

1.- Realizar las reglas de filtrado para el siguiente supuesto:

- Tenemos una red 192.168.0.0 en la que todos los equipos sólo podrán salir a Internet por el puerto 443.
- Tenemos a su vez un servidor web con IP 154.44.0.23 al que pueden conectarse con el puerto 80 o por el 443 todos los equipos de la red 192.168.0.0 pero el resto sólo se podrán conectar por el puerto 443.
- También tenemos un servidor FTP al que se pueden conectar todos los equipos de la red 192.168.0.0 y sólo los pertenecientes a esa red.
- Todo el tráfico proveniente de estos dos servidores se dejará pasar.
- El equipo 192.168.0.15 pertenece al dueño de la empresa y por tanto puede salir a cualquier IP con cualquier servicio. Pero a su equipo sólo podrán llegar paquetes a los puertos 21, 443.

N.º Regla	IP Origen	Puerto Origen	IP Destino	Puerto Destino	Acción
1	192.168.0.0	80	154.44.0.23	-	ACEPTAR
2	192.168.0.0	443	*	-	ACEPTAR
3	192.168.0.0	21	154.44.0.23	-	ACEPTAR
4	*	21	154.44.0.23	-	RECHAZAR
5	154.44.0.23	*	192.168.0.0	-	ACEPTAR
6	192.168.0.15	*	*	-	ACEPTAR
7	*	21	192.168.0.15	-	ACEPTAR
8	*	443	192.168.0.15	-	ACEPTAR
9	192.168.0.0	*	*	-	RECHAZAR
10	*	*	192.168.0.0	-	RECHAZAR

### Iptables

1. iptables -A OUTPUT -s 192.168.0.0/24 -d 154.44.0.23 -p tcp --sport 80 -j ACCEPT
2. iptables -A OUTPUT -s 192.168.0.0/24 -p tcp --sport 443 -j ACCEPT
3. iptables -A OUTPUT -s 192.168.0.0/24 -d 154.44.0.23 -p tcp --sport 21 -j ACCEPT
4. iptables -A FORWARD -d 154.44.0.23 -p tcp --sport 21 -j REJECT
5. iptables -A INPUT -s 154.44.0.23 -d 192.168.0.0/24 -j ACCEPT
6. iptables -A OUTPUT -s 192.168.0.15 -j ACCEPT
7. iptables -A OUTPUT -d 192.168.0.15 -p tcp --sport 21 -j ACCEPT
8. iptables -A INPUT -d 154.44.0.23 -p tcp --sport 443 -j ACCEPT
9. iptables -P OUTPUT DROP
10. iptables -P INPUT DROP

2.- Realizar las reglas de filtrado para el siguiente supuesto:

- Todos los equipos de la red 192.168.0.0 podrán ver páginas Web por el puerto 80.
- Los equipos 192.168.0.3 y 192.168.0.4 podrán enviar paquetes al puerto de FTP de la máquina 193.55.0.2
- La dirección IP 192.168.0.25 se utiliza para equipos visitantes, de modo que no se le permite enviar tráfico de ningún tipo.
- Desde la red 194.2.10.0 se han sufrido varios intentos de intrusión, por lo que todo el tráfico tanto de entrada como de salida hacia esta red no se permite.

N.º Regla	IP Origen	Puerto Origen	IP Destino	Puerto Destino	Acción
1	192.168.0.0	*	194.2.10.0	-	DENEGAR
2	194.2.10.0	*	192.168.0.0	-	DENEGAR
3	192.168.0.25	*	*	-	DENEGAR
4	192.168.0.0	80	*	-	ACEPTA
5	192.168.0.3	21	193.55.0.2	-	ACEPTA
6	192.168.0.4	21	193.55.0.2	-	ACEPTA

3.- Teniendo en cuenta la tabla generada para el ejercicio 2 contesta estas preguntas:

- ¿Crees que llegará a tu equipo un paquete proveniente de la dirección IP 194.2.10.13?  
No, lo impide la regla n.º 2.
- ¿Se podrán enviar paquetes a la dirección IP 194.12.10.13 desde la dirección IP 192.168.0.3?  
Únicamente se podrían enviar paquetes por el puerto 80.