

ACTIVIDAD 04

MECANISMOS DE DEFENSA EN RED

*Francisco Javier Cruz Juarez
177622*

Maestro: Servando Lopez

Actividad 4: Mecanismos de defensa en red.

Objetivo: 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.

#	Acción Solicitada	Regla de iptables
1	Política restrictiva	<pre>iptables -P INPUT DROP</pre> <pre>iptables -P FORWARD DROP</pre> <pre>iptables -P OUTPUT DROP</pre>
2	Tráfico establecido	<pre>iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT</pre>
3	DNS (TCP) saliente de LAN	<pre>iptables -A FORWARD -p tcp -s 192.1.2.0/24 -d 0.0.0.0/0 --dport 53 -m state --state NEW -j ACCEPT</pre>
4	Correo entrante (SMTP)	<pre>iptables -A FORWARD -p tcp -s 0.0.0.0/0 -d 192.1.2.10 --dport 25 -m state --state NEW -j ACCEPT</pre>
5	Correo saliente (SMTP)	<pre>iptables -A FORWARD -p tcp -s 192.1.2.10 -d 0.0.0.0/0 --dport 25 -m state --state NEW -j ACCEPT</pre>
6	HTTP entrante a Web	<pre>iptables -A FORWARD -p tcp -s 0.0.0.0/0 -d 192.1.2.11 --dport 80 -m state --state NEW -j ACCEPT</pre>
7	HTTP saliente de LAN	<pre>iptables -A FORWARD -p tcp -s 192.1.2.0/24 -d 0.0.0.0/0 --dport 80 -m state --state NEW -j ACCEPT</pre>