

PFSENSE

Noah MAILLET
Projet Sandbox





Table of contents

1	Preface.	3
1.1	Présentation de PFSense.....	3
1.2	Prérequis.....	3
2	Création de la machine virtuelle.	4
2.1	Ajout d'une carte réseau.....	7
3	Installation PFSense.....	8
4	Configuration PFSense.....	11
4.1	Interface WAN.	11
4.2	Interface LAN.....	13
4.3	Configuration WebInterface.	14
5	Configuration PFSense – Projet Sandbox.	17
5.1	Règle du Pare-feu – LAN.	17
5.2	Règle du Pare-feu – DMZ.	18
5.3	Règle du Pare-feu – Lan_USER_X.....	19
5.4	NAT	20



1 Preface.

1.1 Présentation de PFSENSE

PFsense est un logiciel open source de pare-feu et de routage basé sur le système d'exploitation FreeBSD. Il est conçu pour fournir une solution de sécurité réseau puissante, flexible et économique, avec un support professionnel disponible. Créé en 2004 par Chris Buechler et Scott Ullrich, PFSense est devenu l'un des pare-feux open source le plus populaire et est utilisé par des milliers d'administrateurs réseau dans le monde entier.

Principales caractéristiques de PFSense :

1. **Interface graphique intuitive** : PFSense offre une interface Web facile à utiliser pour la configuration et la gestion du pare-feu. Cette interface rend la configuration et la surveillance du réseau accessibles même pour les utilisateurs qui ne sont pas des experts en informatique.
2. **Sécurité avancée** : PFSense offre des fonctionnalités de sécurité avancées telles que la protection contre les attaques DDoS, le filtrage des paquets, le blocage des adresses IP indésirables, la détection et la prévention des intrusions, ainsi que la prise en charge du VPN (Virtual Private Network).
3. **Haute disponibilité et redondance** : PFSense peut être configuré pour fonctionner en mode haute disponibilité (HA) et redondance. Cela signifie que si un appareil tombe en panne, un autre prendra automatiquement le relais sans perturber le réseau.
4. **Monitoring et reporting** : PFSense fournit des outils de surveillance et de reporting complets pour aider les administrateurs à suivre l'activité du réseau, à détecter les problèmes potentiels et à prendre des mesures correctives.
5. **Flexibilité et extensibilité** : PFSense est extensible grâce à une architecture de plug-ins. Les utilisateurs peuvent installer des packages supplémentaires pour étendre les fonctionnalités du pare-feu. Certains exemples de packages incluent Squid Proxy, Snort (IDS/IPS), et OpenVPN.
6. **Support communautaire et professionnel** : PFSense est soutenu par une grande communauté d'utilisateurs et de développeurs. Il existe également des options de support professionnel payant pour les entreprises qui souhaitent une assistance plus directe.
7. **SimPLICITÉ de déploiement** : PFSense peut être installé sur un matériel standard, ce qui en fait une solution économique par rapport à certains pare-feux commerciaux qui nécessitent des appareils spécialisés coûteux.

PFSense est une excellente solution pour les entreprises de taille moyenne à grande qui cherchent à sécuriser leur réseau sans dépenser une fortune pour des solutions commerciales. Il est également utilisé par de nombreuses petites entreprises, ainsi que par les administrateurs réseau à domicile qui souhaitent une solution de pare-feu puissante, mais facile à configurer et à gérer.

1.2 Prérequis.

La configuration minimale de PFSENSE est la suivante :

- Processeur : 1Ghz (64bit.)
- RAM : 1Go
- Stockage : 8 Go
- Réseau : 2 cartes réseau (1 WAN & 1 LAN)

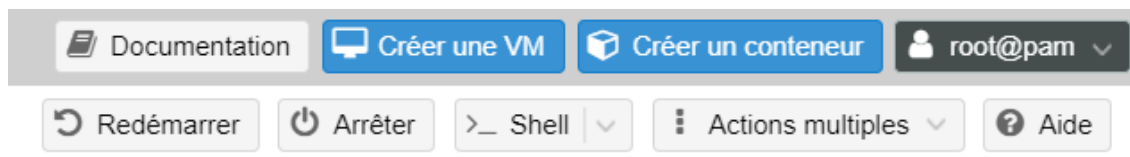


2 Création de la machine virtuelle.

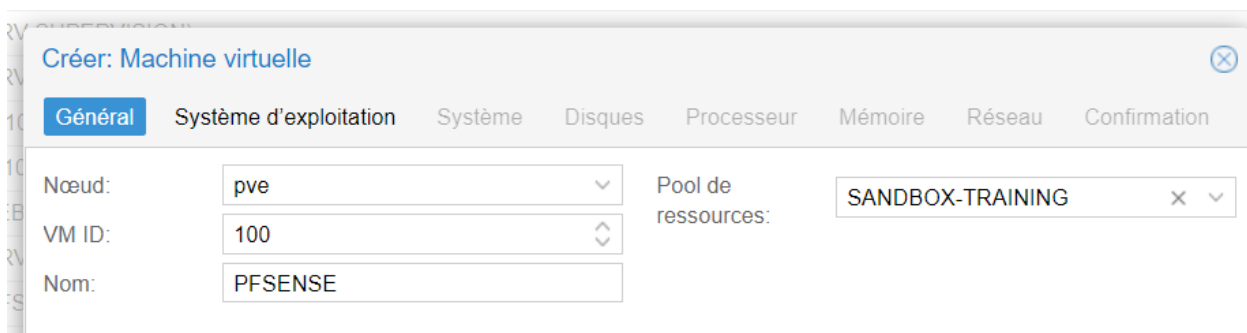
Dans le cadre du projet sandbox, l'outil de virtualisation qui a été retenue est proximal.

Vous pouvez installer PFSENSE tout autre environnement de virtualisation tant que vous respectez la configuration minimale.

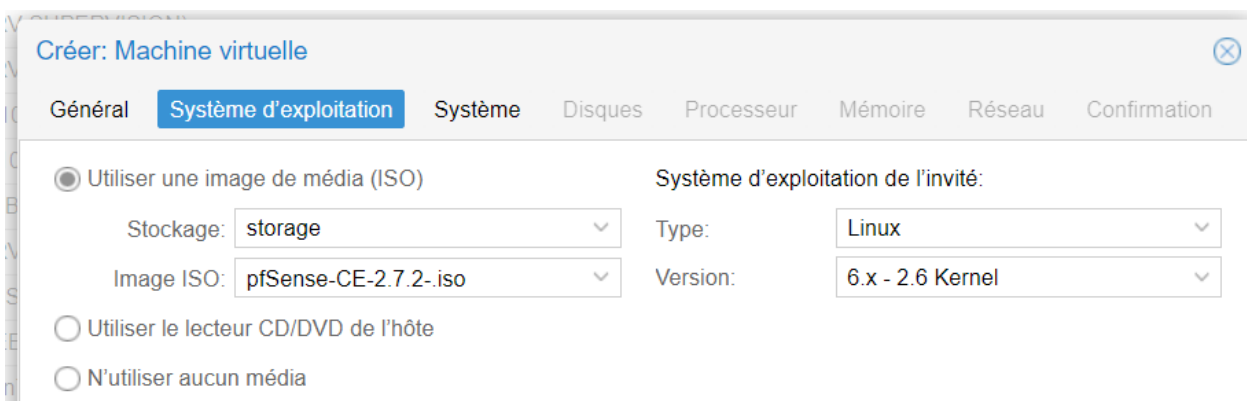
1. Je me connecte à proximaux.
2. Créer une VM.



3. J'attribue un numéro d'ID à la machine virtuelle (ici 100), je nomme ma machine virtuelle et l'intègre à un pool de ressource (ici « SANDBOX-TRAINING ») → Suivant.



4. Je sélectionne l'ISO de PFSENSE → « Suivant ».





5. Je laisse les options par défaut → « Suivant ».

The screenshot shows the 'Créer: Machine virtuelle' window with the 'Système' tab selected. The 'Général' tab is also visible. The 'Système' tab contains the following settings:

- Carte graphique: Par défaut
- Machine: Par défaut (i440fx)
- Micrologiciel: BIOS: Par défaut (SeaBIOS)
- Contrôleur SCSI: VirtIO SCSI single
- Agent QEMU: ☐
- Ajouter un module TPM: ☐

6. J'alloue 10Go d'espace disque → Suivant.

The screenshot shows the 'Créer: Machine virtuelle' window with the 'Disques' tab selected. The 'Système' tab is also visible. The 'Disques' tab contains the following settings:

- scsi0: Disque
- Bus/périphérique: SCSI
- Cache: Par défaut (Aucun ca)
- Contrôleur SCSI: VirtIO SCSI single
- Abandonner: ☐
- Stockage: local-lvm
- IO thread: ☒
- Taille du disque (Gio): 10
- Format: Image disque brute (r)

7. Je laisse la configuration par défaut → suivant.

The screenshot shows the 'Créer: Machine virtuelle' window with the 'Processeur' tab selected. The 'Disques' tab is also visible. The 'Processeur' tab contains the following settings:

- Supports de processeur: 1
- Type: x86-64-v2-AES
- Cœurs: 1
- Total de cœurs: 1



8. J'alloue 1024 MiB → Suivant.

Créer: Machine virtuelle

Général Système d'exploitation Système Disques Processeur **Mémoire** Réseau Confirmation

Mémoire (MiB): 1024

9. Je sélectionne le modèle « Intel E1000 » → suivant.

Créer: Machine virtuelle

Général Système d'exploitation Système Disques Processeur Mémoire **Réseau** Confirmation

☐ Aucun périphérique réseau

Pont (bridge): vmbr0 Modèle: Intel E1000

Étiquette de VLAN: aucun VLAN Adresse MAC: auto

Pare-feu: ☒

10. Je vérifie que toutes les informations sont correctes → terminer.

Créer: Machine virtuelle

Général Système d'exploitation Système Disques Processeur Mémoire Réseau **Confirmation**

Key ↑	Value
cores	1
cpu	x86-64-v2-AES
ide2	storage:iso/pfSense-CE-2.7.2-.iso,media=cdrom
memory	1024
name	PFSENSE
net0	e1000,bridge=vmbr0,firewall=1
nodename	pve
numa	0
ostype	l26
pool	SANDBOX-TRAINING
scsi0	local-lvm:10,ioread=on
scsihw	virtio-scsi-single
sockets	1
vmid	100

☐ Démarrer après création

Avancé ☐ Retour Terminer



2.1 Ajout d'une carte réseau.

1. Je me rends sur la machine virtuelle 100 → Matériel.

Machine virtuelle 100 (PFSENSE) sur le nœud pve Aucune étiquette

Résumé	Ajouter	Supprimer	Éditer	Action disque	Revenir en arrière
Console	Mémoire	1.00 Gio			
Matériel	Processeurs	1 (1 sockets, 1 cores) [x86-64-v2-AES]			
Cloud-Init	BIOS	Par défaut (SeaBIOS)			
Options	Affichage	Par défaut			
Historique des tâches	Machine	Par défaut (i440fx)			
Moniteur	Contrôleur SCSI	VirtIO SCSI single			
Sauvegarde	Lecteur CD/DVD (ide2)	storage:iso/pfSense-CE-2.7.2-iso,media=cdrom,size=854172K			
Réplication	Disque dur (scsi0)	local-lvm:vm-100-disk-0,iothread=1,size=10G			
	Carte réseau (net0)	e1000=BC:24:11:1E:F6:BA,bridge=vmbr0,firewall=1			

2. Ajouter → Carte réseau.
3. Je sélectionne le modèle « Intel E1000 » → je définis le VLAN sur 1 → « Ajouter ».

Ajouter: Carte réseau

Pont (bridge):
vmbr0

Modèle:
Intel E1000

Étiquette de VLAN:
1

Adresse MAC:
auto

Pare-feu:
☒

Aide

Avancé ☐

Ajouter

4. La carte réseau a bien été configurée.



3 Installation PFSENSE.

1. VM 100 → Console → "Start Now".
2. J'accepte les conditions d'utilisation.

```
-----Copyright and distribution notice-----
Copyright and Trademark Notices.

Copyright 2004-2016. Electric Sheep Fencing, LLC ("ESF").
All Rights Reserved.

Copyright 2014-2023. Rubicon Communications, LLC d/b/a Netgate
("Netgate").
All Rights Reserved.

All logos, text, and content of ESF and/or Netgate, including underlying
HTML code, designs, and graphics used and/or depicted herein are
protected under United States and international copyright and trademark
laws and treaties, and may not be used or reproduced without the prior
express written permission of ESF and/or Netgate.

"pfSense" is a registered trademark of ESF, exclusively licensed to
Netgate, and may not be used without the prior express written
permission of ESF and/or Netgate. All other trademarks shown herein are

-----[Accept]-----26%
```

3. « Install PFSENSE » → OK.

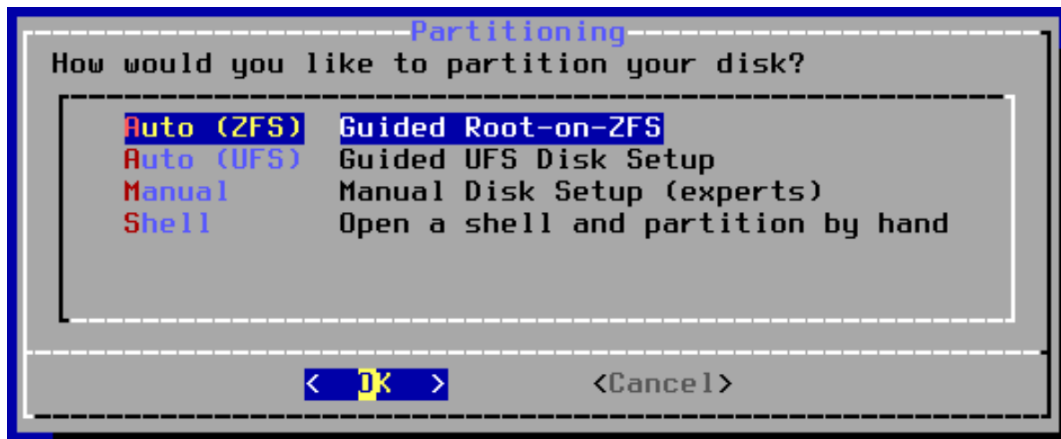
```
-----Welcome-----
Welcome to pfSense!

[Install]      Install pfSense
Rescue Shell  Launch a shell for rescue operations
Recover config.xml Recover config.xml from a previous install

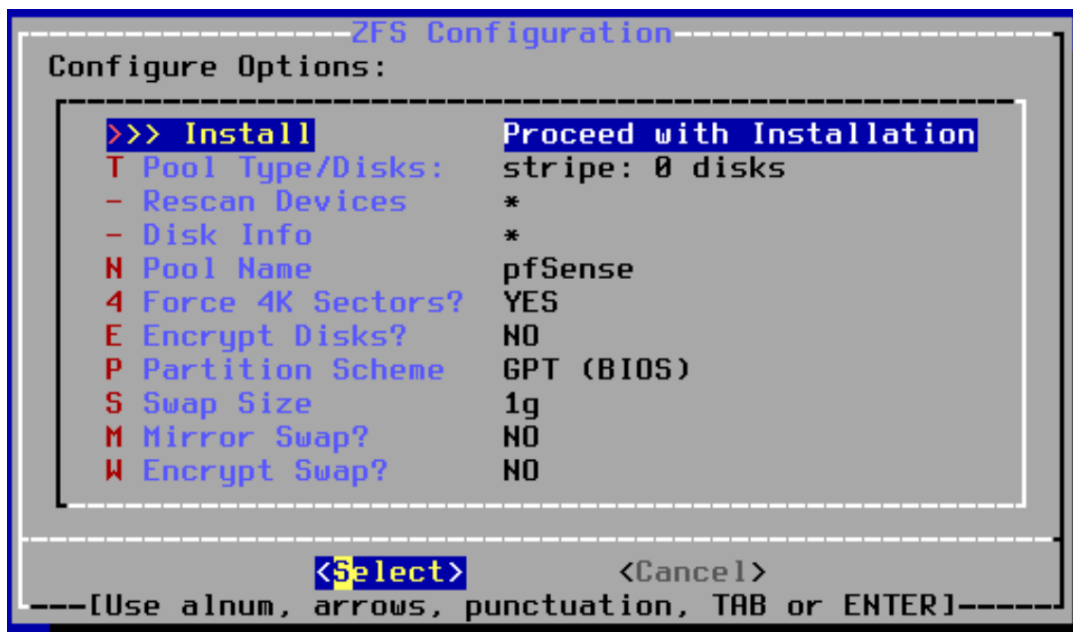
-----< OK >-----<Cancel>-----
```



4. « Auto (ZFS) » → OK.

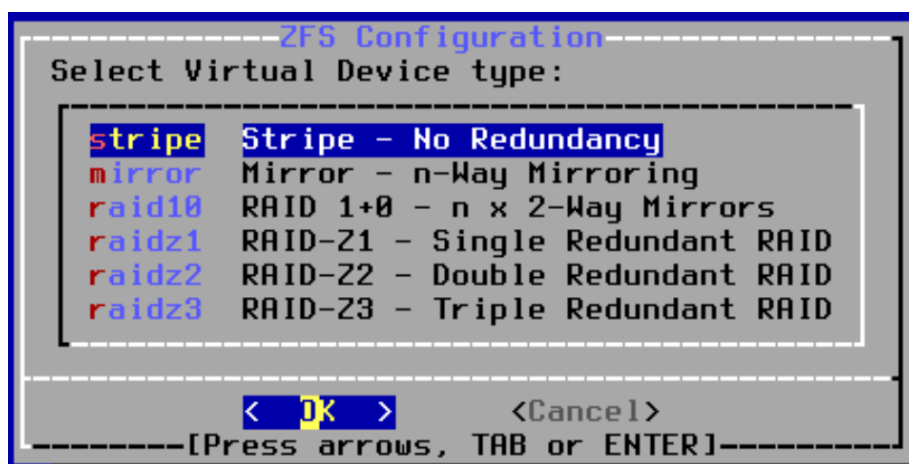


5. « >>> Install » → select.

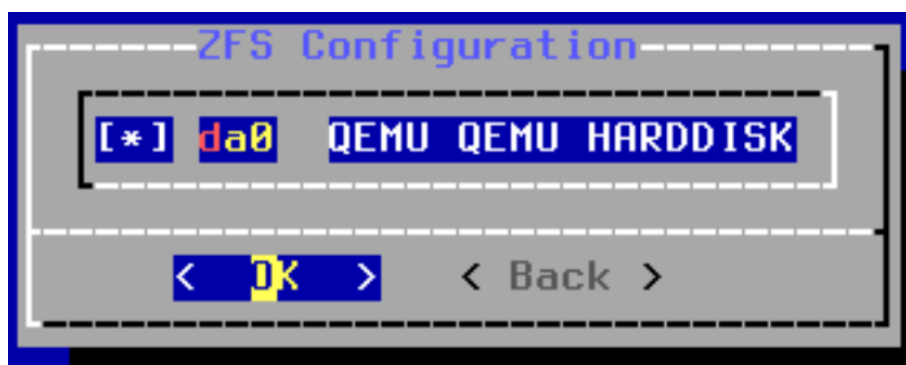




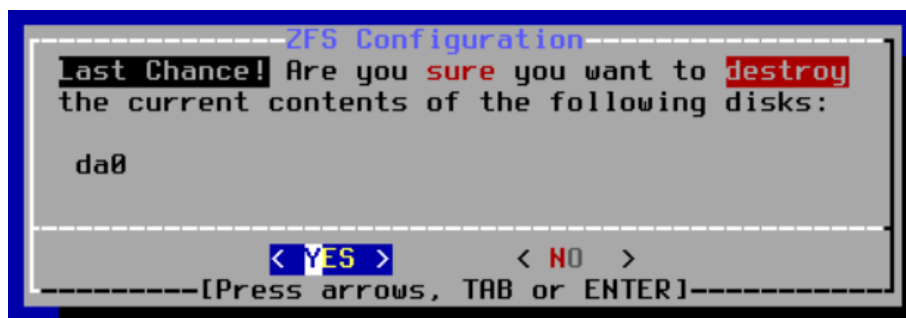
6. « Stripe » → OK.



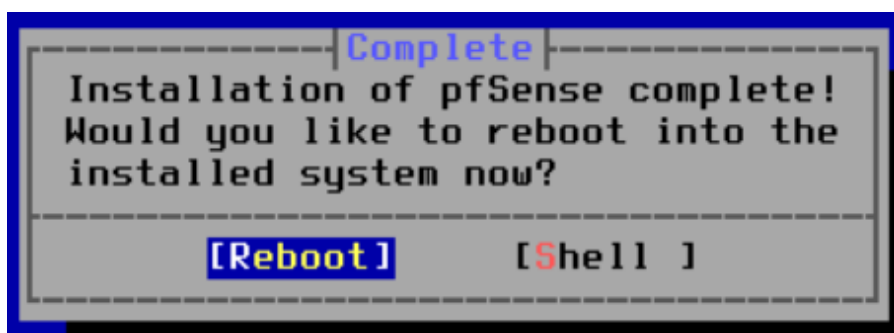
7. Je sélectionne le disque → OK.



8. Yes.



9. Reboot.





4 Configuration PFSENSE.

4.1 Interface WAN.

1. Je me connecte au PFSENSE
2. "2) Set interface(s) IP address".

```
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
```

3. "1 – WAN".

```
Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)
```

4. "n".

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

5. Adresse IP : "192.168.1.200".

```
Enter the new WAN IPv4 address. Press <ENTER> for none:
> 192.168.1.200
```

6. Masque sous réseau: "24 (255.255.255.0)".

```
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 32):
> 24
```

7. Adresse passerelle : "192.168.1.254".

```
For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 192.168.1.254
```

8. Default address: "y".

```
Should this gateway be set as the default gateway? (y/n) y
```



9. DHCP6 : "n".

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

10. "Enter"

11. "DHCP on lan" : "N".

```
Do you want to enable the DHCP server on WAN? (y/n) n
```

12. "HTTP as the webconfigurator" : "N"

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

13. "Enter".

```
Do you want to enable the DHCP server on WAN? (y/n) n
Disabling IPv4 DHCPD...
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 WAN...
Reloading filter...
Reloading routing configuration...
DHCPD...

The IPv4 WAN address has been set to 192.168.1.200/24

Press <ENTER> to continue.
```



4.2 Interface LAN.

1. Je me connecte au PFSense,
2. « Set interface(s) IP address ».

```
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
```

3. "2 – LAN"

```
Available interfaces:

1 - WAN (em0 - static)
2 - LAN (em1 - static)
```

4. "Configure LAN via DHCP" : "N ».
5. Adresse IP : « 192.168.2.254 »

```
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.2.254
```

6. Masque Sous-Réseau : « 24 (255.255.255.0) ».

```
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 LAN IPv4 subnet bit count (1 to 32):
> 24
```

7. « Upstream Gateway » → Entrer.
8. « DHCP6 » → « N ».
9. « IPv6 » → entrer.
10. « DHCP on Lan » → « N ».
11. « http webconfigurator » → entrer.



4.3 Configuration WebInterface.

1. Je me connecte sur proxmox.
2. Je me connecte sur une machine W10
3. Je configure l'adresse IP de la machine :
 - Adresse IP : « 192.168.2.5 »
 - Masque sous réseau : « 255.255.255.0 »
 - Passerelle : « 192.168.2.254 ».

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address:	192 . 168 . 2 . 5
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	192 . 168 . 2 . 254

4. J'ouvre mon navigateur préféré,
5. Je me connecte avec les identifiants : « Admin/pfsense »

SIGN IN

admin

.....

SIGN IN



6. « Next ».

pfSense Setup

Welcome to pfSense® software!

This wizard will provide guidance through the initial configuration of pfSense.

The wizard may be stopped at any time by clicking the logo image at the top of the screen.

pfSense® software is developed and maintained by Netgate®

[Learn more](#)

>> Next

7. « Next ».

Netgate® Global Support is available 24/7

Our 24/7 worldwide team of support engineers are the most qualified to diagnose your issue and resolve it quickly, from branch office to enterprise — on premises to cloud.

We offer several support subscription plans tailored to fit different environment sizes and requirements. Many companies around the world choose Netgate support because:

- Support is available 24 hours a day, seven days a week, including holidays.
- Support engineers are located around the world, ensuring that no support call is missed.
- Our support engineers hold many prestigious network engineer certificates and have years of hands-on experience with networking.

[Learn more](#)

>> Next

8. Je renseigne le nom de domaine « Sandbox.local » → je renseigne les infos du DNS → « Next ».

General Information

On this screen the general pfSense parameters will be set.

Hostname
Name of the firewall host, without domain part.
Examples: pfsense, firewall, edgefw

Domain
Domain name for the firewall.
Examples: home.arpa, example.com

Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.

The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.

Primary DNS Server

Secondary DNS Server

Override DNS ☒
Allow DNS servers to be overridden by DHCP/PPP on WAN

>> Next



9. Je sélectionne « Europe/Paris » → « Next ».

Time Server Information

Please enter the time, date and time zone.

Time server hostname
Enter the hostname (FQDN) of the time server.

Timezone

» Next

10. « WAN interface » → « Next ».

11. « Lan interface » → « Next ».

12. « Admin WebGui Password » → « Next ».

Set Admin WebGUI Password

On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled.

Admin Password

Admin Password AGAIN

» Next

13. « Reload » → « Finish ».



5 Configuration PFsense – Projet Sandbox.

5.1 Règle du Pare-feu – LAN.

(ici le LAN est l'équivalent de l'interface WAN).

Règles (Faire glisser pour changer l'ordre)											
☐	États	Protocole	Source	Port	Destination	Port	Passerelle	File d'attente	Ordonnancement	Description	Actions
Accès Interface Administration PFSense											
☐	✓ 9/1,43 MiB	IPv4 TCP	192.168.1.10	*	LAN address	80 (HTTP)	*	aucun			
HTTPS Bastion - Apache Guacamole											
☐	✓ 24/143,03 MiB	IPv4 TCP/UDP	*	*	10.16.100.253	8443	*	aucun		NAT	
SUPERVISION - Zabbix											
☐	✓ 9/17,22 MiB	IPv4 UDP	*	*	10.16.100.253	161 - 162	*	aucun		NAT	
☐	✓ 0/103 KiB	IPv4 ICMP	*	*	10.16.100.253	161 (SNMP)	*	aucun		NAT	
ANNUAIRE - LDAP											
☐	✓ 0/0 B	IPv4 TCP/UDP	*	*	10.16.100.253	3890	*	aucun		NAT	



5.2 Règle du Pare-feu – DMZ.

Règles (Faire glisser pour changer l'ordre)											
	États	Protocole	Source	Port	Destination	Port	Passerelle	File d'attente	Ordonnancement	Description	Actions
	0/0 B	*	*	*	DMZ Address	80	*	*		Règle anti-blocage	
Accès Internet											
☐	0/99 KiB	IPv4 TCP	DMZ subnets	*	*	80 (HTTP)	*	aucun			
☐	0/0 B	IPv4 TCP	DMZ subnets	*	*	443 (HTTPS)	*	aucun			
DNS											
☐	0/315 KiB	IPv4 UDP	DMZ subnets	*	192.168.1.2	53 (DNS)	*	aucun			
☐	0/6 KiB	IPv4 UDP	DMZ subnets	*	192.168.1.254	53 (DNS)	*	aucun			
☐	0/0 B	IPv4 UDP	DMZ subnets	*	1.1.1.1	53 (DNS)	*	aucun			
ANNUAIRE											
☐	0/0 B	IPv4 TCP/UDP	DMZ subnets	*	192.168.1.1	3890	*	aucun			
SUPERVISION											
☐	0/0 B	IPv4 UDP	DMZ subnets	*	192.168.1.4	*	*	aucun			
☐	0/0 B	IPv4 ICMP any	DMZ subnets	*	192.168.1.4	*	*	aucun			
Apache Guacamole - LAN											



5.3 Règle du Pare-feu – Lan_USER_X.

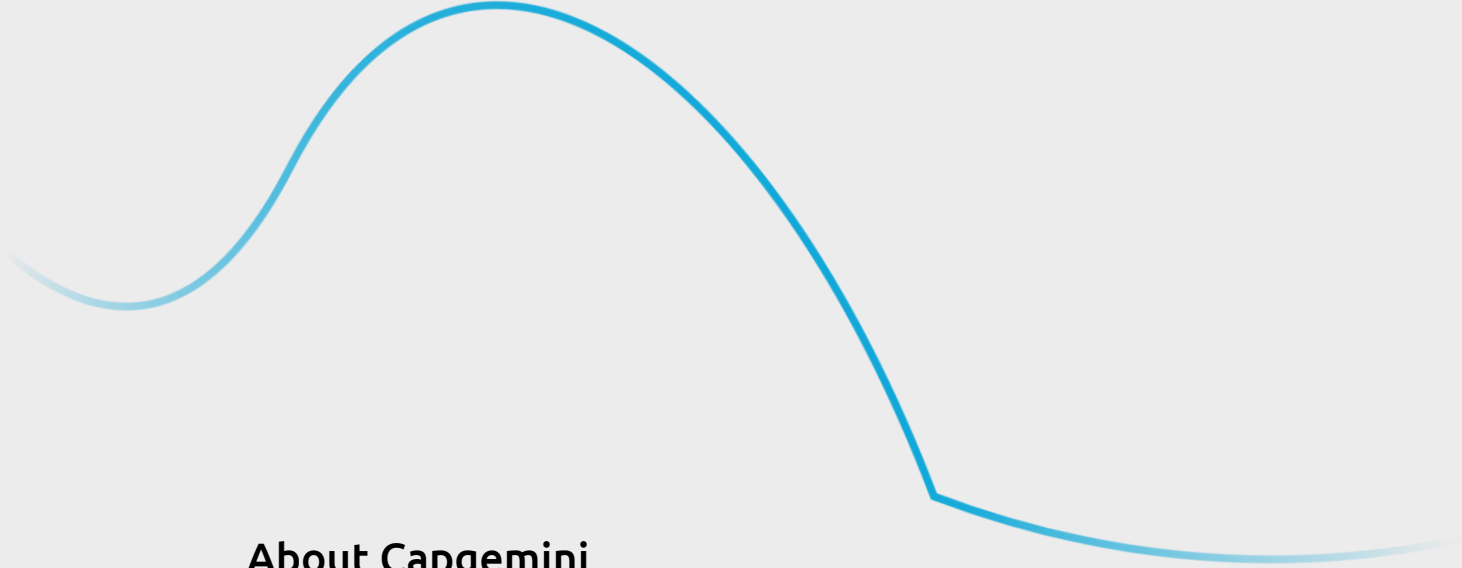
Règles (Faire glisser pour changer l'ordre)											
☐	États	Protocole	Source	Port	Destination	Port	Passerelle	File d'attente	Ordonnancement	Description	Actions
☐		0/0 B	IPv4 TCP	LAN_USER_10 subnets	*	*	80 (HTTP)	*	aucun		
☐		0/0 B	IPv4 TCP	LAN_USER_10 subnets	*	*	443 (HTTPS)	*	aucun		
DNS											
☐		0/0 B	IPv4 UDP	LAN_USER_10 subnets	*	1.1.1.3	53 (DNS)	*	aucun		
☐		0/0 B	IPv4 UDP	LAN_USER_10 subnets	*	1.0.0.3	53 (DNS)	*	aucun		
Apache Guacamole - DMZ											
☐		0/0 B	IPv4 TCP	LAN_USER_10 subnets	*	10.16.100.253	3389 (MS RDP)	*	aucun		
☐		0/0 B	IPv4 TCP	LAN_USER_10 subnets	*	10.16.100.253	22 (SSH)	*	aucun		
Blocage Par défaut											
☐		0/0 B	IPv4+6 *	*	*	*	*	*	aucun		



5.4 NAT

Transfert de port 1:1 Sortant NPt

Règles										
☐	Interface	Protocole	Adresse source	Ports source	Adresse de destination	Ports dest.	IP NAT	Ports NAT	Description	Actions
Connexion SSL - Apache Guacamole										
☐	☒	LAN	TCP/UDP	*	*	192.168.1.3	443 (HTTPS)	10.16.100.253	8443	
Supervision - Zabbix										
☐	☒	LAN	UDP	*	*	192.168.1.3	161 - 162	10.16.100.253	161 - 162	
☐	☒	LAN	ICMP	*	*	192.168.1.3	*	10.16.100.253	*	
Annuaire - LDAP										
☐	☒	LAN	TCP/UDP	*	*	192.168.1.3	3890	10.16.100.253	3890	

A thick, light blue line that starts on the left, curves upwards to a peak, then curves downwards to the right, ending in a slight upward curve.

About Capgemini

Capgemini is a global leader in partnering with companies to transform and manage their business by harnessing the power of technology. The group is guided every day by its purpose of unleashing human energy through technology for an inclusive and sustainable future. It is a responsible and diverse organisation of over 360,000 team members in more than 50 countries. With its strong 55-year heritage and deep industry expertise, Capgemini is trusted by its clients to address the entire breadth of their business needs, from strategy and design of operations, fuelled by the fast evolving and innovative world of clouds, data, AI, connectivity, software, digital engineering and platforms. The group reported in 2022 global revenues of €22 billion.

Get the Future You Want | www.capgemini.com



This document contains information that may be privileged or confidential and is the property of the Capgemini Group.

Company Confidential. Copyright © 2023 Capgemini. All rights reserved.