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?

...

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?

...

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

...

4. ¿Puede un cortafuegos incorporar reglas dinámicamente des de aplicaciones? Pon un ejemplo

...

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

...

6. ¿Qué es un cortafuegos a nivel de paquete? ¿Qué es un cortafuegos a nivel de circuito? ¿Qué es un cortafuegos a nivel de aplicación?

...

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?

...

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?

...

9. Queremos instalar un cortafuegos en una pequeña red local de cinco PCs y un servidor HTTP y SQL, todos con IP pública 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.

...

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

red origen	puerto origen	red destino	puerto destino	protocolo	estado	acción

10. En el ejercicio anterior que normas añadirías al cortafuegos para impedir que los usuarios de nuestra red accedan al exterior excepto a un servidor de correo que utiliza IMAP y SMTP en los puertos estándar.

red origen	puerto origen	red destino	puerto destino	protocolo	estado	acción

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:

- Des de Internet sólo permitiremos tráfico a la red interna hacia el servidor web, a sus puertos 80 y 443.
- Des de 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**

1. 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`