1. Diseña las reglas de configuración para la red 192.168.20.0 de SiCon. Debes tener en cuenta que se trata de una red en la que la seguridad es especialmente importante, y no se permite el acceso desde el exterior a ninguno de los equipos que forman parte de esta red. Dentro de la red se permite el trafico FTP desde cualquier ordenador al equipo con dirección IP 192.168.20.1. Este equipo es el único que tiene autorización para enviar tráfico FTP al exterior y a los equipos que constituyen la red. La empresa considera que el tráfico http puede ser un punto vulnerable, por lo que solo se permite que los equipos realicen conexiones hacia el exterior utilizando el protocolo HTTPS.

N.º Regla	IP Origen	Puerto Origen	IP Destino	Puerto Destino	Acción
1	192.168.20.0	20:21	192.168.20.1	-	PERMITIR
2	192.168.20.1	20:21	*	-	PERMITIR
3	192.168.20.0	443	*	-	PERMITIR
4	192.168.20.0	*	*	-	IGNORAR
5	*	*	192.168.20.0	-	IGNORAR

2. Transforma las reglas del ejercicio anterior a comandos iptables.

IPTABLES

1. iptables -A OUTPUT -s 192.168.20.0/24 -p tcp –sport 443 -j ACCEPT
2. iptables -A OUTPUT -s 192.168.20.1 -p tcp -sport 20:21 -j ACCEPT
3. iptables -A FORWARD -s 192.168.20.0/24 -d 192.168.20.1 -p tcp --sport 20:21 -j ACCEPT
4. iptables -P OUTPUT DROP
5. iptables -P INPUT DROP

3. Interpreta los siguientes comandos y crea la tabla teórica de filtrado asociada a ellos.
   - iptables –A INPUT –p tcp dport ftp –j DROP
   - iptables –A OUTPUT source 194.2.10.0 –j ACCEPT
   - iptables –A INPUT destination 194.2.10.22 –j DROP

N.º Regla	IP Origen	Puerto Origen	IP Destino	Puerto Destino	Acción
1	*	*	194.2.10.0	20:21	IGNORAR
2	194.2.10.0	*	*	-	ACEPTAR
3	*	*	194.2.10.22	-	IGNORAR