Port Knocking

Cela permet de bloquer l'accès au réel port SSH à moins qu'une séquence spécifique de ports ne soit "knock". Ce n'est qu'à ce moment que les règles iptables permettront au port SSH d'être ouvert à l'adresse IP de celui qui aura knock cette séquence de port.

Pour utiliser UFW à la place des iptables allez directement à la fin ! (UFW)

1 - Installation des packages requis

Commençons par installer le service requis:

```
apt-get install knockd
```

Vous aurez peut être besoin d'installer le package `iptables-persistent`. Il permet de charger de manière automatique les règles `iptables` sauvegardées.

```
apt-get install iptables-persistent


# Save current IPv4 rules ? YES
# Save current IPv6 rules ? YES
```

2-Configuration avec IPTABLES

Avant de mettre en marche knockd nous allons modifier certains paramètres par défauts.
Editons le fichier de configuration:

```
nano /etc/knockd.conf
```

Modifiez ou supprimez ce qui s'y trouve afin de mettre les settings suivantes:

```
[options]
        UseSyslog

[openSSH]
        sequence    = 1555,8888,5555
        seq_timeout = 5
        command     = /sbin/iptables -I INPUT -s %IP% -p tcp --dport 22 -j ACCEPT
        tcpflags    = syn
```

```
        cmd_timeout = 15
        stop_command = /sbin/iptables -D INPUT -s %IP% -p tcp --dport 22 -j ACCEPT
```

- `sequence` correspond à la séquence de port à knock dans les 5 secondes.
- `seq_timeout` le temps imparti pour knock les ports
- `command` la commande exécuté pour ouvrir le port ssh à notre IP, Soyez sûr de bien remplacer 22 par votre port SSH.
- `tcpflags` Spécifie qu'il n'acceptera que des segments tcp
- `cmd_timeout` le temps avant que notre IP soit supprimé des iptables, ici, 15 secondes. Cela ne nous déconnectera pas de la session SSH une fois connectée mais préviendra de vous connecter sans knock les ports spécifiés.
- `stop_command` La commande pour supprimer l'accès au port SSH via votre adresse IP. Soyez sûr de bien remplacer 22 par votre port SSH.

Continuons en rajoutant une règle *iptables* afin que les personnes connectées en SSH ne soit pas déconnectées:

```
iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
```

Puis fermons l'accès au port SSH **(Remplacez 22 par le votre)**:

```
iptables -A INPUT -p tcp --dport 22 -j REJECT
```

Démarrons le daemon `netfilter-persistent` associé avec iptables et faisons en sorte qu'il sauvegarde nos règles iptables:

```
systemctl start netfilter-persistent
netfilter-persistent save
netfilter-persistent reload
```

(`sudo netfilter-persistent save` à utiliser à chaque changement de votre firewall que vous voulez sauvegarder)

3 - Mise en route de Knockd

Continuez en allant modifier le fichier `/etc/default/knockd` et mettez `START_KNOCKD` égal à 1.
NB: Vous aurez peut être besoin de changer la command line options afin de mettre le nom de votre interface réseau. Vous pouvez le savoir en tapant "ip addr" par défaut eth1
Redémarrez ensuite knockd `systemctl start knockd`.

Pour vous connectez depuis linux il vous suffit d'installer knockd comme précédemment et d'utiliser la commande:

```
knock -v IP PORT1 PORT2 PORT3 ...
```

Afin d'ouvrir le port SSH. Sous windows vous trouverez de nombreux projets de port knocking disponible sur github facilement installable. Comme: `https://github.com/BetterWayElectronics/port-knocker/releases/tag/1.0` pour le moment (compilez le vous même, on sait jamais).

Pour voir de l'intérieur ce que cela donne une fois que vous avec knock votre port vous pouvez utiliser:

```
tail -f /var/log/syslog
```

(PLEASE READ ME !)- Knockd Bug Not Starting at Boot

Il est probable sur certaines versions de debian comme la 9 (ça m'ai arrivé sur la 11 également □□) que knockd ne redémarre pas au reboot ce qui peut être TRES problèmatique sur un serveur remote. Si cela arrive vous pourrez sûrement vous connecter via la console en ligne de votre host provider.

Pour éviter que cela ce produise vous pouvez réaliser ces étapes:

Identifiez si nous avons le problème:

```
systemctl is-enabled knockd.service
```

cela nous retournera alors `static` !

Pour fix vous allez ensuite ajouter une section [Install] dans le fichier `/lib/systemd/system/knockd.service`:

```
nano /lib/systemd/system/knockd.service
```

Puis rajoutez à la fin:

```
[Install]
WantedBy=multi-user.target
Alias=knockd.service
```

Sauvegardez et activez knockd au démarrage:

```
systemctl enable knockd.service
```

Si vous relancez la commande `systemctl is-enabled knockd.service` vous devriez cette fois avoir la réponse `enabled` !

Hop le tour est joué !

Solutions issu de: https://bugs.debian.org

(UFW) - Si vous utilisez UFW (Ignore this if you used iptables)

Si vous utilisez UFW rien de plus simple commencez par installer le service `knockd`

```
apt-get install knockd
```

Editez le fichier de configuration de la manière suivante:

```
nano /etc/knockd.conf
```

Modifiez ou supprimez ce qui s'y trouve afin de mettre les settings suivantes et remplacez le port 22 par votre port SSH pour la signification des settings remontez à la section **2-Configuration avec IPTABLES**:

```
[options]
        UseSyslog

[openSSH]
        sequence    = 1555,8888,5555
        seq_timeout = 5
        command     = ufw allow from %IP% to any port 22
        tcpflags    = syn
        cmd_timeout = 15
        stop_command = ufw delete allow from %IP% to any port 22
```

Supprimez toute règle déjà mise en place autorisant le traffic depuis votre port SSH. Ces dernières seront gérés directement par UFW.
Puis fermez votre port SSH *(Remplacer 22 par votre port SSH)*.

```
ufw insert 1 deny from any to any port 22
```

Continuez à partir de la section **3- Mise en route de Knockd** !

et voilà :) si jamais n'hésitez pas à me contacter par discord ou mail *(disponible sur mon site)* :)

Revision #6
Created 2021-10-23 08:58:39 UTC by Faces
Updated 2022-06-10 17:50:40 UTC by Faces