Problemas de Arquitectura de Redes, Sistemas y Servicios
Hoja de problemas 10

Problema 10.1: Un usuario de ADSL usa un portátil en su red inalámbrica con la dirección IP 192.168.1.12. Su programa de correo electrónico está configurado como sigue:

```
Cuenta: john.smith@mailsrus.com
Usuario: john.smith
Contraseña: ********
Servidor SMTP: smtp.mailsrus.com ( 88.7.6.30 )
Servidor POP: pop.mailsrus.com ( 88.7.6.32 )
Comprobar mail cada: 5 minutos
```

Capturando el tráfico que se envía por la red inalámbrica observa paquetes cada 5 minutos correspondientes a la comprobación del correo electrónico

a) Indique los datos de los primeros 3 paquetes que observará en uno de esas comprobaciones de correo.

	Dirección IP origen	Puerto origen	Dirección IP destino	Puerto destino	Protocolo
Primer paquete					
Segundo paquete					
Tercer paquete					

b) Indique los datos de los primeros 3 paquetes que observará al enviar un mensaje de correo a `prueba@mailgratis.com`. [Nota: `mailgratis.com` tiene dirección IP 158.2.1.10, si necesita alguna otra dirección IP, déjela indicada]

	Dirección IP origen	Puerto origen	Dirección IP destino	Puerto destino	Protocolo
Primer paquete					
Segundo paquete					
Tercer paquete					

Problema 10.2: Una universidad tiene su red interna separada del exterior por medio de un router que hace de cortafuegos, permitiendo aplicar reglas y eliminar determinados paquetes. El cortafuegos esta configurado para aplique reglas sobre todos los paquetes que procesa para decidir si los envía o no. El cortafuegos esta configurado con las siguientes reglas para que los usuarios puedan navegar por la web.

Si el protocolo es UDP					
IP origen	Puerto origen	IP destino	Puerto destino	mas condiciones	**ACCION**
cualquiera	cualquiera	cualquiera	cualquiera	-	ELIMINAR

Si el protocolo es TCP					
IP origen	Puerto origen	IP destino	Puerto destino	mas condiciones	**ACCION**
cualquiera	80	cualquiera	cualquiera	–	ENVIAR
cualquiera	cualquiera	cualquiera	80	–	ENVIAR
Para todos los demas					ELIMINAR

Sin embargo, un usuario interno lanza su navegador y no consigue conectarse a `www.google.com`. Observando los paquetes que envía su máquina observa que al pulsar enter para que el navegador vaya a la pagina de google se envían sólo paquetes UDP. ¿Qué está pasando? ¿Qué debería cambiar en las reglas del cortafuegos el administrador?

Problema 10.3: El host H1 se encuentra en una red en la que se filtran los paquetes que entran y sólo se permiten paquetes de conexiónes Web. El propietario de H1 quiere utilizar un programa peer-to-peer que utiliza normalmente el puerto TCP 6881 (aunque puede configurarse otro) pero no le funciona porque se eliminan los paquetes al no ser de conexiones web. ¿Cómo puede lograr que funcione el programa a pesar del filtro? ¿Puede conseguirlo si en H1 tiene activado el servidor Web? ¿Cómo cambia esto si el programa peer-to-peer utiliza UDP?

Problema 10.4: Fulanito el hacker consigue infiltrarse en el servidor Web de una empresa detrás de un cortafuegos que sólo deja pasar los paquetes que tienen puerto origen 80 o puerto destino 80. Para dejarse una puerta abierta, instala un servidor de telnet que escucha en el puerto 80 de ese ordenador. Pero cuando intenta conectarse a su servidor de telnet no le funciona... ¿Por qué no funciona?

☐ a) Porque telnet sólo puede funcionar en el puerto 23 como manda el RFC-854

☐ b) Porque los usuarios remotos no sabrán que el servidor está en el puerto 80

☐ c) Porque no se puede tener dos aplicaciones TCP escuchando en el puerto 80

☐ d) Porque telnet usa UDP y el cortafuegos sólo deja pasar los paquetes con el puerto 80 TCP

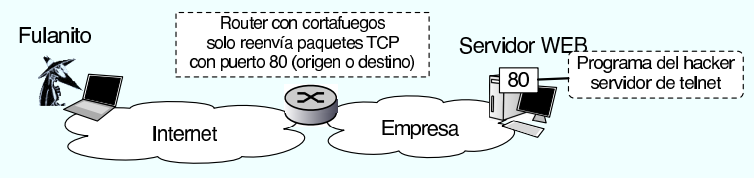
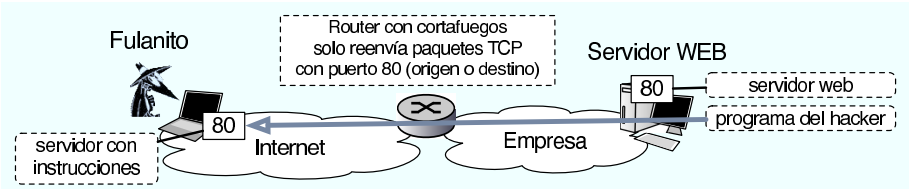


Figura 1: Figura del problema 10.4

Problema 10.5: En una universidad el servidor oficial de correo se encuentra en el servidor S1. El administrador de la red de la universidad intenta evitar que se utilicen otros servidores de correo distintos de S1 en su red. Para ello, dado que el router de salida R1 tiene funcionalidades de firewall y permite aplicar reglas sobre los paquetes, añade una regla: R1 no reenviará paquetes TCP al exterior si tienen el puerto destino 25, salvo si su dirección IP origen es S1. ¿Evitará esto el uso de otros servidores?. Si un usuario del departamento B coloca un servidor de SMTP en un H3. Puede utilizarlo para enviar correo fuera sin usar el servidor S1? ¿Puede usarlo para recibir correo sin usar el servidor S1? Razone las respuestas. ¿Puede un usuario de la red B consultar su cuenta de correo de un servidor externo?¿Por que?



Problema 10.6: Fulanito el hacker consigue infiltrarse en el servidor Web de una empresa detrás de un cortafuegos que sólo deja pasar los paquetes que tienen puerto origen 80 o puerto destino 80. Para dejarse una puerta abierta, instala un programa que cada cierto tiempo establece una conexión con el puerto 80 de un servidor externo controlado por él y se descarga instrucciones por HTTP ¿Qué problema tiene esto?

☐ a) Que HTTP no puede funcionar en el puerto 80 porque el puerto está reservado para la web

☐ b) No tiene ningún problema y debería funcionar

☐ c) Que no se puede tener una conexión TCP al puerto 80 y a la vez escuchar conexiones en el puerto 80

☐ d) Que HTTP usa UDP y el cortafuegos sólo deja pasar los paquetes con el puerto 80 TCP

Problema 10.7: La siguiente traza ha sido capturada en la red de la universidad

```
 1 0.963491 IP 130.206.168.45.60905 > 193.252.23.108.110: S 2357731200:2357731200(0) win 65535
 2 0.964072 IP 193.252.23.108.110 > 130.206.168.45.60905: S 1061601894:1061601894(0) ack 2357731201 win 5792
 3 0.964129 IP 130.206.168.45.60905 > 193.252.23.108.110: . ack 1061601895 win 65535
 4 1.111168 IP 193.252.23.108.110 > 130.206.168.45.60905: P 1061601895:1061601927(32) ack 2357731201 win 5792
 5 1.111753 IP 130.206.168.45.60905 > 193.252.23.108.110: P 2357731201:2357731218(17) ack 1061601927 win 65535
 6 1.112349 IP 193.252.23.108.110 > 130.206.168.45.60905: . ack 2357731218 win 5792
 7 1.200422 IP 193.252.23.108.110 > 130.206.168.45.60905: P 1061601927:1061601956(29) ack 2357731218 win 5792
 8 1.200834 IP 130.206.168.45.60905 > 193.252.23.108.110: P 2357731218:2357731232(14) ack 1061601956 win 65535
 9 1.201287 IP 193.252.23.108.110 > 130.206.168.45.60905: . ack 2357731232 win 5792
10 1.711614 IP 193.252.23.108.110 > 130.206.168.45.60905: P 1061601956:1061601991(35) ack 2357731232 win 5792
11 1.712040 IP 130.206.168.45.60905 > 193.252.23.108.110: P 2357731232:2357731238(6) ack 1061601991 win 65535
12 1.712630 IP 193.252.23.108.110 > 130.206.168.45.60905: . ack 2357731238 win 5792
13 1.861177 IP 193.252.23.108.110 > 130.206.168.45.60905: P 1061601991:1061602000(9) ack 2357731238 win 5792
14 1.861596 IP 130.206.168.45.60905 > 193.252.23.108.110: P 2357731238:2357731244(6) ack 1061602000 win 65535
15 1.862059 IP 193.252.23.108.110 > 130.206.168.45.60905: . ack 2357731244 win 5792
16 2.064350 IP 193.252.23.108.110 > 130.206.168.45.60905: P 1061602000:1061602005(5) ack 2357731244 win 5792
17 2.065276 IP 130.206.168.45.60905 > 193.252.23.108.110: F 2357731244:2357731244(0) ack 1061602005 win 65535
18 2.065890 IP 193.252.23.108.110 > 130.206.168.45.60905: . ack 2357731245 win 5792
19 2.065894 IP 193.252.23.108.110 > 130.206.168.45.60905: F 1061602005:1061602005(0) ack 2357731245 win 5792
20 2.065957 IP 130.206.168.45.60905 > 193.252.23.108.110: . ack 1061602006 win 65535
```

a) Indique a qué aplicación pertenece y qué acción del usuario ha causado esos paquetes

b) Indique cual es el cliente y cual el servidor en esta acción (con sus direcciones IP)