MECANISMOS DE DEFENSA EN RED

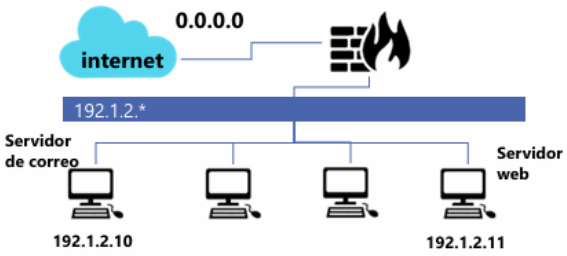
CNO V – SEGURIDAD INFORMATICA

Juan Alejandro Pérez Ventura
180370@upslp.edu.mx

ACTIVIDAD #4

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.



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.

No.	Regla
1	iptables -P INPUT DROP && iptables -P OUTPUT DROP && iptables -P FORWARD DROP
2	iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
3	iptables -A OUTPUT -p tcp -s 192.1.2.0/24 -j ACCEPT
4	iptables -A INPUT -p tcp -d 192.1.2.10 --dport 25 -m state --state NEW -j ACCEPT
5	iptables -A OUTPUT -p tcp -s 192.1.2.10 --sport 25 -j ACCEPT
6	iptables -A INPUT -p tcp -d 192.1.2.11 --dport 80 -m state --state NEW -j ACCEPT
7	iptables -A OUTPUT -p tcp -s 192.1.2.0/24 --dport 80 -j ACCEPT