

Edgar Omar Rodriguez Hernandez

177888

Seguridad Informática

UPSLP

Servando López Contreras

1. Establecer una política restrictiva.

```
iptables -P FORWARD DROP
```

2. Permitir el tráfico de conexiones ya establecidas.

```
iptables -A FORWARD -m state --state ESTABLISHED, RELATED -j ACCEPT
```

3. Aceptar tráfico DNS (TCP) saliente de la red local.

```
iptables -A FORWARD -p tcp -s 192.1.2.0/24 --dport 53 -m state --state NEW -j ACCEPT
```

4. Aceptar correo entrante proveniente de Internet en el servidor de correo.

```
iptables -A FORWARD -p tcp -d 192.1.2.10 --dport 25 -m state --state NEW -j ACCEPT
```

5. Permitir correo saliente a Internet desde el servidor de correo.

```
iptables -A FORWARD -p tcp -s 192.1.2.10 --dport 25 -m state --state NEW -j ACCEPT
```

6. Aceptar conexiones HTTP desde Internet a nuestro servidor web.

```
iptables -A FORWARD -p tcp -d 192.1.2.11 --dport 80 -m state --state NEW -j ACCEPT
```

7. Permitir tráfico HTTP desde la red local a Internet.

```
iptables -A FORWARD -p tcp -s 192.1.2.0/24 --dport 80 -m state --state NEW -j ACCEPT
```