Compte Rendu Détaillé du Projet : Déploiement et Configuration de pfSense avec Proxy Web

Date de rendu : 04/04/2025

Durée du projet :

**1. Contexte et Objectifs**

Objectif principal : Déployer une solution pare-feu open source pfSense pour sécuriser un réseau d’entreprise, incluant la configuration d’un proxy web et la mise en place de règles de filtrage avancées.

Livrables attendus :

- Pare-feu pfSense opérationnel avec interfaces WAN/LAN.

- Proxy web configuré pour le filtrage de contenu et la journalisation.

- Règles de trafic (NAT, filtrage par IP/port).

- Documentation technique (schémas réseau, procédures de sécurité).

Contraintes :

- Respect des politiques de sécurité de l’entreprise (blocage des sites malveillants, restriction des accès).

- Optimisation des performances du proxy (cache, SSL Inspection).

**2. Méthodologie et Organisation**

2.1. Outils Utilisés

- pfSense : Distribution firewall basée sur FreeBSD.

- Proxmox : Virtualisation du serveur pfSense.

- Squid : Proxy web pour le filtrage et le cache.

- Snort/Suricata : IDS/IPS pour la détection d’intrusions.

**3. Phases du Projet**

3.1. Phase 1 : Planification (2h)

Objectif : Définir l’architecture réseau et les besoins en sécurité.

Tâches réalisées :

- Schéma réseau :

- Interfaces : WAN (Internet), LAN (réseau interne), LANSERVEUR ( LAN WS22)

- Spécifications matérielles :

- Machine virtuelle allouée : 2 CPU, 4 Go RAM, 20 Go disque.

- Cartes réseau virtuelles : 2 (WAN, LAN, LANUSER).

3.2. Phase 2 : Installation de pfSense (3h)

Objectif : Installer et configurer les interfaces de base.

Tâches réalisées :

- Installation via ISO :

- Partitionnement UFS (pour la stabilité).

- Configuration des interfaces :

- WAN : DHCP (adresse publique).

- LAN : IP statique `192.168.1.1/24`.

- Accès à l’interface web :

- URL : `https://192.168.1.1` (certificat auto-signé).

- Authentification : Login `Axel`, mot de passe personnalisé.

3.3. Phase 3 : Configuration du Pare-feu (4h)

Objectif : Définir les règles de trafic et sécuriser le réseau.

Tâches réalisées :

- Règles WAN → LAN :

- Blocage par défaut, autorisation du trafic HTTP/HTTPS via proxy.

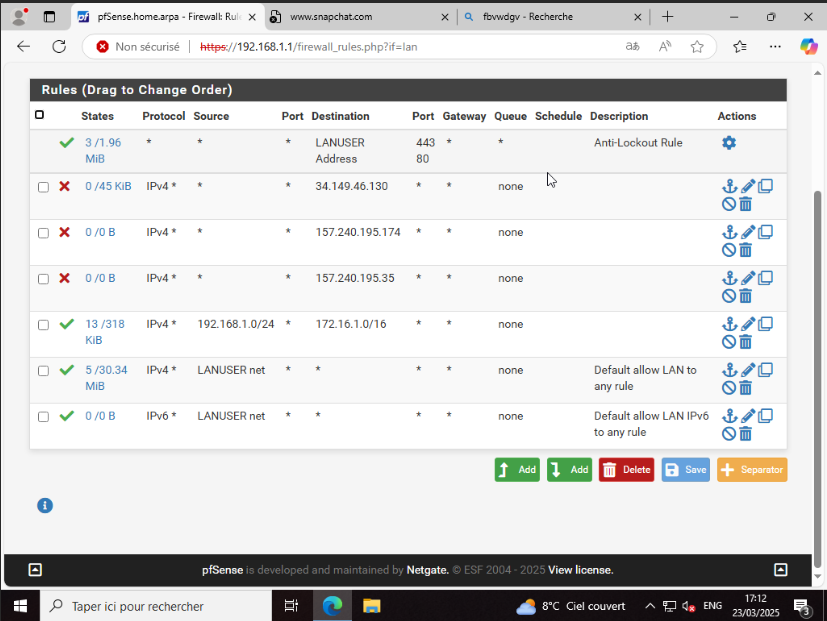
3.4. Phase 4 : Déploiement du Proxy Web (3h)

Objectif : Mettre en place un proxy filtrant et optimisant le trafic web.

Tâches réalisées :

- Configuration :

- Filtrage d’URL : Listes noires (ex: réseaux sociaux, sites malveillants).



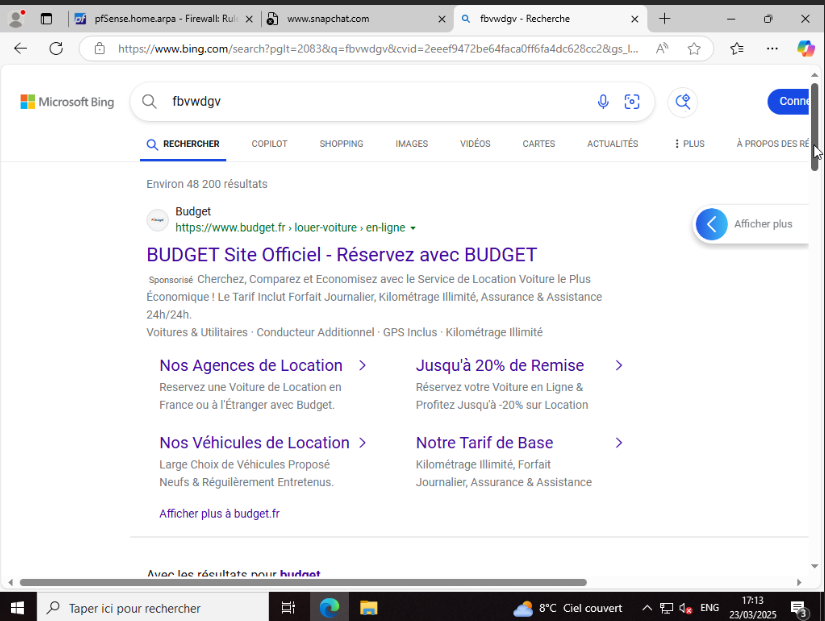
3.5. Phase 5 : Tests et Documentation (2h)

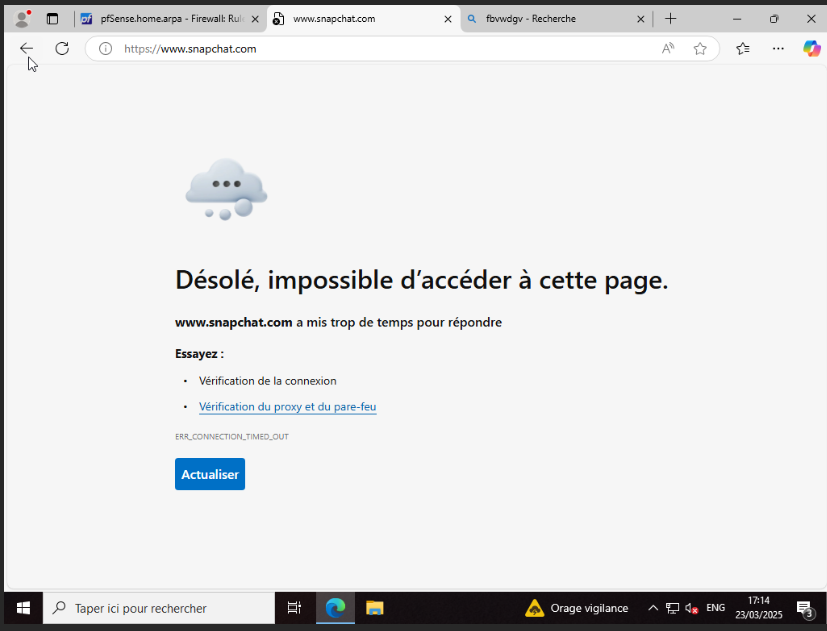
Objectif : Valider le fonctionnement et produire les guides.

Tâches réalisées :

- Tests de connectivité :

- Accès à Internet via proxy (vérification du filtrage). .





- Documentation :

- Guide utilisateur : Configuration du proxy sur les postes clients.

- Fiche technique : Adresses IP, règles de pare-feu, procédures de sauvegarde.

**4. Résultats et Livrables**

4.1. Documentation

- Schéma réseau : Visuel des interfaces et flux autorisés.

**5. Bilan et Améliorations Futures**

- Points forts : Solution open source évolutive, filtrage HTTPS efficace.

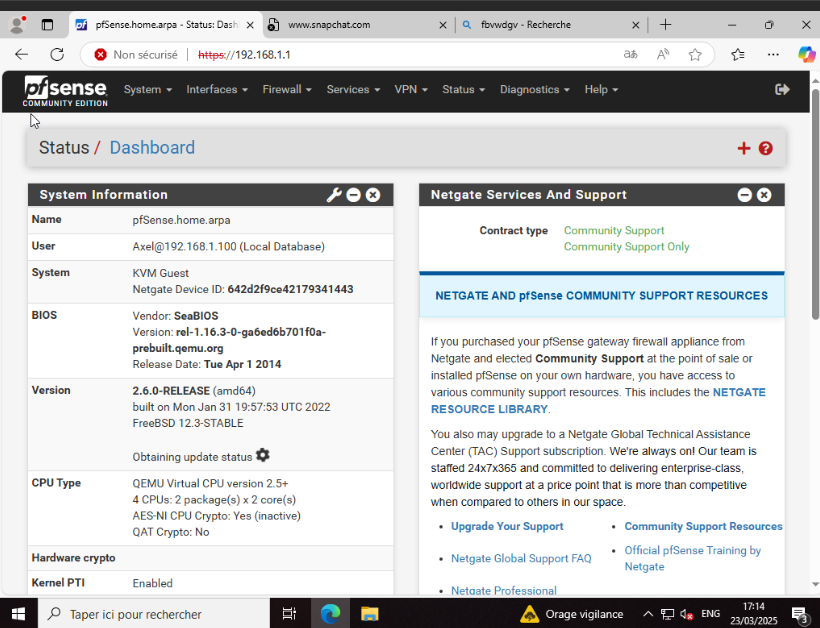
- Axes d’amélioration :

- Ajouter un cluster HA (High Availability) pour la redondance.

- Intégrer un load balancer (HAProxy) pour les services critiques.

**Annexes**

Annexe 1 : Capture d’écran de l’interface pfSense



Légende : Vue des interfaces et état des services.

Équipe Projet

Membres : Axel