Actividad 4

Pedro Damian Jasso Dávila 176658

CNO V

Teniendo en cuenta la topología de red mostrada completa la tabla con las reglas de iptables que deberían aplicarse en el Firewall para llevar a cabo las acciones solicitadas. Las reglas, siempre que sea posible, deben determinar protocolo, dirección IP origen y destino, puerto/s origen y destino y el estado de la conexión.

1. **Establecer una política restrictiva.**

   iptables -P INPUT DROP

2. **Permitir el tráfico de conexiones ya establecidas.**

   iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

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

   iptables -A INPUT -p tcp --sport 53 -d 192.1.2.0/24 -m state --state ESTABLISHED -j ACCEPT

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

   iptables -A INPUT -p tcp --dport 25 -d 192.1.2.10 -m state --state NEW,ESTABLISHED -j ACCEPT

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

   iptables -A OUTPUT -p tcp --dport 25 -d 192.1.2.10 -m state --state NEW,ESTABLISHED -j ACCEPT

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

   iptables -A INPUT -p tcp --dport 80 -d 192.1.2.10 -m state --state NEW,ESTABLISHED -j ACCEPT

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

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