

Cortafuegos

Preguntas

1. ¿En qué consiste un cortafuegos o "firewall"? ¿Qué tipo de tráfico bloquea y a quien va dirigido dicho tráfico? ¿Qué tipo de tráfico no bloquea? ¿Qué no es capaz de hacer un cortafuegos?

Un cortafuegos es un elemento de seguridad de red, que permite o bloquea el tráfico de red que va de un segmento de red a otro, según los parámetros de las cabeceras de red y de transporte de los paquetes de red. En la mayoría de casos los parámetros que el cortafuegos analiza para decidir si filtra o no el paquete son la IP de origen, la IP de destino, el puerto de origen o/y el puerto de destino.

El cortafuegos tiene una lista de reglas, llamada “lista de control de acceso” o ACLs, que se intentan aplicar una a una por orden al paquete de red. Si el paquete encaja con una regla, se le aplica la acción asociada a dicha regla y se descartan las reglas que quedaban. Si el paquete no encaja con ninguna regla, se le aplica una regla más general llamada “política por defecto”.

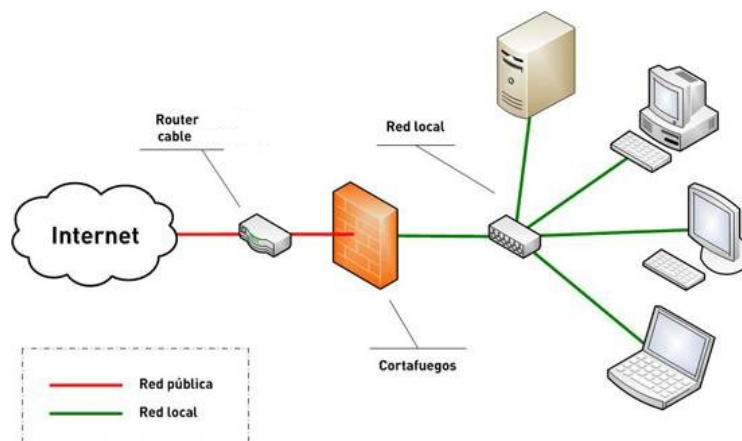
El cortafuegos puede ser un equipo específico, pero también puede estar integrado en un encaminador, por ejemplo. O incluso puede ser un equipo general como un PC con varias tarjetas de red y software específico de cortafuegos.

Debe quedar claro que un cortafuegos no filtra tráfico de red mirando el contenido de los paquetes, aunque algunos cortafuegos de última generación incorporan dicha característica. Son los proxy y los Sistemas de Detección de Intrusos los que exploran el contenido de los paquetes a nivel de capa de aplicación.

También es evidente que un cortafuegos no puede filtrar el tráfico que no pasa por él, así que una decisión importante es donde colocaremos los cortafuegos en nuestra red.

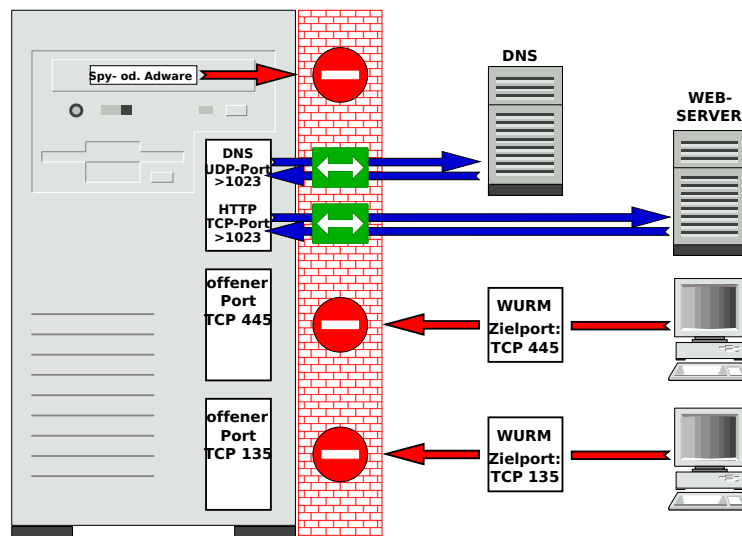
2. ¿Es lo mismo un cortafuegos de red que un cortafuegos personal? ¿Qué tipo de tráfico bloquea un cortafuegos personal y a quien va dirigido dicho tráfico?

Los cortafuegos de red aíslan redes entre sí, normalmente una red más segura y conocida que llamamos LAN (-y coloreamos en verde en los diagramas de red-) y otra red más insegura y fuera de control que llamamos WAN (-y coloreamos en rojo en los diagramas de red-).



En cambio, un cortafuegos personal es un software de cortafuegos que se instala en un PC y que protege únicamente dicho ordenador. Por ejemplo, el cortafuegos personal de Windows. Debido a que se comunica con el sistema operativo, un cortafuegos personal puede llegar a

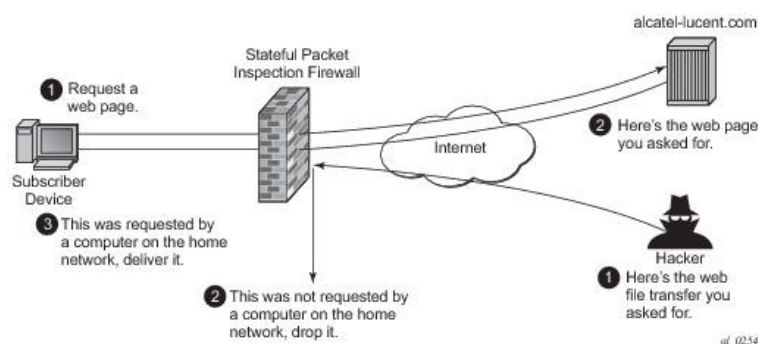
filtrar paquetes teniendo en consideración la aplicación y el usuario que los lanza, así como el contenido del paquete.



3. ¿Qué es un cortafuegos sin estado o "stateless firewall"? ¿Qué diferencia hay con un cortafuegos con estado o "stateful firewall"?

Un cortafuegos sin estado (“primera generación de cortafuegos”) es un cortafuegos que no sabe en que estado se encuentra la conversación TCP de la que le llega un paquete. Solo puede filtrar utilizando IPs y puertos de origen y de destino. Si hemos dejado un puerto abierto, no sabemos si el primer paquete que llega por él es un TCP SYN de inicio de conexión u otro que no tocaba. Si un ordenador se comunica con el exterior, hemos de dejar puertos abiertos para asegurarnos que la respuesta del exterior entra.

Sin embargo, un cortafuegos con estado (“segunda generación de cortafuegos”), tiene memoria y recuerda el estado de la comunicación TCP para comprobar, no ya si las IPs y puertos son los adecuados, sino si ese paquete corresponde al estado de la conexión que toca. En un cortafuegos con estado podemos, por ejemplo, decirle que deje pasar los paquetes del exterior sólo si son respuesta a una comunicación iniciada desde el interior.



4. ¿Puede un cortafuegos incorporar reglas dinámicamente desde aplicaciones? Pon un ejemplo. Sí, a medida que un cortafuegos funciona se pueden añadir nuevas reglas de filtrado.

Imagina por ejemplo un Sistema de Prevención de Intrusos (IPS) que si detecta muchos intentos de acceso SSH infructuosos desde una misma IP, añade una regla de cortafuegos para bloquear dicha IP. O imagina un IPS que si detecta un ataque de denegación de servicio (DOS), añade una regla de cortafuegos para bloquear las IPs que lanzan el ataque.

5. ¿Qué es una DMZ ("zona desmilitarizada") y para qué sirve?

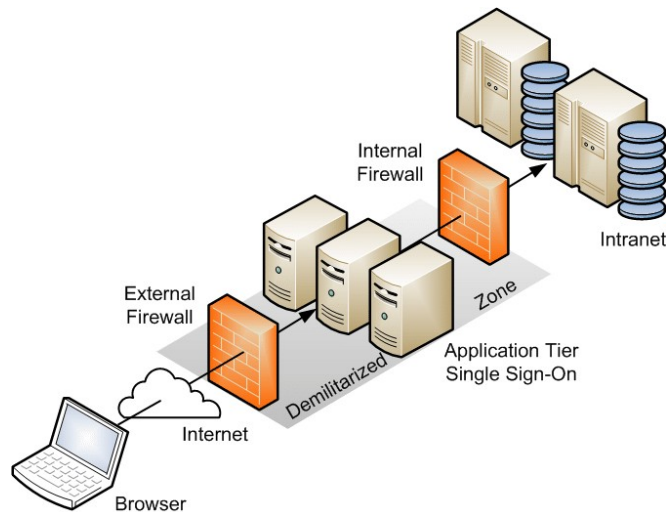
Imagina que tienes tu red protegida del exterior por un cortafuegos detrás de tu router. Sin embargo, existen algunos servicios de tu red a los que quieres dar acceso a clientes de Internet, por lo que abres puertos en el cortafuegos para dejar pasar dicho tráfico. Entonces, si un atacante del exterior consigue, mediante tráfico permitido, tomar control del servidor que está dentro de tu red, puede explorar y atacar el resto de tu red desde dicho servidor, ya que el tráfico interno de tu red no está monitorizado ni bloqueado por el cortafuegos.

Cuando hay sólo una línea de defensa, si el atacante la sobrepasa gana el control de todo. Por ejemplo, el caso de la [línea Maginot](#) en la Segunda Guerra Mundial.

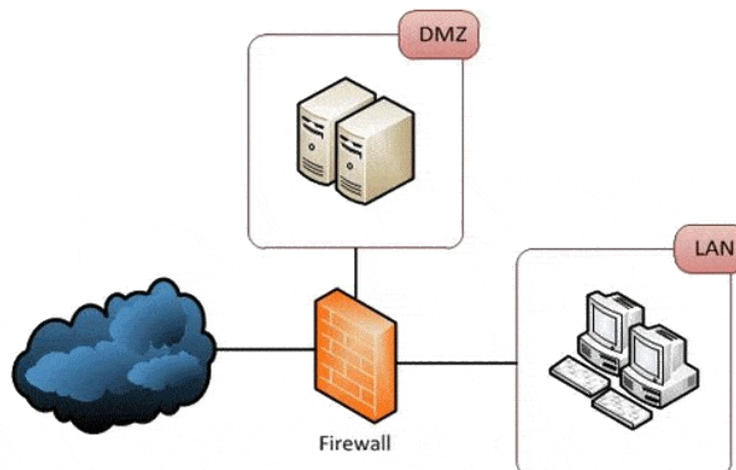
Vamos a aplicar el concepto de seguridad perimetral, en la que no hay una sola línea de defensa, sino varios perímetros defensivos. Si el atacante sobrepasa una línea de protección, detrás encuentra una segunda línea de protección resguardando ítems más valiosos. Piensa en el diseño urbanístico de las [ciudades medievales](#): una muralla protegía toda la ciudad, pero la tenían que abrir para que durante el día entraran mercaderes, por lo que en el interior había una segunda muralla llamada ciudadela protegiendo los palacios.

Una DMZ es una zona de nuestra red (-que coloreamos en naranja en los diagramas de red-), que es parcialmente insegura porque pueden acceder desde el exterior. Separamos nuestra red mediante cortafuegos en dos zonas: la DMZ a la que pueden acceder desde el exterior a algunos servicios que queremos que sean públicos, y la red más interna con el resto de equipos y servidores, a la que protegemos tanto del exterior como de nuestra DMZ.

Podemos conseguir una DMZ utilizando dos cortafuegos que separan dos redes:



También podemos conseguir una DMZ utilizando un único cortafuegos que separa tres redes:



6. ¿Qué es una política restrictiva? ¿Qué es una política permisiva?

Imagina un profesor en la puerta de clase con la lista “negra” de alumnos que no pueden entrar, que deja entrar a todos los que no están en dicha lista. Pues política permisiva es un cortafuegos con reglas que rechazan paquetes y una política por defecto que deja pasar cualquier paquete que no encaje con ninguna de dichas reglas.

Imagina un vigilante en la puerta de una fiesta con la lista “blanca” de invitados que pueden entrar, que prohíbe el acceso a todos los que no están en dicha lista. Pues política restrictiva es un cortafuegos con reglas que aceptan paquetes y una política por defecto que impide pasar cualquier paquete que no encaje con ninguna de dichas reglas.

Normalmente las políticas permisivas son más fáciles de implementar, pero las políticas restrictivas son más seguras.

7. ¿Viene algún software cortafuegos con Windows Server? ¿Desde dónde se instala y desde dónde se administra? ¿Cuál es el software de cortafuegos comercial más conocido para Windows?

Con Windows viene el cortafuegos personal de Windows. Además, todos los antivirus comerciales traen software de cortafuegos personal integrado. Y por si fuera poco hay otro software de cortafuegos personal como [Zone Alarm](#) y [Comodo Firewall](#).

Sin embargo, no conozco ningún software que convierta un Windows en un cortafuegos de red.

8. ¿Cuál es el software de cortafuegos más conocido para Linux? ¿Y para otros sistemas Unix? ¿Qué sistema Unix y distribuciones Linux son especialmente seguras para instalar PCs que hagan de cortafuegos y sistemas de detección de intrusos?

El filtro de paquetes de Linux se llama [Netfilter](#), y en BSD se llama [IPFilter](#).

A dicho cortafuegos se le añaden reglas mediante comandos como [iptables](#), [nftables](#) y [ufw](#).

También se pueden añadir reglas mediante interfaz gráfica como [gufw](#), [fwbuilder](#) y [shorewall](#).

Por último, existen distribuciones de Linux y BSD que convierten un PC con varias tarjetas de red en un cortafuegos de red administrado remotamente vía web. Entre ellas están [Endian](#), [pfSense](#), [OPNsense](#), o [IPFire](#).

9. En el instituto necesitamos proteger la secretaria de posibles ataques. Concretamente queremos proteger los datos de los alumnos que están en un servidor dedicado llamado *Oficinas*. Las secretarías acceden a las aplicaciones administrativas mediante un cliente web que se conecta a un servidor web seguro (HTTPS, puerto 443) en *Oficinas*. Dicho servidor ejecuta páginas dinámicas escritas en PHP que realizan consultas sobre un servidor de bases de datos (MySQL, puerto 3306).

Queremos que solamente el servidor web seguro sea accesible por los navegadores de las secretarías (IPs 192.168.0.4 y 192.168.0.5) y por SSH desde el ordenador del administrador de sistemas (IP 192.168.0.99). Por otro lado queremos que el servidor *Oficinas* únicamente pueda establecer conexión con el exterior para actualizarse (<http://security.ubuntu.com/ubuntu>).

a) Piensa dónde colocarías el cortafuegos y dibuja un esquema de la red.

Aunque el enunciado dice que queremos proteger secretaria, y hay quien optaría por poner un cortafuegos de red para proteger toda la red de oficinas, fíjate que en realidad todas las medidas van a proteger al servidor de oficinas. Quizás con un cortafuegos personal para este

equipo sea suficiente.

b) Escribe las reglas del cortafuegos en la siguiente tabla:

red origen	puerto origen	red destino	puerto destino	protocolo	estado	acción
192.168.0.4		IP servidor	443	TCP		ACCEPT
192.168.0.5		IP servidor	443	TCP		ACCEPT
192.168.0.99		IP servidor	22	TCP		ACCEPT
IP servidor		IP servidor	3306	TCP		ACCEPT
IP servidor					Respuesta	ACCEPT
IP servidor		IP serv DNS	53	UDP		ACCEPT
IP serv DNS	53	IP servidor		UDP		ACCEPT
IP servidor		serv. Ubuntu	80	TCP		ACCEPT
		IP servidor		TCP	Respuesta	ACCEPT
						DENY

10. Queremos instalar un cortafuegos en una pequeña red local de cinco PCs y un servidor HTTP y SQL, todos con IP privada y salida a Internet. Dicho cortafuegos debe proteger los ordenadores de la red de ataques del exterior. También debe proteger el servidor SQL de los ordenadores de la red interna y del exterior, que sólo accederán al servicio de HTTP. (el servicio SQL es accedido sólo por el servicio HTTP del mismo ordenador para crear páginas web dinámicas a partir de la base de datos, pero no queremos que los usuarios realicen consultas directas sobre el servidor de bases de datos). De momento dejamos que los usuarios de nuestra red accedan a cualquier servicio de Internet.

a) Piensa dónde colocarías el cortafuegos y dibuja un esquema de la red.

Necesitamos un cortafuegos de red que proteja toda la red. La cuestión es si ponemos al servidor en una DMZ o le ponemos un cortafuegos personal. Yo opto por la DMZ en un cortafuegos con tres interfaces de red. Un dato que falta: asumo el servidor DNS en Internet.

b) Escribe las reglas del cortafuegos en la siguiente tabla:

red origen	puerto origen	red destino	puerto destino	protocolo	estado	acción
mired		internet				ACCEPT
internet		mired			Respuesta	ACCEPT
internet		mired				DENY
DMZ		internet				ACCEPT
internet		DMZ serv	80	TCP		ACCEPT
internet		DMZ			Respuesta	ACCEPT
internet		DMZ				DENY
mired		DMZ serv	80	TCP		ACCEPT
mired		DMZ				DENY
DMZ serv		mired			Respuesta	ACCEPT
DMZ serv		mired				DENY

Práctica inicial

Vamos a aplicar las reglas de la tabla del anterior ejercicio 9 utilizando la distribución *IPFire*, que convierte un equipo con varias tarjetas de red en un encaminador con cortafuegos. Otras distribuciones igual de válidas son *pfSense* y *OPNsense*, por ejemplo.

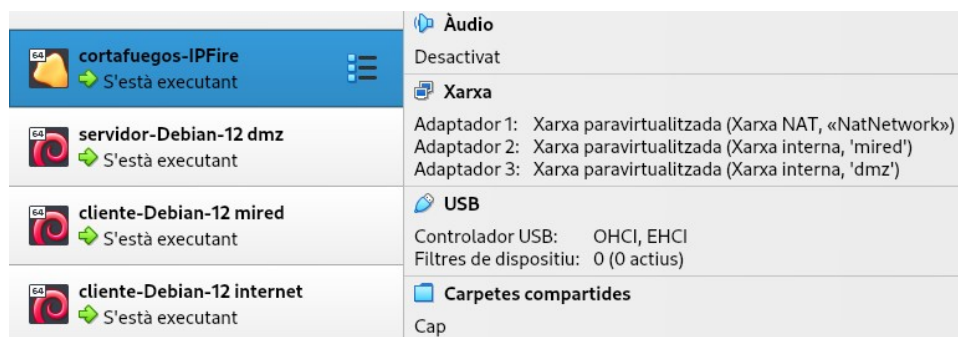
Lo primero que tiene de quedarte claro es que hay muchas soluciones. Todo depende cómo quieras configurar tu red: ¿Querrás DMZ para el servidor o no? ¿Querrás IPs privadas para tu red o no? ¿Qué tipo de red utilizarás en VirtualBox para simular Internet? Tú lo decides, pero cada una de estas decisiones te llevará a una solución o a otra, todas válidas según el caso.

Yo he escogido tener el servidor en una DMZ, utilizar IPs privadas para mis redes, y poner la tarjeta de red de Internet en modo “red NAT”. Estas elecciones no son mejores ni peores que otras. Piensa las anteriores cuestiones y toma tus propias decisiones, de manera razonada. Si no tienes claro que infraestructura montarás y el por qué, no puedes continuar avanzando ni aprender, ya que no sabes lo que te traes entre manos.

Lo segundo que debes hacer es crear la infraestructura de red, es decir, poner las diferentes máquinas virtuales en red. Apenas me detendré en estos pasos, porque me quiero centrar en la solución del cortafuegos. Doy por hecho que sabes instalar IPFire y poner máquinas en red en VirtualBox.

Preparación:

1. Crea una máquina virtual con tres tarjetas de red:
 - a) Red NAT para Internet (zona insegura , color “rojo”, IP por DHCP).
 - b) Red interna “mired” para tu red (zona segura , color “verde”, IP 192.168.100.1).
 - c) Red interna “dmz” para tu DMZ (zona semisegura , color “naranja”, IP 192.168.200.1).



2. Instala *IPFire*, con servicio de DHCP para la red “verde”. Por ejemplo que el DHCP reparta de la 192.168.100.30 a 192.168.100.9 y DNS 1.1.1.1.
3. Consigue tres máquinas virtuales para hacer las pruebas:
 - a) Una la colocarás en Internet (su tarjeta de red en “red NAT”),
 - b) otra la colocarás en tu red (su tarjeta de red en red interna “mired” recibirá IP del router),

c) y la otra será el servidor que colocarás en la DMZ (su tarjeta de red en red interna “dmz” le configurarás IP estática, por ejemplo 192.168.200.5, con gateway 192.168.200.1 y DNS 1.1.1.1).

4. Para distinguirlas rápidamente en pantalla, a la de mi red ponle fondo de pantalla verde, a la de la DMZ ponle fondo de pantalla naranja, y a la de internet ponle fondo de pantalla rojo.
5. Prueba que estas tres máquinas virtuales tengan red y acceso a Internet, por ejemplo haciendo ping a www.xtec.cat. Después, comprueba si se ven entre ellas:
 - a) La de Internet no puede hacer ping ni a la dmz ni a mi red, porque escogí IPs privadas.
 - b) La de mi red sí hace ping a la dmz y sí hace ping a Internet.
 - c) La de la dmz no hace ping a la de mi red y sí hace ping a Internet

6. Acabamos de configurar el servidor instalando algunos servicios, como por ejemplo HTTP, HTTPS, SQL o SSH:

```
$ sudo apt update
```

```
$ sudo apt install apache2 openssh-server mariadb-server
```

Si quieres HTTPS, para tener más puertos con los que jugar en el cortafuegos:

```
$ sudo a2enmod ssl
```

```
$ sudo systemctl restart apache2
```

Por defecto el servidor SQL no es accesible desde otras máquinas, y no es necesario protegerlo con el cortafuegos. Si queremos dejarlo expuesto a la red por el puerto 3306 para hacer pruebas con el cortafuegos, edita su fichero de configuración (en mi caso /etc/mysql/mariadb.conf.d/50-server.cnf) para habilitar la línea:

```
bind-address 0.0.0.0
```

Y accede al servidor SQL con el comando `sudo mysql -u root -p` para crear un usuario administrador que pueda acceder desde cualquier equipo:

```
GRANT ALL PRIVILEGES ON *.* TO 'pepito'@'%' IDENTIFIED BY 'grillo' WITH  
GRANT OPTION;
```

Comprueba en qué puertos escuchan los servicios:

```
sudo ss -pnta | grep LISTEN
```

7. Con la máquina de la red interna entra al gestor web de IPFire, navegando a la URL <https://192.168.100.1:444/> y accediendo con usuario *admin* y la contraseña que escogiste en la instalación para dicho usuario. Explora las opciones de dicha interfaz web administrativa.

Muy bien, esta era la preparación de la infraestructura para las pruebas. Ahora accedemos a la configuración web del cortafuegos y “comienza” el ejercicio:

Sistema Estado Red Servicios

Cortafuegos IPFire Registros

Tráfico: Ent. 0.00 bit/s Sal. 0.00 bit/s

Reglas del Cortafuegos

Reglas del Cortafuegos

Grupos Cortafuegos

Opciones del Cortafuegos

Detección de Intrusiones

Listas de bloqueo de direcciones IP

Bloquear ubicación

Acceso a BLUE

IPTables

Reglas del Cortafuegos

#	Protocolo:	Origen	Destino	Acción
1	TCP	Cualquiera	RED: SMTP	<input checked="" type="checkbox"/>
Block port 25 (TCP) for outgoing connections to the internet				
Green		Internet (Permitido)	ORANGE (Permitido)	
ORANGE		Internet (Permitido)	Green (Bloqueado)	
Política: Permitido				

Ya ves que tenemos una regla de ejemplo para filtrar correo electrónico saliente (SMTP) que nos sobra, y también que la política de la dmz (ORANGE) a la red interna (Green) es bloqueado. Observa bien las políticas por defecto, ya que son las que se aplicarán a los paquetes que no encajen en ninguna regla de las que pongamos.

Borro la regla de ejemplo y añado mis reglas una a una, probándolas a medida que las añado, y clasificandolas en seis grupos para organizarme mejor:

mired → internet, mired → dmz, dmz → internet, dmz → mired, internet → mired, internet → dmz

1. Mi red interna puede salir Internet sin restricciones:

Como esto ya es así, no debo añadir ninguna regla.

2. Mi red interna no debe iniciar conexión a la DMZ excepto al servidor web:

Debo cambiar la política por defecto del tráfico green a ORANGE a bloquear, y habilitar tráfico al puerto 80 y 443. No sé cambiar la política por defecto de IPFire (-quizás no se puede-), así que añado una regla que deniegue el tráfico.

Recuerda que el orden de las reglas será importante.

Pruebo que des de mi red interna puedo navegar por el servidor, pero no hacer SQL, SSH o ping.

Reglas del Cortafuegos

#	Protocolo:	Origen	Registro	Destino	Acción
1	TCP	Green	<input type="checkbox"/>	192.168.200.2: 80	<input checked="" type="checkbox"/>
2	TCP	Green	<input type="checkbox"/>	192.168.200.2: 443	<input checked="" type="checkbox"/>
3	Todos	Green	<input type="checkbox"/>	ORANGE	<input checked="" type="checkbox"/>
Green		Internet (Permitido)	ORANGE (Permitido)		
ORANGE		Internet (Permitido)	Green (Bloqueado)		
Política: Permitido					

3. Mi DMZ puede salir Internet sin restricciones:

Como esto ya es así, no debo añadir ninguna regla.

4. Mi DMZ no debe poder establecer conexiones con máquinas de mi red interna:

Como esto ya es así, no debo añadir ninguna regla.

5. Internet no debe poder establecer conexiones con máquinas de mi red interna:

Como esto ya es así, porque tienen IPs privadas, no debo añadir ninguna regla.

6. Internet debe poder acceder a los puertos del servicio web en la DMZ:

Como el servidor tiene una IP privada, debo abrir reenvío de puertos en el encaminador. Esto quiere decir que des de Internet no pueden acceder al servicio web poniendo la IP del servidor, sino tan solo la IP pública del router, y que el router tendrá una regla de cortafuegos NAT que transforme la IP de destino, cambiando la IP del router en el paquete a la IP del servidor.

Para sentirnos más seguros buscamos “IPFire port forwarding” , o “IPFire NAT” y encontramos una guía: <https://www.ipfire.org/docs/configuration/firewall/rules/port-forwarding>

Reglas del Cortafuegos ⓘ

Origen	
<input type="radio"/> Dirección de origen (dirección MAC/IP o red):	<input type="radio"/> Firewall
<input checked="" type="radio"/> Redes estándar:	<input type="text" value="RED"/>
<input type="radio"/> Ubicación	<input type="text" value="A1 - Anonymous Proxy"/>

NAT	
<input checked="" type="checkbox"/> Usar traducción de direcciones de red (NAT)	
<input checked="" type="radio"/> NAT de destino (DNAT - reenvío de puertos)	Interfaz del Cortafuegos: <input type="text" value="- Automático -"/>
<input type="radio"/> NAT de origen (SNAT)	

Destino	
<input checked="" type="radio"/> Dirección de destino (dirección IP o red):	<input type="radio"/> Firewall
<input type="text" value="192.168.200.2"/>	<input type="text" value="Todos"/>
<input type="radio"/> Redes estándar:	<input type="text" value="Cualquiera"/>
<input type="radio"/> Ubicación	<input type="text" value="A1 - Anonymous Proxy"/>

Protocolo	
<input type="text" value="TCP"/>	
Puerto de origen:	Puerto de destino: <input type="text" value="80"/>
	Puerto externo (NAT): <input type="text" value="80"/>

Reglas del Cortafuegos

#	Protocolo:	Origen	Registro	Destino	Acción
1	TCP	Green	<input type="checkbox"/>	192.168.200.2: 80	<input checked="" type="checkbox"/>
2	TCP	Green	<input type="checkbox"/>	192.168.200.2: 443	<input checked="" type="checkbox"/>
3	Todos	Green	<input type="checkbox"/>	ORANGE	<input checked="" type="checkbox"/>
4	TCP	RED	<input type="checkbox"/>	Cortafuegos : 80 ->192.168.200.2: 80	<input checked="" type="checkbox"/>
5	TCP	RED	<input type="checkbox"/>	Cortafuegos : 443 ->192.168.200.2: 443	<input checked="" type="checkbox"/>
Green		Internet (Permitido)		ORANGE (Permitido)	
ORANGE		Internet (Permitido)		Green (Bloqueado)	
Política: Permitido					

Pruebo de navegar desde Internet por el servidor de la DMZ escribiendo en el navegador la URL con la IP del router IPFire (<http://10.0.2.5/> en mi caso), y sí puedo.

Datos de la práctica

Tenemos la siguiente configuración en máquinas virtuales:

- En nuestra red local un cortafuegos/router accesible por ssh.
- En nuestra red local un servidor web también accesible por ssh.
- En internet un cliente, para hacer pruebas.

El cortafuegos tendrá dos tarjetas de red para unir Internet con la red local:

- El cliente en Internet y el cortafuegos estarán conectados en modo puente (-si dicho cliente quieres que sea la máquina real o "anfitrión"-) o en red NAT (-si dicho cliente es otra máquina virtual).
- El cortafuegos y el servidor de la red local, máquinas virtuales los dos, estarán conectados en red interna.

Queremos manipular el tráfico en el cortafuegos para que:

- Desde Internet sólo permitiremos tráfico a la red interna hacia el servidor web, a sus puertos 80 y 443.
- Desde la red interna hacia el cortafuegos sólo permitiremos conexiones ssh al puerto tcp/22 y preguntas dns al puerto udp/53.
- Tanto el servidor web como el cortafuegos podrán acceder hacia fuera, excepto al puerto tcp/1337.
- El cortafuegos enrutará de la red interna hacia el exterior.

Práctica

1. Manipula la configuración de las tarjetas de red de las máquinas virtuales del servidor y el cliente para que compartan la misma red interna.

En el caso del cortafuegos, he escogido conectar su primera tarjeta de red (*enp0s3*) a Internet en modo puente, mientras que he conectado su segunda tarjeta de red (*enp0s8*) a la red interna en modo red interna. Ambas tarjetas de red tendrán IP fija. Para la red interna he escogido la IP 10.0.0.1.

En el caso del servidor web, en red interna con el cortafuegos, he escogido darle la dirección IP 10.0.0.2.

nano /etc/network/interfaces

```
auto enp0s3
iface enp0s3 inet static
    address    192.168._mi_subred_._mi_IP_+_100_
    netmask    255.255.255.0
    gateway    192.168._mi_subred_.1

auto enp0s8
iface enp0s8 inet static
    address    10.0.0.1
    netmask    255.255.255.0
```

y a continuación reinicia la red y prueba que ésta funciona:

systemctl restart networking

\$ **ping 10.0.0.2**

2. Configura el cortafuegos, escribiendo para ello un pequeño script que se ejecute al inicio:

nano /root/cortafuegos.sh

```
#!/bin/sh
echo "1" > /proc/sys/net/ipv4/ip_forward

# Vacío reglas

iptables -F
iptables -X
iptables -t nat -F

# Política por defecto

iptables -P INPUT DROP
iptables -P OUTPUT ACCEPT
iptables -P FORWARD DROP

# ¡No nos olvidemos del tráfico de red entre procesos de localhost!

iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT

# Tráfico de entrada a la red interna, y reenvío de puertos
# Como el servidor web está en red interna con IP privada,
# redirijo el puerto 80 del router/cortafuegos al 80 del servidor web
```

```

iptables -t nat -A PREROUTING -i enp0s3 -p tcp --dport 80 -j DNAT --to 10.0.0.2:80
iptables -A FORWARD -i enp0s3 -d 10.0.0.2 -p tcp --dport 80 -j ACCEPT
iptables -A FORWARD -i enp0s3 -m state --state ESTABLISHED -j ACCEPT

# Tráfico de salida a Internet, y enrutamiento con NAT

iptables -A FORWARD -i enp0s8 -p tcp --dport 1337 -j DROP
iptables -A FORWARD -i enp0s8 -j ACCEPT
iptables -t nat -A POSTROUTING -s 10.0.0.0/24 -o enp0s3 -j MASQUERADE

# Sólo dejaré entrar tráfico al cortafuegos des de dentro de la red
# al puerto 22 SSH y al puerto 53 DNS

iptables -A INPUT -i enp0s8 -p tcp --dport 22 -j ACCEPT
iptables -A INPUT -i enp0s8 -p udp --dport 53 -j ACCEPT

# Sólo dejaré entrar tráfico al cortafuegos des de dentro y fuera
# de la red si es tráfico respuesta a una conexión tcp y a dns

iptables -A INPUT -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -i enp0s3 -p udp --sport 53 -j ACCEPT

# Prohíbo tráfico de salida del cortafuegos al puerto 1337
# Permito tráfico de salda del cortafuegos al puerto 53

iptables -A OUTPUT -p tcp --dport 1337 -j DROP
iptables -A OUTPUT -p udp --dport 53 -j ACCEPT

```

chmod +x /root/cortafuegos.sh

y a continuación estableced que el servicio se inicie con el ordenador. Tenemos tres maneras de hacerlo.

a) La manera antigua, con el sistema de arranque *init* seria:

mv /root/cortafuegos.sh /etc/init.d/cortafuegos.sh

update-rc.d cortafuegos.sh defaults

b) La manera moderna, con el sistema de arranque *systemd* seria:

nano /etc/systemd/system/cortafuegos.service

```

[Unit]
Description=Cortafuegos systemd service

[Service]
Type=simple
ExecStart=/bin/bash /root/cortafuegos.sh

[Install]
WantedBy=multi-user.target

```

systemctl start cortafuegos

systemctl status cortafuegos

systemctl enable cortafuegos

c) Pero en Debian y Ubuntu tenemos una tercera manera. Cuando tenemos reglas de cortafuegos que están funcionando bien, si instalamos el paquete *iptables-persistent*, dichas reglas se harán persistentes y se cargarán en cada nuevo arranque del equipo:

```
# apt install iptables-persistent
```

Referencias

- <http://en.wikipedia.org/wiki/Firewall>
- <http://www.docum.org/docum.org/kptd/>
- <https://www.digitalocean.com/community/tutorials/a-deep-dive-into-iptables-and-netfilter-architecture>
- <http://pello.io/filez/firewall/iptables.html>
- <https://wiki.nftables.org/wiki-nftables/>
- `man iptables`, `man iptables-extensions`, `man nft`