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

Date de rendu : 04/04/2025

Durée du projet : 20 jours (jours totaux en étant uniquement à l’école)

**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. Rôles de l’Équipe

- Chef de Projet : Planification, coordination des ressources.

-Administrateur Réseau : Configuration des interfaces pfSense,.

- Responsable Sécurité : Déploiement des règles de pare-feu, proxy.

- Technicien Support : Tests de connectivité, dépannage.

- Documentaliste : Rédaction des guides utilisateur et technique.

2.2. 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.

- OpenVPN : Accès sécurisé à distance (optionnel).

**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),

- Spécifications matérielles :

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

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

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 `admin`, 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.

- Règles LAN → WAN :

- Filtrage des IP non autorisées (ex: blocage des réseaux P2P).

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

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

Tâches réalisées :

- Installation de Squid :

```shell

pkg install squid

service squid enable

```

- Configuration :

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

- Cache : Limité à 10 Go, expiration après 7 jours.

- Authentification : Intégration avec Active Directory via LDAP.

- SSL Inspection :

- Déploiement d’un certificat racine sur les postes clients pour décrypter le trafic HTTPS.

3.5. Phase 5 : Sécurité Avancée (2h)

Objectif : Renforcer la protection contre les menaces.

Tâches réalisées :

- IDS/IPS :

- Activation de Suricata pour analyser le trafic en temps réel.

- Règles de détection : Blocage des scans de ports, attaques DDoS.

- Journalisation :

- Export des logs vers un serveur Syslog (ex: Graylog).

- Alertes par email pour les activités suspectes.

3.6. Phase 6 : 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. Pare-feu pfSense Opérationnel

- Statut des services :

- Squid : Actif avec cache de 8,5 Go.

- Suricata : 15 règles actives, 0 attaques détectées lors des tests.

- Performance : Latence réduite de 30% grâce au cache.

4.2. Documentation

- Schéma réseau : Visuel des interfaces, VLANs, et flux autorisés.

- Rapport de sécurité : Liste des règles IDS/IPS et logs d’activité.

**5. Défis Rencontrés et Solutions**

- Problème : Conflit de ports entre Squid et le service NAT.

- Solution : Modification du port d’écoute de Squid (3128 → 8080).

- Problème : Certificat SSL non reconnu par les navigateurs clients.

- Solution : Import manuel du certificat racine dans le magasin de confiance.

**6. 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, règles de pare-feu, et état des services.

Annexe 2 : Configuration Squid pour le filtrage

```plaintext

# Fichier /usr/local/etc/squid/squid.conf

acl blocked\_urls dstdomain "/etc/squid/blocked\_sites.txt"

http\_access deny blocked\_urls

cache\_dir ufs /var/squid/cache 10000 16 256

```

Annexe 3 : Exemple de règle HAProxy (Load Balancer)

```plaintext

# Configuration HAProxy pour répartir le trafic web

frontend http-in

bind \*:80

default\_backend webservers

backend webservers

balance roundrobin

server srv1 10.0.0.2:80 check

server srv2 10.0.0.3:80 check

```

Équipe Projet

Membres : Axel