Procédure d'installation

pfSense CE

sur Debian 11 / 12

Paramètre	Valeur
OS hôte	Debian 11/12
Type d'installation	Machine virtuelle (KVM/QEMU)
RAM recommandée VM	1 Go minimum (2 Go conseillé)
Stockage VM	20 Go minimum
Interfaces réseau	2 minimum (WAN + LAN)
Version pfSense	pfSense CE 2.7.x

1. Introduction

pfSense est une distribution open source basée sur FreeBSD qui permet de créer un pare-feu/routeur complet, fiable et hautement configurable. Étant basé sur FreeBSD, pfSense ne s'installe pas directement sur Debian : il s'installe sur sa propre machine (physique ou virtuelle).

Dans ce guide, nous allons déployer pfSense en tant que machine virtuelle KVM sur un serveur Debian. Cette approche est idéale pour virtualiser le pare-feu sur une infrastructure existante.

- Serveur physique ou VM Debian 11/12 avec KVM/QEMU installé
- VM pfSense avec 2 cartes réseau : WAN (accès internet) et LAN (réseau interne)
- Interface web de pfSense accessible depuis le LAN (port 443)

> ⚠ **Note :** *pfSense ne s'installe pas nativement sur Debian. L'installation se fait obligatoirement depuis l'ISO officielle pfSense dans une VM ou sur du matériel dédié.*

2. Prérequis sur le serveur Debian

▶ 2.1 Mise à jour du système

Avant toute installation, mettre à jour le système Debian pour s'assurer que tous les paquets sont à jour.

```
$ apt update && apt upgrade -y
```

▶ 2.2 Installation de KVM et des outils de virtualisation

KVM (Kernel-based Virtual Machine) est le hyperviseur intégré à Linux. Nous installons également libvirt pour gérer les VMs et virt-manager pour l'interface graphique (optionnel).

```
$ apt install -y qemu-kvm libvirt-daemon-system libvirt-clients bridge-utils
virtinst virt-manager
```

▶ 2.3 Vérification du support de la virtualisation

Vérifier que le processeur du serveur supporte bien la virtualisation matérielle (Intel VT-x ou AMD-V). La commande doit retourner un nombre supérieur à 0.

```
$ egrep -c '(vmx|svm)' /proc/cpuinfo
```

> ℹ **Info :** Un résultat > 0 confirme que la virtualisation matérielle est disponible. Si le résultat est 0, vérifier dans le BIOS que la virtualisation est activée.

▶ 2.4 Ajout de l'utilisateur au groupe libvirt

Ajouter votre utilisateur courant au groupe libvirt pour pouvoir gérer les VMs sans être root.

```
$ usermod -aG libvirt $(whoami)
$ usermod -aG kvm $(whoami)
```

> ⚠ **Note :** *Se déconnecter et se reconnecter après cette commande pour que les changements de groupe prennent effet.*

▶ 2.5 Démarrage et activation de libvirt

Activer le service libvirt au démarrage et le lancer immédiatement.

```
$ systemctl enable --now libvirtd
$ systemctl status libvirtd
```

3. Configuration réseau sur Debian

▶ 3.1 Création d'un bridge réseau

Nous allons créer un bridge réseau (br0) pour connecter la VM pfSense au réseau physique. Le bridge agit comme un commutateur virtuel entre la VM et le réseau réel.

Éditer la configuration réseau de Debian :

```
$ nano /etc/network/interfaces
```

Contenu à adapter (remplacer enp3s0 par votre interface réseau physique) :

```
# Interface physique - désactiver sa config IP directe
auto enp3s0
iface enp3s0 inet manual

# Bridge br0 - remplace l'interface physique
auto br0
iface br0 inet static
    address 192.168.1.10
    netmask 255.255.255.0
    gateway 192.168.1.1
    bridge_ports enp3s0
    bridge_stp off
    bridge_fd 0
```

Appliquer la configuration :

```
$ systemctl restart networking
$ ip addr show br0
```

> ⚠ **Note :** *Adapter l'adresse IP, le masque et la passerelle à votre environnement réseau réel.*

▶ 3.2 Création d'un réseau NAT pour le LAN (optionnel)

Alternativement, créer un réseau virtuel NAT dans libvirt pour le LAN pfSense. Cela isole le réseau interne de l'hôte.

```
$ virsh net-list --all
$ virsh net-start default
$ virsh net-autostart default
```

4. Téléchargement de l'ISO pfSense

▶ 4.1 Téléchargement depuis le site officiel

Télécharger l'image ISO pfSense CE depuis le site officiel de Netgate. L'image est au format .gz et doit être décompressée.

```
$ cd /var/lib/libvirt/images/
$ wget
https://atxfiles.netgate.com/mirror/downloads/pfSense-CE-2.7.2-RELEASE-amd64.iso.g
z
```

> ⚠ **Note :** *Vérifier l'URL sur https://www.pfsense.org/download/ car la version peut avoir évolué.*

▶ 4.2 Décompression de l'image

Décompresser l'archive .gz pour obtenir le fichier ISO utilisable.

```
$ gunzip pfSense-CE-2.7.2-RELEASE-amd64.iso.gz
$ ls -lh pfSense-CE-2.7.2-RELEASE-amd64.iso
```

▶ 4.3 Vérification de l'intégrité (recommandé)

Vérifier le checksum SHA256 de l'ISO pour s'assurer que le téléchargement est intègre.

```
$ sha256sum pfSense-CE-2.7.2-RELEASE-amd64.iso
```

> ℹ **Info :** Comparer le résultat avec le hash SHA256 affiché sur la page de téléchargement officielle pfSense.

5. Création de la machine virtuelle pfSense

▶ 5.1 Création du disque virtuel

Créer un disque dur virtuel de 20 Go en format qcow2, qui offre une allocation dynamique de l'espace.

```
$ qemu-img create -f qcow2 /var/lib/libvirt/images/pfsense.qcow2 20G
```

▶ 5.2 Installation de la VM en ligne de commande

Lancer l'installation de pfSense avec virt-install. La VM est configurée avec 2 interfaces réseau : une en bridge (WAN) et une en réseau NAT interne (LAN).

```
$ virt-install \
  --name pfsense \
  --ram 1024 \
  --vcpus 1 \
  --disk path=/var/lib/libvirt/images/pfsense.qcow2,format=qcow2 \
  --cdrom /var/lib/libvirt/images/pfSense-CE-2.7.2-RELEASE-amd64.iso \
  --network bridge=br0 \
  --network network=default \
  --os-variant freebsd13.0 \
  --graphics vnc,listen=0.0.0.0 \
  --noautoconsole
```

> ⚠ **Note :** *L'option --graphics vnc permet d'accéder à la console VNC de la VM depuis un client VNC (port 5900 par défaut).*

▶ 5.3 Accès à la console VNC

Récupérer le port VNC attribué à la VM, puis se connecter avec un client VNC.

```
$ virsh vncdisplay pfsense
```

Se connecter ensuite depuis un client VNC (ex: TigerVNC, RealVNC) à l'adresse :

```
$ vncviewer <IP_SERVEUR>:5900
```

6. Installation de pfSense (via interface VNC)

Les étapes suivantes se font depuis la console VNC. pfSense démarre sur l'ISO et propose un menu d'installation.

▶ 6.1 Démarrage et acceptation de la licence

- Au démarrage, appuyer sur Entrée pour lancer l'installeur
- Accepter les conditions de licence (Accept)
- Sélectionner Install pfSense

▶ 6.2 Configuration du clavier

- Choisir la disposition du clavier (French (accent keys) pour AZERTY)
- Valider avec Continue

▶ 6.3 Partitionnement du disque

- Sélectionner Auto (ZFS) pour un partitionnement automatique recommandé
- Choisir Stripe (pas de redondance) pour une VM avec un seul disque
- Sélectionner le disque virtuel (da0) et valider
- Confirmer l'effacement du disque avec YES

▶ 6.4 Fin de l'installation

- L'installation copie les fichiers sur le disque (quelques minutes)
- Sélectionner No Shell pour ne pas ouvrir de shell post-install
- Cliquer sur Reboot pour redémarrer

> ⚠ **Note :** *Après le reboot, l'ISO sera éjectée automatiquement si virt-install a bien configuré la VM. Sinon, éjecter manuellement le CD via virsh.*

```
$ virsh change-media pfsense hda --eject
```

7. Configuration initiale de pfSense

▶ 7.1 Attribution des interfaces réseau

Au premier démarrage, pfSense demande d'assigner les interfaces réseau. Répondre via la console VNC :

- Should VLANs be set up now? → n
- WAN interface name → vtnet0 (première interface, connectée à br0)
- LAN interface name → vtnet1 (deuxième interface, réseau interne)
- Confirmer avec y

▶ 7.2 Configuration de l'IP LAN

Dans le menu principal de pfSense (console), choisir l'option 2 (Set interface(s) IP address) pour configurer l'IP du LAN.

- Sélectionner l'interface LAN
- Entrer l'adresse IP LAN : 192.168.2.1
- Entrer le masque : 24
- Valider sans passerelle pour le LAN
- Activer le serveur DHCP sur le LAN si souhaité

> ℹ **Info :** L'IP LAN par défaut est 192.168.1.1. La modifier si elle entre en conflit avec votre réseau existant.

8. Accès à l'interface web de pfSense

▶ 8.1 Depuis un client sur le LAN

Connecter une machine cliente au réseau LAN de pfSense (réseau interne), puis ouvrir un navigateur :

```
$ https://192.168.2.1
```

Identifiants par défaut :

- **admin** Identifiant :
- **pfsense** Mot de passe :

> ⚠ **Note :** *Changer immédiatement le mot de passe par défaut lors de la première connexion !*

▶ 8.2 Assistant de configuration initiale (Setup Wizard)

Au premier login, pfSense lance automatiquement l'assistant de configuration. Renseigner les informations suivantes :

- Hostname : nom de votre pare-feu (ex: pfsense-prod)
- Domain : votre domaine local (ex: local.lan)
- DNS primaire : 8.8.8.8 (Google) ou 1.1.1.1 (Cloudflare)
- Serveur NTP : 0.pfsense.pool.ntp.org
- Configuration WAN : DHCP ou IP statique selon votre FAI
- Configuration LAN : 192.168.2.1 / 24
- Changer le mot de passe admin
- Recharger la configuration et terminer l'assistant

9. Gestion de la VM pfSense avec virsh

▶ 9.1 Commandes de base

Voici les commandes virsh essentielles pour gérer la VM pfSense au quotidien.

```
$ virsh list --all
$ virsh start pfsense
$ virsh shutdown pfsense
$ virsh reboot pfsense
$ virsh destroy pfsense
```

▶ 9.2 Démarrage automatique au boot

Configurer la VM pour démarrer automatiquement avec le serveur Debian.

```
$ virsh autostart pfsense
$ virsh autostart --disable pfsense
```

▶ 9.3 Snapshot de la VM

Créer un snapshot (point de restauration) avant toute modification importante.

```
$ virsh snapshot-create-as pfsense snap-initial --description 'Config initiale
pfSense'
$ virsh snapshot-list pfsense
$ virsh snapshot-revert pfsense snap-initial
```

▶ 9.4 Export/Backup de la VM

Sauvegarder la configuration XML et le disque de la VM.

```
$ virsh dumpxml pfsense > /backup/pfsense.xml
$ cp /var/lib/libvirt/images/pfsense.qcow2 /backup/pfsense-backup.qcow2
```

10. Vérifications post-installation

▶ 10.1 Vérification de la connectivité

Depuis la console pfSense (option 7 - Ping host), tester la connectivité WAN :

- Ping vers 8.8.8.8 pour vérifier l'accès internet
- Ping vers un nom de domaine pour vérifier la résolution DNS

▶ 10.2 Vérification des services sur Debian

```
$ virsh list --all
$ virsh dominfo pfsense
$ systemctl status libvirtd
```

▶ 10.3 Logs de la VM

```
$ virsh console pfsense
$ tail -f /var/log/libvirt/qemu/pfsense.log
```

▶ 10.4 Vérification réseau

```
$ brctl show
$ ip link show
$ virsh net-list --all
```

11. Bonnes pratiques de sécurisation

▶ 11.1 pfSense – Actions immédiates

- Changer le mot de passe admin par défaut (System > User Manager)
- Activer HTTPS uniquement pour l'interface web (System > Advanced)
- Désactiver l'accès WebGUI depuis le WAN (Firewall > Rules > WAN)
- Activer les mises à jour automatiques (System > Update)
- Configurer les alertes email (System > Advanced > Notifications)

▶ 11.2 Serveur Debian hôte

- Restreindre l'accès SSH au serveur KVM

```
$ nano /etc/ssh/sshd_config
# Modifier ou ajouter ces lignes
PermitRootLogin no
PasswordAuthentication no
AllowUsers votre_utilisateur
$ systemctl restart sshd
```

- Installer et configurer fail2ban sur le serveur Debian

```
$ apt install -y fail2ban
$ systemctl enable --now fail2ban
```

12. Mise à jour de pfSense

Les mises à jour se gèrent depuis l'interface web de pfSense.

▶ 12.1 Via l'interface web

- Se connecter à https://192.168.2.1
- Aller dans System > Update
- Cliquer sur Check for Updates
- Si une mise à jour est disponible, cliquer sur Confirm Upgrade

> ⚠ **Note :** *Toujours créer un snapshot de la VM avant d'appliquer une mise à jour majeure.*

▶ 12.2 Via la console (CLI pfSense)

Depuis la console pfSense (option 8 - Shell), il est possible de lancer une mise à jour en ligne de commande :

```
$ pfSense-upgrade -d
```

13. Conclusion

pfSense est maintenant installé et opérationnel en tant que machine virtuelle sur votre serveur Debian. Vous disposez d'un pare-feu/routeur complet avec les fonctionnalités suivantes disponibles depuis l'interface web :

- Pare-feu stateful avec règles avancées
- NAT et routage
- VPN (OpenVPN, IPsec, WireGuard)
- Proxy et filtrage de contenu (Squid, pfBlockerNG)
- Monitoring réseau (Grafana, ntopng)
- Haute disponibilité (CARP/VRRP)

> ℹ **Info :** Documentation complète disponible sur https://docs.netgate.com/pfsense/en/latest/

Procédure rédigée pour pfSense CE 2.7.x sur Debian 11/12 – 2025