



ANEXO T4: cortafuegos e IDS

(Netfilter - iptables)

[Filtros con estado]

Algunos ejemplos de filtro en estado:

- Permitir sólo conexiones salientes

```
iptables -A OUTPUT -p udp -m state --state ESTABLISHED -j ACCEPT
iptables -A OUTPUT -p udp -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -m state --state NEW,ESTABLISHED -j ACCEPT
```

- Obligar a que una conexión TCP se inicie con un segmento SYN:

```
iptables -A INPUT -p tcp ! --syn -m state --state NEW -j DROP
```

- Reglas de aceptación o rechazo de mensajes ICMP

```
iptables -A OUTPUT -p icmp -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -p icmp -m state --state ESTABLISHED,RELATED -j ACCEPT
```

- Aceptar sólo conexiones salientes FTP

```
iptables -A OUTPUT -p tcp --dport 21 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp --sport 21 -m state --state ESTABLISHED -j ACCEPT
```

- Aceptar conexiones activas FTP :

```
iptables -A INPUT -p tcp --sport 20 -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A OUTPUT -p tcp --dport 20 -m state --state ESTABLISHED -j ACCEPT
```

Persistencia Reglas Iptables

- Comandos: `iptables-save` e `iptables-restore` [(-c): contadores, (-n): noflush]

```
iptables-save [-c] > /etc/iptables.rules
iptables-restore [-n] /etc/iptables.rules
```

- En muchas distribuciones se incluyen paquetes (`iptables-services`, `iptables-persistent` o `netfilter-persistent`) para mantener las reglas iptables definidas (salvar, limpiar, recuperar reglas salvadas, ...). Por ejemplo, en Ubuntu usamos `iptables-persistent` y `netfilter-persistent` (instalar ambos):

```
apt install iptables-persistent netfilter-persistent
netfilter-persistent save
netfilter-persistent flush
netfilter-persistent start
systemctl enable netfilter-persistent
```

- Redhat > 7 usa firewalld. Si queremos usar iptables con persistencia hay que desactivar firewalld e instalar el paquete `iptables-services`.

`iptables -persistent`

Yo puedo abrir la conexión hacia si, pero no hacia al no

Mi lista: fuerza remoto NEW y ESTABLISHED
pero NO dentro NEW ESTABLISHED

EN UDP: NO TIEMPO ES ACK-RESPONSE
ICMP es mensaje de respuesta (ACK/NS...)

Los TCP tienen una respuesta SYN. Si es UNICO Nuevo
COMUNICACIÓN Y NO RESPONDE POR SYN LO HAIDO

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

ANEXO T4: cortafuegos e IDS

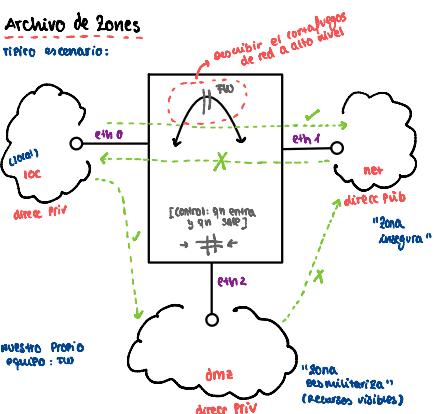
Shorewall

alto nivel para generar reglas iptables

- Herramienta para la config de Netfilter
 - ↳ De alto nivel los requisitos filtrado + en /etc/archivos config
- Interfaz Shorewall → Proporciona un script
 - ↳ Permite activar/desactivar reglas `/etc/rc.d/init.d/shorewall {start|stop|restart,...}`
- Archivos config → /etc/shorewall
 - ↳ shorewall.conf → config B°
 - ↳ zones + zonas contempladas
 - ↳ policy → Políticas por defecto
 - ↳ Rules → reglas o excepciones de las Políticas
 - ↳ Interfaces → identif. de interfaces
 - ↳ SNAT + MASQ → Enmascaramiento

Archivo de Zonas

Típico escenario:



#ZONE	TYPE
fw	firewall
net	ipv4
loc	ipv4
#dmz	ipv4

Archivo Policy

- Políticas por defecto para el intercambio de zonas
- Opciones básicas: ACCEPT, DROP, REJECT
 - ↳ Nivel del registro de actividad (logs)
 - ↳ Tasa de conexiones permitidas
 - ↳ Tasa máxima de rechazos
 - ↳ Num máx conexiones simultáneas

```
#SOURCE DEST POLICY LOG LIMIT:BURST CONNLIMIT
loc net ACCEPT
net all DROP info
SFW net ACCEPT
# The FOLLOWING POLICY MUST BE LAST
all all REJECT info
```

↳ convierte djar una política por defecto

Archivo Rules

Establecer excepciones a Políticas por defecto

- Reenviar todas las conexiones http desde Internet al sistema local 192.168.1.3 (port forwarding)

ACTION	SOURCE	DEST	PROTO	DEST PORTS
DNAT	net	loc:192.168.1.3	tcp	http
- Acepta conexiones ssh al cortafuegos sólo desde la dirección net 130.252.100.70

ACCEPT	net:130.252.100.70	fw	tcp	22
--------	--------------------	----	-----	----
- Redirección las conexiones http locales a un proxy (puerto 8080 del propio cortafuegos)

REDIRECT	loc	8080	tcp	www
----------	-----	------	-----	-----

Archivo Interfaces

- Lista las interfaces red del equipo
 - ↳ Asociadas a la zona donde están
- Pueden iniciarse las direc de difusión y algunos paráms. de configuración
 - ↳ dhcp → si la subred se gestiona con dhcp
 - ↳ noip6ll → introducir entrega datagrama direct origen priv
 - ↳ detect → detectar direc de difusión

```
loc eth0 192.168.1.255
net eth1 206.191.149.255 dhcp
dmz eth2 detect
```

Al menos 2 interfaces
Estos se asocian a las interfaces físicas mediante la opción `physical`.

Archivo masq

Establece el ENMASCARAMIENTO de las direc IP en el tráfico q pasa a través de algunas interfaces

- Ejemplo: El tráfico desde la red privada 192.168.1.0/24 dirigido a la red pública (visible a través del interface eth1) se enmascara en la dirección pública de eth1 (suponemos 217.42.11.145):

INTERFACE	SUBNET	ADDRESS
eth1	192.168.1.0/24	217.42.11.145

- Nota: También valdría la siguiente configuración (suponiendo que eth0 es el interface privado; enmascara cualquier dirección interna con la IP que tenga asignada el interface externo eth1):

eth1	eth0
------	------

Archivo SNAT

Reenviando cuando la direc de ENMASCARAMIENTO es externa

- A partir v 5.0.14
- ¡igo! en la config por defecto sustituye a masq

- Ejemplo 1: Enmascar el tráfico desde la red privada 192.168.1.0/24 dirigido a la red pública (visible a través de eth1)

ACTION	SOURCE	DEST	MASQUERADE
			192.168.1.0/24
			eth1

- Ejemplo 2: Usar una IP de salida dependiendo del servicio

ACTION	SOURCE	DEST	PROTO	PORT	
SNAT	(206.124.146.177)	172.20.1.0/29	eth1	tcp	sntp
SNAT	(206.124.146.176)	172.20.1.0/29	eth1		