Filtrage avec pfSense

Introduction

Dans ce TP, l'objectif était de configurer un pare-feu pfSense pour sécuriser un réseau. pfSense est un système de pare-feu open source basé sur FreeBSD, utilisé pour la gestion du trafic réseau et la protection contre les attaques externes.

Objectifs

1. Installer et configurer pfSense.
2. Créer des règles de filtrage pour autoriser ou bloquer le trafic réseau.
3. Tester la configuration du pare-feu.

Étapes réalisées

1. **Installation de pfSense :**
    - Téléchargez l'ISO de pfSense et installez-le sur une machine virtuelle.
    - Suivez les instructions à l'écran pour l'installation de pfSense. Une fois installé, accédez à l'interface web via l'IP par défaut : http://192.168.1.1.
2. **Configuration initiale de pfSense :**
    - Connectez-vous à l'interface web de pfSense avec le nom d'utilisateur par défaut admin et le mot de passe pfsense.
    - Changez le mot de passe administrateur et configurez l'interface WAN (connexion à Internet) et LAN (réseau interne).
3. **Création des règles de filtrage :**
    - Allez dans Firewall > Rules et ajoutez une règle pour autoriser le trafic interne sur le port 80 (HTTP) :

        Action: Pass

        Interface: LAN

        Address Family: IPv4

        Protocol: TCP

        Source: any

        Destination: LAN address

        Destination port range: HTTP (80)
4. **Test du filtrage :**

- Testez la règle en accédant au réseau local via un navigateur et en vérifiant que l'accès HTTP est autorisé. Essayez également de bloquer un autre service (comme SSH) et vérifiez qu'il est bien bloqué.

Résultats obtenus

Les règles de filtrage ont été configurées avec succès. Le trafic HTTP a été autorisé tandis que d'autres types de trafic ont été bloqués comme prévu.

Conclusion

Ce TP m'a permis de comprendre la mise en place d'un pare-feu pfSense et comment il peut être utilisé pour contrôler et sécuriser les communications réseau au sein d'un réseau d'entreprise.