
Guía de Laboratorio

GL-6

Configuración de Routers Cisco VPN *Site-to-Site* (IPsec) en *ISR1100X-4G*

ISAKMP/IKEv1, transform-set, crypto map y verificación

Elaborado por:
Santiago Aguilar Cárdenas
(Adaptado para prácticas de laboratorio)

Facultad de Ingeniería Electrónica
Universidad Santo Tomás
Seccional Tunja

Información Académica

Guía de Laboratorio GL-6

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-6 – VPN <i>Site-to-Site</i> (IPsec) en routers Cisco ISR1100X-4G.
Modalidad:	Laboratorio físico (equipos reales).
Duración sugerida:	2 a 3 horas (según el nivel del grupo).
Público objetivo:	Estudiantes de pregrado.
Requisitos:	Consola/SSH a routers, direccionamiento IP básico, rutas entre redes y pruebas ping .
Producto esperado:	Túnel IPsec activo, tráfico <i>interesante</i> cifrado, y evidencia con show crypto isakmp sa y show crypto ipsec sa .

PREÁMBULO

Propósito

Esta guía conduce, de forma **paso a paso y verificable**, la habilitación previa de **licenciamiento** y la configuración de una **VPN IPsec sitio a sitio** entre dos routers **Cisco ISR1100X-4G**. 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**.

Nota Importante

Importante (antes de iniciar): en estos equipos se requiere activar el nivel de licencia para habilitar características avanzadas. Ejecute en el router (modo privilegiado):

```
configure terminal
license boot level network-advantage
end
write memory
reload
```

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`.
- Si el túnel no levanta, verifique **rutas**, **NAT** (si aplica), **PSK**, ACL y que el crypto map esté aplicado a la interfaz correcta.

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

1. Unidad 1: Escenario y topología de la práctica	5
1.1. Escenario	5
1.2. Topología de referencia	5
2. Unidad 2: Preparación del router y licenciamiento	7
2.1. Ingreso al equipo y modo privilegiado	7
2.2. Activación de licencia (requisito previo)	7
3. Unidad 3: Parámetros ISAKMP e identificación del tráfico (ACL)	8
3.1. Crear la política ISAKMP (IKEv1)	8
3.2. Configurar la clave precompartida (PSK)	8
3.3. ACL de tráfico interesante	9
4. Unidad 4: Transform-set y Crypto Map	10
4.1. Crear el transform-set	10
4.2. Crear el crypto map	10
5. Unidad 5: Aplicación del crypto map y verificación inicial	11
5.1. Aplicar el crypto map a la interfaz WAN	11
5.2. Guardar configuración	11
5.3. Verificación rápida	11
6. Unidad 6: Pruebas, evidencias y diagnóstico	12
6.1. Generar tráfico para levantar el túnel	12
6.2. Comandos de verificación	12
6.3. Diagnóstico de fallas comunes	12
7. Unidad 7: Actividades de entrega	14
7.1. Checklist de evidencias	14
7.2. Preguntas de análisis	14

Índice de figuras

1.1. Topología red Routers ISR 1100X-4G.	5
--	---

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**.

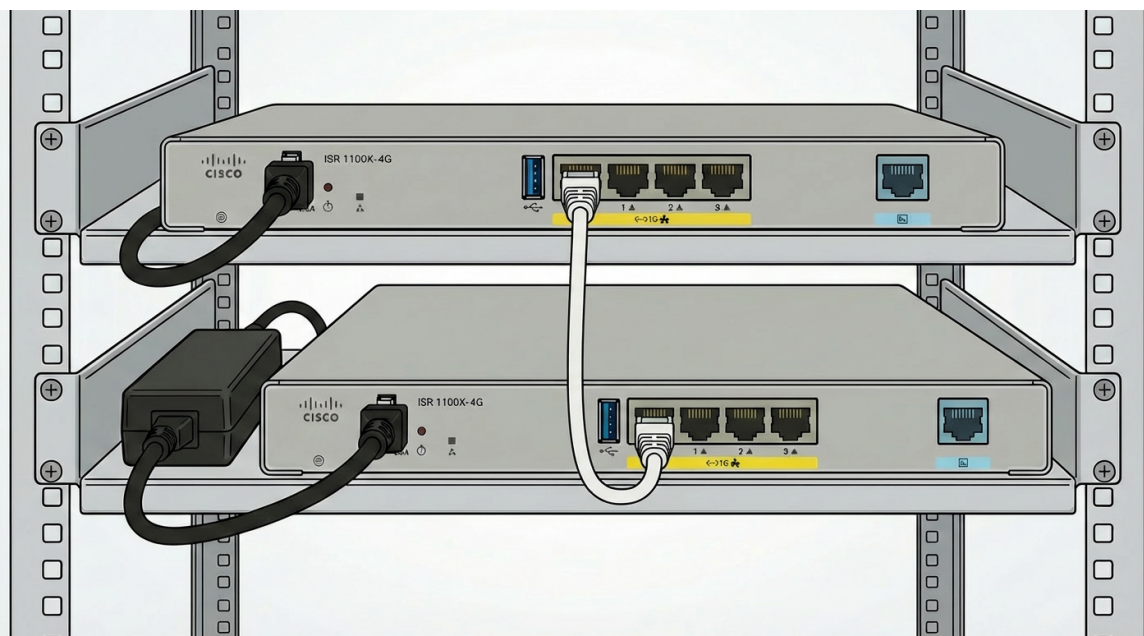


Figura 1.1: Topología red Routers ISR 1100X-4G.

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).

Nota Importante

Use los direccionamientos reales asignados por el docente. En esta guía se incluyen IPs del ejemplo capturado en consola para mostrar comandos y verificación.

Unidad 2: Preparación del router y licenciamiento

2.1 Ingreso al equipo y modo privilegiado

Conéctese por **consola** o **SSH** al router y acceda a modo privilegiado:

```
Router> enable  
Router#
```

2.2 Activación de licencia (requisito previo)

Antes de configurar la VPN, habilite el nivel de licencia requerido. Ejecute exactamente la siguiente secuencia en **cada router**:

```
conf t  
license boot level network-advantage  
end  
write memory  
reload
```

Notas

- Tras el **reload**, vuelva a conectarse y confirme que el equipo cargó correctamente.

Unidad 3: Parámetros ISAKMP e identificación del tráfico (ACL)

3.1 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 14` y `lifetime 86400`.

```
conf t
crypto isakmp policy 10
  encr aes
  hash sha
  authentication pre-share
  group 14
  lifetime 86400
exit
end
```

Nota Importante

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

3.2 Configurar la clave precompartida (PSK)

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

```
En R1
conf t
  crypto isakmp key cisco123 address 192.168.14.98
end

En R2
conf t
  crypto isakmp key cisco123 address 192.168.14.97
end
```

3.3 ACL de tráfico interesante

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

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

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

Unidad 4: Transform-set y Crypto Map

4.1 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 en modo tunnel:

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

4.2 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 192.168.14.98
  set transform-set VPN-SET
  match address 100
end
```

En R2 (peer = R1):

```
conf t
  crypto map VPN-MAP 10 ipsec-isakmp
  set peer 192.168.14.97
  set transform-set VPN-SET
  match address 100
end
```

Unidad 5: Aplicación del crypto map y verificación inicial

5.1 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
```

5.2 Guardar configuración

```
write memory
```

5.3 Verificación rápida

Ejecute los siguientes comandos en ambos extremos:

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

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.

Unidad 6: Pruebas, evidencias y diagnóstico

6.1 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.

6.2 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	192.168.14.97	QM_IDLE	1001	ACTIVE

6.3 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.

Unidad 7: Actividades de entrega

7.1 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).

7.2 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)**?
3. Si el túnel está **ACTIVE** pero no hay conectividad, ¿qué tres verificaciones haría primero?