Sirjan Singh | Cybersecurity | P5



Lab 5 – Pfsense Setup and Remote Desktop

Background: Pfsense software plus is a firewall that can be installed on a physical computer or a virtual machine. It is free to use and open-source and can be managed entirely via a web interface. It is currently ranked 2nd best firewall solutions. It can provide VPN, firewall, and router functionality to homes, businesses, educational institutions, and government agencies. It is a cloud based infrastructure with features including intrusion detection and prevention, load balancing, traffic shaping, GeoIP blocking, dual-stack IPv4 and IPv6 support, DHCP and DNS server, Domain Name blacklisting, multiple VPN.

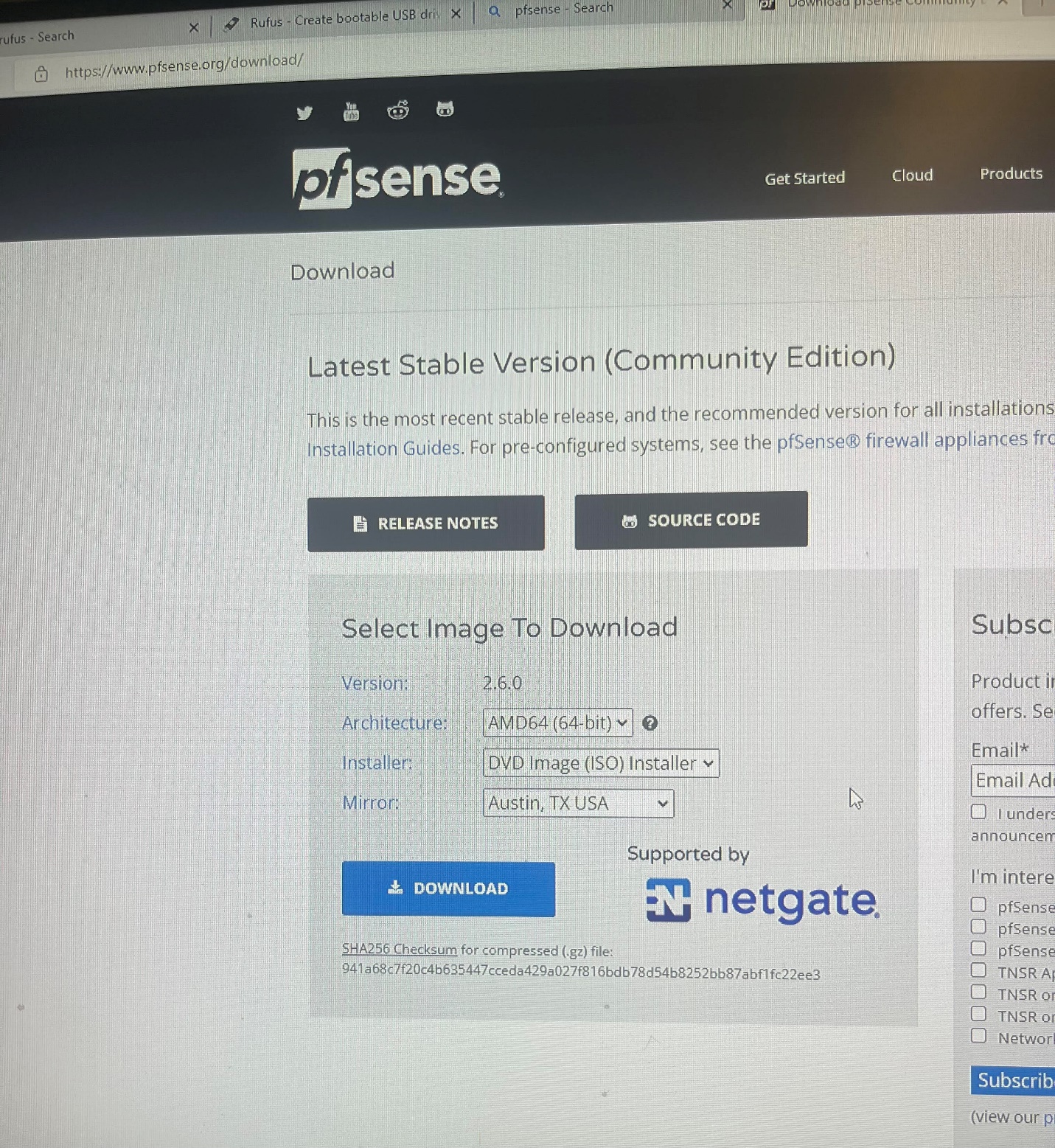
In our lab, we made a bootable flash drive with rufus and downloaded pfsense on it. Then, we took a lenonvo laptop and booted that flash drive into the laptop with the hope that the computer would simply become a firewall. This is a really powerful function for a SOHO because is one does not want to invest in a new, expensive firewall, they can simply use an old computer and put it to great use for online security!

After booting the PC with pfsense, we configured 2 interfaces on the firewall: LAN and WAN. The WAN interface connected straight to the internet through wire, and the lan interface directly connected to a 2750 switch. On that same switch, we connected the 2 PCs we had too. That way, our 2 pcs were now able to get internet through the firewall which was connected to WAN (internet) and we were now on the same network (LAN) as the firewall. After assigning interfaces, we assigned out LAN an address and subnet. Once that was assigned, we simply put the IP address of our lan became the management interface and we were able to access its web GUI.

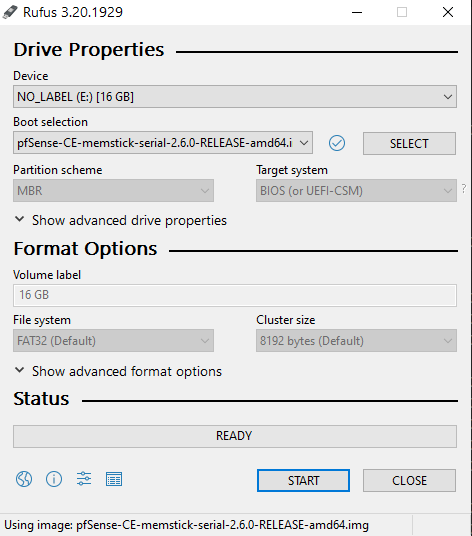
The last step to configuring the SOHO was simply setting up the LAN interface of the firewall to be a DHCP server. The WAN interface on the other hand was a DHCP client that got it’s IP from the internet. After this, we changed our topology a little to test remote desktop. We simply plugged one of the PCs to the internet and it was now part of the WAN. With just a simple port forwarding trick on the firewall, we were able to make it so that the WAN pc could remote desktop to the LAN pc through the firewall.

Lab Steps:

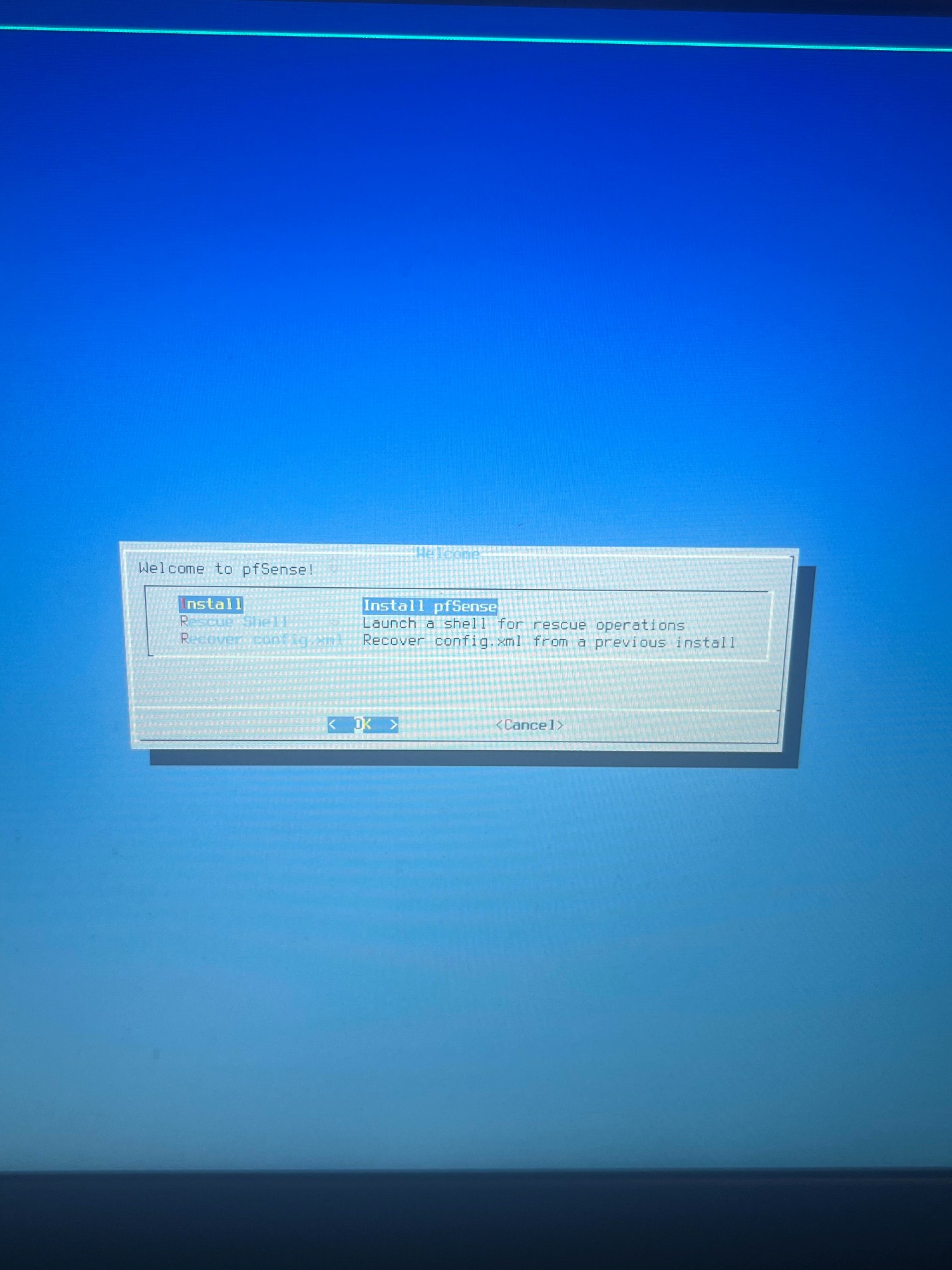
Step 1: Go to the following website to download pfsense on a connected flash drive.



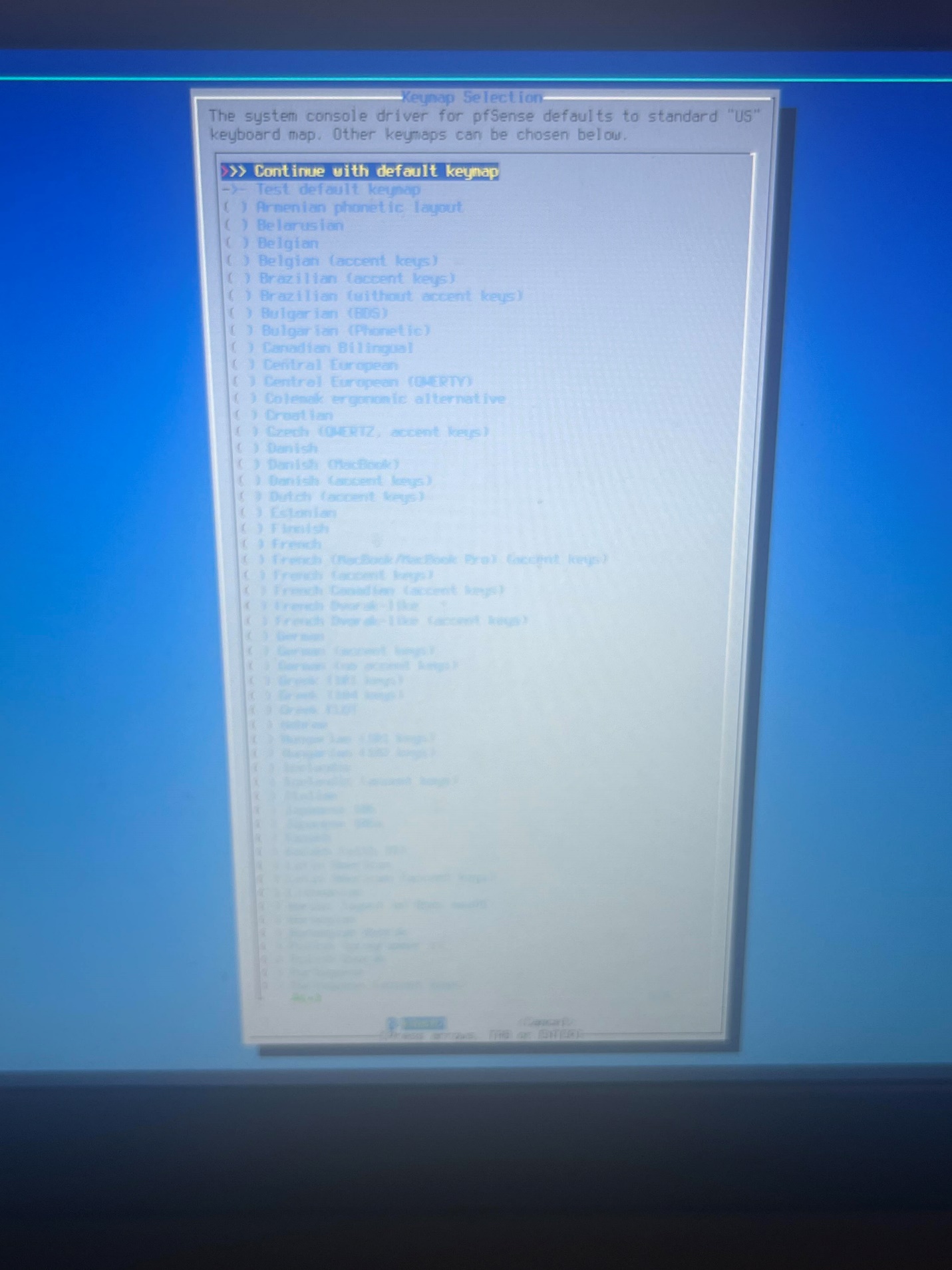
Step 2: Then, to make your flash drive bootable for pfsense, go to rufus.ie/en and click download. Then open Rufus and enter in the following configurations



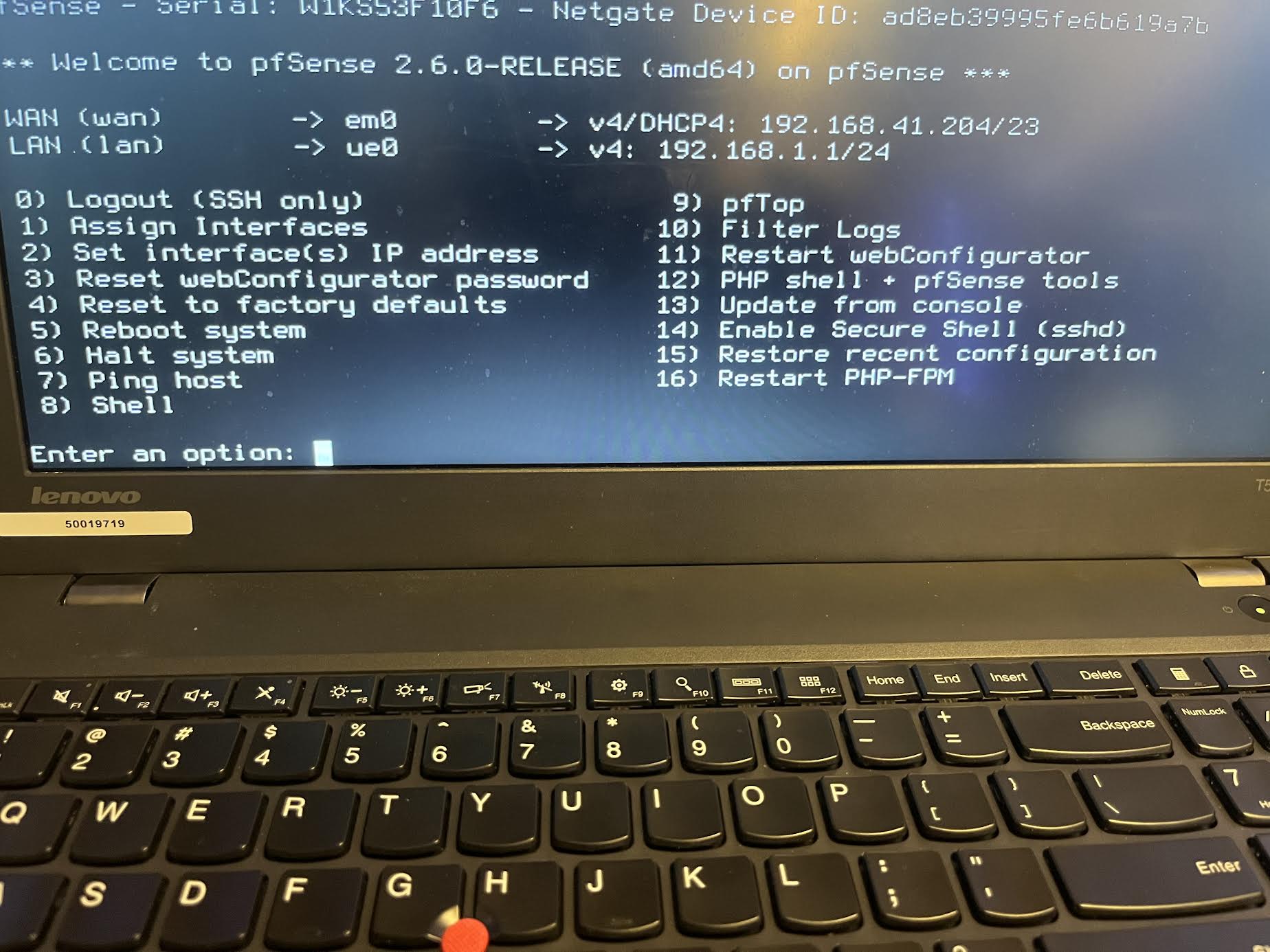
Step 3: Plug your now bootable flash drive in the laptop that you wish to make a pc. Switch on your laptop and go to bios mode. Boot the flash drive onto the computer. Install Pfsense.

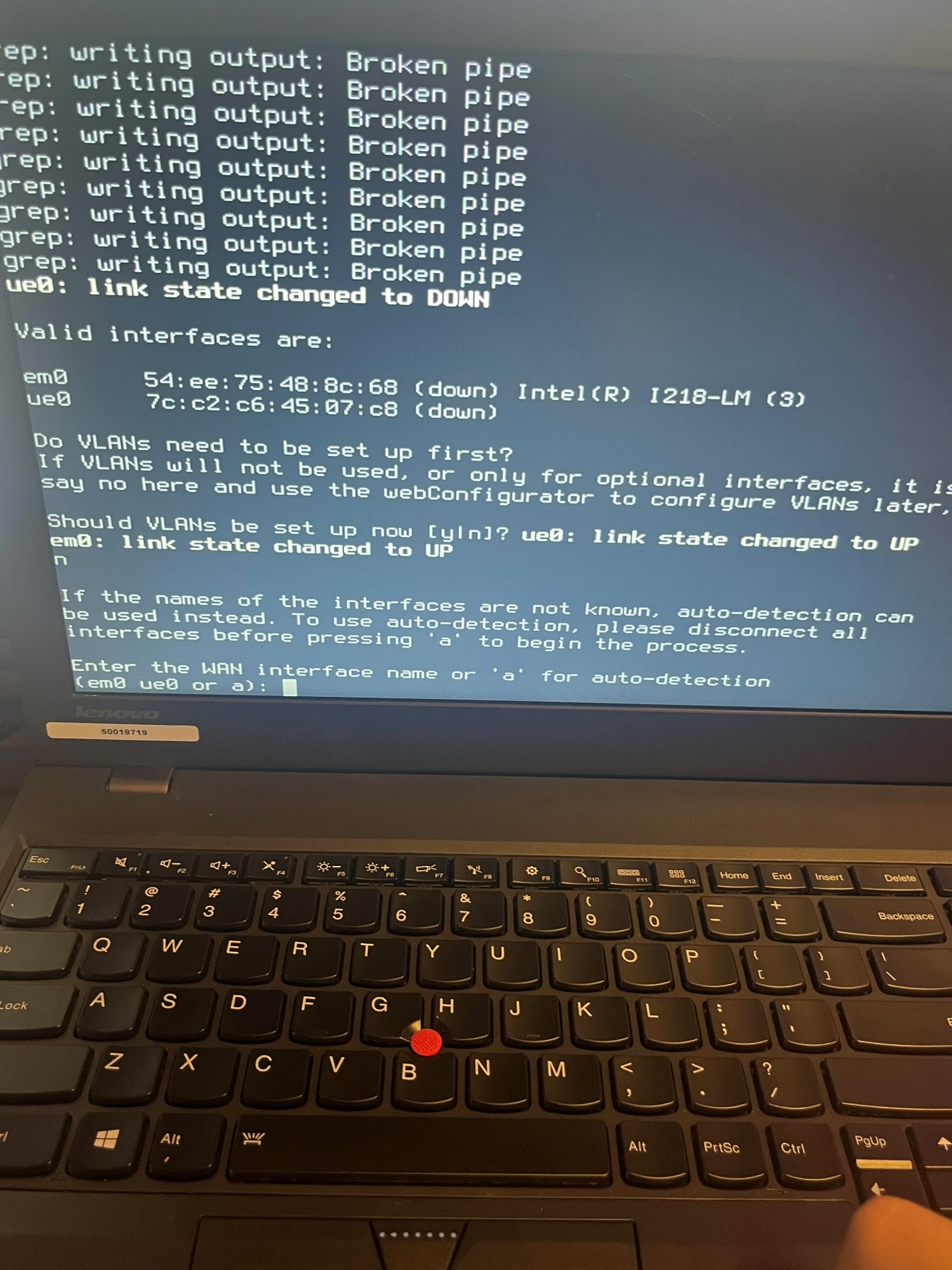


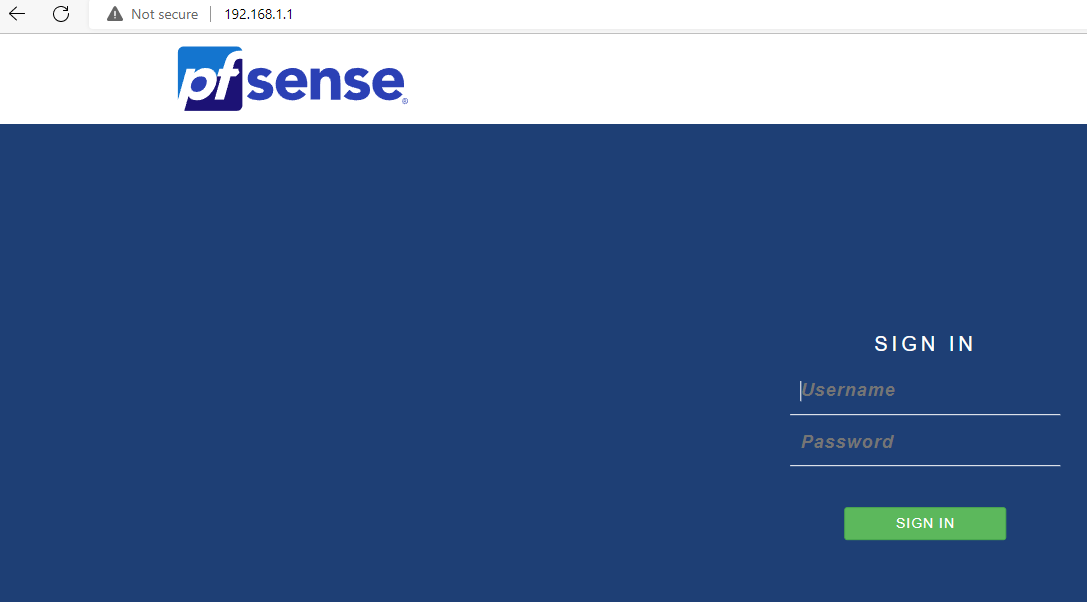
Step 4: Continue with default keymap



Step 5: The result should be the following screen. After this, connect both of your pcs and your firewall to a switch (LAN). Using a dongle, connect your firewall to the internet too (WAN). Your firewall’s WAN interface is going to be a DHCP client. Assign your LAN interface an address and subnet of your choice by pressing 2. Use that address to access the Web Gui of your firewall. Manually put both of your pcs to be in the same subnet as lan.





Step 6: After entering web gui, log in. 

Step 7: go to services > dhcp server. Scroll down to set a dhcp range

\*Your lan address should be part of that subnet, but not in the pool.

Step 8: Now, make both of your pcs to use dhcp. Connect on of the pcs to the internet, and one to remain on the lan switch.

Go to security > nat. Click the left add.

Step 9: Enter the following configs on the page. The single host address should be the address of the LAN computer that you plan on remote desktoping into from the WAN pc.

Problems: The very first problem that we ran into was that we did not have a password for either of our pcs. Yes, we know we’re in a cybersecurity class, but we trust each other so there’s no need for a password.

Anyway, to remote desktop, you absolutely must have a password, otherwise the protocol will prevent you from taking control of another computer. Remote desktop works on port 3389 (which is a designated port for MS-RDP), and the way that that our network design was working was that the wan pc was sending traffic to the wan port on the firewall, the firewall would forward traffic to port 3389 and forward it to the specified single host (lan pc). Therefore, it is important that when you remote desktop, your destination address is the wan port. Instead of that, we had our destination address to be the address of the lan pc. This seemed intuitive but missed the point of having a firewall in the first place.

We also initially did not turn on our dhcp after we made the lan port of the firewall a dhcp server. We realized the if the lan port is a dhcp server, then to be able to access the management gui of the firewall, you need to be a dhcp client of the firewall.