



Gateway y Firewall

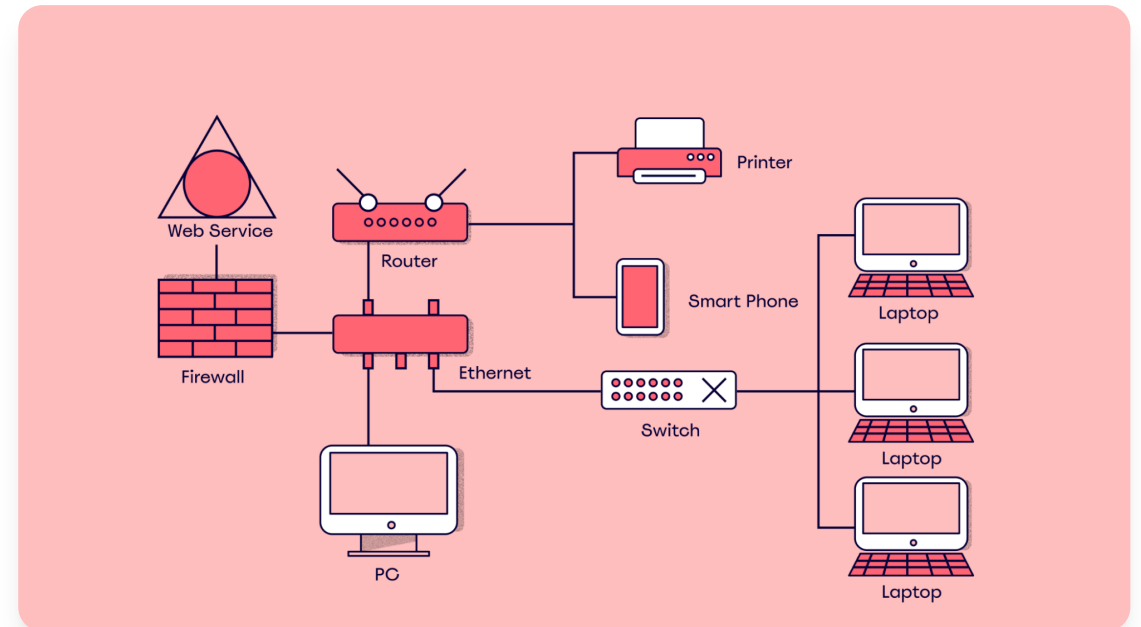
Administración de Seguridad en Linux



Funcionamiento de un Gateway

Encaminamiento de Paquetes

- ✓ El **gateway o router** actúa como punto de interconexión entre diferentes redes
- ✓ Encamina **paquetes que no van dirigidos a él** hacia su destino final
- ✓ Usa **tablas de enrutamiento** para determinar el mejor camino
- ✓ Permite comunicación entre **subredes y la internet**



⌘ Activación del Enrutamiento IP

Método Temporal (sysctl)

Activa el enrutamiento temporalmente hasta el siguiente reinicio:

```
sysctl -w net.ipv4.ip_forward=1
```

i Cambios se pierden al reiniciar el sistema

📄 Método Permanente

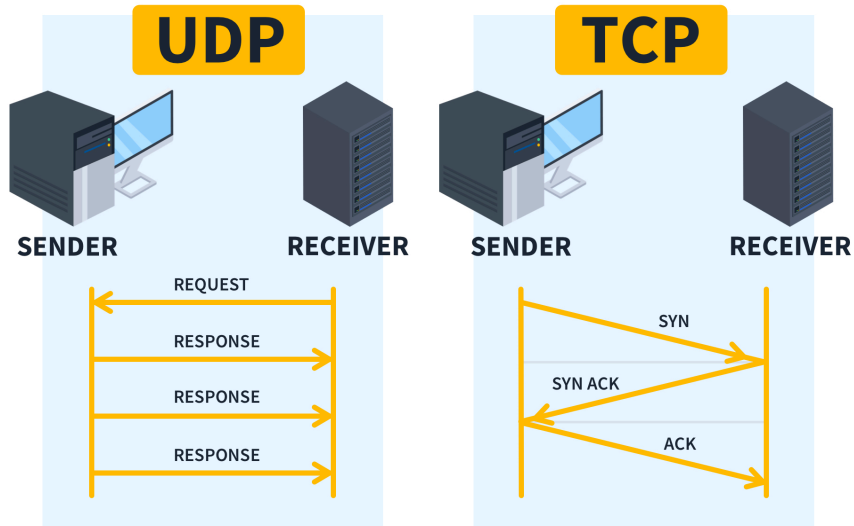
Edita el archivo **/etc/sysctl.conf**:

```
net.ipv4.ip_forward=1
```

Luego aplica los cambios:

```
sysctl -p
```

Puertos de Protocolos de Transporte



TCP - Transmission Control Protocol

- ✓ **Conexión** orientada
- ✓ **Control** de flujo
- ✓ **Confiable** y seguro
- ✓ **Reenvío** de paquetes



UDP - User Datagram Protocol

- ⚡ **Sin** conexión
- ⚡ **Sin** control de flujo
- ⚡ **Más** rápido
- ⚡ **Sin** garantías

Función Principal

Mapea **nombres de servicios** a **números de puerto** y **protocolos**

Resolución de puertos

Convierte nombres legibles en números

Base de datos del sistema

Almacena configuraciones de red estándar

Referencia para aplicaciones

Utilizado por servicios de red

Ejemplo de Contenido

```
# Servicios y puertos comunes
```

```
http 80/tcp www
```

```
https 443/tcp www-https
```

```
ssh 22/tcp
```

```
ftp 21/tcp
```

```
telnet 23/tcp
```

```
smtp 25/tcp mail
```

```
dns 53/tcp domain
```

```
dns 53/udp domain
```

```
pop3 110/tcp pop-3
```

```
imap 143/tcp
```

```
ldap 389/tcp
```

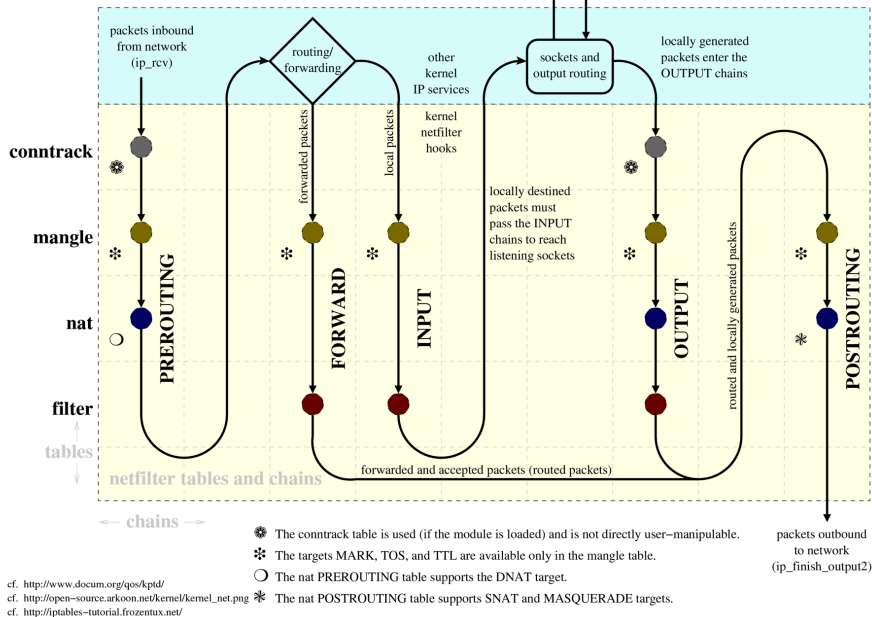
```
mysql 3306/tcp
```

```
postgresql 5432/tcp
```

Filtrado de Puertos en el Kernel de Linux

Netfilter Packet Traversal

<http://linux-ip.net/nf/nfk-traversal.png>
Martin A. Brown, martin@linux-ip.net



Netfilter Framework

Sistema de filtrado de paquetes integrado en el **kernel de Linux**

Herramientas

iptables

nftables

Cadenas

INPUT

OUTPUT

FORWARD

Flujo de Paquetes

Los paquetes atraviesan las cadenas donde se aplican **reglas de filtrado** para permitir o denegar el tráfico

UFW (Ubuntu)



Firewall with UFW on ubuntu

Ubuntu is a Debian-based Linux operating system that is suitable for both desktop and server use. It has a built-in L4 packet filtering system called Netfilter for access control, with an interface called iptables for configuring the Netfilter. However, configuring iptables for novice users can be challenging, so many frontends for iptables have been developed, including The Uncomplicated Firewall (ufw). ufw is included by default in all Ubuntu installations after version 8.04 LTS and provides an easy-to-use interface for managing netfilter.

Zenarmor enables next-generation firewall features on Ubuntu, such as L7 filtering. For starting to protect your network behind Zenarmor, you may easily run the following command on your Ubuntu server:

```
curl https://updates.sunnyvalley.io/getzenarmor | sh
```



Uncomplicated Firewall

Herramienta **simplificada** para gestionar iptables en Ubuntu



Comandos Básicos



ufw enable

Activar firewall



ufw allow 22

Permitir puerto



ufw deny 80

Denegar puerto



ufw status

Ver estado

Características



Simplicidad



Rápido



Fácil uso

Tabla Completa de UFW



Permitir Puertos

Puerto	Protocolo	Comando
22	tcp	<code>ufw allow 22/tcp</code>
80	tcp	<code>ufw allow 80/tcp</code>
443	tcp	<code>ufw allow 443/tcp</code>
8000-9000	tcp	<code>ufw allow 8000:9000/tcp</code>
53	udp	<code>ufw allow 53/udp</code>



Permitir Servicios

Servicio	Puerto	Comando
ssh	22	<code>ufw allow ssh</code>
http	80	<code>ufw allow http</code>
https	443	<code>ufw allow https</code>
smtp	25	<code>ufw allow smtp</code>
ftp	21	<code>ufw allow ftp</code>

firewall-cmd (RedHat)



Firewalld Interface

Herramienta para distribuciones **Red Hat**: RHEL, CentOS, Fedora

```
lhb@linuxhandbook:~$ sudo firewall-cmd --get-active-zones
[sudo] password for lhb:
docker
  interfaces: docker0
public
  interfaces: wlp2s0
work
  interfaces: eth0
lhb@linuxhandbook:~$
```



Comandos Principales



--add-port=80/tcp
Agregar puerto



--reload
Aplicar cambios



--list-all
Ver configuración



--remove-port=80/tcp
Eliminar puerto

★ Ventajas



Dinámico



Zonas



Flexible

Tabla Completa de firewall-cmd



Permitir Puertos

Puerto	Protocolo	Comando
22	tcp	<code>--add-port=22/tcp</code>
80	tcp	<code>--add-port=80/tcp</code>
443	tcp	<code>--add-port=443/tcp</code>
8000-9000	tcp	<code>--add-port=8000-9000/tcp</code>
53	udp	<code>--add-port=53/udp</code>



Permitir Servicios

Servicio	Puerto	Comando
ssh	22	<code>--add-service=ssh</code>
http	80	<code>--add-service=http</code>
https	443	<code>--add-service=https</code>
smtp	25	<code>--add-service=smtp</code>
ftp	21	<code>--add-service=ftp</code>

Preguntas tipo test

1 ¿Cuál es la función principal de un gateway (router) en una red?

2 ¿Cómo se activa el enrutamiento IP de forma permanente en Linux?

3 ¿Cuál es la diferencia principal entre los protocolos TCP y UDP?

4 ¿Cuál es la función del archivo `/etc/services` en el sistema Linux?

5 ¿Qué framework del kernel de Linux gestiona el filtrado de paquetes?

6 ¿Qué herramienta simplificada se utiliza para gestionar firewalls en Ubuntu?

7 ¿Qué comando se utiliza para ver el estado de `firewalld` en Red Hat?

8 ¿Cuáles son las cadenas principales de filtrado en Netfilter?