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

Le pare-feu non compliqué (ufw et gufw - une version de l'interface utilisateur graphique) est une interface qui vise à simplifier le processus de configuration du pare-feu iptables. UFW est particulièrement bien adapté aux pares-feux basés sur l'hôte.

Bien iptables est un outil solide et flexible, il peut être difficile pour les débutants d'apprendre à l'utiliser pour configurer correctement un pare-feu.   
Si on cherche un bon point de départ pour sécuriser un réseau et on ne sait pas quel outil utiliser, UFW peut être un bon choix.

UFW fournit un cadre pour la gestion de netfilter, ainsi qu'une interface de ligne de commande pour manipuler le pare‑feu.

## 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

Si on débute avec un pare-feu, les premières règles à définir sont les politiques par défaut.   
Ces règles contrôlent la manière de gérer le trafic qui ne correspond explicitement à aucune autre règle.

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**

Ces commandes définissent les valeurs par défaut pour refuser les connexions entrantes et autoriser les connexions sortantes. Ces valeurs par défaut du pare-feu peuvent suffire à elles seules pour un ordinateur personnel, mais les serveurs doivent généralement répondre aux demandes entrantes d'utilisateurs externes

## Autorisation des connexions SSH

Si pare-feu UFW est activé maintenant, il refuserait toutes les connexions entrantes.

Cela signifie qu’il faut créer des règles qui autorisent explicitement les connexions entrantes légitimes - les connexions SSH ou HTTP, par exemple - si on souhaite que le serveur réponde à ces types de requêtes.

Si on utilise un serveur dans le nuage, il est souhaitable d’autoriser les connexions SSH entrantes afin de pouvoir se connecter et gérer le serveur.

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

Cette commande va créer une règle de pare-feu qui autorisera toutes les connexions sur le port 22, qui est le port sur lequel le démon SSH écoute par défaut.   
UFW sait ce que allow ssh signifie le port 22 car il est répertorié en tant que service dans le fichier /etc/services.

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**

Maintenant que le pare-feu est configuré pour autoriser les connexions SSH entrantes, il faut l'activer.

## Activation de l'UFW

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

**Remarque** …  
UFW affiche un avertissement indiquant que la commande peut perturber les connexions SSH existantes.   
Une règle de pare-feu est déjà mise en place qui autorise les connexions SSH, donc cela devrait aller pour continuer.

Le pare-feu est maintenant actif.

Pour voir les règles définies, on peut exécuter la commande …  
**>> sudo** **ufw status verbose  
Logging: on (low)  
Default: deny (incoming), allow (outgoing), disabled (routed)  
New profiles: skip  
To Action From  
-- ------ ----  
22/tcp ALLOW IN Anywhere  
1000:2000/tcp ALLOW IN Anywhere  
1000:2000/udp ALLOW IN Anywhere  
Anywhere ALLOW IN 192.168.1.104  
22/tcp (v6) ALLOW IN Anywhere (v6)  
1000:2000/tcp (v6) ALLOW IN Anywhere (v6)  
1000:2000/udp (v6) ALLOW IN Anywhere (v6)**

## Autorisation pour d'autres connexions

On doit autoriser toutes les autres connexions auxquelles le serveur doit répondre.   
Les connexions que l’on doit autoriser dépendent de ses besoins spécifiques.   
Une règle a été écrite pour l’autorisation des connexions en fonction d'un nom de service ou d'un port – SSH et lem port 22.

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**

Il existe plusieurs autres façons d'autoriser d'autres connexions, en plus de spécifier un port ou un service connu.

## 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**

Lors de la spécification des étendues de ports avec UFW, on doit spécifier le protocole (tcp ou udp) auquel les règles doivent s'appliquer.

**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 eth1 to any port 3306**

## Refus de connexions

Si la stratégie par défaut n’a pas été modifiée pour les connexions entrantes, UFW est configuré pour refuser toutes les connexions entrantes.   
En général, cela simplifie le processus de création d'une stratégie de pare-feu sécurisée en obligeant l’administrateur créer des règles qui autorisent explicitement le passage de ports et d'adresses IP spécifiques.

Cependant, on pourrait refuser des connexions spécifiques en fonction de l'adresse IP ou du sous-réseau source, afin de prévenir des attaques sur le serveur.   
De plus, si on aimerait modifier sa stratégie entrante par défaut pour tout autoriser (ce qui n'est pas recommandé), il faut créer des règles de refus pour tous les services ou adresses IP pour lesquelles on ne souhaite pas autoriser les 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

Savoir supprimer des règles de pare-feu est tout aussi important que savoir comment les créer.   
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  
Status: active  
 To Action From  
 -- ------ ----  
[ 1] 22/tcp ALLOW IN Anywhere  
[ 2] 80/tcp ALLOW IN Anywhere   
[ 3] 1000:2000/tcp ALLOW IN Anywhere   
[ 4] 1000:2000/udp ALLOW IN Anywhere  
[ 5] Anywhere ALLOW IN 192.168.1.100  
[ 5] 22/tcp (v6) ALLOW IN Anywhere (v6)  
[ 7] 1000:2000/tcp (v6) ALLOW IN Anywhere (v6)  
[ 8] 1000:2000/udp (v6) ALLOW IN Anywhere (v6)**

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 …  
**Status: inactive**

Sinon …  
**>> sudo** **ufw status verbose  
Logging: on (low)  
Default: deny (incoming), allow (outgoing), disabled (routed)  
New profiles: skip  
To Action From  
-- ------ ----  
22/tcp ALLOW IN Anywhere  
1000:2000/tcp ALLOW IN Anywhere  
1000:2000/udp ALLOW IN Anywhere  
Anywhere ALLOW IN 192.168.1.104  
22/tcp (v6) ALLOW IN Anywhere (v6)  
1000:2000/tcp (v6) ALLOW IN Anywhere (v6)  
1000:2000/udp (v6) ALLOW IN Anywhere (v6)**

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.

**Remarque** …  
Les stratégies par défaut ne seront pas revenues à leurs paramètres d'origine, si elles ont été modifiées à un moment donné.   
Cela donne donner un nouveau départ avec UFW.

## 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**