***I.E.S. Fernando Aguilar Quignon*** 

*C/Conil de la Frontera, 3*

*CP 11010, Cádiz*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Administración de Sistemas Operativos - 1ª Evaluación (RA 4 – CE d, e, f) Unidad Didáctica 4. Configuración multiusuario centralizada

**Ejercicio 1. Investiga sobre el SSH local port forwarding y explica en qué consiste y cómo implementarlo.**

El Local Port Forwarding permite redirigir un puerto local en la máquina cliente a un puerto específico en un host remoto a través de un servidor SSH. Es útil cuando un servicio está disponible sólo en un host remoto y queremos acceder a ese servicio de manera segura desde la máquina local. La conexión se realiza utilizando un túnel SSH.

* El tráfico que se envía desde el puerto local especificado se redirige al puerto de un servidor remoto a través de la conexión SSH.
* Esto permite acceder al servicio remoto como si estuviera ejecutándose localmente en el equipo cliente.

**Comando de SSH:** ssh -L <puerto-local>:<host-remoto>:<puerto-remoto> <usuario>@<servidor-ssh>

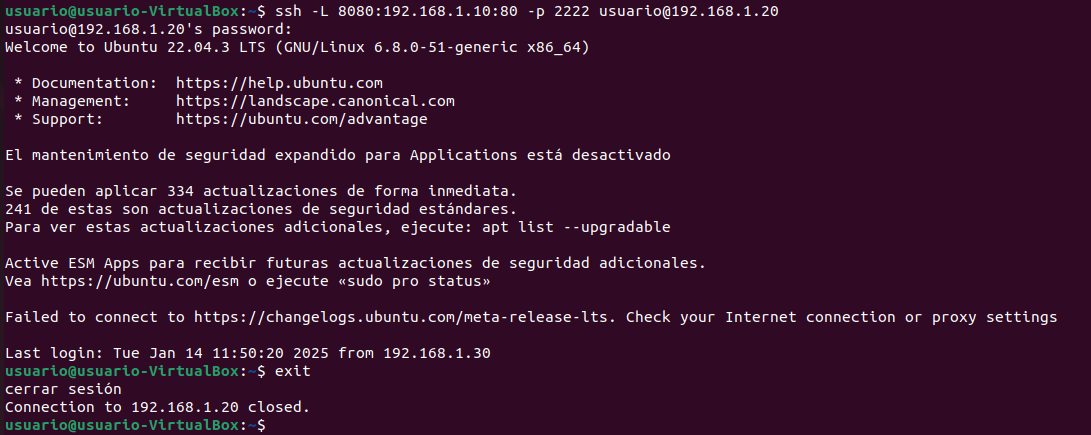
* **<puerto-local>:** Puerto que escuchará en la máquina local.
* **<host-remoto>:** Dirección IP o hostname del servidor al que queremos acceder.
* **<puerto-remoto:** Puertodel servicio en el host remoto.
* **<servidor-ssh>:** Servidor SSH al que nos conectamos**.**

**Ejercicio 2. Aplicando lo anterior, implementa un ejemplo de acceso a un servidor Apache utilizando un túnel en modo local port forwarding.**

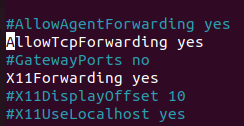
Para hacer este ejercicio vamos a utilizar tres máquinas virtuales:

* **Máquina Destino (192.168.1.10):** En el instalaremos apache y lo usaremos como ruta de destino
* **Maquina Servidor (192.168.1.20):** En ella instalamos openssh-server, la usaremos como túnel
* **Máquina Local (192.168.1.30):** Solo necesitaremos openssh-client

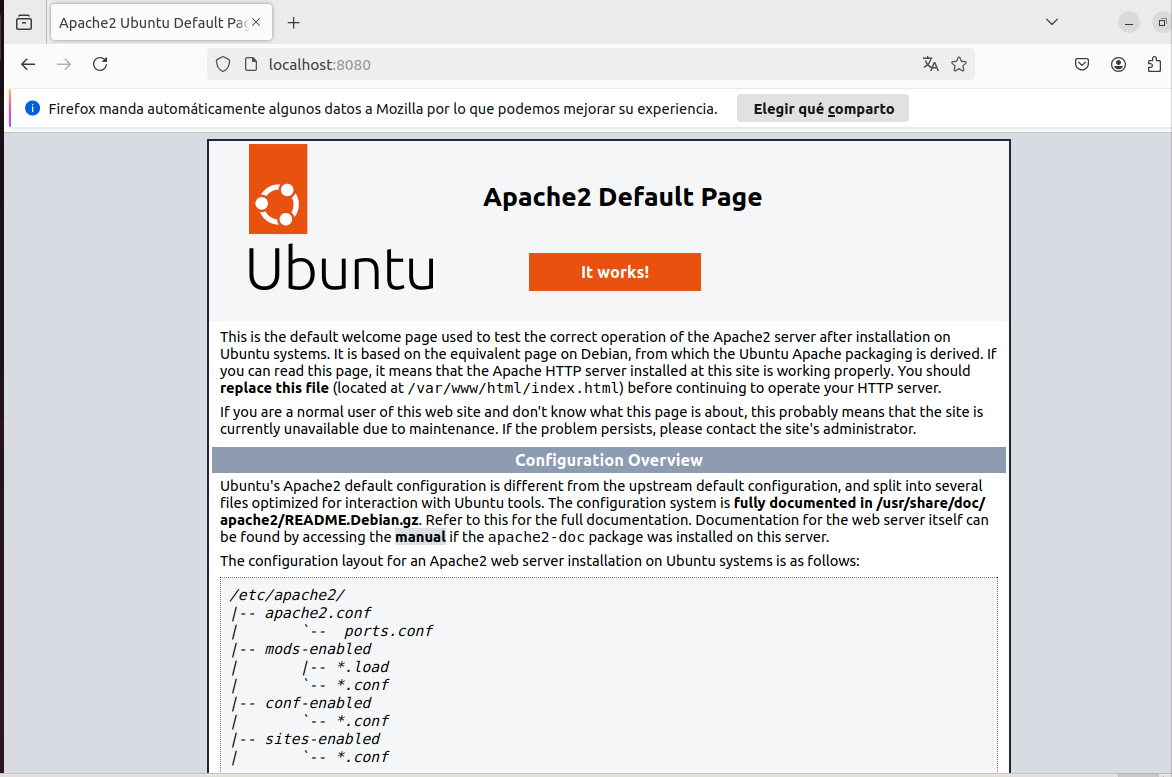
Para hacer este ejercicio necesitaremos conectarnos a la máquina destino (192.168.1.10) desde la máquina local (192.168.1.30) pasando por el servidor (20).



En la configuración del servidor SSH (/etc/ssh/sshd\_config), asegúrate de que las opciones de reenvío de puerto están habilitadas:



Para hacer la comprobación, desde la máquina local abriremos un navegador web para ejecutar: [localhost:8080](http://localhost:8080). Si todo está configurado correctamente, deberías ver la página de inicio de Apache del servidor remoto 192.168.1.20. La página por defecto es similar a:



**Ejercicio 3. Investiga sobre el SSH remote port forwarding y explica en qué consiste y cómo implementarlo.**

El Remote Port Forwarding es la inversa del local port forwarding. Permite que un puerto en el servidor SSH sea redirigido hacia un puerto local de la máquina cliente. Es útil cuando un servicio local necesita ser accesible desde una máquina remota.

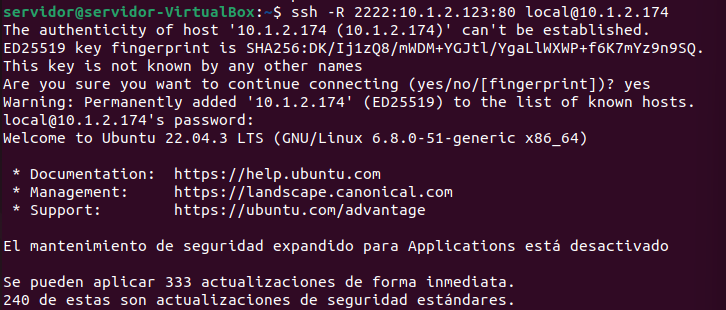
* El puerto en el servidor SSH escucha las conexiones y las redirige a un puerto local en la máquina cliente.
* Es necesario habilitar GatewayPorts en la configuración del servidor SSH para permitir estas conexiones

**Comando de SSH:** ssh -R <puerto-remoto>:<host-local>:<puerto-local> <usuario>@<servidor-ssh>

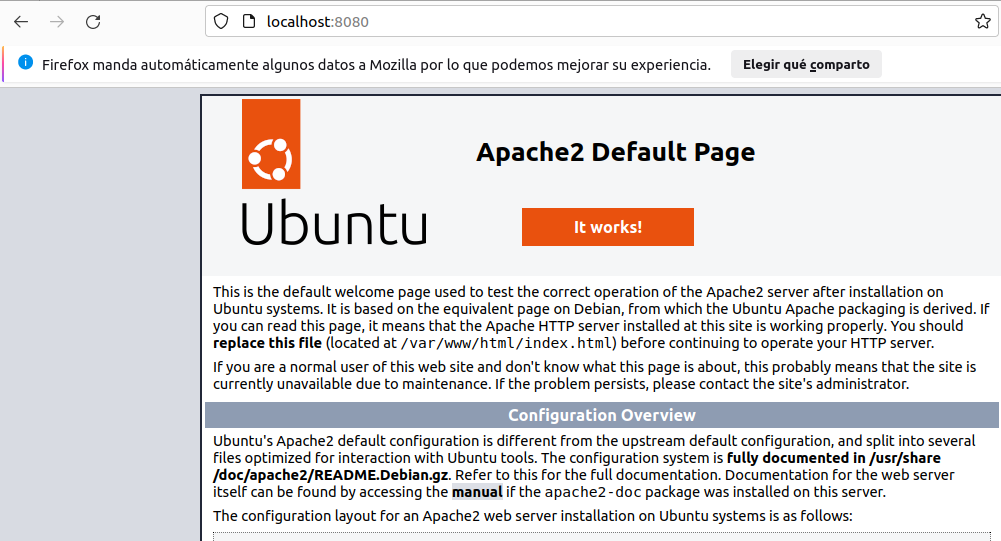
**Ejemplo de uso en SSH**: ssh -R 8080:localhost:80 usuario@192.168.1.20

**Ejercicio 4. Aplicando lo anterior, implementa un ejemplo de acceso a un servidor Apache utilizando un túnel en modo remote port forwarding.**

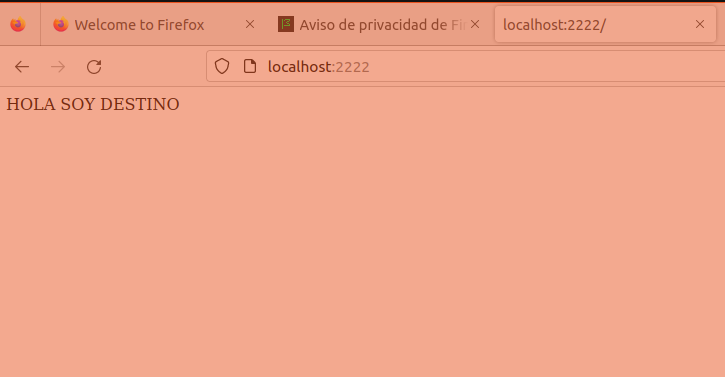
Para este ejercicio vamos a usar el servidor como máquina de puente, para ello usaremos la conexión apuntando hacia el cliente (10.1.2.123) desde el puerto y la dirección de la maquina local (10.1.2.174)



En el servidor podemos comprobar que desde localhost podemos acceder a apache



Y por último deberemos ver desde la máquina local el servidor de apache usando la ruta de dirección del servidor. En este caso vemos el html de apache editado correctamente



**Ejercicio 5. Investiga sobre el SSH dynamic port forwarding y explica en qué consiste y cómo implementarlo.**

**SSH dynamic port forwarding** transforma tu conexión SSH en un proxy SOCKS, permitiendo que todo el tráfico TCP de tu máquina local pase a través del túnel SSH. Esto es útil cuando quieres acceder a servicios en Internet que están bloqueados o no disponibles en tu ubicación, como servicios de streaming o navegación segura.

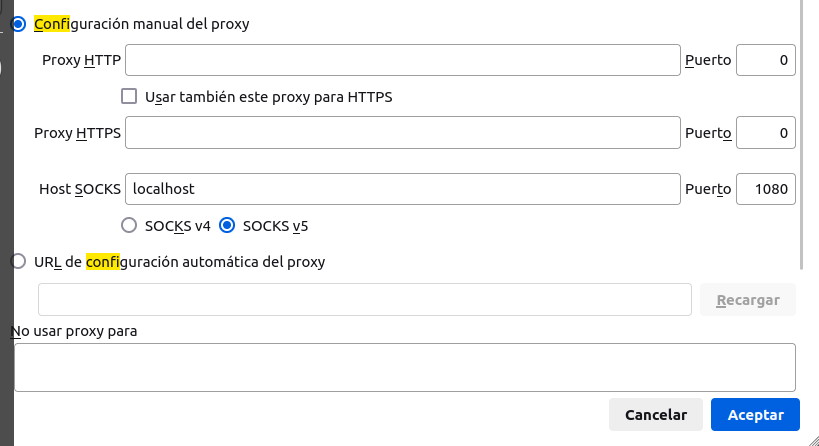
* La máquina local actúa como un proxy SOCKS. Todo el tráfico TCP se redirige a través del túnel SSH

**Comando de SSH:** ssh -D [local\_port] user@remote\_server

**Ejemplo de uso en SSH**: ssh -D 1080 user@remote\_server

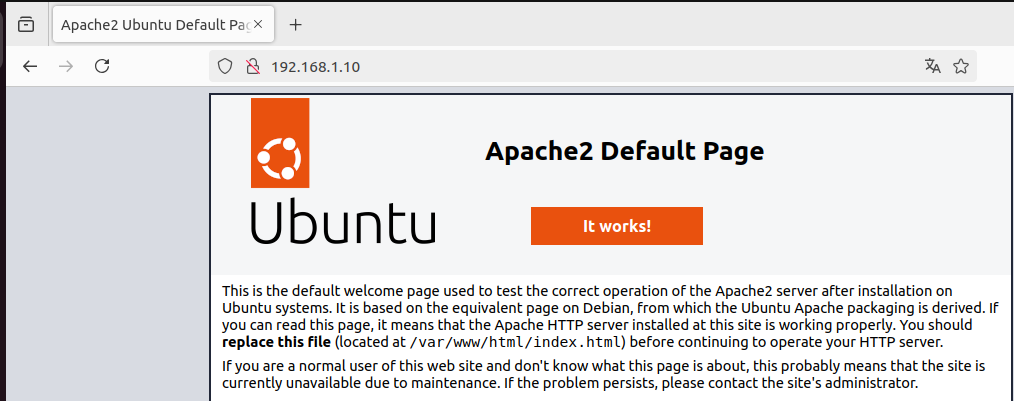
**Ejercicio 6. Aplicando lo anterior, implementa un ejemplo de navegación utilizando un túnel en modo dynamic port forwarding**.

1. Vamos a usar el servidor SSH en la máquina remota con IP 192.168.1.10 y configuraremos un túnel para navegar desde nuestra máquina local (192.168.1.20) a través de este servidor.
2. Crear el túnel SSH con Dynamic Port Forwarding en la máquina local
   1. Ejecuta el comando: ssh -D 1080 usuario@192.168.1.20
   2. Si el túnel se creó correctamente, verás el prompt de la terminal en la máquina remota.
3. Configurar el navegador para usar el túnel SOCKS en la máquina Local
   1. Abre el navegador Firefox
   2. Ve a Configuración → General → Configuración de red → Configuración manual del proxy
   3. Aplicar la siguiente configuración:

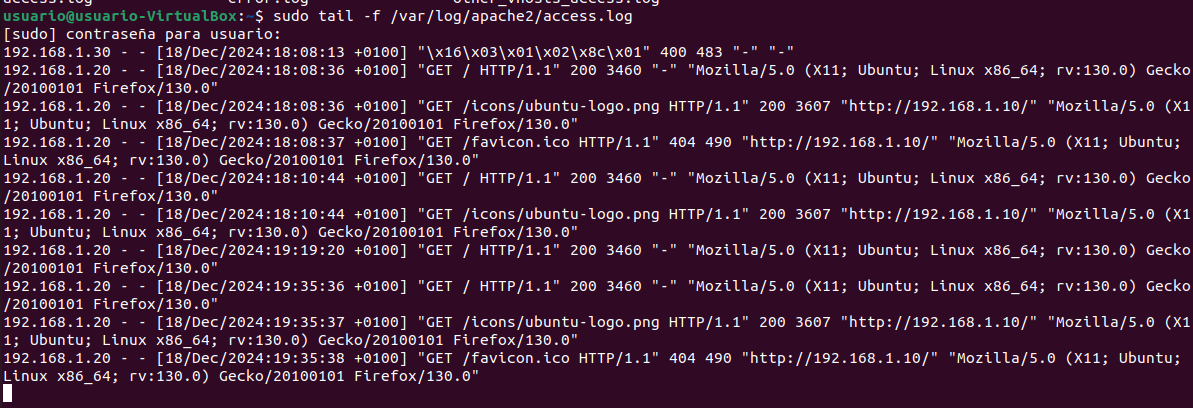


1. Comprobar que la navegación pasa por el túnel

Para hacer la comprobación, desde la máquina local buscaremos desde el navegador la dirección de la máquina destino (192.168.1.10)



Por último podemos ver el registro de la conexión a través de los logs:



En esta imagen comprobamos que el servidor (192.168.1.20) actúa como puente entre estas dos máquinas