

Installation et configuration d'IPFire (Routeur/PareFeu/DHCP)

2.1 Installer IPFire

Étape 1 : Télécharger l'ISO d'IPFire

1. Rendez-vous sur le site officiel d'IPFire.
2. Téléchargez l'ISO adapté à votre architecture (x86_64 pour la plupart des cas).
<https://www.ipfire.org/downloads/ipfire-2.29-core189>
3. Conservez l'ISO dans un dossier accessible pour l'utilisation dans VirtualBox.

Étape 2 : Créer une VM pour IPFire

1. **Dans VirtualBox**, créez une nouvelle machine virtuelle :
 - **Nom** : IPFire.
 - **Type** : Linux.
 - **Version** : Other Linux (64-bit).
2. **Configurer les ressources** :
 - **RAM** : 1 Go.
 - **CPU** : 1 vCPU.
 - **Disque dur** : 5 Go en VDI.
3. **Configurer les adaptateurs réseau** :
 - **Adaptateur 1** : NAT (pour l'accès Internet, interface RED).
 - **Adaptateur 2** : Réseau interne (pour le réseau interne GREEN).

Étape 3 : Installer IPFire

1. Lancez la VM et montez l'ISO d'IPFire.
2. Suivez les étapes d'installation :
 - Acceptez la licence.
 - Sélectionnez le disque dur à utiliser et formatez-le.
 - Configurez un mot de passe pour admin (interface web) et root (console SSH).
 - Une fois l'installation terminée, redémarrez la VM et retirez l'ISO.

Étape 4 : Configuration initiale d'IPFire

1. À la fin du démarrage, suivez les étapes de configuration réseau :
 - **Type de réseau** : Sélectionnez GREEN + RED.
 - **Configuration des interfaces** :
 - **RED (NAT)** : Configuré pour obtenir une adresse IP via DHCP.
 - **GREEN (interne)** : Configurez une IP fixe, par exemple :

- Adresse IP : 192.168.2.1.
 - Masque de sous-réseau : 255.255.255.0.
 - Rappel : toutes les machine du même réseau doivent avoir la même adresse réseau. 192.168.2.X
2. Sauvegardez les paramètres et redémarrez.

Étape 5 : Accéder à l'interface web d'IPFire

1. Depuis une autre machine connectée au réseau interne (GREEN), ouvrez un navigateur.
2. Accédez à l'adresse IP d'IPFire (exemple : <https://192.168.2.1:444>).
3. Connectez-vous avec les identifiants admin et le mot de passe défini.

2.2 Configurer les règles de pare-feu

Étape 1 : Accéder à la configuration du pare-feu

1. Depuis l'interface web d'IPFire, cliquez sur **Firewall** dans le menu principal.
2. Accédez à l'onglet **Firewall Rules**.

Étape 2 : Ajouter une règle pour l'accès SSH à Debian

1. Cliquez sur **Add a new rule**.
2. Configurez les paramètres suivants :
 - **Source** :
 - Type : GREEN (réseau interne).
 - Adresse IP : Any (ou une IP spécifique si vous voulez restreindre).
 - **Destination** :
 - Adresse IP : L'adresse IP fixe de votre machine Debian (par exemple, 192.168.2.10).
 - Protocole : TCP.
 - Port : 22 (port SSH).
3. Ajoutez un commentaire (ex. "Accès SSH à Debian") et cliquez sur **Add**.
4. Appliquez la règle en cliquant sur **Apply changes**.

Étape 3 : Ajouter une règle pour l'accès au serveur Apache

1. Cliquez sur **Add a new rule**.
2. Configurez les paramètres suivants :
 - **Source** :
 - Type : GREEN.

- Adresse IP : Any (ou restreindre selon vos besoins).
- **Destination :**
 - Adresse IP : L'adresse IP du serveur Apache (ex. 192.168.2.10).
 - Protocole : TCP.
 - Ports :
 - **80** (HTTP).
 - **443** (HTTPS).
- 3. Ajoutez un commentaire (ex. "Accès HTTP/HTTPS au serveur Apache") et cliquez sur **Add**.
- 4. Appliquez la règle.

Étape 4 : Ajouter une règle pour le Serveur DHCP/Ubuntu (Optionnel)

Le service DHCP peut être géré par IPFire :

- **Range (192.168.2.100/24-192.168.2.200/24)**
 - **Client Windows 10 ou 11.**
- **IPs Fixe :**
 - **192.168.2.1 = IPFire**
 - **192.168.2.10 = Debian**
 - **192.168.2.11 = Ubuntu**
 - **192.168.2.12 = Serveur 2022**

1. Le protocole DHCP utilise les ports suivants :

UDP 67 : pour les requêtes du client vers le serveur DHCP.

UDP 68 : pour les réponses du serveur vers le client.
2. Cliquez sur **Add a new rule**.
3. Configurez les paramètres suivants :
 - **Source :**
 - Type : GREEN.
 - Adresse IP : Any (ou restreindre selon vos besoins).
 - **Destination :**
 - Adresse IP : L'adresse IP du serveur DHCP (ex. 192.168.2.11).
 - Protocole : UDP.
 - Ports :
 - **Source port 67**
 - **Destination port 68**
 - **Action :**
 - **Allow this traffic**

4. Ajoutez un commentaire (ex. "Accès aux service DHCP/Ubuntu") et cliquez sur **Add**.
5. Appliquez la règle.

Étape 5 : Tester les règles

1. Depuis une machine connectée au réseau GREEN, tentez d'accéder :
 - À Debian via SSH (ssh root@192.168.2.10).
 - Au serveur Apache Debian via un navigateur (http://192.168.2.10).
2. Vérifiez que les connexions fonctionnent correctement.