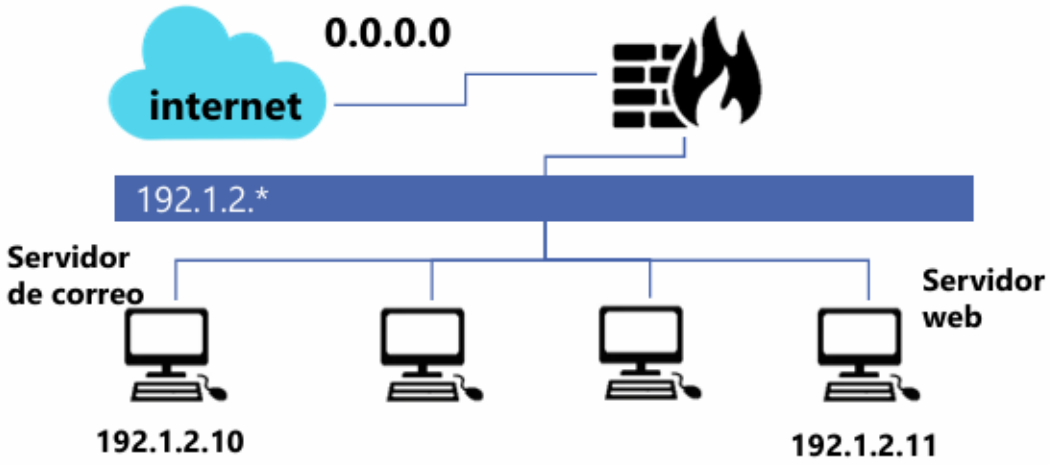
ACT 4. MECANISMOS DE DEFENSA EN RED.

CNO V – Seguridad informática

UPSLP

Josué Emiliano Rosales Ramírez
181760

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.
2. Permitir el tráfico de conexiones ya establecidas.
3. Aceptar tráfico DNS (TCP) saliente de la red local.
4. Aceptar correo entrante proveniente de Internet en el servidor de correo.
5. Permitir correo saliente a Internet desde el servidor de correo.
6. Aceptar conexiones HTTP desde Internet a nuestro servidor web.
7. Permitir tráfico HTTP desde la red local a Internet.

1. Establecer una política restrictiva.

Iptables -L -v -n

2. Permitir el tráfico de conexiones ya establecidas.

Iptables -A INPUT -m state Established -j Accept

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

Iptables -A OUTPUT -p tcp –sports 53 -s 192.1.2.* -j Accept

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

Iptables -A INPUT -p tcp –s 0.0.0.0 -d 192.1.2.11 -j Accept

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

Iptables -A OUTPUT -p tcp –d 0.0.0.0 -s 192.1.2.11 -j Accept

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

Iptables -A INPUT -p tcp -dports 80 -s 0.0.0.0 -j Accept

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

Iptables -A OUTPUT -p tcp –dports 80 -d 0.0.0.0