GNU / Linux — Firewall avec UFW

Uncomplicated Firewall — commandes, règles et exemples

Objectif du cours

Comprendre le rôle de UFW.

Savoir l'activer, le désactiver et vérifier son état.

Créer, afficher, numéroter et supprimer des règles.

Comprendre les règles par défaut, la journalisation, reject et limit.

Lire des règles simples puis des règles plus complètes.

Mémo simple

UFW est une interface simplifiée pour gérer le pare-feu Linux.

L'idée est de rendre les règles plus lisibles et plus faciles à administrer qu'avec des commandes iptables longues.

1. Plan

- Avantages par rapport à iptables
- Commandes de base
- Règles
  - Afficher les règles
  - Afficher les règles numérotées
  - Gérer les règles par défaut
  - Ajouter des règles
  - Supprimer des règles
  - Configuration avancée

2. Avantages par rapport à iptables

- Simplifié
- Devrait à terme permettre une configuration automatique du pare-feu lors de l'installation de programmes en ayant besoin
- Interface graphique : Gufw
- Également pour KDE : ufw-kde

À retenir

iptables permet un contrôle très fin, mais sa syntaxe peut être difficile à lire.
UFW simplifie les opérations courantes : autoriser, refuser, limiter, afficher et supprimer des règles.

3. Commandes de base

Commande	Rôle
ufw enable	Activer UFW et appliquer les règles.
ufw disable	Désactiver UFW.
ufw status	Vérifier le statut.
ufw reload	Recharger UFW et ses règles.
ufw reset	Réinitialiser les règles avec confirmation.
ufw reset --force	Réinitialiser les règles sans confirmation.

```
ufw enable
ufw disable
ufw status
ufw reload
ufw reset
ufw reset --force
```

Attention avant ufw enable

Sur un serveur administré à distance, il faut vérifier qu'une règle autorise SSH avant d'activer le pare-feu.

Sinon, la connexion distante peut être bloquée.

4. Règles — afficher les règles

```
ufw status verbose
```

- Affiche les règles par défaut derrière le mot-clé « Default »
- Affiche ensuite pour chaque règle définie :
  - la version IP concernée est précisée si IPv6, sinon c'est une règle IPv4
  - le port de destination
  - l'action et la direction du trafic
  - l'IP / range source

Afficher les règles numérotées

```
ufw status numbered
```

Pourquoi numéroter ?

Les numéros permettent de supprimer facilement une règle précise avec : ufw delete [numéro].

5. Gérer les règles par défaut

Commande	Rôle
ufw default allow	Autoriser le trafic entrant par défaut.
ufw default deny	Refuser le trafic entrant par défaut.
ufw default allow outgoing	Autoriser le trafic sortant par défaut.
ufw default deny outgoing	Refuser le trafic sortant par défaut.

Logique conseillée dans beaucoup de cas

Entrant : refuser par défaut, puis autoriser uniquement les services nécessaires.

Sortant : autoriser par défaut, sauf besoin particulier.

6. Ajouter des règles

Commande	Rôle
ufw allow [port ou nom du service]	Autoriser une connexion entrante.
ufw deny [port ou nom du service]	Refuser une connexion entrante.
ufw insert 1 deny from [ip]	Refuser une IP entrante et placer la règle avant les autres.

ufw deny [port]/tcp	Refuser une connexion entrante uniquement en TCP.
ufw allow out [port ou nom du service]	Autoriser une connexion sortante.
ufw deny out [port ou nom du service]	Refuser une connexion sortante.

Exemples de lecture

```
ufw allow 22
```

Traduction
Autoriser les connexions entrantes vers le port 22.

```
ufw deny 80/tcp
```

Traduction
Refuser les connexions entrantes TCP vers le port 80.

```
ufw insert 1 deny from 192.168.1.50
```

Traduction
Placer en première position une règle refusant les paquets provenant de 192.168.1.50.

7. Supprimer des règles

Commande	Rôle
ufw delete allow [port ou nom du service]	Supprimer une règle allow.
ufw delete deny [port ou nom du service]	Supprimer une règle deny.
ufw delete [numéro]	Supprimer une règle selon son numéro.

```
ufw status numbered
ufw delete 3
```

Méthode simple

1. Afficher les règles numérotées.
2. Repérer le numéro de la règle.
3. Utiliser ufw delete suivi du numéro.

8. Configuration avancée

Gérer la journalisation

```
ufw logging off
ufw logging low
ufw logging on
ufw logging medium
ufw logging high
ufw logging full
```

Niveau	Effet
off	Désactiver la journalisation.
low / on	Journalisation faible.
medium	Journalisation intermédiaire.
high	Journalisation élevée.
full	Journalisation complète.

Utilisation des services

```
cat /etc/services
```

- Les noms de services sont automatiquement convertis en ports pour les règles.

Exemple

Le nom ssh correspond généralement au port 22.

Une règle peut donc utiliser un numéro de port ou un nom de service.

Placer une règle à une position précise

```
ufw insert [numéro] [règle]
```

- Cette commande place une règle à l'endroit choisi dans la liste.

Reject et Limit

- La règle deny correspond à un drop, la règle reject permet d'informer la source
- La règle limit permet d'accepter les connexions, mais de commencer à les refuser si une adresse IP essaie d'initier plus de 6 connexions en 30 secondes.

Action	Signification
deny	Bloque silencieusement.
reject	Bloque et informe la source.
limit	Autorise, puis limite les tentatives trop nombreuses.

9. Règles complexes

Refuser TCP sur le port 80 pour tout le monde

```
ufw deny proto tcp to any port 80
```

Lecture

deny : refuser
proto tcp : protocole TCP
to any : vers n'importe quelle destination
port 80 : port de destination 80

Refuser un flux TCP provenant du réseau 10.0.0.0/8

```
ufw deny proto tcp from 10.0.0.0/8 to 192.168.0.1 port 25
```

Lecture

Refuser le protocole TCP provenant du réseau 10.0.0.0/8, à destination de 192.168.0.1, sur le port 25.

Refuser un flux UDP provenant de 1.2.3.4

```
ufw deny proto udp from 1.2.3.4 to any port 514
```

Lecture

Refuser le protocole UDP provenant de 1.2.3.4, vers n'importe quelle destination, sur le port 514.

Refuser une règle sortante vers le port 80

```
ufw deny out from 192.168.0.5 to any port 80
```

Lecture

Refuser un flux sortant provenant de 192.168.0.5 vers n'importe quelle destination sur le port 80.

10. Fiche mentale finale

Commande	Rôle
enable / disable	Activer ou désactiver UFW.
status / status verbose	Voir l'état et les règles.
status numbered	Voir les règles avec leurs numéros.
default allow / deny	Définir le comportement par défaut.
allow	Autoriser.
deny	Bloquer silencieusement.
reject	Bloquer avec une réponse.
limit	Limiter les tentatives trop nombreuses.
insert	Placer une règle à une position précise.
delete	Supprimer une règle.
reload	Recharger les règles.
reset	Réinitialiser la configuration.

Ordre simple pour administrer UFW

1. Vérifier ou définir les règles par défaut.
2. Ajouter les exceptions nécessaires.
3. Vérifier avec ufw status verbose ou numbered.
4. Activer ou recharger UFW.
5. Tester les services autorisés.