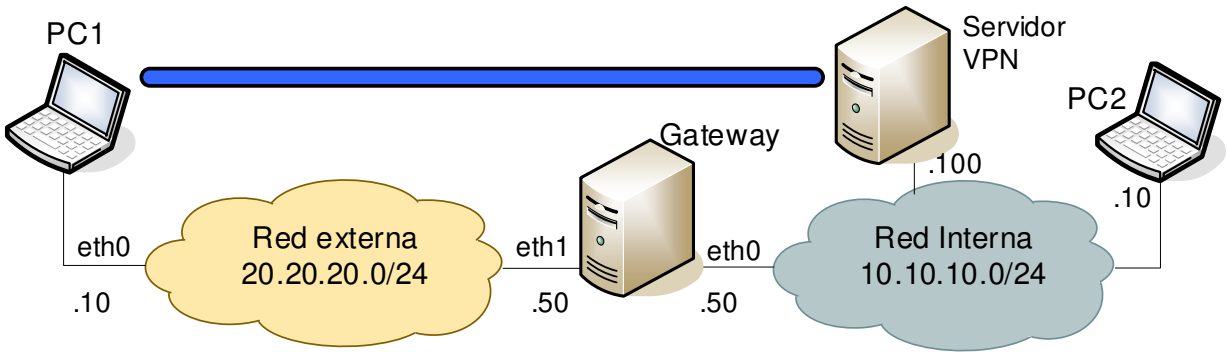
Fecha límite para la entrega: 29 de septiembre de 2024

1. OBJETIVO

Puesta en marcha de una Red Privada Virtual (*VPN, Virtual Private Network*) para la conexión segura a una red remota utilizando el software OpenVPN.

2. ESCENARIO (modo TUN)



Como se aprecia en la figura, el escenario contará con dos redes (externa e interna), un *router* que conecta a ambas, un servidor VPN, un cliente VPN (PC1) y un equipo de la red interna (PC2). El cliente establecerá una conexión VPN con el servidor para acceder a los recursos de la red interna (en nuestro caso, a algún servicio presente en el propio servidor y en el equipo PC2).

Los equipos serán máquinas virtuales Linux conectadas a las redes **externa** e **interna** (ambas serán redes virtuales con las capacidades de conectividad necesarias). El *gateway* contará con **dos interfaces** tendrá activada la función de *forwarding.* Los equipos de la red interna (Servidor y PC2) tendrán el *gateway* como *router* por defecto. El servidor también necesitará activar la función de *forwarding*, al trabajar en modo TUN. El PC externo (PC1) no necesitará configurar el *router* por defecto (aunque lo activaremos inicialmente).

En el esquema se indica el direccionamiento a usar y las direcciones IP fijas que asignaremos a todos los interfaces.

Nota: para habilitar la función de reenvió (*forwarding*) en el Gateway y el Servidor, podemos añadir net.ipv4.ip_forward=1 en el archivo /etc/sysctl.conf y a continuación ejecutar sysctl -p; puede comprobarse el nuevo valor con sysctl net.ipv4.ip_forward.

3. PRÁCTICO

1. Crear el escenario virtualizado propuesto. Configurar las direcciones IP de todos los interfaces y activar el *forwarding* en el *Gateway.* Establecer como *router* por defecto el Gateway en los restantes equipos y comprobar la conectividad. Instalar algún servicio en los equipos PC1, PC2 y Servidor (servidor SSH, Apache, …).
2. Crear una Autoridad de Certificación en el Servidor y emitir los elementos necesarios para nuestra configuración (valores DH y claves/certificados para el servidor y el cliente).
3. Configurar el servidor OpenVPN en **modo TUN** (actuará como *router*), usando el archivo server.conf). Usaremos UDP como protocolo de transporte. Configurar su arranque automático al inicio y arrancar el servicio. También habilitaremos la función de *forwarding* en este equipo Servidor, para que pueda encaminar el tráfico entre sus interfaces.
4. Configurar en el *Gateway* un *port-forwarding* para reenviar al servidor interno todo el tráfico recibido en el puerto udp/1194 de su interface externo (es necesaria una regla iptables nat en PREROUTING).

5. Configurar en el *Gateway* el enmascaramiento para todo el tráfico saliente Comprobar que siguen pudiendo alcanzarse recursos externos desde la red interna (PC2 a PC1). Verificar que se realiza el enmascaramiento usando *tcpdump*.
6. Configurar el cliente OpenVPN en PC1 (client.conf) para conectar al servidor (a través de la IP del Gateway). Para completar esta tarea será necesario copiar los archivos necesarios obtenidos en el apartado 2.
7. Iniciar el cliente y comprobar que se conecta al servidor. Verificar la configuración que se establece en el interface virtual tun del cliente, su tabla de encaminamiento y que es posible alcanzar desde PC1 los recursos ofrecidos por el Servidor a través de la VPN (puede hacer una captura del tráfico intercambiado para verificar que los paquetes se transportan sobre tun0, que a su vez se envía encriptado sobre eth0). Desactivar el *router* por defecto en PC1 y comprobar que sigue siendo posible acceder al Servidor.
8. Compruebe si es posible alcanzar el equipo PC2 desde PC1 a través de la conexión VPN. ¿Qué está sucediendo?
9. Modificar la configuración de PC2 para que pueda comunicar con PC1 a través de la VPN. Nota: también es posible configurar el Gateway para el retorno de los paquetes a través de la VPN, sin modificar el encaminamiento en PC2. Compruebe ambas opciones.

10. **Partes opcionales:**
    a. Realizar una nueva configuración de la conexión OpenVPN, ahora en **modo TAP** o *bridged*. Para ello, en el servidor debe configurarse un bridge entre el interface tap (normalmente tap0) y el interface de conexión a la LAN. Esta configuración se realiza con un *script* adicional (suele incluirse dentro del paquete de OpenVPN). En el modo *bridged*, hay que asociar una IP dinámica de la red destino al cliente VPN. Esto puede hacerse con el servicio DHCP de la red destino, o reservando un rango de direcciones en el propio servidor VPN (en la directiva server-bridge).
    b. Estudiar las características de la solución VPN **WireGuard** (www.wireguard.com). Preparar un escenario para poner en marcha una configuración básica de esta VPN (puede usarse como base la maqueta anterior).

4. FORMA DE ENTREGA

Una vez finalizada la práctica, cada grupo entregará una memoria justificativa en formato PDF. La memoria deberá incluir los pasos seguidos para la realización de cada tarea planteada, comandos utilizados y dificultades encontradas. También incluirá pantallazos con las pruebas de funcionamiento realizadas.

La memoria será ordenada, clara y legible. Se deberán evitar los "listados" innecesarios. Si se considera de interés, podrán incorporarse como anexos a la memoria, debidamente reseñados.

El resultado será un documento único en formato PDF denominado practica1-SPD.pdf que se enviará antes de la fecha de cierre a la dirección de correo electrónico teo.rojo@ceu.es.

Se podrá requerir la defensa individual de la práctica a cualquiera de los miembros del grupo. Deberá guardarse una copia de las máquinas virtuales utilizadas en el desarrollo de la práctica, para poder verificar, si fuera necesario, su correcto funcionamiento.

5. REFERENCIAS

http://openvpn.net/
https://www.wireguard.com/