Ciberseguridad

MECANISMOS DE
DEFENSA EN RED

173030 Sánchez Mayeli

Actividad 04. Mecanismos de defensa en red

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.

Ejercicio, completa los iptables

1. Establecer una política restrictiva.
   iptables -A INPUT -p tcp --dport 443 --j 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 FORWARD -p udp -s 192.1.2.0/24 -d 0.0.0.0/0 --dport 53 -m state --state NEW -j ACCEPT

4. Aceptar correo entrante proveniente de Internet en el servidor de correo.
   iptables -A A INPUT -p tcp 192.1.2.0 -j ACCEPT

5. Permitir correo saliente a Internet desde el servidor de correo.
   iptables -A

6. 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

7. Permitir tráfico HTTP desde la red local a Internet
   iptables -A FORWARD -p tcp -s 192.1.2.0/24 -d 0.0.0.0/0 --dport 443 -m state --state NEW -j ACCEPT