Las respuestas no razonadas, o no que utilicen estrictamente la notación indicada, no serán consideradas como válidas, aunque sean correctas. Recuadra CLARAMENTE tu respuesta a cada apartado. Consigna tu NIA, nombre y apellidos completos en todas las hojas que entregues.

1. **[4,5 ptos.]** En tu nuevo puesto como arquitecto de redes en Gromenagüer Corporation, recibes el encargo de diseñar la nueva infraestructura de la red corporativa, que debe estar compuesta de los siguientes elementos:

   - **Red LAN** interna, con 100 estaciones de trabajo.
   - **Servidores de negocio**, con 2 servidores Web (WEB1 y WEB2) y de correo (EML1 y EML2). Los servidores Web sirven el dominio 'www.gromenaguer.com', que resuelve a la dirección IP 150.20.57.3.
   - **Router de acceso**.

   Las características de los elementos anteriores son las siguientes:

Elemento	Dirección IP	Dirección MAC
Router	150.20.57.1	M1
WEB1	10.0.1.2	M2
WEB2	10.0.1.3	M3
EML1	10.0.1.10	M4
EML2	10.0.1.11	M5

   Con estos datos:

   1. **(1,5 ptos.)** Diseña una arquitectura que proporcione balanceo de carga a los servidores Web descritos utilizando el esquema de *one-arm*. **Haz un esquema claro**, introduciendo y etiquetando todos los elementos necesarios.
   2. **(1,5 ptos.)** En el escenario anterior, imagina que un cliente, con dirección IP 108.1.1.100, desea visitar la página Web de la empresa. ¿Cuál sería el itinerario exacto de la petición HTTP realizada desde que llega al *router* hasta que vuelve al cliente? Copia y rellena una tabla como la siguiente, añadiendo, si lo consideras necesario, aclaraciones sobre la misma.

Orden	IP origen	IP destino	MAC origen	MAC destino
1				
2				
...				

   3. **(1,5 ptos.)** Diseña ahora una arquitectura para proporcionar acceso en alta disponibilidad a todos los servidores (Web y de correo), con las siguientes restricciones:
      - Solo dispones de presupuesto para dos balanceadores y un *switch*.
      - Cada balanceador dispondrá de dos direcciones IP.
      - Los balanceadores deben funcionar bajo el esquema Activo-Pasivo.

Solución:

1. Lo importante en este apartado, además de obviamente especificar el esquema correctamente y conectar bien los elementos, es asignar al balaceandor:
   - Una dirección MAC (cualquiera no utilizada, M6, por ejemplo).
   - Una dirección IP pública, que debe corresponder a 150.20.57.3, el servicio Web que se desea balancear.
   - Un dirección IP privada correcta, que debe estar en el rango 10.0.1.x, para que pueda comunicarse con el resto de elementos.

- Entender que el tráfico, Web en este caso, NO va dirigido al router (150.20.57.1), aunque éste lo procese como parte de la comunicación, sino al balanceador, que, a su vez, redirige la petición al servidor adecuado. Por tanto, en la tabla de flujos no deben aparecer entradas como 108.1.1.100 → 150.20.57.1.

2. Si hemos asignado al balanceador, por ejemplo, M6 como dirección MAC y 10.0.1.1 como dirección IP, el flujo del paquete sería como el siguiente:

Orden	IP origen	IP destino	MAC origen	MAC destino	Comentario
1	108.1.1.100	150.20.57.3	M1	M6	Paquete llega al router, y éste lo enruta al balanceador
2	10.0.1.1	10.0.1.2	M6	M2	Balanceador elige a unos de los servidores Web y le envía la petición
3	10.0.1.2	10.0.1.1	M2	M6	El paquete vuelve al balanceador, que reescribe las direcciones IP originales y reenvía el paquete al router
4	150.20.57.3	108.1.1.100	M6	M1	El router recibe la respuesta, que parece provenir del balanceador, y enruta el paquete a Internet para que vuelva al cliente

3. El esquema Activo-Pasivo para proporcionar alta disponibilidad implica el uso de, al menos, dos balanceadores. Uno de ellos funcionará de forma permanente, hasta su fallo, momento en el que el Pasivo toma el control de su IP y comienza a procesar el tráfico.
   En estos aspectos, los puntos importantes a tener en cuenta son:
   - Los dos balanceadores comparten la dirección IP pública y privada (150.20.57.3, y 10.0.1.1, según los parámetros elegidos para este ejercicio), pero no la dirección MAC. Por tanto, se debe especificar una nueva dirección MAC (M7, por ejemplo), para el nuevo balanceador.
   - Ambos balanceadores deben compartir un enlace dedicado, para su comunicación interna y que les permita detectar la caída de alguno de ellos.

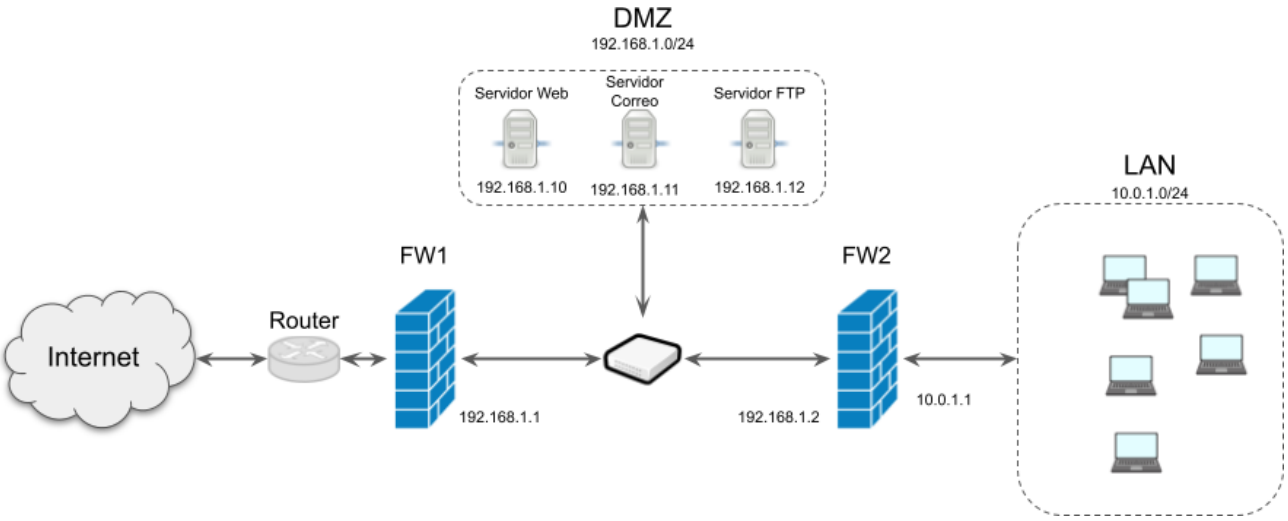
2. **[3 ptos.]** Considera la subred de la figura, donde debes configurar adecuadamente los cortafuegos FW1 y FW2. Para ello, los requisitos que te han pedido son los siguientes:
   - Se desea que el servidor Web sea accesible desde el exterior, por cualquier cliente.
   - Uno de los administradores del sistema desea poder acceder al servidor FTP, para su configuración, desde su casa, donde tiene la dirección IP fija 130.10.45.22. Por lo demás, solo debería ser accesible desde la LAN, puesto que es un servidor de uso interno principalmente.
   - Los usuarios de la LAN han pedido poder navegar por la Web, y enviar y recibir correo por SMTP.

   En este escenario, contesta razonadamente a las siguientes preguntas:

   1. **[2,5 ptos.]** Escribe las reglas de configuración de los cortafuegos, que implementen completamente la política anterior, en tablas similares a la siguiente:

Regla	Acción	IP origen	Puerto origen	IP destino	Puerto destino	Protocolo	Descripción
1							
2							
...							

   2. **[0,5 ptos.]** ¿Qué otras funciones, además de las cortafuegos, realiza el FW2?



Solución:

1. En la configuración de cualquier cortafuegos, conviene empezar por establecer la **política por defecto**, puesto que ésta determina el sentido del resto de reglas. La política de '*todo denegado, excepto lo explícitamente permitido*' es la más segura, y es la que vamos a seguir aquí. Esta regla se coloca la última y, después, el resto, teniendo en cuenta su orden.

   Base de reglas - FW1

Regla	Acción	IP origen	Puerto origen	IP destino	Puerto destino	Protocolo	Descripción
1	ALLOW	ALL	ALL	192.168.1.10	80,443	TCP	Acceso al servidor Web
2	ALLOW	192.168.1.0/24	ALL	ALL	80, 443	TCP	Se permite la navegación Web desde la LAN
3	ALLOW	130.10.45.22	ALL	192.168.1.12	21	TCP	Acceso al servidor FTP para admin
4	ALLOW	ALL	ALL	192.168.1.11	25	TCP	Se permite el acceso al servidor de correo desde el exterior
	DENY	ALL	ALL	ALL	ALL	ALL	Política por defecto

   Explicación de las reglas:
   - *a*) Permite el acceso al servidor Web desde el exterior (Internet).
   - *b*) Permite el acceso a servidores Web desde la LAN. Esta regla es la 'continuación' de la regla 2 del FW2 y, sin ella, el tráfico Web saliente se permitiría en el FW2 pero se tiraría en el FW1 y no llegaría a su destino.
   - *c*) Permite el acceso desde el domicilio del admin al servidor FTP.
   - *d*) Permite el acceso al servidor de correo desde Internet. Sin esta regla, el servidor no recibiría tráfico de otros servidores de correo.
   - *e*) Política por defecto, todo lo no explícitamente permitido es denegado.

   Base de reglas - FW2

Regla	Acción	IP origen	Puerto origen	IP destino	Puerto destino	Protocolo	Descripción
1	ALLOW	10.0.1.0/24	ALL	192.168.1.12	21	TCP	Acceso al servidor FTP desde LAN
2	ALLOW	10.0.1.0/24	ALL	ALL	80, 443	TCP	Se permite la navegación Web al exterior
3	ALLOW	10.0.1.0/24	ALL	192.168.1.11	25	TCP	Se permite la consulta del correo desde la LAN
	DENY	ALL	ALL	ALL	ALL	ALL	Política por defecto

Por otro lado, cualquier cortafuegos moderno soporta, por defecto, que las reglas sean bidireccionales: esto significa que las reglas se aplican por defecto en los dos sentidos, para permitir el establecimiento de una conexión TCP completa y el intercambio de datos. Por ejemplo, en el caso de la consulta del correo electrónico, la regla 5, por sí misma, no permitiría la 'vuelta' de los datos a las máquinas de la LAN. Para evitar que la base de datos se vuelva difícil de leer, los cortafuegos crean automáticamente (aunque no la muestran) la regla 'inversa', que permite la vuelta de los datos.

A la hora de corregir el ejercicio, se tendrán en cuenta, entre otros, los siguientes aspectos:

a) Hay una tabla para cada cortafuegos .
b) Se especifica política por defecto.
c) Se especifica correctamente el puerto FTP (21).
d) Se especifica correctamente el puerto SMTP (se consideran válidos 25, 587 y 465).
e) La columna **Protocolo** está correctamente rellena (en todos los casos, con TCP. Protocolo, en este caso, no hace referencia al protocolo de aplicación, sino al nivel de transporte).

2. Puesto que está interconectando dos redes diferentes, con direccionamiento distinto, el FW2 debe hacer también funciones de *router*.

3. **[2,5 ptos.]** Alice acaba de llegar a un acuerdo para la adquisición de acciones de la empresa de nueva creación de Bob. Para culminar el acuerdo, necesitan completar un contrato utilizando un mecanismo que cumpla con las siguientes restricciones:

   - El contrato debe ser totalmente confidencial y únicamente puede ser leído por Bob.
   - Se debe proporcionar garantía de no repudio por parte de Alice.
   - El proceso debe realizarse de manera estrictamente digital.

   Describe los mecanismos necesarios para completar este acuerdo, y dibuja un esquema que ilustre los pasos del proceso.

Solución: Esquema híbrido de firma digital, con sobre digital.