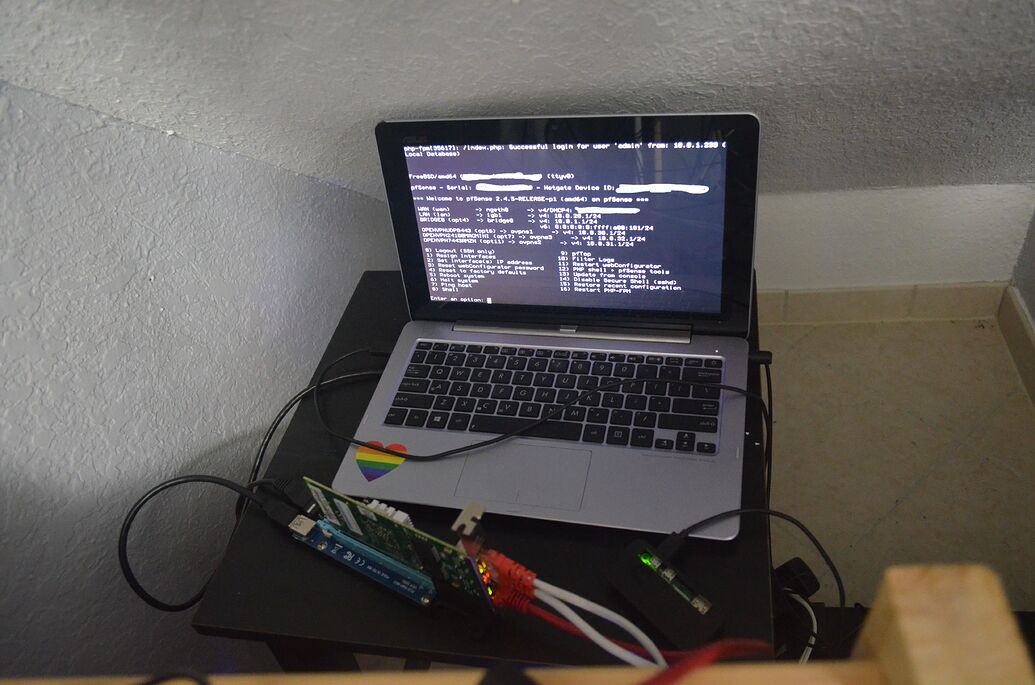
PfSense Configuration and Remote Desktop

Reed Holman | Cyber Security | 11/1/2022



Purpose:

The purpose was to load PfSense onto a flash drive then boot a laptop from that drive. We would then configure both a LAN and a WAN interface and set up a DHCP server for the LAN network.

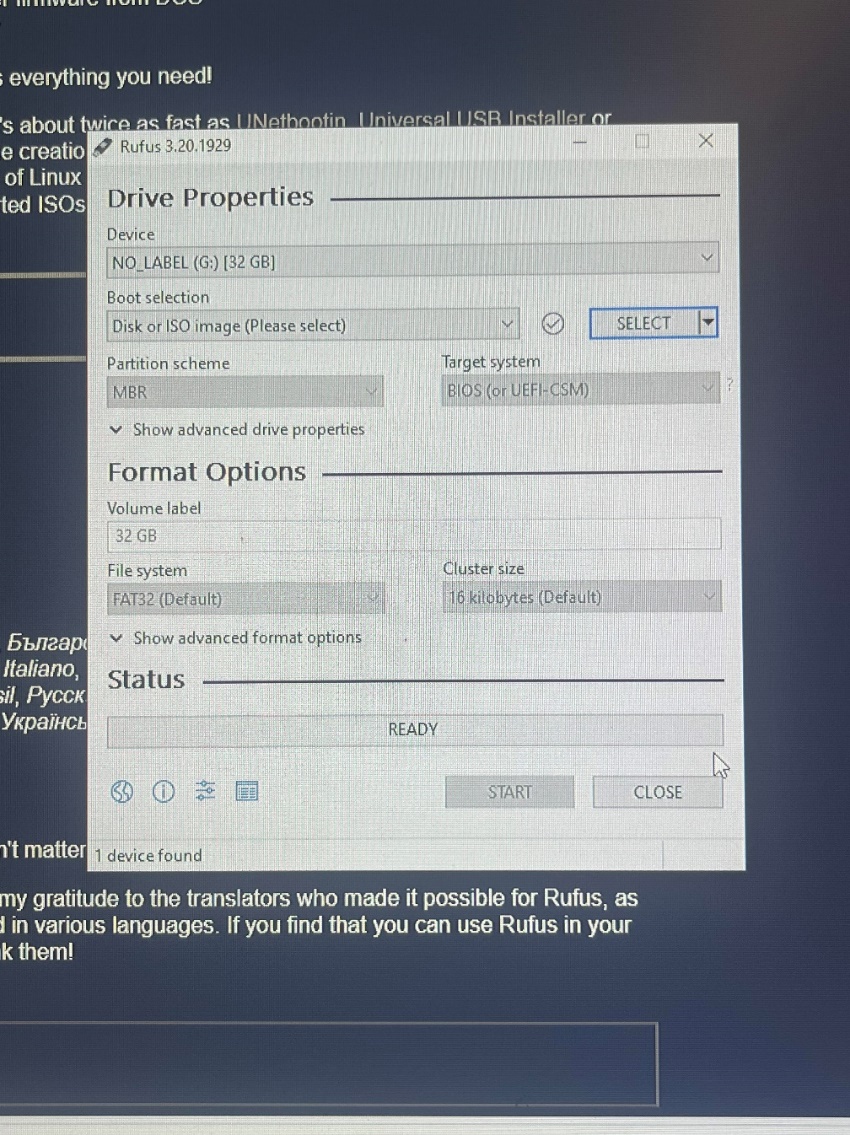
Background:

PfSense is an open-source firewall/router software created in 2004. That means anyone can downland and install it onto their physical devices or virtual machines. PfSense is also very user friendly because almost imminently you can start configuring from their web UI. PfSense has quite a few features like traffic shaping, VPNs, stateful firewall and more.

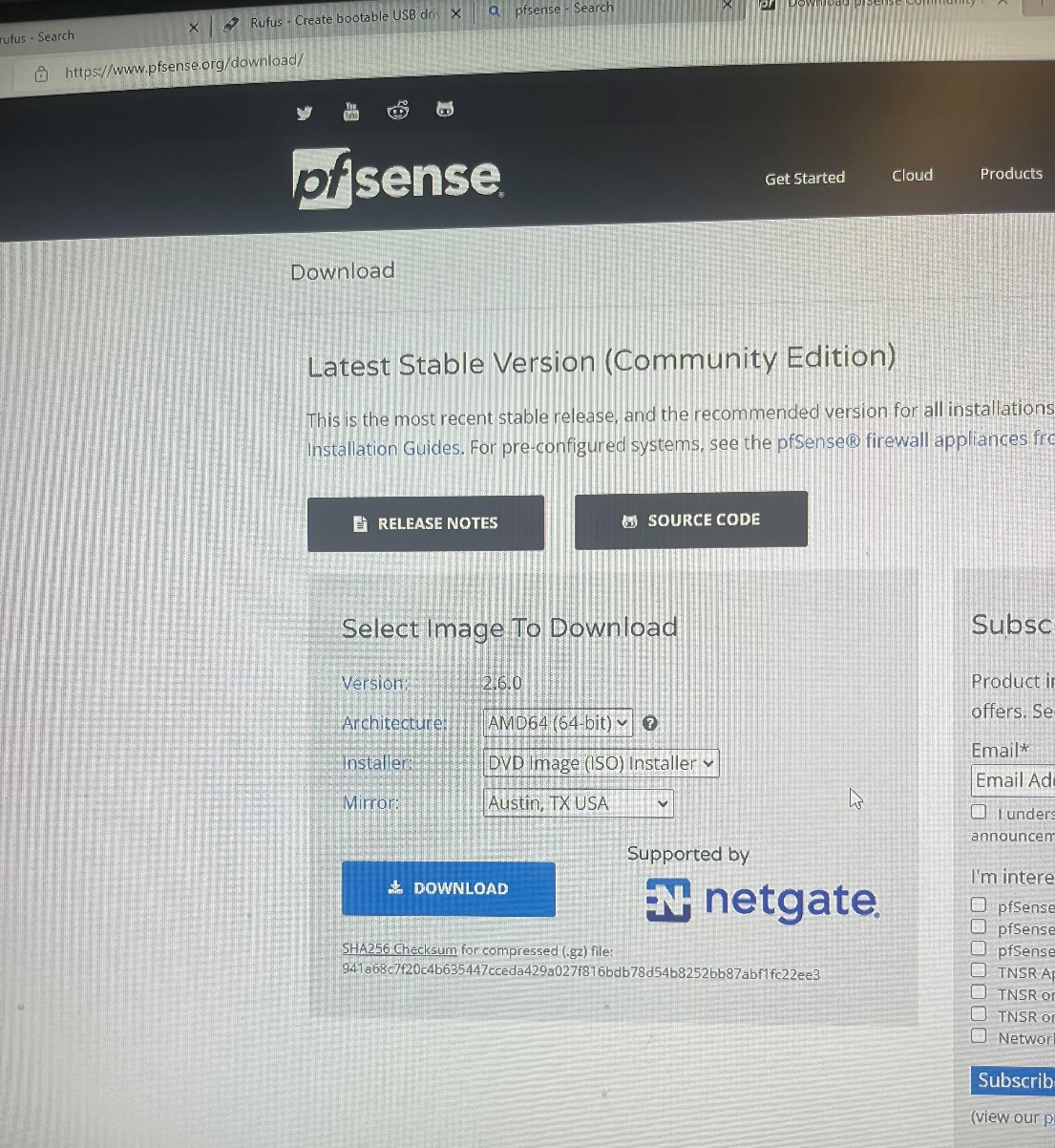
Traffic shaping is a way to control the amount/ type of traffic that goes through your network. This allows us to reduce congestion and latency. A Virtual private network or VPN allows us to set up encrypted connections between different devices. This can enable be who are working from home to access the network securely. The stateful firewall is an important feature of an PfSense. A firewall is something that will help filter traffic and protect your network. A stateless firewall only looks at the header of incoming packets which only contains basic information like source and destination. A stateful firewall is a lot more secure but looks at everything in the packet so it more information to decide and keep your network safe.

Remote desktop is a program that allows a device to connect to another and control it remotely. This can be very useful for companies and other organizations because of the increased number of people working remotely. IT members might find it necessary to access someone’s device to help them fix an issue when they physically cannot access a device. The remote desktop protocol uses port number 3389. The router must be forwarding port 3389 for remote desktop to work properly. There are security concerns that come along with using a protocol like remote desktop. You do not want someone using remote desktop on device in your network that is not supposed to. To safeguard against this, you want complex passwords and strong network policies. Remote desktop is a fairly easy protocol to set up but can be very powerful for managing devices in your network.

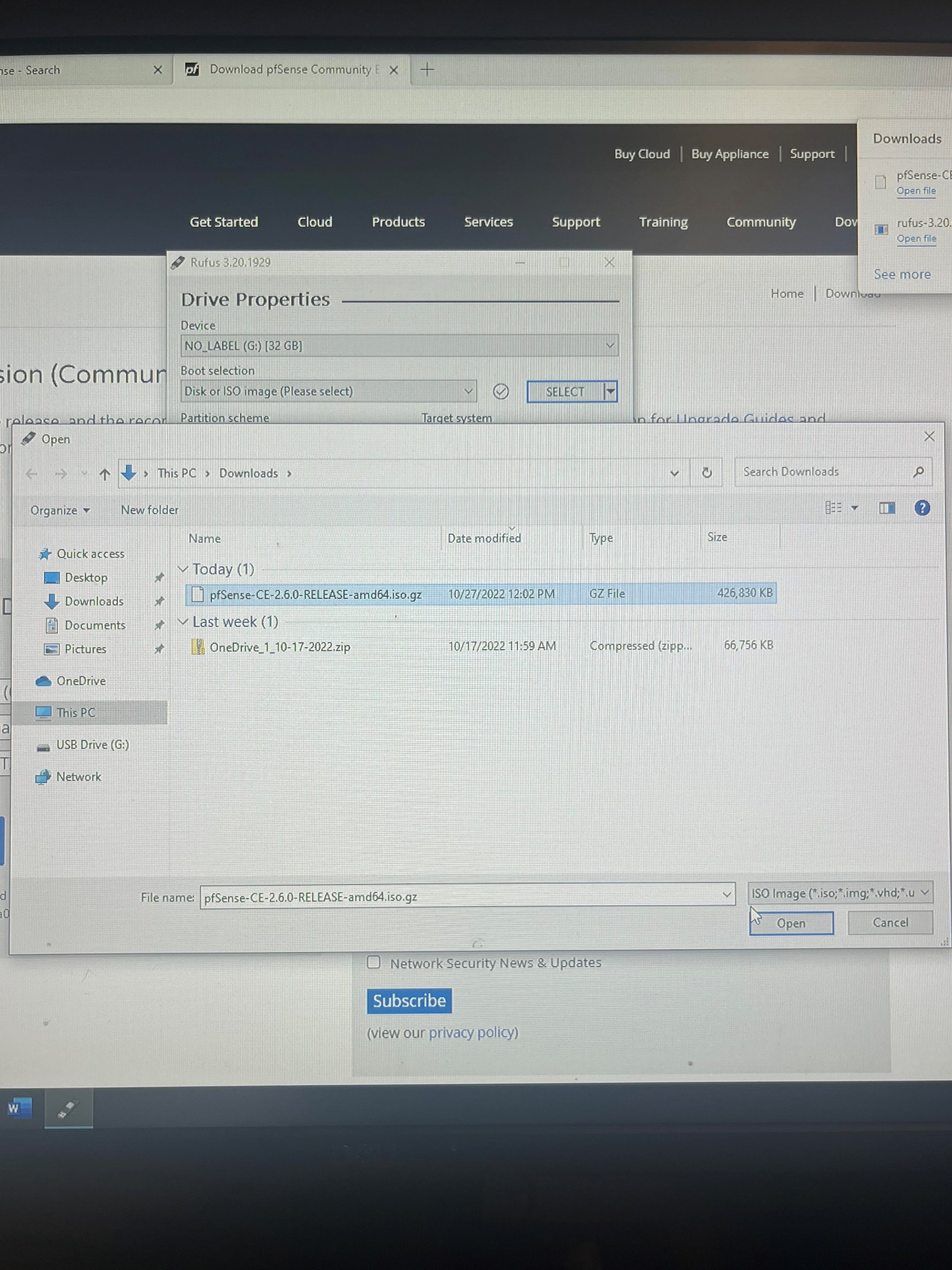
Configuration:



Step 1: Use Rufus to install PfSense onto a flash drive



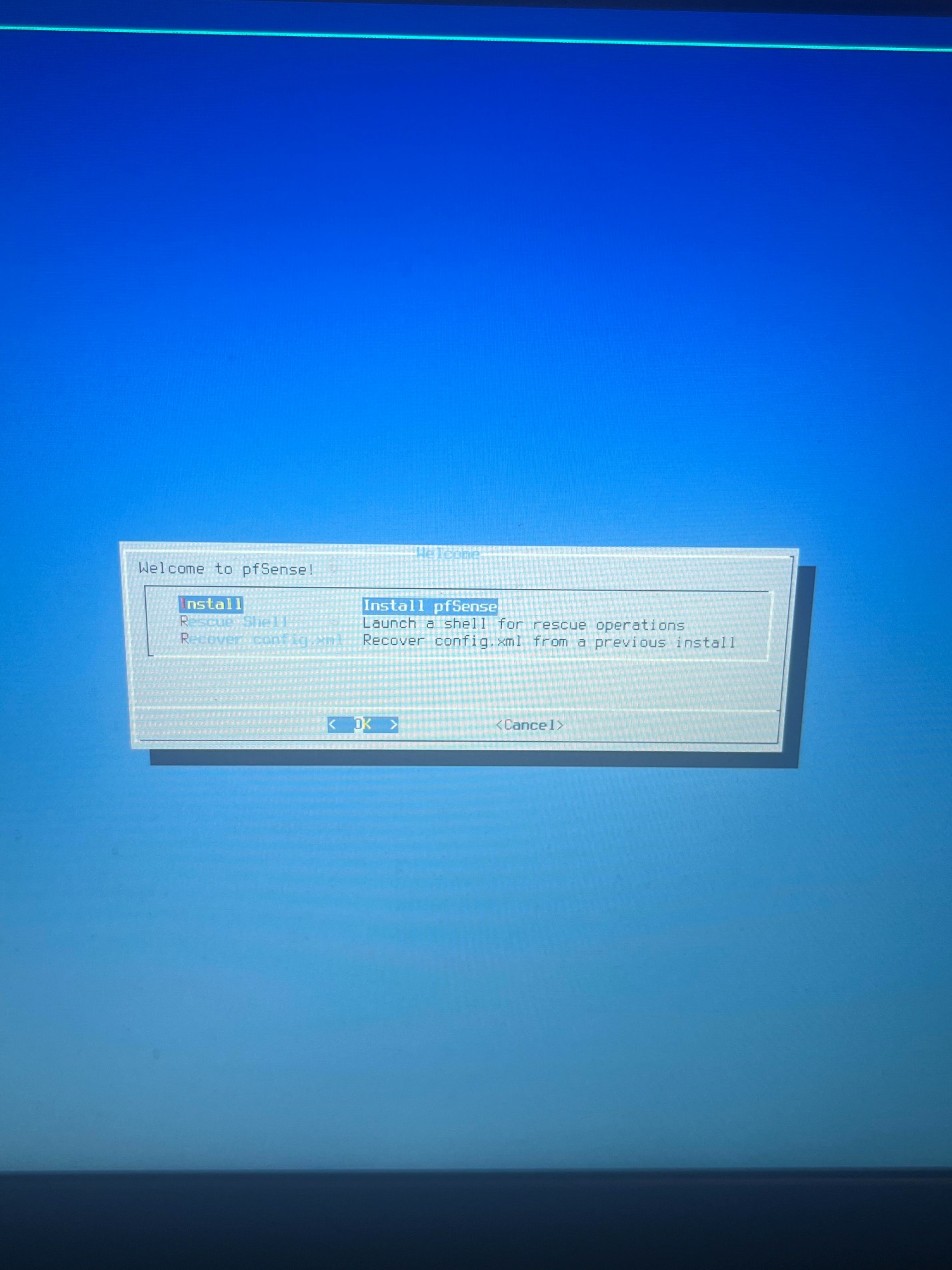
Download the AMD64 version



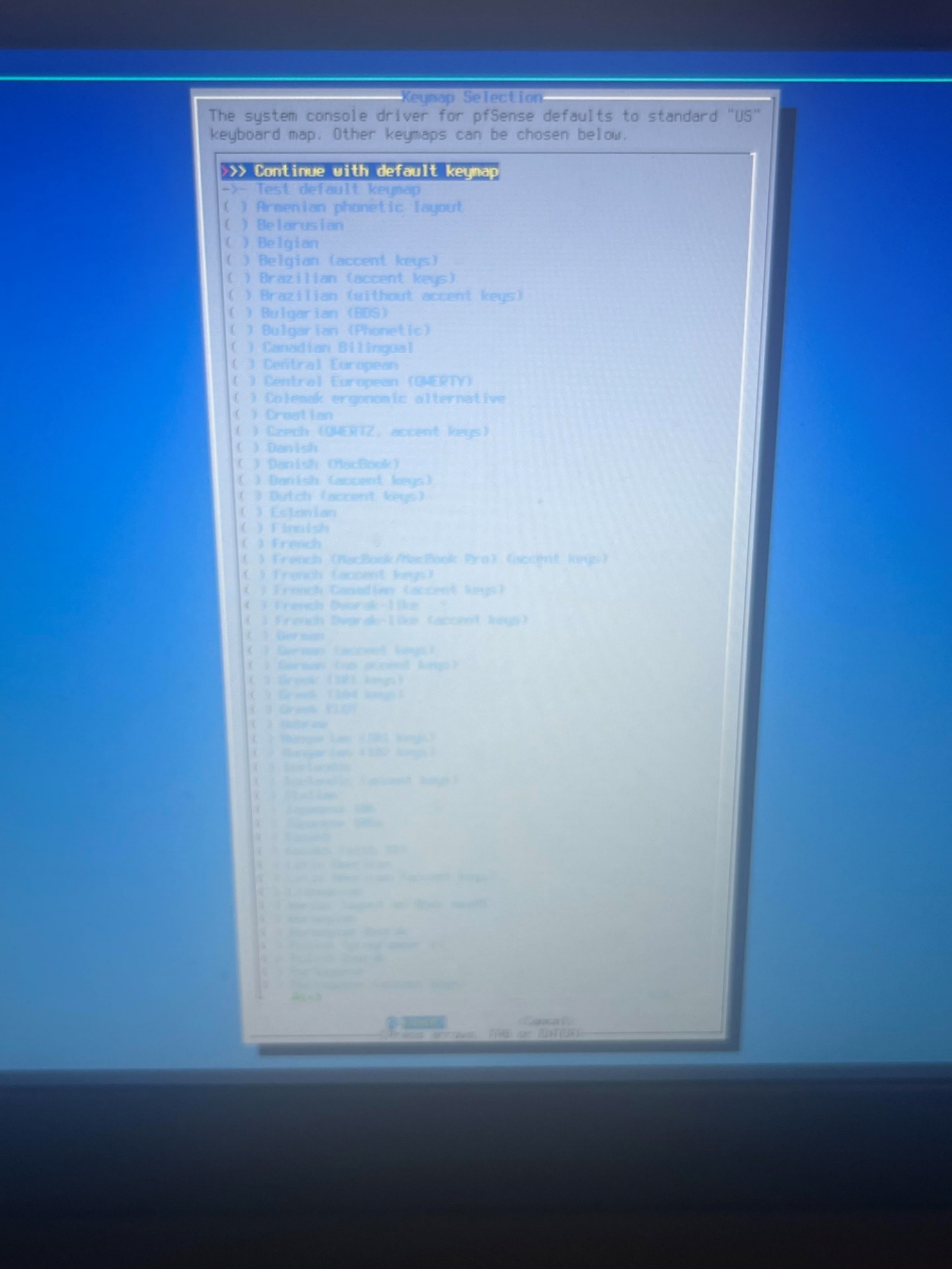
But the PfSense amd64 file onto the drive using Rufus



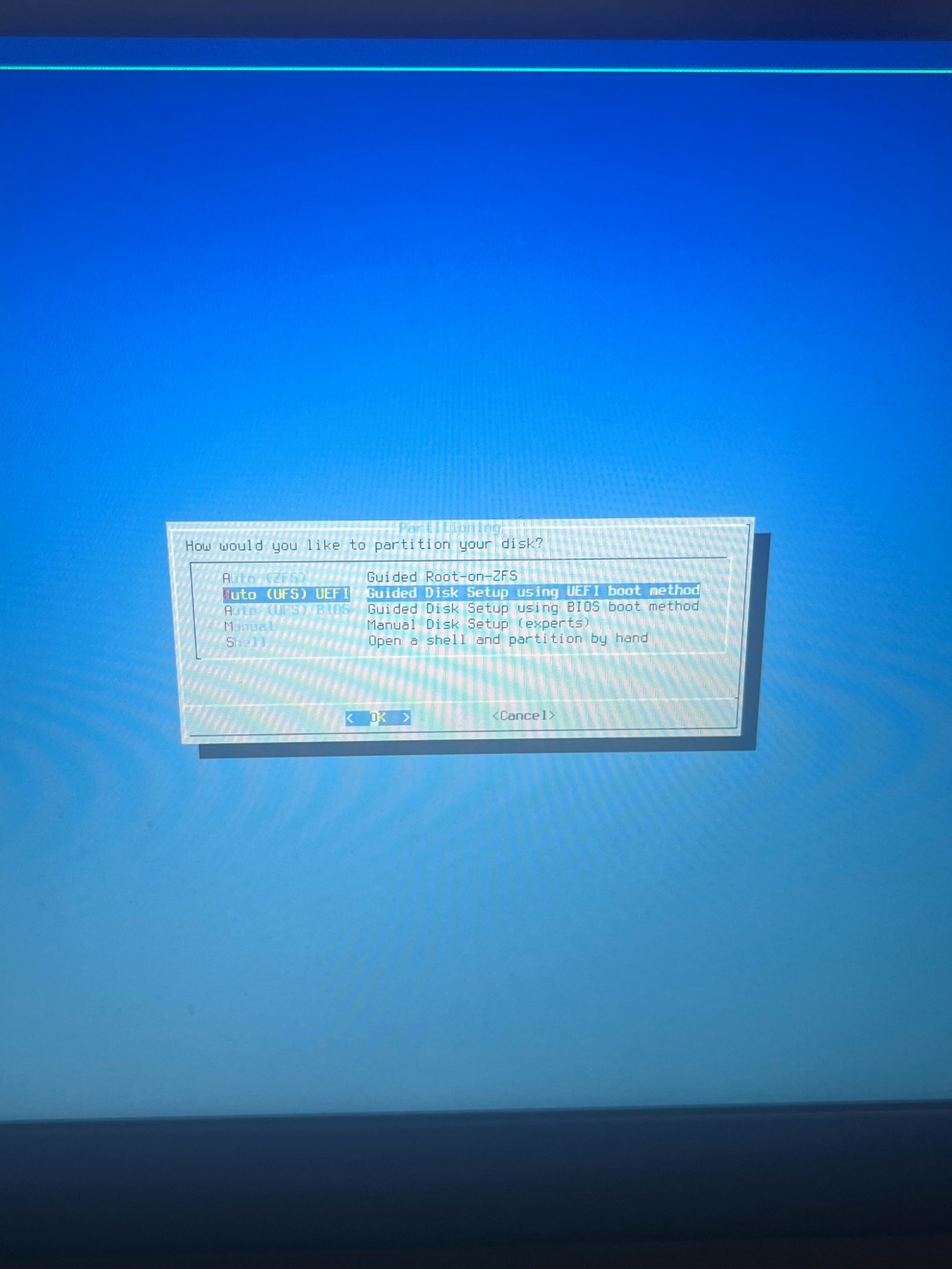
Plug in laptop to internet and into local network.



Install PfSense onto laptop



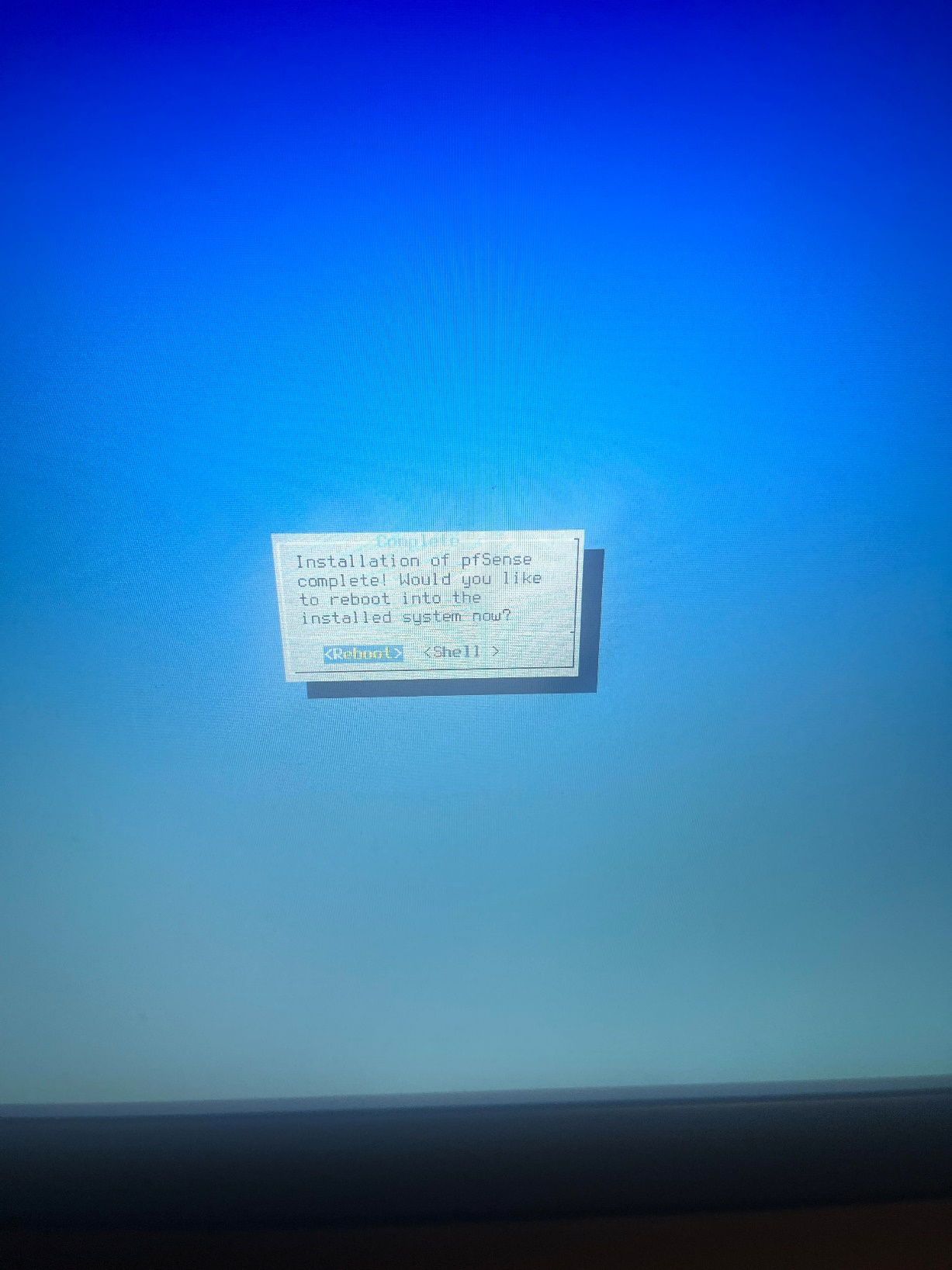
Use default keymap



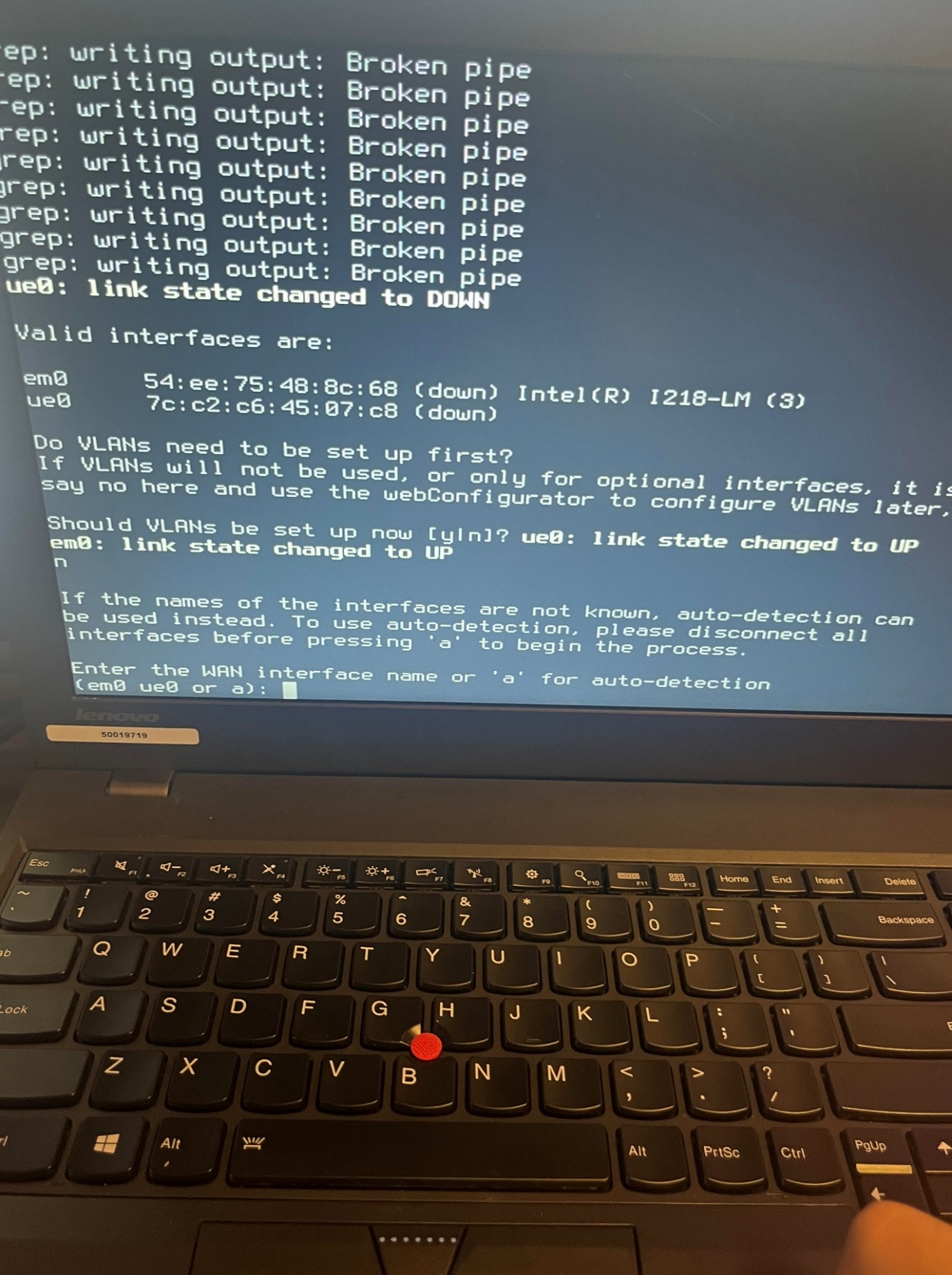
Use the Auto UEFI to partition your disk



Click No, to manual Configuration



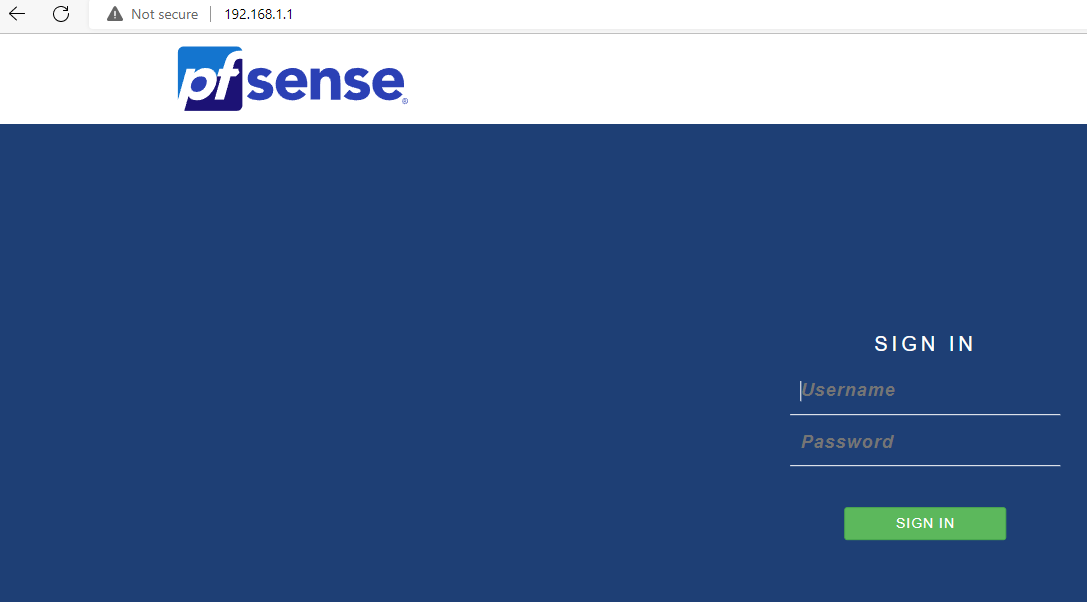
After PfSense is fully installed reboot device



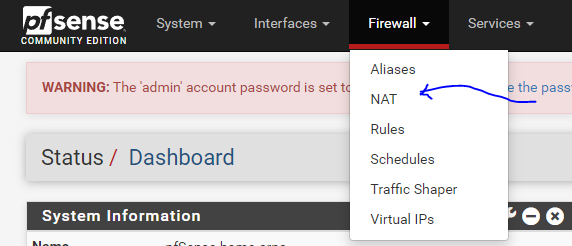
Set which interface is for what network



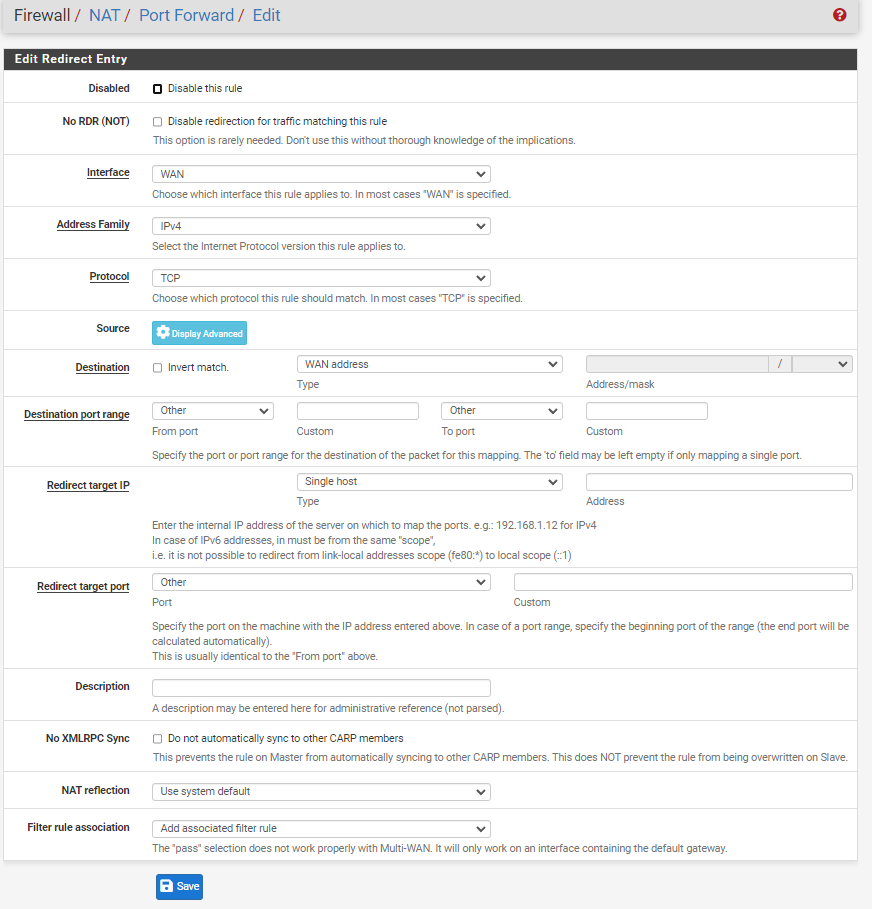
Set interface(s) IP address to access the webConfigurator



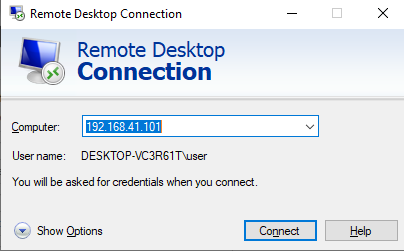
Login using default information



Go to the Firewall dropdown and select NAT.



Make sure Destination says WAN address, and the Destination port range uses 3389 which is Port forwarding. Put the IP address of the PC you want to connect to in the Redirect target IP section.



Problems:

One of our main problems was that we did not have passwords on our pcs (don’t yell at us). Without passwords you are unable to use remote Desktop so even though we had set up everything correctly we could not connect to each other’s pc. Our other major issue was we did not know exactly what we needed to do so we spent a lot of time just trying random things to see what would work. We were over complexing things and once we learned we just needed to create a NAT rule to forward the right port it was simple.

Conclusion:

This lab was very interesting, and I enjoyed it so much I did the lab again at my house with an old laptop I have. This lab is so accessible to anyone, that is why I think it was such an important lab to learn.