TP Configuration PfSense

Sommaire

Introduction

PfSense est un système open source basé sur FreeBSD. Il est utilisé comme pare-feu et routeur dans de nombreux environnements professionnels. Il permet de sécuriser un réseau, de filtrer le trafic, et de gérer les connexions entre plusieurs interfaces (LAN, WAN, etc.).

Il propose aussi des services comme le DHCP, le DNS, le NAT ou encore la gestion de VPN. PfSense est une alternative gratuite et performante à des solutions payantes comme celles de Cisco ou Fortinet.

Ce TP a pour objectif de découvrir PfSense à travers une installation simple, la configuration d'un réseau local, la mise en place de règles de filtrage, et la gestion des utilisateurs. Il permet de comprendre comment PfSense peut être utilisé pour sécuriser un réseau d'entreprise.

Configuration initiale de PfSense et du LAN

Après avoir installé PfSense sur une machine virtuelle, il nous est demandé d'associer les cartes réseaux aux interfaces WAN et LAN, ce qu'on va faire, en mettant notre WAN en DHCP pour qu'il obtienne une adresse directement, puis on va choisir une adresse LAN cohérente pour le bon déroulement du TP.

La configuration de base de PfSense est terminée, on peut maintenant se rendre sur l'interface WEB de PfSense pour l'administrer, en utilisant l'IP locale qu'on a choisi.

Par défaut, le mot de passe de l'interface d'administration est PfSense, et l'identifiant admin. On va changer ça par sécurité, PfSense nous le conseille de lui-même.

Après ça, on va activer le serveur DHCP depuis m'interface WEB, pour que quand une VM soit connectée au LAN, elle se voit attribuée automatiquement une IP. On choisit par exemple d'attribuer une adresse IP entre 192.168.1.50 et 192.168.1.100.

On teste en demarrant une autre machine, dans mon cas la machine qui heberge GLPI.

Tout fonctionne correctement, notre machine virtuelle GLPI obtient une adresse IP de la part de PfSense.

Règles de filtrage

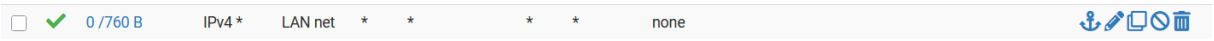
On va maintenant mettre en place des règles de filtrages, pour filtrer le trafic réseau qui transite par PfSense.

Les règles de filtrage dans PfSense sont appliquées en fonction de l'interface réseau. Elles permettent de contrôler les connexions entrantes et sortantes, et de déterminer quel trafic est autorisé ou bloqué.

- Chaque interface (WAN, LAN) a ses propres règles de filtrage.
- Les règles sont appliquées dans l'ordre où elles sont définies, de haut en bas.
- Toutes les connexions sont bloquées, sauf si on crée une règle pour les autoriser.

Dans la page Firewall → Rules, on va créer les règles.

On crée par exemple la règle suivante :



Elle permettra à tous les appareils du LAN d'accéder au WAN.

On peut ainsi créer des règles pour tout ce qu'on veut, par exemple, interdire l'utilisation du protocole FTP, ou http sur certains sites web, ou restreindre les requêtes à HTTPS. Tout est possible.

On va donc essayer de bloquer l'accès a un site en particulier sur notre machine GLPI précisément, mais pas les autres.

Action : Block
Interface : LAN
Source : 192.168.1.50
Destination : 51.38.184.188 (Mon Portfolio)
Protocole : any
Port source/destination : any
Description : Bloquer l'accès à mon portfolio pour cet utilisateur.

On peut essayer de ping mon portfolio depuis la machine virtuelle, mais impossible car PfSense le bloque. On peut d'ailleurs voir sur notre interface PfSense que ma VM a essayé d'accéder en envoyant des paquets.

```
root@server:/etc/network# ping 51.38.184.188
PING 51.38.184.188 (51.38.184.188) 56(84) bytes of data.
^C
--- 51.38.184.188 ping statistics ---
30 packets transmitted, 0 received, 100% packet loss, time 29731ms

root@server:/etc/network#
```

States details

Tracking ID: 1746371605
evaluations: 45
packets: 30
bytes: 2 KiB
states: 0
state creations: 0

Port	Destination	Port	Gateway	Queue
*	LAN Address	80	*	*
*	51.38.184.188	*	*	none
*	*	*	*	none
*	*	*	*	none

Gestion des utilisateurs et accès

On va dans cette partie, gérer les utilisateurs et leurs accès à l'interface, pour sécuriser au mieux PfSense et s'assurer que pas n'importe qui puisse faire n'importe quoi.

Tout se fait depuis le gestionnaire d'utilisateurs sur l'interface WEB.

On commence par créer un utilisateur, en précisant son nom prénom, et mot de passe.

On crée ensuite un groupe d'utilisateur dans l'onglet « groups », on peut créer par exemple un group d'users et un groupe d'administrateurs, en précisant leurs rôles respectifs, et on sauvegarde.

On peut par exemple, donner au groupe "administrateurs" l'accès complet à toutes les pages de configuration, tandis que pour un groupe "users", limiter l'accès aux rapports ou à la visualisation des logs.

On peut aussi restreindre l'accès à l'interface Web en créant une règle dans les Firewall Rules qui limite l'accès à certaines adresses IP ou plages d'adresses.

Par exemple, on peut autoriser l'accès uniquement aux utilisateurs présents dans le sous-réseau 192.168.1.0/24, empêchant ainsi les autres adresses IP d'accéder à l'interface. On renforce ainsi la sécurité au maximum.

Conclusion

Ce TP nous a permis de découvrir et de configurer pfSense, un pare-feu et un routeur open-source, utilisé pour protéger et gérer le trafic réseau dans un environnement contrôlé. Nous avons vu comment installer pfSense sur une machine virtuelle et comment configurer les interfaces réseau pour permettre une communication efficace avec d'autres machines et avec Internet.

Nous avons aussi abordé la configuration du pare-feu, en créant des règles de filtrage et en appliquant des stratégies pour contrôler l'accès à Internet et aux services internes. Nous avons également exploré la gestion des utilisateurs, en apprenant à créer des comptes et à leur attribuer des droits d'accès en fonction de leurs rôles, ce qui permet de renforcer la sécurité du système en contrôlant qui peut accéder à PfSense et avec quels privilèges.