

Mise en place

PFSENSE

Table des matières

1. Présentation de pfSense
2. Pré-requis matériels et réseau
3. Téléchargement et préparation du support d'installation
4. Installation pas à pas
5. Configuration initiale via la console
6. Premier accès WebGUI et assistant
7. Configuration réseau avancée (Interfaces & VLAN)
8. Services intégrés (DHCP, DNS Resolver, NTP)
9. Règles de pare-feu & NAT
10. VPN (OpenVPN • IPSec • WireGuard)
11. Haute Disponibilité (CARP, Sync)
12. Portail captif
13. IDS/IPS et filtrage (Suricata, pfBlockerNG)
14. Sauvegarde & restauration
15. Supervision & mises à jour
16. Bonnes pratiques de sécurité
17. Annexes

Présentation de pfSense

- pfSense est une distribution FreeBSD dédiée aux fonctions de routeur/pare-feu de niveau entreprise.
- Elle intègre un grand nombre de services : DHCP, DNS, VPN, IDS/IPS, portail captif, QoS, etc.

Pré-requis matériels et réseau

- • CPU 64-bit (1 GHz min) • 2 Go RAM • 8 Go de stockage.
- • Au moins 2 interfaces réseau (WAN + LAN).
- • Schéma d'adressage et VLAN planifiés.

Téléchargement et préparation

1. Télécharger l'image ISO x86_64 depuis <https://www.pfsense.org/download/>
2. Créer une clé USB bootable (Rufus / Etcher) ou un périphérique virtuel.
3. Vérifier le hash SHA-256.

Installation pas à pas

- Démarrer sur le support et sélectionner « Install pfSense ».
- Accepter la licence, choisir le clavier (French) et le partitionnement (Auto ZFS).
- Patienter durant la copie des fichiers puis redémarrer.

Configuration initiale console

- Attribuer WAN et LAN (re0 = WAN, re1 = LAN).
- Définir l'IP LAN (ex : 192.168.1.1/24) puis activer DHCP LAN si besoin.

Premier accès WebGUI

- Depuis un PC LAN, ouvrir <https://192.168.1.1>.
- Identifiants par défaut : admin / pfsense.
- Suivre l'assistant (Setup Wizard) : mot de passe, nom d'hôte, DNS, NTP, WAN.

Configuration réseau avancée

- - Ajout d'une interface OPT pour DMZ.
- - Création VLAN : Interfaces > Assign > VLANs.
- - Réseau Wi-Fi invité isolé.

Services intégrés

- DHCP : Pool LAN & réservation statique.
- DNS Resolver en mode récursif + overrides internes.
- NTP synchronisé sur fr.pool.ntp.org.

Règles de pare-feu & NAT

- Politique par défaut « deny all ».
- NAT Port Forward pour un serveur Web interne.
- Aliasing et schedules pour maintenance.

VPN

- • OpenVPN Road-Warrior SSL : création CA, certs, export client.
- • IPsec site-to-site (phase 1/2).
- • WireGuard (plugin).

Haute Disponibilité

- CARP VIP : configuration d'une IP virtuelle partagée.
- XMLRPC Sync pour règles & services.

Portail captif

- Authentification RADIUS / voucher.
- Redirection HTTPS et page personnalisée.

IDS/IPS & filtrage

- Snort/Suricata avec listes ET Pro.
- pfBlockerNG GeoIP + DNSBL.

Sauvegarde & restauration

- Sauvegarde automatique config.xml vers NAS.
- Versioning Git possible.

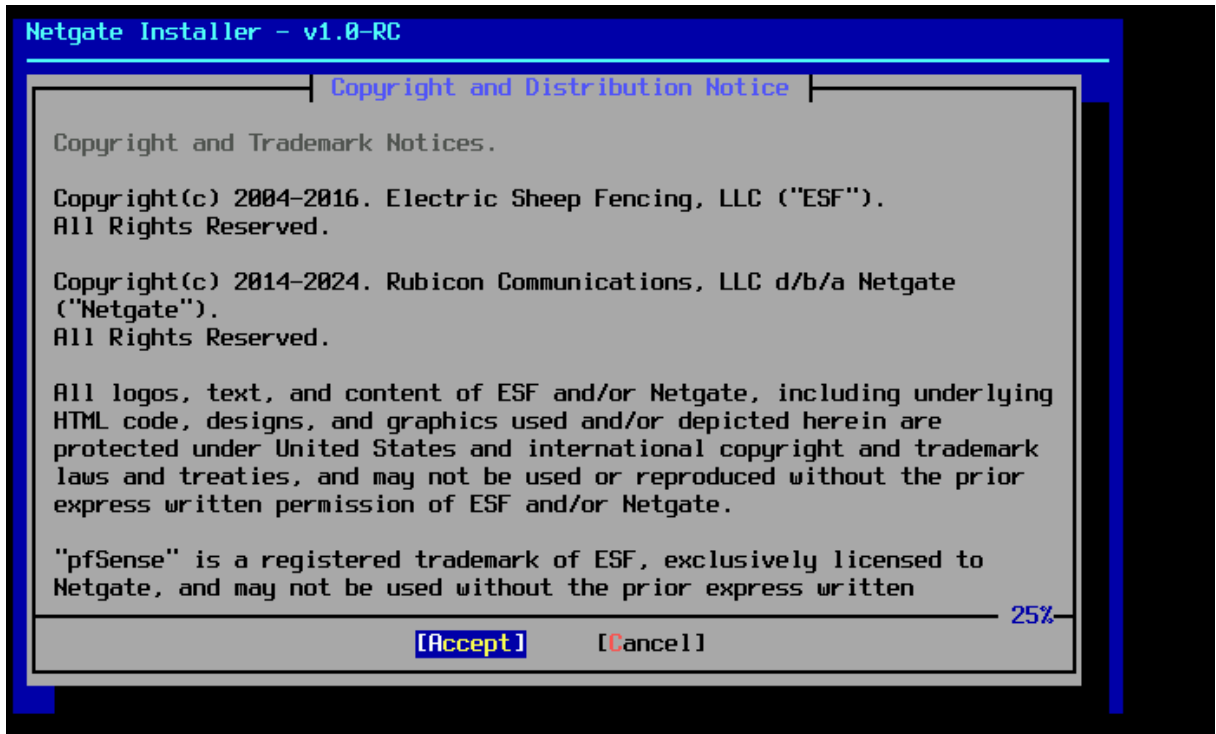
Supervision & mises à jour

- Notifications e-mail, dashboard InfluxDB/Grafana.
- MAJ via System > Update (branch CE stable).

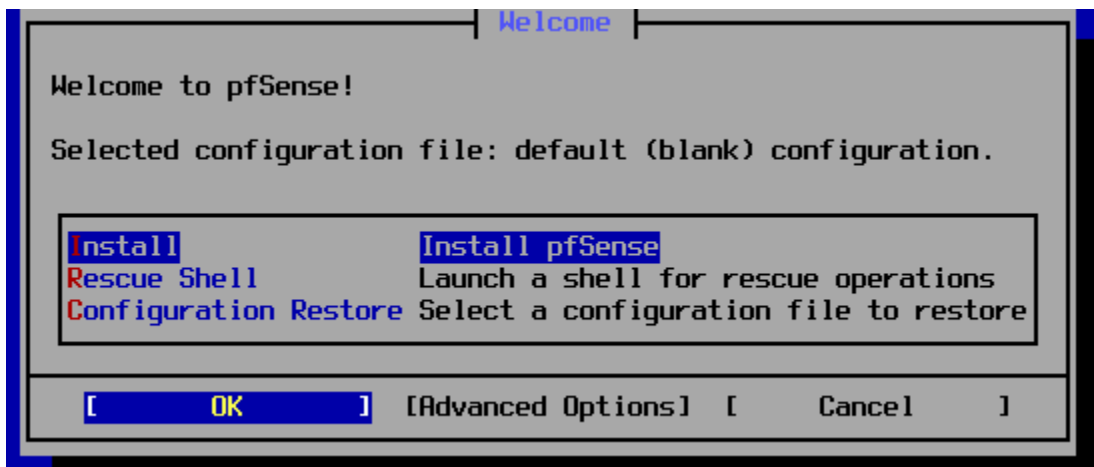
Bonnes pratiques de sécurité

- Accès SSH désactivé par défaut, 2FA WebGUI.
- Segmentation réseau, VLANs.
- Journalisation et retention des logs.

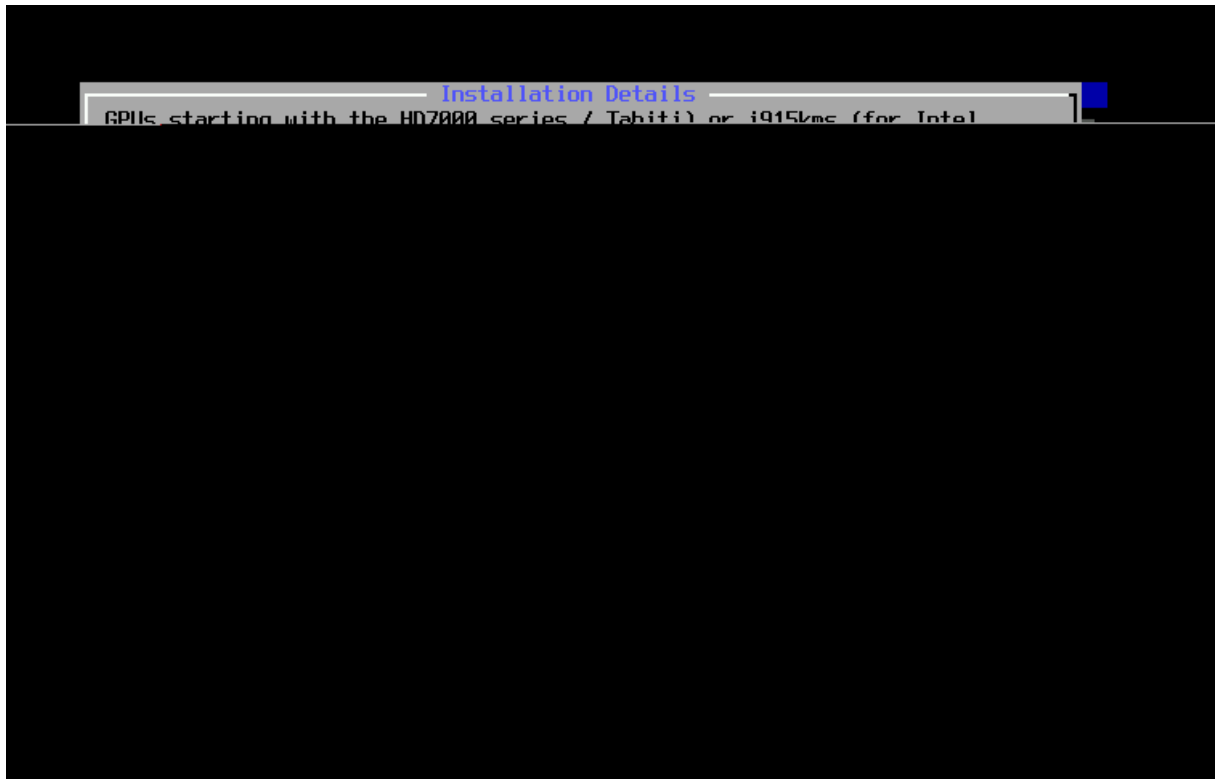
Lors de l'installation de pfSense on va acceptez les conditions d'utilisation :



Par la suite on installe le système :



On continue jusqu'à ce que l'installateur termine d'installer toutes les dépendances :



Par la suite le system reboot et on va arriver sur l'interface de base du pfsense :

```
Generating RRD graphs...done.
Starting syslog...done.
Starting CRON... done.
pfSense 2.8.0-RELEASE amd64 20250521-2312
Bootup complete

FreeBSD/amd64 (pfSense.home.arp) (ttyu0)

Microsoft Azure - Netgate Device ID: 4968701e0df29aa72e63

*** Welcome to pfSense 2.8.0-RELEASE (amd64) on pfSense ***

WAN (wan) -> hn0 -> v4/DHCP4: 172.18.237.245/20

0) Logout / Disconnect SSH          9) pfTop
1) Assign Interfaces                 10) Filter Logs
2) Set interface(s) IP address      11) Restart GUI
3) Reset admin account and 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: █
```