UFW

UFW (Uncomplicated Firewall), que es una interfaz simplificada para **iptables/nftables** (el motor subyacente del *firewall* de Linux).

UFW es mucho más fácil de entender y usar que manipular directamente iptables. Aquí tienes una guía completa paso a paso para configurar UFW.

Configuración de Firewall con UFW (Ubuntu 24.04)

Paso 1: Verificar el Estado de UFW e Instalación

UFW suele venir preinstalado, pero por si acaso, puedes confirmar su estado e instalarlo si es necesario.

1. **Verificar estado:**

   sudo ufw status

   *Si dice **Status: inactive**, necesitas activarlo.*

2. **Instalar (si es necesario):**

   sudo apt install ufw -y

Paso 2: Definir las Políticas por Defecto (Reglas Base)

Lo primero es establecer cómo debe comportarse el *firewall* cuando no hay una regla específica. La práctica de seguridad más recomendada es **denegar (deny) todas las conexiones entrantes** y **permitir (allow) todas las salientes.**

Política	**Significado**	**Comando**
Entrante (Input)	Todo lo que llega al servidor.	sudo ufw default deny incoming
Saliente (Output)	Todo lo que sale del servidor.	sudo ufw default allow outgoing

Ejecución:

Denegar todo el tráfico entrante por defecto

sudo ufw default deny incoming

Permitir todo el tráfico saliente por defecto

sudo ufw default allow outgoing

Paso 3: Permitir Conexiones Esenciales (SSH)

Dado que has denegado todo el tráfico entrante, debes permitir explícitamente el puerto SSH (generalmente el puerto **22**) para no quedarse fuera del servidor.

1. **Permitir el puerto 22 (SSH):**

   sudo ufw allow ssh

Alternativamente, puedes especificar el puerto:

   sudo ufw allow 22/tcp

Paso 4: Habilitar y Verificar el Firewall

Una vez que el acceso SSH está permitido, puedes activar UFW de forma segura.

1. Habilitar UFW:

   Se te preguntará si desea continuar. Escriba y (yes).

   sudo ufw enable

2. Verificar el estado (detallado):

   Confirma que está activo y que la regla de SSH está en su lugar.

   sudo ufw status verbose

   *La salida debe mostrar **Status: active** y la regla 22/tcp (SSH) en la sección To Action.*

3. Verificar el estado (numerado):

   Esto es útil para eliminar reglas específicas.

   sudo ufw status numbered

Paso 5: Añadir Reglas para Servicios Comunes

Añade reglas para cualquier servicio que quiera exponer públicamente (como un servidor web o el servicio Glances/Nagios).

Servicio	**Puerto**	**Comando de Ejemplo**
HTTP (Web)	80	sudo ufw allow http
HTTPS (Web Segura)	443	sudo ufw allow https
Glances	61208	sudo ufw allow 61208/tcp
Nagios Web	80 (ya cubierto por http)	-
Nagios NRPE (para agentes)	5666	sudo ufw allow 5666/tcp

Ejemplos Avanzados de Reglas

- **Permitir acceso a HTTP solo desde una IP específica:**

  sudo ufw allow from 192.168.1.100 to any port 80

- **Permitir un rango de puertos:**

  sudo ufw allow 10000:20000/tcp

- **Denegar un puerto específico (si previamente fue permitido):**

  sudo ufw deny 8080/tcp

Paso 6: Eliminar Reglas

Hay dos formas de eliminar reglas: por número o por regla literal.

1. Eliminar por número (Recomendado):

   Primero, obtén la lista numerada:

   sudo ufw status numbered

   Si deseas eliminar la regla número 3:

   sudo ufw delete 3

2. **Eliminar por regla literal:**

   sudo ufw delete allow 80/tcp

Paso 7: Deshabilitar o Restablecer el Firewall

Si necesitas deshabilitar UFW temporalmente o revertir todas las reglas, usa estos comandos.

1. **Deshabilitar UFW (mantiene las reglas):**

   sudo ufw disable

2. Restablecer UFW (borra todas las reglas):

   Esto devuelve UFW al estado original (deshabilitado y sin reglas definidas).

   sudo ufw reset

Resumen de la Configuración Mínima de Seguridad

Para un servidor básico, los siguientes tres comandos son la configuración de seguridad esencial:

1. Denegar todo lo entrante y permitir lo saliente

```
sudo ufw default deny incoming
```

```
sudo ufw default allow outgoing
```

2. Abrir el puerto SSH (imprescindible)

```
sudo ufw allow ssh
```

3. Activar el firewall

```
sudo ufw enable
```