Mise en place d’un routage et firewall avec pfSense Isolation complète du laboratoire virtualisé

Années : 2025-2026

BTS SIO

Situation professionnelle numéro 2
Mise en place d’un routeur/firewall virtualisé

et isolation du réseau du homelab

Description :

Le routage et la sécurité réseau font partie intégrante des systèmes d’information modernes. Ils répondent à des besoins d’isolation, de protection contre les menaces externes et de gestion fine des flux. Dans le cadre de mon homelab sous Proxmox VE 9, j’ai souhaité virtualiser un routeur/firewall performant afin d’isoler complètement mon laboratoire du réseau domestique tout en conservant un accès Internet fluide et sécurisé.

Mots-clés :

pfSense: Un logiciel qui transforme un ordinateur en pare-feu/routeur très complet pour sécuriser et gérer un réseau.
Firewall: Un système qui contrôle ce qui peut entrer ou sortir d’un réseau, pour le protéger.
Routage: Le fait de faire circuler les données vers la bonne destination dans un réseau.
NAT: Un mécanisme qui permet à plusieurs appareils d’un réseau d’utiliser une seule adresse internet publique.
DHCP serveur: Un service qui donne automatiquement une adresse IP aux appareils quand ils se connectent au réseau.
DNS Resolver: Un service qui transforme les noms de sites (ex : google.com) en adresses IP que les ordinateurs comprennent.
Isolation réseau: Séparer différents réseaux pour éviter qu’ils se mélangent, améliorer la sécurité ou organiser le trafic.
Bridge réseau: Un “pont” qui relie deux réseaux pour qu’ils puissent communiquer comme s’ils étaient un seul.
Proxmox: Un logiciel gratuit qui sert à gérer facilement des machines virtuelles et des conteneurs depuis une interface web.
VM: Un “ordinateur virtuel” qui tourne à l’intérieur d’une machine physique.

Plan de la situation

Le cahier des charges

L’expression des besoins

Dans mon homelab, toutes les VMs étaient jusqu’à présent directement connectées au réseau domestique (192.168.1.0/24).
Ce fonctionnement présente plusieurs inconvénients :
– Exposition directe des VMs à Internet
– Risque de conflit DHCP avec la box
– Manque de réalisme par rapport à une architecture d’entreprise

Je souhaite donc mettre en place un routeur/firewall virtualisé qui :
– Isole totalement le laboratoire dans un sous-réseau dédié (192.168.10.0/24)
– Fournisse un DHCP serveur interne
– Assure le NAT sortant et la résolution DNS
– Permette la mise en place future de règles fines et de VPN

La description de l’existant

Hyperviseur : Proxmox VE 9.0-1 installé et opérationnel
Réseau actuel dans Proxmox :
– Un seul bridge vmbr0 connecté à la carte physique (réseau domestique 192.168.1.0/24)
– Toutes les VMs (Windows 11 Client, Windows Server 2025, etc.) sont attachées à vmbr0
– Adresse IP de l’hôte Proxmox : 192.168.1.250/24

Les offres du marché :

Actuellement, plusieurs solutions de routeurs/firewalls open source ou gratuits sont disponibles en novembre 2025 :

	pfSense CE 2.8.1	**OPNsense 25.7**	**VyOS 1.5**	**Untangle NG Firewall**	**MikroTik RouterOS**
Type	FreeBSD	FreeBSD	Linux	Linux	Linux
Interface web	Très complète	Très complète	CLI + web	Web complète	WinBox + web
NAT / Firewall	Excellent	Excellent	Très bon	Bon	Excellent
DHCP serveur	Oui	Oui	Oui	Oui	Oui
DNS Resolver	Oui	Oui	Non natif	Oui	Oui
Support VLAN	Oui	Oui	Oui	Oui	Oui

L’analyse des choix

OPNsense 25.7 : Fork moderne de pfSense, interface plus « moderne », mises à jour plus fréquentes. Cependant la communauté reste légèrement moins importante et certains plugins (ex. Suricata) sont parfois moins stables.

VyOS 1.5 : Solution orientée CLI, très puissante, mais demande une excellente maîtrise des commandes. Pas adaptée à un étudiant qui veut une interface graphique claire.

Untangle NG Firewall : Très belle interface, mais version gratuite très limitée (publicités, fonctions bloquées).

MikroTik RouterOS : Excellent matériel, mais la version virtualisée est limitée et l’interface WinBox est déroutante au début.

pfSense Community Edition 2.8.1 : Solution historique, maturité exceptionnelle, documentation abondante, plugins très stables, communauté francophone énorme. Parfait pour un projet BTS SIO SISR.

Le choix : pfSense Community Edition 2.8.1

Nous avons opté pour pfSense car c'est la référence open source en matière de firewall/routage. La version 2.8.1 (septembre 2025) apporte le support complet de FreeBSD 14, WireGuard natif, et une interface toujours aussi claire. Aucun autre produit n'offre un tel équilibre entre puissance, simplicité et gratuité.

Les nouveaux risques du routeur/firewall virtualisé

– Point unique de panne: si la VM pfSense tombe tout le labo est isolé d'Internet
– Mauvaise règle firewall: blocage total du trafic sortant
– Exposition de l'interface web pfSense (ports 80/443) si mal protégée
– Attaque par déni de service sur le WAN si NAT mal configuré

Préparation de la mise en place de pfSense :

Le passage à un réseau interne dédié est une étape critique.

Nous devons créer un nouveau bridge dans Proxmox, installer pfSense avec deux cartes réseau, puis migrer progressivement les VMs.

Etape 1 : Création du bridge LAN interne dans Proxmox
Etape 2 : Téléchargement ISO pfSense 2.8.1-CE
Etape 3 : Création de la VM pfSense avec 2 interfaces réseau
Etape 4 : Configuration initiale et tests de connectivité

Mise en œuvre

Préparation du réseau dans Proxmox

Connexion à l'interface web Proxmox → Node → Network

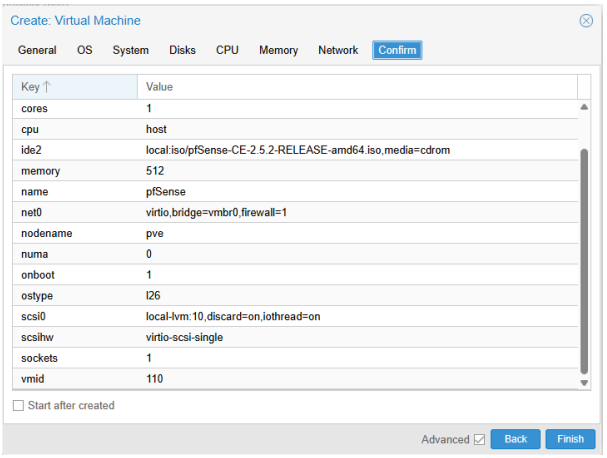
Création d'un nouveau Linux Bridge :

Nom : vmbr1
IPv4/CIDR : (laisser vide – pas d'IP sur ce bridge)
Bridge ports : aucun (réseau purement virtuel)
VLAN : décoché

Résultat :
– vmbr0 reste connecté à la carte physique (WAN)
– vmbr1 sera le LAN interne 192.168.10.0/24

Création et configuration de la VM pfSense

Création de la machine virtuelle (ID 110) :
– OS : No media (on ajoutera l'ISO après)
– CPU : 2 cœurs
– RAM : 2 Go
– Disque : 32 Go (ZFS thin)
– Network :
net0 → VirtIO → bridge vmbr0 (WAN)
net1 → VirtIO → bridge vmbr1 (LAN)
– Ajout de l'ISO pfSense-CE-2.8.1-RELEASE-amd64.iso



Démarrage de la VM → installation classique :
– Keymap : French
– Partitionnement : ZFS
– Redémarrage

À la console pfSense :

Assignation des interfaces :

1. vtnet0 → WAN
2. vtnet1 → LAN

Configuration des interfaces WAN et LAN

```
You can now access the webConfigurator by opening the following URL in your web
browser:
                https://192.168.10.254/

Press <ENTER> to continue.
KVM Guest - Netgate Device ID: 742cb3cfe38bc6489ed6

*** Welcome to pfSense 2.5.2-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> vtnet0     -> v4/DHCP4: 192.168.1.37/24
                                  v6/DHCP6: 2a01:e0a:5c8:4300:be24:11ff:fea1:af5
f/64
 LAN (lan)       -> vtnet1     -> v4: 192.168.10.254/24

 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:
```

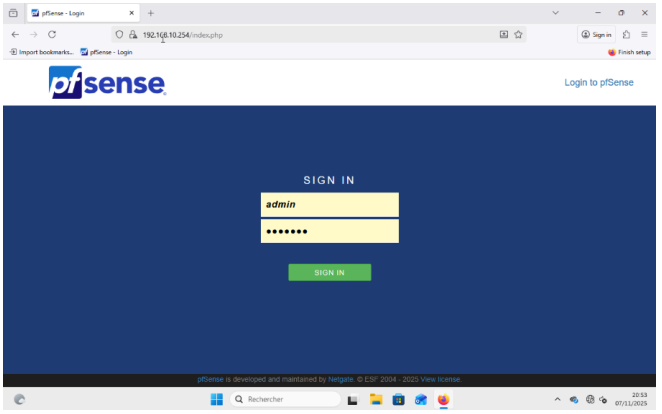
Accès web temporaire depuis le réseau domestique (WAN) : https://192.168.1.254/

Connexion admin / pfsense → changement mot de passe

Configuration WAN :
– IPv4 : DHCP (récupère IP de la box)
– IPv6 : désactivé

Configuration LAN :
– IPv4 : Static
– Adresse : 192.168.10.254/24
– DHCP Server → Enable
Plage : 192.168.10.10 – 192.168.10.100

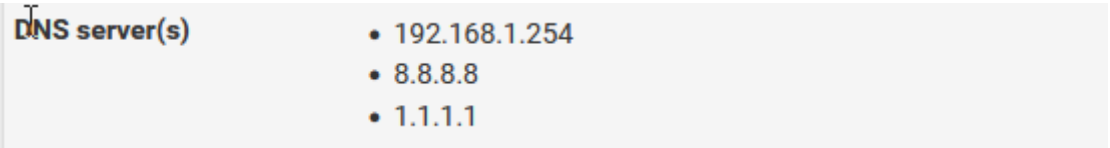
DNS : 192.168.10.254



Mise en place du DHCP serveur et du DNS Resolver

Désactivation du DHCP sur le bridge vmbr1 dans Proxmox

Test depuis une VM temporaire attachée à vmbr1 :
– Obtention IP 192.168.10.x
– Résolution DNS (8.8.8.8) → OK
– Accès Internet → OK



Migration des VMs Windows vers le réseau interne et tests

Migration des cartes réseau :
– VM Windows 11 Client (ID 100) : net0 → vmbr1

– VM Windows Server 2025 (ID 101) : net0 → vmbr1

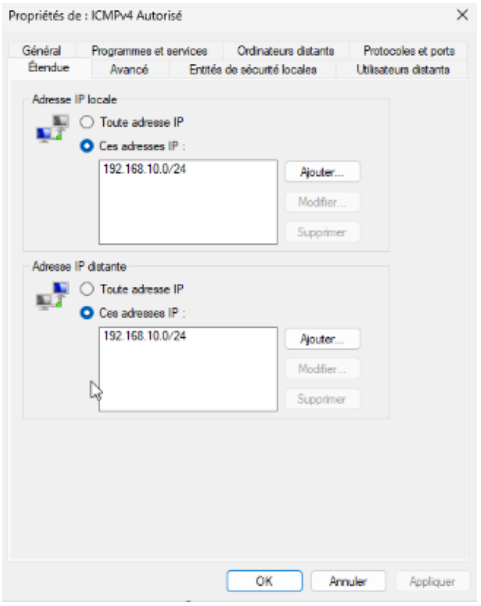
Sur le client Windows 11 :
ipconfig /release
ipconfig /renew
→ Nouvelle IP 192.168.10.10
ping 192.168.10.254 → OK
ping google.com → OK

```
Suffixe DNS propre à la connexion. . . :
Adresse IPv6 de liaison locale. . . . .: fe80::a067:ff97:904b:7b6%2
Adresse IPv4. . . . . . . . . . . . . .: 192.168.10.101
Masque de sous-réseau. . . . . . . . . : 255.255.255.0
Passerelle par défaut. . . . . . . . . : 192.168.10.254
```

```
Suffixe DNS propre à la connexion. . . : home.arpa
Adresse IPv6 de liaison locale. . . . .: fe80::73d1:bf8a:aa4a:b7bf%14
Adresse IPv4. . . . . . . . . . . . . .: 192.168.10.10
Masque de sous-réseau. . . . . . . . . : 255.255.255.0
Passerelle par défaut. . . . . . . . . : 192.168.10.254
```

Sur le serveur :
IP statique 192.168.10.101/24, passerelle 192.168.10.254/24

Règles firewall Windows mises à jour pour autoriser uniquement le réseau 192.168.10.0/24



Bilan

La mise en place de pfSense a permis :
– L'isolation totale du homelab du réseau domestique
– La distribution automatique des adresses et de la résolution DNS
– Un point d'entrée unique pour appliquer des règles de sécurité futures

Le laboratoire reproduit désormais fidèlement l'architecture d'une PME : un firewall/routeur dédié en amont des serveurs et postes.

Cette situation valide parfaitement les compétences SISR en administration réseau, routage et sécurité périmétrique.

Prochaines évolutions possibles :
– Mise en place de VLANs (Management / DMZ / LAN)
– OpenVPN