Wikiprint Book

Title: Iptables

Subject: TracMeteo - SshSecuring

Version: 8

Date: 05/17/2022 07:29:28 AM

Table of Contents

Iptables

```
#configuracion actual
iptables -L -v --line-numbers
#Borrar una regla por nº de linea
iptable -D INPUT 1
```

- Las reglas que se crean con iptables se almacenan en memoria, para salvarlas para el siguiente reinicio **service iptables save**, en caso de editar directamente **/etc/sysconfig/iptables** primero reiniciar el servicio y despues save.
- Para mover reglas a otro equipo copiar **/etc/sysconfig/iptables** y reiniciar /sbin/service iptables restart

```
[root@spock sysconfig]# ls -Z iptables
-rw-------. root root unconfined_u:object_r:admin_home_t:s0 iptables
[root@spock sysconfig]# ls -Z iptables.orig
-rw-------. root root system_u:object_r:system_conf_t:s0 iptables.orig
#Al copiar de otro equipo hay que tener en cuenta seLInux
[root@spock sysconfig]# restorecon -v /etc/sysconfig/iptables
restorecon reset /etc/sysconfig/iptables context unconfined_u:object_r:admin_home_t:s0->unconfined_u:object_r:system_conf_
```

Reglas añadidas para ssh

```
 iptables -A INPUT -i eth1 -s 192.168.202.0/24 -p tcp --dport 22 -j ACCEPT
iptables -A INPUT -i eth0 -s 193.144.202.0/24 -p tcp --dport 22 -j ACCEPT
```

?https://wiki.centos.org/HowTos/Network/IPTables

Modificacion:

?https://we.riseup.net/stefani/iptables-recent-module-and-hit-limits

?http://thiemonagel.de/2006/02/preventing-brute-force-attacks-using-iptables-recent-matching/

?https://www.netfilter.org/documentation/HOWTO/netfilter-extensions-HOWTO-3.html#ss3.16 Recent_patch 3.16

?http://hostechs.com/2008/09/dropping-a-ddos-attack-using-ttl-and-length-in-iptables/

Rechaza aquellas ips que intantan 5 conexiones en las ultimos 60 s

```
-A INPUT -i eth0 -p tcp -m tcp --dport 22 -m state --state NEW -j SSHSCAN
-A SSHSCAN -m recent --set --name SSH --rsource
-A SSHSCAN -m recent --update --seconds 60 --hitcount 5 --name SSH --rsource -j LOG --log-prefix "Anti SSH-Bruteforce: " -
-A SSHSCAN -m recent --update --seconds 60 --hitcount 5 --name SSH --rsource -j DROP
-A SSHSCAN -j ACCEPT
```

Para quitar una maquina los datos de conexiones recientes:

echo "-193.144.202.192" > /proc/self/net/xt_recent/SSH