CORTAFUEGOS

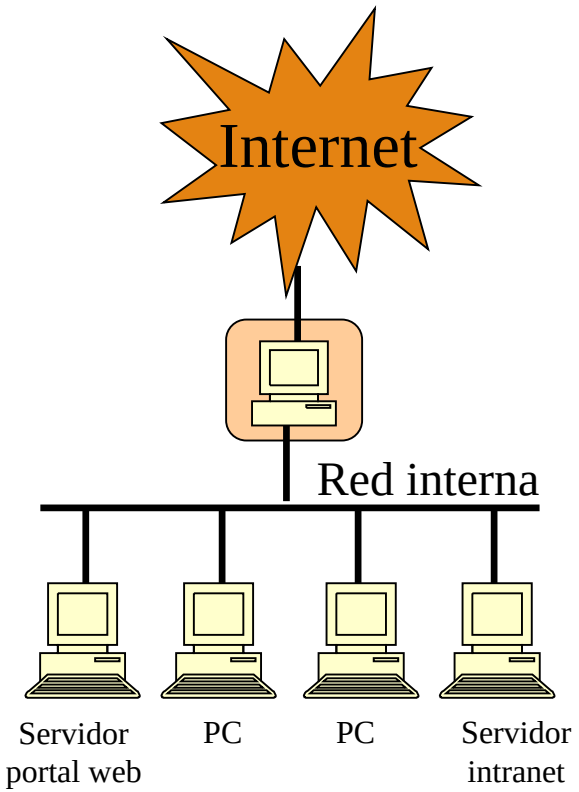
Cortafuegos

Supervisan todo el tráfico de red externo de una organización para asegurarse de que encaja con la política de seguridad definida

Pueden actuar a dos niveles básicos:

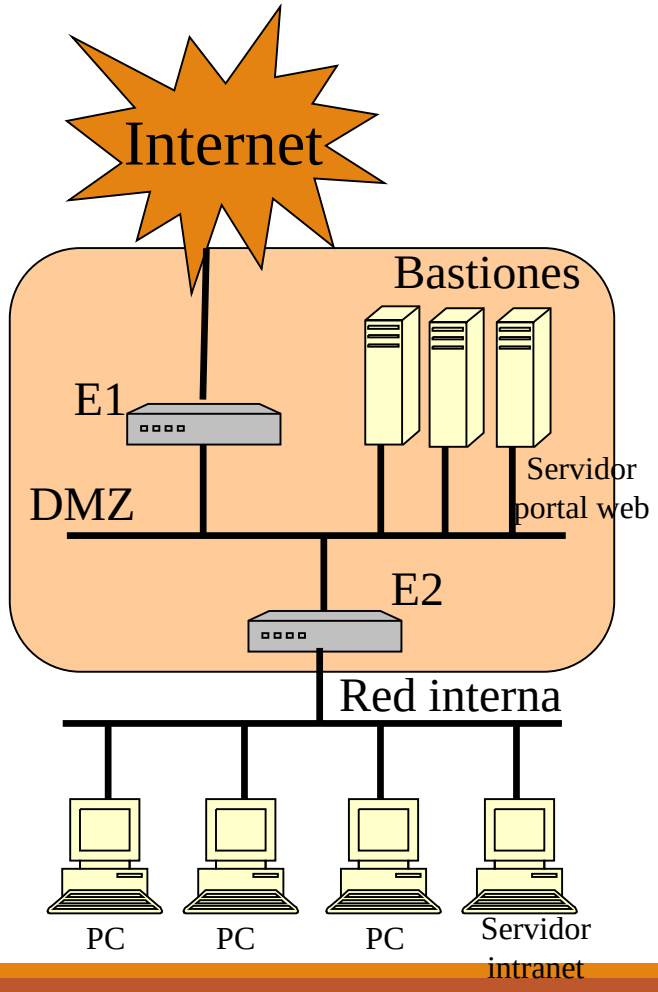
- Transporte/red: filtro de paquetes en base a direcciones IP, puertos de origen/destino y tipo de paquete. No examinan el contenido
- Aplicación: examinan un protocolo de aplicación y actúan como intermediarios (*proxy*)

Configuración sencilla



- El cortafuegos es un equipo con dos interfaces que actúa como encaminador y filtro de paquetes y, opcionalmente, como intermediario y NAT.
- Los equipos de la red interna simplemente encaminan sus paquetes a través del cortafuegos, como si fuera un encaminador corriente
- Configuración relativamente insegura

Configuración con bastiones



- El encaminador/filtro de paquetes E1 sólo permite tráfico entre los bastiones y la Internet
- Algunos bastiones actúan como servidores visibles desde el exterior (web, correo…) y otros actúan como intermediarios (*proxy*) para los ordenadores de la red interna
- El encaminador/filtro de paquetes E2 sólo permite tráfico entre la red interna y los bastiones intermediarios
- Los equipos de la red interna solo pueden acceder a Internet a través de un bastión intermediario, el cual puede imponer filtros
- Se puede usar NAT para los equipos de la red interna

Configuración de IPFW

/etc/rc.conf

- firewall_enable="YES"
- firewall_type="tipo"
- firewall_logging="YES"
- gateway_enable="YES"

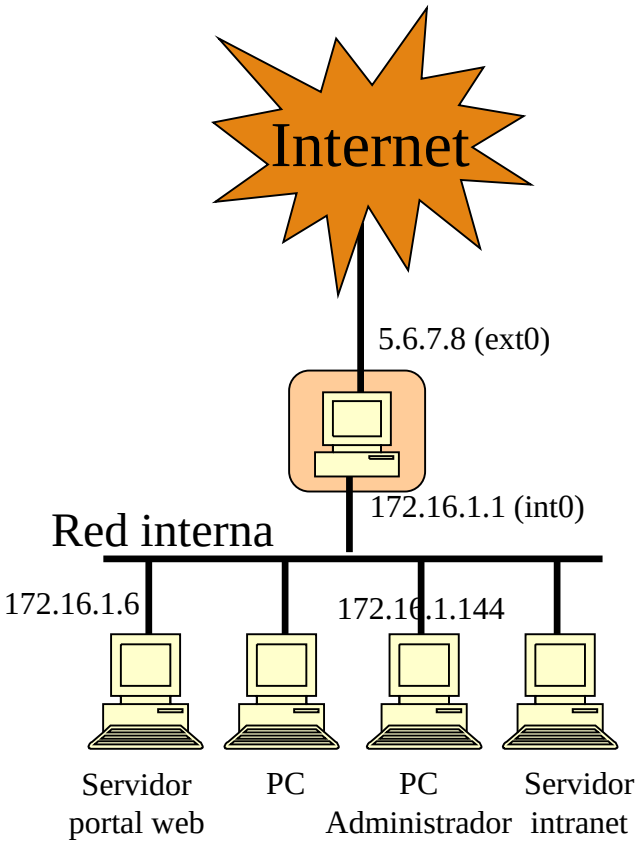
Tipos disponibles

- OPEN, CLIENT, SIMPLE, CLOSED…
- Fichero específico

NAT

- natd_enable="YES"
- natd_interface="interfaz_pública"
- natd_flags="-f /usr/local/etc/natd.conf"

Ejemplo de IPFW (I)




```
# ext0: Interfaz externa, 5.6.7.8

# int0: Interfaz interna, 172.16.1.1

# 172.16.1.0/24: subred interna

# 5.6.7.0/24: subred externa

# 1.2.3.4: servidor DNS externo

# 172.16.1.6: servidor WWW

# Se permite todo el tráfico
 saliente a web y NTP

# Se permite acceder mediante SSH al
 cortafuegos desde 172.16.1.144
```

Ejemplo de IPFW (II)

```
# Reglas de base para el cortafuegos: en negro
# Filtrado preventivo: en púrpura
# Tráfico entrante permitido: en verde
# Tráfico saliente permitido: en naranja
# Tráfico entrante permitido al cortafuegos: en azul
# NAT: en rojo
```

Ejemplo de IPFW (III)

```
# Interfaz local
add allow ip from any to any via lo0
# Filtrar direcciones imposibles
add deny ip from any to 127.0.0.0/8
add deny ip from 127.0.0.0/8 to any
add deny ip from 172.16.1.0/24 to any in via ext0
add deny ip from 5.6.7.0/24 to any in via int0
```

Ejemplo de IPFW (IV)

```
# Filtrar RFC1918 y otras hacia el exterior
add deny ip from any to 10.0.0.0/8 via ext0
add deny ip from 10.0.0.0/8 to any via ext0
# Idem con 172.16.0.0/12, 192.168.0.0/16, 0.0.0.0/8,
# 169.254.0.0/16, 192.0.2.0/24, 224.0.0.0/4 y
# 240.0.0.0/4 (salvo que realmente se usen para algo)
# Traducción mediante NAT en la interfaz pública
add divert 8668 ip from any to any via ext0
```

Ejemplo de IPFW (V)

```
# Permitir conexiones TCP abiertas, fragmentos IP y
# reglas dinámicas
# add allow tcp from any to any established
add check-state
add allow log tcp from me to any setup k-s
add allow log udp from me to any k-s
# ICMP. Se permite todo
# También podría filtrarse por tipos (icmptypes)
add allow icmp from any to any
```

Ejemplo de IPFW (VI)

```
# Tráfico entrante permitido a servidores (tras NAT)
# El resto se deniega y se registra (al final)
add allow log tcp from any to 172.16.1.6 http setup k-s
add allow log tcp from any to 172.16.1.6 https setup k-s
# Tráfico entrante permitido al propio cortafuegos
add allow tcp from 172.16.1.144 to 172.16.1.1 ssh setup k-s
```

Ejemplo de IPFW (VII)

```
# Tráfico saliente permitido (antes de NAT)
# El resto se deniega y se registra (al final)
add allow log tcp from 172.16.1.0/24 to any http setup k-s
add allow log tcp from 172.16.1.0/24 to any https setup k-s
add allow udp from 172.16.1.0/24 to 1.2.3.4 domain k-s
add allow tcp from 172.16.1.0/24 to 1.2.3.4 domain setup k-s
add allow udp from 172.16.1.0/24 to any ntp k-s
# Todo lo demás se prohíbe y se registra
add deny log ip from any to any
```

Ejemplo de IPFW (VIII)

```
# Redirección de puertos (natd.conf)
redirect_port tcp 172.16.1.6:80 80
redirect_port tcp 172.16.1.6:443 443
```

Servicios "fáciles" de filtrar

Orientados a la conexión (TCP)

Usan puertos conocidos fijos

Inician la conexión desde el cliente

Usan una sola conexión por sesión, y viceversa

Usan un protocolo bien diseñado desde el punto de vista de la seguridad