# Netfilter

Installation du paquet qui ajoute un script de démarrage/flush iptables et qui génère un fichier de config par défaut à la base de ce qui est en place au moment de l'installation.

```
apt install netfilter-persistent ulogd2
```

Créer ensuite le fichier `/etc/iptables/rules.v4` avec la syntaxe de la commande iptables-save.

Créer ses propres règles en commande et ensuite enregistrer la configuration.

```
iptables-save > /etc/iptables/rules.v4
ip6tables-save > /etc/iptables/rules.v6
```

```
systemctl status netfilter-persistent
systemctl status ulogd
systemctl start netfilter-persistent
systemctl enable netfilter-persistent
systemctl enable ulogd
```

Pour voir la liste des extensions utilisables avec l'option `-j`.

```
man iptables-extensions
```

Avec ulogd2, il faut utiliser la chaine -j NFLOG –nflog-prefix.

Le log spécifique pour observer les drop des règles de filtrage est par défaut ici :

```
/var/log/ulog/syslogemu.log
```

Pour flusher la configuration au stop, il faut lui indiquer sinon par défaut, les règles persistent à l'arrêt du service. vi /etc/default/netfilter-persistent

```
FLUSH_ON_STOP=1
```

Redémarrer le service pour prendre en compte le fichier et ensuite on peut restoper.

## Deprecated Solution avec script perso

Création d'un script de démarrage sysV qui appel un script pour positionner les règles lors du start et un autre pour les effacer lors du stop.

Création/récupération des trois fichiers suivants.

```
/etc/init.d/iptables
/etc/security/iptables.sh
```

```
/etc/security/flush_iptables.sh
```

Position des permissions.

```
chmod 700 /etc/security/iptables.sh
chmod 700 /etc/security/flush_iptables.sh
chmod 700 /etc/init.d/iptables
```

Positionner le service iptables au lancement de la machine.

```
insserv -n iptables  (-n = dry run)
insserv iptables
ll /etc/rc2.d
```

## Sous RHEL 6

Accès FTP

Sauvegarder les fichiers Netfilter par défaut.

```
cd /etc/sysconfig
cp -p iptables iptables.orig
cp -p iptables-config iptables-config.orig
```

Charger le module ip_conntrack_ftp pour activer le suivi de connexion et rendre la configuration Netfilter statefull.

```
vi /etc/sysconfig/iptables-config

IPTABLES_MODULES="ip_conntrack_ftp"
```

Ajouter une ligne supplémentaire pour autoriser les accès FTP.

```
vi /etc/sysconfig/iptables

-A INPUT -m state --state NEW -m tcp -p tcp --dport 21 -j ACCEPT
```

Relancer iptables.

```
/etc/init.d/iptables restart
```