



UNIVERSIDAD DE COLIMA

FACULTAD DE INGENIERÍA MECÁNICA Y
ELÉCTRICA

SEGURIDAD DE REDES

INGENIERÍA EN COMPUTACIÓN INTELIGENTE

**Práctica: Implementación del servidor
VPN con StrongSwan**

Estudiantes:

Roberto Alejandro Hernández Paredes, Paola Berenice
Robles Becerra

Profesor:

Dr. Leonel Soriano Equigua

Coquimatlán, Colima.

Fecha:

29 de noviembre del 2024

Índice

1. Objetivos:	3
2. Marco Teórico	3
3. Topología de Red	4
4. Desarrollo de la práctica	5
4.1. Instalación y configuración del servidor VPN con StrongSwan	5
4.2. Configuración de la red y las subredes	7
4.3. Instalación y configuración del cliente VPN	7
4.4. Verificación del funcionamiento de la conexión VPN	8
5. Conclusiones	8
6. Agradecimientos	9
7. Referencias	9

Índice de figuras

1.	Topología de la red utilizada en la práctica	5
2.	Configuración del archivo <code>/etc/ipsec.secrets</code>	7
3.	Prueba de <code>ping</code> entre cliente y servidor VPN	8

1. Objetivos:

- Implementación del servidor VPN con StrongSwan: Configurar y poner en marcha un servidor de VPN en un sistema Linux (preferentemente Debian o Ubuntu Server), lo que implica la instalación y configuración de StrongSwan para permitir la conexión segura de clientes a la red interna.
- Configuración de redes y subredes: Configurar adecuadamente el router del laboratorio de telefonía para que funcione con al menos dos subredes. Una subred debe estar conectada al servidor VPN, y la otra debe estar conectada al cliente de VPN, asegurando que haya comunicación entre ambas.
- Instalación y configuración del cliente VPN: Instalar y configurar un cliente VPN en una laptop, que puede ser tanto en Windows como en Linux. Esto permitirá que la laptop se conecte al servidor VPN de forma remota a través de la red configurada.
- Verificación del funcionamiento de la conexión VPN: El equipo de estudiantes deberá demostrar al profesor que el cliente puede conectarse correctamente al servidor y acceder a los recursos de la red interna de manera segura.

2. Marco Teórico

La implementación de redes privadas virtuales (VPN) es esencial para garantizar una comunicación segura y privada entre dos puntos, especialmente cuando se usan redes públicas como internet. En este caso, se utiliza **StrongSwan**, una solución de software de código abierto para implementar VPNs basadas en el protocolo IPsec. StrongSwan es altamente configurable y permite establecer conexiones seguras entre clientes y servidores, asegurando la integridad, confidencialidad y autenticidad de los datos transmitidos.

El protocolo IPsec es un conjunto de protocolos que protege las comunicaciones a nivel de red, proporcionando autenticación de origen y cifrado de datos. Al configurarlo correctamente en el servidor y el cliente, se puede garantizar que los datos enviados entre ambos puntos estén protegidos contra ataques de interceptación y alteración.

El sistema operativo utilizado en el servidor es **Ubuntu Server 24.04**, que es una distribución de Linux enfocada en servidores y administradores de sistemas. Este sistema operativo es elegido debido a su estabilidad, soporte extendido y fácil integración con herramientas de administración de redes como StrongSwan.

El uso de máquinas Raspberry Pi como servidor VPN es adecuado debido a su bajo costo, bajo consumo de energía y capacidad para manejar redes pequeñas a medianas sin problemas. La implementación en una Raspberry Pi también permite la simulación de un entorno de red de oficina pequeña o laboratorio.

3. Topología de Red

La topología de red utilizada en esta práctica consta de tres dispositivos principales: un servidor (Raspberry Pi), un router y un cliente. A continuación, se describe la configuración de cada dispositivo:

- **Servidor (Raspberry Pi):** La dirección IP del servidor es 192.168.1.12, con una máscara de subred de 255.255.255.0 y la puerta de enlace en g0/1.
- **Router:** El router tiene dos interfaces configuradas:
 - g0/1 con dirección IP 192.168.1.254.
 - g0/2 con dirección IP 192.168.2.254.
- **Cliente:** El cliente tiene la dirección IP 192.168.2.12, con una máscara de subred de 255.255.255.0 y la puerta de enlace en g0/2.

La configuración de la topología asegura que las dos subredes, 192.168.1.0/24 para el servidor y 192.168.2.0/24 para el cliente, estén correctamente interconectadas a través del router, lo que permite la comunicación entre el servidor y el cliente mediante la VPN.

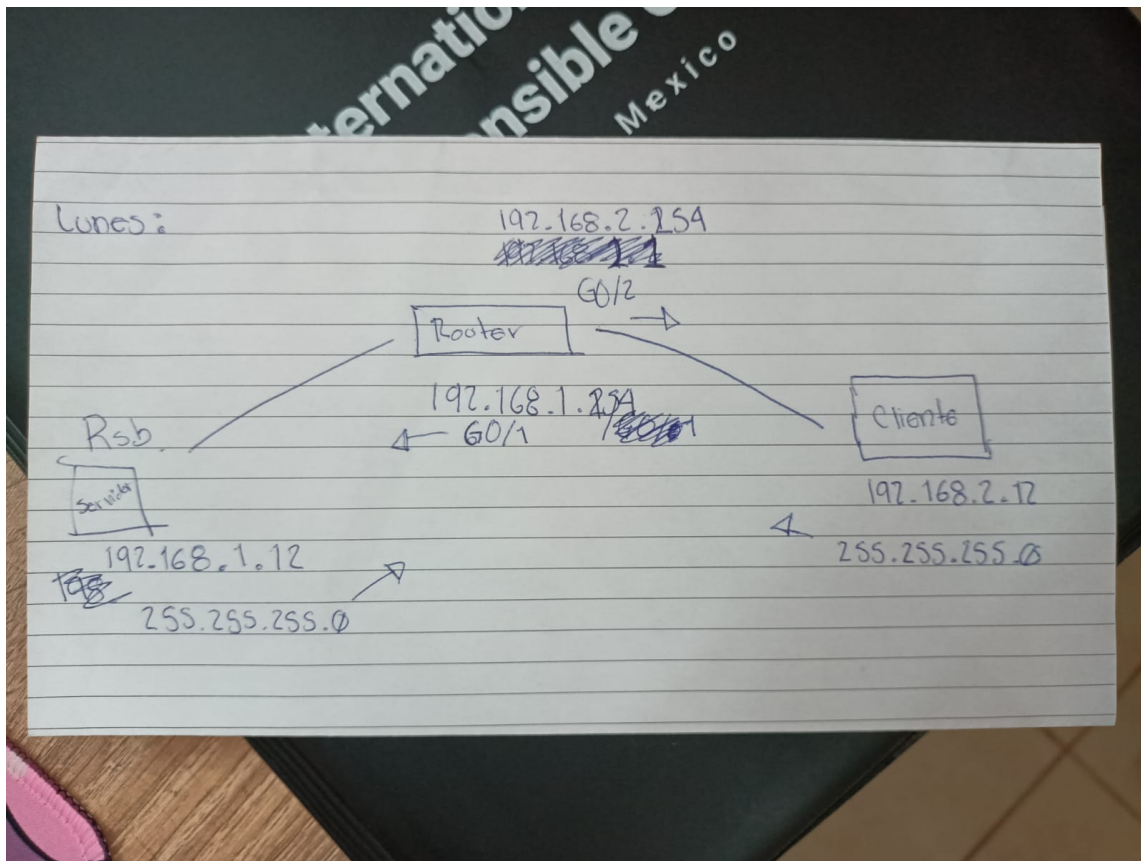


Figura 1. Topología de la red utilizada en la práctica

4. Desarrollo de la práctica

4.1. Instalación y configuración del servidor VPN con StrongSwan

Para la instalación del servidor VPN, seguimos las instrucciones detalladas en el tutorial de DigitalOcean, que describe cómo configurar un servidor VPN IKEv2 con StrongSwan en un sistema Ubuntu 20.04. Los pasos principales incluyen:

1. Actualizar el sistema operativo:

```
sudo apt update
sudo apt upgrade
```

2. **Instalar StrongSwan:**

```
sudo apt install strongswan
```

3. **Habilitar el reenvío de IP:** Se habilita el reenvío de IP para que las conexiones VPN puedan ser redirigidas adecuadamente dentro de la red.

```
sudo nano /etc/sysctl.conf
net.ipv4.ip_forward=1
sudo sysctl -p
```

4. **Configurar el archivo ipsec.conf:** Este archivo contiene la configuración del servidor VPN. Se define la red y los parámetros del protocolo IKEv2.

```
sudo nano /etc/ipsec.conf
```

5. **Configurar el archivo ipsec.secrets:** En este archivo se definen las claves de autenticación para el servidor VPN.

```
sudo nano /etc/ipsec.secrets
```

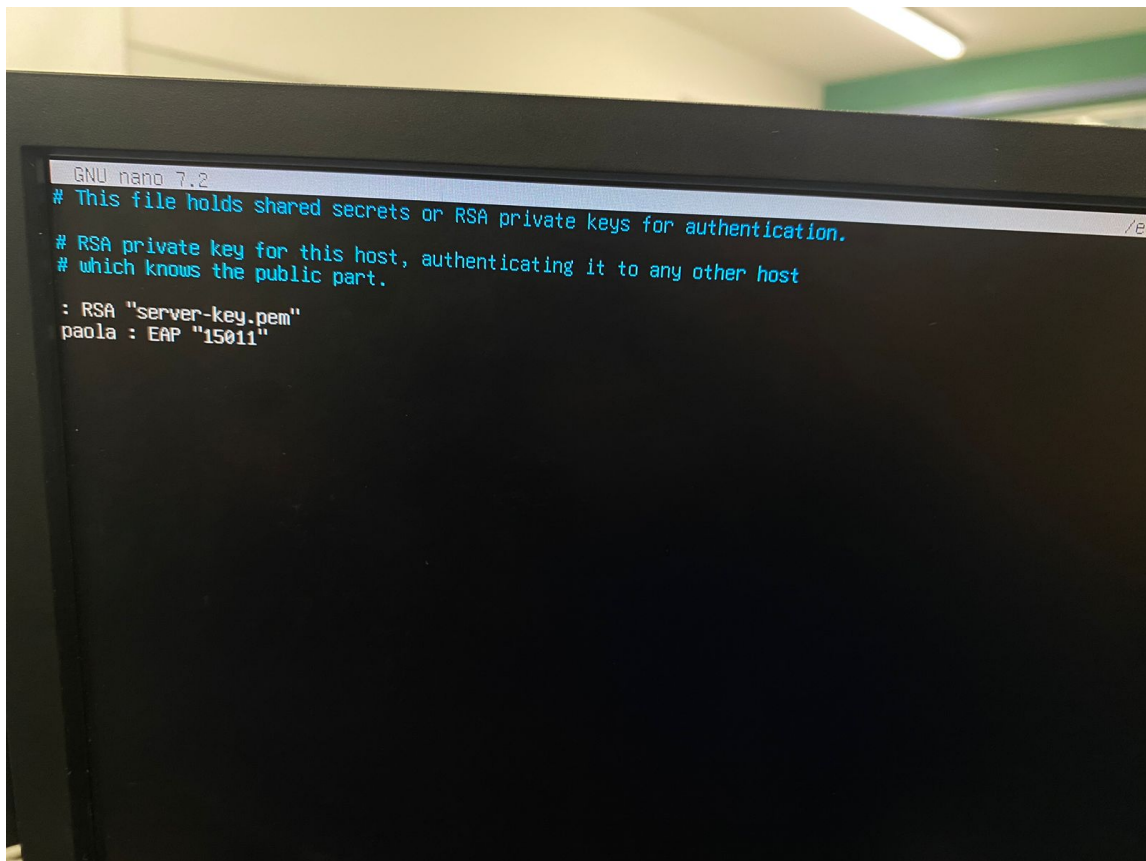



Figura 2. Configuración del archivo `/etc/ipsec.secrets`

4.2. Configuración de la red y las subredes

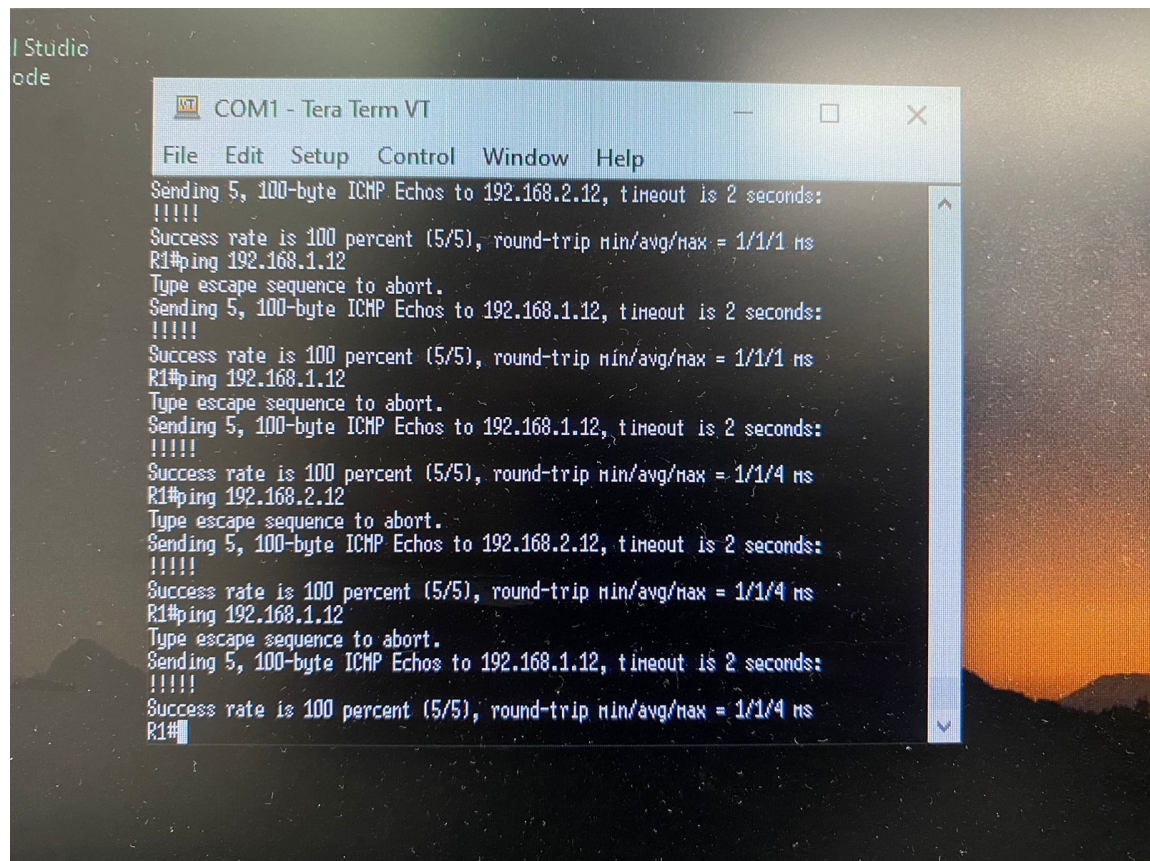
Siguiendo el tutorial, configuramos el router del laboratorio para que tuviera dos subredes. Una subred se conecta al servidor VPN, y la otra a los clientes VPN. Se modificaron las configuraciones de las interfaces del router para asegurarse de que el tráfico VPN pudiera ser dirigido correctamente.

4.3. Instalación y configuración del cliente VPN

Para la instalación del cliente VPN, se configuró una laptop con Ubuntu 20.04. Se instaló el cliente StrongSwan y se configuró para que se conectara al servidor VPN mediante el protocolo IKEv2.

4.4. Verificación del funcionamiento de la conexión VPN

Se realizaron pruebas de conectividad entre el cliente y el servidor VPN. Al ejecutar un ping desde el cliente hacia el servidor y viceversa, se confirmó que la conexión VPN estaba operativa y segura.



The image shows a terminal window titled "COM1 - Tera Term VT" with a menu bar (File, Edit, Setup, Control, Window, Help). The terminal output displays a series of ping tests. Each test involves sending 5, 100-byte ICMP Echoes to a specific IP address with a 2-second timeout. The results for each test are: "!!!!", "Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms", and "R1#ping 192.168.1.12". The tests are performed in a sequence: first to 192.168.2.12, then to 192.168.1.12, then to 192.168.2.12, then to 192.168.1.12, and finally to 192.168.2.12. The prompt "R1#" is visible at the end of the last line.

```
COM1 - Tera Term VT
File Edit Setup Control Window Help
Sending 5, 100-byte ICMP Echoes to 192.168.2.12, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
R1#ping 192.168.1.12
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 192.168.1.12, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
R1#ping 192.168.1.12
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 192.168.1.12, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
R1#ping 192.168.2.12
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 192.168.2.12, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
R1#ping 192.168.1.12
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 192.168.1.12, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
R1#
```

Figura 3. Prueba de ping entre cliente y servidor VPN

5. Conclusiones

La práctica permitió comprender la importancia de las redes privadas virtuales y cómo implementar una solución segura utilizando StrongSwan. Además, se adquirió experiencia en la configuración de redes y subredes, así como en la instalación y administración de servidores VPN en sistemas Linux. Las pruebas de conectividad

demonstraron que la configuración fue exitosa, lo que garantiza una comunicación segura entre los dispositivos conectados a la VPN.

Sin embargo, la parte más difícil de la práctica fue la configuración del servidor, ya que la guía utilizada no era completamente precisa y algunas configuraciones requerían la instalación de paquetes adicionales. Esto obligó a los estudiantes a investigar y ajustar la configuración de manera personalizada, lo que proporcionó una comprensión más profunda del proceso y permitió resolver problemas prácticos de administración de redes.

6. Agradecimientos

Queremos expresar nuestro sincero agradecimiento a Rubén Silva y Rubén Reyna por su invaluable apoyo durante la realización de esta práctica. Nos ayudaron a comprender mejor algunos aspectos teóricos cruciales para la implementación del servidor VPN y también nos proporcionaron parte del material necesario para llevar a cabo la práctica de manera exitosa. Su colaboración fue fundamental para el desarrollo de este proyecto, y les agradecemos sinceramente por su tiempo y esfuerzo.

7. Referencias

- [1] DigitalOcean Community, "How To Set Up an IKEv2 VPN Server with StrongSwan on Ubuntu 20.04," *DigitalOcean*, 2020. [Enlace]. Disponible en: <https://www.digitalocean.com/community/tutorials/how-to-set-up-an-ikev2-vpn-server-with-strongswan-on-ubuntu-20-04-es>. [Accedido: 02-Dic-2024].