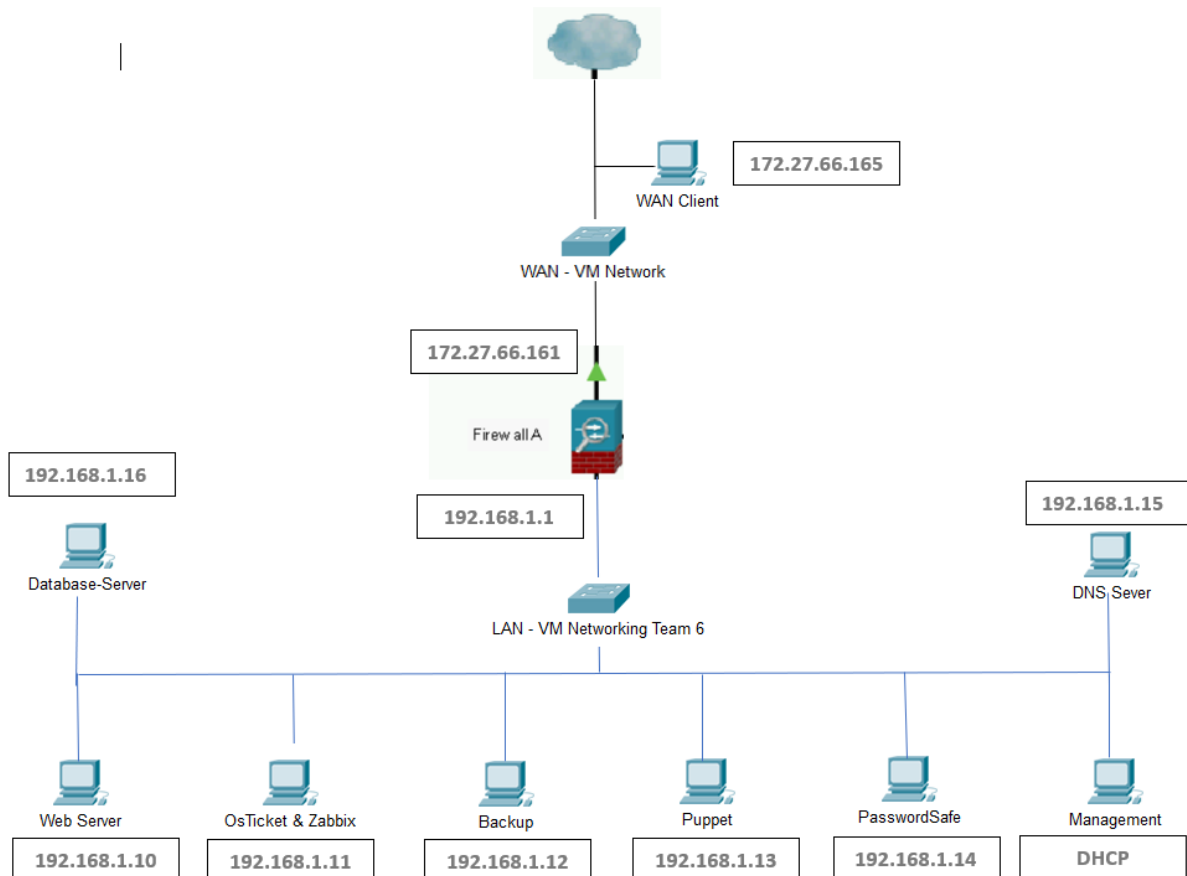


PfSense (Firewall): Handleiding

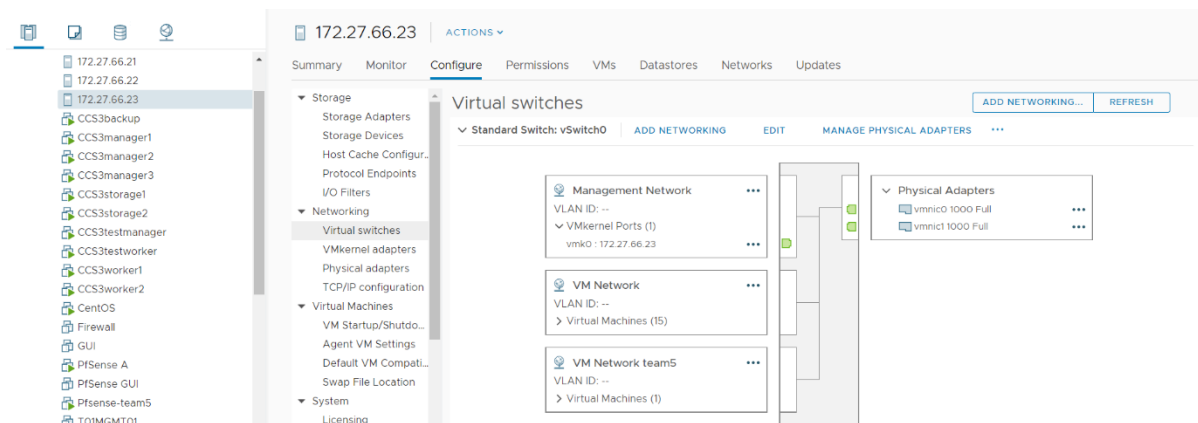
Topology



Bijvoegen Virtuele standard switch LAN kant.

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

Beginsituatie



Step 1: Add Networking!

Virtual switches

ADD NETWORKING...REFRESH

Standard Switch: vSwitch0

ADD NETWORKING

EDIT

MANAGE PHYSICAL ADAPTERS

...

Step 2

172.27.66.23 - Add Networking

1 Select connection type

2 Select target device

3 Connection settings

4 Ready to complete

Select connection type

Select a connection type to create.

☐ VMkernel Network Adapter

The VMkernel TCP/IP stack handles traffic for ESXi services such as vSphere vMotion, iSCSI, NFS, FCoE, Fault Tolerance, vSAN and host management.

☒ Virtual Machine Port Group for a Standard Switch

A port group handles the virtual machine traffic on standard switch.

☐ Physical Network Adapter

A physical network adapter handles the network traffic to other hosts on the network.

Step 3

172.27.66.23 - Add Networking

✓ 1 Select connection type

2 Select target device

3 Create a Standard Switch

4 Connection settings

5 Ready to complete

Select target device

Select a target device for the new connection.

☐ Select an existing standard switch

BROWSE ...

☒ New standard switch

MTU (Bytes)

1500

CANCEL

BACK

NEXT

Step 4: Add adapter vmnic2!

172.27.66.23 - Add Networking

- ✓ 1 Select connection type
- ✓ 2 Select target device
- 3 Create a Standard Switch**
- 4 Connection settings
- 5 Ready to complete

Create a Standard Switch

Assign free physical network adapters to the new switch.

Assigned adapters



Active adapters
Standby adapters
Unused adapters

Select a physical network adapter from the list to view its details.

Add Physical Adapters to the Switch

Network Adapters

vmnic2
vmnic3
vmnic4
vmnic5
vmnic6
vmnic7

All Properties CDP LLDP

Adapter	QLogic Corporation NC382i Integrated Multi Port PCI Express Gigabit Server Adapter
Name	vmnic2
Location	PCI 0000:04:00.0
Driver	qlgbe
Status	
Status	Connected
Actual speed, Duplex	1000 Mb, Full Duplex
Configured speed, Duplex	Auto negotiate
Network	No network

172.27.66.23 - Add Networking

- ✓ 1 Select connection type
- ✓ 2 Select target device
- ✓ 3 Create a Standard Switch
- 4 Connection settings**
- 5 Ready to complete

Connection settings

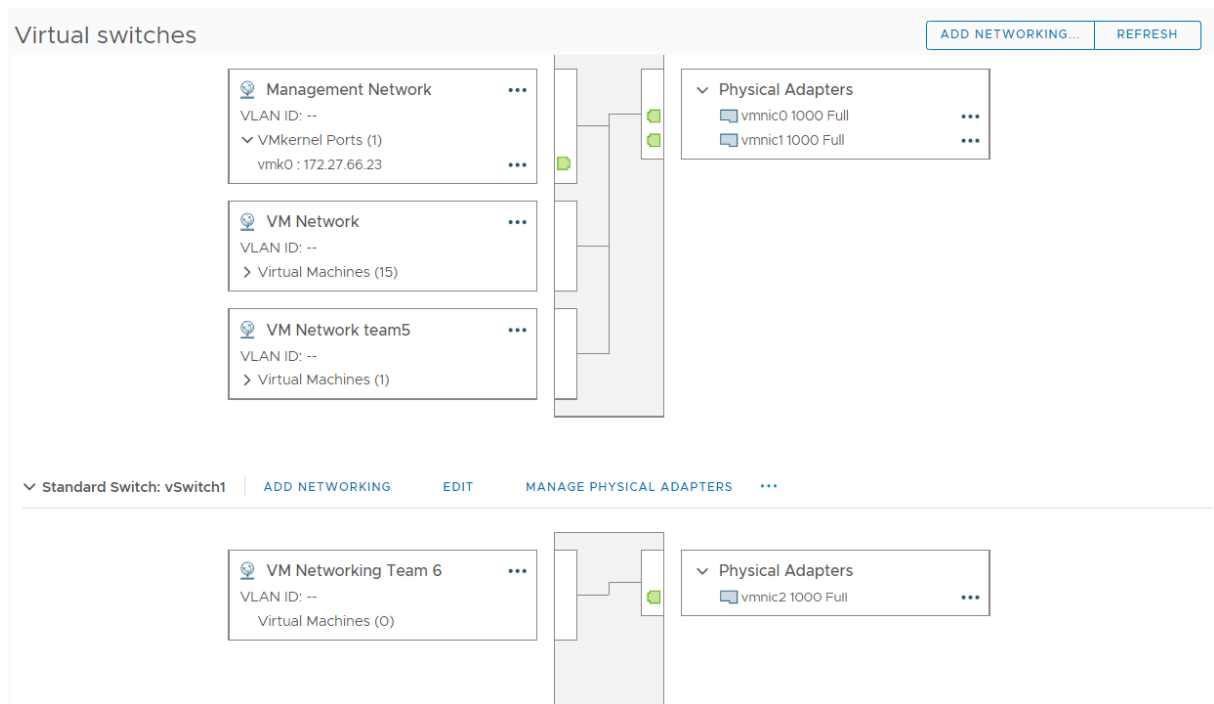
Use network labels to identify migration-compatible connections common to two hosts.

Network label VM Networking Team 6

VLAN ID

None (0)

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

Installed Packages					
Name	Category	Version	Description	Actions	
✓ Open-VM-Tools	emulators	10.1.0.1	VMware Tools is a suite of utilities that enhances the performance of the virtual machine's guest operating system and improves management of the virtual machine.	<div></div> <div></div>	
Package Dependencies:					
 open-vm-tools-nox11-10.2.5_1.2					

Stap 2: pfsense als NTP server instellen

@pfSense > Services > NTP

pfSense COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Services / NTP / Settings

Settings ACLs Serial GPS PPS

NTP Server Configuration

Interface: WAN LAN PFSYNC

Interfaces without an IP address will not be shown.
Selecting no interfaces will listen on all interfaces with a wildcard.
Selecting all interfaces will explicitly listen on only the interfaces/IPs specified.

Time Servers: ☐ Prefer ☐ No Select ☒ Is a Pool

Add + Add

NTP will only sync if a majority of the servers agree on the time. For best results you should configure between 3 and 5 servers ([NTP support pages recommend at least 4 or 5](#)), or a pool. If only one server is configured, it **will** be believed, and if 2 servers are configured and they disagree, **neither** will be believed. Options:
Prefer - NTP should favor the use of this server more than all others.
No Select - NTP should not use this server for time, but stats for this server will be collected and displayed.
Is a Pool - this entry is a pool of NTP servers and not a single address. This is assumed for *.pool.ntp.org.

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

Localization	
Timezone	<div>Europe/Brussels</div> <div>Select a geographic region name (Continent/Location) to determine the timezone for the firewall. Choose a special or "Etc" zone only in cases where the geographic zones do not properly handle the clock offset required for this firewall.</div>
Timeservers	<div>be.pool.ntp.org</div> <div>Use a space to separate multiple hosts (only one required). Remember to set up at least one DNS server if a host name is entered here!</div>
Language	<div>English</div> <div>Choose a language for the webConfigurator</div>

Stap 4: NTP server instellen

Services / NTP / Settings	
<div>Settings</div> <div>ACLs</div> <div>Serial GPS</div> <div>PPS</div>	
NTP Server Configuration	
Interface	<div>WAN</div> <div>LAN</div> <div>PFSYNC</div> <div>Interfaces without an IP address will not be shown. Selecting no interfaces will listen on all interfaces with a wildcard. Selecting all interfaces will explicitly listen on only the interfaces/IPs specified.</div>
Time Servers	<div>be.pool.ntp.org</div> <div><input type="checkbox"/> Prefer</div> <div><input type="checkbox"/> No Select</div> <div><input checked="" type="checkbox"/> Is a Pool</div>

Stap 5: Firewall rules instellen

Block bogon networks

@pfSense > Interfaces > WAN (vmx0)

Reserved Networks	
Block private networks and loopback addresses	<div><input type="checkbox"/></div> <div>Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.</div>
Block bogon networks	<div><input checked="" type="checkbox"/></div> <div>Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received. Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.</div>

Firewall / Rules / WAN											
<div> <div>Floating</div> <div>WAN</div> <div>LAN</div> <div>SYNC</div> </div>											
Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/41.31 MiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogus networks	

Firewall / Rules / Floating											
<div> <div>Floating</div> <div>WAN</div> <div>LAN</div> <div>SYNC</div> </div>											
Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	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							NAT IP	NAT Ports	Description	Actions	
<input type="checkbox"/>	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports					
<input type="checkbox"/>	WAN	TCP	*	*	WAN address	22 (SSH)	192.168.1.10	22 (SSH)	Forward SSH to Server		
<input type="checkbox"/>	WAN	TCP	*	*	WAN address	20	192.168.1.10	20	Forward FTP to Server		
<input type="checkbox"/>	WAN	TCP	*	*	WAN address	21 (FTP)	192.168.1.10	21 (FTP)	Forward FTP to Server		
<input type="checkbox"/>	WAN	TCP	*	*	WAN address	443 (HTTPS)	192.168.1.10	443 (HTTPS)	Open webServer to Internet		
<input type="checkbox"/>	WAN	TCP	*	*	WAN address	80 (HTTP)	192.168.1.10	80 (HTTP)	Open webServer to Internet		
<input type="checkbox"/>	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

Services / **DNS Forwarder**

General DNS Forwarder Options

Enable ☐ Enable DNS forwarder

@pfSense > Services > DNS Resolver

Services / **DNS Resolver** / General Settings

General Settings Advanced Settings Access Lists

General DNS Resolver Options

Enable ☐ Enable 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

System / **General Setup**

System

Hostname
Name of the firewall host, without domain part

Domain
Do not use '.local' as the final part of the domain (TLD). The '.local' domain is **widely used** by mDNS (including Avahi and Apple OS Bonjour/Rendezvous/Airprint/Airplay), and some Windows systems and networked devices. These will not network correctly if they use '.local'. Alternatives such as '.local.lan' or '.mylocal' are safe.

DNS Server Settings

DNS Servers	1.1.1.1	DNS Hostname	none	Delete
	<input type="text" value="1.0.0.1"/> Address Enter IP addresses to be used by the system for DNS resolution. These are also used for the DHCP service, DNS Forwarder and DNS Resolver when it has DNS Query Forwarding enabled.	<input type="text" value="DNS Hostname"/> Hostname Enter the DNS Server Hostname for TLS Verification in the DNS Resolver (optional).	<input type="text" value="none"/> Gateway Optionally select the gateway for each DNS server. When using multiple WAN connections there should be at least one unique DNS server per gateway.	Delete

@pfSense > Services > DNS Forwarder

Services / DNS Forwarder

General DNS Forwarder Options

Enable ☒ Enable 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

Services / DNS Forwarder

General DNS Forwarder Options

Enable ☐ Enable DNS forwarder

@pfSense > Services > DNS Resolver

Services / DNS Resolver / General Settings

General Settings Advanced Settings Access Lists

General DNS Resolver Options

Enable ☒ Enable DNS resolver

Listen Port

The port used for responding to DNS queries. It should normally be left blank unless another service needs to bind to TCP/UDP port 53.

Network Interfaces

All

WAN

LAN

SYNC

WAN1DnsLinkLocal

Interface IPs used by the DNS Resolver for responding to queries from clients. If an interface has both IPv4 and IPv6 IPs, both are used. Queries to other interface IPs not selected below are discarded. The default behavior is to respond to queries on every available IPv4 and IPv6 address.

DNSSEC

☐ Enable DNSSEC Support

DNS Query Forwarding

☐ Enable Forwarding Mode

If this option is set, DNS queries will be forwarded to the upstream DNS servers defined under [System > General Setup](#) or those obtained via DHCP/PPP on WAN (if DNS Server Override is enabled there).

DHCP Registration

☒ Register DHCP leases in the DNS Resolver

If this option is set, then machines that specify their hostname when requesting an IPv4 DHCP lease will be registered in the DNS Resolver so that their name can be resolved. The domain in [System > General Setup](#) should also be set to the proper value.

@pfSense > System > General Setup

System / General Setup

System

Hostname

pfSense-A

Name of the firewall host, without domain part

Domain

mydomain.com

Do not use '.local' as the final part of the domain (TLD). The '.local' domain is widely used by mDNS (including Avahi and Apple OS X's Bonjour/Rendezvous/Airprint/Airplay), and some Windows systems and networked devices. These will not network correctly if the router uses '.local'. Alternatives such as '.local.lan' or '.mylocal' are safe.

DNS Server Settings

DNS Servers

DNS Server

DNS Hostname

none

Add DNS Server

+ Add DNS Server

DNS Server Override

☐ Allow DNS server list to be overridden by DHCP/PPP on WAN

If this option is set, pfSense will use DNS servers assigned by a DHCP/PPP server on WAN for its own purposes (including the DNS Forwarder/DNS Resolver). However, they will not be assigned to DHCP clients.

Disable DNS Forwarder

☐ Do not use the DNS Forwarder/DNS Resolver as a DNS server for the firewall

By default localhost (127.0.0.1) will be used as the first DNS server where the DNS Forwarder or DNS Resolver is enabled and set to listen on localhost, so system can use the local DNS service to perform lookups. Checking this box omits localhost from the list of DNS servers in resolv.conf.

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.      894  4    IN    A      320  320  0      0
;; ANSWER SECTION:
thomasmore.be.      895  0    IN    A      62.213.218.216
;ol.ntp.org.        896  19   IN    A      455  455  0      0
;; 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

System / General Setup

System

Hostname

pfSense-A

Name of the firewall host, without domain part

Domain

mydomain.com

Do not use '.local' as the final part of the domain (TLD). The '.local' domain is widely used by mDNS (including Avahi and Apple OS X Bonjour/Rendezvous/Airprint/Airplay), and some Windows systems and networked devices. These will not network correctly if the Alternatives such as '.local.lan' or '.mylocal' are safe.

DNS Server Settings

DNS Servers

1.1.1.1

cloudflare-dns.com

none

Delete

1.0.0.1

cloudflare-dns.com

none

Delete

Address

Enter IP addresses to be used by the system for DNS resolution. These are

Hostname

Enter the DNS Server Hostname for TLS Verification in the DNS

Gateway

Optionally select the gateway for each DNS server. When using

@pfSense > Services > DNS Resolver > General Settings

DNS Query Forwarding

☒ Enable Forwarding Mode

If this option is set, DNS queries will be forwarded to the upstream DNS servers defined under [System > General Setup](#) or those obtained via DHCP/PPP on WAN (if DNS Server Override is enabled there).

☒ Use SSL/TLS for outgoing DNS Queries to Forwarding Servers

When set in conjunction with DNS Query Forwarding, queries to all upstream forwarding DNS servers will be sent using SSL/TLS on the default port of 853. Note that ALL configured forwarding servers MUST support SSL/TLS queries on port 853.

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

Diagnostics / States / States

States

Reset States

State Filter

Interface

all

Filter expression

1.1.1.1

Filter

Kill filtered states

Kill States

Remove all states to and from the filtered address

States

Interface	Protocol	Source (Original Source) -> Destination (Original Destination)	State	Packets	Bytes
WAN	tcp	10.0.2.4:47488 -> 1.1.1.1:853	FIN_WAIT_2:FIN_WAIT_2	12 / 7	1 KiB / 3 KiB

Stap 9: DNSSec instellen

@pfSense > Services > DNS Resolver

DNSSEC

☒ Enable DNSSEC Support

Stap 10: pfBlockerNG

@pfSense > System > Advanced > Firewall & NAT

System / Advanced / Firewall & NAT

Admin Access

Firewall & NAT

Networking

Miscellaneous

System Tunables

Notifications

Firewall Maximum Table Entries

1000000

Maximum number of table entries for systems such as aliases, sshguard, snort, etc, combined.
Note: Leave this blank for the default. On this system the default size is: 400000

@pfSense > System > Package Manager

[System](#) / [Package Manager](#) / [Available Packages](#)

Installed Packages

Available Packages

Search

Search term

pfBlocker

Both

Search

Clear

Enter a search string or *nix regular expression to search package names and descriptions.

Packages

Name	Version	Description
pfBlockerNG	2.1.4_13	<p>pfBlockerNG is the Next Generation of pfBlocker.</p> <p>Manage IPv4/v6 List Sources into 'Deny, Permit or Match' formats.</p> <p>GeoIP database by MaxMind Inc. (GeoLite2 Free version).</p> <p>De-Duplication, Suppression, and Reputation enhancements.</p> <p>Provision to download from diverse List formats.</p> <p>Advanced Integration for Proofpoint ET IQRisk IP Reputation Threat Sources.</p> <p>Domain Name (DNSBL) blocking via Unbound DNS Resolver.</p>

Package Dependencies:

[lighttpd-1.4.49](#) [whois-5.2.17](#) [GeoIP-1.6.12](#) [grepclid-2.0](#) [aggregate-1.6_1](#) [php72-7.2.10](#) [php72-intl-7.2.10](#)

+ Install

Enable pfBlockNG

[Firewall](#) / [pfBlockerNG](#) / [General](#)

General

Update

Alerts

Reputation

IPv4

IPv6

DNSBL

GeoIP

Logs

Sync

General Settings

LINKS

[Firewall Alias](#) [Firewall Rules](#) [Firewall Logs](#)

Enable pfBlockerNG

☒ Enable/Disable

Interface/Rules Configuration

Inbound Firewall Rules

LAN
SYNC
WIFI
WAN

Select the Inbound interface(s) you want to apply auto rules to:

Outbound Firewall Rules

LAN
SYNC
WIFI
WAN

Select the Outbound interface(s) you want to apply auto rules to:

Block

Default: Block

Select 'Rule action' for Inbound rules:

Reject

Default: Reject

Select 'Rule action' for Outbound rules:

Cron Update Schedule

Firewall / pfBlockerNG / General ?

General Update Alerts Reputation IPv4 IPv6 DNSBL GeolP Logs Sync

General Settings

LINKS Firewall Alias Firewall Rules Firewall Logs

Enable pfBlockerNG ☒ Enable/Disable

Keep Settings ☒ Keep settings
Note: With 'Keep settings' enabled, pfBlockerNG will maintain run state on Installation/Upgrade.
If 'Keep Settings' is not 'enabled' on pkg Install/De-Install, all settings will be Wiped!
Note: To clear all downloaded lists, uncheck these two checkboxes and 'Save'. re-check both boxes and run a 'Force Update'

CRON Settings
Every hour :00 0 0
Default: Every hour Select the Cron hour interval. Default: :00 Select the Cron update minute. Default: 0 Select the Cron start hour. Default: 0 Select the 'Daily/Weekly' start hour.

@pfSense > Firewall > pfBlockerNG > Update → run

Firewall / pfBlockerNG / Update ?

General Update Alerts Reputation IPv4 IPv6 DNSBL GeolP Logs Sync

Update Settings

Firewall Alias Firewall Rules Firewall Logs

Status NEXT Scheduled CRON Event will run at 16:00 with 00:46:54 time remaining.
[Refresh to update current status and time remaining.](#)

Force Options **** AVOID **** Running these "Force" options - when CRON is expected to RUN! i

Select 'Force' option ☒ Update ☐ Cron ☐ Reload

[Run](#) [View](#)

Log

Running Force Update Task

UPDATE PROCESS START [03/23/20 15:13:07]
====[DNSBL Process]=====

[test] exists.

====[Continent Process]=====

====[Aliastables / Rules]=====

No changes to Firewall rules, skipping Filter Reload
No Changes to Aliases, Skipping pfctl Update

UPDATE PROCESS ENDED

@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
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

List Settings ⓘ

IPv4 Lists
Format State Source Header/Label

Add

List Action
Default: Disabled ⓘ

Update Frequency
Default: Never
Select how often List files will be downloaded. This must be within the Cron Interval/Start Hour settings.



Weekly (Day of Week)
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
Default: Enable
Select - Logging to Status: System Logs: FIREWALL (Log)
This can be overridden 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	 
					<input type="button" value="+ Add"/>

 Save

WAN

Firewall / Rules / WAN

Floating WAN LAN SYNC WIFI

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0 / 81 KiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	
<input type="checkbox"/>	0 / 0 B	IPv4 *	pfB_CiscoTalos	*	*	*	*	none		pfB_CiscoTalos auto rule	

LAN

Firewall / Rules / LAN

Floating WAN LAN SYNC WIFI

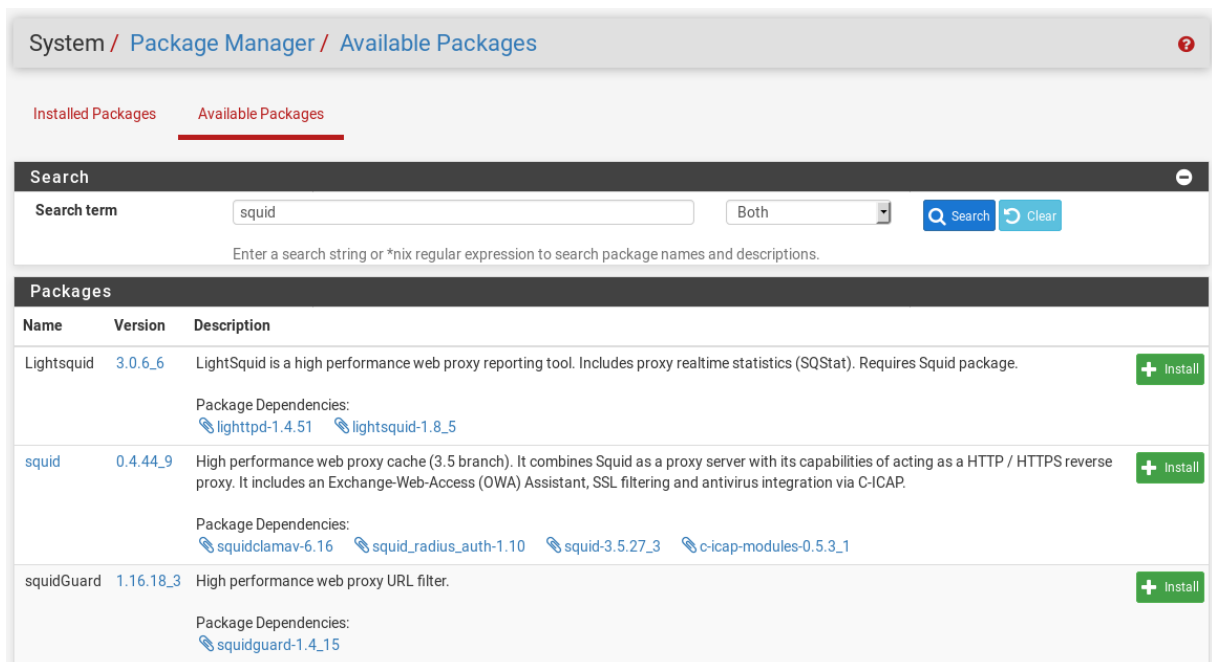
Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	1 / 2.59 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input checked="" type="checkbox"/>	0 / 79 KiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	
<input type="checkbox"/>	0 / 0 B	IPv4 *	*	*	pfB_CiscoTalos	*	*	none		pfB_CiscoTalos auto rule	

Stap 10: Squid ClamAV configureren

@pfSense > System > PacketManager > Packages

Squid zoeken en installeren



System / Package Manager / Available Packages

Installed Packages Available Packages

Search

Search term: squid Both Search Clear

Enter a search string or *nix regular expression to search package names and descriptions.

Packages

Name	Version	Description	
Lightsquid	3.0.6_6	LightSquid is a high performance web proxy reporting tool. Includes proxy realtime statistics (SQStat). Requires Squid package. Package Dependencies: lighttpd-1.4.51 lightsquid-1.8_5	+ Install
squid	0.4.44_9	High performance web proxy cache (3.5 branch). It combines Squid as a proxy server with its capabilities of acting as a HTTP / HTTPS reverse proxy. It includes an Exchange-Web-Access (OWA) Assistant, SSL filtering and antivirus integration via C-ICAP. Package Dependencies: squidclamav-6.16 squid_radius_auth-1.10 squid-3.5.27_3 c-icap-modules-0.5.3_1	+ Install
squidGuard	1.16.18_3	High performance web proxy URL filter. Package Dependencies: squidguard-1.4_15	+ Install

@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

System / Package Manager / Available Packages

Installed Packages Available Packages

Search

Search term Both

Enter a search string or *nix regular expression to search package names and descriptions.

Packages

Name	Version	Description
Lightsquid	3.0.6_6	LightSquid is a high performance web proxy reporting tool. Includes proxy realtime statistics (SQStat). Requires Squid package.

Package Dependencies:
[lighttpd-1.4.51](#) [lightsquid-1.8_5](#)

Squid ClamAV aanzetten door onderstaande vakjes aan te vinken

@pfsense > services > squid proxy server > antivirus

pfsense COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

Package / Proxy Server: Antivirus / Antivirus

General Remote Cache Local Cache Antivirus ACLs Traffic Mgmt Authentication Users Real Time Sync

ClamAV Anti-Virus Integration Using C-ICAP

Enable AV ☒ Enable Squid antivirus check using ClamAV.

Google Safe Browsing ☒ Enables Google Safe Browsing support.
 Google Safe Browsing database includes information about websites that may be phishing sites or possible sources of malware.
Warning: This option consumes significant amount of RAM.

ClamAV Database Update

Optionally, you can schedule ClamAV definitions updates via cron. Select the desired frequency here. [i](#)

Important: Set to 'every 1 hour' if you want to use Google Safe Browsing feature.
 Click the button below **once** to force the update of AV databases immediately. **Note:** This will take a while. Check freshclam log on the 'Real Time' tab for progress information.