Configuración de un Firewall en un Entorno de Red

Parte 1: Introducción al Firewall y Entorno de Configuración

Paso 1: Revisión de la Configuración de Red Actual

En Linux:

```
ip a  # Ver interfaces de red
ip route  # Ver rutas
```

En Windows:

```
ipconfig /all
```

Observaciones:

- Identificar direcciones IP, subredes y puertas de enlace.

Paso 2: Instalación y Verificación del Firewall

En Ubuntu/Debian (UFW):

```
sudo apt install ufw -y
sudo ufw enable  # Activar el firewall
sudo ufw status verbose  # Verificar estado
```

Verificación:

- Asegurarse de que el firewall está activo (Status: active).

Parte 2: Configuración Básica del Firewall

Paso 3: Configuración de Políticas por Defecto

```
sudo ufw default deny incoming  # Bloquear tráfico entrante
sudo ufw default allow outgoing  # Permitir tráfico saliente
```

Paso 4: Permitir Tráfico para Servicios Específicos

```
sudo ufw allow 22/tcp  # SSH
sudo ufw allow 80/tcp  # HTTP
sudo ufw allow 443/tcp  # HTTPS
```

Verificación:

```
sudo ufw status numbered  # Listar reglas aplicadas
```

Parte 3: Configuración Avanzada del Firewall

Paso 5: Crear Reglas de Filtrado por IP

Permitir acceso SSH solo desde una IP específica:

sudo ufw allow from 192.168.1.100 to any port 22

Bloquear una IP maliciosa:

sudo ufw deny from 10.0.0.5

Paso 6: Configuración de Reglas para Redes Internas y Externas

Permitir tráfico HTTP/HTTPS desde cualquier origen (externo):

sudo ufw allow 80/tcp

sudo ufw allow 443/tcp

Permitir acceso total a la red interna (ej. 192.168.1.0/24):

sudo ufw allow from 192.168.1.0/24

Parte 4: Monitoreo y Ajustes del Firewall

Paso 7: Monitoreo de Logs del Firewall

En UFW, los logs se encuentran en:

tail -f /var/log/ufw.log

Filtrar tráfico bloqueado:

grep "\[UFW BLOCK\]" /var/log/ufw.log

Paso 8: Ajuste de Reglas Basado en Monitoreo

- Ejemplo: Si el tráfico legítimo es bloqueado, agregar una regla específica:

sudo ufw allow from 203.0.113.5 to any port 3306 # Permitir MySQL desde una IP
