|  |  |
| --- | --- |
| ufw - Dagorret Notes | Uncomplicated Firewall (ufw) |

# Uncomplicated Firewall (ufw)

## Installation

Debian n'installe pas UFW par défaut.   
Il peut être facilement installé en entrant la commande suivante dans le terminal en tant que super utilisateur …  
**>> sudo apt install ufw**

**Remarque** …  
La simple installation du pare-feu ne l'activera pas automatiquement et aucune règle ne sera définie par défaut.

## Utilisation d'IPv6 avec UFW (facultatif)

Si IPv6 est activé sur le serveur, il faut s’assurer qu'UFW est configuré pour prendre en charge IPv6 afin qu'il gère les règles de pare-feu pour IPv6 en plus d'IPv4.

Pour ce faire, on accède au fichier de configuration d’UFW …  
**>> sudo nano /etc/default/ufw**

Ensuite, on ajoute la ligne suivante …  
**IPV6=yes**

On enregistre et on ferme le fichier.   
Désormais, lorsque UFW est activé, il sera configuré pour écrire à la fois des règles de pare-feu IPv4 et IPv6.

## Configuration des stratégies par défaut

Par défaut, UFW est configuré pour refuser toutes les connexions entrantes et autoriser toutes les connexions sortantes. Cela signifie que toute personne essayant d'atteindre le serveur ne pourra pas se connecter, tandis que toute application au sein du serveur pourra atteindre le monde extérieur.

Pour définir les valeurs par défaut utilisées par UFW …  
**>> sudo ufw default deny incoming  
>> sudo ufw default allow outgoing**

## Autorisation des connexions SSH

Pour configurer le serveur pour autoriser les connexions SSH entrantes …  
**>> sudo ufw allow ssh**

Cependant, il est possible d’écrire une règle équivalente en spécifiant le port au lieu du nom du service.   
Par exemple, cette commande fonctionne de la même manière …  
**>> sudo ufw allow 22**

Si on a configuré le démon SSH pour utiliser un port différent, on doit spécifier le port approprié.   
Par exemple, si le serveur SSH écoute sur le port 2222 …  
**>> sudo ufw allow 2222**

## Activation de l'UFW

Pour activer UFW …  
**>> sudo ufw enable**

## Affichage des règles

Pour voir les règles définies, on peut peut exécuter la commande …  
**>> sudo** **ufw status verbose**

## Autorisation pour d'autres connexions

Il est également possible de le faire pour …

* HTTP sur le port 80, qui est utilisé par les serveurs Web sans chiffrement …  
  **>> sudo** **ufw allow http**   
  ou   
  **>> sudo** **ufw allow 80**
* HTTPS sur le port 443, qui est utilisé par les serveurs Web avec chiffrement …  
  **>> sudo** **ufw allow https**   
  ou   
  **>> sudo** **ufw allow 443**

## Étendues de ports spécifiques

On peut spécifier des étendues de ports avec UFW.   
Certaines applications utilisent plusieurs ports au lieu d'un seul.

Par exemple, pour autoriser les connexions X11 (affichage avec Linux), qui utilisent les ports 6000 à 6007 …  
**>> sudo** **ufw allow <Étendue de ports>/<Protocole>**  
**>> sudo** **ufw allow 6000:6007/tcp**  
ou   
**>> sudo** **ufw allow 6000:6007/udp**

**Remarque** …  
Le fait de ne pas spécifier le protocole autorise automatiquement les deux protocoles, ce qui est acceptable dans la plupart des cas.

## Adresses IP spécifiques

Lorsque l’on travaille avec UFW, il est également possible de spécifier des adresses IP.   
Par exemple, si on souhaite autoriser les connexions à partir d'une adresse IP spécifique …  
**>> sudo** **ufw allow from <Adresse IP>  
>> sudo** **ufw allow from 192.168.1.100**

On peut également spécifier un port spécifique auquel l'adresse IP est autorisée à se connecter en ajoutant to any port suivi du numéro de port. …  
**>> sudo** **ufw allow from 192.168.1.100 to any port 22**

## Sous-réseaux

Si on souhaite autoriser un sous-réseau d'adresses IP, on peut le faire en utilisant la notation CIDR pour spécifier un masque de réseau.   
**>> sudo** **ufw allow from <Sous-réseau>/<Notation CIDR>  
>> sudo** **ufw allow from 192.168.1.0/24**

De même, on peut également spécifier le port de destination …  
**>> sudo** **ufw allow from 192.168.1.0/24** **to any port 22**

## Connexions à une interface réseau spécifique

Si on aimerait créer une règle de pare-feu qui ne s'applique qu'à une interface réseau spécifique on peut le faire en spécifiant **allow in on** suivi du nom de l'interface réseau …  
**>> sudo** **ufw allow in on <Interface> to any port 80  
>> sudo** **ufw allow in on ens33 to any port 80**

Si on souhaite que le serveur de **base de données MySQL** (port 3306) écoute les connexions sur l'interface réseau privée eth1 …  
**>> sudo** **ufw allow in on <Interface> to any port <Numéro de port>  
>> sudo** **ufw allow in on ens33 to any port 3306**

## Refus de connexions

On peut alors utiliser les mêmes commandes (ci-dessus) en remplaçant allow par deny …  
**>> sudo** **ufw deny <Prtoocole>  
>> sudo** **ufw deny http**

Si on souhaite refuser certaines connexions …  
**>> sudo** **ufw deny from <Adresse IP>  
>> sudo** **ufw deny from 192.168.1.100**

## Suppression des règles

Il existe deux manières différentes de spécifier les règles à supprimer …

* par numéro de règle   
  ou
* par la règle réelle (similaire à la façon dont les règles ont été spécifiées lors de leur création).

### Suppression par numéro de règle

Si on utilise le numéro de règle pour supprimer des règles de pare-feu, la première chose à faire est d'obtenir une liste des règles de pare-feu actives.   
La commande d'état UFW possède une option pour afficher des nombres à côté de chaque règle …  
**>> sudo** **ufw status numbered**

Si on décide de supprimer la règle 2, celle qui autorise les connexions au port 80 (HTTP), on peut la spécifier dans une commande de suppression UFW …  
**>> sudo** **ufw delete <Numéro de règle>  
>> sudo** **ufw delete 2**

**Remarque** …  
Cette commande affiche une invite de confirmation demandant la confirmation de la suppression de la règle

### Suppression par règle réelle

L'alternative aux numéros de règle consiste à spécifier la règle réelle à supprimer.   
Par exemple, si on souhaite supprimer la règle allow http …  
**>> sudo** **ufw delete allow http**ou  
**>> sudo** **ufw delete allow 80**

**Remarque** …  
Cette méthode supprimera les règles IPv4 et IPv6, si elles existent.

## Vérification du statut et des règles UFW

À tout moment, on peut vérifier l'état d'UFW …  
**>> sudo** **ufw status verbose**Si UFW est désactivé, ce qui est le cas par défaut, le pare-feu affiche …

Sinon …  
**>> sudo** **ufw status verbose**

## Désactivation ou réinitialisation du pare-feu

Si on décide de ne pas utiliser UFW, il est possible de le désactiver …  
**>> sudo** **ufw disable**Toutes les règles qui ont été créées avec UFW ne seront plus actives.   
il est toujours d'exécuter la commande  
**>> sudo** **ufw enable**

Si vous on a configuré des règles UFW mais que l’on décide de recommencer depuis le début, on peut utiliser la commande reset …  
**>> sudo** **ufw reset**

Cette commande désactivera UFW et supprimera toutes les règles précédemment définies.

## Interface graphique

Si on ne souhaite pas gérer son pare-feu via la ligne de commande, une interface utilisateur graphique est disponible pour UFW appelée GUFW.   
On peut l'installer à l’aide du gestionnaire de paquets en recherchant gufw ou on peut exécuter la commande suivante depuis le terminal …  
**>> sudo apt install gufw**