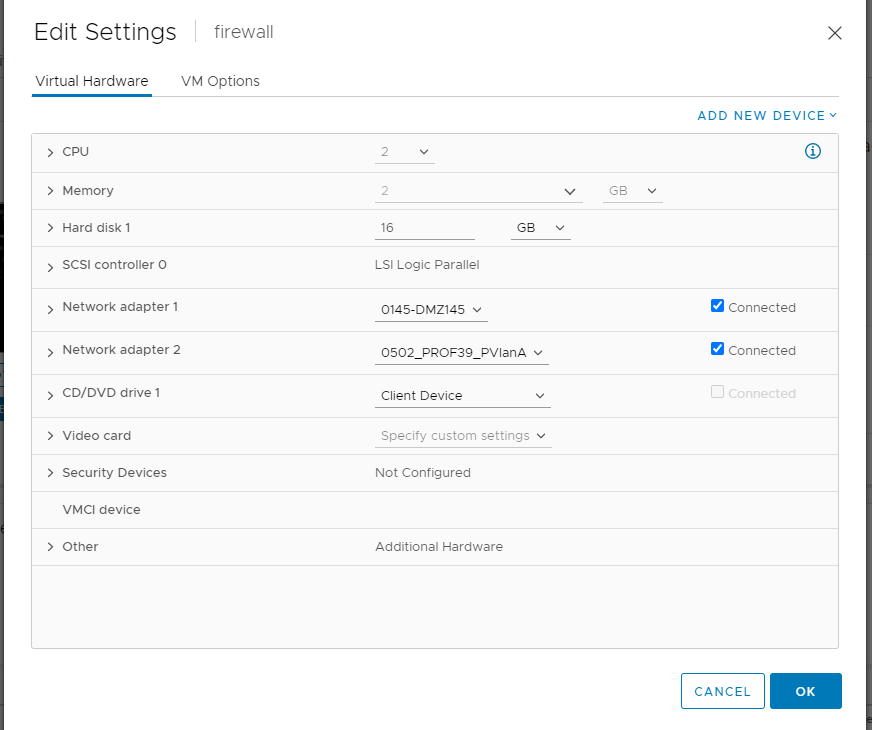
# Opzetten VMs

Maak een VM aan met het PFSense template die beschikbaar is in de map “vcenter.fhict-int.nl -> Netlab-DC -> \_Templates -> Various -> Templ\_pfSense\_2.5”. Zorg er voor dat “Power on machine” niet aan staat.

Open de instellingen van de VM en verander de netwerk adapters naar de settings die je wil hebben op je PFSense. Netwerk adapter 1 is je WAN interface (waar je verkeer vandaan komt) en je netwerk adapter 2 is je LAN interface (alles in deze interface staat ‘achter’ de firewall). In dit geval wil ik alles wat in de PVlanA staat beschermen.

Als je de machines die je achter je firewall wil hebben al eerder hebt aangemaakt, dien je van deze machines de netwerk adapter te veranderen naar de netwerk adapter 2 van je PFSense VM.

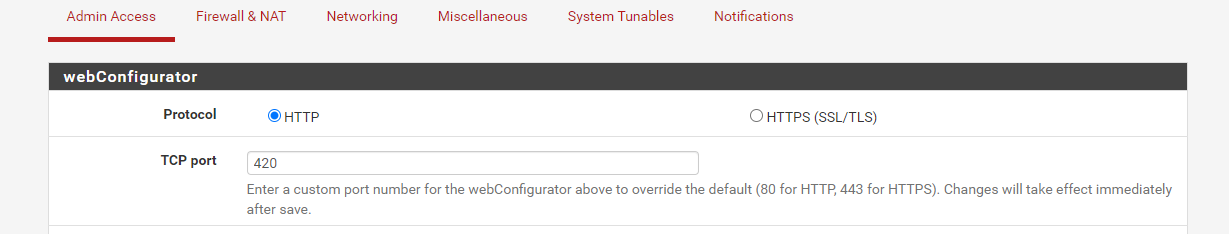


# Opzetten PFSense

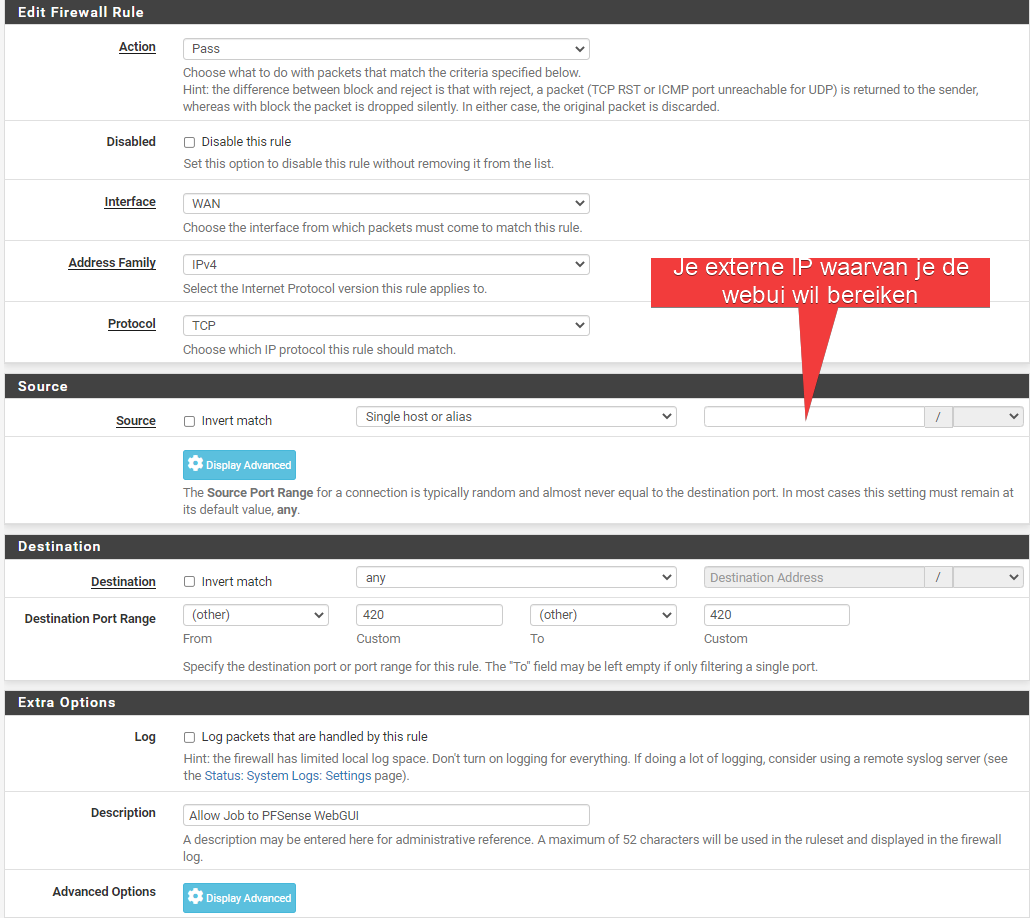
Start PFSense op en kies optie ‘2’. Kies hier om de WAN interface aan te passen. Voor hier je IPadres en gateway in die je hebt gekregen van school via je mail (of gebruik de default waardes van je netwerk-adapter 1 netwerk).

Ga naar het IP adres van je PFSense (dit kan via een interne VM die in je WAN of LAN zit, of vanaf je eigen PC als je WAN exposed word naar het internet). Als het goed is kan je nu hier je PFSense web interface bereiken. Zo niet, zie het ‘troubleshooting’ hoofdstuk.

Het is aangeraden om je standaard port aan te passen als je achter je PFSense een server wil zetten, zodat je later het standaard verkeer naar de HTTP/HTTPS port kan doorrouteren naar je server (standaard login is admin:pfsense, vergeet dit niet te veranderen). Ga dan naar ‘System -> advanced -> tabje Admin Access’ en verander daar ‘TCP port’ naar de port waar je je WebUI op wil hebben.



Vanaf nu kan je alleen je WebUI bereiken via <pfsense\_ip>:<je gekozen port>. Echter kan je (waarschijnlijk) deze alleen bereiken als je de PFSense firewall rules uitzet (dit doe je bij troubleshooting ‘ik kan niet bij mijn WebUI’). Om dit te voorkomen moet je wat ALLOW regels toevoegen aan je firewall (standaard zit alles netjes dicht). Ga hiervoor naar ‘firewall -> rules’ en ga naar het kopje ‘WAN’. Er word aangeraden aan dit los te doen voor elke groespgenoot en niet een ‘any’ rule aan te maken. Zo zorg je er voor dat er geen onbekende mensen bij je PFSense kunnen komen.

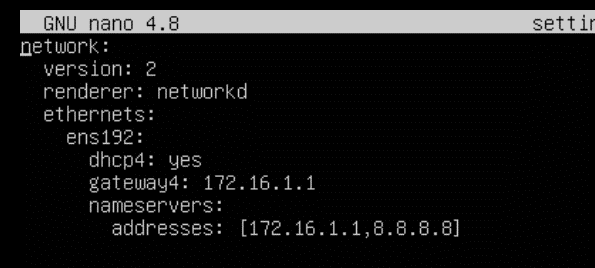


# Je devices een Statisch IP adres geven

Zorg er voor dat je device die je toegankelijk wil maken zijn IP verkrijgt via de DHCP server (in dit geval is je DHCP server je PFSense).

## Voor Linux:

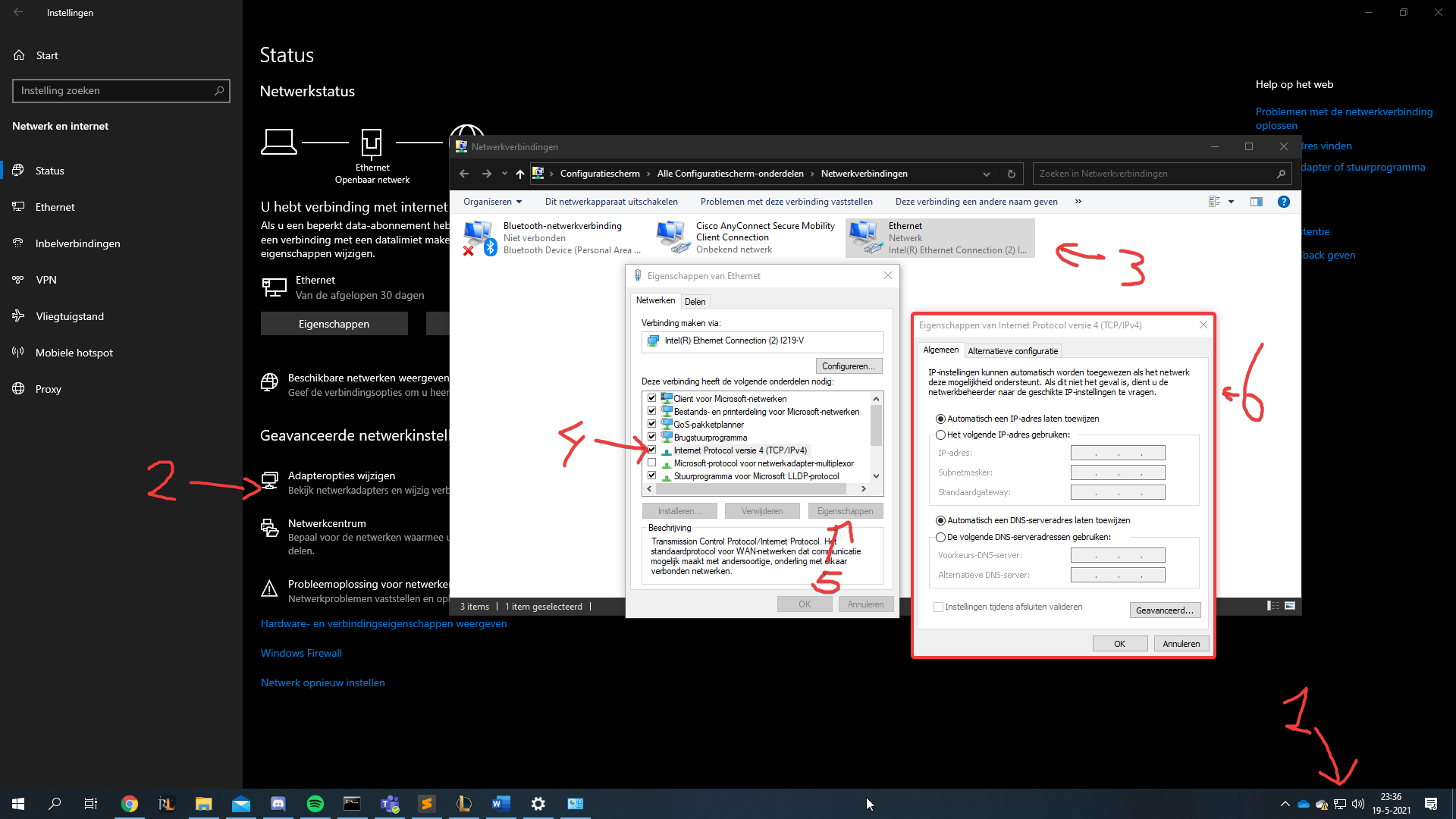
Maak een file aan in /etc/netplan en geef hem een naam, zolang hij maar met ‘.yaml’ eindigd (bijvoorbeeld settings.yaml). Na het maken van deze file voer je ‘sudo netplan apply’ uit. Nu worden de netwerkinstellingen opgeslagen. Een voorbeeld van een settings.yaml staat hieronder. Het veld ‘gateway4’ dient gevult te worden met het IP adres van de PFSense. Dit geld ook voor het eerste adres in de ‘addresses’ array. Eventueel kan je een ‘fallback’ DNS zetten naar bijvoorbeeld Google DNS.



Als je nu ‘ifconfig -a’ uitvoert heb je als het goed is nu een lokaal ip adres wat lijkt op ‘172.16.1.X’ (of in ieder geval binnen de range van je PFSense LAN netwerk). Zo niet, dan moet je je DHCP lease droppen met ‘sudo dhclient -r’ en daarna ‘sudo dhclient’.

## Voor Windows:

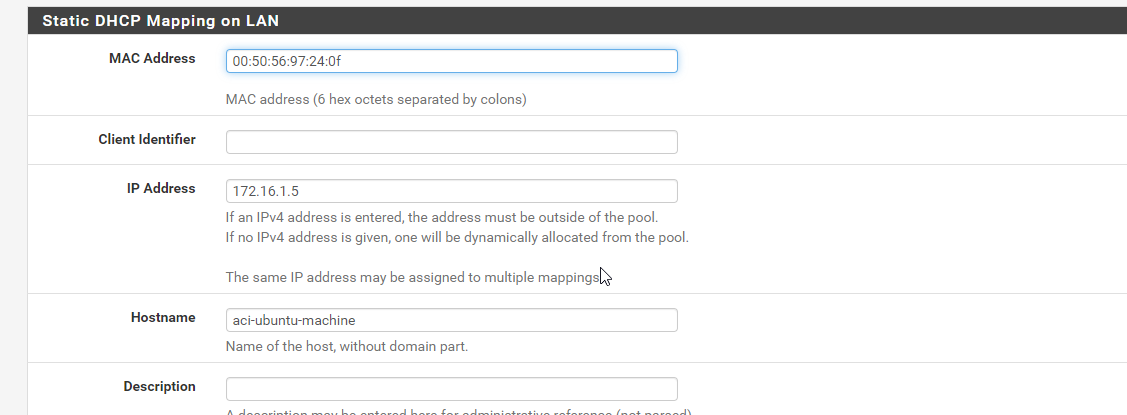
Als je niks in je Windows machine gezet hebt veranderd aan de netwerk instellingen kan je gemakkelijk via CMD je nieuwe IP adres krijgen. Dit kan je verkrijgen met de commando’s ‘ipconfig /release’ en ‘ipconfig /renew’. Als je wel netwerk instellingen hebt aangepast dien je deze terug te zetten naar de standaard waardes.



## Het statische IP instellen op je PFSense

Zorg er voor dat je nu in je PFSense je beveiligde machine een statisch IP geeft. Doe dit via de web interface In de WebUI, ga naar ‘status -> DCHP leases’. Als het goed staat hier nu je machine tussen. Druk op het knopje naast de machine om hem een statisch IP te geven.

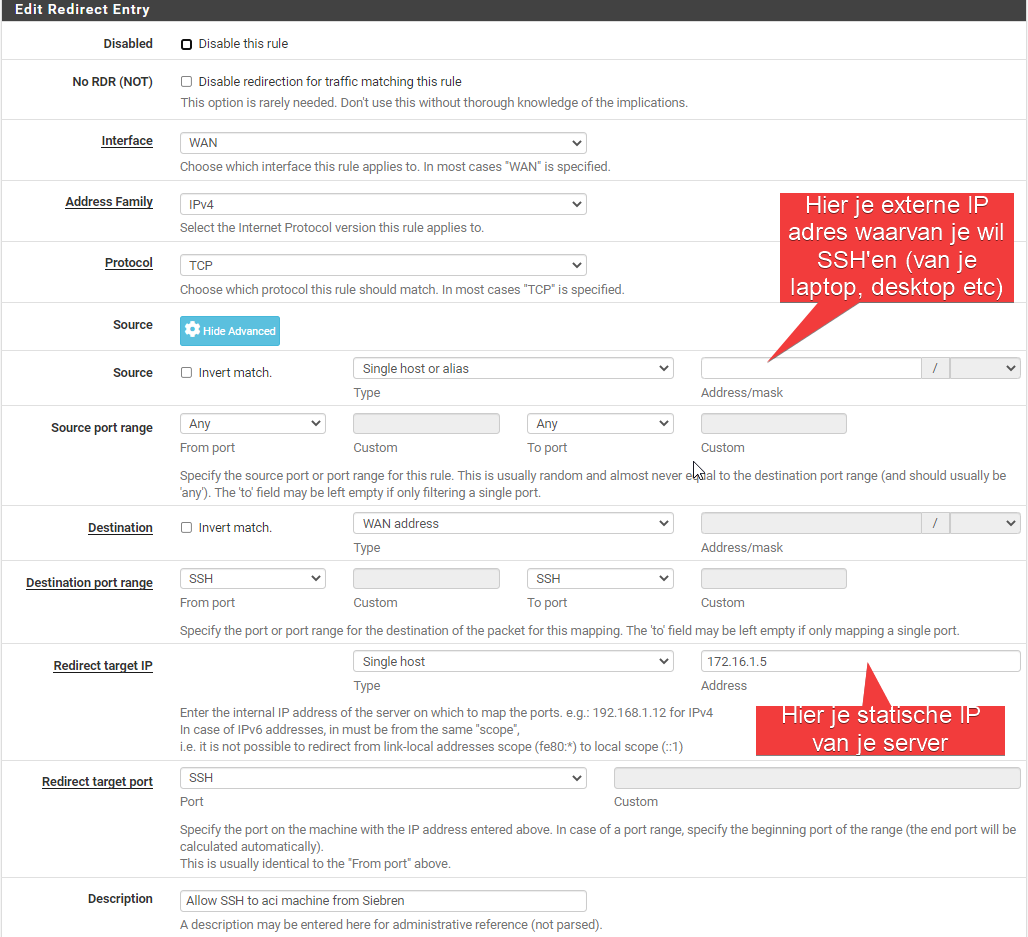
In dit geval kiest dit voorbeeld voor ‘172.16.1.5’ maar je kan alles tussen 172.16.1.2 en 172.16.1.10 kiezen (deze range kan je eventueel groter of kleiner maken in de WebUI instellingen van je PFSense).



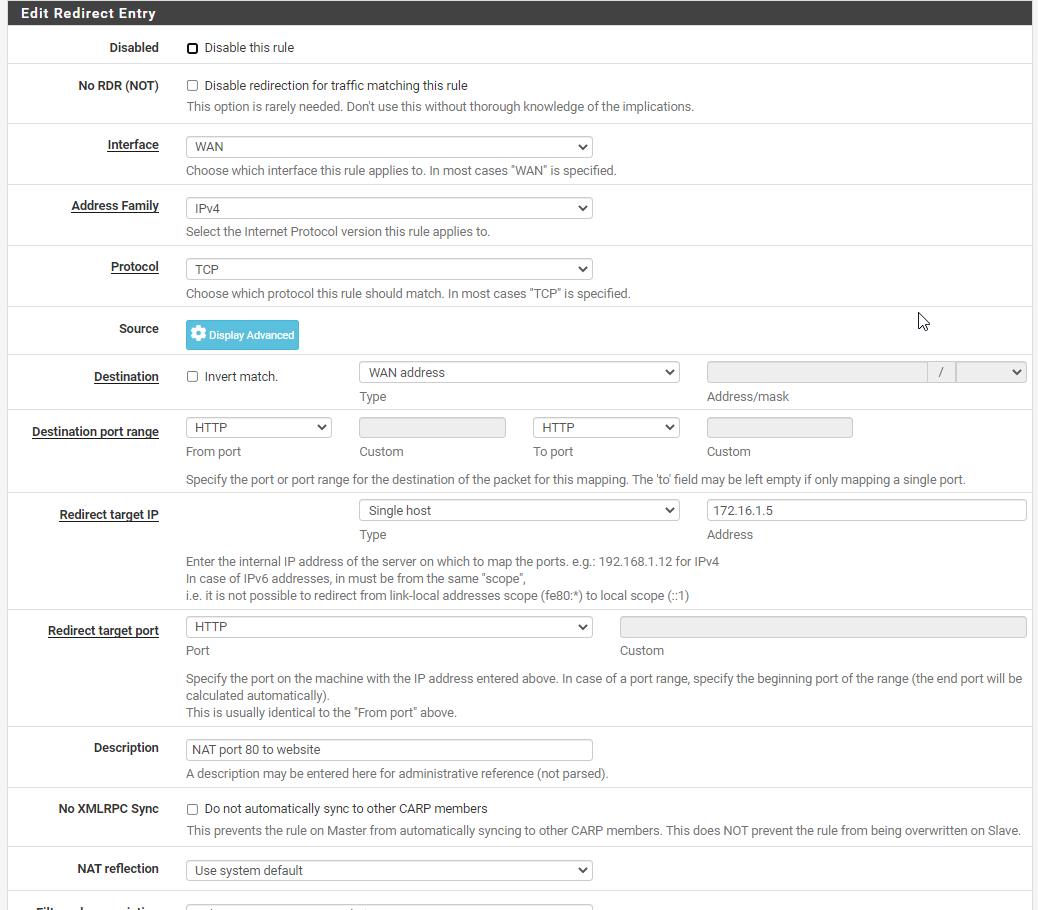
Als je nu weer je DHCP lease dropt op je machine, heb je als het goed is het lokale IP die je hem net hebt gegeven.

# Netwerkrequests doorrouteren naar een device achter je PFSense (NAT)

Nu kan je firewall en NAT rules aanmaken. Om bijvoorbeeld weer te kunnen SSH’en naar je Linux machine, kan je een NAT rule aanmaken via ‘firewall -> NAT’. Ik raad aan dit handmatig voor elk extern IP te doen van je groepsgenoten (en geen ‘any’ source gebruiken) zo houd je alles netjes dicht.



Nu wil je nog je website kunnen bereiken als je die op je server hebt draaien. Ook dit is een NAT regel. Hier wil je de source WEL op ‘any’ houden zodat iedereen bij je website kan. Als je dit wel wil restricten kan dat uiteraard. Die ziet er als volgt uit.



# Troubleshooting

## Ik kan niet bij mn WebUI?

In de PFSense VM, kies dan optie ‘8’ om een shell te openen en voer het commando ‘pfctl -d’ uit om tijdelijk de firewall rules te disablen. Om dit weer aan te zetten, gebruik dan -e. Standaard bij een reboot of het veranderen van een regel gaat de pfctl weer op aan. Dus die moet je dan weer uitzetten. Hoe je permanent kan verbinden word in het document uitgelegd.

## Ik krijg een HTTP\_REFERER error?

Voer het commando ‘pfSsh.php playback disablereferercheck’ in de shell van PFSense.