PFSENSE

Noah MAILLET

Projet Sandbox

Table of contents

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 :

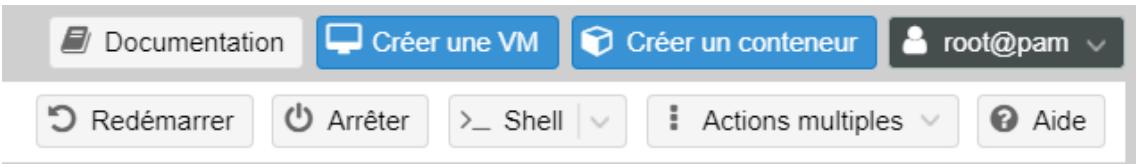
- Processeur : 1Ghz (64bit.)
- RAM : 1Go
- Stockage : 8 Go
- Réseau : 2 cartes réseau (1 WAN & 1 LAN)

2 Création de la machine virtuelle.

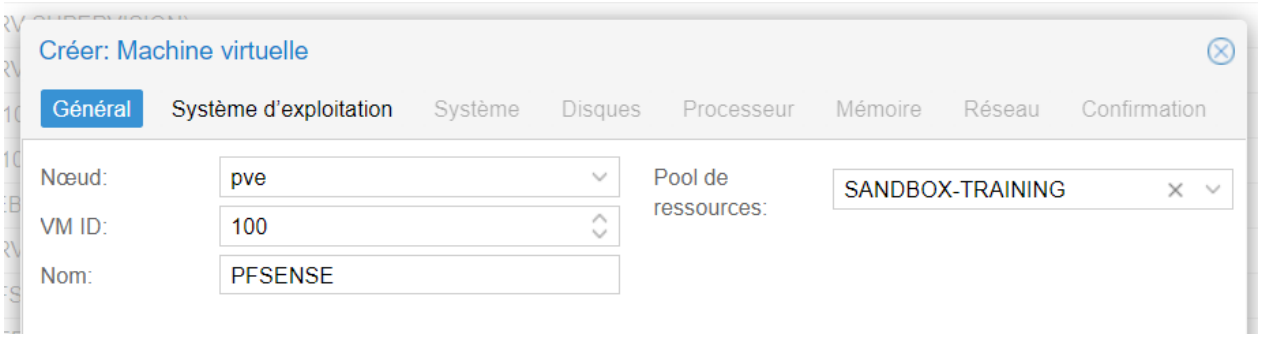
Dans le cadre du projet sandbox, l'outil de virtualisation qui a été retenue est proximal.

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

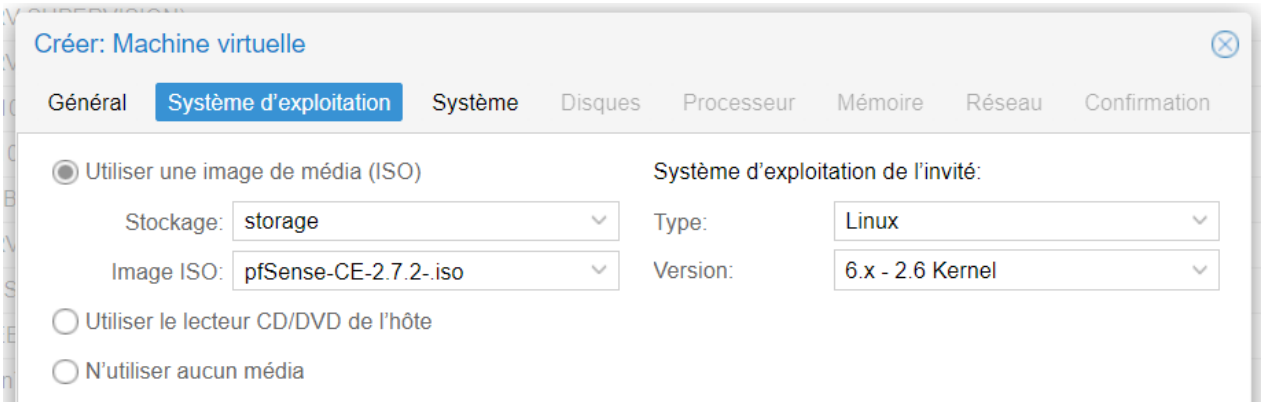
1. Je me connecte à proximaux.
2. Créer une VM.



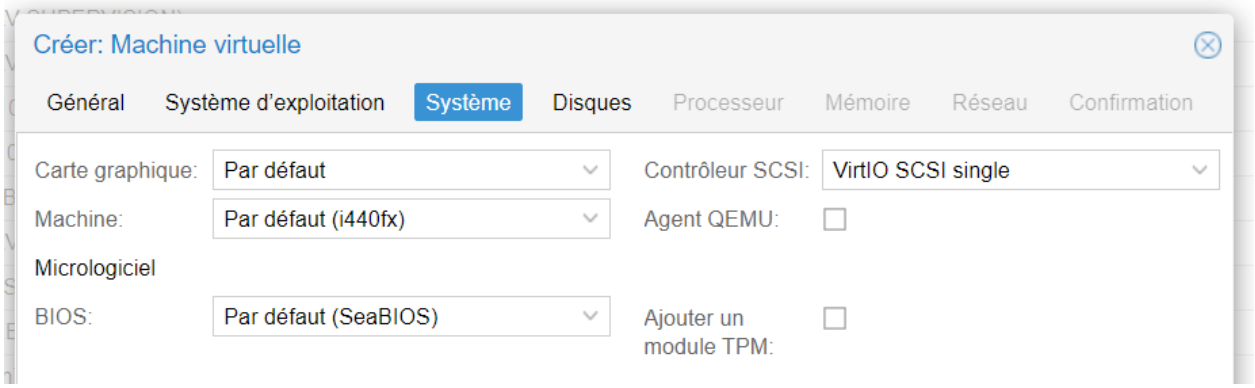
3. J'attribue un numéro d'ID à la machine virtuelle (içi 100), je nomme ma machine virtuelle et l'intégré à un pool de ressource (içi « SANDBOX-TRAINING ») ➔ Suivant.



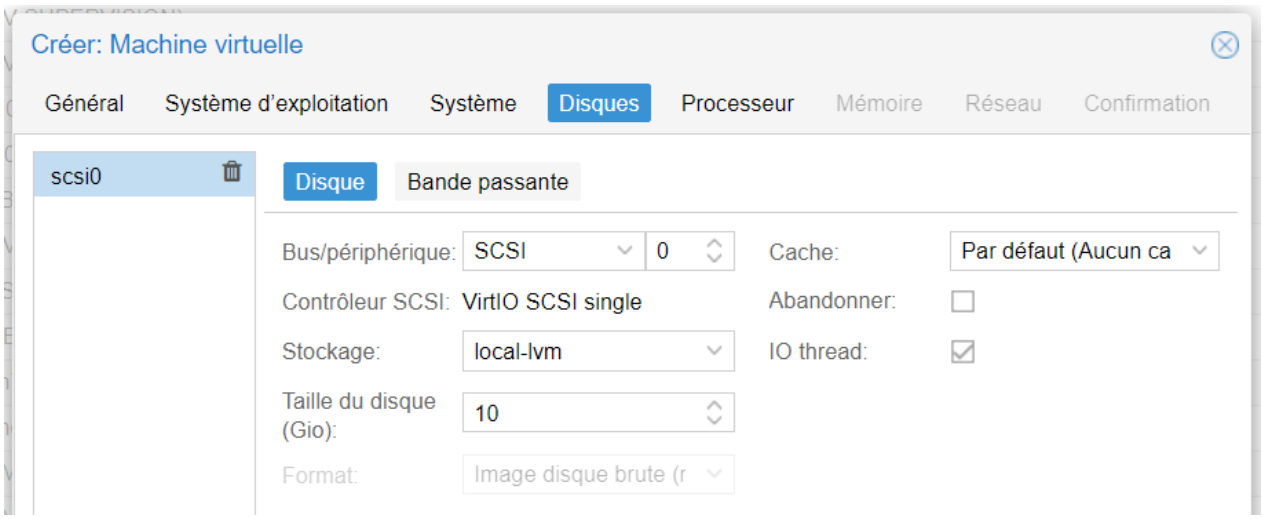
4. Je sélectionne l'ISO de PFSENSE ➔ « Suivant ».



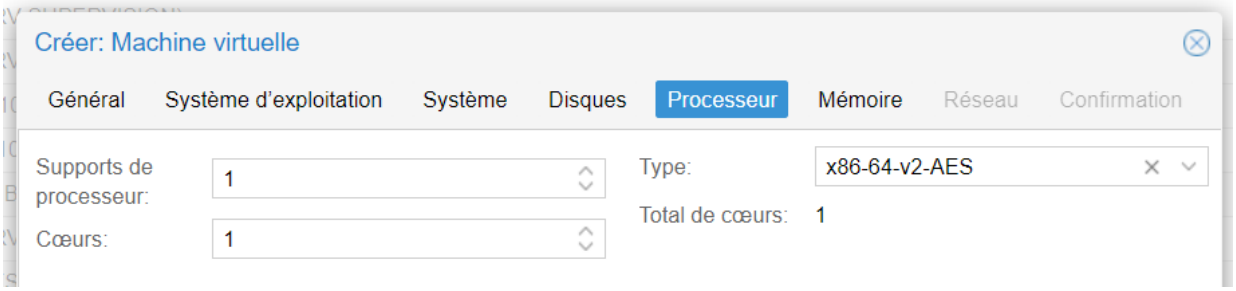
5. Je laisse les options par défaut ➔ « Suivant ».



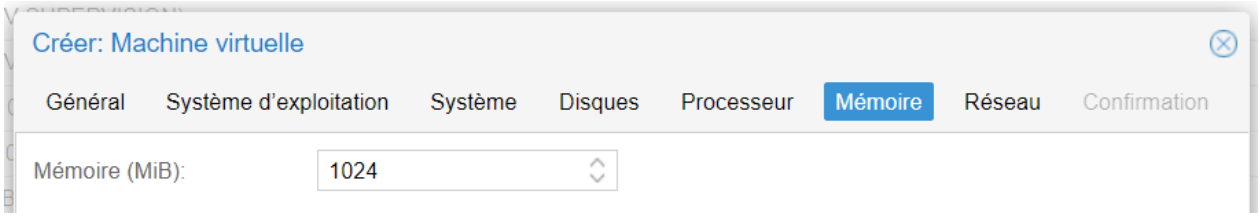
6. J'alloue 10Go d'espace disque ➔ Suivant.



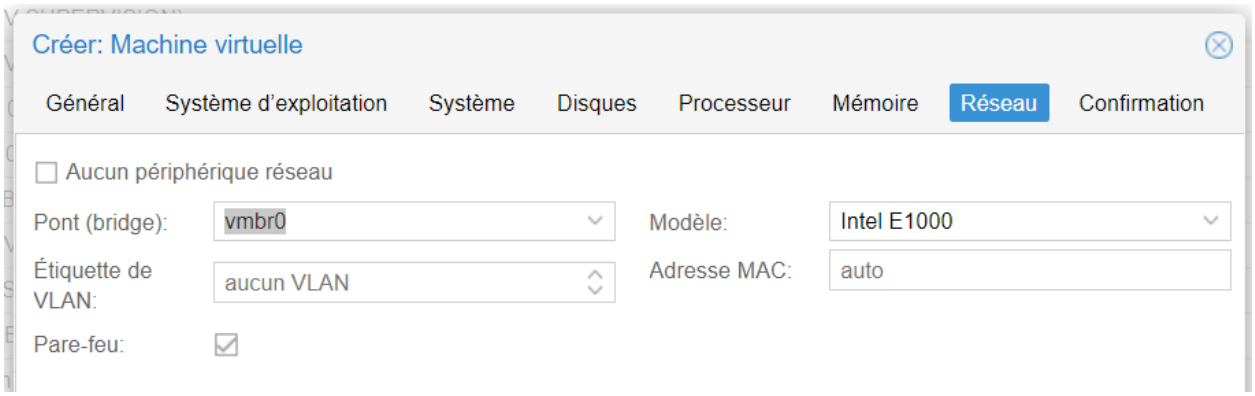
7. Je laisse la configuration par défaut ➔ suivant.



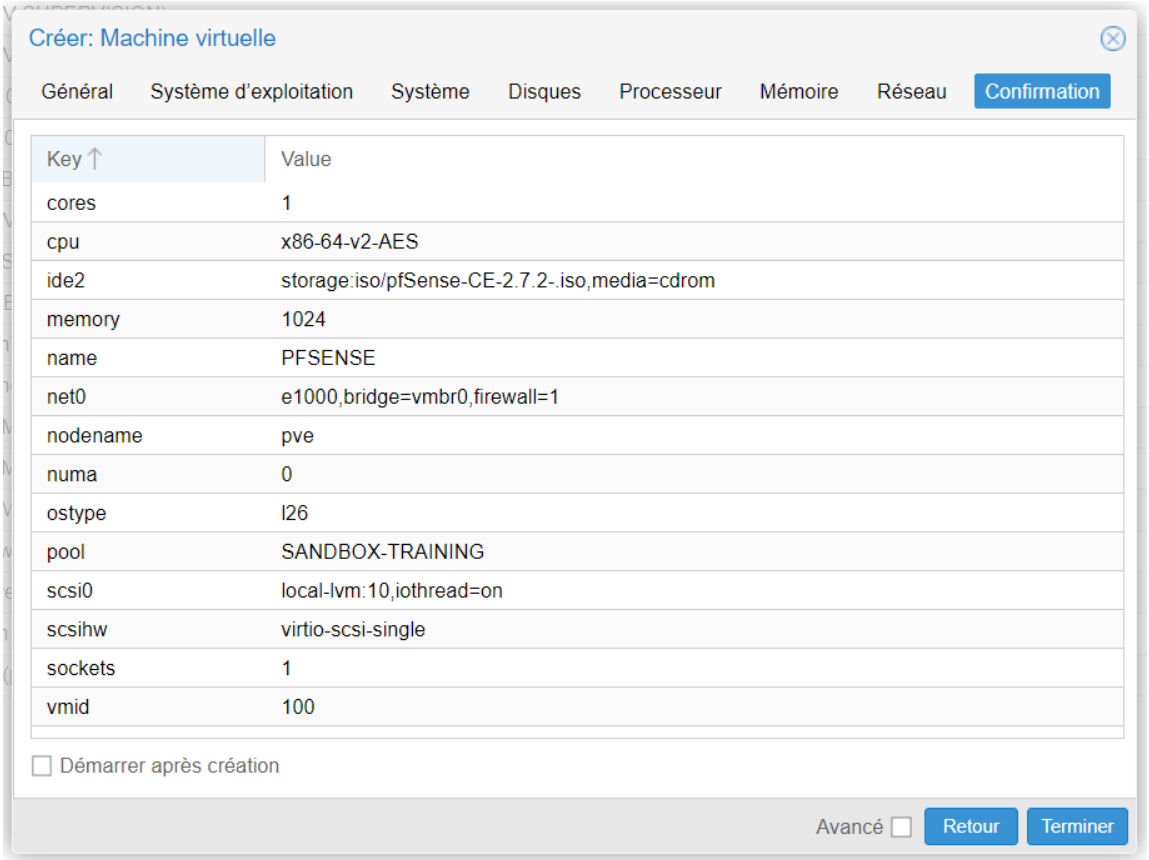
8. J'alloue 1024 MiB ➔ Suivant.



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

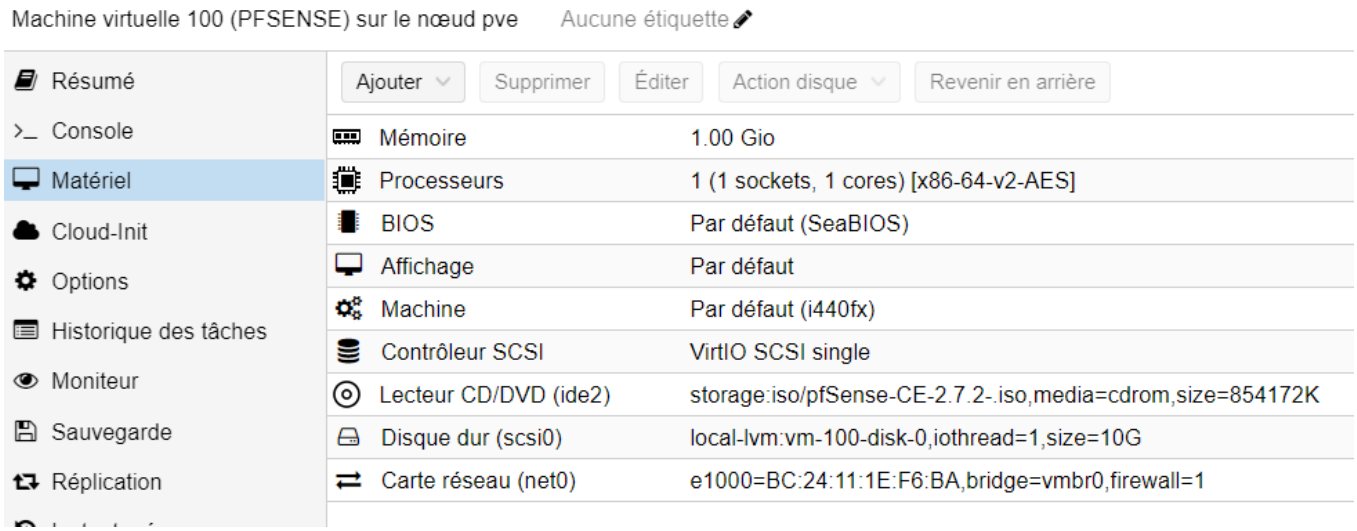


10. Je vérifie que toutes les informations sont correctes ➔ terminer.

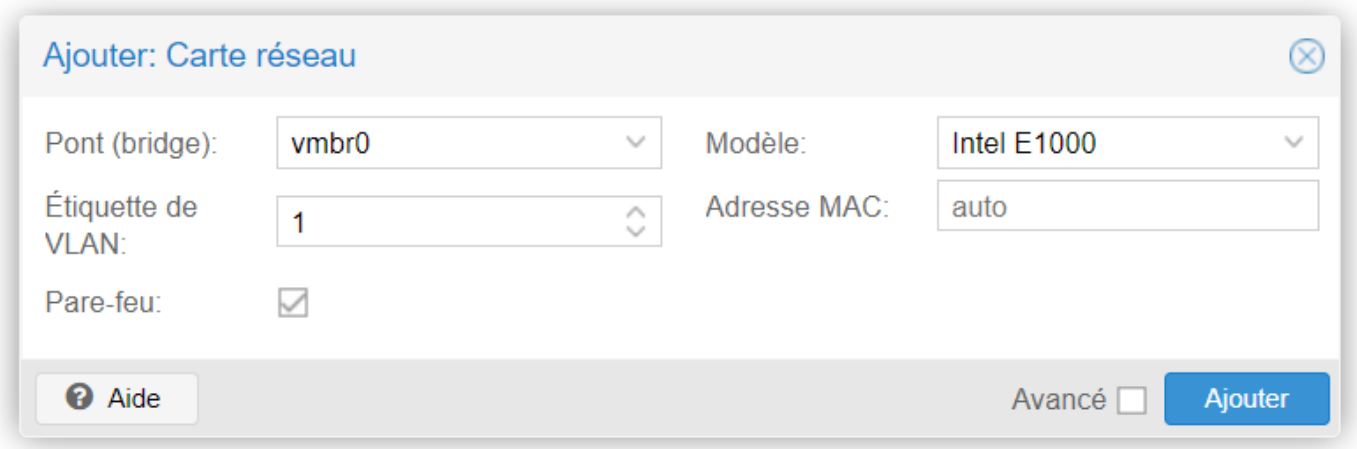


2.1 Ajout d'une carte réseau.

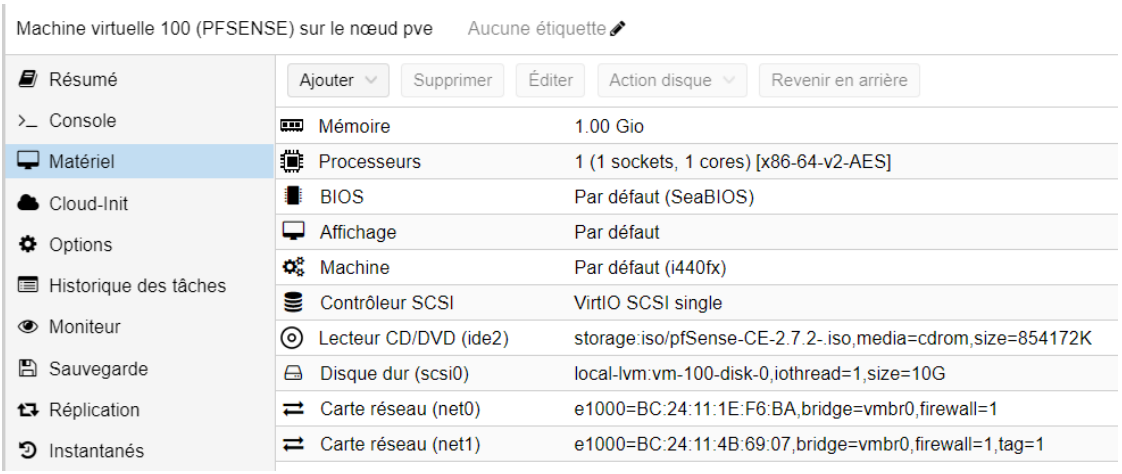
1. Je me rends sur la machine virtuelle 100 ➔ Matériel.



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

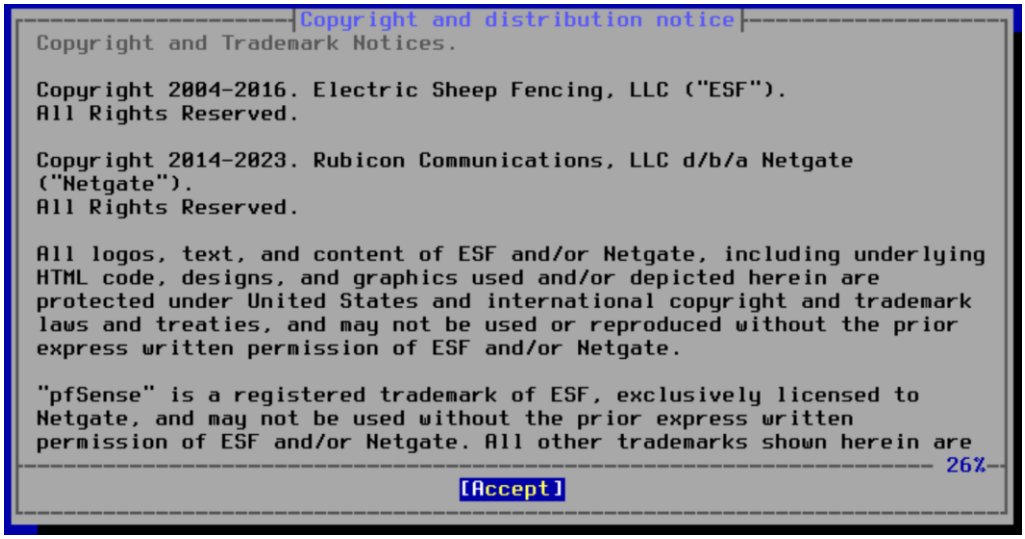


4. La carte réseau a bien été configurée.

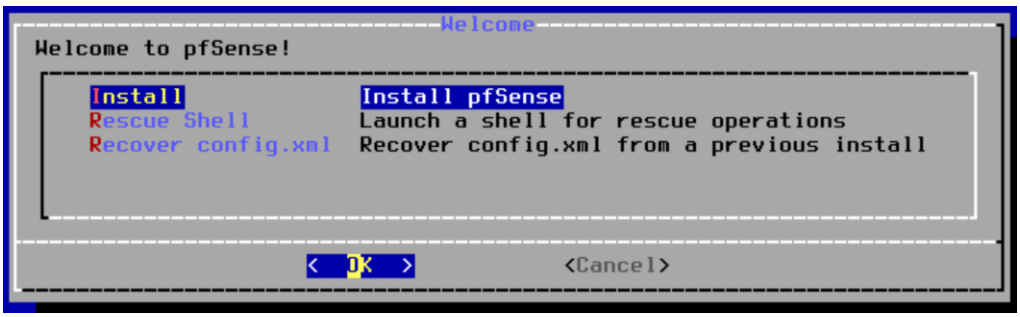


3 Installation PFSENSE.

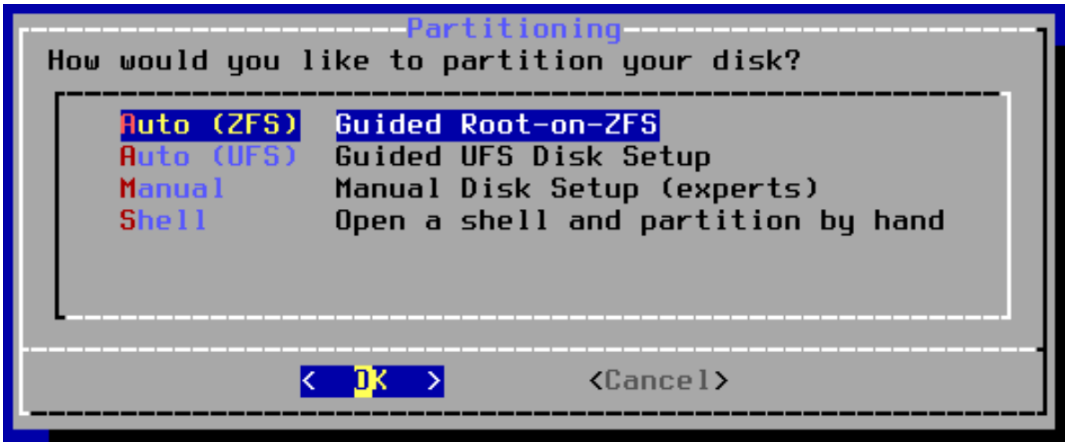
1. VM 100 ➔ Console ➔ “Start Now”.
2. J’accepte les conditions d’utilisation.



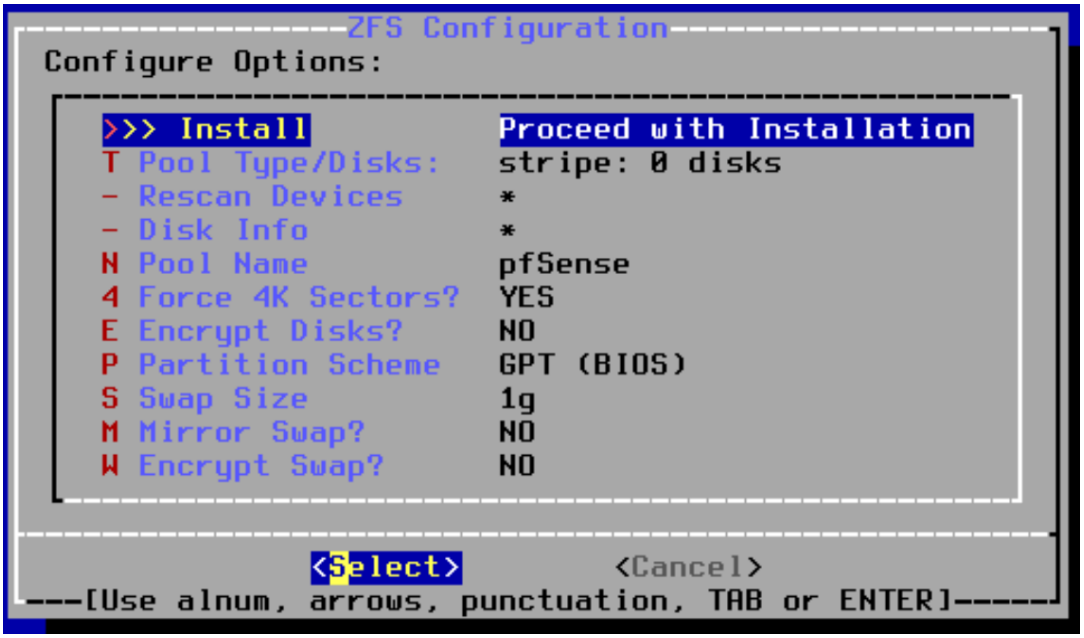
3. « Install PFSENSE » ➔ OK.



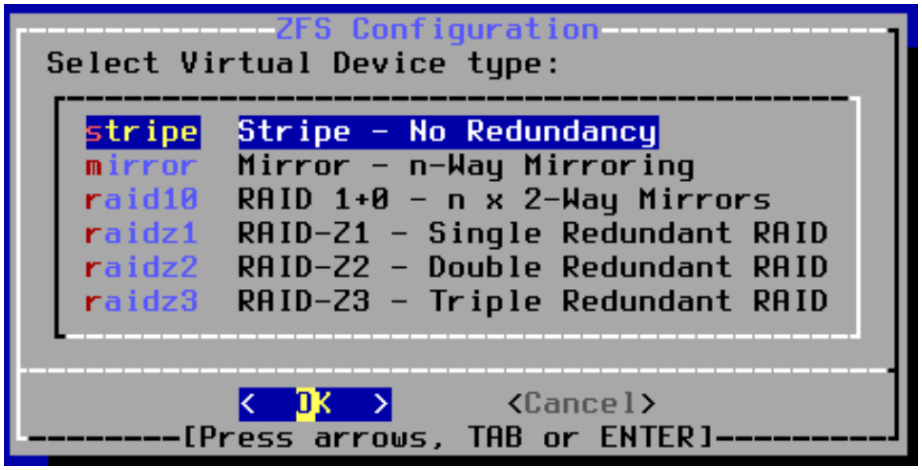
4. « Auto (ZFS) » ➔ OK.



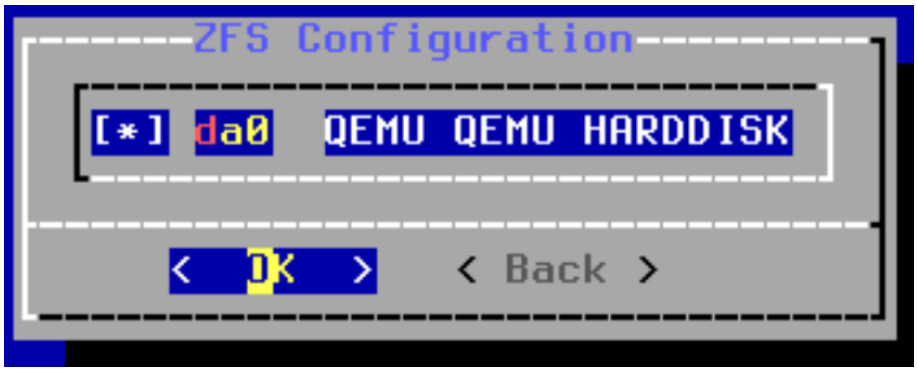
5. « >>> Install » ➔ select.



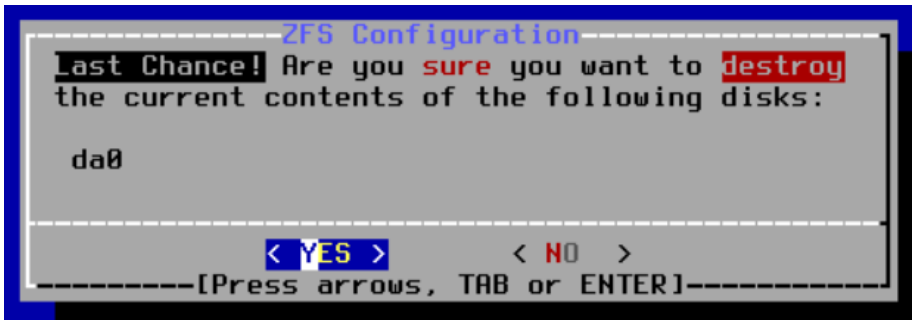
6. « Stripe » ➔ OK.



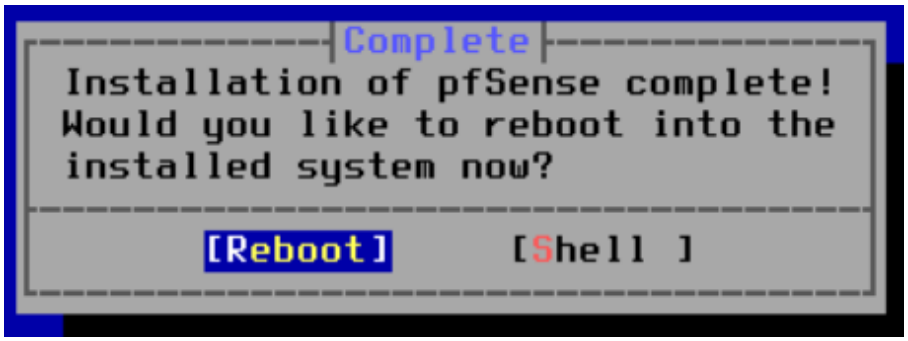
7. Je sélectionne le disque ➔ OK.



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”.

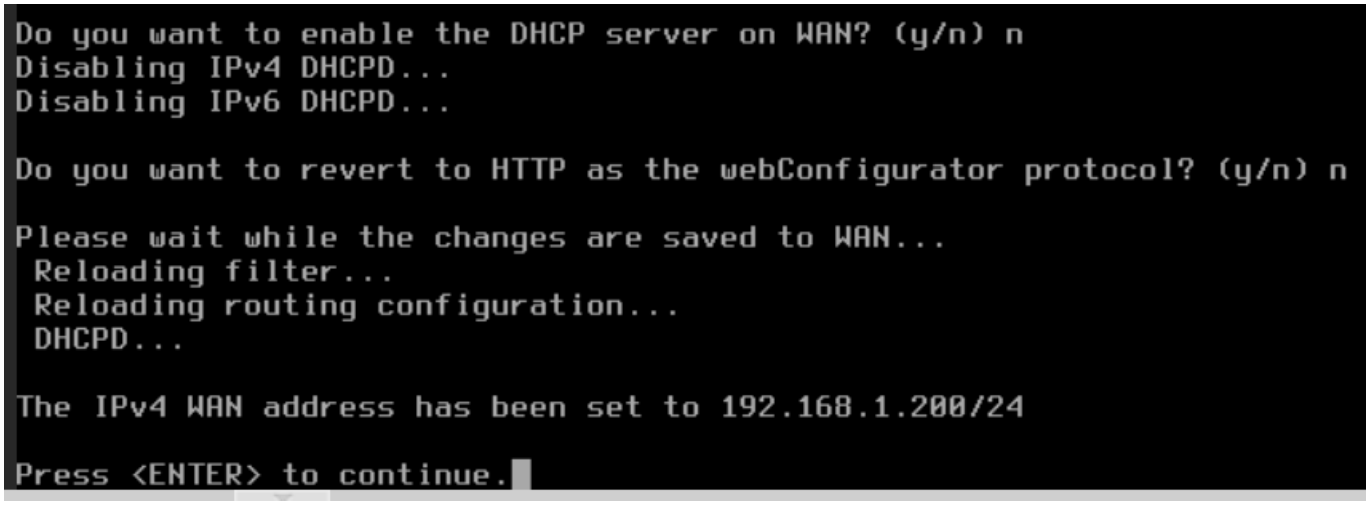
```
Should this gateway be set as the default gateway? (y/n) y
```

9. DHCP6 : “n”.

10. “Enter”
11. “DHCP on lan” : “N”.

12. “HTTP as the webconfigurator” : “N”

13. “Enter”.



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) ».

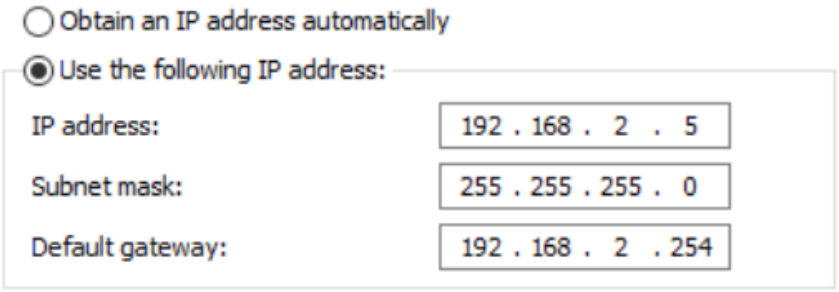
```
Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

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.

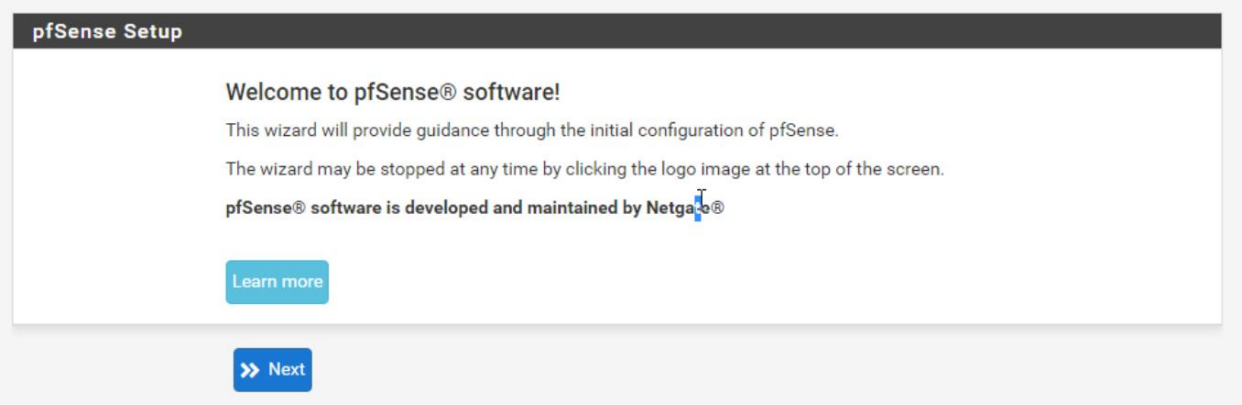
1. Je me connecte sur proxmox.
2. Je me connecte sur une machine W10
3. Je configure l'adresse IP de la machine :

- Adresse IP : « 192.168.2.5 »
- Masque sous réseau : « 255.255.255.0 »
- Passerelle : « 192.168.2.254 ».

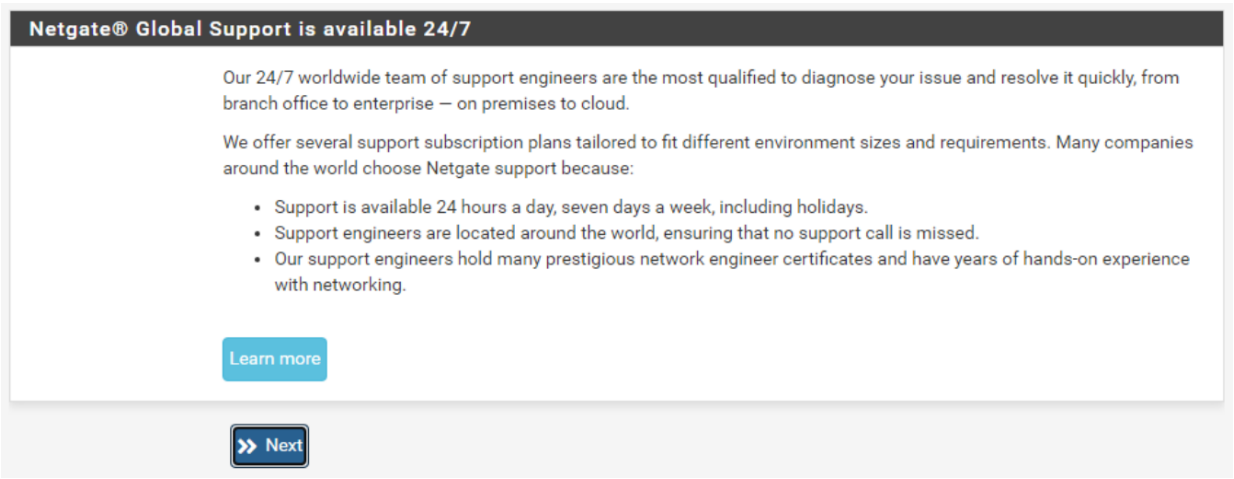


4. J'ouvre mon navigateur préféré,
5. Je me connecte avec les identifiants : « Admin/pfsense »

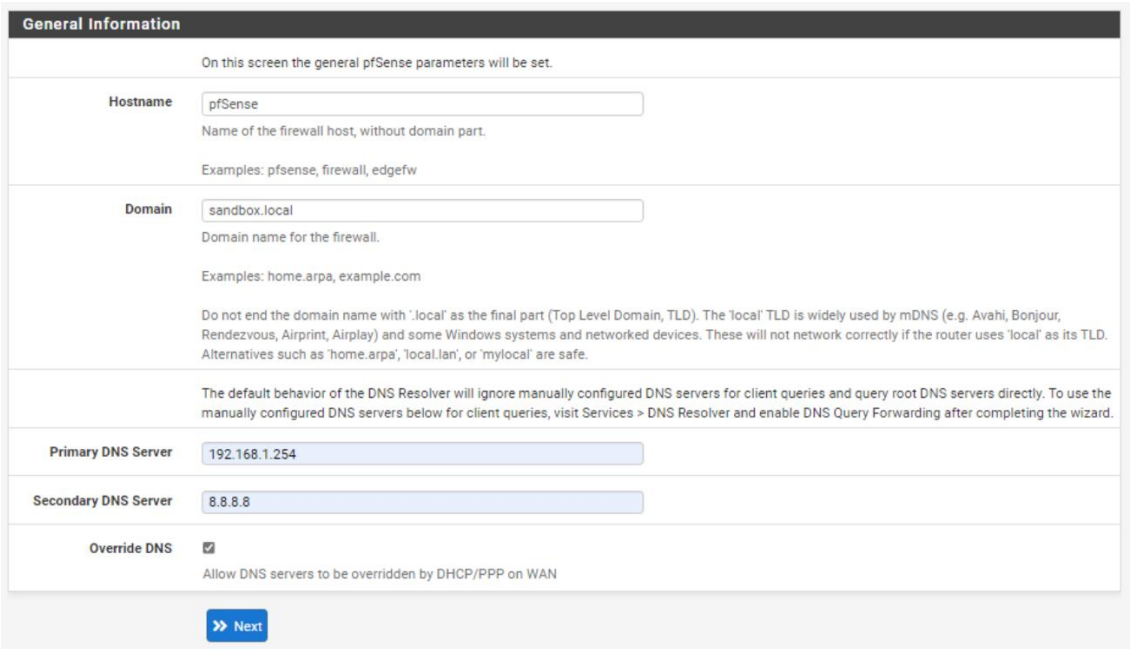
6. « Next ».



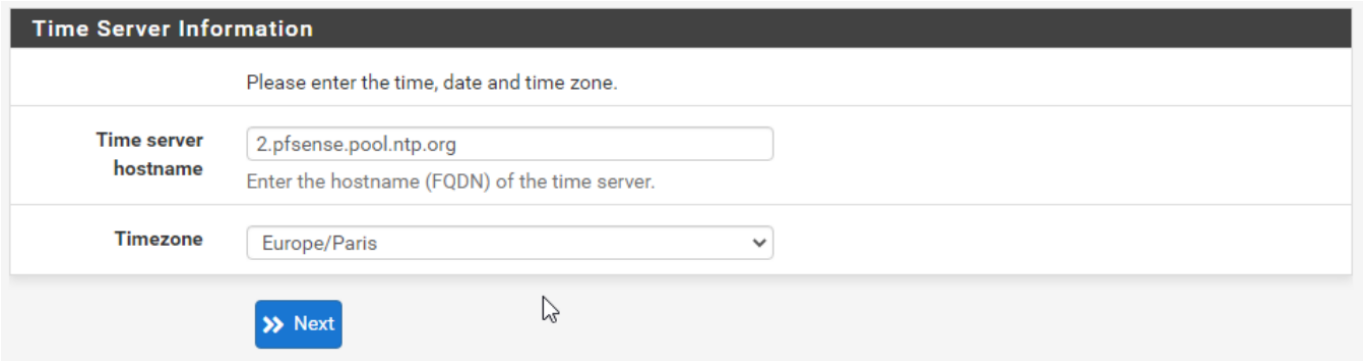
7. « Next ».



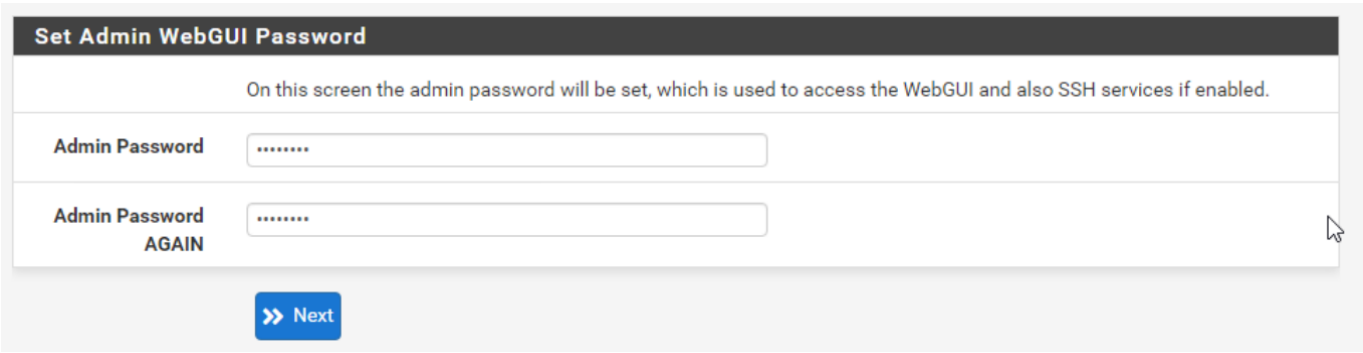
8. Je renseigne le nom de domaine « Sandbox.local » ➔ je renseigne les infos du DNS ➔ « Next ».



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



10. « WAN interface » ➔ « Next ».
11. « Lan interface » ➔ « Next ».
12. « Admin WebGui Password » ➔ « 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 - LLDAP										
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											🗑
☐ ✓	0/158 KiB	IPv4 TCP/UDP	DMZ subnets	*	LAN subnets	22 (SSH)	*	aucun			⚓ ✎ ⧉ ⊘ 🗑 ✕
☐ ✓	1/746,05 MiB	IPv4 TCP/UDP	DMZ subnets	*	LAN subnets	3389 (MS RDP)	*	aucun			⚓ ✎ ⧉ ⊘ 🗑 ✕
Apache Guacamole - LAN_USER_10											🗑
☐ ✓	0/0 B	IPv4 TCP/UDP	DMZ subnets	*	LAN_USER_10 subnets	22 (SSH)	*	aucun			⚓ ✎ ⧉ ⊘ 🗑 ✕
☐ ✓	0/0 B	IPv4 TCP/UDP	DMZ subnets	*	LAN_USER_10 subnets	3389 (MS RDP)	*	aucun			⚓ ✎ ⧉ ⊘ 🗑 ✕
Apache Guacamole - LAN_USER_20											🗑
☐ ✓	0/0 B	IPv4 TCP/UDP	DMZ subnets	*	LAN_USER_20 subnets	22 (SSH)	*	aucun			⚓ ✎ ⧉ ⊘ 🗑 ✕
☐ ✓	0/0 B	IPv4 TCP/UDP	DMZ subnets	*	LAN_USER_20 subnets	3389 (MS RDP)	*	aucun			⚓ ✎ ⧉ ⊘ 🗑 ✕
Apache Guacamole - LAN_USER_30											🗑
☐ ✓	0/0 B	IPv4 TCP/UDP	DMZ subnets	*	LAN_USER_30 subnets	22 (SSH)	*	aucun			⚓ ✎ ⧉ ⊘ 🗑 ✕
☐ ✓	0/0 B	IPv4 TCP/UDP	DMZ subnets	*	LAN_USER_30 subnets	3389 (MS RDP)	*	aucun			⚓ ✎ ⧉ ⊘ 🗑 ✕
Blocage par défaut											🗑
☐ ✕	0/235 KiB	IPv4+6 *	*	*	*	*	*	aucun			⚓ ✎ ⧉ ⊘ 🗑

5.3 Règle du Pare-feu – Lan_USER_X.

Règles (Faire glisser pour changer l'ordre)

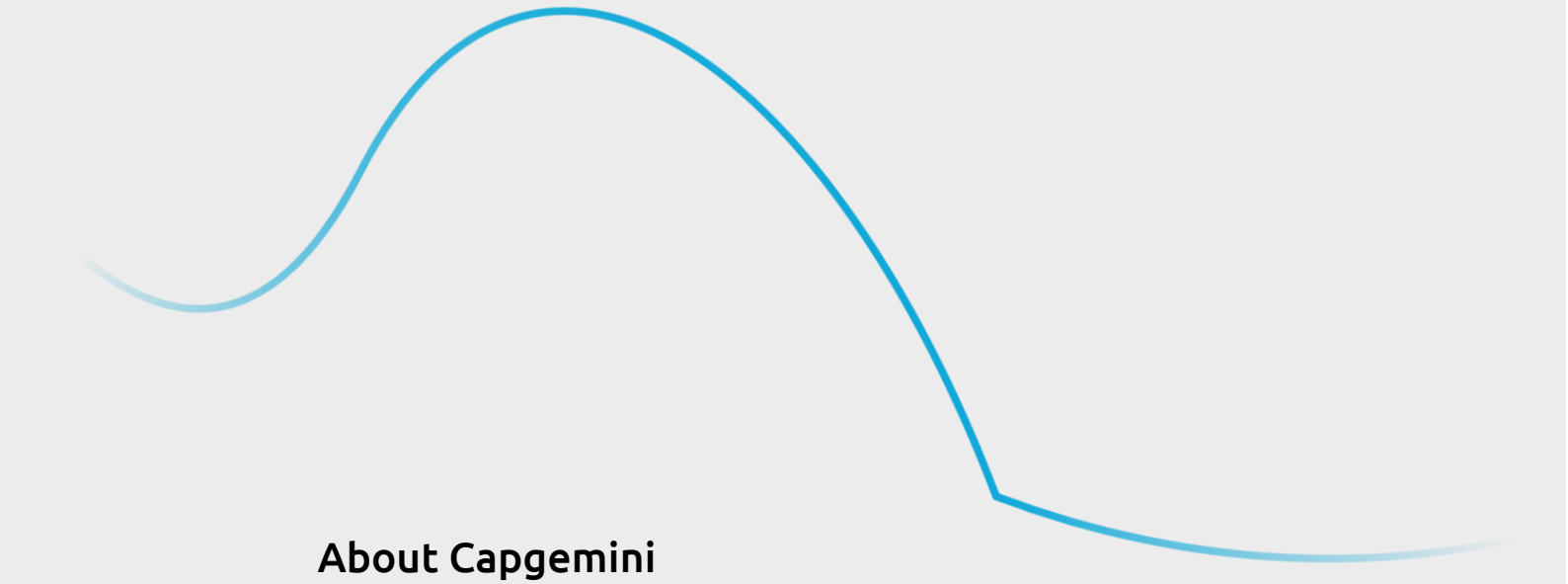
	États	Protocole	Source	Port	Destination	Port	Passerelle	File d'attente	Ordonnancement	Description	Actions
☐	✓	0/0 B	IPv4 TCP	LAN_USER_10 subnets	*	*	80 (HTTP)	*	aucun		
☐	✓	0/0 B	IPv4 TCP	LAN_USER_10 subnets	*	*	443 (HTTPS)	*	aucun		
DNS											
☐	✓	0/0 B	IPv4 UDP	LAN_USER_10 subnets	*	1.1.1.3	53 (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		
Supervsion - 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 - LLDAP										
	LAN	TCP/UDP	*	*	192.168.1.3	3890	10.16.100.253	3890		



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