Bisoños Usuarios de GNU/Linux de Mallorca y Alrededores | Bergantells Usuaris de GNU/Linux de Mallorca i Afegitons

Ferm: itpables para vagos (13343 lectures)

Per **Mateu Batle Sastre**, ***Mateu*** (http://www.mbatle.com/)

Creado el 21/10/2001 21:33 modificado el 21/10/2001 21:33

Ferm *es una aplicación que permite definir las reglas de iptables sin tener que escribir tanto y de forma más clara (sintaxis parecida al C). Os pongo un ejemplo de ello.*

Ferm permite la definición de las reglas de forma estructurada, permite definir listas, bloques, variables, etc. Además es compatible con iptables, ipchains e ipfwadmin. Una de las pocas desventajas que tiene es que está escrito en Perl, pero nadie es perfecto ;-)

Instalarlo es fácil, lo podeis hacer con un simple **apt-get install ferm** si teneis la suerte de estar casados con una Debian. O para los más desafortunados, lo podeis encontrar en la página de su autor Auke Kok[1]. Actúa como un parser del lenguaje que genera los correspondientes comandos iptables. A continuación os pongo de un fichero de configuración del ferm (ferm.cfg):

```
option iptables
option clearall
option createchains
option automod

# variables
set LOCETH eth0
set LOCNET 192.168.0.0/24
set INTETH eth1
set INTNET 11.22.33.44/255.255.255.192
set INTIP 11.22.33.44

# Loopback rules
chain INPUT interface lo ACCEPT;
chain OUTPUT outerface lo ACCEPT;

# Rules local net
chain INPUT  {
  policy DENY;
  interface $LOCETH saddr $LOCNET ACCEPT;
  interface $INTETH {
    saddr $LOCNET DENY log;
    goto inet-in;
  }
}

chain OUTPUT {
  policy ACCEPT;
  saddr $LOCNET ACCEPT;
  outerface $INTETH goto inet-out;
}

chain FORWARD {
  policy ACCEPT;
  interface $LOCETH ACCEPT;
}

chain POSTROUTING {
  LOG;
  table nat outerface $INTETH snat $INTIP;
```

```
}

# Rules internet

chain inet-in {
  protocol (tcp udp) {
    # intruders
    dport (1080 1243 2049 3128:3129 5432 5999:6003 6670 6711 6969 7100) DENY log;
    dport (12345:12346 21544 23456 27374 30100 31337 31789 50505) DENY log;
    dport 1023:65535 ACCEPT;
  }
  protocol icmp ACCEPT;
  protocol tcp dport (22 25 80 113 443) ACCEPT;
  DENY log;
}

chain inet-out {
  ACCEPT;
}
```

Ahora para activar estas reglas basta ejecutar **ferm ferm.cfg**, y si ademas queremos ver las lineas de iptables que genera le añadimos la opción **--lines** y obtenemos lo siguiente:

```
iptables -F -t filter
iptables -F -t nat
iptables -F -t mangle
iptables -X -t filter
iptables -X -t nat
iptables -X -t mangle
iptables -t filter -A INPUT -i lo -j ACCEPT
iptables -t filter -A OUTPUT -o lo -j ACCEPT
iptables -t filter -P INPUT DROP
iptables -t filter -A INPUT -i eth0 -s 172.27.3.0/24 -j ACCEPT
iptables -t filter -A INPUT -i eth1 -s 172.27.3.0/24 -j LOG
iptables -t filter -A INPUT -i eth1 -s 172.27.3.0/24 -j DROP
iptables -t filter -N inet-in
iptables -t filter -A INPUT -i eth1 -j inet-in
iptables -t filter -P OUTPUT ACCEPT
iptables -t filter -A OUTPUT -s 172.27.3.0/24 -j ACCEPT
iptables -t filter -N inet-out
iptables -t filter -A OUTPUT -o eth1 -j inet-out
iptables -t filter -P FORWARD ACCEPT
iptables -t filter -A FORWARD -i eth0 -j ACCEPT
iptables -t filter -N POSTROUTING
iptables -t filter -A POSTROUTING -j LOG
iptables -t nat -A POSTROUTING -o eth1 -j SNAT --to 213.96.91.82
iptables -t filter -A inet-in -p tcp --dport 1080 -j LOG
iptables -t filter -A inet-in -p tcp --dport 1080 -j DROP
iptables -t filter -A inet-in -p tcp --dport 1243 -j LOG
iptables -t filter -A inet-in -p tcp --dport 1243 -j DROP
iptables -t filter -A inet-in -p tcp --dport 2049 -j LOG
iptables -t filter -A inet-in -p tcp --dport 2049 -j DROP
iptables -t filter -A inet-in -p tcp --dport 3128:3129 -j LOG
iptables -t filter -A inet-in -p tcp --dport 3128:3129 -j DROP
iptables -t filter -A inet-in -p tcp --dport 5432 -j LOG
iptables -t filter -A inet-in -p tcp --dport 5432 -j DROP
iptables -t filter -A inet-in -p tcp --dport 5999:6003 -j LOG
iptables -t filter -A inet-in -p tcp --dport 5999:6003 -j DROP
iptables -t filter -A inet-in -p tcp --dport 6670 -j LOG
iptables -t filter -A inet-in -p tcp --dport 6670 -j DROP
iptables -t filter -A inet-in -p tcp --dport 6711 -j LOG
iptables -t filter -A inet-in -p tcp --dport 6711 -j DROP
iptables -t filter -A inet-in -p tcp --dport 6969 -j LOG
iptables -t filter -A inet-in -p tcp --dport 6969 -j DROP
iptables -t filter -A inet-in -p tcp --dport 7100 -j LOG
iptables -t filter -A inet-in -p tcp --dport 7100 -j DROP
iptables -t filter -A inet-in -p udp --dport 1080 -j LOG
iptables -t filter -A inet-in -p udp --dport 1080 -j DROP
iptables -t filter -A inet-in -p udp --dport 1243 -j LOG
iptables -t filter -A inet-in -p udp --dport 1243 -j DROP
```

```
iptables -t filter -A inet-in -p udp --dport 2049 -j LOG
iptables -t filter -A inet-in -p udp --dport 2049 -j DROP
iptables -t filter -A inet-in -p udp --dport 3128:3129 -j LOG
iptables -t filter -A inet-in -p udp --dport 3128:3129 -j DROP
iptables -t filter -A inet-in -p udp --dport 5432 -j LOG
iptables -t filter -A inet-in -p udp --dport 5432 -j DROP
iptables -t filter -A inet-in -p udp --dport 5999:6003 -j LOG
iptables -t filter -A inet-in -p udp --dport 5999:6003 -j DROP
iptables -t filter -A inet-in -p udp --dport 6670 -j LOG
iptables -t filter -A inet-in -p udp --dport 6670 -j DROP
iptables -t filter -A inet-in -p udp --dport 6711 -j LOG
iptables -t filter -A inet-in -p udp --dport 6711 -j DROP
iptables -t filter -A inet-in -p udp --dport 6969 -j LOG
iptables -t filter -A inet-in -p udp --dport 6969 -j DROP
iptables -t filter -A inet-in -p udp --dport 7100 -j LOG
iptables -t filter -A inet-in -p udp --dport 7100 -j DROP
iptables -t filter -A inet-in -p tcp --dport 12345:12346 -j LOG
iptables -t filter -A inet-in -p tcp --dport 12345:12346 -j DROP
iptables -t filter -A inet-in -p tcp --dport 21544 -j LOG
iptables -t filter -A inet-in -p tcp --dport 21544 -j DROP
iptables -t filter -A inet-in -p tcp --dport 23456 -j LOG
iptables -t filter -A inet-in -p tcp --dport 23456 -j DROP
iptables -t filter -A inet-in -p tcp --dport 27374 -j LOG
iptables -t filter -A inet-in -p tcp --dport 27374 -j DROP
iptables -t filter -A inet-in -p tcp --dport 30100 -j LOG
iptables -t filter -A inet-in -p tcp --dport 30100 -j DROP
iptables -t filter -A inet-in -p tcp --dport 31337 -j LOG
iptables -t filter -A inet-in -p tcp --dport 31337 -j DROP
iptables -t filter -A inet-in -p tcp --dport 31789 -j LOG
iptables -t filter -A inet-in -p tcp --dport 31789 -j DROP
iptables -t filter -A inet-in -p tcp --dport 50505 -j LOG
iptables -t filter -A inet-in -p tcp --dport 50505 -j DROP
iptables -t filter -A inet-in -p udp --dport 12345:12346 -j LOG
iptables -t filter -A inet-in -p udp --dport 12345:12346 -j DROP
iptables -t filter -A inet-in -p udp --dport 21544 -j LOG
iptables -t filter -A inet-in -p udp --dport 21544 -j DROP
iptables -t filter -A inet-in -p udp --dport 23456 -j LOG
iptables -t filter -A inet-in -p udp --dport 23456 -j DROP
iptables -t filter -A inet-in -p udp --dport 27374 -j LOG
iptables -t filter -A inet-in -p udp --dport 27374 -j DROP
iptables -t filter -A inet-in -p udp --dport 30100 -j LOG
iptables -t filter -A inet-in -p udp --dport 30100 -j DROP
iptables -t filter -A inet-in -p udp --dport 31337 -j LOG
iptables -t filter -A inet-in -p udp --dport 31337 -j DROP
iptables -t filter -A inet-in -p udp --dport 31789 -j LOG
iptables -t filter -A inet-in -p udp --dport 31789 -j DROP
iptables -t filter -A inet-in -p udp --dport 50505 -j LOG
iptables -t filter -A inet-in -p udp --dport 50505 -j DROP
iptables -t filter -A inet-in -p tcp --dport 1023:65535 -j ACCEPT
iptables -t filter -A inet-in -p udp --dport 1023:65535 -j ACCEPT
iptables -t filter -A inet-in -p icmp -j ACCEPT
iptables -t filter -A inet-in -p tcp --dport 22 -j ACCEPT
iptables -t filter -A inet-in -p tcp --dport 25 -j ACCEPT
iptables -t filter -A inet-in -p tcp --dport 80 -j ACCEPT
iptables -t filter -A inet-in -p tcp --dport 113 -j ACCEPT
iptables -t filter -A inet-in -p tcp --dport 443 -j ACCEPT
iptables -t filter -A inet-in -j LOG
iptables -t filter -A inet-in -j DROP
iptables -t filter -A inet-out -j ACCEPT
```

--Mateu

Lista de enlaces de este artículo:

1. http://www.geo.vu.nl/~koka/ferm/

E-mail del autor: mbatle _ARROBA_ mbatle.com