

Ufw sur Raspberry Pi : Installer un pare-feu

Un pare-feu bloque tous les ports sauf ceux utiles et filtre les accès par adresse IP

ufw (Uncomplicated Fire Wall) est une interface simple pour gérer le pare-feu iptables installé par défaut sur le système d'exploitation Raspberry Pi.

Pré-requis

Installation

- **Installez ufw** et son interface graphique **gufw** sur votre Raspberry Pi :

```
pi@framboise:~ $ sudo apt install ufw gufw
```

- **Autorisez les accès** HTTP, HTTPS et SSH pour tout le monde :

```
pi@framboise:~ $ sudo ufw allow http
pi@framboise:~ $ sudo ufw allow https
pi@framboise:~ $ sudo ufw allow ssh
```

- **Activez le pare-feu :**

```
pi@framboise:~ $ sudo ufw enable
```

Attention, cela l'active aussi au redémarrage du Raspberry Pi.

Si vous perdez la connexion maintenant, vous ne pourrez plus continuer avec un accès distant, même en redémarrant.

Il faudra vous connecter physiquement au Raspberry Pi pour désactiver ufw ou changer la configuration.

D'où la nécessité d'autoriser SSH.

Si par malheur cela arrivait,



1. éteignez votre Raspberry Pi
2. retirez la carte µSD et placez dans un lecteur sur un PC
3. Dans `/media/USER/rootfs/etc/ufw/ufw.conf`, mettez **ENABLED=no**

</media/USER/rootfs/etc/ufw/ufw.conf>



```
# Set to yes to start on boot.  
If setting this remotely, be  
sure to add a rule  
# to allow your remote  
connection before starting ufw.  
Eg: 'ufw allow 22/tcp'  
ENABLED=no
```

- **Vérifiez** que tout est ok avant de continuer :

```
pi@framboise:~ $ sudo ufw status  
Status: active
```

To	Action	From
--	-----	----
80	ALLOW	Anywhere
443	ALLOW	Anywhere
22/tcp	ALLOW	Anywhere
80 (v6)	ALLOW	Anywhere (v6)
443 (v6)	ALLOW	Anywhere (v6)
22/tcp (v6)	ALLOW	Anywhere (v6)

Configuration

Utilisation

Ce document décrit quelques-unes des options de base de la ligne de commande.

Il est également possible d'utiliser pour toutes les commandes ufw l'option **-dry-run**, qui montre les résultats de la commande sans faire de modification.

- **activer ou désactiver le pare-feu :**
 - **activer le pare-feu et le lancer au redémarrage :**

```
pi@framboise:~ $ sudo ufw enable
```

- **désactiver le pare-feu et ne pas le lancer au démarrage :**

```
pi@framboise:~ $ sudo ufw disable
```

- **ports**

- **Autoriser l'accès à un port** (le port 22 dans notre exemple) :

```
pi@framboise:~ $ sudo ufw allow 22
```

- **Refuser l'accès à un port** (encore le port 22 dans notre exemple):

```
pi@framboise:~ $ sudo ufw deny 22
```

- **service :**

- Vous pouvez également spécifier le **service** que vous autorisez ou refusez sur un port. Dans cet exemple, nous refusons tcp sur le port 22 :

```
pi@framboise:~ $ sudo ufw deny 22/tcp
```

- Vous pouvez **spécifier le service** (ssh, http, https ...) même si vous ne savez pas quel port il utilise. Cet exemple permet l'accès au service ssh via le pare-feu :

```
pi@framboise:~ $ sudo ufw allow ssh
```

- **status**

- **status** répertorie tous les paramètres actuels du pare-feu :

```
pi@framboise:~ $ sudo ufw status
Status: active
```

To	Action	From
--	-----	----
80	ALLOW	Anywhere
443	ALLOW	Anywhere
22/tcp	ALLOW	Anywhere
80 (v6)	ALLOW	Anywhere (v6)
443 (v6)	ALLOW	Anywhere (v6)
22/tcp (v6)	ALLOW	Anywhere (v6)

- **status numbered** id avec les numéros des filtres :

```
pi@framboise:~ $ sudo ufw status numbered
Status: active
```

To	Action	From
--	-----	----
[1] 80	ALLOW IN	Anywhere
[2] 443	ALLOW IN	Anywhere
[3] 22/tcp	ALLOW IN	Anywhere
[4] 80 (v6)	ALLOW IN	Anywhere (v6)
[5] 443 (v6)	ALLOW IN	Anywhere (v6)

[6] 22/tcp (v6)

ALLOW IN

Anywhere (v6)

Désinstallation

Voir aussi

- (fr) <https://raspberrytips.fr/securiser-raspberry-pi/>

Basé sur « [17 Conseils pour Sécuriser votre Raspberry Pi comme un Pro](#) » par Patrick Fromaget.

From:

<http://doc.nfrappe.fr/> - **Documentation du Dr Nicolas Frappé**

Permanent link:

<http://doc.nfrappe.fr/doku.php?id=logiciel:internet:ufw:raspi:start>



Last update: **2022/11/08 19:28**