INSTALLATION ET CONFIGURATION

pfSENSE

Pare-feu et routeur pour l'infrastructure virtualisée Proxmox

BTS SIO – Option SISR

Sasiraj GUNARATNARAJAH

Année 2025 – 2026

Document 2/7 – Projet Infrastructure Proxmox

1. Présentation

pfSense est une distribution firewall open source basée sur FreeBSD, développée et maintenue par Netgate. Elle offre des fonctionnalités de pare-feu, de routage, de NAT, de VPN et bien d'autres services réseau, le tout gérable via une interface web intuitive.

Dans le cadre de notre infrastructure virtualisée sur Proxmox, pfSense joue le rôle central de passerelle réseau. Il interconnecte les différents segments réseau (WAN, LAN-SRV, LAN-PDT) et contrôle l'ensemble des communications entre ces zones grâce à ses règles de filtrage.

Pourquoi pfSense ?

- Gratuit et open source, adapté à un contexte pédagogique comme professionnel
- Interface web complète pour la configuration et la supervision
- Support multi-interfaces, idéal pour la segmentation réseau
- Fonctionnalités avancées : VPN (OpenVPN, IPsec), DHCP, DNS relay, proxy, haute disponibilité
- Largement utilisé en entreprise, reconnu pour sa stabilité et sa sécurité

Rôle dans l'infrastructure

pfSense est le point névralgique de la sécurité réseau. Il assure les fonctions suivantes :

- Routage inter-VLAN entre les segments WAN, LAN-SRV et LAN-PDT
- Filtrage du trafic selon le principe du moindre privilège
- Translation d'adresses (NAT) pour l'accès Internet des réseaux internes
- Services DHCP et DNS relay pour les postes clients (configurés ultérieurement)

2. Prérequis

Ressources de la machine virtuelle

Paramètre	Valeur
VM ID	102
Nom	FW-site1
Système d'exploitation	pfSense 2.7.2 (basé sur FreeBSD)
CPU	2 vCPU
Mémoire vive	2048 Mo (2 Go)
Disque	20 Go (SATA)
Interfaces réseau	3 cartes Intel E1000 (net0: vmbr0, net1: vmbr1, net2: vmbr2)

Bridges Proxmox

Avant de créer la VM pfSense, les bridges virtuels suivants doivent être créés dans Proxmox (noeud → System → Network) :

Bridge	Zone réseau	Configuration
vmbr0	WAN	Lié à la carte réseau physique – accès Internet
vmbr1	LAN-SRV	Bridge interne sans port physique – réseau des serveurs
vmbr2	LAN-PDT	Bridge interne sans port physique – réseau des postes de travail

> *Les bridges vmbr1 et vmbr2 sont créés sans adresse IP et sans port physique. Ce sont de simples commutateurs virtuels. C'est pfSense qui portera les adresses IP de passerelle sur ses interfaces connectées à ces bridges.*

3. Création de la machine virtuelle

La création de la VM pfSense s'effectue depuis l'interface web de Proxmox (Create VM). Voici les étapes de configuration :

1. General : nommer la VM « FW-site1 » avec l'ID 102
2. OS : sélectionner l'ISO pfSense préalablement téléchargée, type « Other »
3. System : laisser les paramètres par défaut
4. Disks : Bus SATA, taille 20 Go
5. CPU : 2 cores
6. Memory : 2048 Mo
7. Network : Bridge vmbr0, modèle Intel E1000

Après la création, ajouter deux cartes réseau supplémentaires dans Hardware → Add → Network Device :

- net1 : Bridge vmbr1 (LAN-SRV), modèle Intel E1000
- net2 : Bridge vmbr2 (LAN-PDT), modèle Intel E1000

> *Insérer ici une capture d'écran de la configuration Hardware de la VM dans Proxmox montrant les 3 cartes réseau.*

4. Installation de pfSense

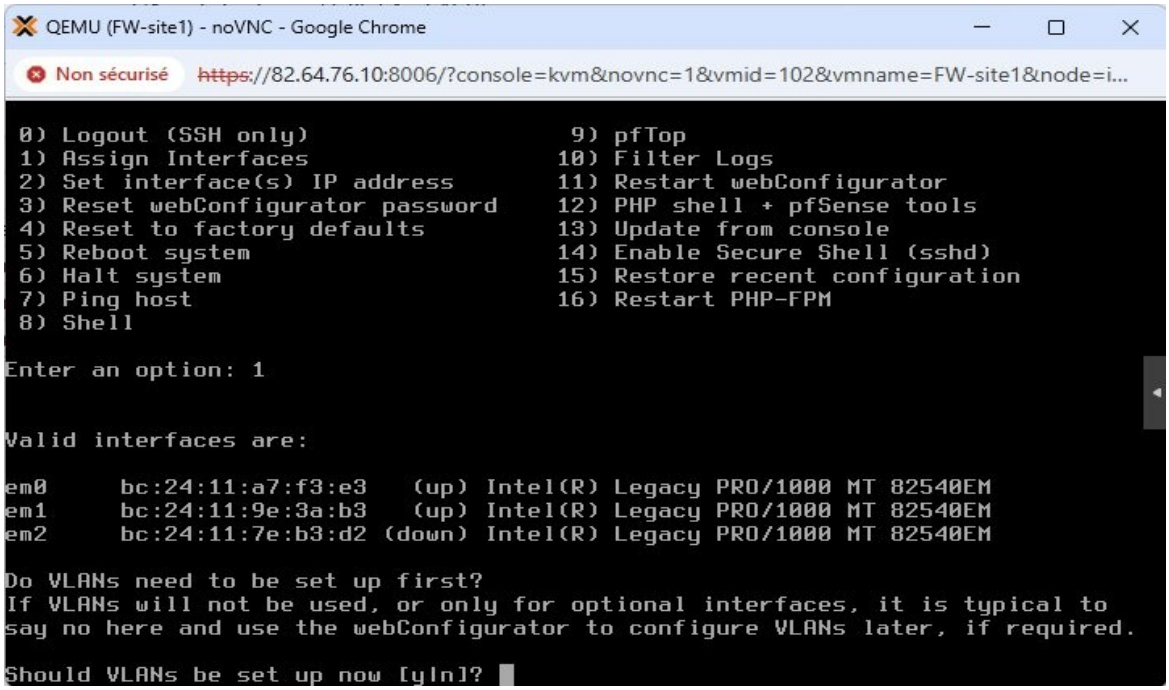
Au démarrage de la VM, pfSense boot sur l'ISO. L'installation se déroule en quelques étapes simples :

8. Accepter le contrat de licence (Copyright and distribution notice)
9. Sélectionner « Install » pour lancer l'installation
10. Choisir la disposition clavier souhaitée (French pour AZERTY)
11. Sélectionner le mode de partitionnement Auto (UFS) pour une configuration simple
12. Confirmer le disque cible et valider l'installation
13. Une fois terminé, sélectionner « Reboot » pour redémarrer

Après le redémarrage, pfSense affiche la console de configuration avec la détection des interfaces réseau.

5. Assignation des interfaces réseau

Après l'installation, pfSense propose d'assigner les interfaces réseau détectées. Trois interfaces Intel E1000 sont visibles, correspondant aux trois bridges Proxmox configurés précédemment.



La console affiche les trois interfaces détectées (em0, em1, em2). L'assignation est la suivante :

Interface pfSense	Carte réseau	Bridge Proxmox	Zone réseau
WAN	em0 (vtnet0)	vmbr0	Accès Internet
LAN	em1 (vtnet1)	vmbr1	LAN-SRV (serveurs)
OPT1	em2 (vtnet2)	vmbr2	LAN-PDT (postes)

À la question « Should VLANs be set up now? », répondre « n ». Les VLANs ne sont pas nécessaires dans cette architecture car chaque segment réseau dispose de son propre bridge Proxmox.

6. Configuration des adresses IP

Une fois les interfaces assignées, l'étape suivante consiste à configurer les adresses IP de chaque interface. Cette opération s'effectue depuis la console via l'option 2 « Set interface(s) IP address ».

6.1 – Interface WAN (em0)

L'interface WAN est connectée au réseau domestique via le bridge vmbr0. Elle reçoit une adresse IP statique sur le même sous-réseau que la box Internet :

Paramètre	Valeur
Adresse IPv4	192.168.1.100
Masque	/24 (255.255.255.0)
Passerelle	192.168.1.254 (box Internet)
IPv6	Non configuré
DHCP	Désactivé – adresse statique

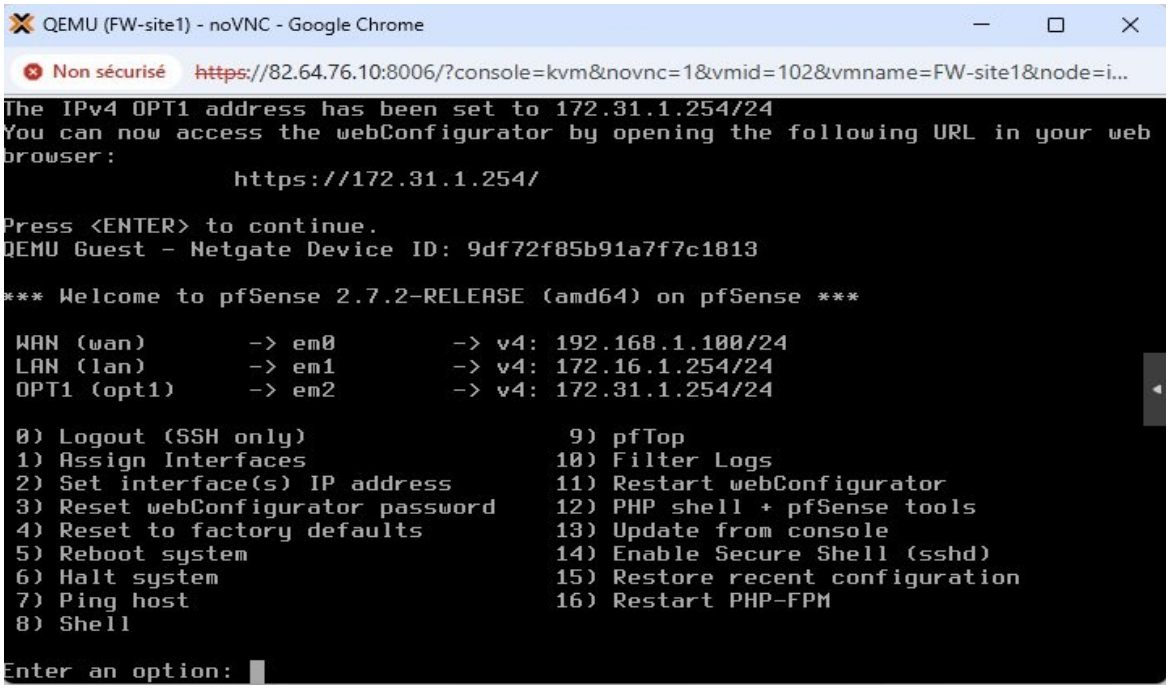
6.2 – Interface LAN (em1) – Réseau serveurs

Paramètre	Valeur
Adresse IPv4	172.16.1.254
Masque	/24 (255.255.255.0)
Passerelle	Aucune (interface locale)
DHCP	Désactivé – les serveurs utilisent des IP fixes

6.3 – Interface OPT1 (em2) – Réseau postes de travail

Paramètre	Valeur
Adresse IPv4	172.31.1.254
Masque	/24 (255.255.255.0)
Passerelle	Aucune (interface locale)
DHCP	Désactivé (sera configuré ultérieurement si nécessaire)

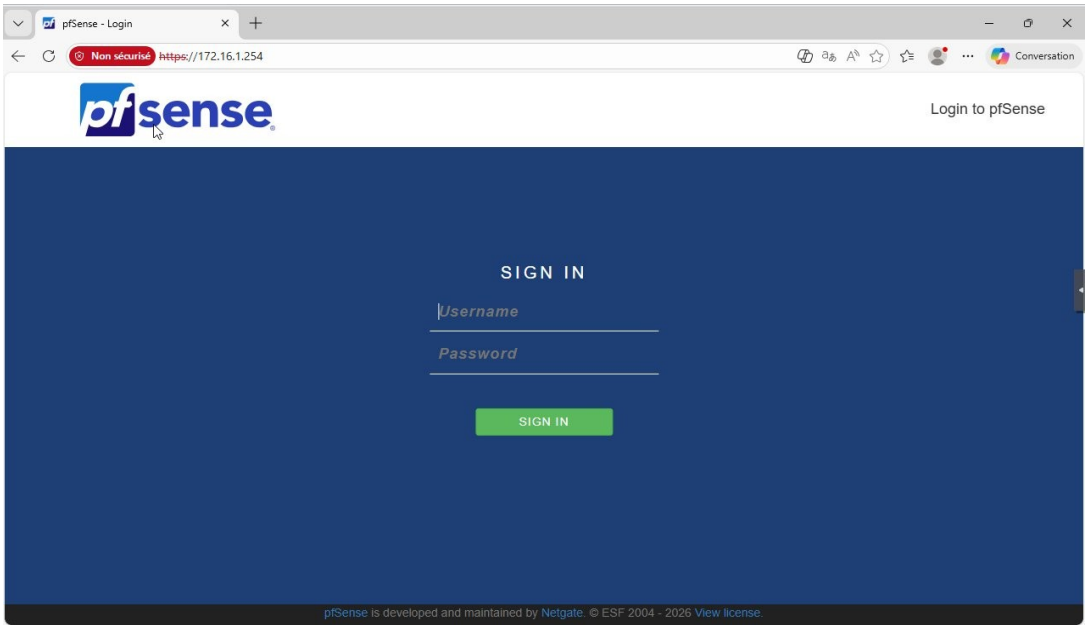
Après la configuration des trois interfaces, le menu console de pfSense affiche le récapitulatif des adresses IP attribuées :



Les trois interfaces sont correctement configurées avec leurs adresses IP respectives. pfSense est désormais opérationnel et joignable depuis le réseau LAN-SRV.

7. Configuration initiale via l'interface web

L'interface web de pfSense est accessible depuis le serveur Windows Server (SRV-AD) situé sur le réseau LAN-SRV, en accédant à l'adresse https://172.16.1.254. L'administration du pare-feu s'effectue exclusivement depuis le réseau serveurs, ce qui est conforme aux bonnes pratiques de sécurité : on n'administre jamais un firewall depuis un réseau non sécurisé.



La connexion s'effectue avec les identifiants par défaut (admin / pfsense). Un assistant de configuration initiale (wizard) se lance et permet de définir les paramètres généraux :

Paramètre	Valeur
Hostname	FW-site1
Domain	infrasasi.local
DNS primaire	8.8.8.8 (Google DNS)
DNS secondaire	1.1.1.1 (Cloudflare DNS)
Fuseau horaire	Europe/Paris
Mot de passe admin	Modifié (mot de passe personnalisé)

> *Les DNS publics (8.8.8.8 et 1.1.1.1) sont configurés temporairement. Une fois le serveur Active Directory opérationnel, l'adresse 172.16.1.10 sera ajoutée en DNS principal pour la résolution des noms du domaine interne.*

8. Activation de l’interface OPT1 (LAN-PDT)

Par défaut, l’interface OPT1 est désactivée dans pfSense. Il faut l’activer et la renommer pour qu’elle soit fonctionnelle. Cette opération s’effectue depuis l’interface web : Interfaces → OPT1.

Les paramètres suivants sont appliqués :

- Enable Interface : coché
- Description : LAN_PDT
- IPv4 Configuration Type : Static IPv4
- IPv4 Address : 172.31.1.254 / 24

Après avoir enregistré (Save), cliquer sur Apply Changes pour activer les modifications.

> *Insérer ici une capture d’écran de la page de configuration de l’interface OPT1.*

9. Règles de pare-feu

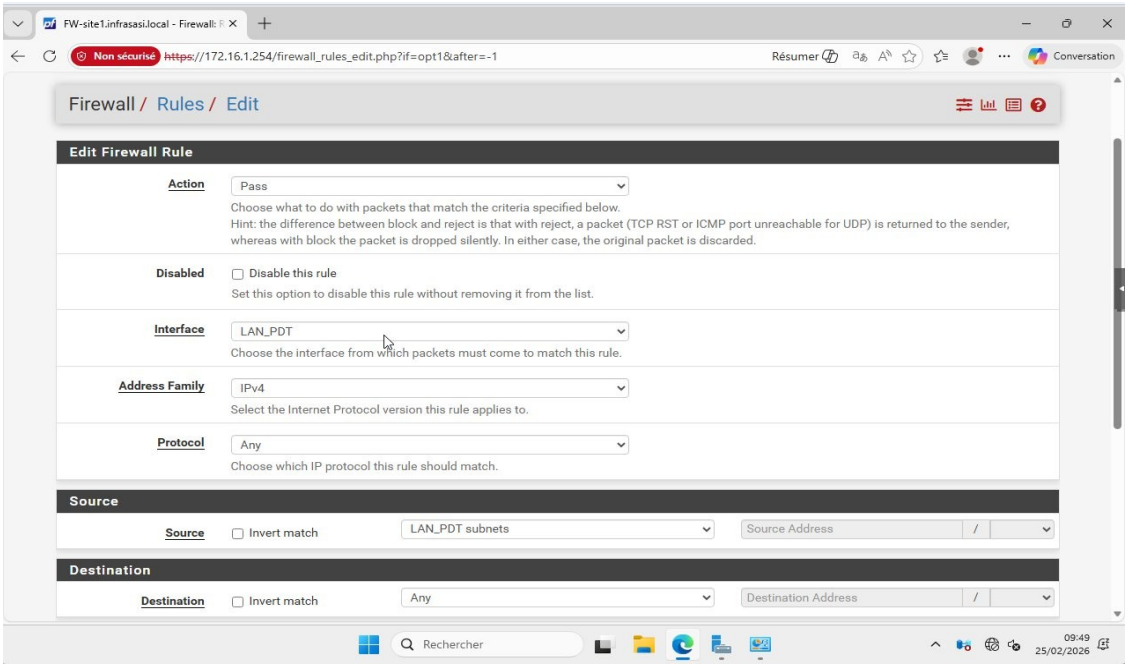
pfSense applique par défaut une politique de blocage : tout le trafic est refusé sauf si une règle l'autorise explicitement. L'interface LAN dispose d'une règle « pass any » par défaut, mais l'interface OPT1 (LAN_PDT) ne possède aucune règle. Il faut donc en créer une pour permettre aux postes de travail de communiquer.

Règle LAN-SRV (LAN)

L'interface LAN (réseau serveurs) dispose déjà d'une règle par défaut autorisant tout le trafic sortant. Cette règle permet aux serveurs d'accéder à Internet et de communiquer entre eux sans restriction initiale. Elle sera affinée ultérieurement selon la matrice de flux définie dans la documentation d'infrastructure.

Règle LAN-PDT (OPT1)

Une règle est créée pour autoriser le trafic depuis le réseau des postes de travail. La configuration est accessible depuis Firewall → Rules → onglet LAN_PDT :



Paramètre	Valeur
Action	Pass
Interface	LAN_PDT
Address Family	IPv4
Protocole	Any
Source	LAN_PDT subnets
Destination	Any

> *Cette règle permissive est temporaire et sera remplacée par des règles plus restrictives une fois tous les services déployés, conformément à la matrice de flux définie dans le document d'infrastructure.*

10. Récapitulatif de la configuration

Interface	Adresse IP	Sous-réseau	Rôle
WAN (em0)	192.168.1.100	192.168.1.0/24	Accès Internet via la box
LAN (em1)	172.16.1.254	172.16.1.0/24	Réseau serveurs (LAN-SRV)
OPT1 (em2)	172.31.1.254	172.31.1.0/24	Réseau postes (LAN-PDT)

11. Conclusion

pfSense est désormais installé et configuré comme passerelle principale de l'infrastructure. Les trois segments réseau (WAN, LAN-SRV, LAN-PDT) sont opérationnels et les règles de filtrage de base sont en place.

L'administration du pare-feu s'effectue exclusivement depuis le réseau serveurs (LAN-SRV) via l'interface web sécurisée en HTTPS, ce qui respecte les bonnes pratiques de sécurité.

La configuration sera complétée au fur et à mesure du déploiement des services :

- Ajout du serveur DNS interne (172.16.1.10) une fois Active Directory configuré
- Configuration du service DHCP pour le réseau LAN-PDT si nécessaire
- Affinement des règles de filtrage selon la matrice de flux
- Mise en place éventuelle d'un VPN site-à-site

Le prochain document détaillera le déploiement de Windows Server 2022 avec Active Directory et DNS sur le réseau LAN-SRV.