

Laboratorio 7 Ciberseguridad
Sesión #7 Configuración de un Firewall en un Entorno de Red

Jesús Rodrigo Toro Navarro

Universidad Popular del Cesar

06/05/2025

Introducción

La creciente dependencia de las redes informáticas en todos los sectores — empresarial, educativo, gubernamental, entre otros— ha generado una necesidad urgente de establecer mecanismos efectivos de protección contra accesos no autorizados, ataques cibernéticos y vulnerabilidades del sistema. En este contexto, los firewalls desempeñan un papel esencial como primera línea de defensa, ya que permiten gestionar y controlar el tráfico de red de acuerdo con un conjunto de reglas previamente definidas.

Un firewall bien configurado no solo bloquea accesos sospechosos, sino que también garantiza que los servicios esenciales permanezcan disponibles para los usuarios autorizados. Además, permite segmentar redes internas de las externas, establecer zonas seguras (como DMZ), y realizar un seguimiento constante de los eventos que ocurren en la red, contribuyendo así a la detección y prevención temprana de incidentes de seguridad.

Este laboratorio está diseñado para proporcionar a los estudiantes una experiencia práctica en la configuración y gestión de un firewall en un entorno de red simulado. A través de una serie de pasos estructurados, se explorarán conceptos básicos y avanzados relacionados con el filtrado de tráfico, la definición de políticas de seguridad, la administración de accesos por direcciones IP, y la implementación de reglas específicas para redes internas y externas. Asimismo, se enfatiza la importancia del monitoreo y la capacidad de ajustar las configuraciones del firewall en función de los resultados observados.

El trabajo realizado en esta sesión contribuye a desarrollar competencias fundamentales en seguridad de redes, habilidades muy valoradas en los entornos profesionales actuales, y forma parte integral de la formación en administración de redes y sistemas.

Comandos Sección 7

Kali Linux

>sudo su

Eleva los privilegios actuales a root (superusuario), permitiendo ejecutar comandos administrativos sin necesidad de anteponer sudo continuamente.
Precaución: Aumenta el riesgo de realizar cambios críticos en el sistema.

>Apt install ufw -y

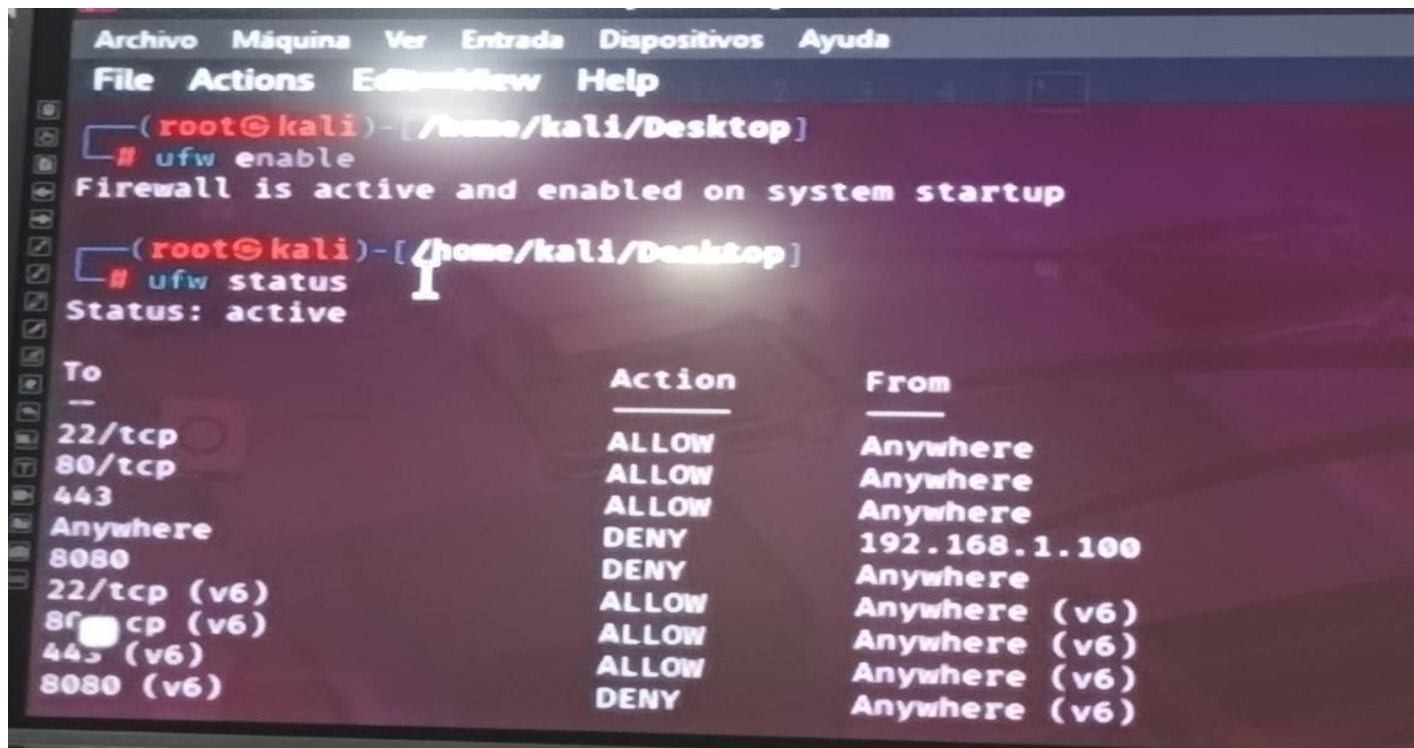
Instala UFW utilizando el gestor de paquetes apt. La opción -y acepta automáticamente todas las confirmaciones necesarias

>Ufw enable

Activa el firewall UFW y carga las reglas configuradas hasta ese momento.

>Ufw status

Muestra el estado actual de UFW (activo/inactivo) y las reglas configuradas.



The screenshot shows a terminal window with a menu bar at the top: Archivo, Máquina, Ver, Entrada, Dispositivos, Ayuda. Below the menu bar is a title bar: File, Actions, Edit, View, Help. The terminal content shows the following commands and output:

```
(root@kali)-[/home/kali/Desktop]
# ufw enable
Firewall is active and enabled on system startup

(root@kali)-[/home/kali/Desktop]
# ufw status
Status: active
```

To	Action	From
22/tcp	ALLOW	Anywhere
80/tcp	ALLOW	Anywhere
443	ALLOW	Anywhere
Anywhere	DENY	192.168.1.100
8080	DENY	Anywhere
22/tcp (v6)	ALLOW	Anywhere (v6)
80/tcp (v6)	ALLOW	Anywhere (v6)
443 (v6)	ALLOW	Anywhere (v6)
8080 (v6)	DENY	Anywhere (v6)

>apt install iptables -y

El comando `ufw default allow incoming` establece la política predeterminada de UFW para permitir todo el tráfico entrante.

```
>iptables -p INPUT DROP
```

Esta regla bloquea por defecto todo el tráfico entrante a menos que se especifiquen excepciones.

```
>iptables -p OUTPUT ACCEPT
```

Este comando establece la política por defecto para el tráfico saliente en ACCEPT (permitir todo el tráfico saliente).

```
>ufw allow ssh
```

Este comando configura UFW para permitir el tráfico en el puerto 22 (SSH).

```
>ufw allow http
```

Este comando configura UFW para permitir el tráfico en el puerto 80 (HTTP).

```
>iptables -A INPUT -p tcp --dport 22 -j ACCEPT
```

Este comando agrega una regla a iptables en la cadena INPUT que permite tráfico TCP en el puerto 22 (SSH).

```
>iptables -A INPUT -p tcp --dport 80 -j ACCEPT
```

Este comando agrega una regla a iptables para permitir tráfico TCP en el puerto 80 (HTTP).

```
>ufw status numbered
```

Este comando muestra el estado de UFW (si está activo o no) y lista las reglas configuradas con números.

```
>ufw allow from 192.168.1.20
```

Permite el tráfico entrante desde la dirección IP 192.168.1.20, para todos los puertos y protocolos.

```
>iptables -L
```

Lista todas las reglas actualmente cargadas en las cadenas de iptables (INPUT, FORWARD, OUTPUT).

```
> ufw deny from 192.168.1.20
```

Bloquea todo el tráfico proveniente de la IP 192.168.1.20.

```
> ufw allow from 192.168.1.21
```

Permite tráfico desde la IP 192.168.1.21.

> ufw deny from 192.168.1.21

Bloquea tráfico desde la misma IP.

> iptables A- INPUT -s 192.168.1.45 -j ACCEPT

Permite tráfico entrante desde la IP 192.168.1.45 para cualquier puerto/protocolo, si no hay reglas que lo bloqueen antes.

```
# ufw status numbered
Status: active

      To      Action      From
--      -
[ 1] 22/tcp    ALLOW IN    Anywhere
[ 2] 80/tcp    ALLOW IN    Anywhere
[ 3] 443       ALLOW IN    Anywhere
[ 4] Anywhere  DENY IN     192.168.1.100
[ 5] 8080      DENY IN     Anywhere
[ 6] Anywhere  ALLOW IN     192.168.1.20
[ 7] 22/tcp (v6) ALLOW IN    Anywhere (v6)
[ 8] 80/tcp (v6) ALLOW IN    Anywhere (v6)
[ 9] 443 (v6)  ALLOW IN    Anywhere (v6)
[10] 8080 (v6)  DENY IN     Anywhere (v6)
```

(root@kali)-[/home/kali/Desktop]

```
(root@kali)-[/home/kali/Desktop]
# ufw status numbered
Status: active

      To      Action      From
--      -
[ 1] 22/tcp    ALLOW IN    Anywhere
[ 2] 80/tcp    ALLOW IN    Anywhere
[ 3] 443       ALLOW IN    Anywhere
[ 4] Anywhere  DENY IN     192.168.1.100
[ 5] 8080      DENY IN     Anywhere
[ 6] Anywhere  DENY IN     192.168.1.20
[ 7] Anywhere  ALLOW IN     192.168.1.21
[ 8] 22/tcp (v6) ALLOW IN    Anywhere (v6)
[ 9] 80/tcp (v6) ALLOW IN    Anywhere (v6)
[10] 443 (v6)  ALLOW IN    Anywhere (v6)
[11] 8080 (v6)  DENY IN     Anywhere (v6)
```

(root@kali)-[/home/kali/Desktop]

>iptables -L

Lista las reglas actuales de iptables de forma básica

>ufw allow from 192.168.1.20

Permite todo el tráfico entrante desde la dirección IP 192.168.1.20

```
# ufw status numbered
Status: active

    To Action From
--
[ 1] 22/tcp ALLOW IN Anywhere
[ 2] 80/tcp ALLOW IN Anywhere
[ 3] 443 ALLOW IN Anywhere
[ 4] Anywhere DENY IN 192.168.1.100
[ 5] 8080 DENY IN Anywhere
[ 6] Anywhere ALLOW IN 192.168.1.20
[ 7] 22/tcp (v6) ALLOW IN Anywhere (v6)
[ 8] 80/tcp (v6) ALLOW IN Anywhere (v6)
[ 9] 443 (v6) ALLOW IN Anywhere (v6)
[10] 8080 (v6) DENY IN Anywhere (v6)
```

> ufw deny from 192.168.1.20

Bloquea todo el tráfico entrante desde la dirección IP 192.168.1.20

> ufw allow from 192.168.1.21

El comando ufw allow from 192.168.1.21 configura UFW (Uncomplicated Firewall) para permitir todo el tráfico entrante desde la IP 192.168.1.21.

```
(root@kali)-[/home/kali/Desktop]
# ufw status numbered
Status: active

    To Action From
--
[ 1] 22/tcp ALLOW IN Anywhere
[ 2] 80/tcp ALLOW IN Anywhere
[ 3] 443 ALLOW IN Anywhere
[ 4] Anywhere DENY IN 192.168.1.100
[ 5] 8080 DENY IN Anywhere
[ 6] Anywhere DENY IN 192.168.1.20
[ 7] Anywhere ALLOW IN 192.168.1.21
[ 8] 22/tcp (v6) ALLOW IN Anywhere (v6)
[ 9] 80/tcp (v6) ALLOW IN Anywhere (v6)
[10] 443 (v6) ALLOW IN Anywhere (v6)
[11] 8080 (v6) DENY IN Anywhere (v6)

(root@kali)-[/home/kali/Desktop]
```

> ufw deny from 192.168.1.21

El comando `ufw deny from 192.168.1.21` configura UFW (Uncomplicated Firewall) para denegar todo el tráfico entrante desde la IP 192.168.1.21.

```
>iptables -A INPUT -s 192.168.1.45 -j ACCEPT
```

Permite tráfico entrante desde la IP 192.168.1.45 en todos los puertos y protocolos, a menos que otra regla lo bloquee primero.

```
>iptables -L
```

Lista las reglas actuales de iptables en todas las cadenas (INPUT, FORWARD, OUTPUT).

```
>ufw allow from 192.168.1.20
```

Permite todo el tráfico entrante desde la IP 192.168.1.20.

```
>ufw deny from 192.168.1.20
```

Bloquea todo el tráfico entrante desde la misma IP.

```
>iptables -A INPUT -s 192.168.1.20 -j ACCEPT
```

En iptables, esta regla permite el tráfico entrante desde la IP 192.168.1.20 para cualquier puerto y protocolo.

```
>iptables -L -line-numbers
```

Muestra las reglas activas en iptables con números de línea, lo cual es útil para borrar reglas específicas con `-D`.

```
>iptables -D INPUT 9
```

Elimina la regla número 9 de la cadena INPUT.

```
>ufw deny from any to any port 8080
```

Bloquea todo el tráfico desde cualquier IP a cualquier IP, pero solo en el puerto 8080.

```
> ufw deny from any to any port 3600
```

Bloquea todo el tráfico desde cualquier IP a cualquier IP, pero solo en el puerto 3600.

```
>iptables -A INPUT -s tcp --dport 8080 -j DROP
```

Todo tráfico entrante con protocolo TCP dirigido al puerto 8080 será bloqueado sin respuesta.

CONCLUSIÓN

La realización de este laboratorio permitió comprender y aplicar de forma práctica los conceptos fundamentales de seguridad de red mediante la configuración de firewalls utilizando dos herramientas ampliamente utilizadas en sistemas Linux: UFW (Uncomplicated Firewall) e iptables. A través de diversos comandos, se logró gestionar el tráfico entrante y saliente, establecer políticas predeterminadas, permitir o denegar accesos específicos por dirección IP, y bloquear puertos utilizados por servicios potencialmente vulnerables.

El uso de UFW facilitó la creación rápida de reglas de seguridad gracias a su sintaxis simple, mientras que iptables ofreció un mayor nivel de control y personalización para situaciones más complejas. También se analizó el orden de evaluación de las reglas, la importancia de evitar conflictos entre UFW e iptables, y la necesidad de validar sintaxis correcta para evitar errores que podrían comprometer la conectividad o la seguridad del sistema.

Finalmente, el laboratorio destacó la importancia del monitoreo continuo y la gestión adecuada de las políticas de seguridad en entornos de red, reafirmando que un firewall bien configurado es una herramienta esencial para proteger los sistemas frente a accesos no autorizados, ataques de red y otras amenazas externas.