Documentation Technique Générale de l’infrastructure de base

Introduction

Cette documentation technique décrit l'architecture réseau mise en place, mettant en vedette le déploiement d'un pfSense comme pare-feu et routeur. Le réseau est conçu pour prendre en charge plusieurs segments, notamment LAN SERVEUR, LAN CLIENT, DMZ, et un accès WAN.

1. pfSense Configuration

Un second document est disponible ci-dessous afin de regarder la configuration complète du serveur pfSense ainsi que toutes ses règles.

2. Périphériques Connectés de base

2.1 Windows 10 Client

- Connecté à l'interface LAN CLIENT de pfSense.
- Obtient une adresse IP via DHCP.

2.2 Ubuntu Client

- Connecté à l'interface LAN CLIENT de pfSense.
- Obtient une adresse IP via DHCP.

2.3 Windows Server

- Connecté à l'interface LAN SERVEUR de pfSense.
- Adresse IP statique définie à 172.16.0.254.
- Service ADDS
- Service DNS
- Il me sert à manger le pfSense

2.4 Ubuntu Server dans Docker (DMZ)

- Exécuté dans l'interface DMZ de pfSense.
- Adresse IP attribuée statiquement à 172.19.0.254.
- Utilisation de Docker pour la gestion des conteneurs dans la DMZ.

3. Périphériques Connectés au réseau de base (Projets)

3.1 Ubuntu Server FOG

- Connecté à l'interface LAN SERVEUR de pfSense.
- Adresse IP statique définie à 172.16.0.250.

3.2 Ubuntu Server Asterisk

- Connecté à l'interface LAN SERVEUR de pfSense.
- Adresse IP statique définie à 172.16.0.253.

3.3 Ubuntu Server Guacamole

- Connecté à l'interface LAN SERVEUR de pfSense.
- Adresse IP statique définie à 172.16.0.251.

3.4 Ubuntu Server GLPI

- Connecté à l'interface LAN SERVEUR de pfSense.
- Adresse IP statique définie à 172.16.0.249.

3.5 Ubuntu Server OpenVPN

- Connecté à l'interface LAN SERVEUR de pfSense.
- Adresse IP statique définie à 172.16.0.248.

3.6 Ubuntu Server PiHole

- Connecté à l'interface LAN SERVEUR de pfSense.
- Adresse IP statique définie à 172.16.0.247.

Chacun de ces services sont indépendants. Ils peuvent donc fonctionner individuellement ou tous ensemble. J'ai ajouté le PiHole qui n'est pas vraiment un projet, il me sert uniquement de bloqueur de publicité.

4. Topologie du Réseau

La topologie du réseau est structurée de manière à séparer les segments internes (LAN SERVEUR et LAN CLIENT) de la zone démilitarisée (DMZ) qui héberge les services exposés au public. Le pare-feu pfSense agit comme point de contrôle centralisé, assurant une segmentation efficace du trafic.

Documentation Technique du Réseau pfSense

Version

- pfSense Version: 22.9

Système

- Nom de l'hôte: pfSense
- Domaine: home.arpa
- Optimisation: normal
- Interface DNS: 172.16.0.254, 1.0.0.1
- Fuseau horaire: Etc/UTC

Utilisateurs et Groupes

- Utilisateur Administrateur: admin (ID utilisateur: 0)
  - Groupe: admins
  - Privilèges: user-shell-access
  - Mot de passe: (hash)

Interfaces

- **WAN**
  - Type: hn0
  - Adresse IP: DHCP
  - Description: WAN
- **LAN**
  - Type: hn3
  - Adresse IP: 172.16.0.1/16
  - Description: LAN
- **LANCLIENT**
  - Type: hn2
  - Adresse IP: 192.168.1.1/24
  - Description: LANCLIENT
- **DMZ**
  - Type: hn1
  - Adresse IP: 172.19.0.1/16
  - Description: DMZ

Règles DHCP

- LAN: Plage de 172.16.0.10 à 172.16.255.245
- LANCLIENT: Plage de 192.168.1.10 à 192.168.1.50

Règles NAT

1. **OpenVPN:**
   - WAN IP: Port 1194 -> 172.16.0.248:1194 (TCP/UDP)
2. **SIP Asterisk:**
   - WAN IP: Port 5060 -> 172.16.0.253:5060 (UDP)
3. **FTP Docker:**
   - WAN IP: Port 20 -> 172.19.0.254:20 (TCP/UDP)
4. **NAT NGINX DOCKER:**
   - WAN IP: Port 80 -> 172.19.0.254:80 (TCP/UDP)
5. **NAT NGINX PROXY MANAGER DOCKER:**
   - WAN IP: Port 81 -> 172.19.0.254:81 (TCP/UDP)
6. **NAT FRESHRSS DOCKER:**
   - WAN IP: Port 86 -> 172.19.0.254:86(TCP/UDP)
7. **SSH DOCKER:**
   - WAN IP: Port 24 -> 172.19.0.254:22 (TCP)
8. **SSH Asterisk:**
   - WAN IP: Port 25 -> 172.16.0.253:22 (TCP)
9. **SSH Guacd:**
   - WAN IP: Port 26 -> 172.16.0.251:22 (TCP)
10. **Guacd Int:**
    - WAN IP: Port 443 -> 172.16.0.251:443 (TCP)
11. **SSH FOG:**
    - WAN IP: Port 27 -> 172.16.0.250:22 (TCP)

Règles de Pare-feu

- Autoriser le trafic de LAN vers WAN.
- Autoriser le trafic IPv6 de LAN vers WAN.
- Autoriser le trafic de DMZ vers WAN pour l'adresse IP 172.16.0.254 (SSH).

Règles de Pare-feu OPT1 (LANCLIENT)

- Autoriser le trafic de LANCLIENT vers WAN pour l'adresse IP 172.16.0.254.

Règles de Pare-feu OPT2 (DMZ)

- Autoriser le trafic de DMZ vers WAN pour l'adresse IP 172.16.0.254.
- Bloquer le trafic de DMZ vers LAN.
- Autoriser le trafic de DMZ vers LAN pour l'adresse IP 172.16.0.254.

Règles de Pare-feu par Défaut

- Bloquer le trafic de WAN vers LAN.
- Autoriser le trafic de LAN vers n'importe quelle destination.
- Autoriser le trafic IPv6 de LAN vers n'importe quelle destination.
- Bloquer le trafic de OPT1 vers LAN.
- Autoriser le trafic de OPT1 vers WAN pour l'adresse IP 172.16.0.254.
- Bloquer le trafic de OPT2 vers LAN.
- Autoriser le trafic de OPT2 vers WAN pour l'adresse IP 172.16.0.254.

Schéma Réseau