Guía de Laboratorio

GL-5

Configuración de Routers Cisco Packet Tracer
VPN *Site-to-Site* (IPsec)

Elaborado por:

Santiago Aguilar Cárdenas

Facultad de Ingeniería Electrónica

Universidad Santo Tomás

Seccional Tunja

Información Académica

Guía de Laboratorio

GL-5

Elaborado por:

Santiago Aguilar Cárdenas

Director del Trabajo de Grado:
Ph.D. William Fabián Chaparro Becerra

Codirectores del Trabajo de Grado:
M.Sc. Angélica María Salazar Madrigal
M.Sc. Cristian David Parra Camacho

Facultad de Ingeniería Electrónica
Universidad Santo Tomás
Seccional Tunja

Información del Documento

Ficha técnica

Guía:	GL-5 – VPN *Site-to-Site* (IPsec).
Modalidad:	Simulación.
Duración sugerida:	2 a 3 horas (según el nivel del grupo).
Público objetivo:	Estudiantes de pregrado.
Requisitos:	Direccionamiento IP básico, rutas entre redes y pruebas `ping`.
Producto esperado:	Túnel IPsec activo, tráfico *interesante* cifrado, y evidencia con `show crypto isakmp sa` y `show crypto ipsec sa`.

Facultad de Ingeniería Electrónica
Universidad Santo Tomás
Seccional Tunja

PREÁMBULO

Propósito

Esta guía conduce, de forma **paso a paso y verificable**, la configuración de una **VPN IPsec sitio a sitio** entre dos routers **Cisco Packet Tracer**. Se configura **ISAKMP/IKEv1**, el **ACL de tráfico interesante**, el **transform-set** y el **crypto map**. Al final, el estudiante debe evidenciar que el tráfico entre las LAN viaja **cifrado**.

Criterios de trabajo

- Mantenga coherencia entre redes LAN, la IP del **peer** y el ACL de **tráfico interesante**.
- Guarde evidencias: `show run | sec crypto`, `show crypto isakmp sa` y `show crypto ipsec sa`.

Competencias

- Configura y valida un túnel **VPN IPsec sitio a sitio** en routers Cisco.
- Aplica criterios de seguridad para proteger tráfico entre redes LAN remotas.
- Interpreta salidas de diagnóstico para verificar el estado de IKE e IPsec.

Objetivos

1. Activar el nivel de licencia requerido para funciones avanzadas (*network-advantage*).
2. Definir parámetros de **ISAKMP/IKEv1** (política, cifrado, hash, autenticación, grupo DH y lifetime).
3. Configurar **clave precompartida (PSK)** y el **ACL de tráfico interesante**.
4. Crear **transform-set** y **crypto map** (peer, transform-set y match ACL).
5. Aplicar el **crypto map** en la interfaz WAN y verificar el establecimiento del túnel.
6. Ejecutar pruebas de conectividad y evidenciar contadores de cifrado/descifrado en `show crypto ipsec sa`.

Resultados esperados

- Túnel IPsec levantado y estable entre ambos routers.
- Conectividad verificada entre las dos LAN mediante pruebas de `ping`.
- Evidencias de cifrado/descifrado observadas en `show crypto ipsec sa`.
- Registro técnico de configuración y validación listo para entrega.

Índice general

Índice de figuras

1

Unidad 1: Escenario y topología de la práctica

1.1 Escenario

Dos sedes de una organización requieren intercambiar información entre sus redes internas (LAN) a través de un enlace WAN no confiable. Para proteger la confidencialidad e integridad del tráfico, se implementará una **VPN IPsec sitio a sitio** entre dos routers **Cisco ISR1100X-4G**.

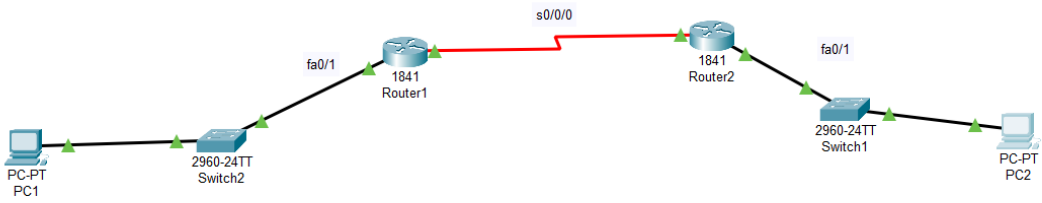

Figura 1.1: Topología red Routers ISR 1100X-4G.

Reto

Configurar una VPN IPsec (IKEv1/ISAKMP) que cifre el **tráfico interesante** entre la LAN-A y la LAN-B, verificando que el túnel quede **ACTIVE** y que aumenten los contadores de paquetes cifrados/descifrados.

1.2 Topología de referencia

La práctica se realiza con dos routers (R1 y R2), cada uno conectado a su respectiva LAN y a un enlace WAN entre routers.

- **LAN-A**: red interna detrás de R1 (ejemplo: `192.168.13.0/25`).
- **LAN-B**: red interna detrás de R2 (ejemplo: `192.168.14.0/26`).
- **Enlace WAN**: red de tránsito entre R1–R2 (direcciones del ejemplo: `192.168.14.97` y `192.168.14.98`).

2

Unidad 2: Parámetros ISAKMP e identificación del tráfico (ACL)

2.1 Crear la política ISAKMP (IKEv1)

En **R1 y R2** configure una política ISAKMP. El ejemplo usa `policy 10`, cifrado `aes`, hash `sha`, autenticación `pre-share`, `group 1` y `lifetime 86400`.

```
conf t
 crypto isakmp policy 10
  encr aes
  hash sha
  authentication pre-share
  group 1
  lifetime 86400
 exit
end
```

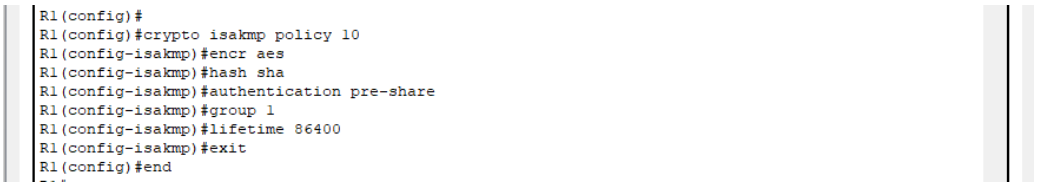

Figura 2.1: Evidencia de configuración ISAKMP en Router 1

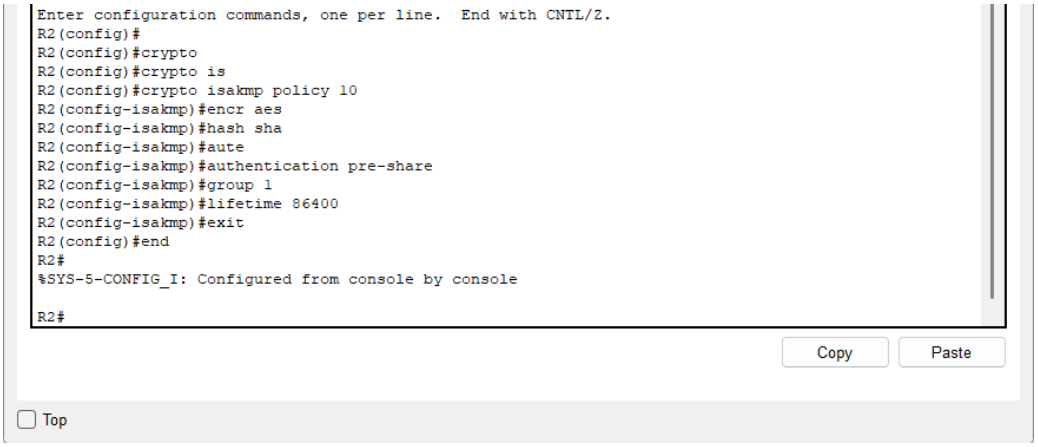

Figura 2.2: Evidencia de configuración ISAKMP en Router 2

Nota Importante

Tome capturas de pantalla de la configuración en **Router 1** y **Router 2**, incluyendo los comandos ejecutados y su salida, como evidencia para el informe final.

Nota Importante

Los parámetros deben ser **idénticos en ambos extremos** o la negociación IKE fallará.

2.2 Configurar la clave precompartida (PSK)

Defina una clave y amárrela a la IP del **peer** (extremo remoto). Ejemplo:

```
Router 1
conf t
 crypto isakmp key cisco123 address 192.168.14.98
end

Router 2
conf t
 crypto isakmp key cisco123 address 192.168.14.97
end
```

2.3 ACL de tráfico interesante

El **ACL** define qué tráfico debe cifrarse. En el ejemplo se usa el ACL `100` permitiendo `ip` entre las LAN:

```
Router 1
conf t
 access-list 100 permit ip 192.168.13.0 0.0.0.127 192.168.14.0 0.0.0.63
end

Router 2
conf t
 access-list 100 permit ip 192.168.14.0 0.0.0.63 192.168.13.0 0.0.0.127
end
```

3

Unidad 3: Transform-set y Crypto Map

3.1 Crear el transform-set

El transform-set define cómo se protegerán los paquetes en IPsec (Fase 2). En el ejemplo se usa `esp-aes` y `esp-sha-hmac`

```
conf t
 crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
end
```

3.2 Crear el crypto map

Cree el mapa, asigne el peer, el transform-set y el ACL de tráfico interesante:

En R1 (peer = R2):

```
conf t
 crypto map VPN-MAP 10 ipsec-isakmp
  set peer 192.168.14.198
  set transform-set VPN-SET
  match address 100
end
```

En R2 (peer = R1):

```
conf t
 crypto map VPN-MAP 10 ipsec-isakmp
  set peer 192.168.14.197
  set transform-set VPN-SET
  match address 100
end
```

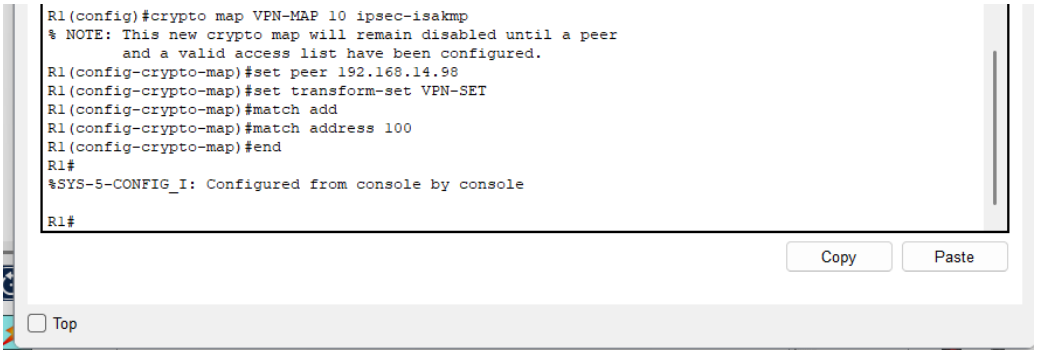

Figura 3.1: Evidencia de configuración (tra1)

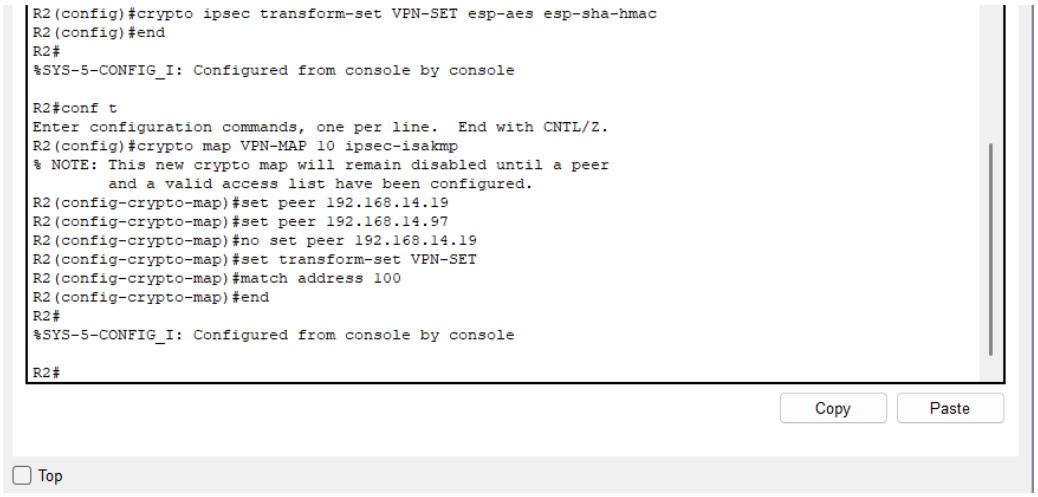

Figura 3.2: Evidencia de configuración (tra2)

4

Unidad 4: Aplicación del crypto map y verificación inicial

4.1 Aplicar el crypto map a la interfaz WAN

Aplique el crypto map en la interfaz que conecta hacia el **peer** (interfaz WAN). En el ejemplo se usa `GigabitEthernet0/0/1`:

```
conf t
 interface GigabitEthernet0/0/1
  crypto map VPN-MAP
 exit
end
```

Al aplicarlo, el router puede mostrar un mensaje similar a:

```
%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

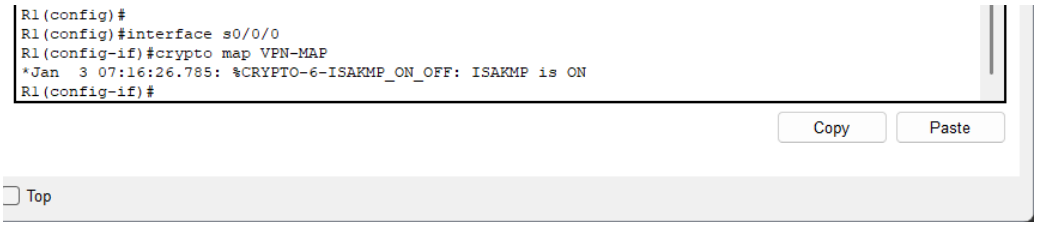

Figura 4.1: Aplicación del crypto map ON

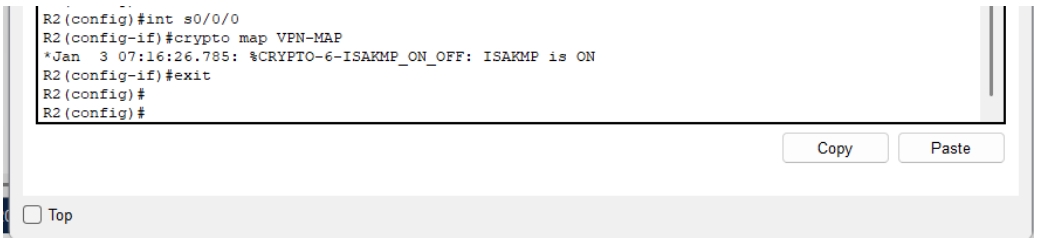

Figura 4.2: Aplicación del crypto map ON

4.2 Guardar configuración

```
write memory
```

4.3 Verificación rápida

Ejecute los siguientes comandos en ambos extremos:

```
show run | section crypto
show crypto isakmp sa
show crypto ipsec sa
```

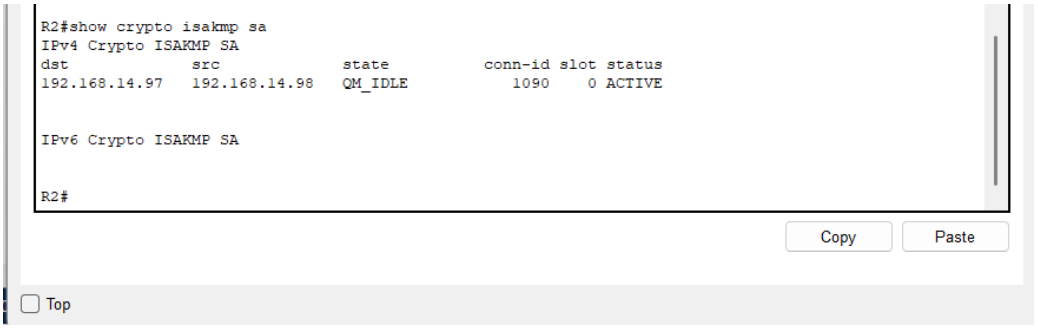

Figura 4.3: Evidencia

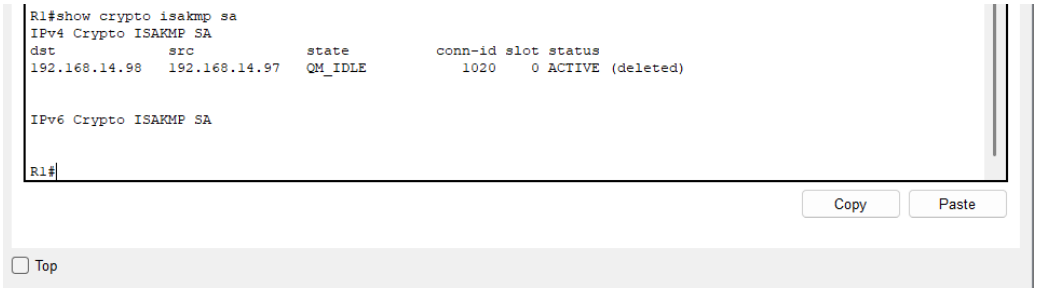

Figura 4.4: Evidencia

Nota Importante

Si aún no hay tráfico entre LAN-A y LAN-B, es posible que `show crypto isakmp sa` aparezca vacío. Genere tráfico (pings) para disparar la negociación.

5

Unidad 5: Pruebas, evidencias y diagnóstico

5.1 Generar tráfico para levantar el túnel

Desde un host en la LAN-A haga `ping` a un host en la LAN-B. Si está probando desde el router, puede forzar el origen.

Ejemplo desde R1:

```
ping 192.168.14.1 source 192.168.13.1
```

Qué se espera ver

- En `show crypto isakmp sa`: estado **QM_IDLE** y **ACTIVE**.
- En `show crypto ipsec sa`: contadores de `#pkts encaps/encrypt` y `#pkts decaps/decrypt` aumentando.

5.2 Comandos de verificación

```
show crypto isakmp sa
show crypto ipsec sa
```

Un estado típico correcto (referencia):

```
IPv4 Crypto ISAKMP SA
 dst              src              state      conn-id status
192.168.14.198   192.168.14.197   QM_IDLE      1001    ACTIVE
```

5.3 Diagnóstico de fallas comunes

1. **No aparece ningún SA:**
   - Verifique conectividad al peer (`ping <peer>`).
   - Confirme que la política ISAKMP coincide en ambos extremos.
   - Revise la PSK y la IP asociada con `crypto isakmp key ... address ....`
2. **SA IKE activa pero sin contadores IPsec:**

- El ACL de tráfico interesante no coincide con el tráfico real.
- No hay rutas entre LAN-A y LAN-B (ver `show ip route`).
- El crypto map está aplicado a la interfaz incorrecta.

3. **% Invalid source address**:
   - Está usando como `source` una IP que no pertenece a ninguna interfaz **UP** del router. Use una IP configurada y activa.

6

Unidad 6: Actividades de entrega

6.1 Checklist de evidencias

1. Captura/registro de la activación de licencia y reinicio (comandos `license boot level network-advantage` y `reload`).
2. Salida de `show run | section crypto` en R1 y R2.
3. Salida de `show crypto isakmp sa` mostrando **ACTIVE**.
4. Salida de `show crypto ipsec sa` mostrando contadores (encaps/decaps) distintos de cero.
5. Pruebas de conectividad entre un host de LAN-A y un host de LAN-B (pings o tráfico real).

6.2 Preguntas de análisis

Responda de forma breve:

1. ¿Qué función cumple el **ACL de tráfico interesante** en IPsec?
2. ¿Cuál es la diferencia entre **Fase 1 (ISAKMP/IKE)** y **Fase 2 (IPsec)**?