Le contenu est disponible sous licence GNU Free Documentation License 1.3 ou ultérieure sauf mention contraire.

Uncomplicated FireWall

Le contenu est disponible sous licence GNU Free Documentation License 1.3 ou ultérieure sauf mention contraire.

Introduction & Démystification

Qu'est-ce que UFW ?

UFW signifie *Uncomplicated FireWall*.

Mais attention aux apparences : UFW n'est pas un "pare-feu" au sens strict. C'est une **interface de commande (Frontend)**.

- **Le Moteur (Le Vrai Chef)** : C'est **Netfilter** (intégré au noyau Linux).
- **Le Traducteur (UFW)** : Quand tu tapes une commande UFW, il la traduit instantanément en règles complexes pour iptables ou nftables (le backend moderne).

Le Mythe de la "Simplicité"

Il existe une rumeur tenace chez les "Barbus du SysAdmin" (et apparemment chez certains professeurs) : *« UFW est simpliste et moins capable que iptables. »*

C'est techniquement faux.

UFW manipule le **même** moteur de sécurité que les autres. Un port fermé par UFW est tout aussi fermé que s'il l'était par une commande nftables de trois lignes. La différence ? UFW privilégie la lisibilité humaine à l'obscurité syntaxique.

> **Note :** Dire que UFW est "moins capable", c'est comme dire qu'écrire en C++ est "moins capable" que d'écrire en Assembleur.

Comparatif de la Douleur

La preuve par l'exemple. Voici la même action (Autoriser le SSH uniquement pour le réseau local 192.168.1.0/24) :

Outil	Commande (Syntaxe)	Verdict
UFW	ufw allow from 192.168.1.0/24 to any port 22	**Clean.** Lisible par un humain normal. On comprend l'intention immédiatement.
IPTABLES	iptables -A INPUT -p tcp -s 192.168.1.0/24 --dport 22 -j ACCEPT	**Rétro.** Efficace, mais si tu oublies le -A ou le -j, tu pleures.
NFTABLES	nft add rule ip filter input ip saddr 192.168.1.0/24 tcp dport 22 accept	**Verbeux.** Très puissant pour le scripting complexe, mais overkill pour ouvrir un port.

> **Conclusion :** UFW n'est pas "limité". C'est un *wrapper* intelligent. Il permet des règles complexes (limit rate, routing, interfaces spécifiques) tout en gardant une syntaxe qui évite l'erreur humaine (la cause n°1 des piratages).

Le contenu est disponible sous licence GNU Free Documentation License 1.3 ou ultérieure sauf mention contraire.

GESTION DE Uncomplicated FireWall

L'Audit (Voir ce qui se passe)

Avant de supprimer quoi que ce soit, il faut observer. On ne coupe pas le fil rouge sans vérifier s'il est relié à la bombe ou à la machine à café.

Commande	Description	Note
sudo ufw status	État basique	"Actif" ou "Inactif". Le minimum syndical.
sudo ufw status verbose	État détaillé	Affiche le logging et les politiques par défaut (Drop/Reject). Utile pour l'audit de sécu.
sudo ufw status numbered	La plus importante	Affiche les règles avec un **numéro d'index** [1], [2]... Indispensable pour la chirurgie.

L'Analogie : Utilise toujours numbered. Sans les numéros, tu es comme Neo aveugle dans le troisième film : tu agis au pifomètre.

Le Journal de Bord (LOGGING)

Quand ça ne marche pas, ou quand tu suspectes une attaque, tu as besoin de preuves. UFW est bavard, mais seulement si tu lui demandes.

Commande	Description	Note
sudo ufw logging on	Active les logs (Niveau Low par défaut).	**Vital.** Sans ça, tu es sourd et aveugle.
sudo ufw logging medium	Log aussi les paquets invalides/nouveaux non conformes.	Utile si tu suspectes du spoofing ou une attaque bizarre.
sudo ufw logging off	Coupe le sifflet au firewall.	À utiliser uniquement si ton disque dur est plein à craquer (ou pour cacher des preuves...).

Où sont les preuves ? Les logs atterrissent généralement dans /var/log/ufw.log ou via la commande dmesg.

> **Note :** *"Dans l'espace, personne ne vous entend crier. Mais sous Linux, /var/log entend tout."*

Le contenu est disponible sous licence GNU Free Documentation License 1.3 ou ultérieure sauf mention contraire.

L'ÉCRITURE DES RÈGLES (De la truelle au scalpel)

Dans UFW, il y a plusieurs façons de demander la même chose. C'est la différence entre dire "Oouvre la porte !" et "Ouvre le sas numéro 4 pour le personnel autorisé uniquement".

Tableau des niveaux de précision :

Niveau	Syntaxe de la commande	Commentaire
Niveau 1 (Le Touriste)	sudo ufw allow 80	**Bourrin.** Tu ouvres le port 80 en TCP *et* UDP pour *toute la planète*. C'est ce que le prof appelle "simpliste", et il a raison. C'est la truelle.
Niveau 2 (L'Admin Junior)	sudo ufw allow 80/tcp	**Mieux.** Tu spécifies au moins le protocole. On évite d'ouvrir l'UDP inutilement. C'est le minimum syndical pour ne pas passer pour un amateur.
Niveau 3 (Le Standard)	sudo ufw allow from 192.168.1.0/24 to any port 80 proto tcp	**Sérieux.** Là on parle. On définit la source (le réseau Admin), la destination et le protocole. C'est précis, c'est propre.
Niveau 4 (Le Paranoïaque)	sudo ufw limit http	**Gandalf Style.** "Vous ne passerez pas... trop vite". UFW bloque l'IP si elle tente plus de 6 connexions en 30 secondes. Protection anti-bruteforce native.

Niveau 5 : Si le server à plusieurs carte réseaux (ex: une carte eth0 reliée à Internet et une eth1 reliée au réseau admin sécurisé). Et que tu ne veux surtout pas que le port SSH soit ouvert sur la carte Internet !

```
sudo ufw allow in on eth1 proto tcp to any port 22 comment 'SSH LAN Only'
```

Si un pirate attaque sur eth0 (Internet), la règle est ignorée -> Accès Refusé.

> **Note :** C'est comme avoir une porte blindée côté rue, et une porte ouverte côté jardin. Si tu dis juste "Ouvre la porte", tu ouvres les deux. Précise toujours *quelle* porte.

LA SYNTAXE ULTIME (la "Mona Lisa" des règles de pare-feu)

Cette syntaxe permet de tout définir en une ligne, commentaire inclus pour l'auditabilité.

```
sudo ufw allow in on eth1 proto tcp from 192.168.139.0/24 to any port 80 comment 'HTTP LAN Only'
```

Décomposition anatomique :

# in on eth1	La règle ne s'applique QUE si le câble est branché sur la carte eth1
# proto tcp	On verrouille le protocole (pas d'UDP accidentel)
# from 192.168.139.0/24	Seul le réseau de confiance a le droit de toquer à la porte
# to any	Vers n'importe quelle interface du serveur (on peut remplacer any par l'IP précise du serveur si on veut être psycho-rigide)
# port 80	Le port d'écoute (classique)
# comment '…'	**Vital.** Quand tu feras un status dans 6 mois, tu me remercieras de savoir *pourquoi* cette règle existe

Le contenu est disponible sous licence GNU Free Documentation License 1.3 ou ultérieure sauf mention contraire.

La Suppression (L'Élagage)

Il y a deux écoles pour supprimer une règle. Celle du chirurgien et celle du bibliothécaire.

La Chirurgicale (Par Numéro)

C'est la méthode la plus rapide, mais elle demande de la concentration.

- Affiche les numéros :

```
sudo ufw status numbered
```

- Supprime la règle numéro X (disons la 4) :

```
sudo ufw delete 4
```

⚠ **Avertissement :** Attention, quand tu supprimes la règle [4], la règle [5] devient la nouvelle [4]. Les numéros se décalent vers le haut immédiatement. Si tu veux supprimer la 4 et la 5, supprime la 4, **revérifie les numéros**, puis supprime la nouvelle 4. Ne fais pas "delete 4" puis "delete 5" à l'aveugle, sinon tu vas couper la mauvaise racine.

> **Note :** "Supprimer une règle par numéro sans revérifier la liste après chaque suppression, c'est comme jouer au Démineur en cliquant au hasard. Ça finit mal."

La Bibliothécaire (Par Règle Explicite)

C'est la méthode verbeuse. Elle est plus sûre car elle ne dépend pas de l'ordre des lignes. Si la règle change de numéro, la commande fonctionnera quand même. Le principe est simple : on reprend la commande de création, et on insère delete après ufw.

Supprimer une règle simple (ex: allow 80/tcp) :

```
sudo ufw delete allow 80/tcp
```

Supprimer une règle complexe (notre Mona Lisa) :

```
sudo ufw delete allow in on eth1 proto tcp from 192.168.139.0/24 to any port 80 comment 'HTTP LAN Only'
```

> **Note :** "C'est la méthode idéale pour les scripts ou les paranoïaques. Contrairement à la méthode par numéro, ici pas de 'Roulette Russe'. Si la règle n'existe pas, UFW te dira simplement qu'il ne trouve rien, au lieu de supprimer un truc au hasard."

Le contenu est disponible sous licence GNU Free Documentation License 1.3 ou ultérieure sauf mention contraire.

La Réinitialisation (Le "Reboot" Tactique)

Tu as fait n'importe quoi ? Tu as ouvert plus de ports qu'un bar à marins un samedi soir ? Tu veux tout raser et recommencer proprement ?

La commande de la Terre Brûlée :

```
sudo ufw reset
```

Effet : Désactive UFW, supprime **toutes** les règles actives et remet tout à zéro (par défaut : tout bloquer en entrée).

Note : Il te demandera confirmation. C'est le moment de vérifier que tu as bien un accès physique ou console à ATLAS, car si tu fais ça à distance sans remettre le SSH immédiatement derrière... *Game Over*.

Recharger la Matrice

Parfois, UFW boude. Si tu modifies des fichiers de configuration à la main (dans /etc/ufw/), les changements ne sont pas immédiats.

```
sudo ufw reload
```

Ça recharge les règles sans couper les connexions actives (normalement). C'est le *soft reset*.

Le contenu est disponible sous licence GNU Free Documentation License 1.3 ou ultérieure sauf mention contraire.

Installation de UFW

```
user@lab-debian-24:~$ sudo apt install ufw
```

Définitions des règles par défault (On ferme tout en entrée, on laisse tout sortir)

```
user@lab-debian-24:~$ sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
user@lab-debian-24:~$ sudo ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
```

Autorisation du port SSH

```
user@lab-debian-24:~$ sudo ufw allow proto tcp from 192.168.1.0/24 to any port 22 comment 'SSH LAN Only'
Rules updated
Rules updated (v6)
```

Activation du FireWall (c’est le moment de prier!)

```
user@lab-debian-24:~$ sudo ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
```

Vérification

```
user@lab-debian-24:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
80/tcp                     ALLOW IN    192.168.1.0/24             # HTTP LAN ONLY
22/tcp                     ALLOW IN    192.168.1.0/24             # SSH LAN ONLY
```