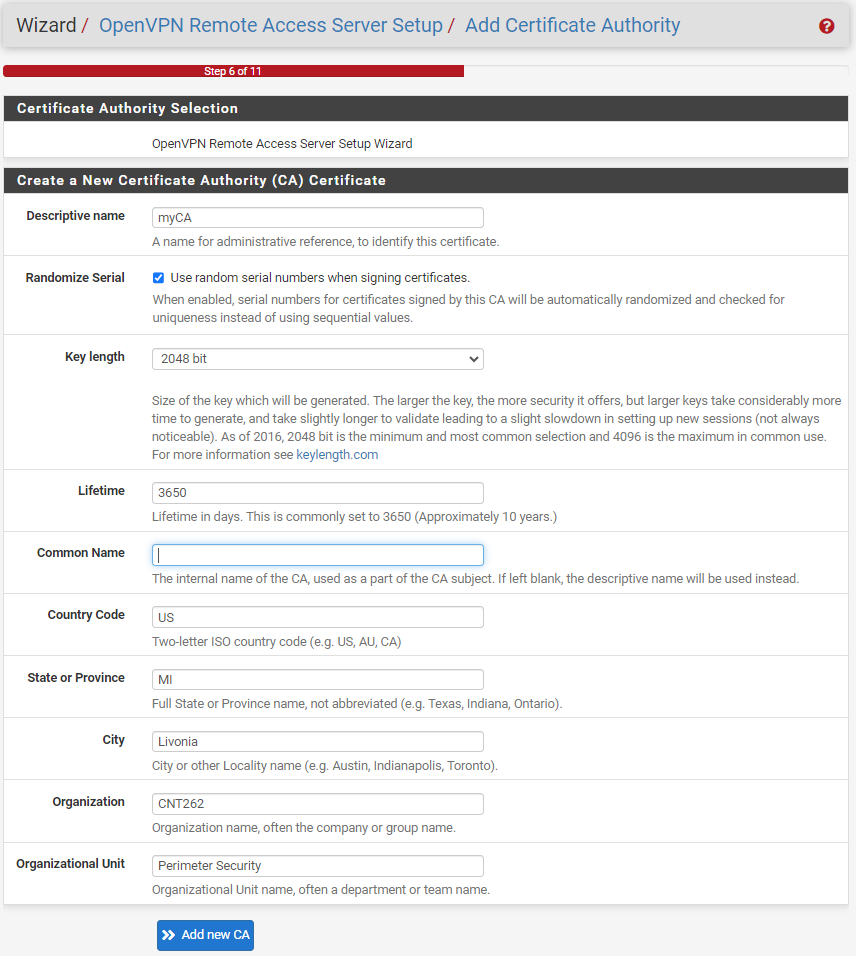
Once there, click the “Wizards” link at the top of the page



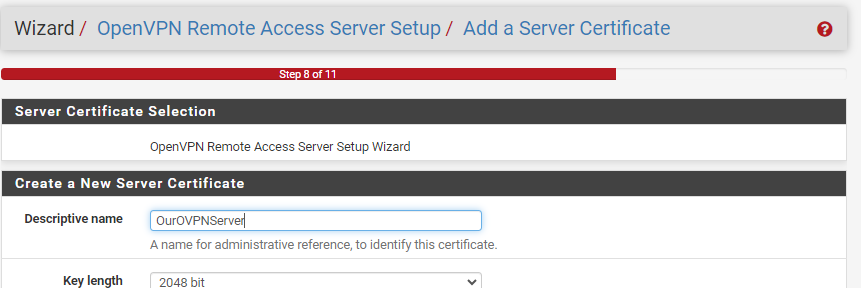
Choose “Local User Access”, then click “Next”



OpenVPN requires certificates to provide authentication and encryption functionality. Fill in the details as shown below to create an internal Certificate Authority within pfSense. When finished, click “Add new CA”



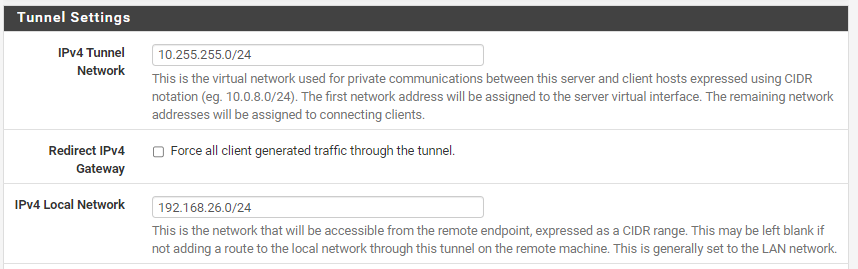
The next step is to create a server certificate. Choose a name for your server to be included in the certificate (the rest of the settings are auto-filled). Click “Create new Certificate” when done



The next page is where the bulk of the VPN configuration comes into play. It’s relatively simple, although it can be tweaked with many settings for improved security.

Use the following settings:

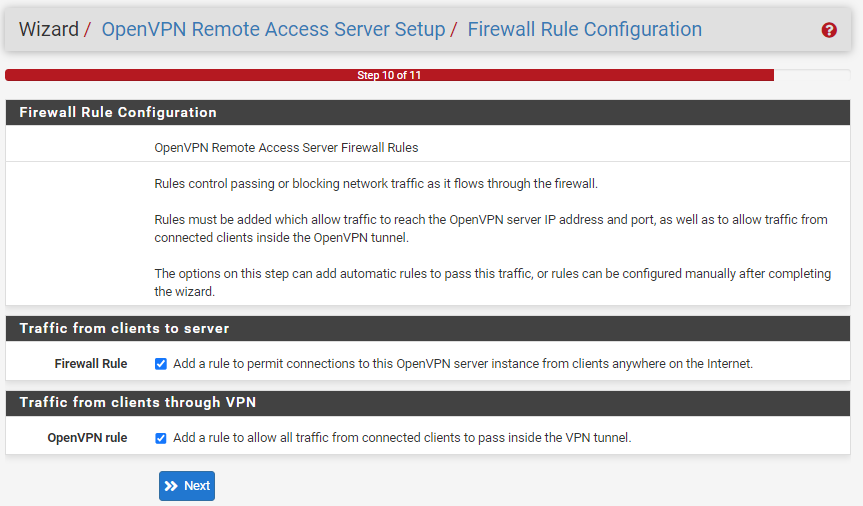
* General OpenVPN Server Information – Give a Description of “CNT262 OpenVPN Server”
* Endpoint Configuration – Leave Defaults
* Cryptographic Settings – Leave Defaults
* Tunnel Settings
  + Tunnel Network – **10.255.255.0/24**
  + Local Network – Use the subnet of your LAN network currently configured in pfSense. In this example it will be **192.168.26.0/24** because that is the network the LAN interface of the firewall is part of – yours will likely be different!
  + Leave the remainder of the settings at defaults.



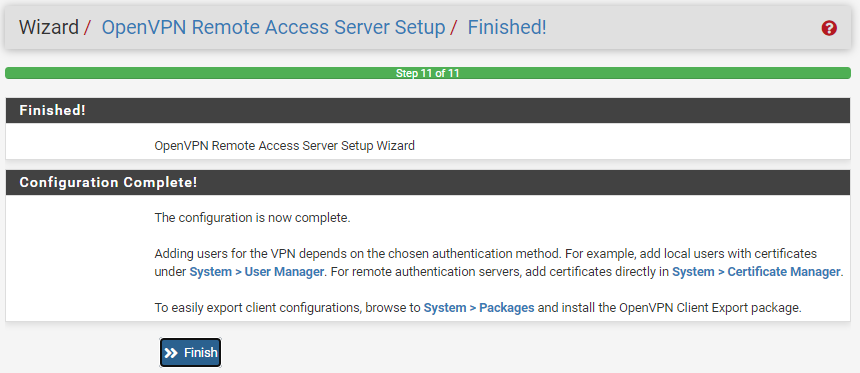
* Client Settings – Leave Defaults

When finished, click “Next”

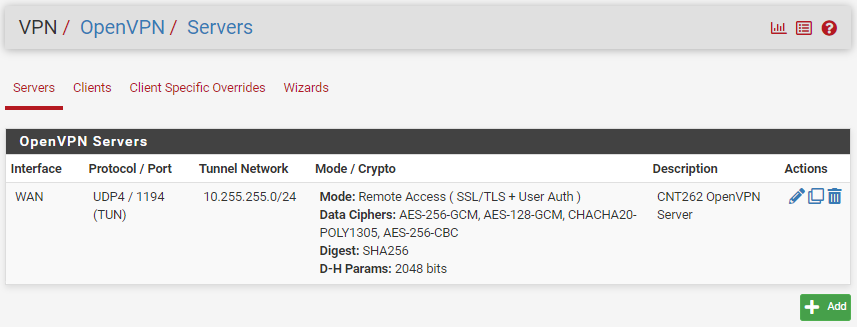
At the “Firewall Rule Configuration” step, check the “Firewall Rule” and “OpenVPN Rule” boxes. When ready, click “Next”



At the final screen of the wizard, click “Finish”

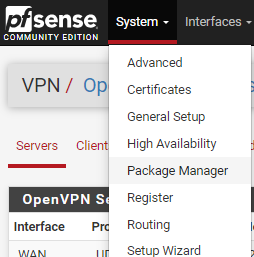


You should now see the newly created OpenVPN server instance – We’re not done yet though!

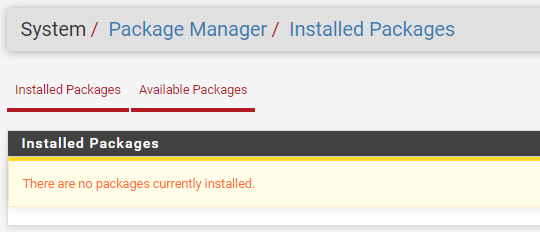


**VPN Client Configuration**

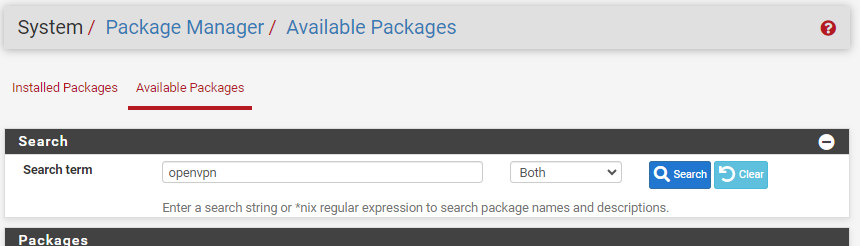
Open the System>Package Manager menu item



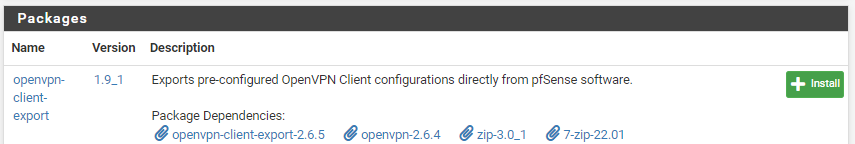
Click the Available Packages link



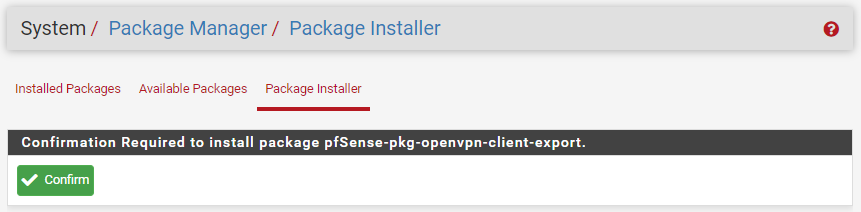
In the search box, type “openvpn”, then click the “Search” button



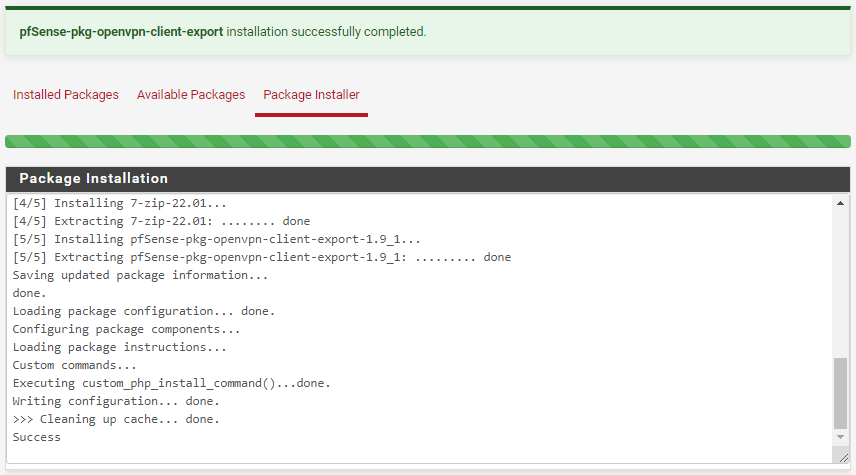
In the results, locate the “openvpn-client-export” package, then click the “Install” button



Click “Confirm” to continue installing the package

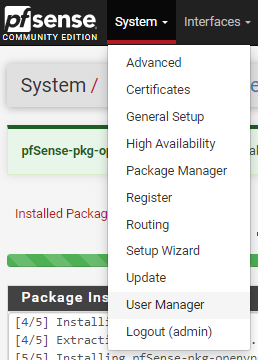


The installation process may take a few minutes. Monitor the progress bar for status. Once the package is successfully installed, we can continue to the user configuration portion of the setup.

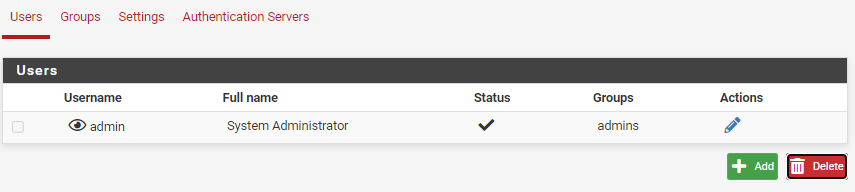


**Create VPN Users**

Go to the System>User Manager menu item



Click “Add” to create a new user for VPN remote access



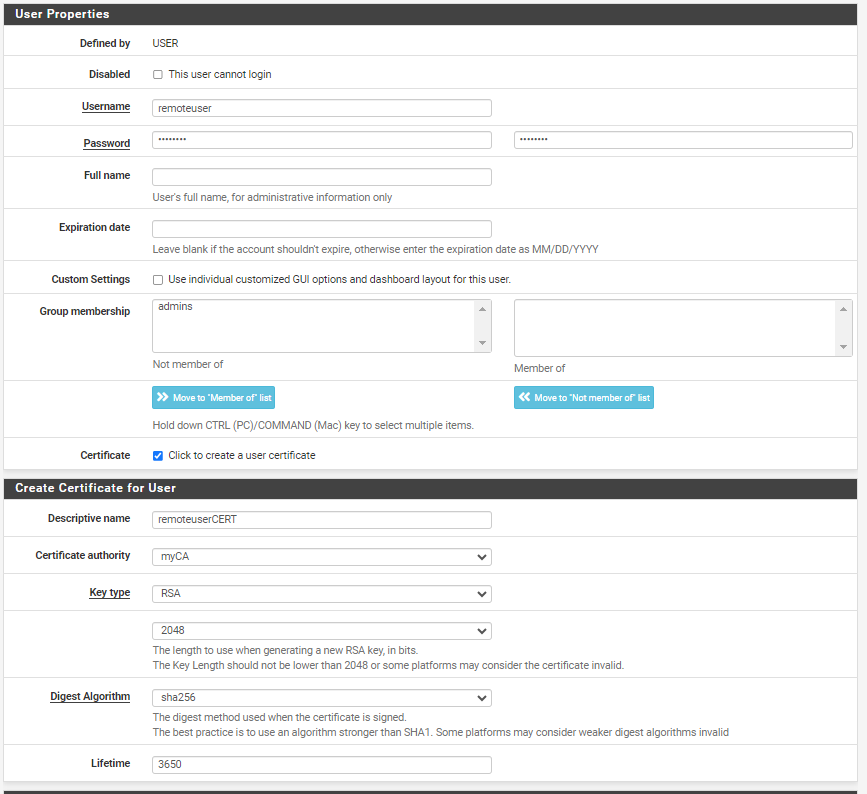
At the “User Properties” screen, fill in the user name and password (**use something you’ll remember!**).

**Check the “Certificate” box** to create a certificate for the user that can be used for authentication as well.

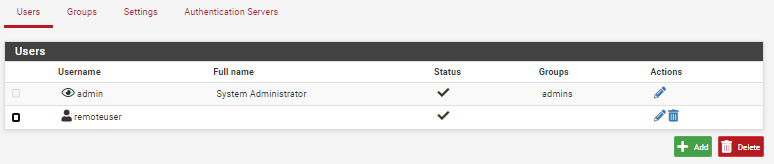
Provide a ”Descriptive name” of ***remoteuserCERT***

You can leave all other settings at the default.

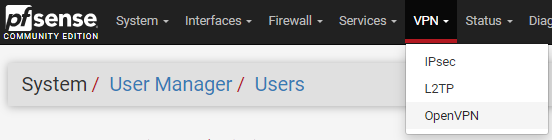
When finished, click “Save”



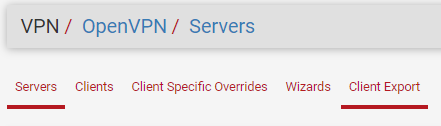
The new user will appear in the Users list



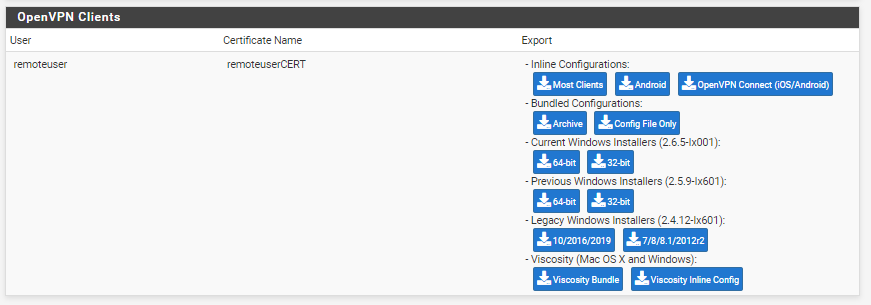
Go back to the VPN>OpenVPN menu item.



Click the “Client Export” link

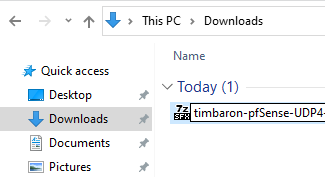


Scroll down to the bottom of the page and locate the “OpenVPN Clients” section



Click the “Current Windows Installer” link to download the Windows Installer that matches the version of Windows you are running (64-bit). This wizard will automatically include the necessary setup information for our clients (and for other operating systems other than Windows).

Once the file downloads, locate it on your workstation and RENAME IT so that it is obviously yours.

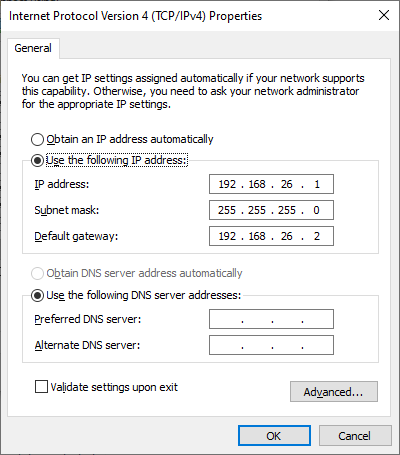


We will need to copy it to another machine within the classroom to emulate an Internet device connecting to the WAN IP address of the firewall. Use a USB stick or ask your instructor for assistance getting this file on another workstation so that it can be installed. Before we do the install though, we have one more task before we can complete testing the VPN connection. **Do this before continuing with the next step.**

**Preparing the Test/Housekeeping**

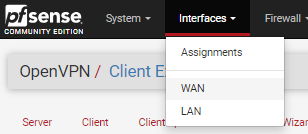
To test the VPN connection, we need to be able to show that we can access something on the internal LAN network of the firewall we setup as a VPN server. Perform the following steps on the PC that is host to your pfSense VM:

1. Using the steps from the Week 7 Activity, download/extract/open the USBWebServer8.6 application on the computer where you have your pfSense virtual machine.
2. Make sure to set the default gateway of the VmNet8 adapter to the IP address on the LAN interface of your pfSense virtual machine. This is an example, use a value appropriate for your machine.

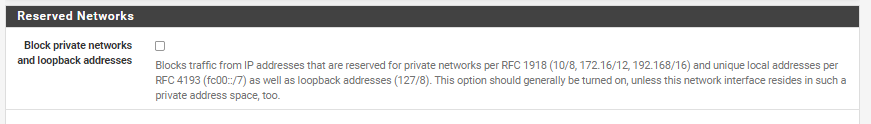


We also need to verify that RFC1918 (IPv4 Private) IPs are not being blocked by the WAN interface (we only need to do this because we are working in a LAN that uses private IPv4 addresses).

Navigate to the Interfaces>WAN menu item



Scroll to the bottom of the page and verify that the “Block private networks and loopback addresses” option is NOT checked (or uncheck it if it is)



Save and apply the changes.

You are ready to move on to the Client Configuration and VPN testing portions of the Lab