

0.1 [Iptables] Bloquer les IP de la RIAA

0.1.1 1. Introduction :

Le but est d'utiliser les listes d'ip de la RIAA¹ (Recording Industry Association of America) et ses copains pour établir des règles de firewall sous Linux, grâce à "iptables". Il existe à ma connaissance au moins 2 listes de ce genre : Peer Guardian et ipprefix. Il y a 2 étapes. La première est de récupérer la version cvs de iptables . En effet, la version actuelle sur les distributions est la 1.2.7, permet de filtrer sur des réseaux tels que 192.168.1.0/24, mais pas par exemple 192.168.1.12 a 192.168.1.56. Le module permettant ça est "iprange" . Syntaxe :

```
iptables -A INPUT -m iprange --src-range 192.168.1.12-192.168.1.56 -j REJECT
```

Les 2 valeurs extrêmes sont comprises dans la règle . Pour les généralités sur iptables, cf la doc par exemple sur Iptables². La seconde étape est de mettre les plages d'ip récupérées sur les sites de Peer Guardian et de ipprefix au format attendu par iprange. En effet ce module est assez pointilleux la dessus, et n'interprète pas de la même manière 010.102.052.000 que 10.102.52.0 ... Et bien évidemment les listes sont dans le format 000.000 .. Je n'ai fait pour le moment qu'un script de conversion pour ipprefix. C'est très certainement perfectible, mes compétences en shell sont essentiellement la lecture du "Advanced Bash-Scripting Guide"³, tuto bash⁴. Si quelqu'un voit des améliorations, je suis évidemment preneur. La conversion dure un certain temps, c'est normal. Il y a environ 2000 plages à traiter. Je ferai un script de conversion pour les listes de Peer Guardian, à moins que quelqu'un ne se dévoue avant. Voici ma méthode, qui n'engage que moi elle aussi, testée sans problème sur une Debian fraîchement installée =. Je n'ai pas testé sur Mandriva, j'ai toujours eu des soucis à retrouver un automount après compil ...

0.1.2 2. Installation de la version CVS de Iptables :

Récupération de iptables 1.2.8 cvs :

```
cvs -d :pserver :cvs@pserver.netfilter.org :/cvspublic login
```

(quand on vous demande un mot de passe, tapez 'cvs').

```
cvs -d :pserver :cvs@pserver.netfilter.org :/cvspublic co netfilter/userspace netfilter/patch-o-matic
```

J'ai du m'y reprendre à 2 fois pour me logguer Pour compiler iptables, on va avoir besoin des sources du noyau :

– Version Debian :

```
apt-get install kernel-source-2.4.18
cd /usr/src/
bunzip2 kernel-source-2.4.18.tar.bz2
tar xvf kernel-source-2.4.18.tar
ln -s kernel-source-2.4.18 linux
```

– Version Mandriva :

¹<http://www.riaa.com/>

²<http://www.netfilter.org>

³<http://library.psyon.org/os/linux/abs-guide/>

⁴<http://www.truostonme.net/didactels/148.html>

- ```

urpmi kernel-source
urpmi kernel-header

```
- Version Red Hat :

```

cd /où_se_trouve_kernel_source_sur_le_cdrom
rpm -Uvh kernel-source

```
  - Version Slackware :

```

installpkg /mnt/cdrom/slackware/d/kernel-headers-x.x.xx-xxxx-x.tgz
installpkg /mnt/cdrom/slackware/k/kernel-source-x.x.xx-noarch-x.tgz

```

Appliquez le patch base/iprange

```

cd netfilter/patch-o-matic
./runme base

```

Là, lisez, c'est écrit.

```

cd ../netfilter/userspace
make

```

Pas de souci particulier après compilation, donc je désinstalle le iptables de la Debian.

```

apt-get remove iptables
make install

```

À ce stade, il faut refaire un kernel et cocher IP range match support dans la config de netfilter. En cas de soucis, on trouve plein de doc sur ce sujet. Par exemple ici : [Trustonme](#)<sup>5</sup>.

### 0.1.3 3. Utilisation de la liste de ipprefix :

Utiliser le script `ipprefix2iptables.sh`<sup>6</sup>. Syntaxe :

```

ipprefix2iptables.sh URL FICHER_DE_SORTIE

```

L'url à passer en paramètre est celle de la page <http://cvs.suche.org/horde/chora/cvs.php/ip.prefix><sup>7</sup> sur le site ( clic droit, copier l'adresse du lien ). Le fichier de sortie est ce que vous voulez, il sera utilisé plus tard par le script de firewall lui même. On a au resultat ceci :

#### **Plage\_IP chiffre Commentaire**

```

1.0.0.0-1.255.255.255 011 InternetAssignedNumbersAuthority
2.0.0.0-2.255.255.255 011 InternetAssignedNumbersAuthority
3.0.0.0-3.255.255.255 120 GeneralElectricCompany
4.3.58.0-4.3.58.255 200 GTEIntelligentNetworkServices
4.35.12.0-4.35.15.255 200 dsl genuity net
4.43.96.0-4.43.96.255 000 MediaForce(P2Pmonitoring)(valid)
4.43.96.0-4.43.96.255 000 MediaForce

```

Je n'ai pas trop cherché à savoir la signification du chiffre. Veuillez à vérifier que le fichier de sortie est valide, il faudra certainement ajouter des tests pour ceci. Pour être vraiment complet sur le sujet, je signale que [8](#), a fait un script perl `ipdb2iptables.pl`<sup>9</sup>. Ce script est analogue à `ipprefix2iptables.sh`, avec l'avantage d'utiliser les listes de Peer Guardian et d'`ipprefix`.

<sup>5</sup> [?id=35](#)

<sup>6</sup> <http://file.trustonme.net/data/ipprefix2iptables.sh>

<sup>7</sup> <http://cvs.suche.org/horde/chora/cvs.php/ip.prefix>

<sup>8</sup> [pistolero@toursombre.dyndns.org](mailto:pistolero@toursombre.dyndns.org)

<sup>9</sup> <http://www.trustonme.net/didactels/downloads/ipdb2iptables.pl>

#### 0.1.4 4. Mise en place du filtrage :

Ci joint le script `firewall_riaa.sh`<sup>10</sup>, en complément bien sur d'un firewall "normal".  
Utilisation :

```
firewall_riaa.sh {start|stop|restart|status}
```

Il faut lui spécifier le fichier d'entrée en l'éditant :

```
blacklist=votre_fichier_de_blacklist
```

Pour un démarrage automatique, il suffit de mettre ça dans un `rc.local` quelconque. Les erreurs du genre "iptables v1.2.8 : iprange match : Bad IP address XXX" peuvent arriver, j'ai eu certaines plages d'adresses invalides sur le site de `ipprefix`. Elles ne sont pas prises en compte, mais ça n'a pas d'autre influence. Le lancement est un peu long, vu la longue liste, mais je n'ai pas remarqué de ralentissement notable, la machine qui fait fonctionner ça est un petit k6-2 à 240 Mhz environ, avec 128 Mo EDO.

---

<sup>10</sup>[http://file.trustonme.net/data/firewall\\_riaa.sh](http://file.trustonme.net/data/firewall_riaa.sh)