

Documentation technique

*27/03/2024
Installation et
configuration du
pare-feu PfSense*

Sommaire

- Définition
- Schéma réseau
- Prérequis
- Installation de PfSense
- Configuration de l'IP de l'interface PfSense
- Configuration des VLAN sur l'interface PfSense
- Etablissement de règles de firewall
- Configuration du NAT

Définition

PfSense

PfSense est un système d'exploitation open source basé sur FreeBSD, conçu pour être utilisé comme pare-feu, routeur et passerelle de sécurité. Parmi les pare-feu gratuit les plus utilisés, il offre une gamme de fonctionnalités avancées de sécurité et de routage.

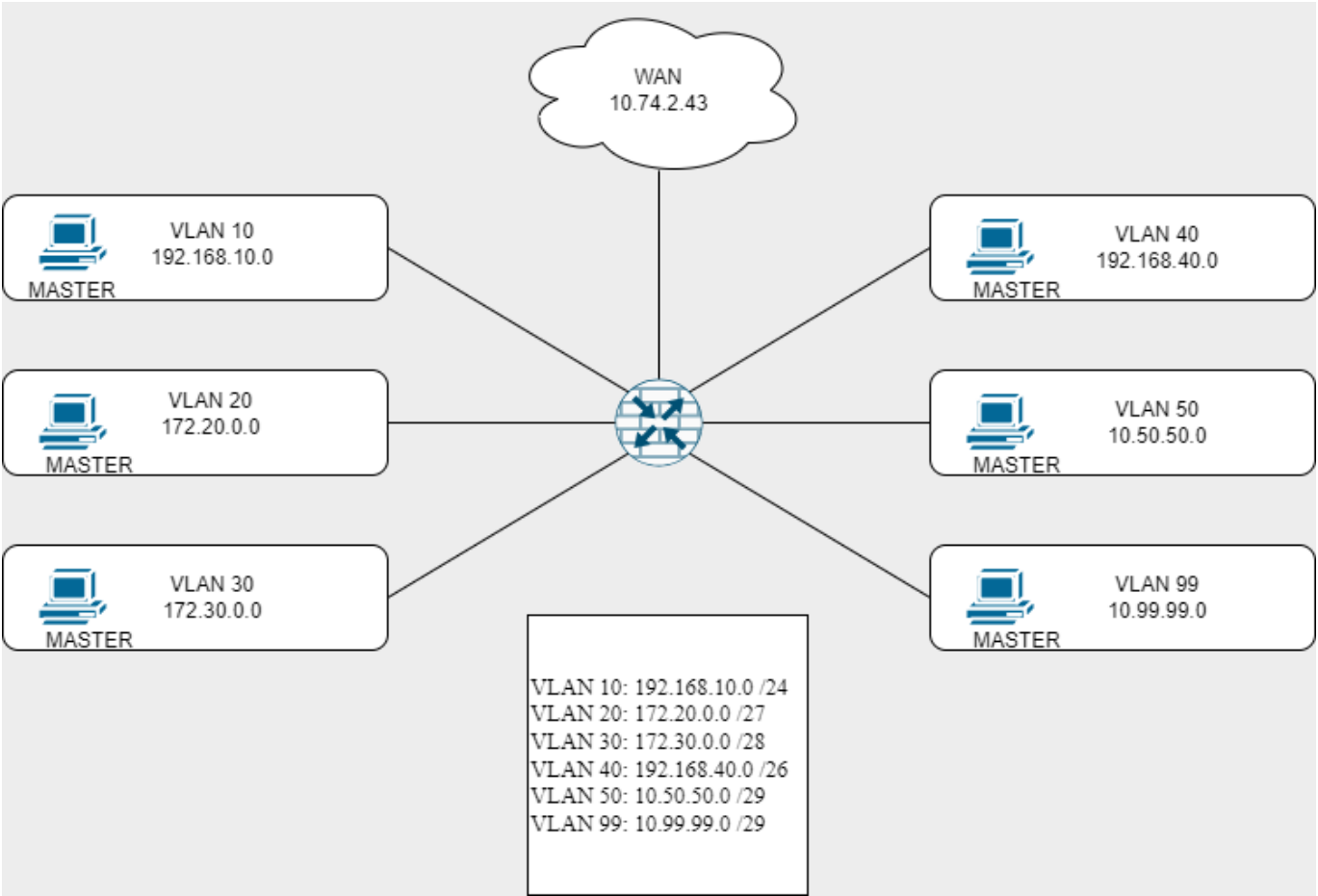
Pare-feu

Un pare-feu est un équipement de protection du réseau. Il surveille le trafic entrant et sortant et décide s'il est autorisé ou non à passer par certains ports en fonction des règles de sécurité prédéfinies.

Fonctionnalités

- **Pare-feu avancé** : PfSense inclut un pare-feu puissant qui peut être configuré pour filtrer le trafic réseau en fonction de critères tels que les adresses IP source et destination, les ports TCP/UDP, les protocoles, etc.
- **NAT** (Network Address Translation) : Il prend en charge la translation d'adresses réseau pour permettre à plusieurs périphériques sur un réseau privé d'accéder à Internet via une seule adresse IP publique.
- **VPN** (Virtual Private Network) : PfSense permet la création de tunnels VPN pour sécuriser la communication entre différents réseaux ou pour permettre l'accès sécurisé à distance aux ressources réseau.
- **Load balancing** et haute disponibilité : Il offre des fonctionnalités de répartition de charge et de redondance pour garantir la disponibilité et la performance des services réseau.
- **Proxy Web** : Il peut être configuré pour agir en tant que serveur proxy HTTP/HTTPS (avec SQUID) et pour filtrer le contenu Web en fonction de politiques définies par l'utilisateur.
- **Contrôle de la bande passante** : PfSense permet de limiter et de prioriser le trafic réseau en fonction de différents critères, ce qui est utile pour optimiser l'utilisation de la bande passante dans un réseau. la fonction ou toute autre caractéristique pertinente.

Schéma réseau

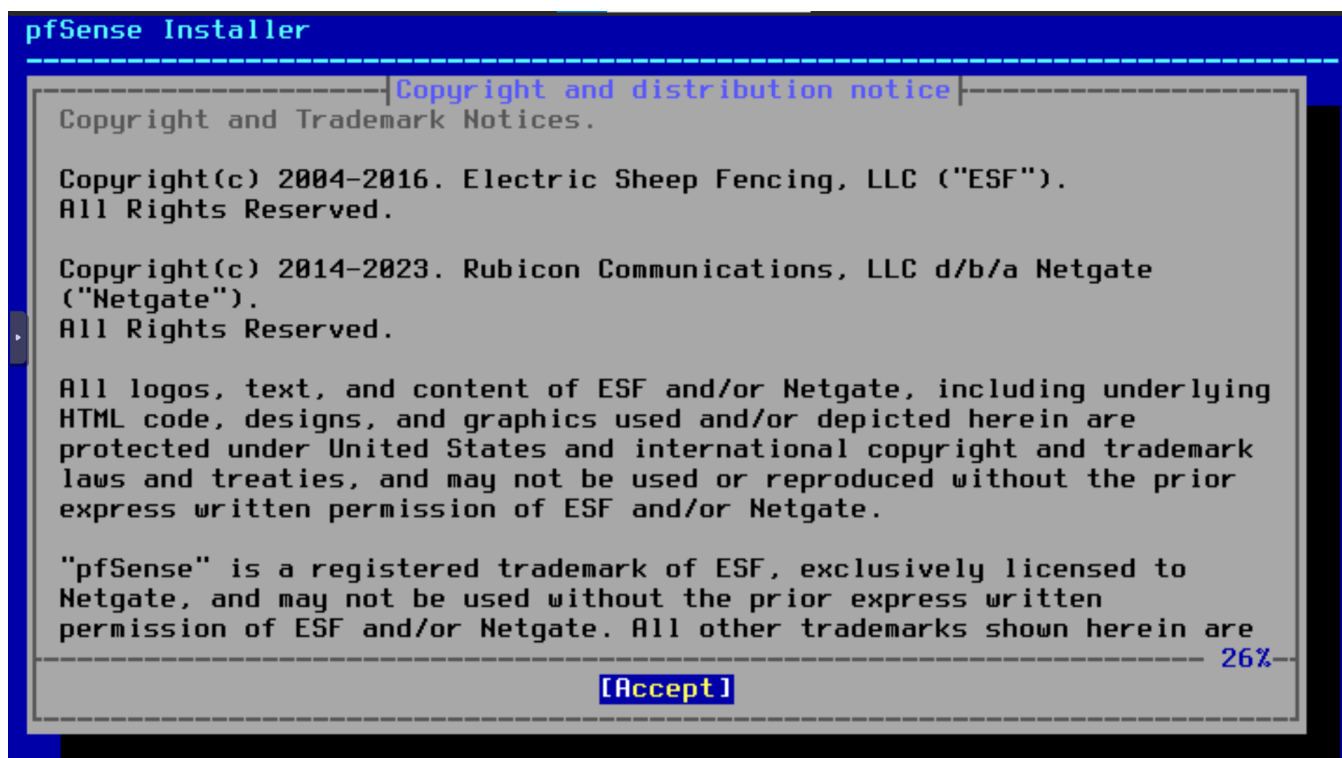


Prérequis

- Processeur 1,4 GHz 64 bits
- A minima 1 Go de RAM
- 8 Go d'espace disque
- Une ou plusieurs cartes réseaux
- Une clé bootable avec l'ISO de la dernière version de PfSense

Installation de PfSense

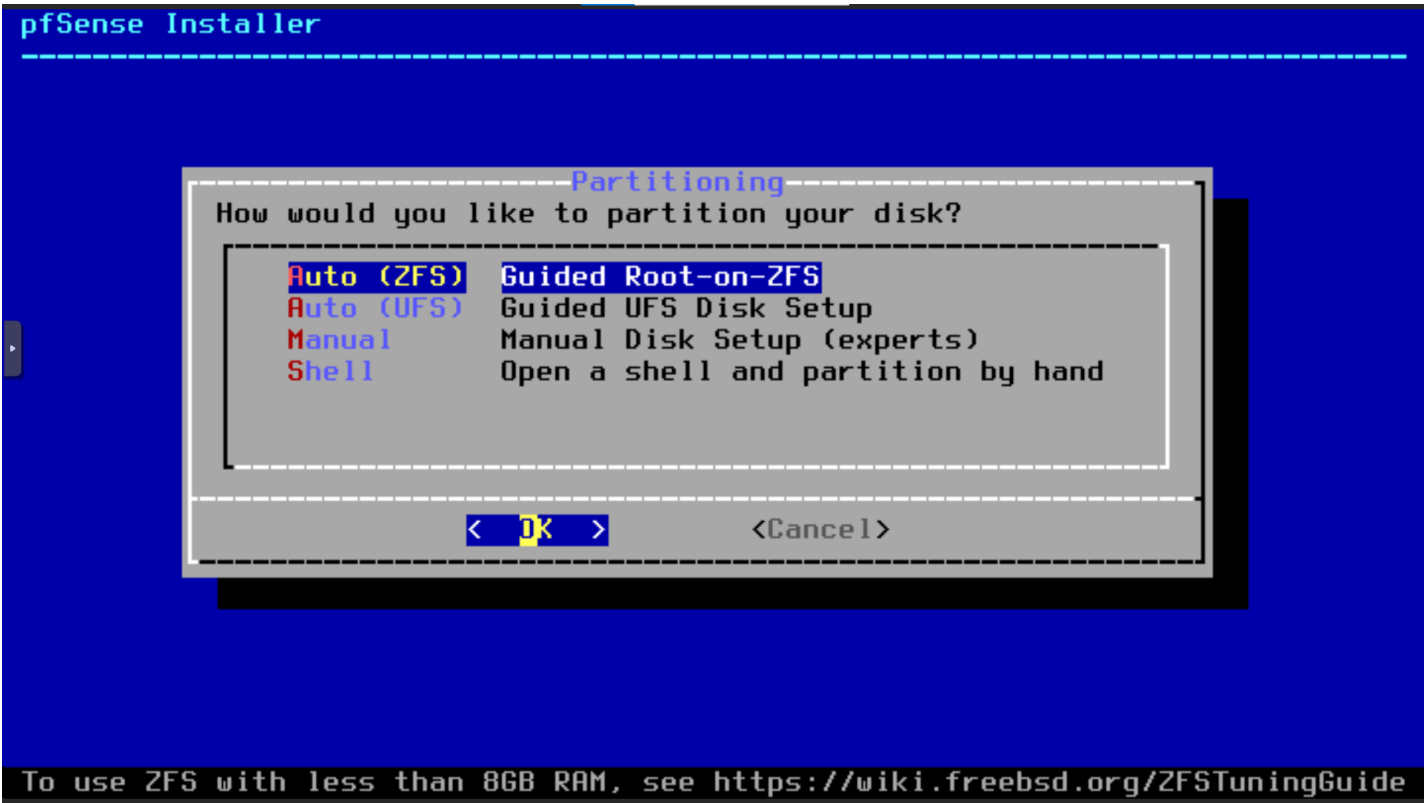
Après avoir fait booter la machine sur l'ISO PfSense, l'installation commence.
Il faut accepter la licence utilisateur.



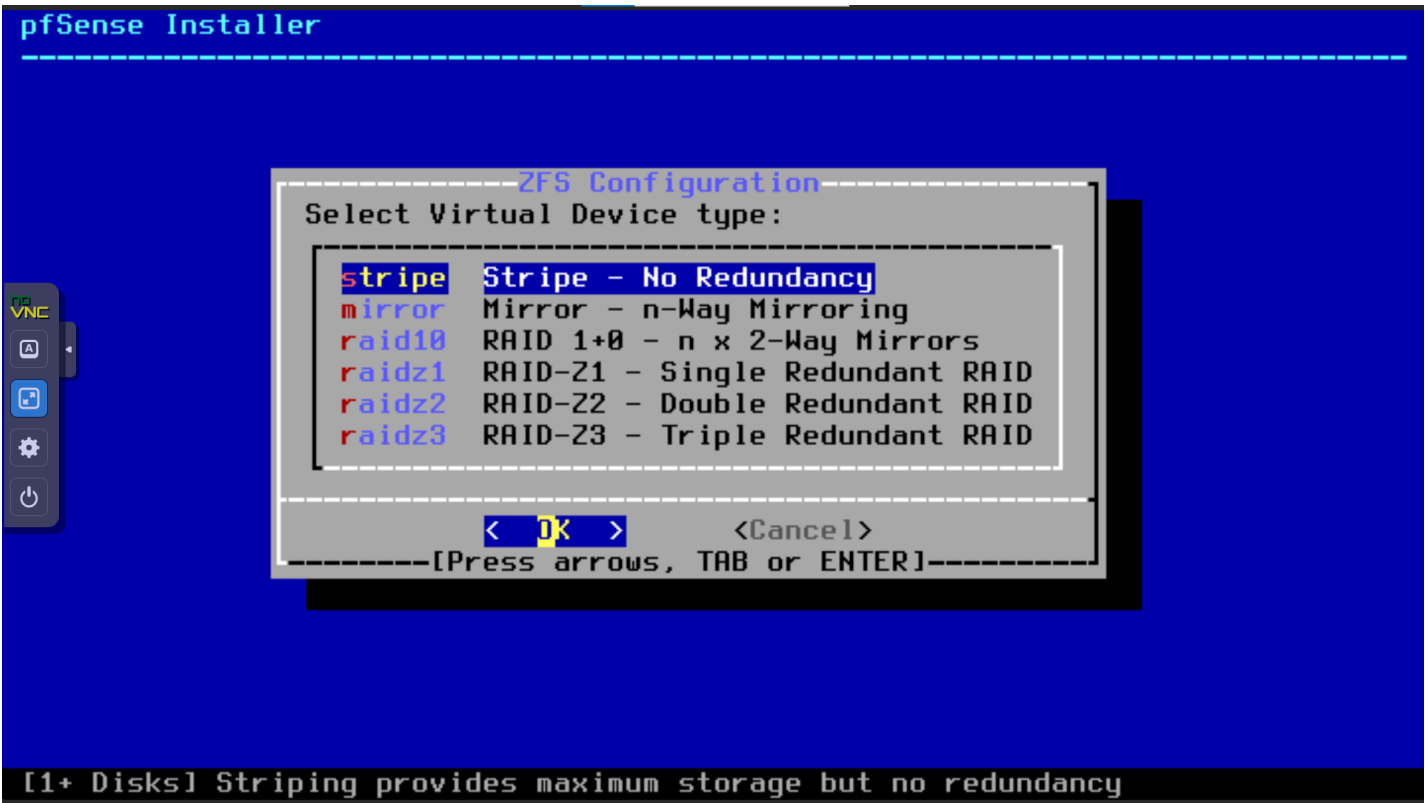
Choisir l'installation.



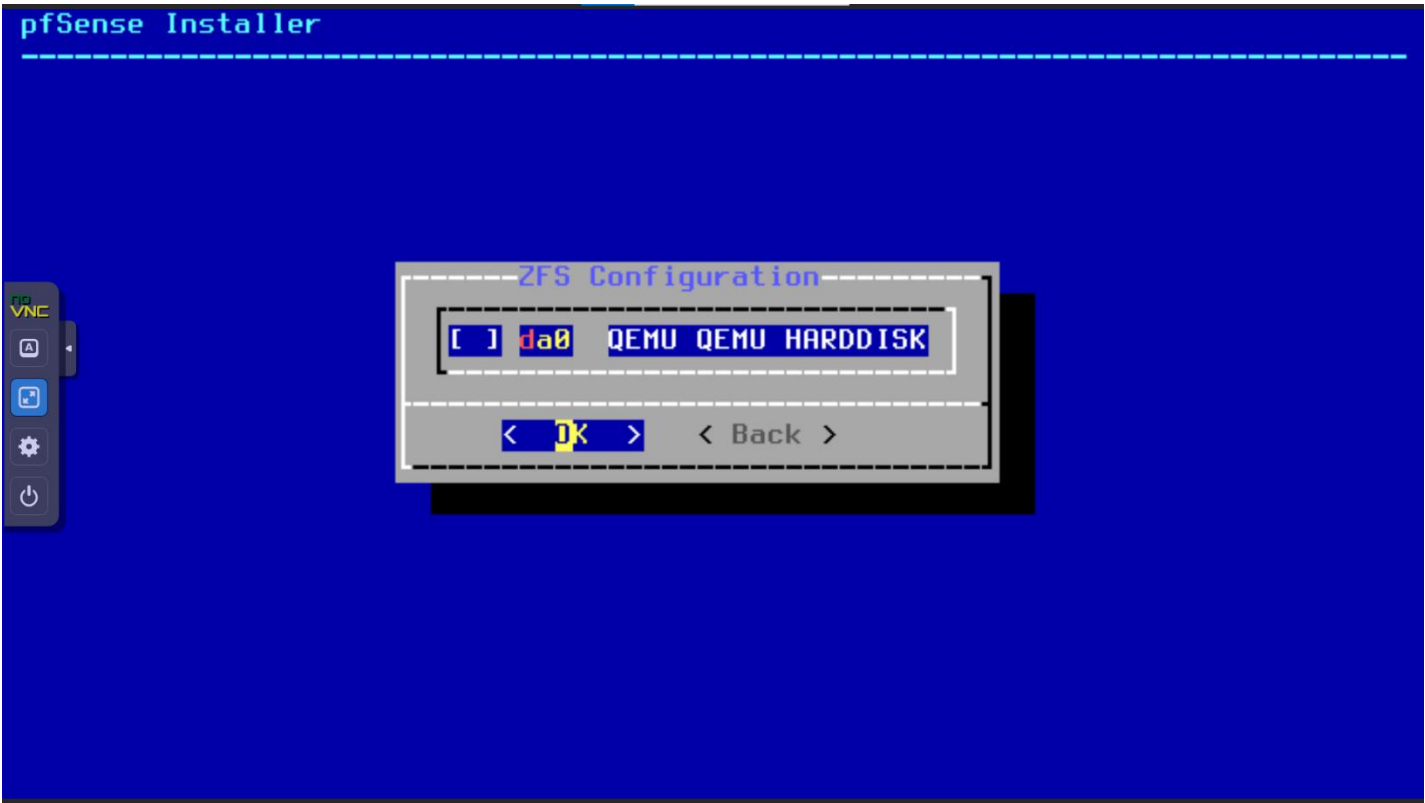
Sélectionner l'installation Auto en ZFS (système de fichiers open source sous licence CDDL).



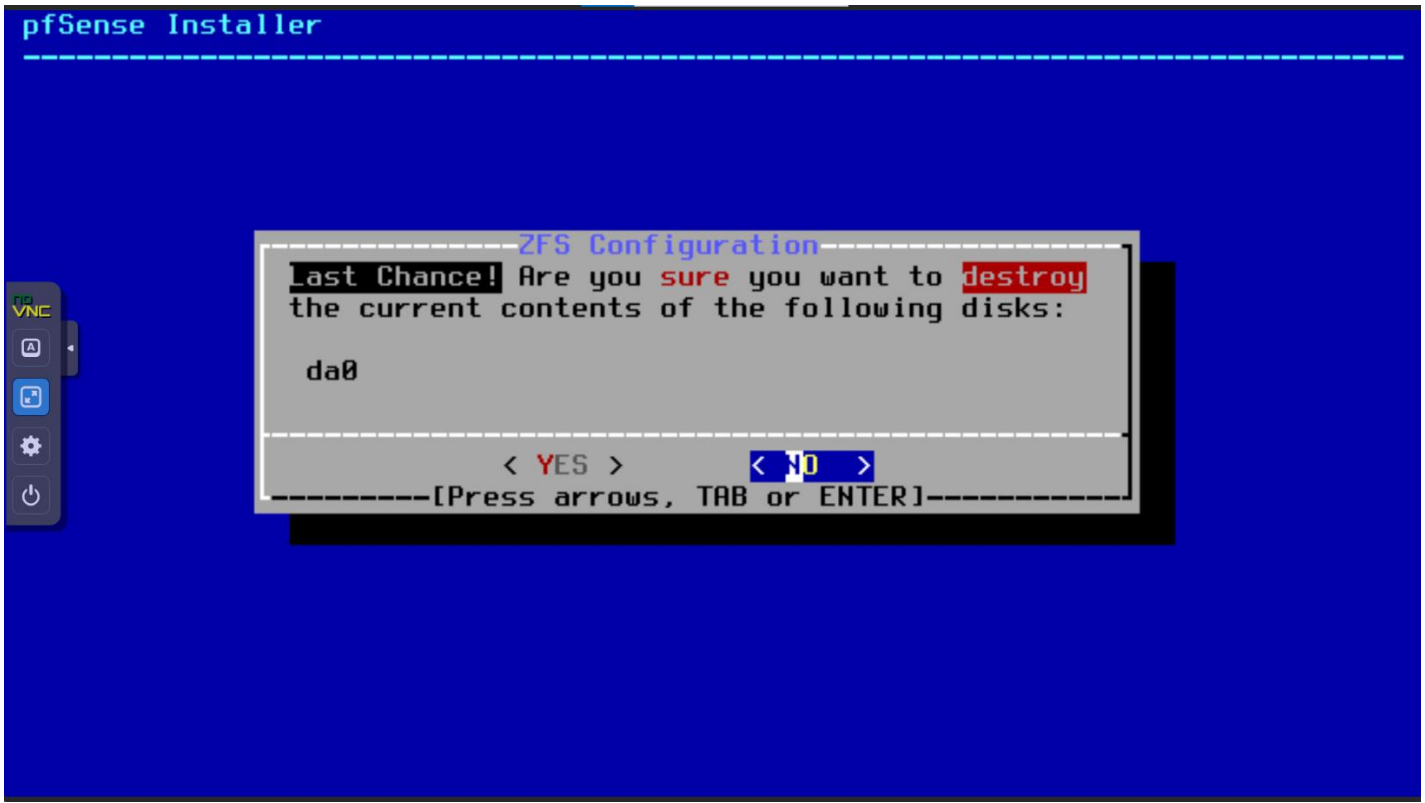
Prendre l'installation sur un équipement (sans redondance).



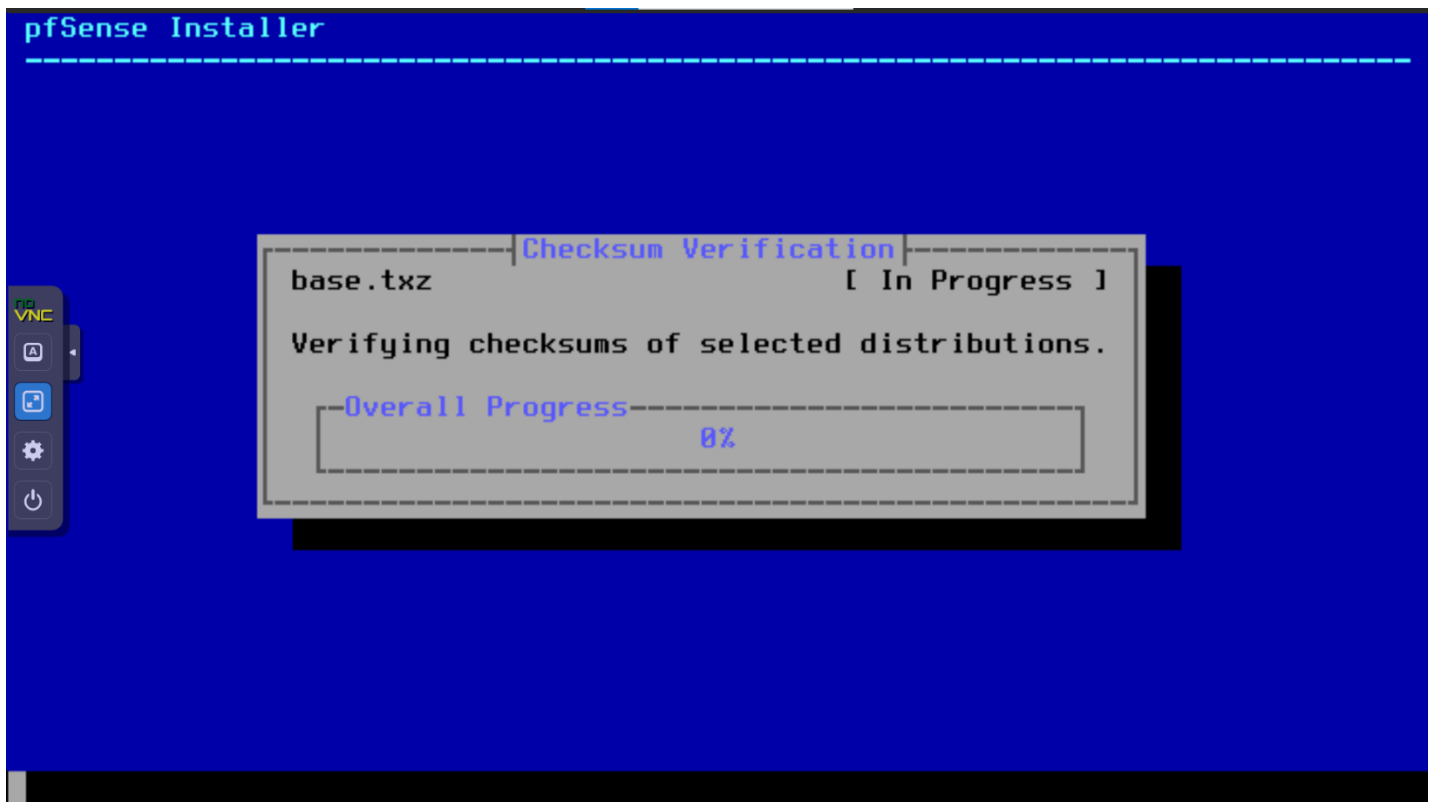
Sélectionner son disque.



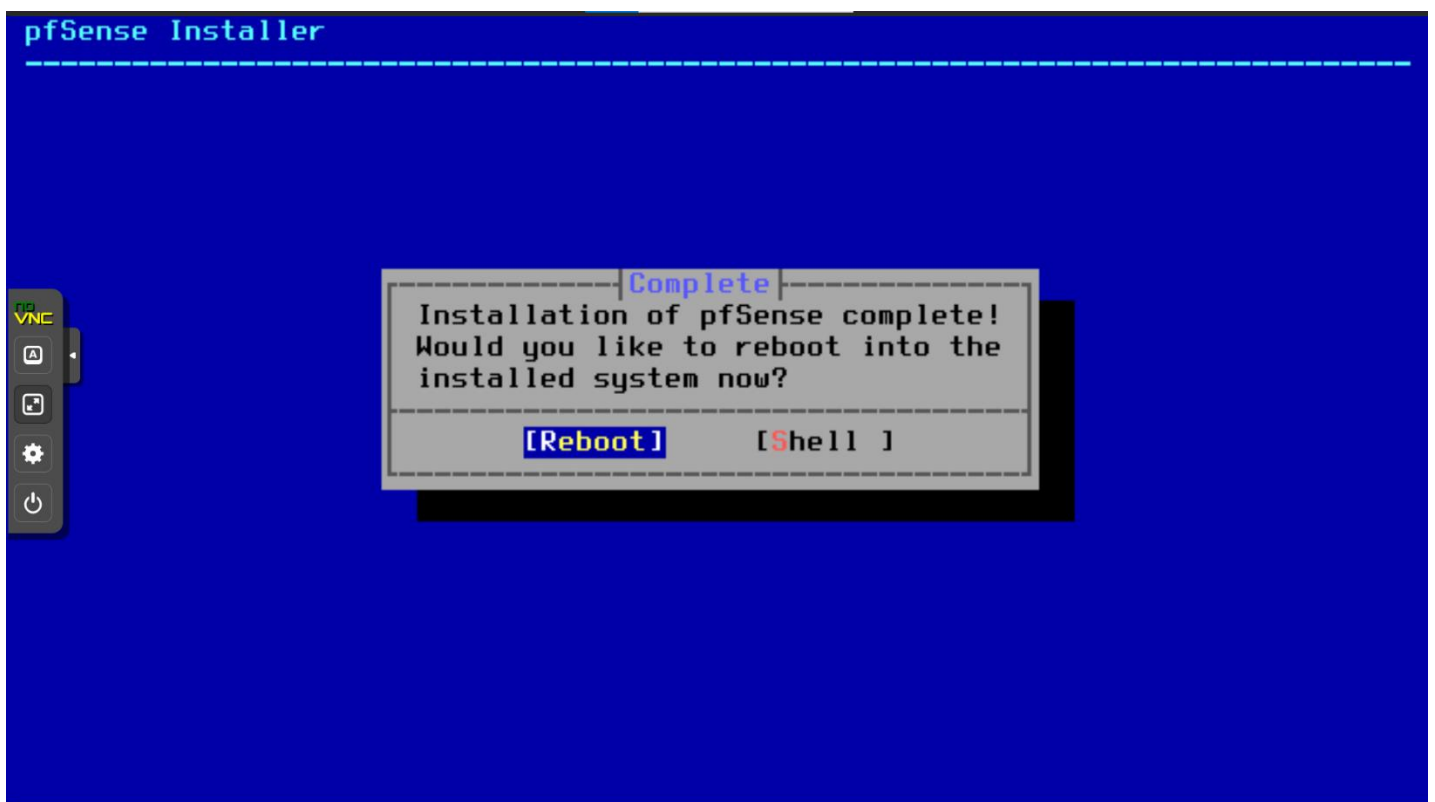
Et valider l'écriture.



L'installation va se faire.



A la fin de l'installation, redémarrer la machine.



Configuration de l'IP de l'interface PfSense

PfSense est basé sur FreeBSD (une version d'Unix), il faudra donc faire la configuration en ligne de commandes.

Il faut dans un premier temps assigner une interface au WAN. Pour cela, il faut sélectionner vtnet0 qui correspond au vmbr0 de Proxmox qui est la carte réseau virtuelle WAN.

```
vtnet0 02:bb:0c:4e:b1:5e (down) VirtIO Networking Adapter

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [yln]? y
VLAN Capable interfaces:

vtnet0 02:bb:0c:4e:b1:5e (up)

Enter the parent interface name for the new VLAN (or nothing if finished):

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
(vtnet0 or a): vtnet0

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

The interfaces will be assigned as follows:

WAN -> vtnet0

Do you want to proceed [yln]? y

Writing configuration...done.
One moment while the settings are reloading... done!
Configuring loopback interface...done.
Configuring WAN interface...█
```

Une fois que c'est fait, PfSense obtiendra une IP en DHCP. C'est l'adresse de l'interface web du pare-feu.

```
*** Welcome to pfSense 2.7.0-RELEASE (amd64) on pfSense ***

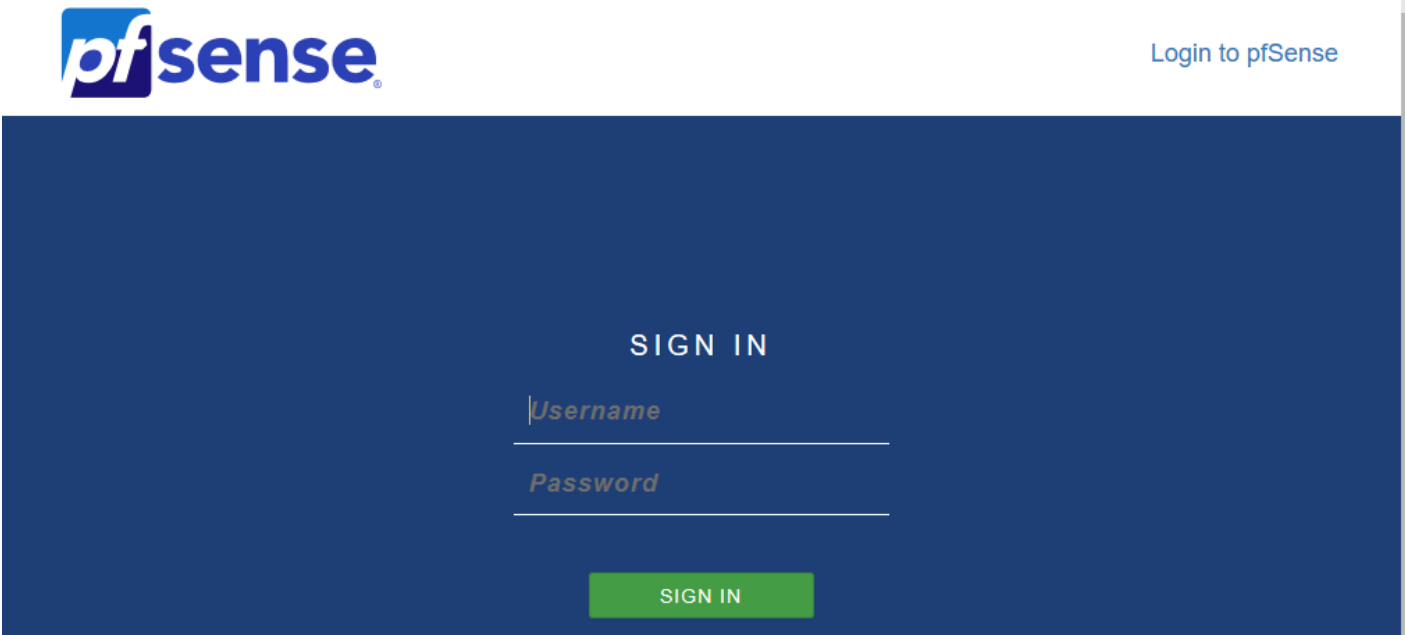
WAN (wan) -> vtnet0 -> v4/DHCP4: 10.74.2.43/22

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: █
```

Configuration des VLAN sur l'interface PfSense

Il faut se rendre sur l'adresse IP du PfSense pour accéder à son interface Web.



Une fois dessus, il faudra se connecter avec l'utilisateur *admin* et le mot de passe par défaut. Il sera par la suite demandé de le modifier en allant dans **System, User Manager, Users** et **Edit**.

Users Groups Settings Authentication Servers

User Properties

Defined by	SYSTEM		
Disabled	<input type="checkbox"/> This user cannot login		
Username	admin		
Password	*****	<input type="password"/>	
Full name	System Administrator <small>User's full name, for administrative information only</small>		
Expiration date	<input type="text"/> <small>Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY</small>		
Custom Settings	<input type="checkbox"/> Use individual customized GUI options and dashboard layout for this user.		
Group membership	<div>Not member of</div>	<div>Member of</div> <div>admins</div>	

pfSense
COMMUNITY EDITION

System

Interfaces

Firewall

Services

VPN

Status

Diagnostics

Help

System / User Manager / Users

?

Users

Groups

Settings

Authentication Servers

Users

	Username	Full name	Status	Groups	Actions
<input type="checkbox"/>	admin	System Administrator	✓	admins	

+ Add

Delete

i

Une fois que c’est fait, il faut se rendre sur **Interfaces**, **VLANs** et **Edit** afin d’ajouter les VLAN créés préalablement sur Proxmox à PfSense.

pfSense
COMMUNITY EDITION

System

Interfaces

Firewall

Services

VPN

Status

Diagnostics

Help

Interfaces / VLANs / Edit

?

VLAN Configuration

Parent Interface	<div>vtnet1 (02:ce:9a:d7:03:dc)</div> <div>Only VLAN capable interfaces will be shown.</div>
VLAN Tag	<div>VLAN 1</div> <div>802.1Q VLAN tag (between 1 and 4094).</div>
VLAN Priority	<div>0</div> <div>802.1Q VLAN Priority (between 0 and 7).</div>
Description	<div>Description</div> <div>A group description may be entered here for administrative reference (not parsed).</div>

Save

pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 [View license](#).

Ici, tous les VLAN sont ajoutés :

pfSense
COMMUNITY EDITION

System

Interfaces

Firewall

Services

VPN

Status

Diagnostics

Help

Interfaces / VLANs

?

Interface Assignments

Interface Groups

Wireless

VLANs

QinQs

PPPs

GREs

GIFs

Bridges

LAGGs

VLAN Interfaces

Interface	VLAN tag	Priority	Description	Actions
vtnet1	1			
vtnet2	2			
vtnet3	3			
vtnet4	4			
vtnet5	5			
vtnet6	6			

+ Add

PFSENSE

COUSIN Antonin
EL GARHI Myriam

12

Une fois que les VLAN ont été ajoutés sur l'interface, il est possible de vérifier sur la machine qu'ils ont tous été pris en compte. Ici, nous pouvons voir que tous nos VLAN ont bien été ajouté au firewall.

```
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> vtnet0      -> v4/DHCP4: 10.74.2.43/22
VLAN10 (lan)   -> vtnet1      -> v4: 192.168.10.1/24
VLAN20 (opt1)  -> vtnet2      -> v4: 172.20.0.1/27
VLAN30 (opt2)  -> vtnet3      -> v4: 172.30.0.1/28
VLAN40 (opt3)  -> vtnet4      -> v4: 192.168.40.1/26
VLAN50 (opt4)  -> vtnet5      -> v4: 10.50.50.1/29
VLAN99 (opt5)  -> vtnet6      -> v4: 10.99.99.1/29
```

Etablissement des règles de firewall

Afin d'utiliser le pare-feu, il est nécessaire d'établir des règles autorisant ou refusant le flux de tels ou tels paquets.

Flottant(e)WAVLAN10VLAN20VLAN30VLAN40VLAN50VLAN99OpenVPN

Règles (Faire glisser pour changer l'ordre)

<input type="checkbox"/>	États	Protocole	Source	Port	Destination	Port	Passerelle	File d'attente	Ordonnancement	Description	Actions
<input checked="" type="checkbox"/>	0/22,55 MiB	*	*	*	VLAN10 Address	443 80	*	*		Règle anti-blocage	
<input type="checkbox"/>	0/0 B	IPv4 TCP/UDP	VLAN10 subnets	*	*	445 (MS DS)	*	aucun			
<input type="checkbox"/>	0/0 B	IPv4 TCP/UDP	VLAN10 subnets	*	*	21 (FTP)	*	aucun			
<input type="checkbox"/>	0/480 B	IPv4 ICMP echorep, echoreq	VLAN10 subnets	*	*	*	*	aucun		ping	
<input type="checkbox"/>	0/29 KiB	IPv4 TCP/UDP	VLAN10 subnets	*	*	53 (DNS)	*	aucun			
<input type="checkbox"/>	0/7,66 MiB	IPv4 TCP/UDP	VLAN10 subnets	*	*	80 (HTTP)	*	aucun			
<input type="checkbox"/>	5/186,85 MiB	IPv4 TCP/UDP	VLAN10 subnets	*	*	443 (HTTPS)	*	aucun			
<input type="checkbox"/>	0/0 B	IPv4 TCP/UDP	VLAN10 subnets	*	*	3478 (STUN)	*	aucun		accès chrome RDP	
<input type="checkbox"/>	0/0 B	IPv4 TCP/UDP	VLAN10 address	3128	*	*	*	aucun		squid	
<input type="checkbox"/>	0/1,85 MiB	IPv4 *	*	*	*	*	*	aucun			

AjouterAjouterSupprimerToggleCopierEnregistrerSéparateur

Dans les règles établies dans chaque VLAN, on retrouve celles qui permettent l'accès aux sites Internet (en autorisant les protocoles HTTP/HTTPS et DNS pour la résolution de nom de domaine).

Ainsi que celles qui permettent le transfert de fichiers (en autorisant les protocole FTP et SMB) pour permettre au NAS de fonctionner.

Ou encore le ping entre machines du même VLAN ou de VLAN différents (en autorisant le protocole ICMP en echo request et echo reply).

D'autres ports et protocoles plus spécifiques peuvent être autorisés en fonction de chaque VLAN comme le protocole STUN sur le port 3478 ici pour permettre la connexion en bureau à distance via Chrome Remote Desktop, l'ouverture du port 1723 pour le tunnel VPN, du port 3128 pour le proxy SQUID ou encore 3389 pour le protocole RDP.

Configuration du NAT

Le NAT peut être mis en place depuis **NAT** dans l'onglet **Pare-feu**. Sur PfSense, il fonctionne sous forme de règles. Il existe plusieurs méthodes de NAT dont le port forwarding (redirection de port) ou le 1:1.

