



[TÍTULO DEL DOCUMENTO]

CNV – Seguridad Informatica

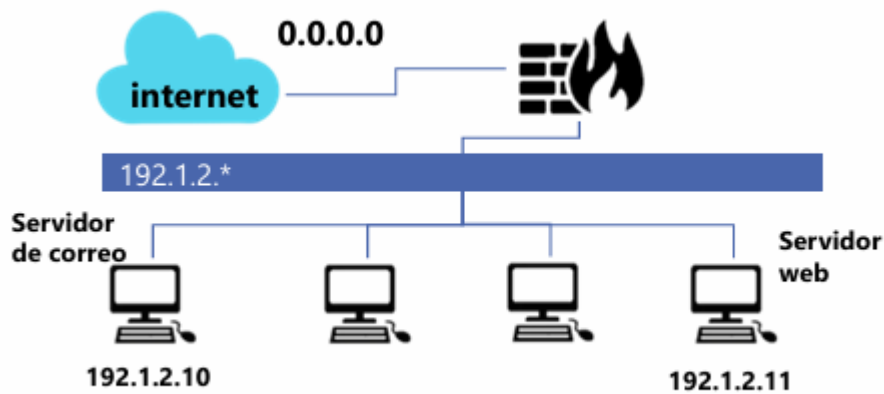


4 DE FEBRERO DE 2026

JOSE ARMANDO PALOMO CERDA 175932

MSTRO. SERVANDO LOPEZ CUEVAS

Universidad Politécnica de San Luis Potosi



Basado en la topología de la imagen, estos son los datos clave:

Red Local: 192.1.2.0/24

Servidor de Correo: 192.1.2.10

Servidor Web: 192.1.2.11

Establecer una política restrictiva.

```
iptables -P FORWARD DROP
```

Permitir el tráfico de conexiones ya establecidas.

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

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

```
Iptables -A FORWARD -p tcp -s 192.168.1.0/24 -d 0.0.0.0/0 --dport 53 -m state --state NEW -j ACCEPT
```

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

```
iptables -A FORWARD -p tcp -s 0.0.0.0/0 -d 192.1.2.10 --dport 25 -m state --state NEW -j ACCEPT
```

Permitir correo saliente a Internet desde el servidor de correo.

```
iptables -A FORWARD -p tcp -s 192.168.1.0 -d 0.0.0.0/0 --dport 25 -m state --state NEW -j ACCEPT
```

Aceptar conexiones HTTP desde Internet a nuestro servidor web.

```
iptables -A FORWARD -p tcp -s 0.0.0.0/0 -d 192.1.2.11 --dport 80 -m state --state NEW -j ACCEPT
```

Permitir tráfico HTTP desde la red local a Internet

```
iptables -A FORWARD -p tcp -s 192.168.1.0/24 -d 0.0.0.0/0 --dport 80 -m state --state NEW -j ACCEPT.
```