

# Documentatie Configuratie PfSense:

## Inhoudsopgave

1. [Intro](#)
2. [Algemene configuratie](#)
3. [Vlans](#)
4. [Firewall](#)
  - 4.1. [Aliases](#)
  - 4.2. [Firewall Regels](#)
5. [Automatisatie](#)
6. [Routing](#)
7. [Bronnen](#)

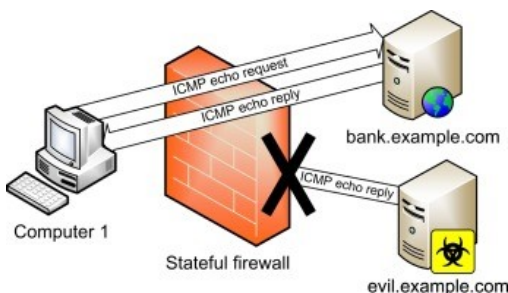
## 1. Intro

Voor we beginnen met het configureren van deze firewall moeten we eerst weten hoe PfSense werkt en wat we precies willen doen met PfSense.

PfSense is een [Stateful](#) firewall. Bij default zal PfSense al het verkeer tegenhouden die door de WAN interface gaat. Dit betekent dat als er bijvoorbeeld verkeer komt van een ander netwerk of het internet door de firewall, zal PfSense deze packets bij default tegenhouden door een impliciete firewall regel op de WAN interface.

Als je host systeem bijvoorbeeld op de LAN bevindt en naar google.com gaat, controleert PfSense de LAN interface regels en staat het verkeer toe door de default LAN regels. Het creëert dan een staat. Een staat is wat de firewall vertelt wat er aan de hand is met elke verbinding die met succes tot stand is gebracht. De firewall houdt ze allemaal bij in een statustabel.

Bij elke status onthoudt de firewall een hoop informatie over die verbinding. Het weet dat een bepaalde PC verbinding heeft gemaakt met website google.com door een bepaalde poort. Als PfSense vervolgens een antwoord van google.com ontvangt zal PfSense dit verkeer toelaten naar de PC. Staten duren niet te lang en zullen vervallen nadat ze inactief zijn.



In dit project heeft onze firewall de volgende taken:

- zulu2 bevindt zich tussen VLANs 600 en 700.
- OS: De meest recente stabiele versie van PfSense.
- Deze Firewall heeft NAT uitgeschakeld! NAT is actief op de router Router1.
- Configureer deze firewall zodanig dat enkel die poorten openstaan die echt nodig zijn binnen uw netwerk.
- Configureer deze firewall zodanig dat je vanuit elk subnet van je netwerk/LAN(zowel de VLANs als de router subnets) kan communiceren met het internet.

In de volgende secties zullen we PfSense stap voor stap configureren zodat het elke taak wordt gerealiseerd.

## 2. Algemene configuratie

Voor we beginnen met de echte doelfunctionaliteit in te stellen van PfSense gaan we eerst zorgen dat de benaming, timezone, routing,... enzovoort van de firewall goed is ingesteld. We beginnen met de benaming en timezone, vergeet niet op save te klikken na elke wijziging.

- Navigeer naar System -> General Setup
  - Hostname: Zulu2
  - Domain: red.local

**System**

Hostname

Zulu2

Name of the firewall host, without domain part

Domain

red.local

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.

- Zet de timezone in naar Brussel.
  - Timezone: Europe/Brussels

**Localization**

Timezone

Europe/Brussels

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.

Nu moeten we nog de router "Router1" toevoegen als default gateway voor onze firewall.

- Navigeer naar System -> Routing
  - Klik op Add
  - Gateway: 172.18.1.105
  - Description: Router1

Gateways							
	Name	Default	Interface	Gateway	Monitor IP	Description	Actions
<input checked="" type="checkbox"/>	WANGW (default)	Default (IPv4)	WAN	172.18.1.105	172.18.1.105	Router1	

Het admin account gebruik nog steeds het default password "pfsense", we gaan dit ook veranderen.

- Navigeer naar System -> User Manager
  - Klik op Edit User van admin (Potlood)
  - Password: Admin2019

We moeten outbound NAT uitschakelen omdat dit de taak is van Router1.

- Navigeer naar Firewall -> NAT
  - Klik op de Outbound tab
  - Vink Disable Outbound NAT rule generation aan

Outbound NAT Mode				
Mode	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Automatic outbound NAT rule generation. (IPsec passthrough included)		Hybrid Outbound NAT rule generation. (Automatic Outbound NAT + rules below)	Manual Outbound NAT rule generation. (AON - Advanced Outbound NAT)	Disable Outbound NAT rule generation. (No Outbound NAT rules)

We gaan DHCP requests relaysen naar de DHCP server in ons domein. (zorg dat DHCP server uit staat)

- Navigeer naar Services -> DHCP Relay
  - Vink Enable DHCP relay on interface aan
  - Kies LAN interface
  - Destination Server: 172.18.1.1

**DHCP Relay Configuration**

**Enable** ☒ Enable DHCP relay on interface

**Interface(s)**

WAN  
 LAN

Interfaces without an IP address will not be shown.

☐ Append circuit ID and agent ID to requests  
 If this is checked, the DHCP relay will append the circuit ID (pfSense interface number) and the agent ID to the DHCP request.

**Destination server**

172.18.1.1

This is the IPv4 address of the server to which DHCP requests are relayed.




### 3. Vlans

We gaan 2 Vlans "600" en "700" toevoegen aan de firewall.

- Navigeer naar Interfaces -> Assignments
  - Ga naar de VLans tab
  - Klik op Add
  - Parent Interface: Wan
  - Vlan Tag: 700


Nu moeten we hetzelfde doen voor LAN interface.

- Klik op Add
- Parent Interface: Lan
- Vlan Tag: 600

VLAN Interfaces				
Interface	VLAN tag	Priority	Description	Actions
em0 (wan)	700			 
em1 (lan)	600			 

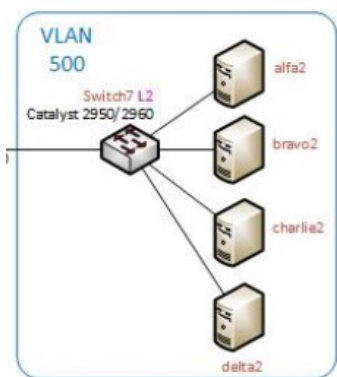
We moeten deze interfaces nog manueel toevoegen.

- Ga naar de Interface Assignments tab
- Klik 2 keer op Add

Interface	Network port	
WAN	em0 (08:00:27:8b:94:60)	
LAN	em1 (08:00:27:d0:e8:aa)	 Delete
OPT1	VLAN 700 on em0 - wan	 Delete
OPT2	VLAN 600 on em1 - lan	 Delete

## 4. Firewall

We moeten onze firewall instellen zodanig dat de juiste (niet alle!) poorten openstaan van servers in VLAN 500 zodat andere netwerken ermee kunnen communiceren. Deze servers zijn: alfa2 (Domeincontroller met DNS), bravo2 (2de Domeincontroller en DNS), charlie2 (mailserver) en delta2 (webserver).





### 4.1 Aliases

Voor we regels toevoegen aan de firewall, gaan we Ip's en poorten groeperen om het ons gemakkelijker te maken. We zullen zo in het totaal veel minder regels moeten toevoegen. We gaan eerst Ip's van de Domeincontrollers groeperen, en dan groeperen we de poorten.























- Navigeer naar Firewall -> Aliases
  - Klik op Add
  - Name: Domeincontrollers
  - Ip: 172.18.1.66 (alpha2)
  - Ip: 172.18.1.67 (bravo2)

#### Firewall Aliases IP

Name	Values	Description	Actions
DomeinControllers	172.18.1.66, 172.18.1.67		 

Nu gaan we alle poorten toevoegen die we nodig hebben en deze groeperen. Hier is een lijst van alle poorten die worden gebruikt voor windows servers.

- Klik op de Ports tab
- Voeg de aliases toe met dezelfde values als onderstaande afbeelding








































































Firewall Aliases Ports			
Name	Values	Description	Actions
ADWSPorts	9389	Ports for ADWS	 
DNSServer	53	Ports for DNS Server	 
GCPorts	3268, 3269	Ports for Global Catalog	 
IPsecISAKMP	500	Ports for IPsec ISAKMP	 
LDAPPorts	389, 636	Ports for LDAP	 
Mailserver	143, 993, 110, 995, 25, 587, 2525, 465, 25025	Ports for Mailserver	 
NATTPorts	4500	Ports for NAT-T	 
PRTGPorts	8085, 23560, 23570	Ports for PRTG	 
RPCPorts	135, 49152:65535	Ports for RPC	 
SMBPorts	445	Ports for SMB	 
Webserver	443, 80	Ports for webserver	 

Nu kunnen we naar de firewall regels gemakkelijker instellen.

## 4.2 Firewall Regels

Omdat PfSense een [Stateful](#) moeten we alleen regels toevoegen aan de WAN interface. Andere netwerken kunnen initieel communiceren met specifieke poorten en hosts die wij zullen bepalen.

- Navigeer naar Firewall -> Rules
- Voeg één voor één de regels toe aan de Wan interface met dezelfde values als onderstaande afbeelding.

Rules (Drag to Change Order)												
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions	
	0 / 0 B	*	RFC 1918 networks	*	*	*	*	*		Block private networks		
	0 / 0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks		
	 0 / 0 B	IPv4 TCP	*	*	172.18.1.68	Mailserver	*	none			   	
	 0 / 0 B	IPv4 TCP	*	*	172.18.1.69	Webserver	*	none			   	
	 0 / 0 B	IPv4 TCP	*	*	DomeinControllers	GCPorts	*	none			   	
	 0 / 0 B	IPv4 TCP	*	*	DomeinControllers	ADWSPorts	*	none			   	
	 0 / 0 B	IPv4 TCP/UDP	*	*	DomeinControllers	LDAPPorts	*	none			   	
	 0 / 0 B	IPv4 UDP	*	*	DomeinControllers	IPsecISAKMP	*	none			   	
	 0 / 0 B	IPv4 UDP	*	*	DomeinControllers	NATTPorts	*	none			   	
	 0 / 0 B	IPv4 TCP	*	*	DomeinControllers	RPCPorts	*	none			   	
	 0 / 0 B	IPv4 TCP	*	*	DomeinControllers	SMBPorts	*	none			   	
	 0 / 0 B	IPv4 TCP/UDP	*	*	DomeinControllers	DNSServer	*	none			   	
	 0 / 0 B	IPv4 ICMP any	172.16.0.0/16	*	*	*	*	none			   	

PfSense is nu volledig configureerd en is klaar voor de productieomgeving, we moeten alleen nog de interface namen en LAN ip veranderen in de productieomgeving zelf.

## 5. Automatisatie

Om het hele installatie en configuratie proces te versnellen is het nodig om zoveel mogelijk te automatiseren. Voor PfSense bestaan er ook Vagrant boxes, maar omdat deze boxes outdated zijn en het niet zo praktisch is om met vagrant in productieomgeving te werken gaan we gewoon met de ISO file werken. Het manueel installeren van PfSense duurt niet lang, alleen het configureren kan veel tijd in beslag nemen. Voor de configuratie van PfSense te automatiseren bestaat er een tool op de WebGUI die ons kan helpen. PfSense kan namelijk een XML bestand lezen (of opslaan) waarin alle configuratie staat en deze uitvoeren op het systeem, dit zullen we nu proberen.

We maken een backup te maken van de configuratie.

- Navigeer naar Diagnostics -> Backup & Restore
  - Backup Area: All
  - Download configuration as XML

Backup Configuration	
Backup area	All
Skip packages	<input type="checkbox"/> Do not backup package information.
Skip RRD data	<input checked="" type="checkbox"/> Do not backup RRD data (NOTE: RRD Data can consume 4+ megabytes of config.xml space!)
Encryption	<input type="checkbox"/> Encrypt this configuration file.
<a href="#">Download configuration as XML</a>	

We laden een custom configuratie.



- Navigeer naar Diagnostics -> Backup & Restore
  - Restore Area: All
  - Configuration File: Zulu2 (XML file voor productieomgeving)
  - Restore Configuration

Restore Backup	
Open a pfSense configuration XML file and click the button below to restore the configuration.	
Restore area	All
Configuration file	<a href="#">Choose File</a> Zulu2.xml
Encryption	<input type="checkbox"/> Configuration file is encrypted.
<a href="#">Restore Configuration</a>	
The firewall will reboot after restoring the configuration.	

## 6. Routing

Omdat onze firewall tussen 2 routers bevindt, moeten we ook doen aan routing. Wij kiezen ervoor om statische routes toe te voegen in plaats van dynamische routing (OSPF) te gebruiken. Dit komt omdat OSPF de routing tables niet wil bijhouden bij pfsense in de productie. Het is ook veel meer werk om dynamische routing in te zetten omdat we dan ook de package manager moeten updaten en dus direct internet connectie nodig hebben in de productieomgeving.

- Navigeer naar System -> Routing
- Navigeer naar Static Routes tab
- Voeg één voor één de static routes toe volgens de onderstaand afbeelding

Static Routes					
	Network	Gateway	Interface	Description	Actions
✔	172.18.1.64/27	LAN_Gateway - 172.18.1.101	LAN		   
✔	172.18.1.96/30	LAN_Gateway - 172.18.1.101	LAN		   
✔	172.18.1.0/26	LAN_Gateway - 172.18.1.101	LAN		   
✔	172.18.0.0/24	LAN_Gateway - 172.18.1.101	LAN		   

## 7. Bronnen

<http://pfsensesetup.com/ip-spoofing-and-defenses/>

<https://docs.netgate.com/pfsense/en/latest/nat/index.html>

<https://docs.netgate.com/pfsense/en/latest/book/config/pfsense-xml-configuration-file.html>

<https://docs.netgate.com/pfsense/en/latest/config/manually-editing-the-pfsense-configuration.html>

<https://docs.netgate.com/pfsense/en/latest/usermanager/locked-out-of-the-webgui.html>

<https://nguvu.org/pfsense/pfsense-baseline-setup/>

<https://docs.netgate.com/pfsense/en/latest/book/firewall/firewall-fundamentals.html>

<https://support.microsoft.com/en-us/help/832017/service-overview-and-network-port-requirements-for-windows>