

**Actividad 06**

Beltrán Reyna David – 183636

Universidad Politécnica de San Luis Potosí | Ingeniería en Tecnologías de la Información

Curso del Núcleo Optativo V: Seguridad Informática

Mtro. Servando López Contreras

6to. Semestre

Grupo: T46A

a 15 de febrero de 2026

## Contenido

Actividad 06: Implementación del protocolo IPSec VPN .....	3
Introducción .....	3
Diseño y topología de red .....	3
Activación de licencias de seguridad.....	4
R1 .....	4
R3 .....	5
Configuraciones Iniciales de enrutamiento.....	5
R1 .....	6
R3 .....	7
ISP .....	8
Asignación de nombres clave .....	8
R1 .....	8
R3 .....	9
ISP .....	9
Configuración de Fase 1 (ISAKMP) y Fase 2 (IPSec y Transform Set) .....	10
R1 .....	10
R3 .....	11
Pruebas de Conectividad y Verificación .....	12
Ping.....	12
Comandos.....	13
Conclusiones .....	13

Referencias.....	15
------------------	----

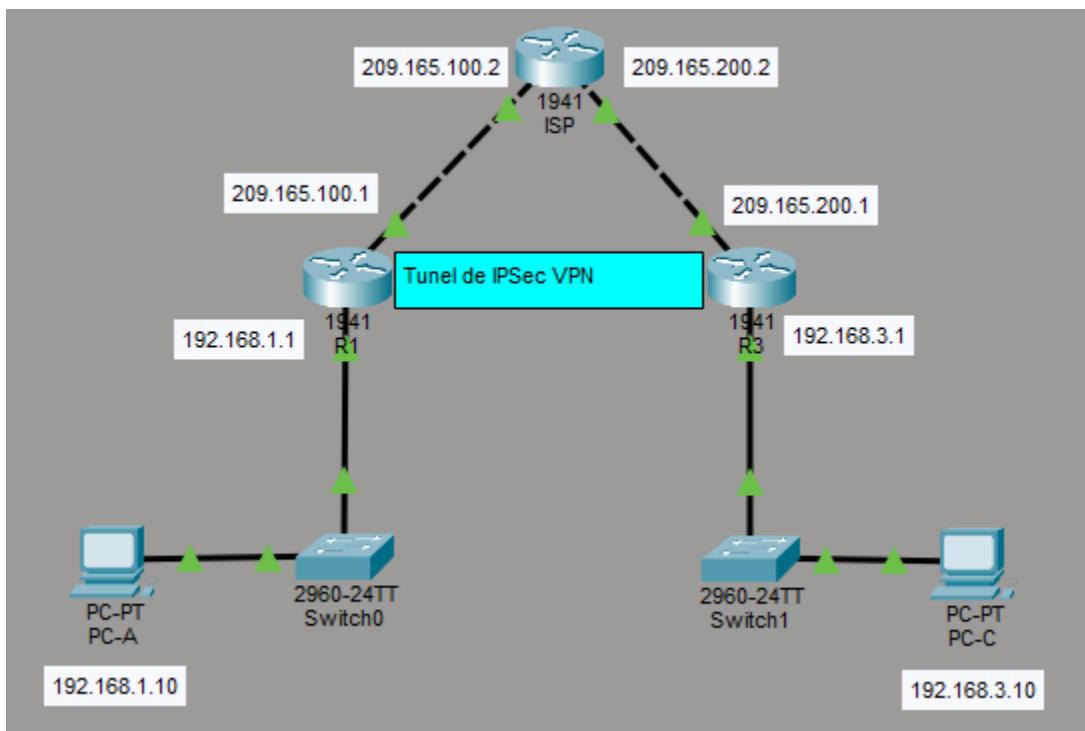
## Actividad 06: Implementación del protocolo IPSec VPN

### Introducción

Esta actividad documenta la creación de una **VPN IPSec Site-to-Site** en Packet Tracer utilizando routers Cisco 1941 con licencias **Security K9**. El objetivo principal es establecer un túnel cifrado que garantice la **confidencialidad e integridad** de los datos entre dos sedes remotas conectadas a través de un ISP. Para ello, se configuran políticas **ISAKMP** de Fase 1 y conjuntos de transformación de Fase 2 para proteger el tráfico "interesante" de la red.

### Diseño y topología de red

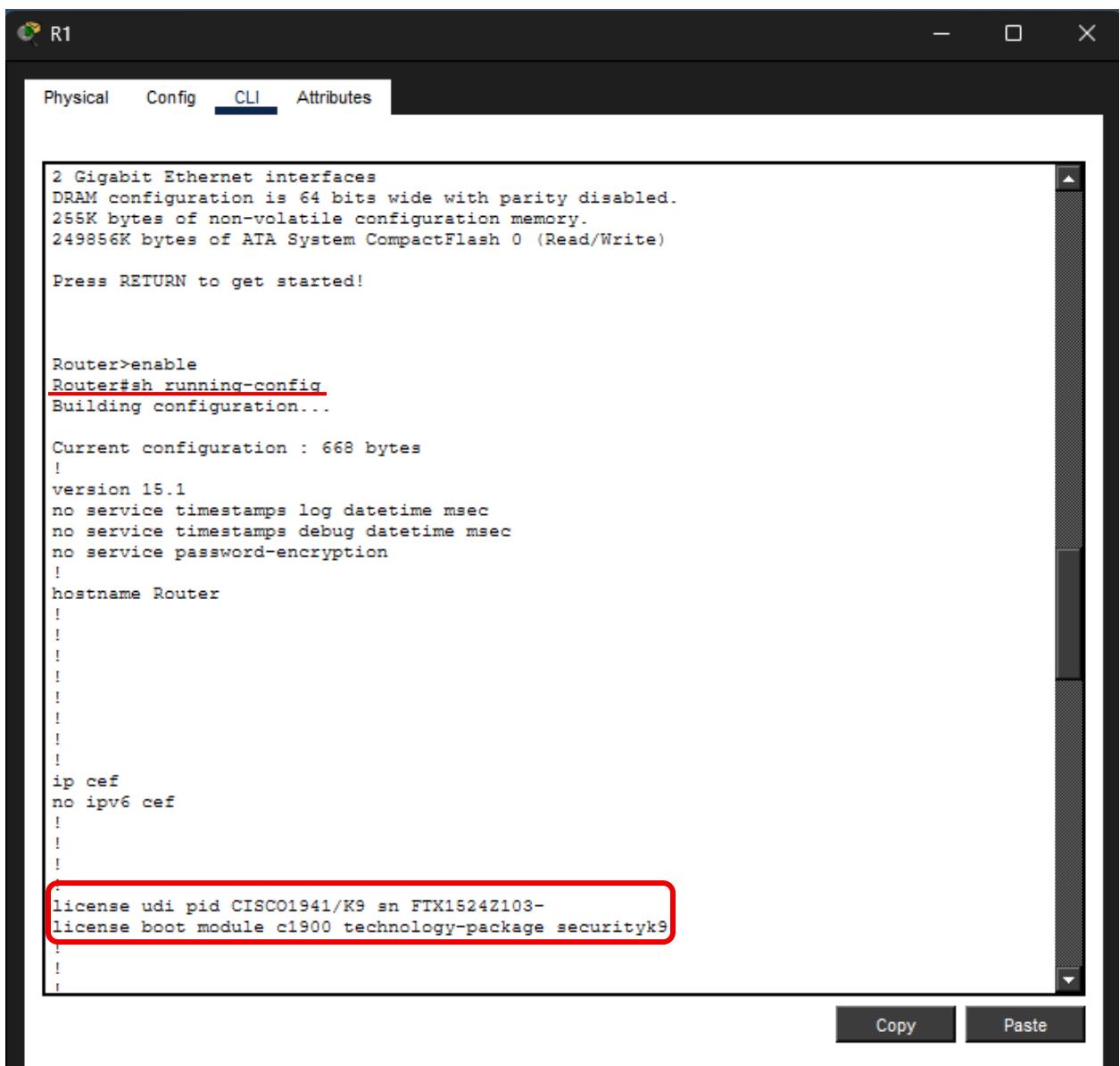
La topología utilizada incluye tres routers Cisco 1941 (R1, R3 e ISP), dos switches 2960 y dos terminales finales (PC).



## Activación de licencias de seguridad

Antes de iniciar con la VPN, es obligatorio habilitar el paquete de seguridad en los routers de la serie 1900, ya que sin la licencia "Security K9" los comandos de criptografía no estarán disponibles. Para ello, debemos utilizar los comandos de *license boot module c1900 technology-package securityk9* y *reload* (reinicio) del dispositivo para cargar el paquete tecnológico.

**R1**



```
2 Gigabit Ethernet interfaces
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

Press RETURN to get started!

Router>enable
Router#sh running-config
Building configuration...

Current configuration : 668 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
!
license udi pid CISCO1941/K9 sn FTX1524Z103-
license boot module c1900 technology-package securityk9
```

R3

```

2 Gigabit Ethernet interfaces
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

Press RETURN to get started!

Router>enable
Router#sh running-config
Building configuration...

Current configuration : 668 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
!
license udi pid CISCO1941/K9 sn FTX15249LWG-
license boot module c1900 technology-package securityk9
!
!
```

**Copy**    **Paste**

## Configuraciones Iniciales de enrutamiento

Antes de establecer el túnel, la red debe tener conectividad básica a través del ISP.

- **Interfaces:** Configuración de IPs en las interfaces GigabitEthernet y encendido de las mismas.
- **Rutas por Defecto:** Configuración de rutas estáticas hacia el ISP para simular la salida a internet (ip route 0.0.0.0 0.0.0.0 [IP]).

**R1**

The screenshot shows a window titled 'R1' with a tab bar at the top containing 'Physical', 'Config', 'CLI' (which is selected), and 'Attributes'. The main area displays a command-line interface history. The configuration commands entered by the user are highlighted with red boxes:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface gigabitEthernet 0/0
Router(config-if)#ip address 209.165.100.1 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

Router(config-if)#exit
Router(config)#interface gigabitEthernet 0/1
Router(config-if)#ip address 192.168.1.10 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

Router(config-if)#exit
Router(config)#ip route 0.0.0.0 0.0.0.0 209.165.100.2
Router(config)#exit

Router#
%SYS-5-CONFIG_I: Configured from console by console
```

At the bottom right of the window are 'Copy' and 'Paste' buttons.

**R3**

The screenshot shows a window titled 'R3' with a tab bar at the top: Physical, Config, **CLI**, and Attributes. The CLI tab is selected, displaying a command-line interface session. The session starts with 'Router>enable' and proceeds through configuration commands for Gigabit Ethernet interfaces. Two sections of the session are highlighted with red boxes:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface gigabitEthernet 0/0
Router(config-if)#ip address 209.165.200.1 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

Router(config-if)#exit
Router(config)#interface gigabitEthernet 0/1 192.168.3.1 255.255.255.0
^
% Invalid input detected at '^' marker.

Router(config)#interface gigabitEthernet 0/1 192.168.3.1
^
% Invalid input detected at '^' marker.

Router(config)#interface gigabitEthernet 0/1 192.168.3.10
^
% Invalid input detected at '^' marker.

Router(config)#interface gigabitEthernet 0/1
Router(config-if)#ip address 192.168.3.10 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

Router(config-if)#do wr
Building configuration...
[OK]
Router(config-if)#ip route 0.0.0.0 0.0.0.0 209.165.200.2
Router(config)#do wr
Building configuration...
[OK]
```

At the bottom right of the CLI window are two buttons: 'Copy' and 'Paste'.

**ISP**

```

--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: no

Press RETURN to get started!

Press RETURN to get started!

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface gigabitEthernet 0/1
Router(config-if)#ip address 209.165.200.2 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

Router(config-if)#exit
Router(config)#interface gigabitEthernet 0/0
Router(config-if)#ip address 209.165.100.2 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

Router(config-if)#exit
Router(config)#do wr
Building configuration...
[OK]
Router(config)#

```

**Copy**    **Paste**

**Asignación de nombres clave****R1**

```

Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#

```

**R3**

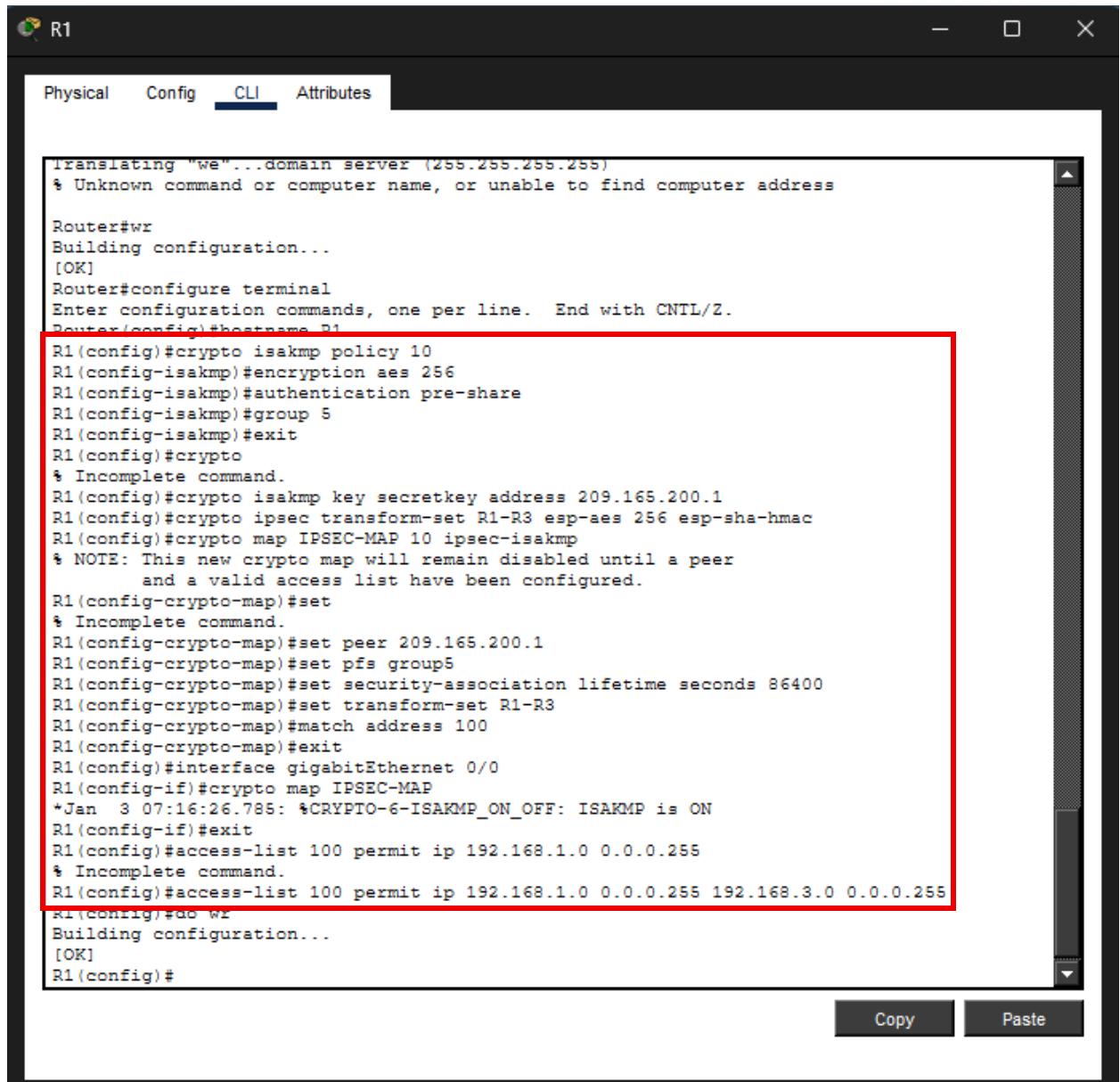
```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R3
R3(config)#+
```

**ISP**

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname ISP
ISP(config)#+
```

## Configuración de Fase 1 (ISAKMP) y Fase 2 (IPSec y Transform Set)

R1



The screenshot shows a Windows command-line interface window titled 'R1' with a black background. The title bar has tabs for 'Physical', 'Config', 'CLI' (which is selected), and 'Attributes'. The main area contains a redacted configuration command, followed by a large block of configuration text. The text starts with 'Router#wr' and ends with 'R1(config)#do wr'. The configuration includes setting an ISAKMP policy (policy 10), defining an encryption type (aes 256), specifying authentication (pre-share), creating a group (group 5), and exiting the ISAKMP configuration mode. It then moves to a crypto map configuration (IPSEC-MAP 10) with a peer IP of 209.165.200.1, setting security associations for 86400 seconds, and defining a transform set (R1-R3). It also creates an access list (100) permitting traffic from 192.168.1.0/255.255.255.255 to 192.168.3.0/255.255.255.255. Finally, it exits the interface configuration mode. The configuration text is highlighted with a red rectangle.

```
Router#wr
Building configuration...
[OK]
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#encryption aes 256
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 5
R1(config-isakmp)#exit
R1(config)#crypto
% Incomplete command.
R1(config)#crypto isakmp key secretkey address 209.165.200.1
R1(config)#crypto ipsec transform-set R1-R3 esp-aes 256 esp-sha-hmac
R1(config)#crypto map IPSEC-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
R1(config-crypto-map)#set
% Incomplete command.
R1(config-crypto-map)#set peer 209.165.200.1
R1(config-crypto-map)#set pfs group5
R1(config-crypto-map)#set security-association lifetime seconds 86400
R1(config-crypto-map)#set transform-set R1-R3
R1(config-crypto-map)#match address 100
R1(config-crypto-map)#exit
R1(config)#interface gigabitEthernet 0/0
R1(config-if)#crypto map IPSEC-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config-if)#exit
R1(config)#access-list 100 permit ip 192.168.1.0 0.0.0.255
% Incomplete command.
R1(config)#access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
R1(config)#do wr
Building configuration...
[OK]
R1(config)#
```

Copy      Paste

**R3**

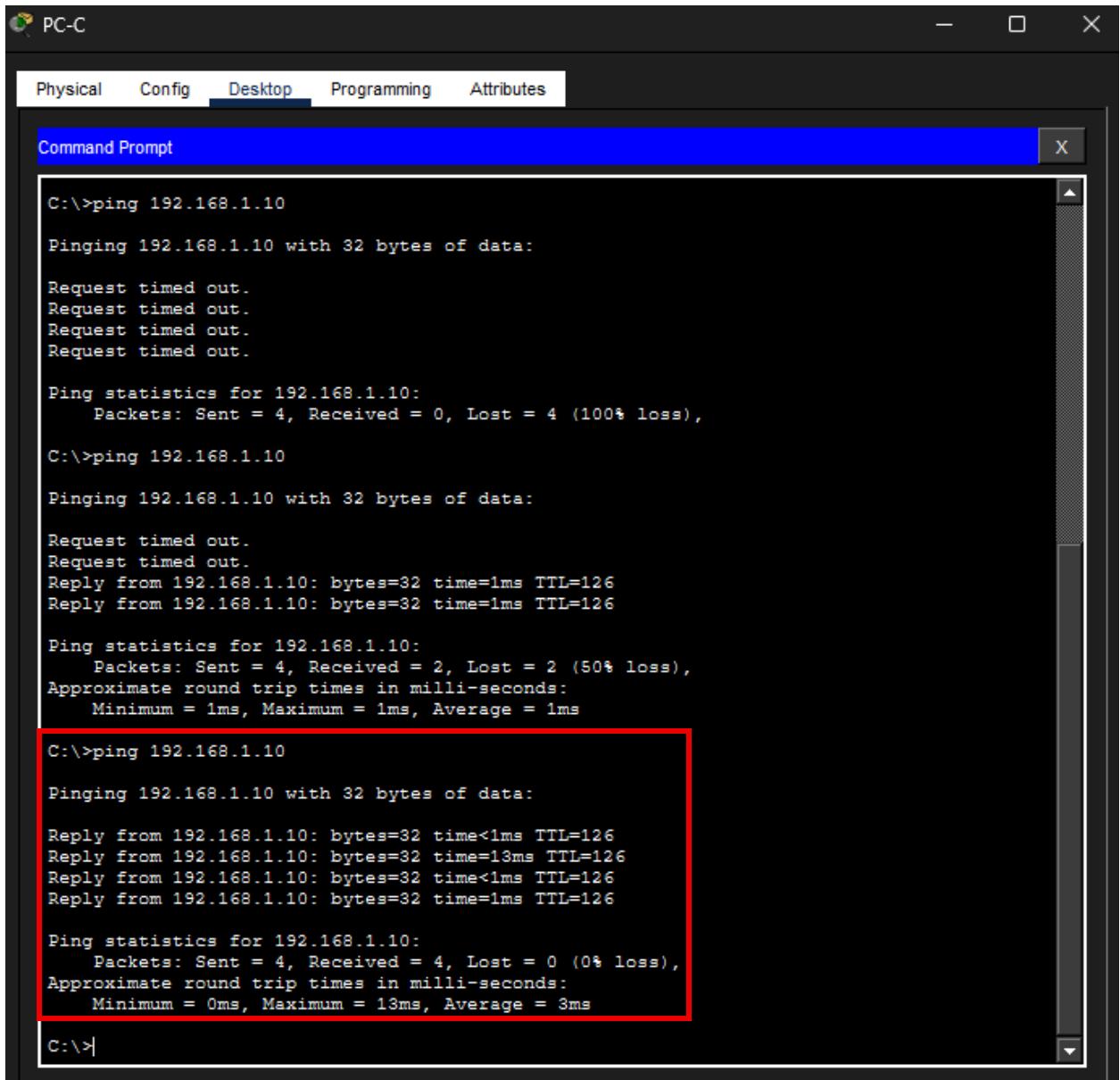
```
R3>enable
R3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#crypto isakmp policy 10
R3(config-isakmp)#encryption aes 256
R3(config-isakmp)#authentication pre-share
R3(config-isakmp)#group 5
R3(config-isakmp)#exit
R3(config)#crypto isakmp key secretkey address 209.165.100.1
R3(config)#crypto ipsec transform-set R3-R1 esp-aes 256 esp-sha-hmac
          ^
% Invalid input detected at '^' marker.

R3(config)#crypto ipsec transform-set R3-R1 esp-aes 256 esp-sha-hmac
R3(config)#crypto map IPSEC-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
      and a valid access list have been configured.
R3(config-crypto-map)#set peer 209.165.100.1
R3(config-crypto-map)#set pfs group5
R3(config-crypto-map)#set security-association lifetime seconds 86400
R3(config-crypto-map)#set transform-set R3-R1
R3(config-crypto-map)#match address 100
R3(config-crypto-map)#exit
R3(config)#interface gigabitEthernet 0/0
R3(config-if)#crypto map IPSEC-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R3(config-if)#access-list 100 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
R3(config)#do wr
Building configuration...
[OK]
R3(config)#[
```

Copy      Paste

## Pruebas de Conectividad y Verificación

### Ping



```
PC-C

Physical Config Desktop Programming Attributes

Command Prompt X

C:\>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.10:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 192.168.1.10: bytes=32 time=1ms TTL=126
Reply from 192.168.1.10: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.10:
  Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
Approximate round trip times in milli-seconds:
  Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Reply from 192.168.1.10: bytes=32 time<1ms TTL=126
Reply from 192.168.1.10: bytes=32 time=13ms TTL=126
Reply from 192.168.1.10: bytes=32 time<1ms TTL=126
Reply from 192.168.1.10: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.10:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 13ms, Average = 3ms

C:\>
```

## Comandos

- Verificación de la comunicación exitosa entre las computadoras de ambos extremos

```
R1#show crypto ISAKMP SA
IPv4 Crypto ISAKMP SA
dst          src          state      conn-id slot status
209.165.200.1 209.165.100.1 QM_IDLE           1061   0 ACTIVE

IPv6 Crypto ISAKMP SA
```

- show crypto isakmp sa: Para verificar que la Fase 1 está en estado "QM\_IDLE"

```
R1#show crypto ipsec sa
interface: GigabitEthernet0/0
  Crypto map tag: IPSEC-MAP, local addr 209.165.100.1

  protected vrf: (none)
  local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
  current_peer 209.165.200.1 port 500
    PERMIT, flags={origin is acl,}
  #pkts encaps: 6, #pkts encrypt: 6, #pkts digest: 0
  #pkts decaps: 7, #pkts decrypt: 7, #pkts verify: 0
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 0, #recv errors 0

  local crypto endpt.: 209.165.100.1, remote crypto endpt.:209.165.200.1
  path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
  current outbound spi: 0xC5B3901E(3316879390)

  inbound esp sas:
    spi: 0x7AB0DF32(2058411826)
--More--
```

## Conclusiones

La implementación fue exitosa, validada por el estado **QM\_IDLE** en la fase de gestión de claves y el cifrado activo de paquetes confirmado mediante el comando *show crypto ipsec sa*. Las pruebas de conectividad demostraron que el túnel encapsula y protege el tráfico de extremo a extremo de manera efectiva. Este ejercicio refuerza la importancia de los protocolos de seguridad para mitigar riesgos de interceptación en infraestructuras de red corporativas.



## Referencias

**Telecom Tips.** (2025, 29 mayo). *Cómo configurar VPN IPsec Site-to-Site en Packet Tracer | Guía Paso a Paso*. YouTube. <http://www.youtube.com/watch?v=RZ4RreDjhk>