UFW (firewall)

UFW (Uncomplicated Firewall)

UFW (Uncomplicated Firewall) est un outil de gestion de pare-feu conçu pour simplifier l'utilisation de `iptables`, le pare-feu sous-jacent de Linux. Créé pour être convivial, UFW permet aux utilisateurs, même ceux qui n'ont pas une grande expérience avec les systèmes de pare-feu, de configurer des règles de sécurité réseau rapidement et efficacement. Il est particulièrement populaire sur des distributions comme Ubuntu.

UFW gère l'accès aux ports réseau en autorisant ou bloquant le trafic entrant et sortant, offrant ainsi une couche de protection essentielle contre les attaques extérieures. Sa simplicité d'utilisation, combinée à sa puissance, en fait un outil idéal pour sécuriser les serveurs, les ordinateurs personnels ou les réseaux domestiques.

Avec une syntaxe intuitive et des commandes simples, UFW permet d'appliquer des règles de pare-feu courantes en quelques étapes seulement, tout en offrant la flexibilité nécessaire pour gérer des configurations réseau plus complexes.

Quelques commandes essentielles pour UFW :

- **Installation (si nécessaire) :**
  - Sur Ubuntu :

    ```
    sudo apt install ufw
    ```

  - Sur Arch Linux :

    ```
    sudo pacman -S ufw
    ```

- **Activer et désactiver UFW :**
  - Active le pare-feu UFW :

    ```
    sudo ufw enable
    ```

  - Désactive le pare-feu UFW :

```
sudo ufw disable
```

- **Vérifier l'état de UFW :**
  - Affiche l'état actuel du pare-feu et les règles actives :

```
sudo ufw status
```

  - Affiche l'état avec plus de détails (par exemple, si le pare-feu est actif ou inactif) :

```
sudo ufw status verbose
```

- **Autoriser et bloquer des connexions :**
  - Autorise les connexions entrantes sur le port 22 (par exemple, pour SSH) :

```
sudo ufw allow 22
```

  - Bloque les connexions entrantes sur le port 80 (HTTP) :

```
sudo ufw deny 80
```

  - Autorise le trafic entrant en provenance de l'adresse IP `192.168.1.100` :

```
sudo ufw allow from 192.168.1.100
```

  - Bloque tout trafic provenant de l'adresse IP `203.0.113.1`:

```
sudo ufw deny from 203.0.113.1
```

- **Autoriser ou bloquer des connexions pour des services spécifiques :**
  - Autorise les connexions SSH (équivalent à `sudo ufw allow 22`) :

```
sudo ufw allow ssh
```

  - Autorise le trafic HTTP (port 80) :

```
sudo ufw allow http
```

  - Autorise le trafic HTTPS (port 443) :

```
sudo ufw allow https
```

- **Supprimer des règles :**
  - Supprime la règle qui autorise les connexions sur le port 22 :

```
sudo ufw delete allow 22
```

  - Supprime la règle qui bloque les connexions sur le port 80 :

```
sudo ufw delete deny 80
```

- **Limiter les tentatives de connexion pour prévenir les attaques bruteforce :**
  - Limite les connexions SSH pour prévenir les tentatives répétées d'attaques bruteforce :

```
sudo ufw limit ssh
```

- **Gérer les règles par IP ou sous-réseau :**
  - Autorise les connexions SSH depuis un sous-réseau spécifique (`192.168.1.0/24`) :

```
sudo ufw allow from 192.168.1.0/24 to any port 22
```

- **Réinitialiser UFW :**
  - Réinitialise UFW à sa configuration par défaut, supprimant toutes les règles existantes :

```
sudo ufw reset
```

Configuration de base pour UFW :

1. **Activer UFW et autoriser les connexions SSH :**
   - Avant d'activer UFW sur un serveur distant, assure-toi de permettre les connexions SSH, sinon tu pourrais te bloquer toi-même :

```
sudo ufw allow ssh sudo ufw enable
```

2. **Configurer les règles de pare-feu pour un serveur web :**
   - Pour un serveur web typique, tu pourrais vouloir autoriser le trafic HTTP et HTTPS, tout en bloquant tout le reste :

```
sudo ufw allow http sudo ufw allow https sudo ufw enable
```

3. **Limiter les connexions SSH pour plus de sécurité :**
   - Pour protéger ton serveur des attaques bruteforce SSH :

```
sudo ufw limit ssh
```

4. **Autoriser les connexions depuis un réseau local seulement :**
   - Si tu veux autoriser les connexions à un service seulement depuis un réseau local spécifique :

```
sudo ufw allow from 192.168.1.0/24 to any port 3306
```

   - Cela autorise les connexions à MySQL (port 3306) uniquement depuis le sous-réseau `192.168.1.0/24`.
5. **Afficher et gérer les règles :**
   - Après avoir configuré tes règles, tu peux toujours vérifier l'état actuel avec :

```
sudo ufw status
```

Revision #6
Created 23 August 2024 12:59:08 by qoyri
Updated 23 August 2024 13:17:51 by qoyri