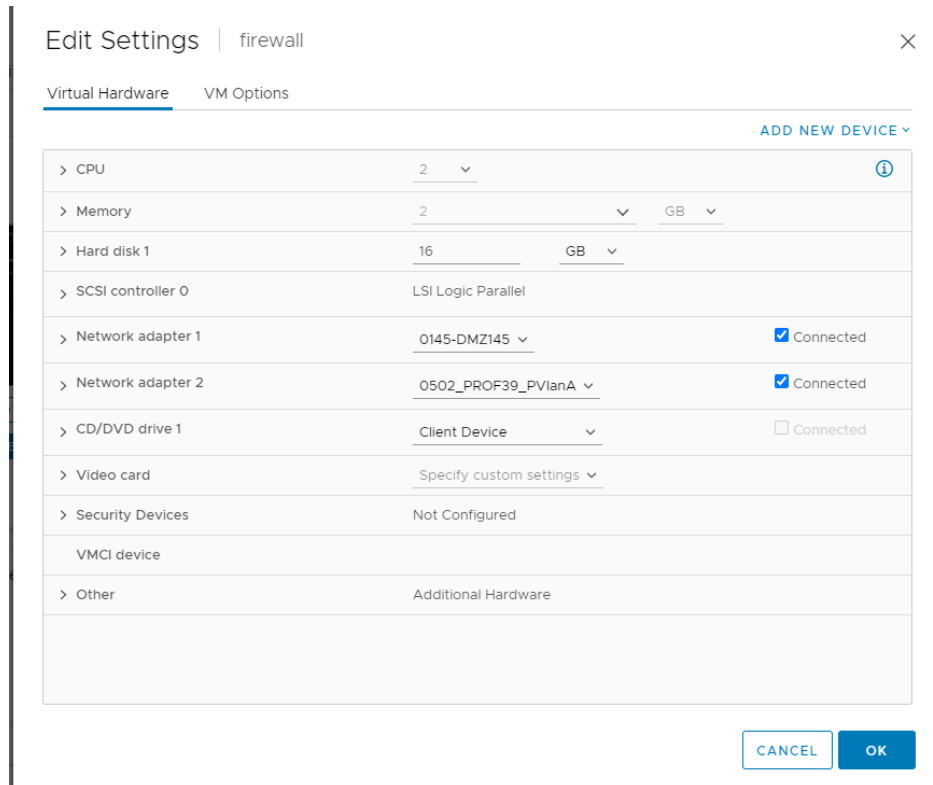


Opzetten VMs

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.



The screenshot shows the 'Edit Settings' window for a VM, with the 'firewall' tab selected. The 'Virtual Hardware' tab is active, and the 'ADD NEW DEVICE' button is visible. The settings are as follows:

Device	Value	Connected
CPU	2	
Memory	2 GB	
Hard disk 1	16 GB	
SCSI controller 0	LSI Logic Parallel	
Network adapter 1	0145-DMZ145	<input checked="" type="checkbox"/> Connected
Network adapter 2	0502_PROF39_PVlanA	<input checked="" type="checkbox"/> Connected
CD/DVD drive 1	Client Device	<input type="checkbox"/> Connected
Video card	Specify custom settings	
Security Devices	Not Configured	
VMCI device		
Other	Additional Hardware	

At the bottom, there are 'CANCEL' and 'OK' buttons.

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.



This is a close-up of the 'Network adapter 1' setting. It shows the adapter is set to '0502_PROF39_PVlanA' and is connected.

Device	Value	Connected
Network adapter 1	0502_PROF39_PVlanA	<input checked="" type="checkbox"/> Connected

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.

Admin Access Firewall & NAT Networking Miscellaneous System Tunables Notifications

webConfigurator

Protocol ☒ HTTP ☐ HTTPS (SSL/TLS)

TCP port

Enter a custom port number for the webConfigurator above to override the default (80 for HTTP, 443 for HTTPS). Changes will take effect immediately after save.

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.

Edit Firewall Rule

Action

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled ☐ Disable this rule
Set this option to disable this rule without removing it from the list.

Interface

Choose the interface from which packets must come to match this rule.

Address Family

Select the Internet Protocol version this rule applies to.

Protocol

Choose which IP protocol this rule should match.

Source

Source ☐ Invert match

[Display Advanced](#)

The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.

Destination

Destination ☐ Invert match

Destination Address

Destination Port Range

From Custom To Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log ☐ Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options [Display Advanced](#)

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:

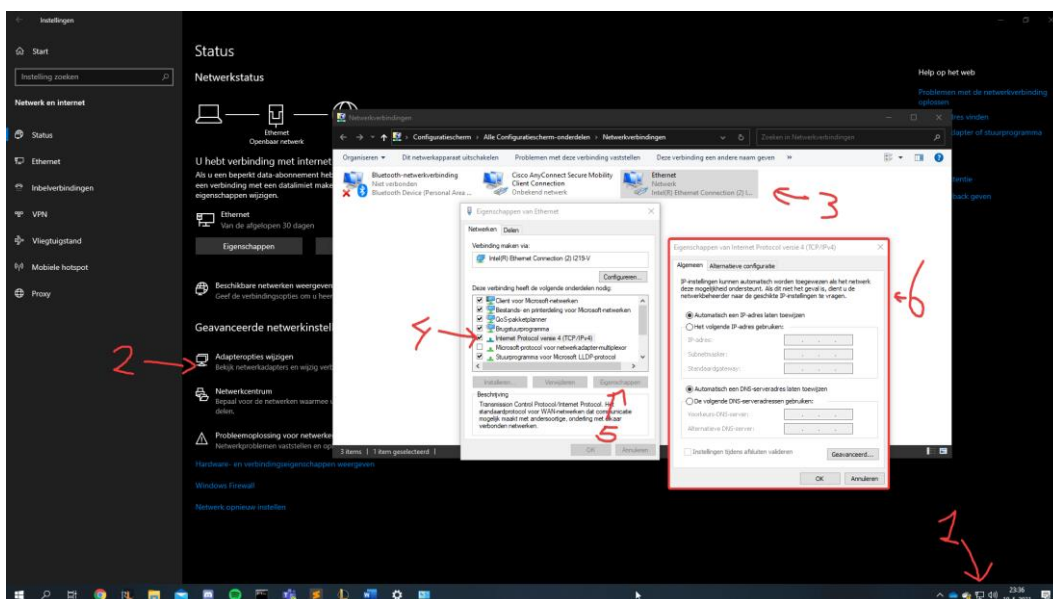
Maak een file aan in /etc/netplan en geef hem een naam, zolang hij maar met '.yaml' eindigt (bijvoorbeeld settings.yaml). Na het maken van deze file voer je 'sudo netplan apply' uit. Nu worden de netwerkinstellingen opgeslagen. Een voorbeeld van een settings.yaml staat hieronder. Het veld 'gateway4'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

```
GNU nano 4.8 settings.yaml
network:
  version: 2
  renderer: networkd
  ethernets:
    ens192:
      dhcp4: yes
      gateway4: 172.16.1.1
      nameservers:
        addresses: [172.16.1.1, 8.8.8.8]
```

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 network). 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 -> DHCP 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).

Static DHCP Mapping on LAN	
MAC Address	<input type="text" value="00:50:56:97:24:0f"/> <small>MAC address (6 hex octets separated by colons)</small>
Client Identifier	<input type="text"/>
IP Address	<input type="text" value="172.16.1.5"/> <small>If an IPv4 address is entered, the address must be outside of the pool. If no IPv4 address is given, one will be dynamically allocated from the pool. The same IP address may be assigned to multiple mappings.</small>
Hostname	<input type="text" value="aci-ubuntu-machine"/> <small>Name of the host, without domain part.</small>
Description	<input type="text"/> <small>A description may be entered here for administrative reference (not saved)</small>

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.

Edit Redirect Entry

Disabled ☐ Disable this rule

No RDR (NOT) ☐ Disable redirection for traffic matching this rule
This option is rarely needed. Don't use this without thorough knowledge of the implications.

Interface WAN
Choose which interface this rule applies to. In most cases "WAN" is specified.

Address Family IPv4
Select the Internet Protocol version this rule applies to.

Protocol TCP
Choose which protocol this rule should match. In most cases "TCP" is specified.

Source [Hide Advanced](#)

Source ☐ Invert match. Type Address/mask

Source port range From port To port To port Custom
Specify the source port or port range for this rule. This is usually random and almost never equal to the destination port range (and should usually be 'any'). The 'to' field may be left empty if only filtering a single port.

Destination ☐ Invert match. Type Address/mask

Destination port range From port To port To port Custom
Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.

Redirect target IP Type Address
Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4
In case of IPv6 addresses, it must be from the same "scope", i.e. it is not possible to redirect from link-local addresses scope (fe80::) to local scope (::1)

Redirect target port Port Custom
Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically).
This is usually identical to the "From port" above.

Description
A description may be entered here for administrative reference (not parsed).

Hier je externe IP adres waarvan je wil SSH'en (van je laptop, desktop etc)

Hier je statische IP van je server

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.

Edit Redirect Entry

Disabled ☐ Disable this rule

No RDR (NOT) ☐ Disable redirection for traffic matching this rule
This option is rarely needed. Don't use this without thorough knowledge of the implications.

Interface WAN
Choose which interface this rule applies to. In most cases "WAN" is specified.

Address Family IPv4
Select the Internet Protocol version this rule applies to.

Protocol TCP
Choose which protocol this rule should match. In most cases "TCP" is specified.

Source [Display Advanced](#)

Destination ☐ Invert match. Type Address/mask

Destination port range From port To port To port Custom
Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.

Redirect target IP Type Address
Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4
In case of IPv6 addresses, it must be from the same "scope", i.e. it is not possible to redirect from link-local addresses scope (fe80::) to local scope (::1)

Redirect target port Port Custom
Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically).
This is usually identical to the "From port" above.

Description
A description may be entered here for administrative reference (not parsed).

No XMLRPC Sync ☐ Do not automatically sync to other CARP members
This prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.

NAT reflection

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.