Configuration du service firewalld

1 Présentation

> **Note :** Un **pare-feu** (ou **Firewall**) est un dispositif logiciel permettant de filtrer les paquets réseau afin de mettre en place une politique de sécurité. Un pare-feu peut être avec états (*stateful firewall*) (il mémorise l'état des connexions, en vérifie la conformité et applique des règles adaptées) ou sans état (*stateless firewall*) (il applique des règles sur chaque paquet de manière indépendante). Plus d'information ici [a].
>
> a. http://fr.wikipedia.org/wiki/Pare-feu_(informatique)

Le pare-feu alma-linux (appelé `firewalld`) est sans état. Quelques caractéristiques :

- Les machines auxquelles s'appliquent le filtrage son rangées dans des **zones**. Il existe par défaut des zones que vous pouvez utiliser.
- Une fois les zones définies, nous allons ouvrir ou fermer des services pour ces zones.
- **Firewalld** gère un état courant et un état permanent (restauré après redémarrage). Une configuration marquée comme permanente nécessite un rechargement afin de l'appliquer.

> **Note :** Vous trouverez une description plus précise sur ce site [a].
>
> a. https://www.linuxtricks.fr/wiki/firewalld-le-pare-feu-facile-sous-linux

2 Quelques exercices sur `client0`

Placez vous dans le `client0`, installez ou vérifiez la présence de **firewalld** :

```
# installation
dnf -y install firewalld

# démarrage
systemctl enable firewalld
systemctl restart firewalld
```

Firewalld identifie les machines à partir de zones pour leurs appliquer des règles de filtrage. Déroulez une-à-une les actions ci-dessous afin de comprendre le fonctionnent :

```
# interroger la version
firewall-cmd --version

# quelles sont les zones
firewall-cmd --get-zones

# création d'une zone "no-ssh"
firewall-cmd --new-zone=no-ssh --permanent
# demander au FW de recharger la configuration
firewall-cmd --reload

# ajout de client1 à la zone
firewall-cmd --zone=no-ssh --add-source=192.168.0.101

# autoriser ssh à partir des machines de "no-ssh"
firewall-cmd --zone=no-ssh --add-service=ssh

# vérifiez
firewall-cmd --zone=no-ssh --list-all

# À faire: vérifiez sur client1 que la connexion fonctionne vers client0

# interdire ssh à partir des machines de "no-ssh"
firewall-cmd --zone=no-ssh --remove-service=ssh

# À faire: vérifiez que client1 ne peut plus se connecter sur client0

# re-autoriser ssh à partir des machines de "no-ssh" de façon permanente
firewall-cmd --zone=no-ssh --add-service=ssh --permanent
firewall-cmd --reload
```