TP 11 Redes Privadas Virtuales

Fecha de Entrega: Chivilcoy: 21/11/2022 - Luján 28/11/2022

Objetivo: Conocer herramientas de uso extendido para configurar redes privadas virtuales. Reconocer los escenarios de uso habituales de VPN y los servicios de seguridad asociados. Categorías ISO: FCAP**S**.

Bibliografía

- HERTZOG, R.; MAS, R. 2015. Capítulo 10. Sección 2: "Red privada virtual". En *El manual del Administrador de Debian*. Freexian. https://debian-handbook.info/browse/es-ES/stable/sect.virtual-private-network.html
- YONAN J. 2003. *The User-Space VPN and OpenVPN*. http://52.52.21.174/papers/BLUG-talk/index.html

Experiencia de laboratorio

Elija para esta experiencia de laboratorio un compañero/a de trabajo con el cual realizará la actividad. Un equipo actuará de cliente y otro de servidor.

Túnel punto a punto simple Para llevar a cabo esta experiencia se utilizará la herramienta "Open VPN". Se requiere por lo tanto instalar los siguientes paquetes:

```
apt-get install openvpn
```

Para la primera experiencia, y por fines didácticos, se realizará una conexión punto a punto con la mínima configuración posible.

1. **En el servidor**: Crear un túnel y asignarle la interfaz virtual `tun0` . Configurar la ip `10.9.8.1` al extremo local del túnel y `10.9.8.2` al extremo remoto.

   ```
   openvpn --dev tun0 --ifconfig 10.9.8.1 10.9.8.2
   ```

2. **En el cliente**: Crear el otro extremo del túnel y la interfaz virtual con el comando.

   ```
   openvpn --remote IP_SERVIDOR_VPN --dev tun0 --ifconfig 10.9.8.2 10.9.8.1
   ```

3. Verificar que la interfaz del túnel (`tun0`) está activa mediante el comando `ip link` ¿Cuántas interfaces de red posee ahora el host? ¿Cuáles de ellas son reales/físicas?

4. Compruebe que la configuración haya sido exitosa utilizando el comando `ping` contra el extremo opuesto del túnel.

5. Realice una captura durante la ejecución del ping (en el cliente o en el servidor) en la interfaz virtual `tun0` . Guardela con el nombre captura `vpn-simple-tun.pcapng` . ¿Es posible visualizar los mensajes ICMP?

6. Destruya el túnel en el extremo del cliente y realice una captura en la interfaz física del equipo al momento de volver a crearlo. Además repita la operación de realizar un `ping` . Guarde la captura con el nombre `vpn-simple-eth.pcapng` . ¿Es posible visualizar los mensajes ICMP? ¿Por qué?

Túnel punto a punto con cifrado simétrico En este escenario se utiliza una configuración donde se requiere de un usuario y contraseña para poder establecer el túnel.

1. **En el servidor**, crear una nueva clave con:

   ```
   openvpn --genkey --secret secret.key
   ```

2. Se debe copiar la clave generarda en el servidor al equipo del cliente. Puede utilizar para ello el comando `scp` .

3. **En ambos extremos**, ubique el archivo de clave `.key` en el directorio `/etc/openvpn/`

4. **En el servidor** cree el archivo `/etc/openvpn/tun0.conf` para configurar la interfaz y luego incorpore los siguientes parámetros:

   ```
   dev tun0
   ifconfig 10.9.8.1 10.9.8.2
   secret /etc/openvpn/secret.key
   ```

5. **En el cliente**, configure también una interfaz en el archivo `/etc/openvpn/tun0.conf` con los siguientes parámetros:

   ```
   remote ip-del-servidor
   dev tun0
   ifconfig 10.9.8.2 10.9.8.1
   secret /etc/openvpn/secret.key
   ```

6. **En el servidor** levante el túnel de configurado con:

   ```
   openvpn --config /etc/openvpn/tun0.conf
   ```

7. **En el cliente** Inicie una captura y luego levante el túnel configurado con el mismo comando utilizado en el punto anterior. Realice un ping al extremo del tunel correspondiente al servidor. Guarde la captura con nombre `vpn-simetrico.pcapng` . ¿Es posible ver los mensajes ICMP en la captura?

Tunel punto a punto con WireGuard y cifrado asimétrico Si bien este escenario puede realizarse mediante OpenVPN con certificados X.509 utilizando una Infraestructura de Clave Pública (PKI) propia, en esta oportunidad utilizaremos una tecnología de reciente creación que basa su funcionamiento en cifrado asimétrico utilizando una arquitectura y un protocolo novedoso: WireGuard.

1. Instale la herramienta (válido para debian 11, para debian 10 debe agregarse el repositorio backports: https://backports.debian.org/):

   ```
   apt update
   apt install wireguard
   ```

   Para otros sistemas operativos ver: https://www.wireguard.com/install/

2. **En ambos equipos extremos de la vpn** genere su par de claves públicas y privadas

   ```
   wg genkey > private.key
   cat private.key
   wg pubkey < private.key > public.key
   cat public.key
   ```

3. **En el servidor** crear una nueva interfaz de red llamada wg0 y asignarle una IP

```
ip link add wg0 type wireguard
ip addr add 10.9.8.1/24 dev wg0
```

4. **En el cliente** crear una nueva interfaz de red llamada wg0 y asignarle una IP

```
ip link add wg0 type wireguard
ip addr add 10.9.8.2/24 dev wg0
```

5. **En ambos equipos** asignar la clave privada a la interfaz de red y levantar la interfaz

```
wg set wg0 private-key ./private.key
ip -4 addr show
ip link set wg0 up
```

6. **En ambos equipos**, indicar la dirección IP del extremo y su respectiva clave pública

```
wg set wg0 listen-port PUERTO_LOCAL peer CLAVE_PUB \
allowed-ips IPVIRTUAL_EXTREMO/32 endpoint IPREAL_EXTREMO:PUERTO_EXTREMO
```

   Las variables son las siguientes:

   - `PUERTO_LOCAL` es el puerto en el cual Wireguard va a escuchar en ese host.
   - `CLAVE_PUB` es la clave pública del otro extremo.
   - `IPVIRTUAL_EXTREMO` es la IP 'virtual', la que pertenece a la red conformada por la VPN. En este caso se viene utilizando 10.9.8.1 para el server y 10.9.8.2 para el cliente.
   - `IPREAL_EXTREMO` es la IP en la LAN del otro extremo.
   - `PUERTO_EXTREMO` es el puerto en el cual está escuchando el servicio en el otro extremo (ya funciona conque el 'cliente' especifique el `PUERTO_LOCAL` del servidor, pero pueden ser iguales y recíprocos).

7. Pueden comprobar el estado de la VPN wiregard en ambos lados con los comandos:

```
wg show
wg showconf wg0
```

8. Iniciar captura sobre la interfaz REAL del equipo.

9. Visualizar la tabla de rutas y probar el enlace VPN

```
ip route show
ping 10.9.8.X
```

10. Detener la captura y determinar con ella el protocolo de transporte utilizado, los puertos origen y destino, e indicar si Wireshark interpreta apropiadamente las PDUs del protocolo de "aplicación" WireGuard

Trabajo práctico

1. ¿Porqué no es posible visualizar las PDU de openVPN en la captura `vpn-simple-tun.pcapng` ?

2. Identifique en la captura `vpn-simple-eth.pcapng` , los mensajes de establecimiento del túnel y busque los paquetes correspondientes a los mensajes ICMP Echo Request y Echo Repl. ¿Para qué se utiliza el campo HMAC?

3. ¿Qué identifican las direcciones IP luego de la instrucción `ifconfig` ?

4. ¿Qué servicios de seguridad se proveen en la experiencia de laboratorio denominada “Tunel punto a punto simple”?
5. ¿Por qué usted considera que se utiliza en la experiencia de “Tunel punto a punto simétrico” un archivo de clave secreto en lugar de una cadena de texto corta?
6. ¿Qué servicios de seguridad se proveen en la experiencia de laboratorio denominada “Tunel punto a punto simétrico”?
7. En la captura `vpn-simetrico.pcapng` ¿Es posible ver los mensajes ICMP? ¿y las ip internas del tunel? ¿Qué datos de usuario puede extraer de la captura?
8. ¿Qué configuración debe aplicarse para convertir el tunel punto a punto creado en las experiencias en una VPN tipo: a) equipo a red y b) red a red?.
9. Describa las principales diferencias entre OpenVPN y WireGuard.