TEMA

Tema 9. Cortafuegos

Administración de sistemas informáticos en Red

Seguridad y alta disponibilidad

Autor/a: Joaquín Erencia

Linkia FP

Tema 9: Cortafuegos

¿Qué aprenderás?

- Qué funciones tiene el cortafuegos.
- Los tipos de cortafuegos que hay.
- Cómo se configura el cortafuegos IPTABLES.

¿Sabías que…?

- Se están instalando cortafuegos en Android.

9.1. Introducción

Dedicamos un tema específico a la herramienta de Seguridad perimetral por excelencia: el cortafuegos.

Como su nombre indica es la barrera que impide que los problemas (fuegos) que recorren el mundo de Internet entren en nuestra casa y continúen con su propagación.

Ya hemos visto en temas anteriores la innumerable variedad de ataques para conseguir entrar en nuestros sistemas informáticos (¡sí, sí, en el tuyo también!) debido a la necesidad que tenemos de que se encuentren conectadas al mundo exterior.

9.2. Conceptos básicos

Un **cortafuegos** es un sistema de red cuya única función es separar dos redes informáticas y consistente en permitir o denegar el paso de la comunicación de una red a otra mediante el protocolo TCP/IP.

Debemos tener en cuenta una cosa muy importante: El firewall no protege ante virus, spam y spyware. Necesitamos los otros sistemas que componen la seguridad para estar protegidos.

Para instalar el sistema cortafuegos adecuado necesitamos tener en cuenta:

- Todo el tráfico entre las dos redes debe pasar por el cortafuegos. Recordad las DMZ.
- Solo el tráfico que cumpla con las reglas podrá atravesar el cortafuegos.
- El sistema operativo ha de estar preparado para proteger al cortafuegos.

9.3. Clasificaciones y funcionamiento

9.3.1. Clasificación de cortafuegos general

- **Cortafuegos por hardware**. Son unos dispositivos que se añaden a la red local y se sitúan normalmente entre el punto de acceso a Internet y el switch que distribuye el tráfico por los equipos de esta.

    - Este tipo de cortafuegos analizan y filtran todo el tráfico que entra y sale de la red y bloquea aquellos elementos que no cumplen con las reglas de seguridad establecidas por el administrador.

    - En muchos routers nos encontramos que ya vienen con este firewall instalado. Estos tipos de firewall se configuran por el navegador web, normalmente.

- **Cortafuegos por software**: Es una aplicación que se instala en el ordenador. Realiza la misma función que el cortafuegos de software, pero su ámbito de aplicación es el tráfico de red que se genera hacia o desde el ordenador en el que se instala.

  Sus características son:

    - Suelen venir con el sistema operativo y son para uso personal.
    - Son simples de instalar, normalmente ya viene activados y el Sistema Operativo nos avisa no están funcionando.
    - Parece que no, pero es recomendable tener uno por equipo en la red.
    - Si son de pago, suele incorporar protecciones extra.

Otra clasificación sería en función de la capa del modelo OSI en la que trabajen:

- **Cortafuegos a nivel de Red (Router con firewall)**

  Cada paquete que pasa a través de él es inspeccionado y se revisa:

  - Dirección IP de origen y destino.
  - Puerto de origen y destino.
  - Protocolo de los datos.
  - Si el paquete es un inicio de una petición de conexión.

  Uno de los firewall más conocidos a este nivel es el IPTABLES, el cual trataremos más adelante con más detalle.

- **Cortafuegos a nivel de circuito**

  Se trata del firewall anterior, pero trabajando en la Capa de Transporte. Aquí se revisa el establecimiento, seguimiento y liberación de las conexiones entre las máquinas emisoras y receptoras

- **Cortafuegos a nivel de aplicación**

  Los servidores proxy se comunican con otros servidores del exterior de la red en nombre de los usuarios. En el siguiente tema hablaremos más detenidamente de ellos.

También los podemos clasificarlos en función de su funcionamiento:

- **NAT** (Network Address Translation)

NAT consiste en asociar las subredes IP internas detrás de una o de un conjunto de direcciones IP. Las peticiones de los host de la subred son gestionadas como si fueran de una misma IP. Recordad la configuración NAT de las máquinas virtuales. Esta configuración permite una gestión más sencilla pues solo hay que revisar una única IP. El problema está en que una vez realizada la conexión no podemos controlar qué hace el usuario.

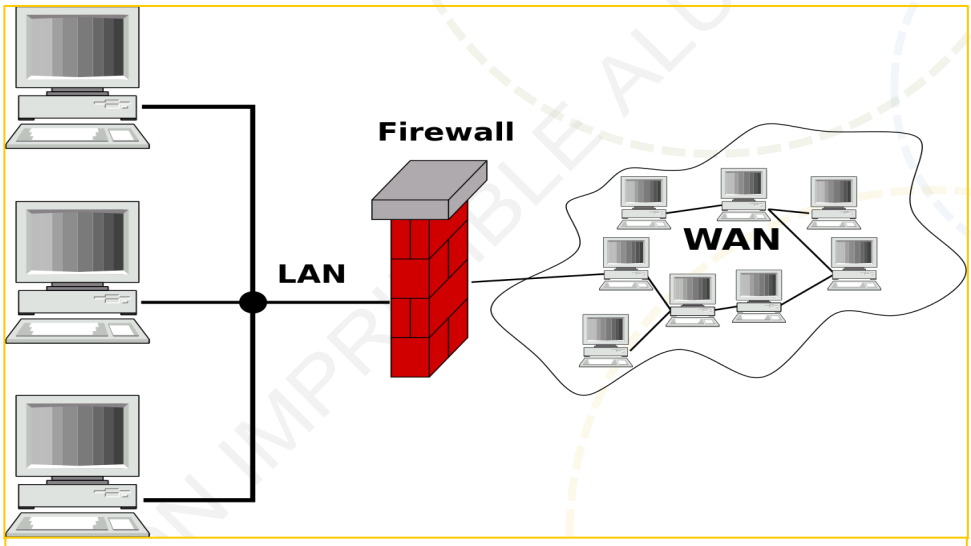
¿Cómo funciona NAT?

NAT traduce las direcciones IP privadas de la red interna en una IP pública para que la red pueda enviar paquetes al exterior.

Para el host privado el proceso es sencillo. Este envía un paquete a su router o Gateway, el cual cambia la dirección de origen por su IP pública. A este proceso se le denomina Source-NAT (SNAT). De esta manera el host remoto responderá a la IP pública. La recepción de la respuesta es inversa, traduce la IP pública de nuevo en la IP privada del PC que envió el paquete.

Dentro del router existe la Tabla de NAT, en la que se guarda una entrada para cada conexión. Cada vez que un host privado realiza una conexión, se agrega una entrada a la Tabla de NAT.

Si lo que queremos es que un equipo externo se pueda conectar con un equipo de la red interna debe hacer lo que denominados un Destination-NAT (DNAT). En la tabla de NAT debemos agregar una entrada donde indicamos que todo el tráfico que llegue que vaya dirigido a determinado puerto, sea dirigido al equipo de la red interna en cuestión. Esto es lo que comúnmente se denomina “Abrir Puertos”.



- **Filtrado de Paquetes**

Este cortafuegos lee cada paquete de datos que pasa dentro y fuera de una LAN. El filtrado lo realiza en función de unas reglas. Se personaliza a través de la utilidad IPTABLES en el firewall. Los clientes no necesitan ninguna configuración. No puede filtrar aplicaciones todo lo realiza a nivel de red

- **Proxy**

  Este cortafuegos filtra todas las peticiones de cierto protocolo desde el cliente de la red a esta. Después el cortafuegos hace esa misma petición hacia internet. Actúa como buffer entre los usuarios remotos y las máquina cliente. El problema radica en que ante una gran cantidad de peticiones pueden actuar como cuellos de botella y ralentizarlas mucho

9.3.2. ¿Cómo funciona el cortafuegos?

Para realizar su función, el cortafuegos tiene un conjunto de reglas predefinidas que permiten:

- Autorizar una conexión (**Allow**)
- Bloquear una conexión (**Deny**)
- Redireccionar una conexión (**Drop**)

El conjunto de estas reglas permite disponer de un método de filtrado dependiendo de la política de seguridad de la organización.

En función de lo anterior el firewall puede:

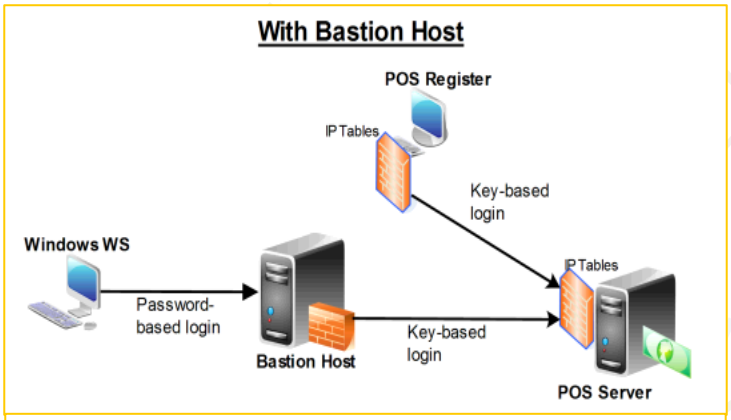
- Administrar los accesos de los usuarios a los servicios privados de la red.
- Registrar todos los intentos de entrada y salida de la red. Los almacena en archivos .log.
- Filtrar paquetes en función de su origen, destino y número de puerto. A esto se le denomina Filtrado de Direcciones. Un ejemplo sería bloquear el acceso a la IP 192.168.100.1 a través del puerto 22.
- Filtrar determinados tipos de protocolos de nuestra red. A esto se le denomina Filtrado por Protocolo. Un ejemplo sería no permitir el servicio SSH o FTP en nuestra red.
- Controlar el número de conexiones que se están produciendo desde un mismo punto y bloquearlas en el caso de que superen un número de determinado. Este sistema permite defendernos de ataques de **DoS.**
- Controlar las aplicaciones que pueden acceder a Internet. Por ejemplo, no queremos que se pueda acceder a **Spotify.**
- Detección de puertos que están en escucha y no deberían estarlo. Este sistema nos protege de **BackDoors**, por ejemplo.

9.4. Topología de los cortafuegos

Vamos a analizar dónde se instalan los cortafuegos y qué objetivo tiene cada instalación.

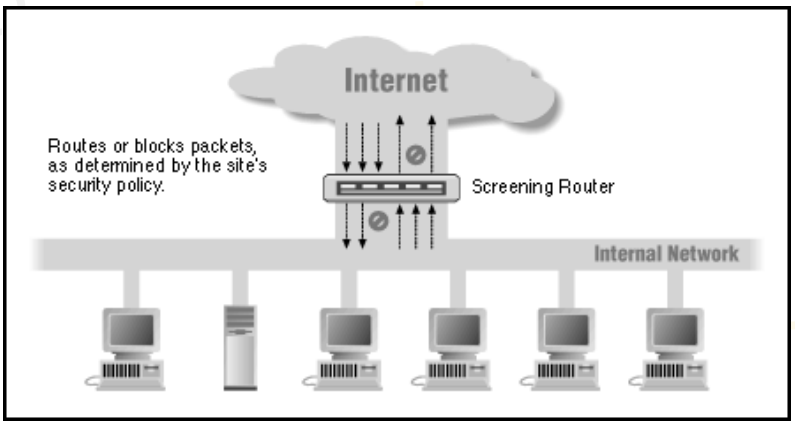
9.4.1. Bastion Host

Son los cortafuegos más importantes. Se instalan en puntos clave de la seguridad de la red. Se revisan regularmente para poder detectar ataques.



9.4.2. Screening Router

Es un router utilizado para el filtrado de paquetes entre redes. Tiene la capacidad de bloquear el tráfico entre redes basándose en direcciones y puertos TCP/IP. Actualmente casi todos los routers comerciales lo traen. Para su configuración utiliza reglas ACL asociadas a la interfaz.

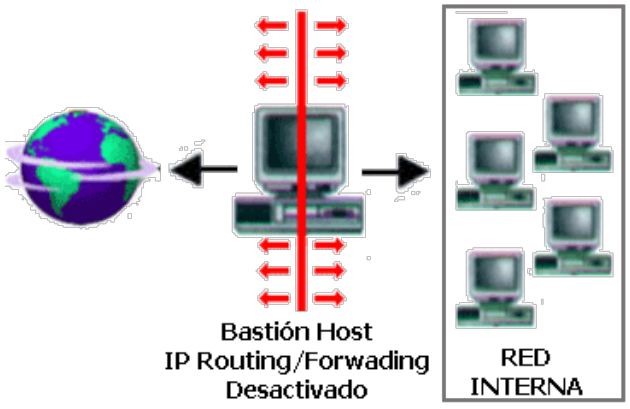


9.4.3. Dual-Homed Host

Se instala en un servidor dos tarjetas de red independientes. Una está conectada a Internet y la otra a la red que se quiere proteger, desactivando las funciones de reenvío TCP/IP. Por lo tanto, el tráfico directo entre la red interna e internet está bloqueado. Para la conexión de los equipos utilizaremos IP Forwarding.

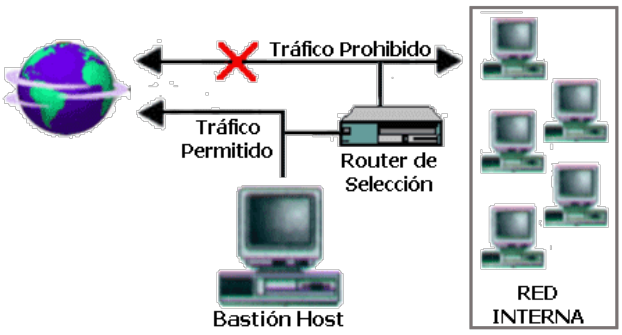
Con esta topología, el administrador debe decidir entre dos filosofías:

- Se permite a cada aplicación de manera independiente el acceso a Internet.
- Se permite a cada usuario de manera independiente el acceso a Internet. En este caso, si un intruso reactiva el reenvío TCP/IP tendrá libre acceso a toda la red.



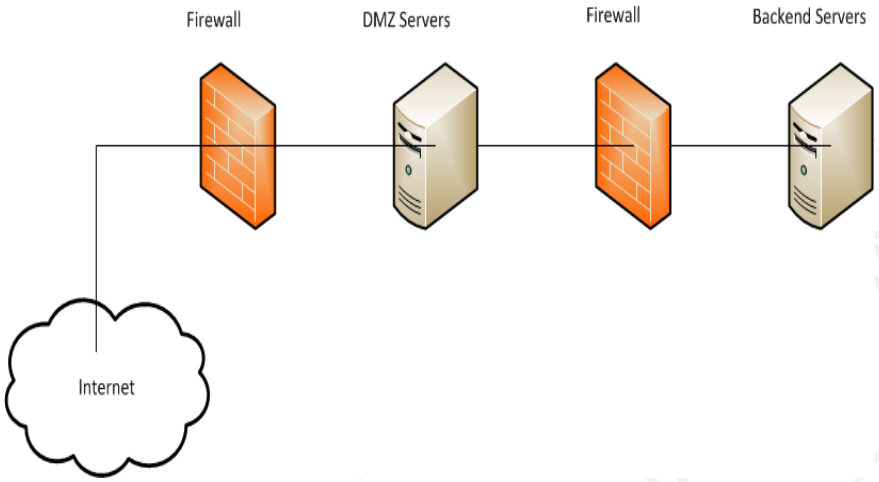
9.4.5. Screen Host

Es la combinación de los anteriores: un Bastion host haciendo de Dual-Homed Host más un Screening Router. El host hace de barrera para las aplicaciones y el router filtra los paquetes.



9.4.6. Screened Subnet

Se utiliza en caso de necesitar tener una subred aislada situada entre la red interna e Internet. Estos router permiten que esta subred aislada sea accesible desde Internet y desde la red interna, pero bloquea el acceso desde Internet a la red Interna. Es la configuración de las DMZ.



9.5. IPTABLES

Esta herramienta de comandos es la más utilizada en la creación de reglas. Es una línea de comandos con su propia sintaxis y aunque el objetivo no es dominarlo, sí vamos a tratar de explicar lo más importante.

Vamos a empezar con un poco de teoría de IPTABLES:

Concepto de Tablas: En IPTABLES existen tres tablas por defecto y cada una de ellas tiene una función y unas reglas determinadas.

- Tabla de filtro (Filter): Es la responsable de filtrar un paquete. Todos los paquetes cumplen las reglas de esta tabla. Dentro de esta tabla nos encontramos con estas opciones:
  - **INPUT** (entrada)
  - **OUTPUT** (salida)
  - **FORWARD** (redirección)
- Tabla de NAT: Es la responsable de las reglas de traducción de direcciones o puertos. Dentro de esta tabla nos encontramos con estas opciones:
  - **PREROUTING** (antes de realizar la conversión entre IP pública y privada)
  - **POSTROUTING** (después de realizar la conversión entre IP pública y privada)
  - **OUTPUT** (salida)
- Tabla de Destrozo (Mangle): Es la responsable de cambiar opciones como el tiempo de vida del paquete TTL (Time To Live). No profundizaremos más.

En este ejemplo vemos el camino que sigue un paquete a través de las tablas:

1. Desde el exterior recibimos una petición SSH, a la IP del cliente 10.0.0.10.
2. Esta petición entra por la tarjeta del cortafuegos que está conectada a Internet, la eht0.
3. El paquete revisa las reglas de la Tabla de NAT (PREROUTING).
4. El paquete es enrutado a la tarjeta adecuada, en este caso la eth1.
5. El paquete revisa las reglas de la Tabla Filter (FORWARD).
6. El paquete revisa las reglas de la Tabla de NAT (POSTROUTING).
7. Se realiza la conexión con el host 10.0.0.10 pero solo SSH.

Ahora viene la parte de entender mejor lo de arriba con práctica.

Vamos a empezar iniciando el servicio (¡OJO! doy por sentado que lo habéis instalado y reiniciado la máquina).

service iptables start

La sintaxis de iptables está separada por niveles. El nivel principal es la cadena. Una cadena especifica el estado en el cual se puede manipular un paquete.

iptables -A chain -j target

Opciones más usadas del comando iptables:

- -L listar las cadenas de reglas
- -F eliminar y reiniciar los valores de las reglas
- -A añadir una cadena de regla a una tabla
- -P añadir una regla (política) por defecto
- -t tabla sobre la que trabaremos
- -i interfaz de red de entrada del paquete
- -o interfaz de red de salida del paquete
- -s dirección de IP de origen del paquete
- -d dirección de IP de destino del paquete
- - - dport número del puerto de destino
- -m dirección mac de una interface
- -j acción a realizar
- -D borrar una regla determinada

La *chain* es el nombre de la cadena para una regla. Las que tenemos por defecto son:

- INPUT
- OUTPUT
- FORWARD

El *target* es la acción a realizar. Las que tenemos son:

- DROP (rechazar)
- ACCEPT (aceptar)
- MASQUERADE (enmascarar)

Lo primero será borrar todo lo que tengamos hecho, para que no se solapen cosas y tengamos funcionamientos indeseados:

```
iptables -F INPUT
iptables -F FORWARD
iptables -F OUTPUT
iptables -F -t nat
```

Para empezar, vamos a establecer algunas políticas básicas (-P) para que desde el comienzo puedan servir como base para la construcción de reglas más detalladas definidas por el usuario.

iptables -P INPUT DROP	(todos los paquetes que entran se bloquean)
iptables -P OUTPUT DROP	(todos los paquetes que salen se bloquean)
iptables -P FORWARD DROP	(todos los paquetes que se enrutan se bloquean)

Vamos a guardar las reglas para que no se borren:

```
/sbin/service iptables save
```

Y se almacenan en el archivo /etc/sysconfig/iptables

Bien, tenemos las bases montadas. A continuación, vamos a preparar lo más básico, que el usuario pueda conectase a Internet.

```
iptables -A INPUT -p tcp -m tcp --sport 80 -j ACCEPT
iptables -A OUTPUT -p tcp -m tcp --dport 80 -j ACCEPT
iptables -A INPUT -p tcp -m tcp  - -sport 443 -j ACCEPT
iptables -A INPUT -p tcp -m tcp  - -dport 443 -j ACCEPT
```

A continuación, podemos seguir con permitir el acceso remoto a la red interna desde fuera de la red. Habilitaremos el SSH que nos encripta conexiones remotas a los servicios LAN.

```
iptables -A INPUT -p tcp  - -dport 22 -j ACCEPT
iptables -A OUTPUT -p udp - -sport 22 -j ACCEPT
```

De esta manera, podemos ir añadiendo servicios que queremos que se habiliten. Recordad que primero lo hemos bloqueado todo.

Bien, subamos el nivel. Vamos a habilitar NAT. Recordad que hemos creado una política que bloqueaba el reenvío de paquetes. Ahora permitamos a la red el reenvío.

iptables -A FORWARD -i eth1 -j ACCEPT

iptables -A FORWARD -o eht1 -j ACCEPT

Siendo eth1 la tarjeta del cortafuegos del lado interno y -i (entrada) y -o (salida)

Ahora ya podemos desde fuera de la red interna con los equipos de la red interna, pero no permite a estos conectarse con Internet. Para ello tenemos que habilitar el enmascaramiento de IP (convertir la IP privada en IP pública).

iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

Siendo eth0 la tarjeta del cortafuegos del lado exterior.

Si queremos personalizar más el proceso, le podemos determinar qué IP es la que queremos que reciba los mensajes de respuesta.

iptables -t nat -A PREROUTING -i eth0 -p tcp –dport 80 -j DNAT - - to 172.32.0.24:80

En este ejemplo todas las peticiones HTTP entrantes se reenvían exclusivamente a la IP 172.32.0.24

Para aumentar nuestra seguridad, podemos bloquear puertos que no son utilizados por ninguna aplicación y que se pueden utilizar para fines maliciosos.

iptables -A OUTPUT -o eth0 -p tcp - - dport 31337 - - sport 31337 -j DROP

iptables -A FORWARD -o eth0 -o tcp - - dport 31337 - - sport 31337 -j DROP

Y, por supuesto, conjuntos de red o una subred.

iptables -A FORWARD -s 192.168.1.0/24 -i eth0 -j DROP

Existe una opción que es REJECT en vez de DROP. La diferencia está en que REJECT rechaza la conexión y envía un mensaje de conexión rechazada al usuario que se está intentando conectar.

Os adjunto un ejemplo comentado de archivo de configuracion de iptables:

```
## Vaciamos las reglas
iptables -F
iptables -X
iptables -t nat -F


## Establecemos políticas predeterminada
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -t nat -P PREROUTING ACCEPT
iptables -t nat -P POSTROUTING ACCEPT


# Aceptamos todo de localhost
/sbin/iptables -A INPUT -i lo -j ACCEPT


# A nuestra IP le dejamos todo
iptables -A INPUT -s 192.168.2.1 -j ACCEPT


# A otra ip interna le permitimos todo
iptables -A INPUT -s 192.168.2.99 -j ACCEPT
iptables -A INPUT -s 192.168.2.100 -j ACCEPT


# A una subred interna le permitimos todo
iptables -A INPUT -s 192.168.1.0/24 -j ACCEPT
# O a un rango de una subred
iptables -I INPUT -m iprange --src-range 192.168.1.2-192.168.1.100 -j ACCEPT


# Permitimos una conexion a ssh y telnet (22 y 23) desde un equipo
iptables -A INPUT -s 192.168.2.10 -p tcp --dport 22:23 -j ACCEPT


# A otro le permitimos acceso FTP
iptables -A INPUT -s 212.176.121.111 -p tcp --dport 20:21 -j ACCEPT
```

```
# El puerto 80 y 8080 (www) abierto, para un servidor web.
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
iptables -A INPUT -p tcp --dport 8080 -j ACCEPT


# Y el resto, lo cerramos
# Indicamos que se almacenen los accesos a los puertos que vamos a cerrar
iptables -A INPUT -p tcp -m tcp --dport 22:23 -j LOG --log-prefix 'INTENTO DE ACCESO A SSH ' --log-level 4
iptables -A INPUT -p tcp -m tcp --dport 20:21 -j LOG --log-prefix 'INTENTO DE ACCESO A FTP ' --log-level 4
iptables -A INPUT -p tcp -m tcp --dport 6001 -j LOG --log-prefix 'INTENTO DE ACCESO A 6001 ' --log-level 4


iptables -A INPUT -p tcp --dport 20:21 -j DROP
iptables -A INPUT -p tcp --dport 22:23 -j DROP
iptables -A INPUT -p tcp --dport 6001 -j DROP


# Cerramos rango de los puertos privilegiados. Cuidado con este tipo de
# barreras, antes hay que abrir a los que si tienen acceso.
iptables -A INPUT -p tcp --dport 1:1024 -j DROP
iptables -A INPUT -p udp --dport 1:1024 -j DROP


# impedimos iniciar conexion los puertos altos
# (puede que ftp no funcione)
iptables -A INPUT -p tcp --syn --dport 1025:65535 -j DROP


# Cerramos otros puertos que estan abiertos
iptables -A INPUT -p tcp --dport 3306 -j DROP
iptables -A INPUT -p tcp --dport 10000 -j DROP
```

9.6. Los registros de seguridad del firewall

Ya hemos comentado que todo lo que pasa en el cortafuegos se almacena en archivos de texto, logs. Ahora lo que tenemos que hacer es revisarlos y no solo para mirar los eventos negativos sino todo en general, pues no puede enseñar cosas sobre la configuración que hemos realizado.

En el ejemplo anterior podéis ver que almacenamos en el log los intentos de acceso a ciertos puertos.

Este listado de sucesos se encuentra con todos los del sistema Linux en ***/var/log/messages*** y en **/etc/syslog.conf.** Como no nos interesa vamos a crear nuestro propio fichero:

- Editamos el archivo **/etc/syslog.conf**
- Añadimos al final la siguiente línea

```
kern.warning  /var/log/iptables.log
```

9.7. Pruebas de funcionamiento

Una vez hemos configurado el cortafuego, se recomienda realizar un conjunto de pruebas para determinar si cumple lo que queremos.

Os adjunto un listado de servicios online para comprobar su funcionamiento:

- Free Online Firewall Test
- Hackerwatch
- Audit My PC
- Test de velocidad

Recursos y enlaces

- Cortafuegos Linux. UFW 1

  Objetivo: En esta práctica vamos a poder instalar y configurar el cortafuegos UFW en una distribución Ubuntu Desktop.

- Cortafuegos Linux. UFW 2

  Objetivo: En esta práctica vamos a poder instalar y configurar el cortafuegos UFW en una distribución Ubuntu Desktop.

- Cortafuegos Windows. Bloquear PING

  Objetivo: En esta práctica vamos a aprender cómo configurar el Firewall de Windows para que solo nos puedan hacer ping desde redes privadas. Esto es una buena medida de seguridad.

- Servidor Cortafuegos-Proxy Linux. pfSense

  Objetivo: En esta práctica vamos a instalar el servidor pfSense y realizamos una configuración del mismo.

  La máquina dispone de dos tarjetas, una que se conecta a Internet y otra que se conecta a la red interna.

  IPTABLES

- Ejemplos IPTABLES

- Listado Cortafuegos

- Firewall Fortinet

- Firewall Netgear

- Firewall Cisco

- Free Online Firewall Test

- Hackerwatch

- Audit My PC

- Test de velocidad

Test de autoevaluación

1. Indica cuál de los siguientes routers es el que se encontrará en un DMZ:

a) Screening Router
b) Screening Subnet
c) Bastion Router
d) Dual Homed Host

2. Indica en cuál de los siguientes routers aplicaremos reglas ACL:

a) Screening Router
b) Screening Subnet
c) Bastion Router
d) Dual Homed Host

3. Indica con cuál de las siguientes ordenes listamos las reglas del Iptables:

a) iptables -F
b) iptables -A
c) iptables -L
d) iptables -p

4. Indica en cuál de los siguientes routers cerramos la entrada por los puertos del 1 al 1024:

a) iptables -A OUTPUT -p tcp --dport 1:1024 -j DROP
   iptables -A OUTPUT -p udp --dport 1:1024 -j DROP
b) iptables -A OUTPUT -p tcp --dport 1:1024 -j ACCEPT
   iptables -A OUTPUT -p udp --dport 1:1024 -j ACCEPT
c) iptables -A INPUT -p tcp --dport 1:1024 -j DROP
   iptables -A INPUT -p udp --dport 1:1024 -j DROP
d) iptables -A INPUT -p tcp --dport 1:1024 -j ACCEPT
   iptables -A INPUT -p udp --dport 1:1024 -j ACCEPT

SOLUCIONARIOS

Test de autoevaluación

1. Indica cuál de los siguientes routers es el que se encontrará en un DMZ:

a) Screening Router
b) **Screening Subnet**
c) Bastion Router
d) Dual Homed Host

2. Indica en cuál de los siguientes routers aplicaremos reglas ACL:

a) **Screening Router**
b) Screening Subnet
c) Bastion Router
d) Dual Homed Host

3. Indica con cuál de las siguientes ordenes listamos las reglas del Iptables:

a) iptables -F
b) iptables -A
c) **iptables -L**
d) iptables -p

4. Indica en cuál de los siguientes routers cerramos la entrada por los puertos del 1 al 1024:

a) iptables -A OUTPUT -p tcp --dport 1:1024 -j DROP
   iptables -A OUTPUT -p udp --dport 1:1024 -j DROP
b) iptables -A OUTPUT -p tcp --dport 1:1024 -j ACCEPT
   iptables -A OUTPUT -p udp --dport 1:1024 -j ACCEPT
c) **iptables -A INPUT -p tcp --dport 1:1024 -j DROP**
   iptables -A INPUT -p udp --dport 1:1024 -j DROP
d) iptables -A INPUT -p tcp --dport 1:1024 -j ACCEPT
   iptables -A INPUT -p udp --dport 1:1024 -j ACCEPT