



Universidad Politécnica de San Luis Potosí

Ingeniería en Tecnologías de la Información

Actividad 06

Implementación IPSec VPN

Alumno:

Erik De La Rosa Rodríguez

Matrícula: 177700

Asignatura:

CNG V: Seguridad Informática

Docente:

Mtro. Servando López Contreras

San Luis Potosí, S.L.P.
16 de febrero de 2026

Introducción

En esta práctica se realizó la configuración de una VPN IPsec sitio a sitio entre dos redes locales, utilizando routers Cisco dentro del simulador Packet Tracer. El objetivo fue establecer un túnel seguro entre dos subredes a través de una red pública simulada (ISP).

Justificación del módulo de seguridad

Durante la configuración inicial de la VPN, los routers no aceptaban los comandos relacionados con IPsec, como:

- `crypto isakmp`
- `crypto ipsec`
- `crypto map`

Esto ocurrió porque el paquete tecnológico de seguridad (**securityk9**) no estaba habilitado en los routers.

Por lo tanto, fue necesario activar el módulo de seguridad mediante el siguiente comando:

```
license boot module c1900 technology-package securityk9
```

Posteriormente se reinició el router para que la licencia se aplicara correctamente.

Sin este módulo activo, el router no puede ejecutar funciones criptográficas ni establecer túneles VPN, ya que dichas capacidades forman parte del paquete de seguridad del sistema operativo Cisco IOS.

Topología de red

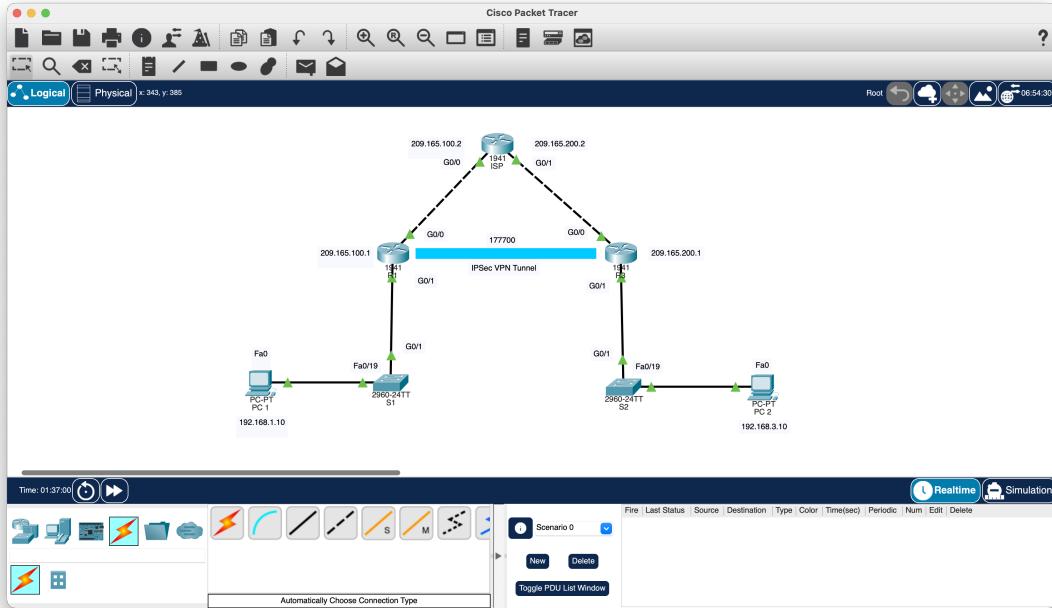


Figura 1: Topología general de la práctica

Esquema de direccionamiento

- Red LAN izquierda: 192.168.1.0/24
- Red LAN derecha: 192.168.3.0/24
- Enlace R1–ISP: 209.165.100.0/30
- Enlace R3–ISP: 209.165.200.0/30

Activación del módulo de seguridad

Evidencia en R1

The screenshot shows a Cisco R1 router's CLI interface. The title bar says "R1". Below it is a navigation bar with tabs: Physical, Config, **CLI**, and Attributes. The main area is titled "IOS Command Line Interface". The terminal window displays the following text:

```
R1(config)#license boot module c1900 technology-package securityk9
PLEASE READ THE FOLLOWING TERMS CAREFULLY. INSTALLING THE LICENSE OR
LICENSE KEY PROVIDED FOR ANY CISCO PRODUCT FEATURE OR USING SUCH
PRODUCT FEATURE CONSTITUTES YOUR FULL ACCEPTANCE OF THE FOLLOWING
TERMS. YOU MUST NOT PROCEED FURTHER IF YOU ARE NOT WILLING TO BE BOUND
BY ALL THE TERMS SET FORTH HEREIN.

Use of this product feature requires an additional license from Cisco,
together with an additional payment. You may use this product feature
on an evaluation basis, without payment to Cisco, for 60 days. Your use
of the product, including during the 60 day evaluation period, is
subject to the Cisco end user license agreement
http://www.cisco.com/en/US/docs/general/warranty/EUIKEN_.html
If you use the product feature beyond the 60 day evaluation period, you
must submit the appropriate payment to Cisco for the license. After the
60 day evaluation period, your use of the product feature will be
governed solely by the Cisco end user license agreement (link above),
together with any supplements relating to such product feature. The
above applies even if the evaluation license is not automatically
terminated and you do not receive any notice of the expiration of the
evaluation period. It is your responsibility to determine when the
evaluation period is complete and you are required to make payment to
Cisco for your use of the product feature beyond the evaluation period.

Your acceptance of this agreement for the software features on one
product shall be deemed your acceptance with respect to all such
software on all Cisco products you purchase which includes the same
software. (The foregoing notwithstanding, you must purchase a license
for each software feature you use past the 60 days evaluation period,
so that if you enable a software feature on 1000 devices, you must
purchase 1000 licenses for use past the 60 day evaluation period.)

Activation of the software command line interface will be evidence of
your acceptance of this agreement.

ACCEPT? [yes/no]: yes
% use 'write' command to make license boot config take effect on next boot

R1(config)#: %IOS_LICENSE_IMAGE_APPLICATION-6-LICENSE_LEVEL: Module name = C1900 Next reboot level = securityk9 and License = securityk9
end
R1#
%SYS-5-CONFIG_I: Configured from console by console
write
Building configuration...
[OK]
R1#reload
Proceed with reload? [confirm]
R1#reload
Proceed with reload? [confirm]ySystem Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB, DIMMO = 0 MB
CISCO1941/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 64/-1 (On-board/DIMMO) bit mode with ECC disabled

Readonly ROMMON initialized
program load complete, entry point: 0x80803000, size: 0x1b340
program load complete, entry point: 0x80803000, size: 0x1b340

IOS Image Load Test
Digitally Signed Release Software
```

At the bottom right of the terminal window are "Copy" and "Paste" buttons. At the bottom left is a "Top" button.

Figura 2: Activación del paquete de seguridad en R1

Evidencia en R3

The screenshot shows a Cisco IOS Command Line Interface (CLI) window titled "R3". The window has tabs at the top: Physical, Config, **CLI**, and Attributes. The main area displays the following text:

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

R3 con0 is now available

Press RETURN to get started.

R3>enable
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#license boot module cl900 technology-package securityk9
R3(config)#end
R3#
#SYS-5-CONFIG_I: Configured from console by console
write
Building configuration...
[OK]
R3#reload
Proceed with reload? [confirm]
System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO1941/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 64/-1(On-board/DIMM0) bit mode with ECC disabled
Readonly ROMMON initialized
program load complete, entry point: 0x80803000, size: 0x1b340
program load complete, entry point: 0x80803000, size: 0x1b340

IOS Image Load Test
Digitally Signed Release Software
program load complete, entry point: 0x81000000, size: 0x2bb1c58
Self decompressing the image :
#####
#
```

At the bottom right of the text area are "Copy" and "Paste" buttons. At the bottom left is a "Top" button.

Figura 3: Activación del paquete de seguridad en R3

Configuración básica de red

Configuración en R1

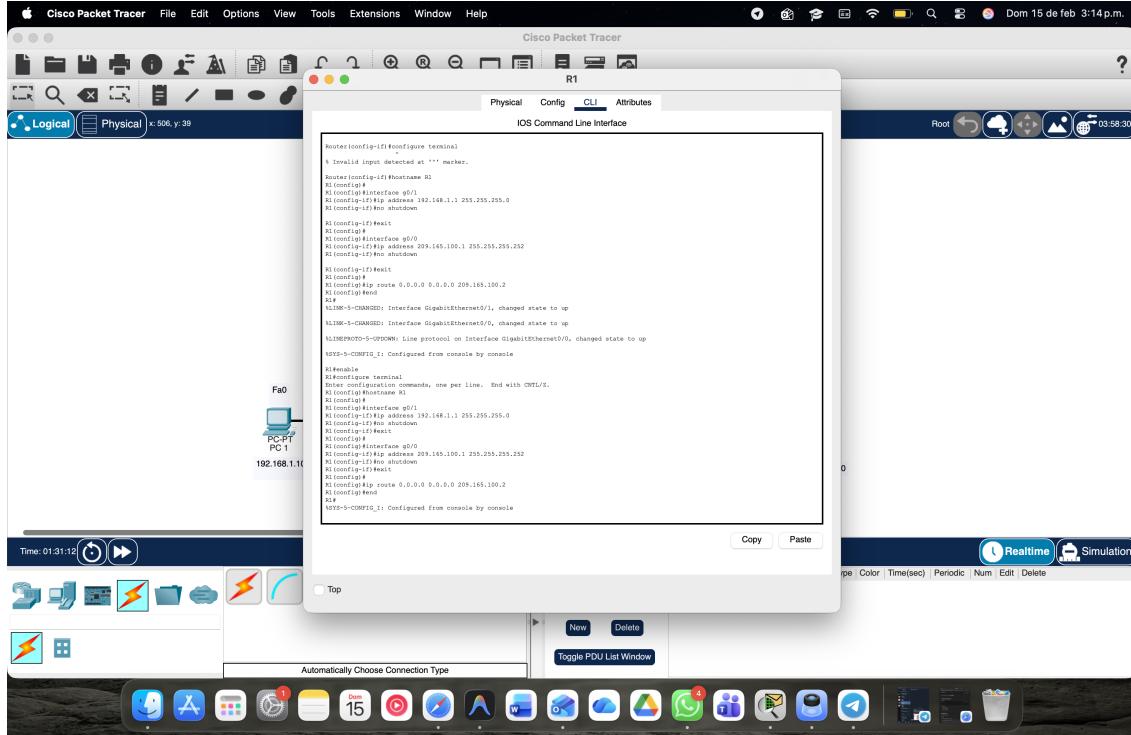


Figura 4: Configuración de red en R1

Configuración en R3

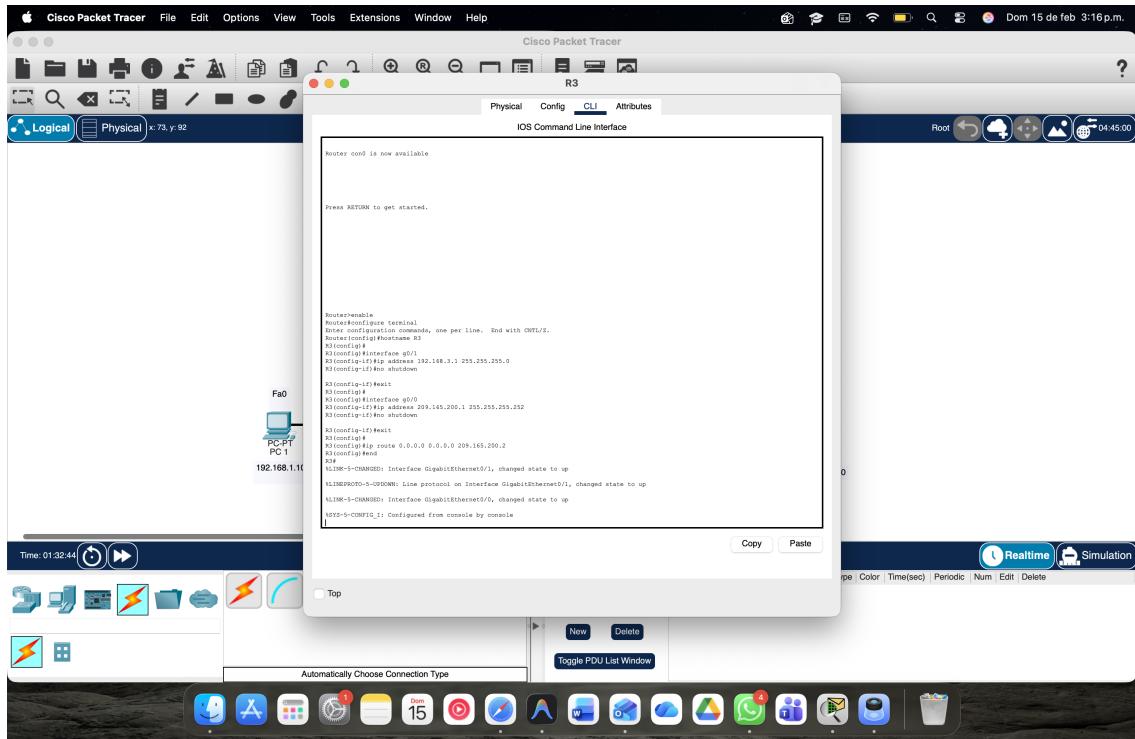


Figura 5: Configuración de red en R3

Configuración del ISP

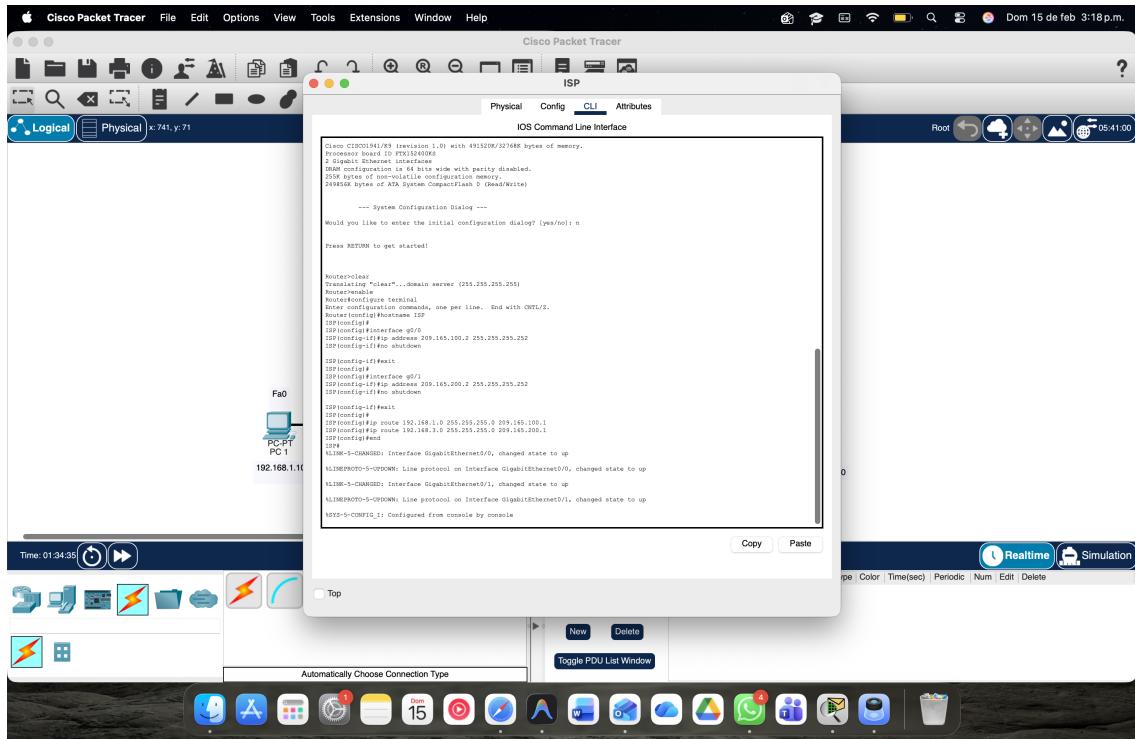


Figura 6: Configuración del router ISP

Configuración de la VPN

Configuración en R1

Figura 7: Configuración de IPsec en R1

Configuración en R3

The screenshot shows a terminal window titled "R3" with the following tabs: Physical, Config, CLI (which is selected), and Attributes. The window title is "IOS Command Line Interface". The terminal content displays the configuration commands entered on R3:

```
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on interface GigabitEthernet0/1, changed state to up
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on interface GigabitEthernet0/0, changed state to up
%SYS-5-CONFIG_I: Configured from console by console

R3#enable
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#enable
% Incomplete command.
R3(config)#conf t
% Incomplete command value
R3(config)#hostname R3
R3(config)#no ip domain-lookup
R3(config)#
R3(config)#interface g0/1
R3(config-if)# ip address 192.168.3.1 255.255.255.0
R3(config-if)# no shutdown
R3(config-if)# exit
R3(config)#
R3(config)#interface g0/0
R3(config-if)# ip address 209.165.200.1 255.255.255.252
R3(config-if)# no shutdown
R3(config-if)# exit
R3(config)#
R3(config)#ip route 0.0.0.0 0.0.0.0 209.165.200.2
R3(config)#end
R3#write
Building configuration...
[OK]
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#enable
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#crypto isakmp policy 10
R3(config-isakmp)#encryption aes
R3(config-isakmp)#hash sha
R3(config-isakmp)#authentication pre-share
R3(config-isakmp)#group 2
R3(config-isakmp)#lifetime 86400
R3(config-isakmp)#exit
R3(config)#crypto isakmp key cisco address 209.165.100.1
R3(config)#crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
R3(config)#access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
R3(config)#crypto map VPN-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
% in the access-list have been configured.
R3(config-crypto-map)#set peer 209.165.100.1
R3(config-crypto-map)#set transform-set VPN-SET
R3(config-crypto-map)#match address 110
R3(config-crypto-map)#exit
R3(config)#interface g0/0
R3(config-if)#crypto map VPN-MAP
*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R3(config-if)#exit
R3(config)#

```

At the bottom right of the terminal window are "Copy" and "Paste" buttons. At the bottom left is a "Top" button.

Figura 8: Configuración de IPsec en R3

Verificación del túnel

Estado de las asociaciones IPsec

```
R1#show crypto ipsec sa
interface: GigabitEthernet0/0
  Crypto map tag: VPN-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 encap: 14, #pkts encrypt: 14, #pkts digest: 0
  #pkts decaps: 14, #pkts decrypt: 14, #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 1, #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 jdb GigabitEthernet0/0
  current outbound spi: 0x43700271(3278951025)

  inbound esp sas:
    spi: 0xA5b166D8(2779866840)
      transform: esp-aes esp-sha-hmac ,
      in use settings ={Tunnel, }
      conn id: 2005, flow_id: FFGA:1, crypto map: VPN-MAP
      sa timing: remaining key lifetime (k/sec): (4525504/3346)
      IV size: 16 bytes
      replay detection support: N
      Status: ACTIVE

  inbound ah sas:
  inbound pcp sas:
  outbound esp sas:
    spi: 0x43700271(3278951025)
      transform: esp-aes esp-sha-hmac ,
      in use settings ={Tunnel, }
      conn id: 2006, flow_id: FFGA:1, crypto map: VPN-MAP
      sa timing: remaining key lifetime (k/sec): (4525504/3346)
      IV size: 16 bytes
      replay detection support: N
      Status: ACTIVE

  outbound ah sas:
  outbound pcp sas:

R1#show run | section crypto
crypto isakmp policy 10
  encr aes
  authentication pre-share
group 2
  crypto isakmp key cisco address 209.165.200.1
  crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
  crypto map VPN-MAP 10 ipsec-isakmp
    set peer 209.165.200.1
    set transform-set VPN-SET
    match address 110
  crypto map VPN-MAP
R1#
R1#
```

Top

Copy Paste

Figura 9: Estado de las asociaciones IPsec

Prueba de conectividad entre PCs



The screenshot shows a Cisco ASA 5505 firewall interface titled "PC 1". The top navigation bar includes tabs for Physical, Config, Desktop (which is selected), Programming, and Attributes. Below the tabs is a "Command Prompt" window with a blue header containing an "X" button. The command prompt displays several ping commands and their results:

```
Request timed out.  
Reply from 192.168.3.10: bytes=32 time<1ms TTL=125  
  
Ping statistics for 192.168.3.10:  
    Packets: Sent = 4, Received = 1, Lost = 3 (75% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 0ms, Maximum = 0ms, Average = 0ms  
  
C:\>ping 192.168.1.1ping 209.165.100.2ping 209.165.200.1ping 192.168.3.10  
Invalid Command.  
  
C:\>ping 192.168.1.1  
  
Pinging 192.168.1.1 with 32 bytes of data:  
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255  
  
Ping statistics for 192.168.1.1:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 0ms, Maximum = 0ms, Average = 0ms  
  
C:\>ping 209.165.100.2  
  
Pinging 209.165.100.2 with 32 bytes of data:  
Reply from 209.165.100.2: bytes=32 time<1ms TTL=254  
  
Ping statistics for 209.165.100.2:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 0ms, Maximum = 0ms, Average = 0ms  
  
C:\>ping 209.165.100.1  
  
Pinging 209.165.100.1 with 32 bytes of data:  
Reply from 209.165.100.1: bytes=32 time<1ms TTL=255  
  
Ping statistics for 209.165.100.1:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 0ms, Maximum = 0ms, Average = 0ms  
  
C:\>ping 192.168.3.10  
  
Pinging 192.168.3.10 with 32 bytes of data:  
Reply from 192.168.3.10: bytes=32 time<1ms TTL=125  
  
Ping statistics for 192.168.3.10:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 0ms, Maximum = 1ms, Average = 0ms  
  
C:\>
```

At the bottom left of the interface, there is a "Top" button.

Figura 10: Prueba de ping exitosa a través del túnel VPN

Conclusión

Durante la práctica se configuró exitosamente un túnel VPN IPsec entre dos redes remotas utilizando routers Cisco. Inicialmente, los comandos de seguridad no estaban disponibles debido a que el paquete **securityk9** no estaba habilitado, lo cual impedía la configuración del túnel.

Tras activar el módulo de seguridad y reiniciar los equipos, fue posible aplicar la configuración criptográfica y establecer el túnel IPsec correctamente. Las pruebas de conectividad confirmaron que el tráfico entre ambas redes viaja cifrado a través del túnel.

Esta práctica permitió comprender:

- El funcionamiento de una VPN sitio a sitio.
- La importancia de los módulos de seguridad en routers Cisco.
- El proceso de negociación ISAKMP e IPsec.