Documentation de Configuration : Routeur pfSense

Introduction

Un routeur est un équipement réseau qui permet de connecter différents réseaux entre eux et de gérer le trafic de données. pfSense est un système d'exploitation basé sur FreeBSD, conçu pour transformer un PC ou une VM en un routeur/pare-feu performant, sécurisé et configurable.

Il offre :

- Une gestion avancée des règles de pare-feu,
- Des fonctionnalités VPN,
- Une interface web pour l'administration,
- Une redondance et équilibrage de charge,
- Et des services tels que DHCP, DNS, NAT, etc.

---

1. Installation de pfSense en VM

1. Créer une machine virtuelle nommée `pfSense-modele`.
2. Sélectionner l'OS : **Other > FreeBSD (64-bit)**.
3. Ajouter **3 cartes réseau** dans l'ordre suivant :
    - `em0` : mode **bridge**
    - `em1` : **LAN Segment** nommé `LAN`
    - `em2` : **LAN Segment** nommé `DMZ`

---

2. Configuration des interfaces au démarrage

Après le premier boot :

1. Lancer l'option `1 - Assign interfaces`.
2. Répondre `n` à la question sur les VLAN.
3. Assigner les interfaces :
    - WAN → `em0` → MAC correspondante → `172.31.200.1/16`
    - LAN → `em1` → `172.17.255.254/16`
    - DMZ → `em2` → `192.168.17.254/24`
4. Terminer avec `exit`, puis `6 - Halt System` pour sauvegarder.

---

3. Accès à l'interface Web

Lancer la VM, puis depuis un navigateur, accéder à :

```
cpp
CopierModifier
```

```
http://172.17.255.254
```

Identifiants par défaut :

- **admin / pfsense**

---

4. Vérification et gestion

Dans l'interface web :

- Configurer les plages DHCP sur les interfaces LAN et DMZ.
- Ajouter les règles de pare-feu pour permettre la communication entre LAN ↔ DMZ si nécessaire.
- Activer le service DNS Resolver ou DNS Forwarder.

5. Configuration des Règles de Pare-feu dans pfSense

Règle par défaut

pfSense **bloque tout le trafic entrant** sur toutes les interfaces sauf le LAN par défaut. Il faut donc créer des règles pour permettre certaines communications selon les besoins.

✅ Objectifs de configuration :

WAN (em0) – `172.31.200.1/16`

- **Règle 1 :** Bloquer tout le trafic entrant sauf pour les connexions établies (par défaut).
- **Règle 2 (optionnel)** : Ouvrir certains ports (SSH, HTTPS, VPN, etc.) si nécessaire.

LAN (em1) – `172.17.255.254/16`

- **Règle 1 :** Autoriser tout trafic sortant vers Internet (WAN).
- **Règle 2 :** Autoriser les communications vers la DMZ (ex : accès à un serveur Web).

```
txt
CopierModifier
Action : Pass
Interface : LAN
Source : LAN Net (172.17.0.0/16)
Destination : DMZ Net (192.168.17.0/24)
Port : any
Description : Autorise le LAN à accéder à la DMZ
```

DMZ (em2) – `192.168.17.254/24`

- **Règle 1 :** Autoriser uniquement certains services vers LAN (ex : retour de requêtes Web).
- **Règle 2 :** Interdire l'accès de la DMZ vers Internet sauf exceptions.

```
txt
CopierModifier
Action : Pass
Interface : DMZ
Source : DMZ Net (192.168.17.0/24)
Destination : LAN Net (172.17.0.0/16)
Port : HTTP/HTTPS (si nécessaire)
Description : Permet les réponses Web de la DMZ vers le LAN
```

---

6. Plan des VLANs

Les VLAN permettent de **segmenter logiquement** le réseau pour améliorer la sécurité et l'organisation.

Nom	VLAN ID	Réseau IP	Utilisation
LAN Grp1	101	172.17.0.0/16	Réseau interne (AD, BDD)
DMZ Grp1	201	192.168.17.0/24	Serveurs exposés

Configuration des VLANs dans pfSense :

1. Aller dans **Interfaces > Assignments > VLANs**.
2. Cliquer sur **+ Add**.
3. Créer les VLANs suivants :
   - VLAN 101 → Interface parent `em1` (LAN)
   - VLAN 201 → Interface parent `em2` (DMZ)
4. Ensuite, ajouter ces interfaces depuis **Interfaces > Assignments**.

7. Plan de Routage & NAT dans pfSense

🔄 Objectif du routage

Le but est de permettre la communication entre :

- Le LAN ↔ DMZ (selon les règles de sécurité),
- Le LAN ↔ WAN (accès Internet),
- La DMZ ↔ WAN (limité et contrôlé).

📌 Routage interne (automatique dans pfSense)

pfSense agit comme **passerelle** pour tous les sous-réseaux configurés sur ses interfaces. Aucune route statique n'est nécessaire si :

- Les interfaces LAN (172.17.255.254) et DMZ (192.168.17.254) sont bien configurées.
- Le pare-feu autorise le trafic entre interfaces.

Exemple :

- Une machine LAN (172.17.0.10) veut accéder à Web (192.168.17.1) :
  - Passerelle : `172.17.255.254`
  - Le trafic transite via pfSense si une règle de pare-feu le permet.

🔐 NAT – Network Address Translation

NAT vers Internet (WAN)

Par défaut, pfSense applique une règle **NAT automatique** :

- Toute IP interne (LAN ou DMZ) qui communique vers Internet est **masquée** par l'IP WAN (`172.31.200.1`).

Exemple de règle de NAT manuelle (si nécessaire) :

Pour exposer un serveur Web DMZ (`192.168.17.1`) sur le port 80 :

```
plaintext
CopierModifier
Interface : WAN
External IP : 172.31.200.1 (ou IP publique)
Protocol : TCP
External Port : 80
Internal IP : 192.168.17.1
Internal Port : 80
Description : Accès Web externe vers DMZ
```

✳ Résumé du routage/NAT

Source	Destination	Type	Condition
LAN → Internet	NAT	Automatique via WAN	
DMZ → Internet	NAT	Bloqué sauf règle spécifique	
LAN → DMZ	Routage direct	Autorisé via règle	
DMZ → LAN	Routage direct	Très restreint	
Internet → DMZ	NAT (port forward)	Si nécessaire (web, etc.)	