

# ACTIVIDAD 3 - UFW

Cristóbal Suárez Abad

SEGURIDAD Y ALTA DISPONIBILIDAD - 2º ASIR

## Índice

ACTIVIDAD UFW.....	2
<b>Parte 1: Reconocimiento y Seguridad Inicial</b> .....	2
<b>Parte 4: El Club VIP (Filtrado por IP)</b> .....	5
<b>Parte 4: Gestión y Limpieza</b> .....	6
<b>Parte 5: Reto Final</b> .....	8

# ACTIVIDAD UFW

## Parte 1: Reconocimiento y Seguridad Inicial

Instalar la herramienta ufw y evita bloquear el ssh si lo estás usando.

1. **Verificación:** Comprueba si **ufw** está instalado. Si no, instálalo.

- Comprobar:

**ufw --version**

```
[root@server2asir usuario]$ufw --version
ufw 0.36.1
Copyright 2008-2021 Canonical Ltd.
Tu Nombre sábado, 24 enero 2026 15:31
```

- Para instalarlo:

**sudo apt update**

**sudo apt install ufw -y**

2. **Estado actual:** Ejecuta el comando para ver el estado.

**systemctl status ufw**

```
[root@server2asir usuario]$systemctl status ufw
● ufw.service - Uncomplicated firewall
   Loaded: loaded (/lib/systemd/system/ufw.service; enabled; vendor preset: enabled)
   Active: active (exited) since Sat 2026-01-24 12:41:17 UTC; 2h 52min ago
     Docs: man:ufw(8)
   Main PID: 573 (code=exited, status=0/SUCCESS)
    CPU: 2ms

ene 24 12:41:17 server2asir systemd[1]: Starting Uncomplicated firewall...
ene 24 12:41:17 server2asir systemd[1]: Finished Uncomplicated firewall.
```

**sudo ufw status verbose**

```
[root@server2asir usuario]$sudo ufw status verbose
Status: inactive
Tu Nombre sábado, 24 enero 2026 15:31
```

3. **La Regla de Oro (¡IMPORTANTE!)**: Antes de encender el firewall, **deben** permitir el tráfico SSH, o perderán la conexión remota al activarlo.

Elige uno de los dos, es lo mismo:

**sudo ufw allow ssh**

**sudo ufw allow 22/tcp**

```
[root@server2asir usuario]$sudo ufw allow 22/tcp
Rules updated
Rules updated (v6)
```

```
[root@server2asir usuario]$sudo ufw allow ssh
Skipping adding existing rule
Skipping adding existing rule (v6)
```

4. **Encendido**: Ahora sí, activa el firewall.

**sudo ufw enable**

```
[root@server2asir usuario]$sudo ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
```

5. ¿Qué política por defecto se ha aplicado a las conexiones entrantes (incoming)?  
¿Por qué crees que es así?

```
[root@server2asir usuario]$sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip
```

To	Action	From
22/tcp	ALLOW IN	Anywhere
22/tcp (v6)	ALLOW IN	Anywhere (v6)

La política por defecto es bloquear todo lo entrante (incoming), permitir todo lo que sale (outgoing) y deshabilitar el “routed”.

Porque es el principio de “mínimo privilegio” (PoLP): “es un concepto relacionado con la seguridad de la información según el cual un usuario o entidad solo debe tener acceso a los datos, los recursos y las aplicaciones que necesite para llevar a cabo una determinada tarea”<sup>1</sup>.

<sup>1</sup> <https://www.paloaltonetworks.es/cyberpedia/what-is-the-principle-of-least-privilege>

## Parte 2: El Portero de Servicios

Supongamos que este servidor va a funcionar como un Servidor Web.

1. **Abrir tráfico web:** Permite el tráfico HTTP (puerto 80) y HTTPS (puerto 443).

```
sudo ufw allow 80/tcp
sudo ufw allow 443/tcp
```

```
[root@server2asir usuario]$sudo ufw allow 80/tcp
Rule added
Rule added (v6)
Tu Nombre sábado 24 enero 2026 15:50
[root@server2asir usuario]$sudo ufw allow 443/tcp
Rule added
Rule added (v6)
Tu Nombre sábado 24 enero 2026 15:50
```

2. **Verificación:** Muestra el estado para confirmar que las reglas se han agregado tanto para IPv4 como para IPv6.

```
[root@server2asir usuario]$sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To Action From
--
22/tcp ALLOW IN Anywhere
80/tcp ALLOW IN Anywhere
443/tcp ALLOW IN Anywhere
22/tcp (v6) ALLOW IN Anywhere (v6)
80/tcp (v6) ALLOW IN Anywhere (v6)
443/tcp (v6) ALLOW IN Anywhere (v6)
```

3. **Simulación:** Desde otro PC en la red, intenta hacer un **ping** a la máquina. Por defecto, UFW suele permitir ICMP, pero es bueno comprobarlo.

```
C:\Users\Cristobal>ping 10.2.7.108

Haciendo ping a 10.2.7.108 con 32 bytes de datos:
Respuesta desde 10.2.7.108: bytes=32 tiempo=22ms TTL=62
Respuesta desde 10.2.7.108: bytes=32 tiempo=21ms TTL=62
Respuesta desde 10.2.7.108: bytes=32 tiempo=21ms TTL=62
|
```

## Parte 4: El Club VIP (Filtrado por IP)

Imagina que el acceso a la base de datos (puerto 3306) solo debe permitirse desde la computadora del "Administrador" (otra IP de la red local).

1. **Regla específica:** Permite el tráfico al puerto 3306 **solo** desde una IP específica

**sudo ufw allow from 10.2.7.31 to any port 3306**

```
[root@server2asir usuario]$sudo ufw allow from 10.2.7.31 to any port 3306
Rule added
```

2. **Subredes:** Ahora permite el acceso a un servicio de archivos (ej. puerto 2049) a toda la subred.

**sudo ufw allow from 10.2.7.0/24 to any port 2049**

```
[root@server2asir usuario]$sudo ufw allow from 10.2.7.0/24 to any port 2049
Rule added
```

```
[root@server2asir usuario]$sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip
```

To	Action	From
---	-----	----
22/tcp	ALLOW IN	Anywhere
80/tcp	ALLOW IN	Anywhere
443/tcp	ALLOW IN	Anywhere
3306	ALLOW IN	10.2.7.31
2049	ALLOW IN	10.2.7.0/24
22/tcp (v6)	ALLOW IN	Anywhere (v6)
80/tcp (v6)	ALLOW IN	Anywhere (v6)
443/tcp (v6)	ALLOW IN	Anywhere (v6)

## Parte 4: Gestión y Limpieza

1. Permite las conexiones Telnet

El puerto de Telnet es el "23":

**sudo ufw allow 23/tcp**

```
[root@server2asir usuario]$sudo ufw allow 23/tcp
Rule added
Rule added (v6)
```

2. **Lista** las reglas por números

**sudo ufw status numbered**

```
[root@server2asir usuario]$sudo ufw status numbered
Status: active
```

	To	Action	From
	--	-----	----
[ 1]	22/tcp	ALLOW IN	Anywhere
[ 2]	80/tcp	ALLOW IN	Anywhere
[ 3]	443/tcp	ALLOW IN	Anywhere
[ 4]	3306	ALLOW IN	10.2.7.31
[ 5]	2049	ALLOW IN	10.2.7.0/24
[ 6]	23/tcp	ALLOW IN	Anywhere
[ 7]	22/tcp (v6)	ALLOW IN	Anywhere (v6)
[ 8]	80/tcp (v6)	ALLOW IN	Anywhere (v6)
[ 9]	443/tcp (v6)	ALLOW IN	Anywhere (v6)
[10]	23/tcp (v6)	ALLOW IN	Anywhere (v6)

3. Borra la regla de Telnet usando su número de índice.

Hay que borrar la de IPv4 e IPv6

**sudo ufw delete 6**

```
[root@server2asir usuario]$sudo ufw delete 6
Deleting:
  allow 23/tcp
Proceed with operation (y|n)? y
Rule deleted
```

```
[root@server2asir usuario]$sudo ufw status numbered
Status: active
```

	To	Action	From
	--	-----	----
[ 1]	22/tcp	ALLOW IN	Anywhere
[ 2]	80/tcp	ALLOW IN	Anywhere
[ 3]	443/tcp	ALLOW IN	Anywhere
[ 4]	3306	ALLOW IN	10.2.7.31
[ 5]	2049	ALLOW IN	10.2.7.0/24
[ 6]	22/tcp (v6)	ALLOW IN	Anywhere (v6)
[ 7]	80/tcp (v6)	ALLOW IN	Anywhere (v6)
[ 8]	443/tcp (v6)	ALLOW IN	Anywhere (v6)
[ 9]	23/tcp (v6)	ALLOW IN	Anywhere (v6)

sudo ufw delete 9

```
[root@server2asir usuario]$sudo ufw delete 9
Deleting:
  allow 23/tcp
Proceed with operation (y|n)? y
Rule deleted (v6)
```

4. Lista la regla de nuevo

```
[root@server2asir usuario]$sudo ufw status numbered
Status: active
```

	To	Action	From
	--	-----	----
[ 1]	22/tcp	ALLOW IN	Anywhere
[ 2]	80/tcp	ALLOW IN	Anywhere
[ 3]	443/tcp	ALLOW IN	Anywhere
[ 4]	3306	ALLOW IN	10.2.7.31
[ 5]	2049	ALLOW IN	10.2.7.0/24
[ 6]	22/tcp (v6)	ALLOW IN	Anywhere (v6)
[ 7]	80/tcp (v6)	ALLOW IN	Anywhere (v6)
[ 8]	443/tcp (v6)	ALLOW IN	Anywhere (v6)

## Parte 5: Reto Final

**Escenario:** Tienes un servidor que está sufriendo intentos de ataque por fuerza bruta al SSH. Necesitas configurar el firewall para una protección robusta.

### Instrucciones del reto:

1. **Resetear:** Comienza de cero (sin reinstalar)

**sudo ufw reset**

```
[root@server2asir usuario]$sudo ufw reset
Resetting all rules to installed defaults. This may disrupt existing ssh
connections. Proceed with operation (y|n)? y
Backing up 'user.rules' to '/etc/ufw/user.rules.20260124_161112'
Backing up 'before.rules' to '/etc/ufw/before.rules.20260124_161112'
Backing up 'after.rules' to '/etc/ufw/after.rules.20260124_161112'
Backing up 'user6.rules' to '/etc/ufw/user6.rules.20260124_161112'
Backing up 'before6.rules' to '/etc/ufw/before6.rules.20260124_161112'
Backing up 'after6.rules' to '/etc/ufw/after6.rules.20260124_161112'
```

```
[root@server2asir usuario]$sudo ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
Tu Nombre sábado 24 enero 2026 16:15
[root@server2asir usuario]$sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip
```

2. **Denegar todo:** Asegura que por defecto todo lo entrante esté bloqueado.

Sería este comando “**sudo ufw default deny incoming**”, pero no es necesario, porque esa es la política que se activa por defecto.

```
Tu Nombre sábado 24 enero 2026 16:15
[root@server2asir usuario]$sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
Tu Nombre sábado 24 enero 2026 16:16
[root@server2asir usuario]$sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip
```

3. **Rate Limiting:** En lugar de un simple `allow ssh`, investiga y aplica una regla que limite la tasa de conexión (limit) para proteger el puerto 22 contra fuerza bruta<sup>2</sup>.

```
sudo ufw limit ssh
```

```
Tu Nombre sábado 24 enero 2026 16:23
[root@server2asir usuario]$sudo ufw limit ssh
Rule added
Rule added (v6)
```

```
[root@server2asir usuario]$sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip
```

To	Action	From
22/tcp	LIMIT IN	Anywhere
22/tcp (v6)	LIMIT IN	Anywhere (v6)

4. **Servidor Web Seguro:** Permite el tráfico al puerto 80 y 443.

```
sudo ufw allow 80/tcp
sudo ufw allow 443/tcp
```

```
Tu Nombre sábado 24 enero 2026 16:23
[root@server2asir usuario]$sudo ufw allow 80/tcp
Rule added
Rule added (v6)
Tu Nombre sábado 24 enero 2026 16:23
[root@server2asir usuario]$sudo ufw allow 443/tcp
Rule added
Rule added (v6)
Tu Nombre sábado 24 enero 2026 16:23
[root@server2asir usuario]$sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip
```

To	Action	From
22/tcp	LIMIT IN	Anywhere
80/tcp	ALLOW IN	Anywhere
443/tcp	ALLOW IN	Anywhere
22/tcp (v6)	LIMIT IN	Anywhere (v6)
80/tcp (v6)	ALLOW IN	Anywhere (v6)
443/tcp (v6)	ALLOW IN	Anywhere (v6)

---

<sup>2</sup> <https://www.cyberciti.biz/faq/howto-limiting-ssh-connections-with-ufw-on-ubuntu-debian/>

5. **Rango de Gestión:** Permite acceso total (todos los puertos) **solo** desde la IP que tu elijas

**sudo ufw allow from 10.2.7.56**

```
[root@server2asir usuario]$sudo ufw allow from 10.2.7.56
Rule added
Tu Nombre sábado 24 enero 2026 16:27
```

6. **Log:** Activa el registro de eventos (**logging**) en nivel bajo.

**sudo ufw logging low**

**Logs en: /var/log/ufw.log**

```
Tu Nombre sábado 24 enero 2026 16:29
[root@server2asir usuario]$sudo ufw logging low
Logging enabled
Tu Nombre sábado 24 enero 2026 16:31
```

7. Comprueba algunos de las reglas añadidas

```
Tu Nombre sábado 24 enero 2026 16:32
[root@server2asir usuario]$sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To Action From
--
22/tcp LIMIT IN Anywhere
80/tcp ALLOW IN Anywhere
443/tcp ALLOW IN Anywhere
Anywhere ALLOW IN 10.2.7.56
22/tcp (v6) LIMIT IN Anywhere (v6)
80/tcp (v6) ALLOW IN Anywhere (v6)
443/tcp (v6) ALLOW IN Anywhere (v6)
```