Documentation pfSense

Ce document explique comment installer et configurer pfSense, un pare-feu et routeur open-source basé sur FreeBSD.

1. Présentation

pfSense est une distribution libre de pare-feu/routeur, offrant :

- Filtrage de paquets (firewall) et NAT avancé
- VPN (OpenVPN, IPsec)
- Surveillance via Grafana/InfluxDB (extensions)
- Haute disponibilité (CARP, pfsync)
- Portail captif pour contrôle d'accès utilisateur

2. Prérequis

- Matériel dédié ou VM (1 CPU, 1 Go RAM minimum, 2 interfaces réseau).
- ISO pfSense téléchargée sur <https://www.pfsense.org/download/>.
- Clé USB (pour installation sur machine physique).
- Accès à la console (monitor/serial) ou interface VM.

3. Installation

3.1. Préparation du média

1. Téléchargez l'ISO pfSense (Architecture AMD64).

Créez une clé USB bootable avec Rufus (Windows) ou dd (Linux/macOS) :

```
dd if=pfSense-CE-2.6.0-RELEASE-amd64.iso of=/dev/sdX bs=4M status=progress
```

3.2. Installation sur VM (ex. VirtualBox)

1. Créez une VM :
 - Type : BSD → FreeBSD (64-bit)
 - RAM : ≥ 1 Go
 - Disque : ≥ 10 Go
 - Réseaux : NAT (WAN) et Adapter en Bridge ou Internal (LAN)
2. Montez l'ISO pfSense et démarrez la VM.
3. Suivez l'assistant : acceptation EULA, configuration clavier (français si besoin), partition automatique.
4. À la fin, acceptez le redémarrage sans l'ISO.

4. Configuration initiale

4.1. Interfaces réseau

- WAN (interface em0) : DHCP ou IP statique fournie par l'ISP.
- LAN (interface em1) : exemple 192.168.1.1/24.

À la première connexion, pfSense propose d'attribuer les interfaces WAN et LAN.

4.2. Accès Web GUI

Depuis une machine du réseau LAN, ouvrez un navigateur sur :

`http://192.168.1.1`

- 1.
2. Identifiants par défaut : admin / pfsense.
3. L'assistant de configuration vous guide : mot de passe admin, fuseau horaire (Europe/Paris), WAN/LAN.

5. Configuration de base

5.1. NAT et firewall

- Rules : Firewall > Rules > LAN (autoriser la sortie HTTP/HTTPS).
- NAT : Firewall > NAT > Outbound : mode automatique ou hybride pour config manuelle.

5.2. DHCP Server

- Services > DHCP Server > LAN : activer et définir plage DHCP (192.168.1.100–192.168.1.200).

5.3. DNS Resolver

- Services > DNS Resolver : activé par défaut, fournit la résolution récursive.

6. VPN OpenVPN

1. Services > OpenVPN > Wizards : suivez l'assistant pour créer une CA, un serveur, des utilisateurs.
2. Téléchargez le client .ovpn pour la distribution.

7. Sauvegarde et mise à jour

- Sauvegarde : Diagnostics > Backup & Restore.
- Mise à jour : System > Update : vérifier et appliquer les patches.

8. Bonnes pratiques

- Modifier le port Web GUI (System > Advanced > Admin Access).
- Configurer un VLAN pour séparer les réseaux.
- Mettre en place la haute disponibilité CARP si nécessaire.
- Monitorer via SNMP ou exporter vers Grafana.