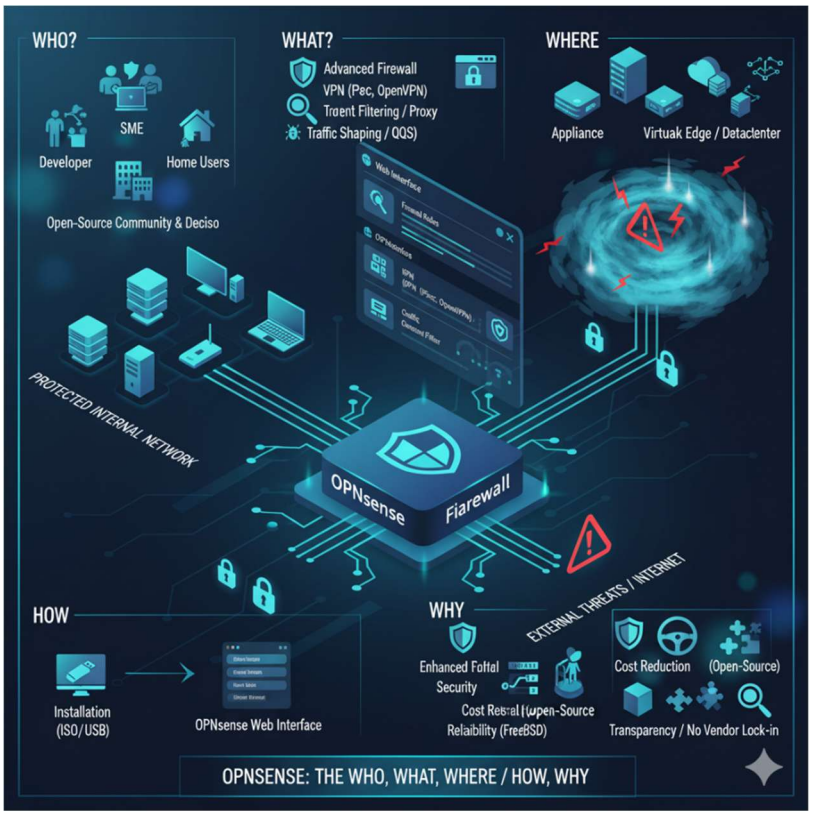
# Procédure

Mise en place d’une infrastructure interne avec **ESXi**, WindowsServer, Windows 11 et **OPNsense**



# Table des matières

# INTRODUCTION

OPNsense est un pare-feu de nouvelle génération (NGFW), un routeur, et une solution de gestion unifiée des menaces.
C'est un système d'exploitation complet (basé sur FreeBSD) qui transforme un matériel informatique standard (PC, serveur, appliance dédiée) en une passerelle de sécurité réseau puissante.
Il est conçu pour être un pare-feu de nouvelle génération, un routeur et une solution de gestion unifiée des menaces (UTM), rivalisant avec des solutions commerciales coûteuses. OPNsense permet aux organisations de toutes tailles de sécuriser leurs réseaux, de contrôler le trafic et de garantir la disponibilité des services avec une grande flexibilité et une interface utilisateur intuitive.
Il intègre également des fonctionnalités telles que l'authentification multi-facteurs, le support des VLANs, et une gestion centralisée des logs. Son système de mise à jour régulier assure une sécurité et des performances optimales, intégrant les dernières avancées en matière de protection contre les menaces.
OPNsense est administrable via une interface web moderne et réactive, facilitant la configuration et la surveillance des différentes politiques de sécurité du réseau.

Il offre des fonctionnalités telles que :

- Un pare-feu avancé avec des règles de filtrage d'état.
- Des capacités VPN (IPsec, OpenVPN, WireGuard).
- Un système de détection et de prévention d'intrusion (IDS/IPS).
- Un proxy web (avec mise en cache et filtrage de contenu).
- La gestion du trafic (QoS, shaping).
- Le support des VLANs, DHCP, DNS.
- L'authentification multi-facteurs.

Les raisons d'utiliser OPNsense sont multiples :

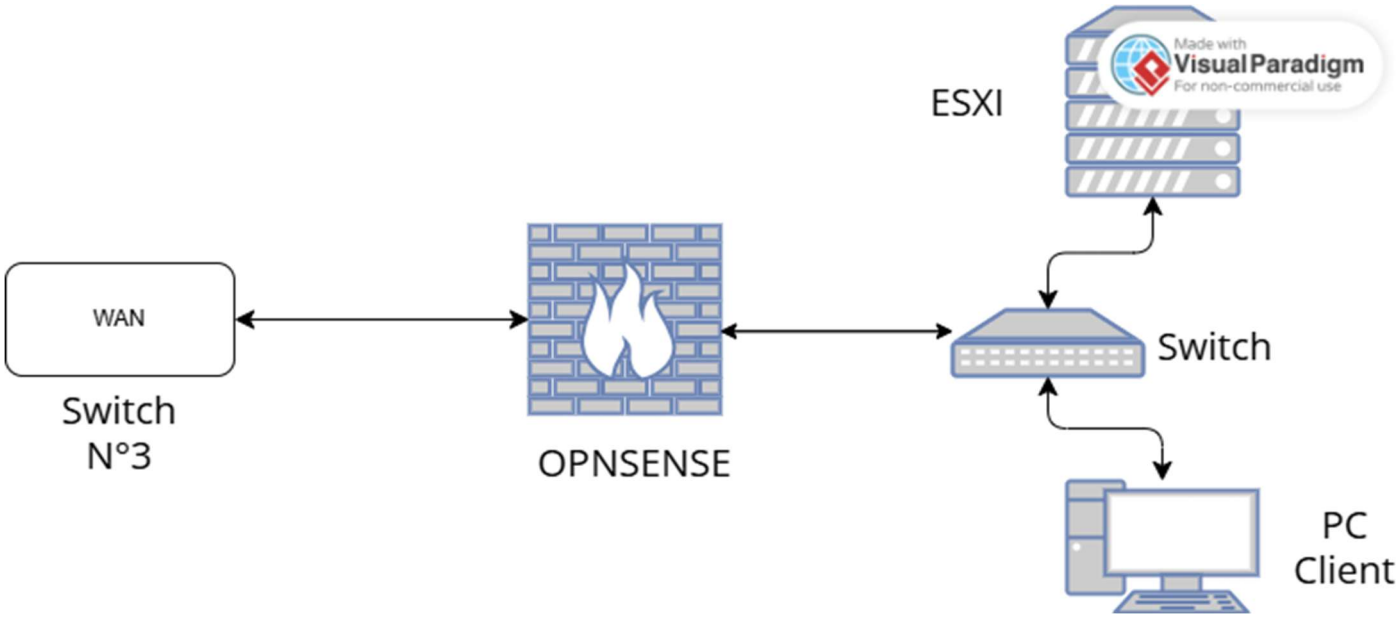
- **Sécurité Renforcée** : Protéger les réseaux contre les menaces externes, les intrusions, les logiciels malveillants et les accès non autorisés.
- **Contrôle du Trafic** : Gérer et prioriser le trafic réseau, limiter la bande passante, bloquer l'accès à certains sites ou applications.
- **Réduction des Coûts** : Fournir une alternative open-source performante et gratuite (ou avec un coût matériel minimal) aux solutions de pare-feu commerciales coûteuses.
- **Flexibilité et Personnalisation** : Sa nature open-source permet une grande adaptabilité et la possibilité d'ajouter des plugins et des fonctionnalités spécifiques.

- **Fiabilité** : Basé sur FreeBSD, un système d'exploitation réputé pour sa stabilité et sa sécurité.
- **Transparence** : L'open-source garantit qu'il n'y a pas de "portes dérobées" cachées et permet un audit par la communauté.
- **Indépendance Vis-à-Vis des Fournisseurs** : Éviter le verrouillage par un fournisseur (vendor lock-in).

## A. Matériel & Adressage IP

| Équipement | Rôle | Adresse IP / Masque |
|---|---|---|
| Switch | Distribution réseau | |
| ESXi | Hyperviseur | 192.168.40.100 /24 |
| OPNsense | Pare-feu / Routeur | LAN : 192.168.40.254 /24<br>WAN : 10.16.27.92 /24 |
| PC Client | Machine de test | DHCP via OPNsense (192.168.40.1 – 192.168.40.100) |

## B. Diagramme réseau



# C. Configuration des équipements

## 1. Préparation du matériel

1. Connexion du switch à l'hyperviseur ESXi, à OPNsense et au PC de test.
2. Vérifier que le serveur ESXi et le PC client sont correctement alimentés et câblés.
3. Connexion des deux cartes réseau de l'OPNsense (une pour le WAN, l'autre pour le LAN).

## 2. Installation et configuration d'OPNsense

1. Création d'une machine OPNsense avec une clé bootable réalisée via Rufus.
2. Pré-requis :
    - Disque : 10 Go minimum
    - RAM : 2 Go minimum
    - 2 cartes réseau (WAN et LAN)
3. Lancement de l'installation d'OPNsense en suivant le guide IT-Connect :
   Tutoriel OPNsense
4. Connexion à l'interface web via :
    - URL : https://192.168.1.1
    - Utilisateur : root / Mot de passe :
5. Modification de l'adresse IP de l'interface web :
    - Nouvelle adresse : https://192.168.40.254
6. Modification du mot de passe pour plus de sécurité :
    - Utilisateur : root / Mot de passe :
7. Vérification / configuration des interfaces :
    - WAN : 10.16.27.141 /24 (connecté au réseau externe)
    - LAN : 192.168.40.254 /24 (réseau interne)
8. Activation du DHCP sur le LAN :
    - Plage définie : 192.168.40.1 – 192.168.40.100
9. Configuration de la passerelle WAN :
    - Passerelle : 10.16.27.254
    - Le PC client a désormais un accès réseau.

## 3. Serveur ESXi

1. Réflexion sur l'ajout d'iDRAC pour la supervision des VM.
2. Sécurité ESXi :
    - Utilisateur : root / Mot de passe :
3. Passage de l'adresse IP du DHCP en IP statique.
4. Importation des ISO dans ESXi :
    - Création d'un sous-dossier ISO dans le stockage pour une meilleure organisation.

### 3.1 Debian

1. Installation de Debian puis configuration.
   Procédure IT-Connect
2. Création de deux profils :
    - Utilisateur admin : root
    - Utilisateur : GLPI
3. Mise à jour du système :
    - **apt update && apt upgrade** (sécurité du futur serveur GLPI).
4. Installation du serveur GLPI :
    - Installation de la base de données : MariaDB
    - Utilisateur BDD : glpi_adm /// MotDePasseRobuste
5. Installation de GLPI.
6. Nom du serveur web : GLPI.ESXI – IP : 192.168.40.80

### 3.2 Windows Server

1. Installation de Windows Server.
    - Administrateur /// MDPadmin44
    - Nom de domaine racine : esxi-srv.local
2. Installation de l'ADDS (Active Directory Domain Services).
3. Installation du contrôleur de domaine :
    - Mot de passe DSRM :
    - NetBIOS : ESXI-SRV
4. Connexion RDP sur le serveur.

### 4. PC Clients

- Installation d’un client virtuel W11 sur ESXI.
- Utilisateur : pc-client
- Intégration au domaine : esxi-srv.local

## D. Problèmes rencontrés

Après la fin de l’installation du réseau local, nous avons décidé de rejoindre le réseau sio_sflx (où est hébergé le serveur Zabbix).

Pour cela, nous avons désinstallé le rôle ADDS.

Lors de la fusion des deux réseaux (connexion du réseau local ESXi avec le réseau local sio_sflx), la communication n’a pas fonctionné.

Nous avons tenté :

- Des modifications de règles dans le pare-feu des OPNsense
- La création de routes passerelles pour joindre leur réseau en 10.16.27.121

Malgré ces tentatives, nous n’avons réussi qu’à ping leur serveur Internet en 192.168.20.1.

## CONCLUSION

En définitive, OPNsense se positionne comme une solution de sécurité réseau incontournable, démontrant qu'une protection de niveau professionnel n'est pas l'apanage des logiciels propriétaires coûteux. En combinant la puissance de FreeBSD avec une suite complète de fonctionnalités de pare-feu de nouvelle génération, de VPN et de gestion des menaces, OPNsense offre une alternative open-source performante, flexible et constamment mise à jour. Que ce soit pour sécuriser un réseau domestique, une petite entreprise ou une infrastructure de datacenter complexe, sa gestion intuitive via interface web et sa robustesse en font un choix stratégique pour tout administrateur soucieux de la sécurité, du contrôle et de l'optimisation de son infrastructure réseau. OPNsense incarne ainsi une approche moderne et accessible de la cybersécurité, garantissant tranquillité d'esprit et résilience face aux menaces numériques en constante évolution.