Práctica 5: DMZ con doble firewall usando Shorewall

-MANUEL CACHALDORA BORRAJO
-LUCAS GÓNZALEZ TORRES
-MARTÍN GÓMEZ CARREÑO

1. Descripción breve del filtrado realizado por cada cortafuegos

El objetivo del ejercicio es configurar dos cortafuegos, denominados *acceso* y *contención*, utilizando Shorewall para gestionar el tráfico entre tres zonas: la red interna, la DMZ y la red externa.

Cortafuegos de Acceso:

El cortafuegos de acceso regula el tráfico entre la red externa y los equipos de la DMZ, así como el tráfico entre la red externa y la red interna.

Este cortafuegos realiza las siguientes funciones principales:

-Enmascaramiento (SNAT):
Traducción de las direcciones de origen para la red interna (10.10.10.0/24) y la DMZ (10.20.20.0/24) en el tráfico saliente hacia la red externa.

-Redirección (DNAT):
Las conexiones entrantes desde la red externa hacia servicios públicos de la DMZ (HTTP, HTTPS, SMTP y POP3) son redirigidas a la máquina en la DMZ (10.20.20.22).

-Filtrado de tráfico:
*Permite únicamente conexiones entrantes desde la red externa a los servicios públicos especificados.
*Permite el tráfico desde la red interna hacia la red externa solo para servicios web (HTTP y HTTPS) y SSH.
*Controla el acceso desde la red interna hacia la DMZ.

Cortafuegos de Contención:

El cortafuegos de contención regula el tráfico entre la red interna, la DMZ y la red externa.

No realiza enmascaramiento de direcciones, ya que esta tarea se delega al cortafuegos de acceso.

Las principales funciones del cortafuegos de contención son:

-Filtrado de tráfico:
*Permite tráfico desde la red interna hacia la DMZ para servicios específicos (HTTP, HTTPS, SMTP, POP3 y SSH).
*Permite conexiones desde la DMZ hacia la red interna solo para el servicio MySQL.
*Permite consultas DNS desde la red interna y la DMZ hacia la red externa.

-Política de denegación por defecto:
Todas las conexiones no explícitamente permitidas son denegadas y registradas.

2. Detallar la configuración Shorewall empleada en el cortafuegos de acceso

2.1. Definición de zonas empleada:

En el cortafuegos de acceso se definen las siguientes zonas:
***net:** Corresponde a la red externa (193.147.87.0/24).
***dmz:** Representa la zona desmilitarizada (10.20.20.0/24).
***fw:** Es la zona interna del cortafuegos.

2.2. Ficheros de configuración:

Archivo zones: /etc/shorewall/zones

# ZONE	TYPE	OPTIONS
fw	firewall	
dmz	ipv4	
net	ipv4	

Archivo interfaces: /etc/shorewall/interfaces

# ZONE	TYPE	OPTIONS
net	enp0s8	dhcp,nosmurfs
dmz	enp0s83	dhcp,nosmurfs
loc	enp0s9	dhcp,nosmurfs

Archivo hosts: /etc/shorewall/hosts

# ZONE	TYPE	OPTIONS
dmz	enp0s3:10.20.20.0/24	

Archivo policy: /etc/shorewall/policy

# SOURCE	DEST	POLICY	LOG LEVEL
fw	all	ACCEPT	
net	all	DROP	info
dmz	all	DROP	
all	all	REJECT	info

Archivo rules: /etc/shorewall/rules

# ACTION	SOURCE	DEST	PROTO	DPORT
DNAT	net	dmz:10.20.20.22	tcp	80,443
DNAT	net	dmz:10.20.20.22	tcp	25,110
ACCEPT	dmz	net	tcp	53
ACCEPT	dmz	net	udp	53
ACCEPT	loc	dmz:10.20.20.22	tcp	80,443
ACCEPT	loc	net	tcp	80,443
ACCEPT	loc	net	tcp	22
ACCEPT	loc	dmz	tcp	22

Archivo snat: /etc/shorewall/snat

# ACTION	SOURCE	DEST
MASQUERADE	10.10.10.0/24	enp0s8
MASQUERADE	10.20.20.0/24	enp0s8

3. Detallar la configuración Shorewall empleada en el cortafuegos de contención

3.1. Definición de zonas empleada

En el cortafuegos de contención se definen las siguientes zonas:
***loc:** Corresponde a la red interna (10.10.10.0/24).
***dmz:** Representa la zona desmilitarizada (10.20.20.0/24).
***fw:** Es la zona interna del cortafuegos.

3.2. Ficheros de configuración

Archivo zones

# ZONE	TYPE	OPTIONS
fw	firewall	
dmz	ipv4	
net	ipv4	

Archivo interfaces

# ZONE	TYPE	OPTIONS
loc	enp0s3	dhcp,nosmurfs
dmz	enp0s8	dhcp,nosmurfs

Archivo hosts

# ZONE	HOST(S)	OPTIONS
loc	enp0s3:10.10.10.0/24	
dmz	enp0s8:10.20.20.0/24	

Archivo policy

# SOURCE	DEST	POLICY	LOG LEVEL
fw	all	ACCEPT	

loc	all	DROP	info
dmz	all	DROP	
all	all	REJECT	info

Archivo rules

# ACTION	SOURCE	DEST	PROTO	DPORT
ACCEPT	loc	dmz:10.20.20.22	tcp	80,443
ACCEPT	loc	dmz:10.20.20.22	tcp	25,110
ACCEPT	loc	dmz	tcp	22
ACCEPT	dmz	loc:10.10.10.11	tcp	3306
ACCEPT	loc	net	tcp	53
ACCEPT	loc	net	ucp	53

```
# ACTION   SOURCE    DEST        PROTO   DPORT
ACCEPT     loc       dmz         tcp     80,443
ACCEPT     loc       dmz         tcp     25,110
ACCEPT     loc       dmz         tcp     22
ACCEPT     dmz       loc:10.10.10.11 tcp  3306
ACCEPT     loc       net         tcp     53
ACCEPT     loc       net         udp     53
```

4. Descripción de las pruebas de funcionamiento realizadas

Para verificar el cumplimiento de las reglas de filtrado, se realizaron escaneos de puertos con nmap desde las diferentes máquinas del entorno (fuera, dmz, dentro) hacia las demás. A continuación, se detallan los resultados obtenidos:

Escaneo desde la máquina externa (fuera)
nmap -P0 -T4 193.147.87.47

Resultados: Solo están abiertos los puertos HTTP (80), HTTPS (443), SMTP (25) y POP3 (110) hacia la máquina de la DMZ (10.20.20.22).

Escaneo desde la máquina interna (dentro)
nmap -P0 -T4 10.10.10.1 10.20.20.22

Resultados: Se confirma acceso a los servicios web (HTTP, HTTPS) y correo (SMTP, POP3) en la DMZ, y acceso SSH a ambas máquinas.

Escaneo desde la máquina de la DMZ
nmap -P0 -T4 10.10.10.11

Resultados: Solo está abierto el puerto MySQL (3306) hacia la máquina interna.

Conclusión

La configuración realizada cumple con los requisitos establecidos, asegurando que:

*El tráfico permitido se restringe a las reglas definidas en los cortafuegos de acceso y contención.
*Se garantiza la seguridad de las redes mediante políticas de denegación por defecto.
*Se cumple con los servicios específicos permitidos, como se verificó en las pruebas con nmap

---