Procédure Déploiement Pare-feu pfSense

Sommaire

1. Cahier des charges – Expression des besoins

1.1 Descriptif de l'existant

Actuellement, les serveurs de l'entreprise (Web, hyperviseurs) et les postes clients sont connectés sur un même réseau local plat, directement exposé au routeur (box) du fournisseur d'accès. Il n'y a pas de segmentation réseau stricte ni de filtrage avancé des ports et protocoles, ce qui représente une faille de sécurité majeure.

1.2 Besoin(s)

- Déployer un pare-feu (Firewall) en tête de réseau pour contrôler le trafic entrant (WAN) et sortant (LAN).
- Assurer les fonctions de passerelle par défaut (Gateway), de routage et de serveur DHCP pour le réseau local.
- Disposer d'une interface d'administration graphique (WebGUI) pour gérer les règles de filtrage facilement.

1.3 Contrainte(s)

- **Coût :** Utiliser une solution logicielle Open Source sans licence payante.
- **Architecture :** La solution doit être virtualisée (hyperviseur VMware). Elle nécessitera la création et l'assignation de deux cartes réseau virtuelles distinctes pour séparer physiquement le trafic public du trafic privé.

2. Ressources

2.1 Ressources mises à disposition

- **Environnement de virtualisation :** Hyperviseur Proxmox ou VMWare permettant la création de commutateurs virtuels isolés (VMnet / LAN Segments).
- **Machine d'administration :** Une machine virtuelle cliente (Windows) connectée exclusivement sur le réseau local interne pour accéder à l'interface de gestion du pare-feu.

2.2 Ressources nécessaires

- **Logiciel :** Image ISO de la dernière version de pfSense (basée sur le système d'exploitation FreeBSD).
- **Matériel virtuel (pour pfSense) :** 1 vCPU, 1 Go de RAM, et 10 Go d'espace disque.

2.3 Gestion des ressources

La gestion des interfaces réseau est le point critique. La "Carte réseau 1" de la VM sera reliée au monde extérieur (Mode NAT ou Accès par pont) pour représenter le **WAN**. La "Carte réseau 2" sera reliée à un réseau virtuel isolé (Host-Only ou LAN Segment) pour représenter le **LAN**.

3. Analyse

3.1 Descriptifs des solutions

- **Appliance matérielle propriétaire (ex: Fortigate, Cisco ASA, Sophos) :** Solutions clés en main très performantes, avec un support technique inclus. Elles nécessitent l'achat d'un boîtier physique et d'abonnements annuels coûteux.
- **Pare-feu logiciel Open Source (ex: pfSense, OPNsense) :** Solutions gratuites de niveau entreprise s'installant sur n'importe quel matériel standard ou machine virtuelle. L'administration se fait via une interface Web très complète.

3.2 Comparaison des solutions

Critères	**Pare-feu propriétaire (ex: Fortinet)**	**Pare-feu Open Source (pfSense - Choisi)**
Coût d'acquisition	Élevé (Matériel + Licence)	**Totalement Gratuit**
Flexibilité matérielle	Limitée au boîtier acheté	**Totale (Virtualisable sur mesure)**
Système de base	OS Propriétaire fermé	**FreeBSD (Robuste et sécurisé)**
Interface d'administration	WebGUI propriétaire	**WebGUI intuitive et complète**

3.3 Choix d'une solution – Argumentation

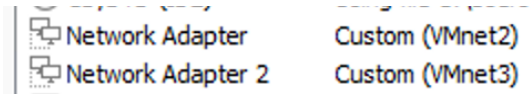
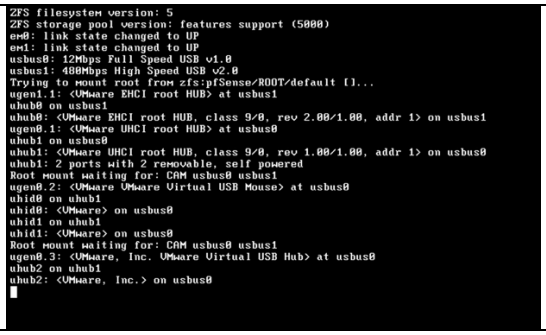
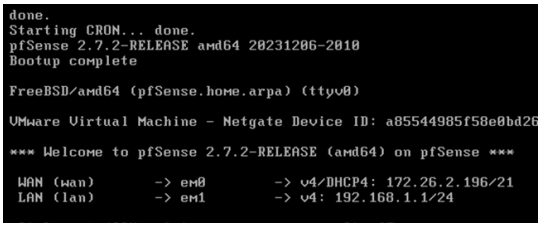
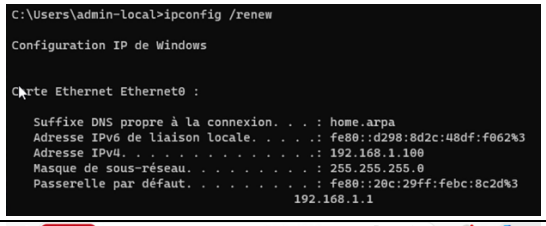
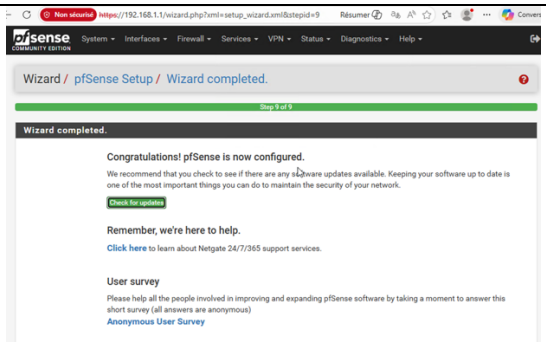
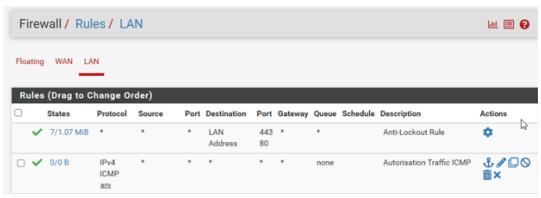
Le choix s'est porté sur **pfSense**. C'est une référence absolue dans le monde de l'open source pour la sécurité réseau. Sa capacité à être virtualisé sans perte de fonctionnalités nous permet de sécuriser notre infrastructure sans investir dans du matériel dédié, tout en offrant des performances dignes des solutions professionnelles payantes.

3.4 Étude de l'impact sur le SI existant

- **Architecture :** pfSense devient le point de passage obligatoire pour toutes les communications.
- **Sécurité :** Par défaut, pfSense bloque absolument tout le trafic entrant (WAN vers LAN). Il faudra créer des règles d'ouverture de ports (NAT / Port Forwarding) spécifiques si nous voulons rendre notre serveur Web interne accessible depuis l'extérieur.

4. Mise en place

4.1 Réalisation en suivant le phasage énoncé précédemment

Étape	Description	Images
1	**Préparation de la VM :** Création de la VM pfSense sous VMware. Ajout d'une 2ème carte réseau pour avoir une interface WAN (NAT) et une interface LAN (Réseau privé virtuel isolé).	 VMnet2 = WAN VMnet3 = LAN
2	**Installation de base :** Démarrage sur l'ISO pfSense, acceptation des conditions, formatage du disque (Auto (ZFS)) et redémarrage système.	
3	**Assignation des interfaces (CLI) :** Sur l'écran noir de pfSense, vérification de l'assignation automatique des cartes (em0 pour WAN, em1 pour LAN) et définition de l'adresse IP statique du LAN (ex: 192.168.1.1/24).	
4	**Test client :** Démarrage de la VM cliente Windows connectée sur le même réseau isolé que le LAN de pfSense. Vérification de l'obtention d'une IP dynamique via la commande ipconfig.	
5	**Configuration WebGUI :** Depuis le navigateur du client Windows, connexion à *https://192.168.1.1*. Connexion avec les identifiants par défaut (admin / pfsense) et finalisation via le "Setup Wizard".	
6	**Création d'une règle (Firewall) :** Dans le menu "Firewall > Rules > LAN", ajout d'une règle pour autoriser le trafic ICMP (Ping) ou restreindre un accès spécifique pour valider le filtrage.	

5. Bilan

5.1 Conclusion

Le déploiement du pare-feu pfSense est un succès. L'infrastructure est désormais segmentée : le réseau interne (LAN) est protégé des requêtes extérieures. La machine virtuelle pfSense assure parfaitement son rôle de serveur DHCP et de passerelle de sécurité. La gestion des flux réseaux est désormais centralisée et facilement modifiable depuis l'interface graphique.

5.2 Auto-critique / Auto-évaluation

- **Points forts :** L'installation de base est très rapide. La politique du "tout bloquer par défaut" sur l'interface WAN garantit une sécurité maximale dès la première minute de mise en production.
- **Points de vigilance :** La gestion des cartes réseau sous VMware demande beaucoup de rigueur. Si l'on inverse la carte WAN et la carte LAN lors de l'assignation, on expose l'interface d'administration sur le réseau public. De plus, il faut être très prudent lors de l'édition des règles LAN pour ne pas se bloquer soi-même l'accès à l'interface Web (Lock-out).

5.3 Compétence(s) SISR mobilisée(s)

- **Administrer et sécuriser les infrastructures :** Mise en œuvre d'un équipement de filtrage réseau (Firewall).
- **Gérer le patrimoine informatique :** Déploiement d'un service de cœur de réseau (Routage, DHCP).