Actividad 1: Mecanismos de Defensa en Redes

Seguridad en Redes y Análisis Inteligente de Amenazas

Alumno: Julio Ortiz Bort

14 de diciembre de 2025

Índice

1. Introducción

La presente memoria documenta el proceso de análisis, diseño y aplicación de mecanismos de defensa en una arquitectura de red corporativa basada en la herramienta NETinVM. La actividad tiene como objetivo reforzar los conocimientos sobre topologías seguras, cortafuegos y la gestión de una DMZ mediante la configuración adecuada de reglas de `iptables` en el cortafuegos (FW).

2. Descripción de la topología

Para esta práctica se desplegó una topología con tres segmentos:

- **Red externa (Internet):** 10.5.0.0/24
- **DMZ:** 10.5.1.0/24
- **Red interna:** 10.5.2.0/24

El cortafuegos FW interconecta los tres segmentos mediante:

- `eth0`: 10.5.0.254 (Internet)
- `eth1`: 10.5.1.254 (DMZ)
- `eth2`: 10.5.2.254 (Red interna)

En la topología se desplegaron las siguientes máquinas:

- **fw**: cortafuegos
- **exta**: host externo
- **dmza**: servidor web en DMZ
- **inta**: cliente de red interna

3. Proceso de aseguramiento del cortafuegos

3.1. 1. Análisis inicial

Tras conectarse al cortafuegos, se listaron las reglas existentes en la tabla `filter`, observando excesivos permisos.

3.2. 2. Limpieza de reglas

Se eliminaron todas las reglas mediante:

```
iptables -F
iptables -X
```

3.3. 3. Establecimiento de políticas seguras

Se configuraron políticas por defecto restrictivas:

```
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
```

3.4. 4. Permitir tráfico de conexiones establecidas

Se agregaron las reglas estándar de flujo:

```
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

3.5. 5. Reglas específicas solicitadas

A continuación se generaron las reglas exigidas por Example:

- Permitir DNS saliente desde la red interna hacia 1.1.1.1 y 1.0.0.1.
- Redirigir tráfico web de la red interna al servidor web de la DMZ.
- Permitir tráfico HTTPS saliente desde DMZA hacia Internet.
- Permitir administración SSH del servidor web únicamente desde EXTA.
- Permitir que FW actualice paquetes mediante HTTPS y SFTP hacia 82.194.78.250.
- Permitir futuras conexiones RDP de la red interna al servidor 10.5.1.89.

4. Tabla de reglas IPTables

Acción solicitada	**Regla IPTables aplicada**
1. Listar reglas en modo detallado	`iptables -L`
2. Eliminar todas las reglas	`iptables -F`

3. Políticas restrictivas	`iptables -P INPUT DROP`
	`iptables -P OUTPUT DROP`
	`iptables -P FORWARD DROP`

Acción solicitada	**Regla IPTables aplicada**

Permitir conexiones establecidas	`iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT`
	`iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT`
	`iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT`

DNS desde la red interna a 1.1.1.1 y 1.0.0.1	`iptables -A FORWARD -i eth2 -o eth0 -p udp --dport 53 -d 1.1.1.1 -m state --state NEW -j ACCEPT` `iptables -A FORWARD -i eth2 -o eth0 -p udp --dport 53 -d 1.0.0.1 -m state --state NEW -j ACCEPT`
Redirección HTTPS desde red interna a DMZA	`iptables -t nat -A PREROUTING -i eth2 -p tcp --dport 443 -j DNAT --to-destination 10.5.1.10`
DMZA acceso HTTPS a Internet	`iptables -A FORWARD -i eth1 -o eth0 -p tcp --dport 443 -m state --state NEW -j ACCEPT`
SSH desde EXTA a DMZA	`iptables -A FORWARD -i eth0 -s 10.5.0.10 -d 10.5.1.10 -p tcp --dport 22 -m state --state NEW -j ACCEPT`
Actualizaciones del FW a 82.194.78.250 (HTTPS, SFTP)	`iptables -A OUTPUT -o eth0 -p tcp -d 82.194.78.250 -m multiport --dports 443,22 -m state --state NEW -j ACCEPT`
Acceso RDP desde la red interna al futuro servidor 10.5.1.89	`iptables -A FORWARD -i eth2 -o eth1 -p tcp -d 10.5.1.89 --dport 3389 -m state --state NEW -j ACCEPT`

Cuadro 1: Tabla 1. Reglas de IPTables aplicadas

5. Conclusión

El cortafuegos ha sido configurado siguiendo estrictos principios de mínima exposición y control exhaustivo del flujo de tráfico entre los tres segmentos de red. Todas las reglas implementadas permiten únicamente las acciones explícitamente autorizadas por el cliente, logrando así un entorno más seguro y estable.

Anexo — Referencia al manual de `iptables`

Para la elaboración y validación de las reglas de cortafuegos utilizadas en este trabajo, se ha consultado la documentación oficial del comando `iptables`, disponible en el manual de Linux. Esta fuente proporciona una descripción detallada de todas las opciones, parámetros y módulos que pueden emplearse en la gestión del filtrado de paquetes en

sistemas GNU/Linux.

Referencia consultada:
`https://linux.die.net/man/8/iptables`

Dicha documentación ha servido como apoyo técnico para comprender la sintaxis, estructura y funcionamiento de las reglas IPTABLES, así como para garantizar que las configuraciones aplicadas cumplen con el comportamiento esperado en un entorno seguro y controlado.