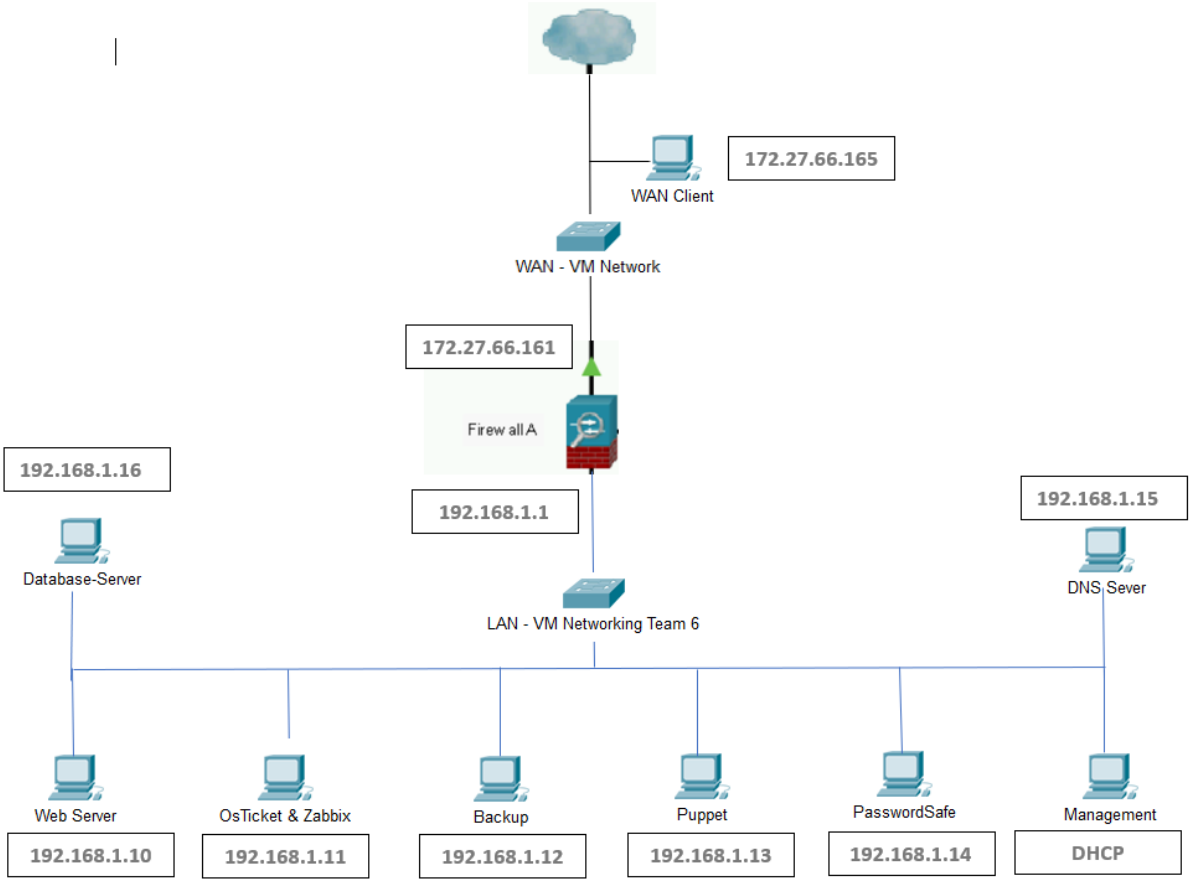
PfSense (Firewall): Handleiding

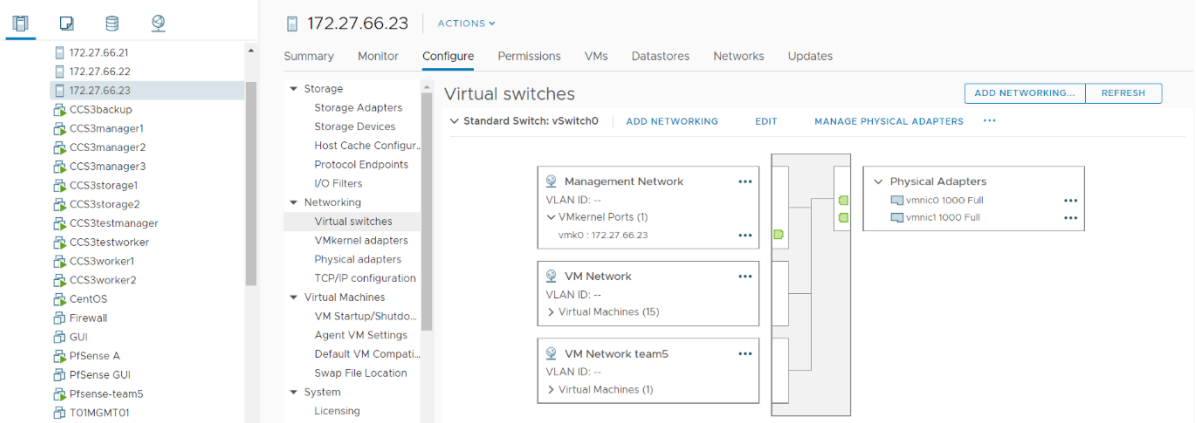
Topology



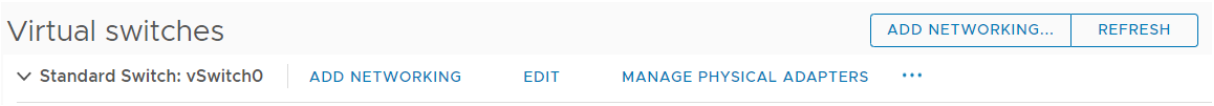
Bijvoegen Virtuele standard switch LAN kant.

Deze stappen uitvoeren op de 3 hosting-clusters (identiek! Anders werkt het niet).

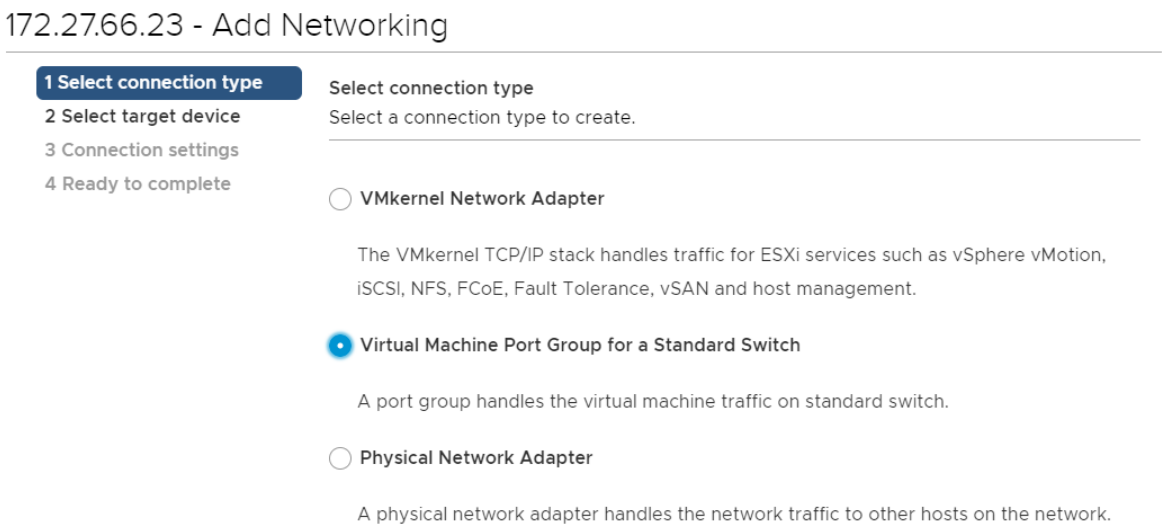
Beginsituatie



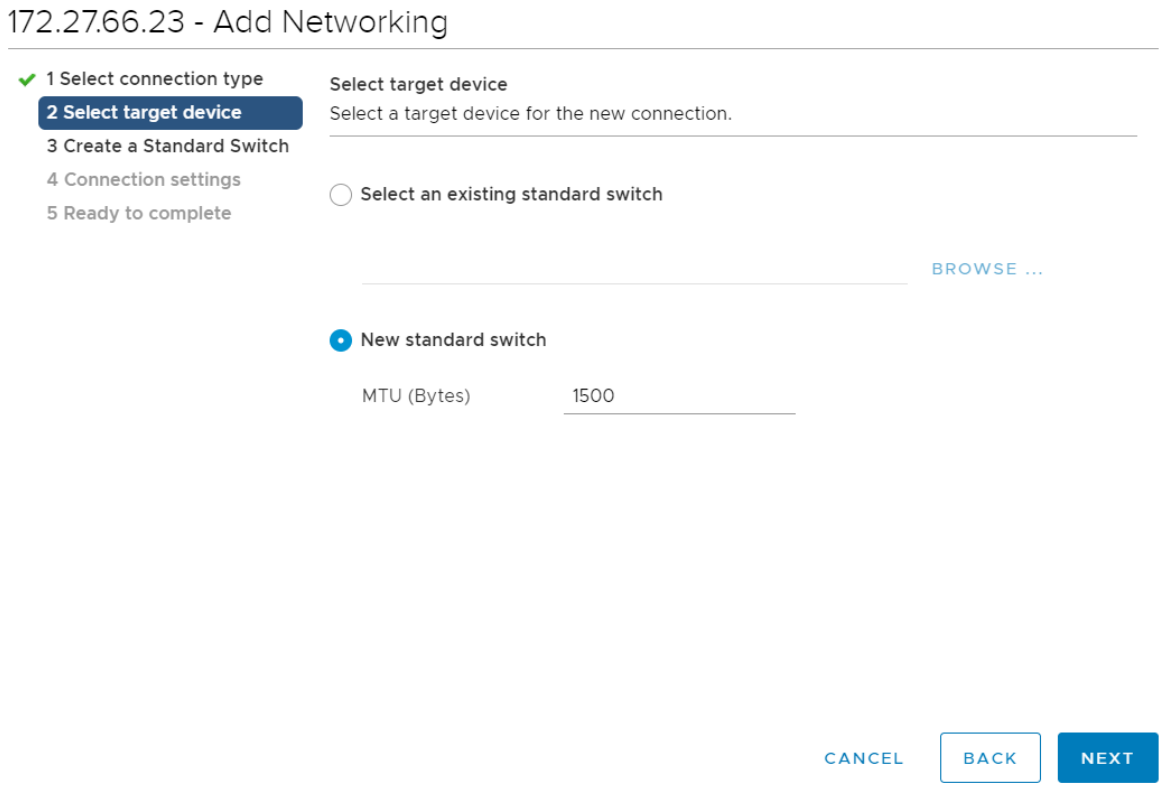
Stap 1: Add Networking!



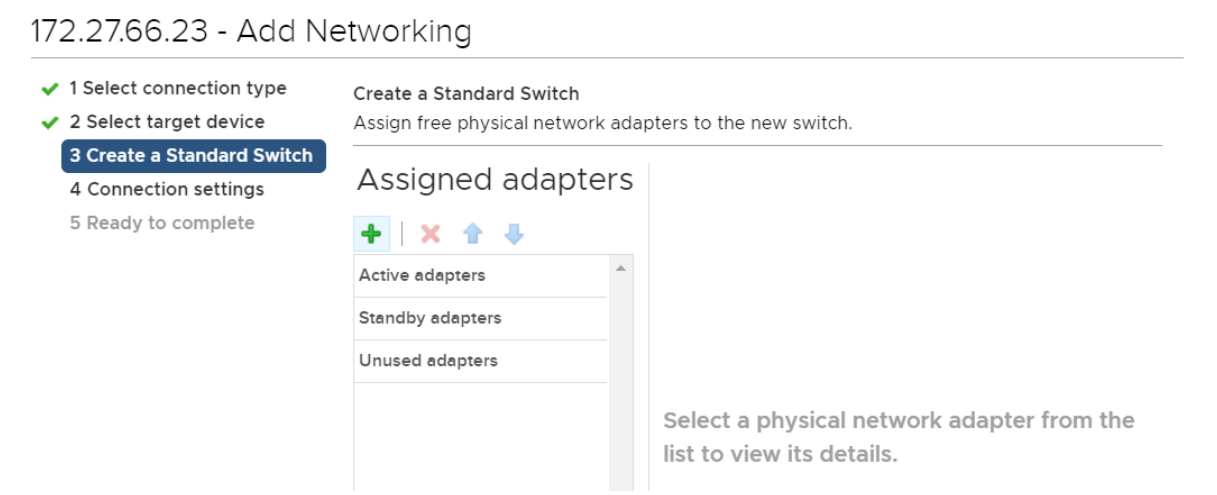
Stap 2

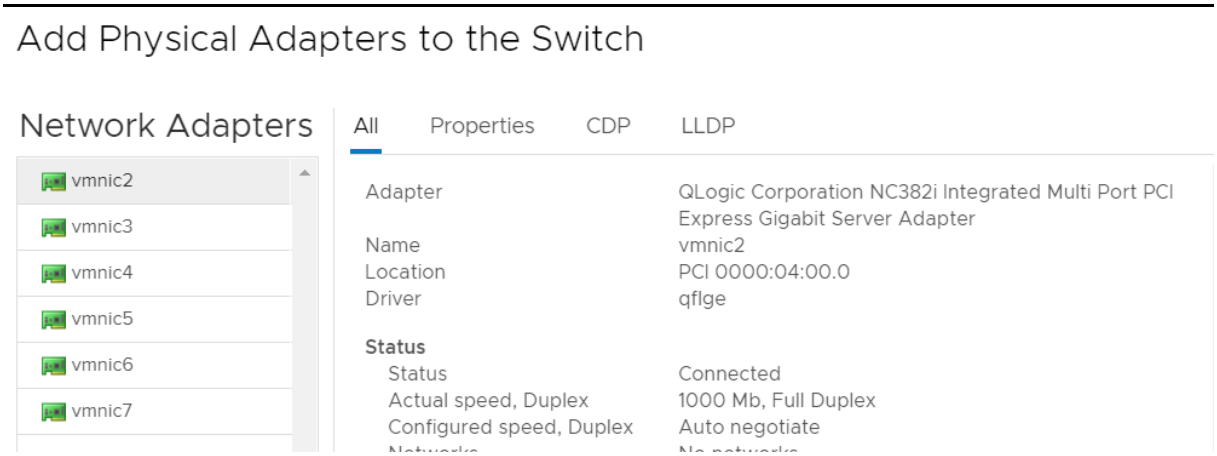


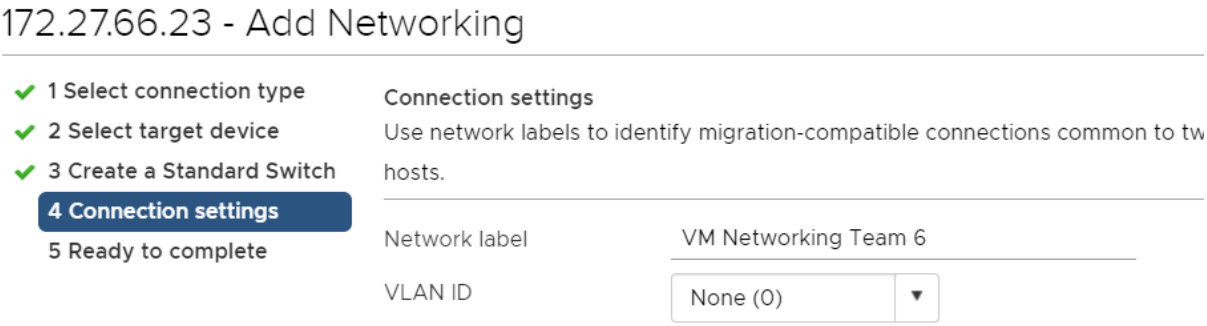
Stap 3



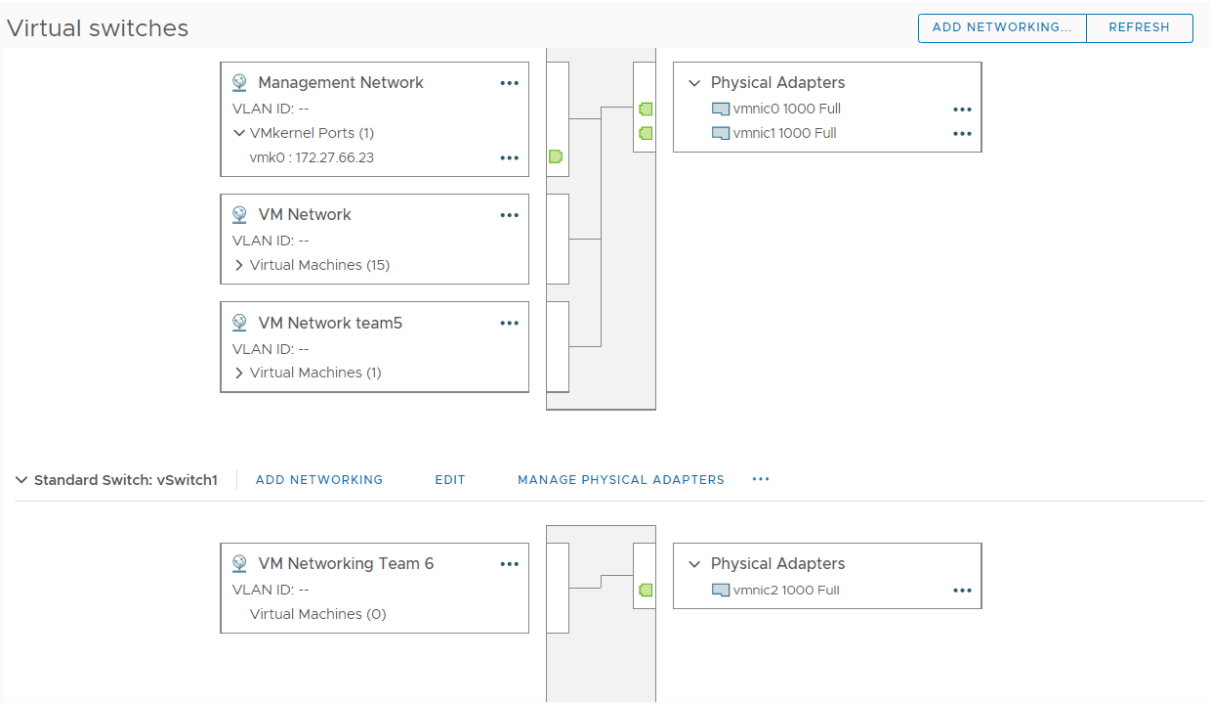
Stap 4: Add adapter vmnic2!







Eindsituatie:



VM network = WAN

VM Networking Team 6 = LAN

Installatie PfSense A

Stap 1: configure the NIC

```
Should VLANs be set up now [y|n]? n

If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(vmx0 vmx1 or a): vmx0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(vmx1 a or nothing if finished): vmx1

The interfaces will be assigned as follows:

WAN  -> vmx0
LAN  -> vmx1
```

Stap 2: Set an ip address to WAN

```
VMware Virtual Machine - Netgate Device ID: cd209225b4393d21a115

*** Welcome to pfSense 2.4.5-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> vmx0       -> v4/DHCP4: 172.27.66.93/24
 LAN (lan)       -> vmx1       -> v4: 192.168.1.1/24

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option: 2

Available interfaces:

1 - WAN (vmx0 - dhcp, dhcp6)
2 - LAN (vmx1 - static)

Enter the number of the interface you wish to configure: 1
```

```
Available interfaces:

1 - WAN (vmx0 - dhcp, dhcp6)
2 - LAN (vmx1 - static)

Enter the number of the interface you wish to configure: 1

Configure IPv4 address WAN interface via DHCP? (y/n) n

Enter the new WAN IPv4 address.  Press <ENTER> for none:
> 172.27.66.162

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new WAN IPv4 subnet bit count (1 to 31):
> 24

For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 172.27.66.254
```

```
  Configure IPv6 address WAN interface via DHCP6? (y/n) n

  Enter the new WAN IPv6 address.  Press <ENTER> for none:
  >

  Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

  Please wait while the changes are saved to WAN...
   Reloading filter...
   Reloading routing configuration...
   DHCPD...

  The IPv4 WAN address has been set to 172.27.66.162/24
```

```
Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 192.168.1.100
Enter the end address of the IPv4 client address range: 192.168.1.201
Disabling IPv6 DHCPD...
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

Please wait while the changes are saved to LAN...
 Reloading filter...
 Reloading routing configuration...
 DHCPD...

The IPv4 LAN address has been set to 192.168.1.2/24
You can now access the webConfigurator by opening the following URL in your web
browser:
                https://192.168.1.2/
```

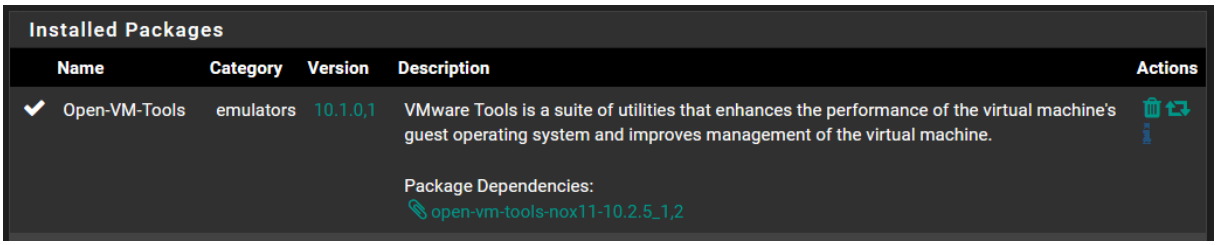
Installatie Management VM (GUI)

Ga naar https://192.168.1.1

Log in met admin en wachtwoord pfsense

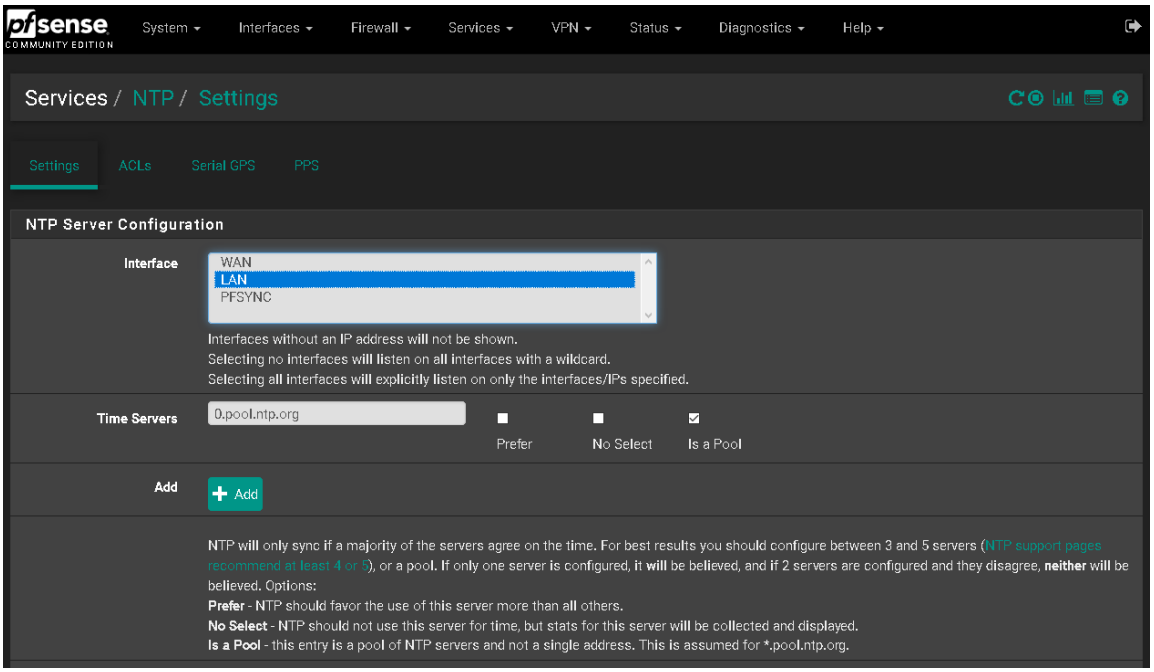
Stap 1: Package manager installeren

@pfSense > System > Packages



Stap 2: pfsense als NTP server instellen

@pfSense > Services > NTP



Test

Ntp server aan het luisteren? → sudo nmap -p123 -sU -Pn 192.168.1.1

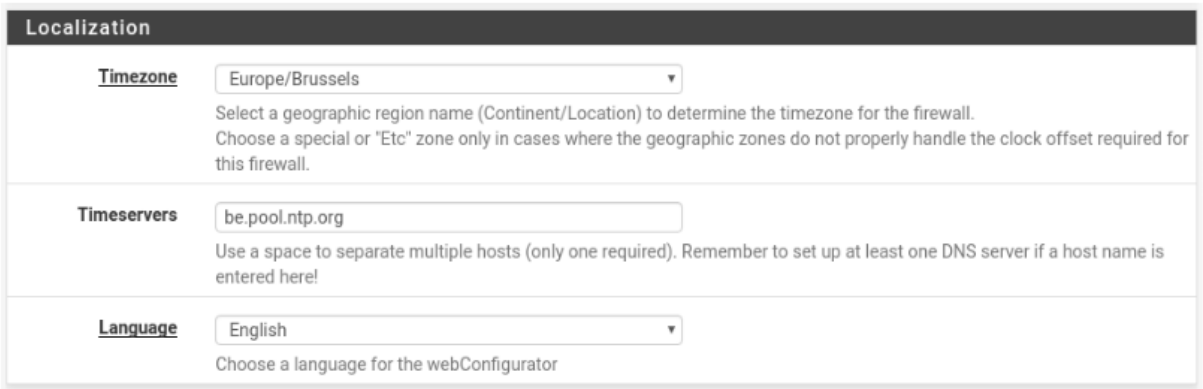
sudo apt install ntpdate

sudo ntpdate -q 192.168.1.1 ***(+ tijdszone aanpassen)***

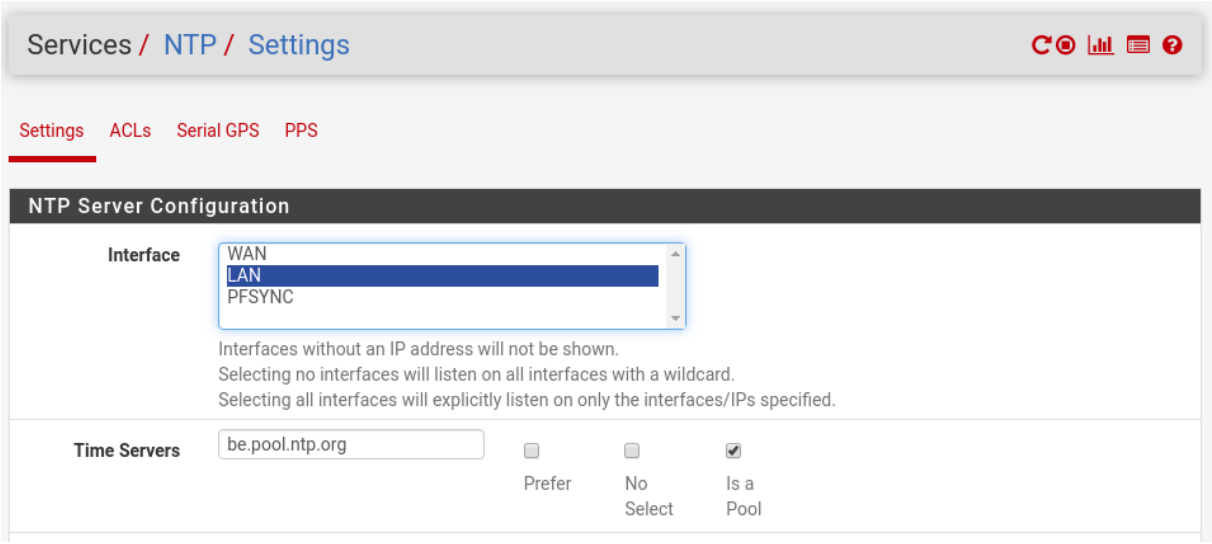
date → check of het de juiste datum heeft

Stap 3: NTP client instellen

@pfSense > System > General Setup



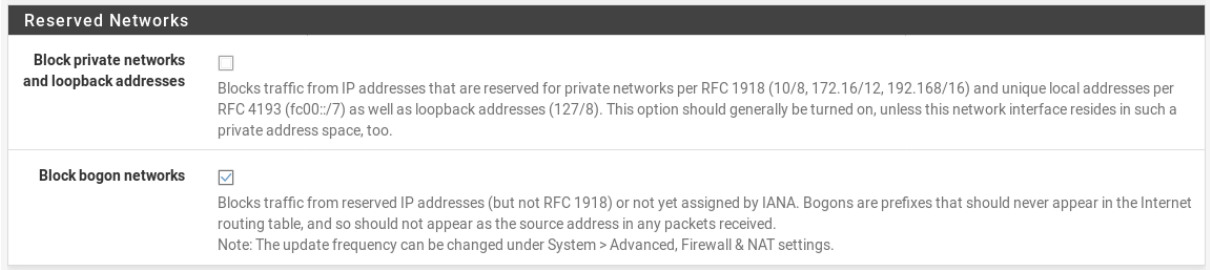
Stap 4: NTP server instellen



Stap 5: Firewall rules instellen

Block bogon networks

@pfSense > Interfaces > WAN (vmx0)



Firewall / Rules / WAN

Floating WAN LAN SYNC

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✖	0 /41.31 MiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	

Firewall / Rules / Floating

Floating WAN LAN SYNC

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✔	0 /0 B	IPv4+6 ICMP any	*	*	*	*	*	none		Allow ICMP on all interfaces	

Stap 6: NAT Port Forwarding

@pfSense > Firewall > NAT > Port Forward

Port Forward 1:1 Outbound NPt

Rules

	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
✔	WAN	TCP	*	*	WAN address	22 (SSH)	192.168.1.10	22 (SSH)	Forward SSH to Server	
✔	WAN	TCP	*	*	WAN address	20	192.168.1.10	20	Forward FTP to Server	
✔	WAN	TCP	*	*	WAN address	21 (FTP)	192.168.1.10	21 (FTP)	Forward FTP to Server	
✔	WAN	TCP	*	*	WAN address	443 (HTTPS)	192.168.1.10	443 (HTTPS)	Open webServer to Internet	
✔	WAN	TCP	*	*	WAN address	80 (HTTP)	192.168.1.10	80 (HTTP)	Open webServer to Internet	
✔	WAN	TCP	*	*	WAN address	55414	192.168.1.12	55414	Urbuackup to Server	

Stap 7: DHCP Pool instellen + DNS servers

@pfsense > Services > DHCP server

Range

192.168.1.100

From

192.168.1.201

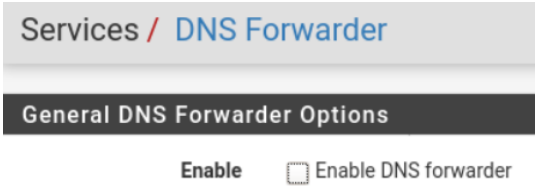
DNS servers

1.1.1.1

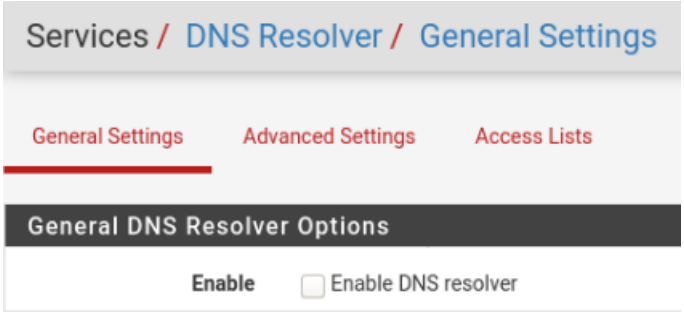
1.0.0.1

Stap 8: DNS Zero ground

@pfSense > Services > DNS Forwarder



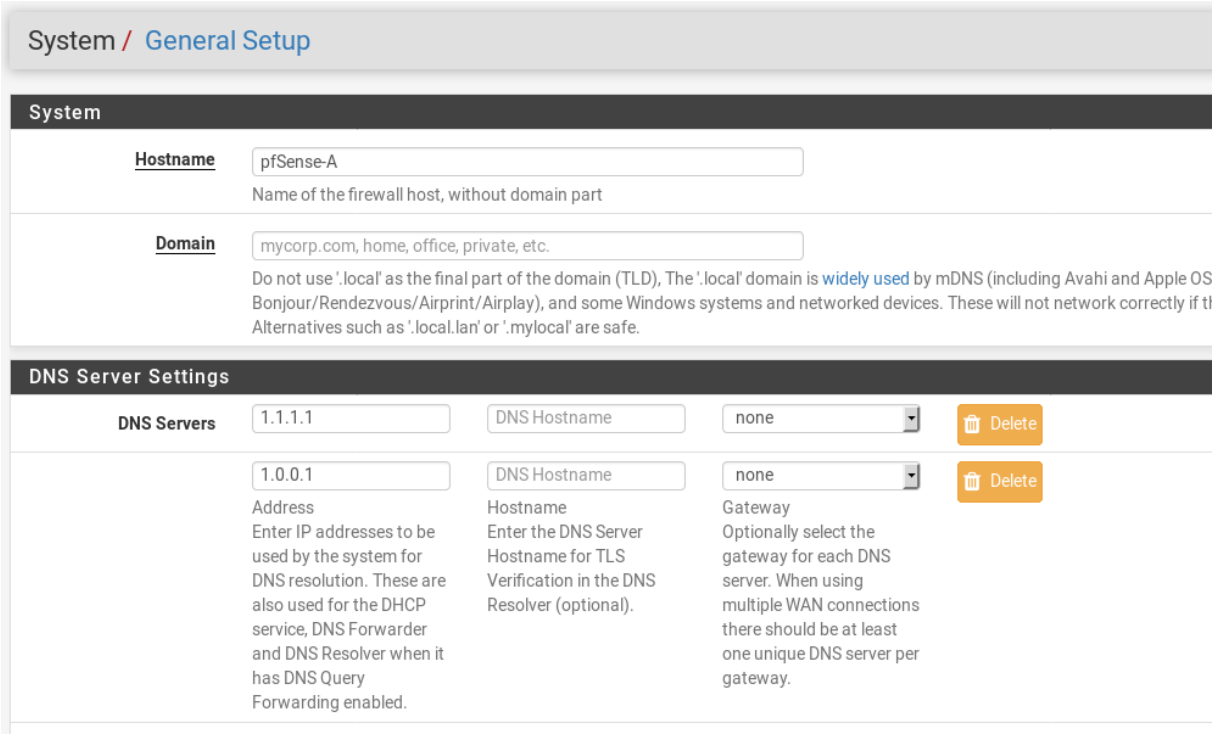
@pfSense > Services > DNS Resolver



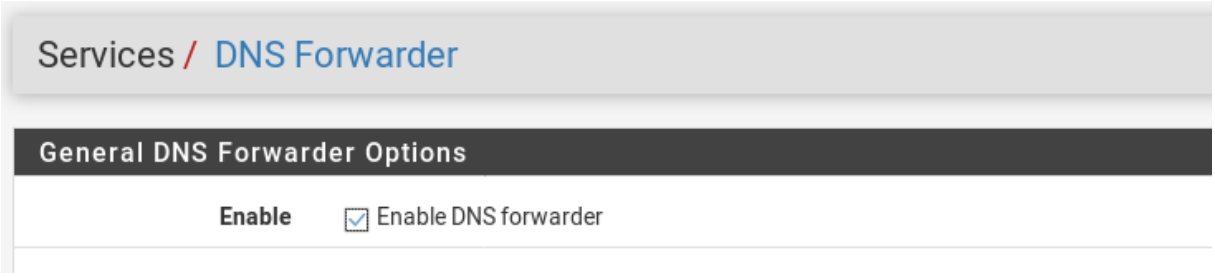
Test of de DNS service is disabled

```
root@kali:~# dig @172.16.0.252 thomasmore.be

; <<>> DiG 9.11.5-P4-5.1+b1-Debian <<>> @172.16.0.252 thomasmore.be
; (1 server found)
;; global options: +cmd
;; connection timed out; no servers could be reached
```

@pfSense > System > General Setup



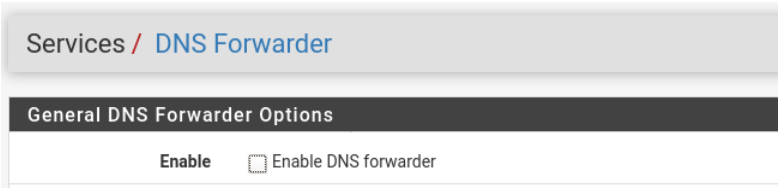
@pfSense > Services > DNS Forwarder



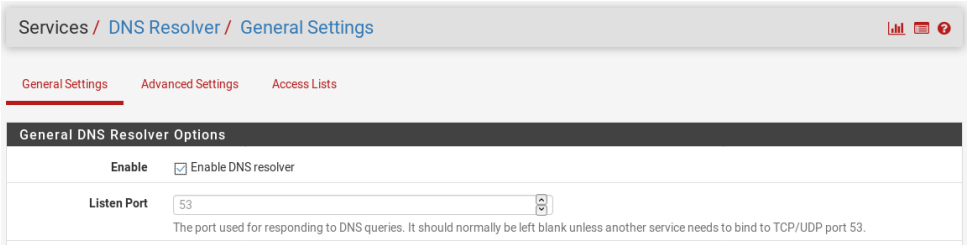
Test pfsense DNS Forwarder

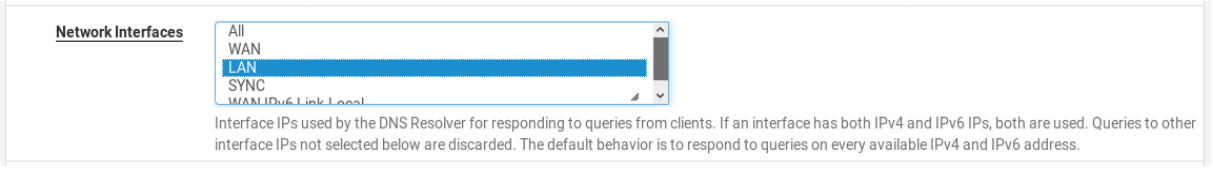
```
root@kali:~# dig @172.16.0.252 thomasmore.be

; <<>> DiG 9.11.5-P4-5.1+b1-Debian <<>> @172.16.0.252 thomasmore.be
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40049
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;thomasmore.be.                 IN      A

;; ANSWER SECTION:
thomasmore.be.          3570    IN      A       62.213.218.216

;; Query time: 0 msec
;; SERVER: 172.16.0.252#53(172.16.0.252)
;; WHEN: Mon Feb 03 21:26:22 EST 2020
;; MSG SIZE  rcvd: 58
```

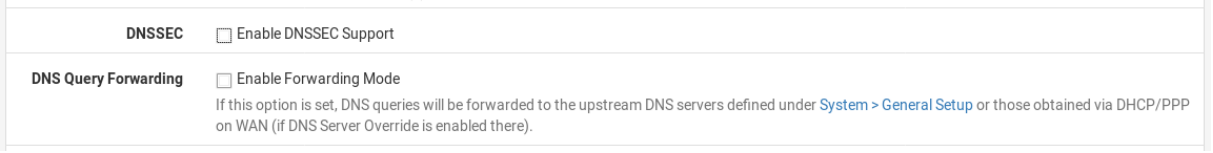
@pfSense > Services > DNS Forwarder



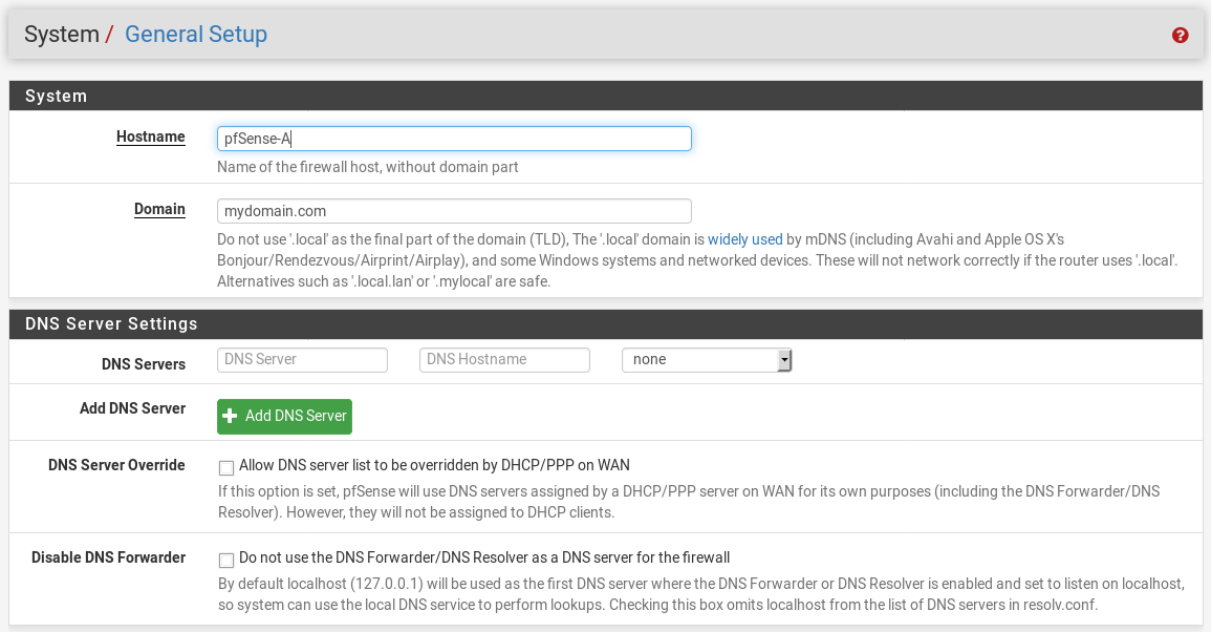
@pfSense > Services > DNS Resolver







@pfSense > System > General Setup

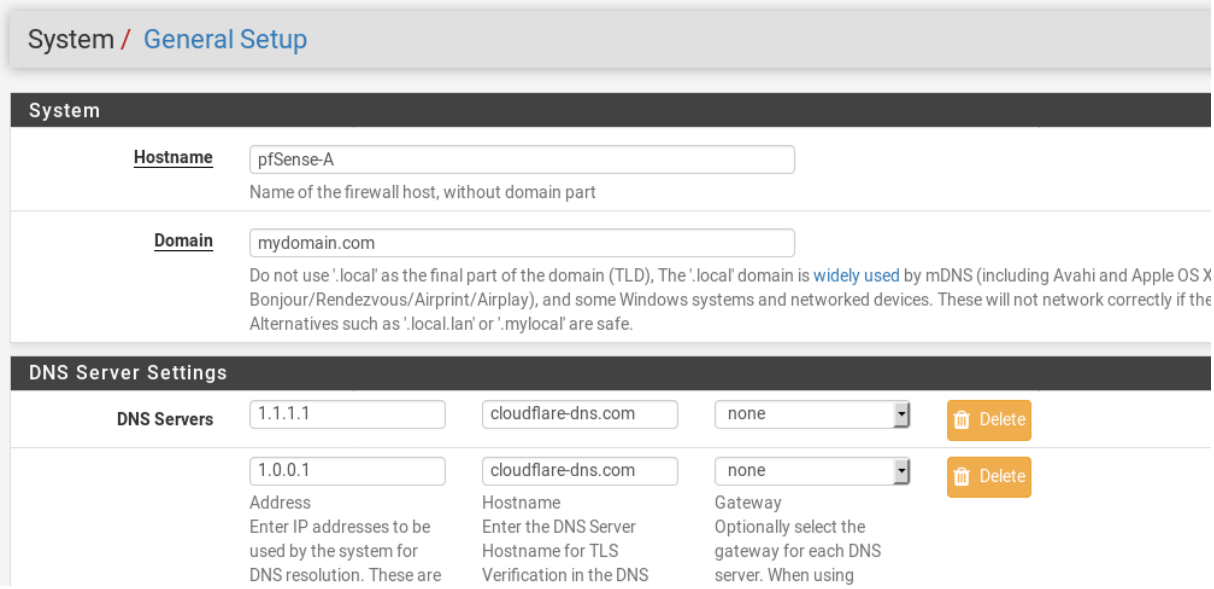


Test onze name server

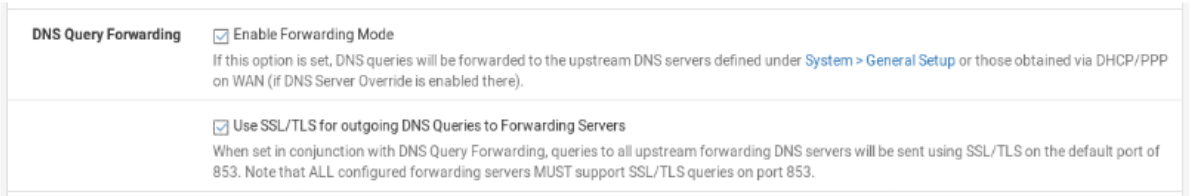
```
root@kali:~# dig @172.16.0.252 thomasmore.be

; <<>> DiG 9.11.5-P4-5.1+b1-Debian <<>> @172.16.0.252 thomasmore.be
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 707
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;thomasmore.be.                 IN      A

;; ANSWER SECTION:
thomasmore.be.          3519    IN      A       62.213.218.216

;; Query time: 0 msec
;; SERVER: 172.16.0.252#53(172.16.0.252)
;; WHEN: Tue Feb 25 15:32:57 EST 2020
;; MSG SIZE  rcvd: 58
```

Vind de DNS cache onder @pfSense > Status > DNS Resolver

@pfSense > System > General Setup



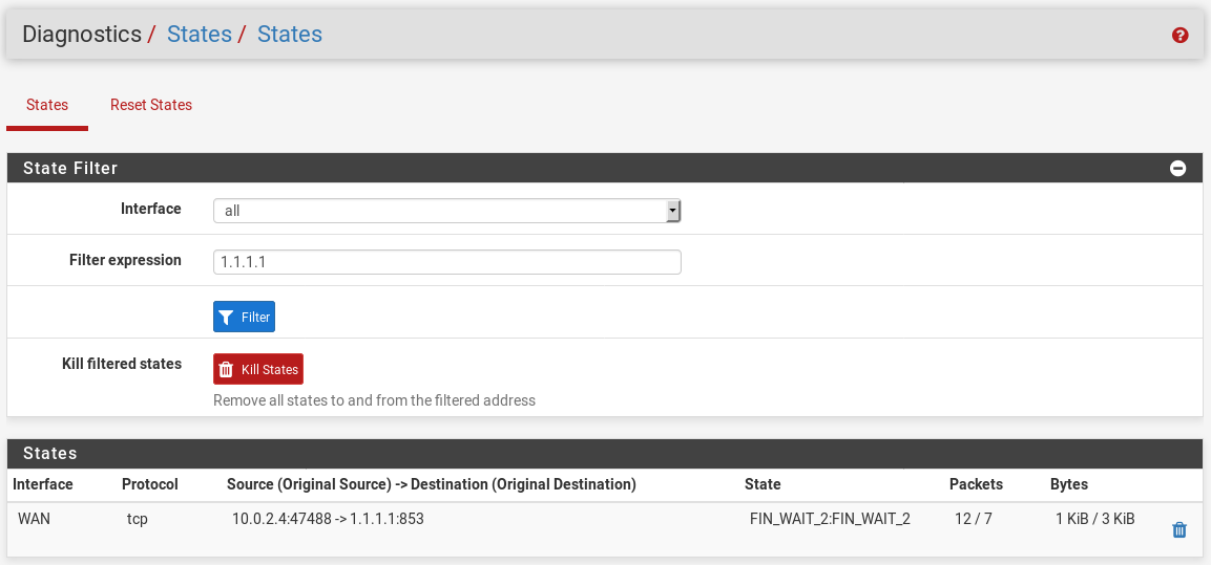
@pfSense > Services > DNS Resolver > General Settings



Test

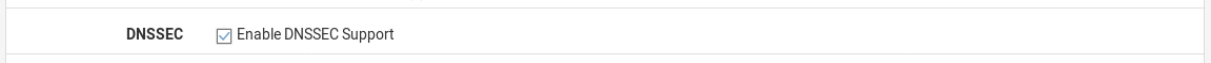
```
root@kali:~# dig @172.16.0.252 www.thomasmore.be

; <<>> DiG 9.11.5-P4-5.1+b1-Debian <<>> @172.16.0.252 www.thomasmore.be
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54215
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.thomasmore.be.             IN      A

;; ANSWER SECTION:
www.thomasmore.be.      1764    IN      A       62.213.218.216

;; Query time: 101 msec
;; SERVER: 172.16.0.252#53(172.16.0.252)
;; WHEN: Tue Feb 25 16:01:52 EST 2020
;; MSG SIZE  rcvd: 62
```

@pfSense > Diagnostics > States



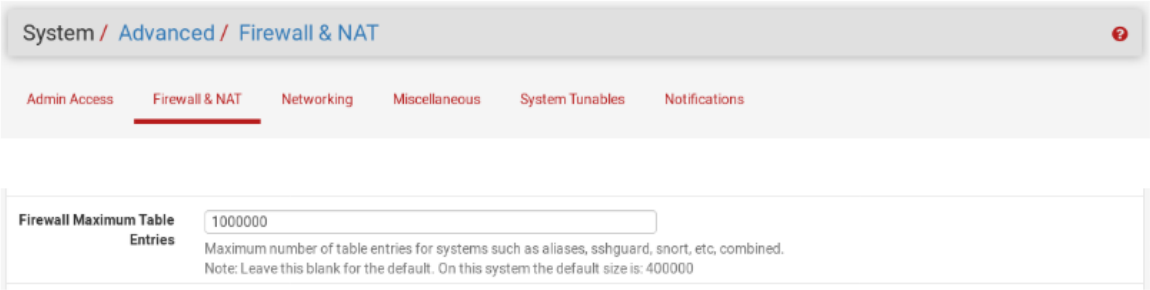
Stap 9: DNSSec instellen

@pfSense > Services > DNS Resolver

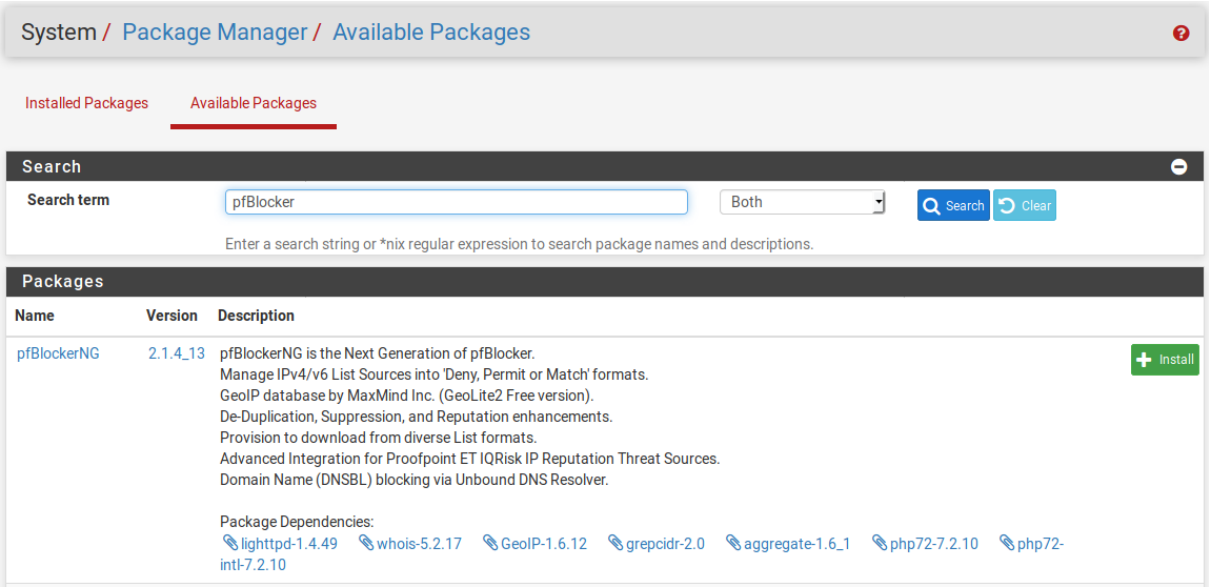


Stap 10: pfBlockerNG

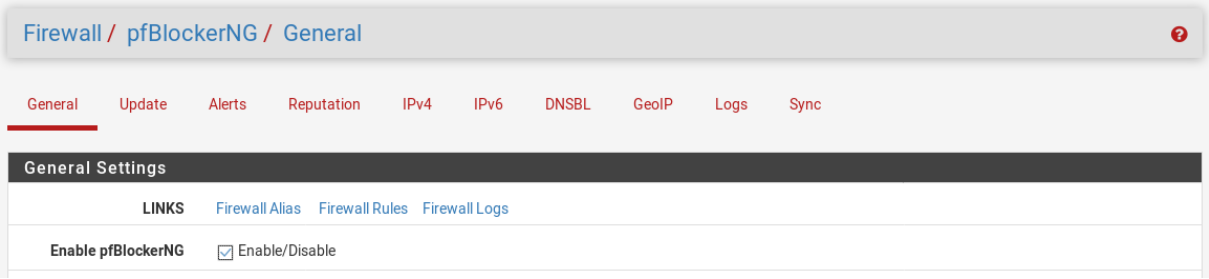
@pfSense > System > Advanced > Firewall & NAT

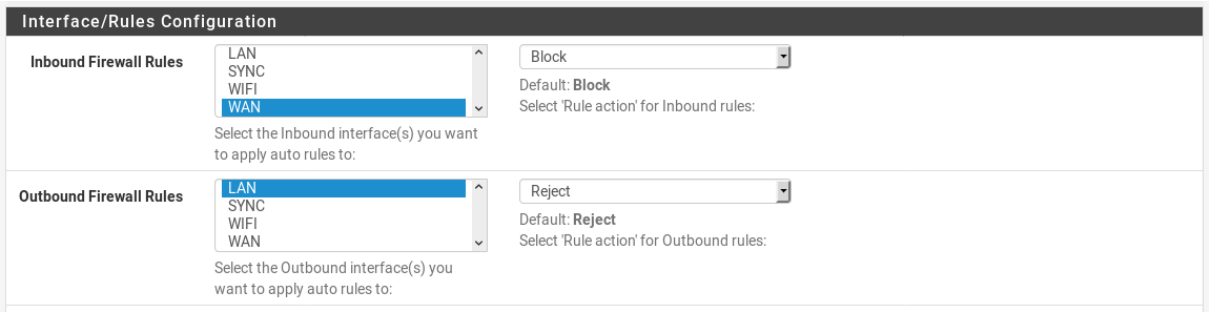


@pfSense > System > Package Manager

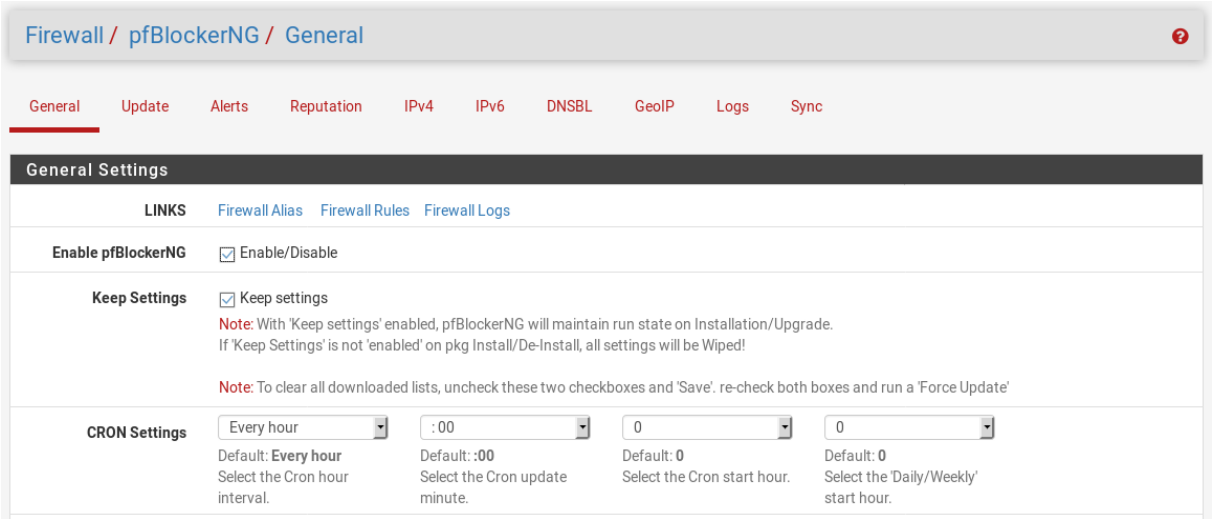


Enable pfBlockNG

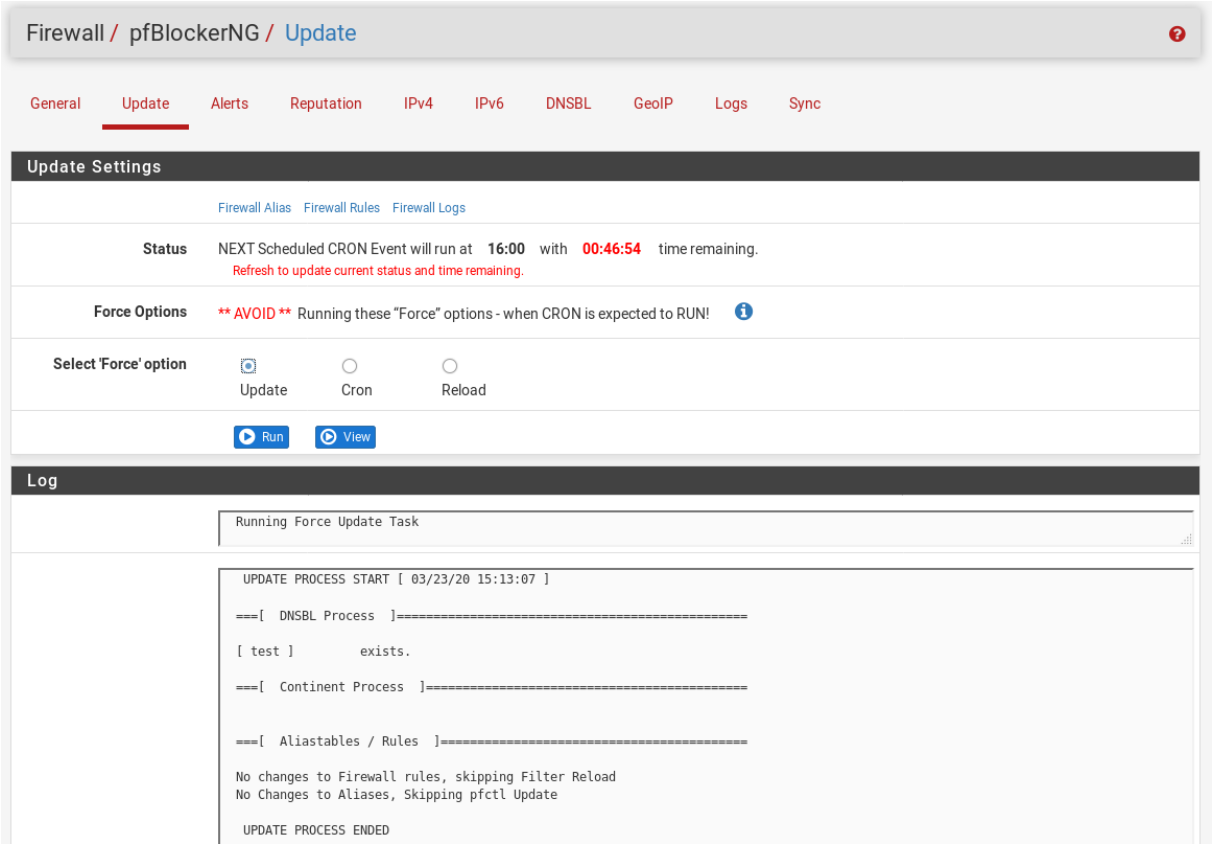




Cron Update Schedule



@pfSense > Firewall > pfBlockerNG > Update → run



@pfSense > Firewall > pfBlockerNG > IPv4

Firewall / pfBlockerNG / Edit / IPv4

General | Update | Alerts | Reputation | IPv4 | IPv6 | DNSBL | GeoIP | Logs | Sync

IPv4 Settings

LINKS	Firewall Alias Firewall Rules Firewall Logs
Alias Name	CiscoTalos Enter Alias Name (Example: Badguys) Do not include **'pfBlocker' or 'pfB_'** in the Alias Name, it's done by package. **International, special or space characters will be ignored in firewall alias names.**
List Description	Cisco Talos IP Blacklist
List Settings	
IPv4 Lists	Auto (Format) / ON (State) / https://talosintelligence.com/documents/ip-blacklist (Source) / CT_IPs (Header/Label)
Add	Add
List Action	Deny Both Default: **Disabled**
Update Frequency	Every Hour Default: **Never** Select how often List files will be downloaded. **This must be within the Cron Interval/Start Hour settings.**
Weekly (Day of Week)	Monday Default: **Monday** Select the 'Weekly' (Day of the Week) to Update This is only required for the 'Weekly' Frequency Selection. The 24 Hour Download 'Time' will be used.
Enable Logging	Enable Default: **Enable** Select - Logging to Status: System Logs: FIREWALL (Log) This can be overriden by the 'Global Logging' Option in the General Tab.

Resultaat:

Firewall / pfBlockerNG / IPv4

General | Update | Alerts | Reputation | IPv4 | IPv6 | DNSBL | GeoIP | Logs | Sync

Alias Name	Alias Description	Action	Frequency	Logging	
CiscoTalos	Cisco Talos IP Blacklist	Deny_Both	01hour	enabled	
					Add

Save

WAN

Firewall / Rules / WAN

Floating | WAN | LAN | SYNC | WIFI

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✖	0 /81 KiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	
✖	0 /0 B	IPv4 *	pfB_CiscoTalos	*	*	*	*	none		pfB_CiscoTalos auto rule	

LAN

Firewall / Rules / LAN

Floating | WAN | LAN | SYNC | WIFI

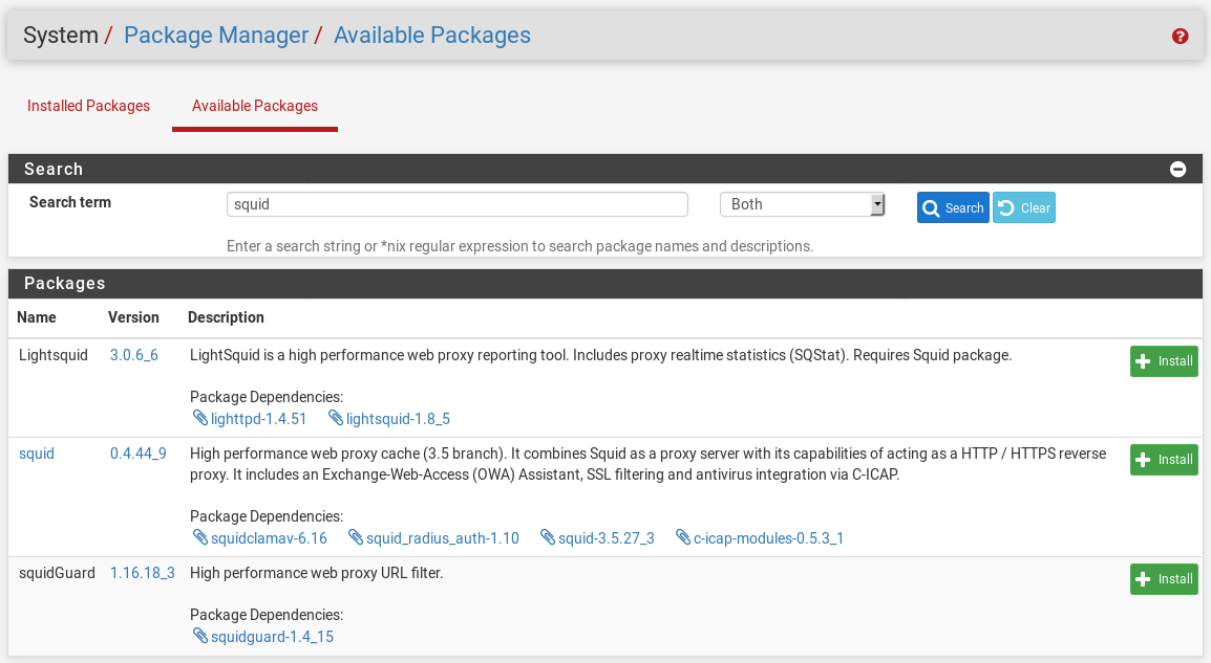
Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✔	1 /2.59 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
✖	0 /79 KiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	
	0 /0 B	IPv4 *	*	*	pfB_ CiscoTalos	*	*	none		pfB_CiscoTalos auto rule	

Stap 10: Squid ClamAV configureren

@pfSense > System > PacketManager > Packages

Squid zoeken en installeren



@pfSense > Services > Squid Proxy Server > Local Cache

Hard disk cache size (in MB) → 3000

@pfSense > Services > Squid Proxy Server > General

Enable squid proxy → aanvinken

Proxy Interface(s) → LAN

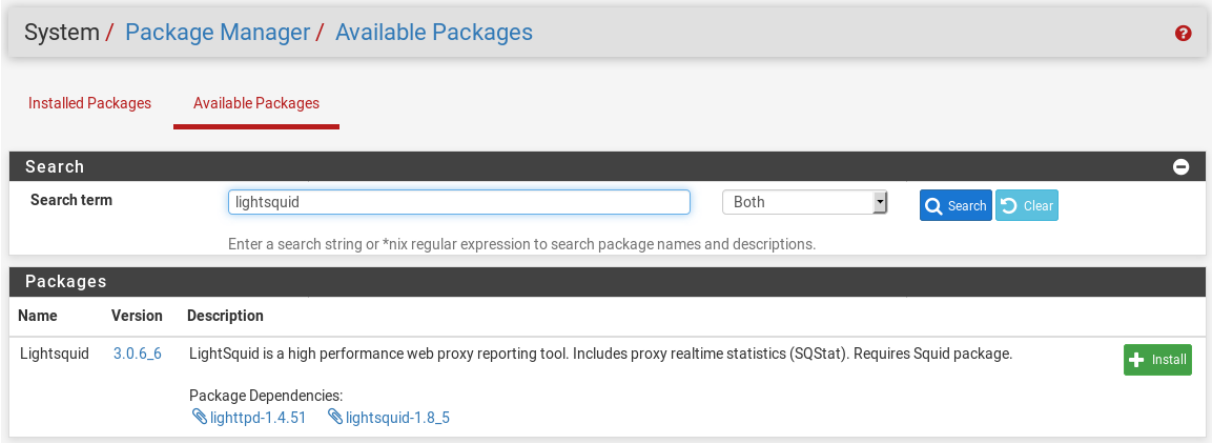
Transparent Proxy → niet aanvinken

Enabled logging → aanvinken

Log Store Directory → /var/squid/log

@pfSense > System > PacketManager > Packages

LightSquid installeren



Squid ClamAV aanzetten door onderstaande vakjes aan te vinken

@pfsense > services > squid proxy server > antivirus