

Actividad 04

1. Establecer una política restrictiva.

```
Iptables -P INPUT -p tcp -j REJECT
```

```
Iptables -P OUTPUT -p tcp -j REJECT
```

2. Permitir el tráfico de conexiones ya establecidas.

```
iptables -A INPUT -p tcp \ -m state --state ESTABLISHED -j ACCEPT
```

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

```
iptables -A OUTPUT -p tcp --dport 53 -s 192.1.2. * -j ACCEPT
```

4. Aceptar correo entrante proveniente de Internet

en el servidor de correo.

```
iptables -A INPUT -s 192.1.2.11 -d 192.1.2.10 -- -j ACCEPT
```

5. Permitir correo saliente a Internet desde el

servidor de correo.

```
iptables -A OUTPUT -s 192.1.2.10 -d 192.1.2.11 -j ACCEPT
```

6. Aceptar conexiones HTTP desde Internet a

nuestro servidor web.

```
iptables -A INPUT -p tcp -s 192.1.2.11 --dport 80 -j ACCEPT
```

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

```
iptables -A INPUT -p tcp -s 192.1.2. * -d 192.1.2.10 -j ACCEPT
```