



FEBRUARY 16, 2026

# IMPLEMENTACIÓN IPSEC VPN

## ACTIVIDAD 6



BRUNO AXEL PUENTE LUNA 177876  
UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

## Contenido

Introducción .....	2
Topología propuesta .....	2
Desarrollo.....	3
Habilitar licencia de seguridad.....	8
Trafico interesante .....	11
FASE 1 – ISAKMP (negociación) .....	12
FASE 2 – Transform Set (cómo se protegerán los datos) .....	13
FASE 3 – Crypto Map .....	14
FASE 4 – Aplicar a la interfaz WAN (la que va al ISP) .....	15
Conclusión .....	17

# Introducción

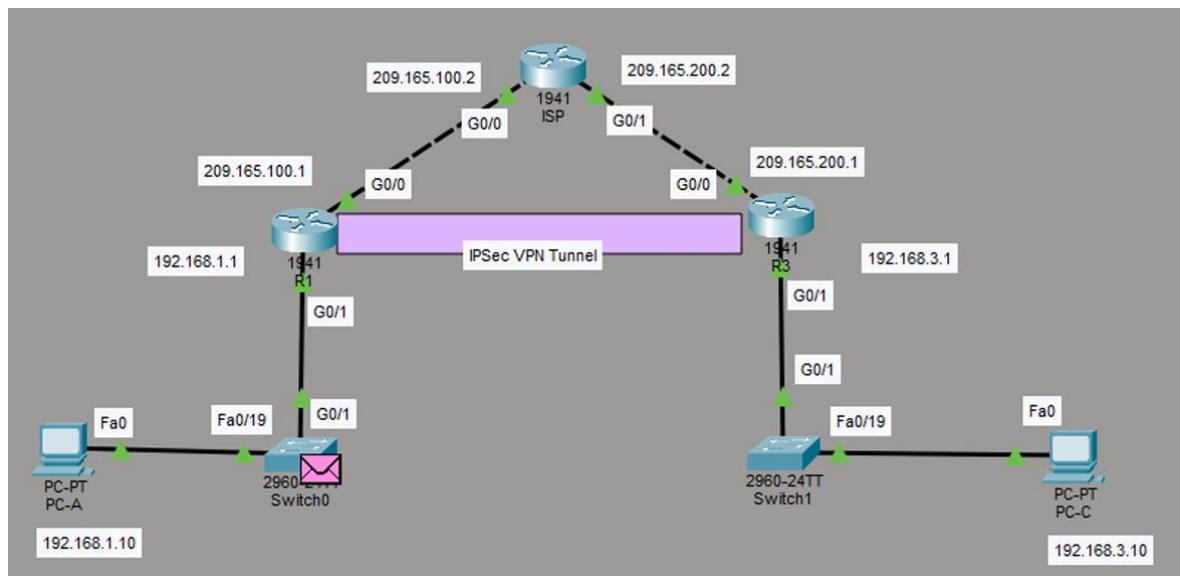
La protección de datos en redes públicas suele ser complicado por el libre acceso a este tipo de redes, los datos pueden ser modificados y/o suplantados durante su tránsito. Una opción para la protección de estos es IPSec (Internet Protocol Security), un conjunto de protocolos que opera en la capa de red y permite establecer canales de comunicación seguros mediante mecanismos criptográficos de autenticación, integridad y confidencialidad.

IPSec funciona encapsulando y protegiendo los paquetes IP mediante asociaciones de seguridad negociadas entre los extremos del túnel. Para ello emplea dos fases principales de establecimiento: la negociación inicial de parámetros criptográficos y autenticación entre pares, y posteriormente la definición de cómo será protegido el tráfico considerado válido o “interesante”. A nivel práctico, esto permite que dos redes privadas intercambien información como si estuvieran directamente conectadas, aun cuando el medio intermedio sea inseguro.

En esta práctica se implementa una VPN IPSec en Packet Tracer, configurando routers que actúan como extremos del túnel. El objetivo es establecer una comunicación segura entre dos redes LAN asegurando que el tráfico intercambiado esté cifrado y autenticado antes de atravesar la red pública simulada.

## Topología propuesta

La siguiente imagen ilustra como deberá de ser construida la topología en la práctica, mostrando los puertos a conectar y sus respectivas direcciones.



## Desarrollo

Empezamos construyendo la topología de red, como se ilustraba en el ejemplo, seguimos las mismas conexiones con el mismo equipo (Routers 1941; Switch 2960) y el mismo cableado.

Realizamos la configuración física de las computadoras, puesto que es lo único que no se configura en los comandos posteriores:

### PC-A

IP: 192.168.1.10

Mask: 255.255.255.0

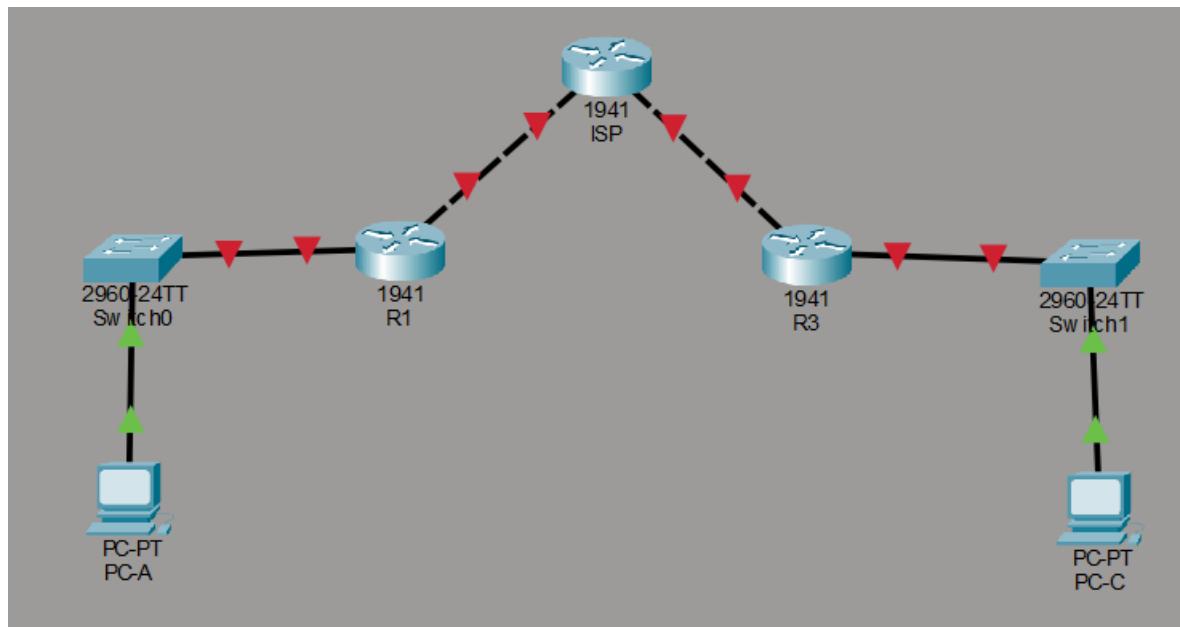
Gateway: 192.168.1.1

### PC-C

IP: 192.168.3.10

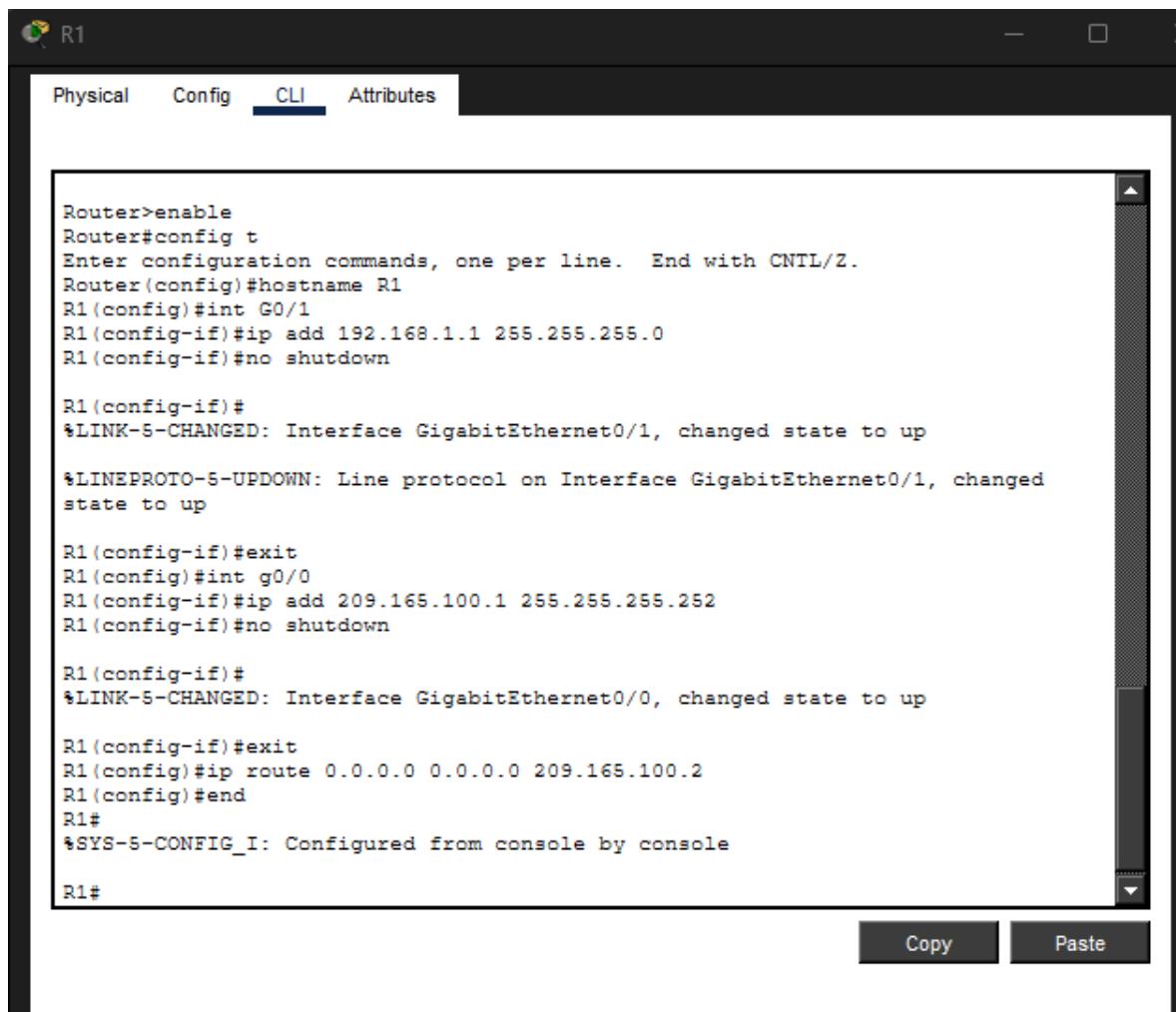
Mask: 255.255.255.0

Gateway: 192.168.3.1



Proseguimos configurando el Router 1, con los siguientes comandos, esto para indicar las direcciones de entrada y salida, creando un correcto direccionamiento:

- ENABLE
- CONFIG TERMINAL
- HOSTNAME R1
- INT G0/0
- IP ADD 209.165.100.1 255.255.255.252
- NO SHUTDOWN
- INT G0/1
- IP ADD 192.168.1.1 255.255.255.0
- NO SHUTDOWN
- EXIT
- IP ROUTE 0.0.0.0 0.0.0.0 209.165.100.2



```
Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#int G0/1
R1(config-if)#ip add 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown

R1(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

R1(config-if)#exit
R1(config)#int g0/0
R1(config-if)#ip add 209.165.100.1 255.255.255.252
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

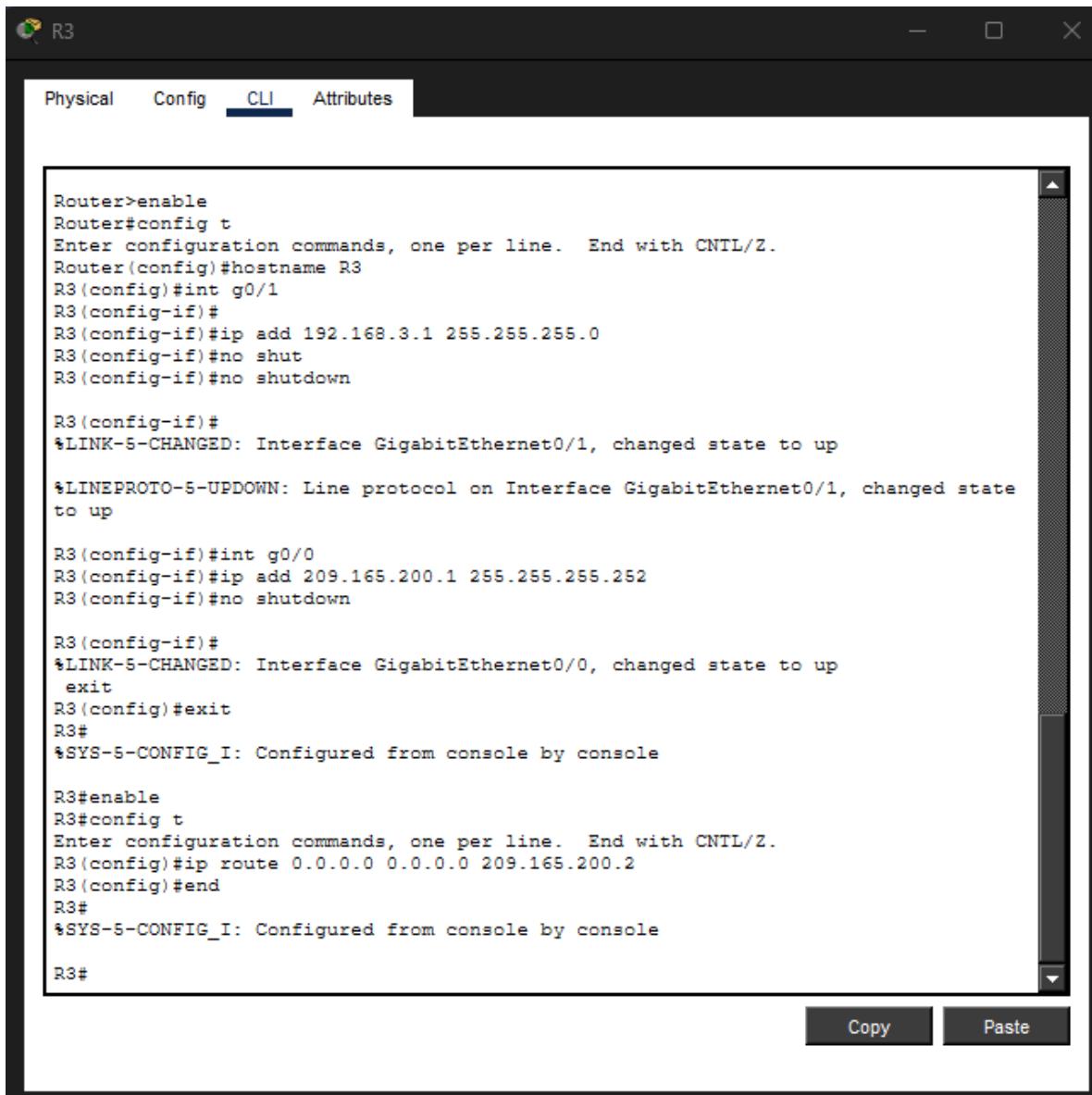
R1(config-if)#exit
R1(config)#ip route 0.0.0.0 0.0.0.0 209.165.100.2
R1(config)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#
```

The screenshot shows a software interface for managing network devices. At the top, there's a toolbar with icons for Physical, Config, CLI (which is highlighted in blue), and Attributes. Below the toolbar is a large text area containing the command-line configuration history for Router 1. The configuration includes setting the hostname to 'R1', configuring interface G0/1 with IP 192.168.1.1, enabling it, and then configuring interface g0/0 with IP 209.165.100.1, enabling it, and finally creating a default route. At the bottom of the configuration pane, there are 'Copy' and 'Paste' buttons.

Se realizaron los mismos pasos para R3:

- ENABLE
- CONFIG TERMINAL
- HOSTNAME R3
- INT G0/0
- IP ADD 209.165.200.1 255.255.255.252
- NO SHUTDOWN
- INT G0/1
- IP ADD 209.165.200.1 255.255.255.252
- NO SHUTDOWN
- EXIT
- IP ROUTE 0.0.0.0 0.0.0.0 209.165.200.2



The screenshot shows a window titled 'R3' with a toolbar at the top labeled 'Physical', 'Config', 'CLI', and 'Attributes'. The 'CLI' tab is selected. The main area displays the following configuration commands:

```

Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R3
R3(config)#int g0/1
R3(config-if)#
R3(config-if)#ip add 192.168.3.1 255.255.255.0
R3(config-if)#no shut
R3(config-if)#no shutdown

R3(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

R3(config-if)#int g0/0
R3(config-if)#ip add 209.165.200.1 255.255.255.252
R3(config-if)#no shutdown

R3(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
exit
R3(config)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#enable
R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ip route 0.0.0.0 0.0.0.0 209.165.200.2
R3(config)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console

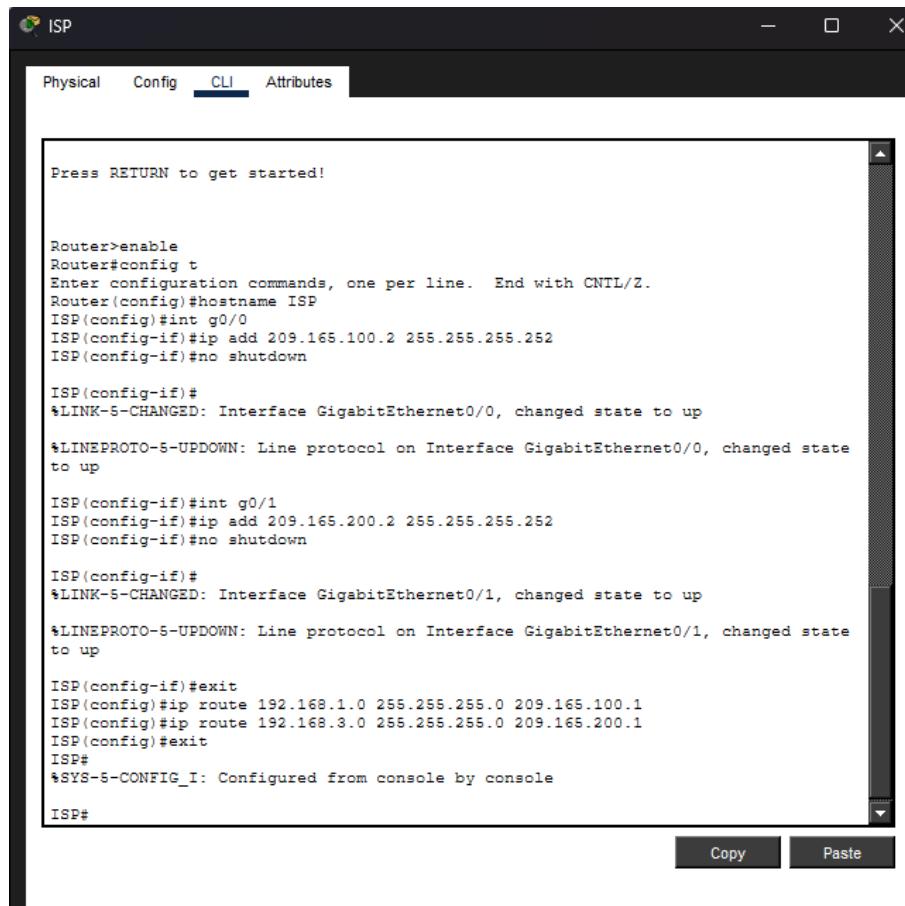
R3#

```

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

Después se realizó la configuración para el ISP, el cual cuenta con comandos similares:

- Enable
- config t
- hostname ISP
- int g0/0
- ip add 209.165.100.2 255.255.255.252
- no shutdown
- int g0/1
- ip add 209.165.200.2 255.255.255.252
- no shutdown
- exit
- ip route 192.168.1.0 255.255.255.0 209.165.100.1
- ip route 192.168.3.0 255.255.255.0 209.165.200.1



The screenshot shows a terminal window titled "ISP". The window has tabs at the top: "Physical", "Config", "CLI" (which is selected), and "Attributes". The main area of the window displays the following configuration session:

```
Press RETURN to get started!

Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#hostname ISP
ISP(config)#int g0/0
ISP(config-if)#ip add 209.165.100.2 255.255.255.252
ISP(config-if)#no shutdown

ISP(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

ISP(config-if)#int g0/1
ISP(config-if)#ip add 209.165.200.2 255.255.255.252
ISP(config-if)#no shutdown

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

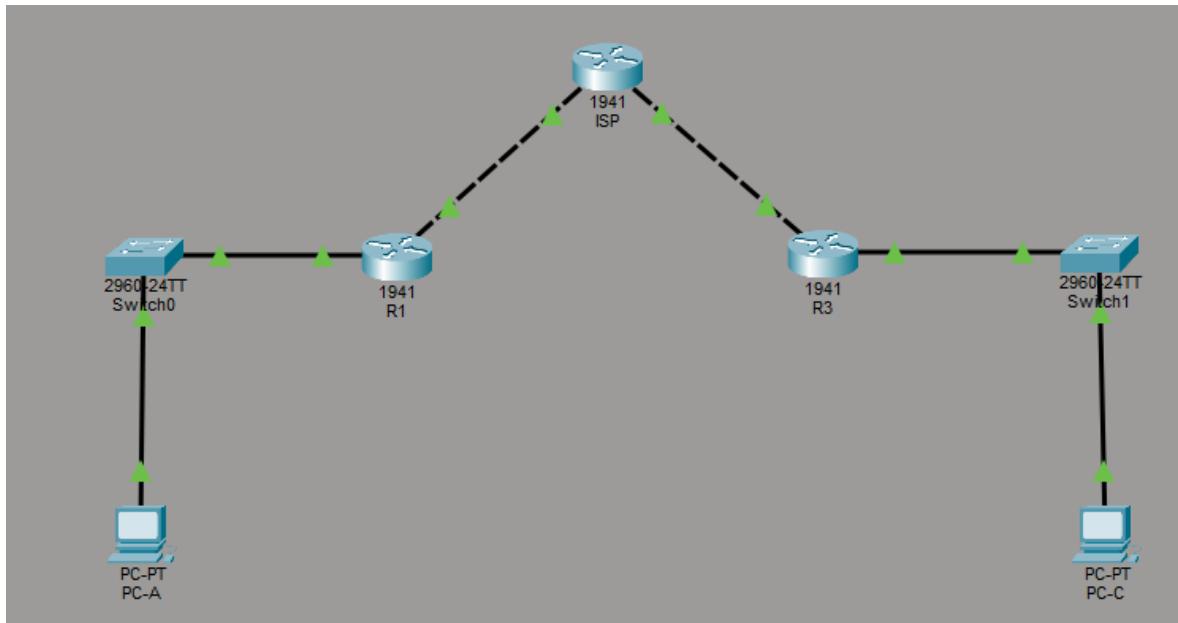
*LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

ISP(config-if)#exit
ISP(config)#ip route 192.168.1.0 255.255.255.0 209.165.100.1
ISP(config)#ip route 192.168.3.0 255.255.255.0 209.165.200.1
ISP(config)#exit
ISP#
*SYS-5-CONFIG_I: Configured from console by console

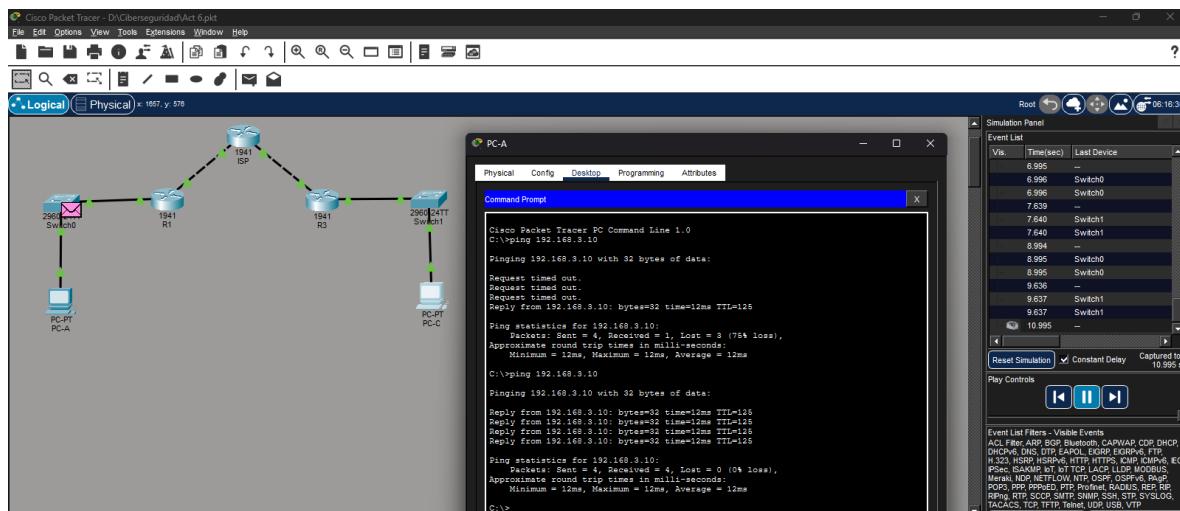
ISP#
```

At the bottom right of the terminal window, there are "Copy" and "Paste" buttons.

Con esto, nuestra topología estaría completada, solo falta realizar un ping de PC-A a PC-C



Se realizo el ping, al principio no se detectaba la ruta, al ser un dispositivo recién configurado, se deben de setear las solicitudes ARP y anotar las MAC's en las tablas de los routers, con una simple repetición de comandos, nuestros pings fueron exitosos.



Con la topología concluida, avanzamos al siguiente paso que es habilitar las licencias de seguridad.

## Habilitar licencia de seguridad

Para habilitar las licencias de seguridad en R1 y R3, simplemente seguimos los siguientes comandos en cada interfaz, con esto el router nos preguntara si deseamos proseguir, dando una confirmación, se instalarán las licencias, simplemente tenemos que grabar la memoria de cada uno de nuestros routers y reiniciar, y se habilitaran nuestras licencias.

Sin estas licencias, no podemos implementar IPSec VPN.

- enable
- conf t
- license boot module c1900 technology-package securityk9
- exit
- write memory
- reload

R1

Physical    Config    **CLI**    Attributes

```
* Invalid input detected at marker.

R1(config)#licen
R1(config)#license boot module c1900 tech
R1(config)#license boot module c1900 technology-package securi
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/English/EU1KEN\_.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]: y
* 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
|
```

R3

Physical    Config    **CLI**    Attributes

```
R3>enable
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#license boot module c
R3(config)#license boot module c1900 tec
R3(config)#license boot module c1900 technology-package secur
R3(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/English/EU1KEN\_.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]: y
% use 'write' command to make license boot config take effect on next boot

R3(config)#: %IOS_LICENSE_IMAGE_APPLICATION-6-LICENSE_LEVEL: Module name = C1900
Next reboot level = securityk9 and License = securityk9
```

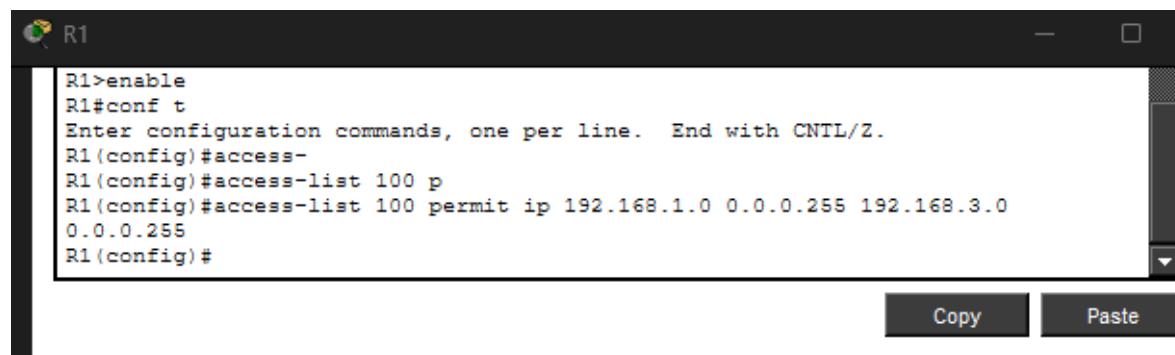
Copy      Paste

## Trafico interesante

El tráfico interesante es el que definimos en la ACL; cuando un paquete coincide con esa regla (entre 192.168.1.0 y 192.168.3.0), el router sabe que debe protegerlo usando IPSec y no enviarlo en texto plano.

Se implemento con los siguientes comandos en cada interfaz:

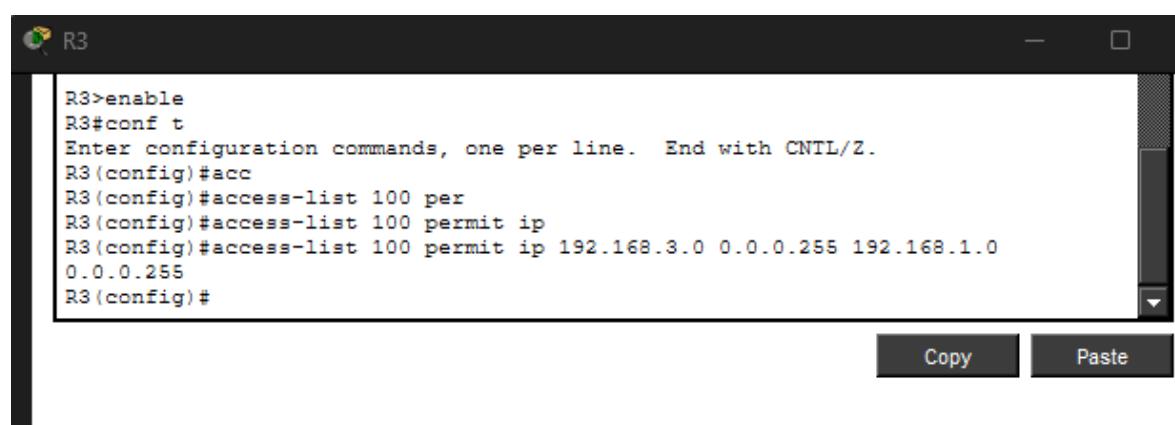
- enable
- conf t
- access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255



```
R1>enable
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#access-
R1(config)#access-list 100 p
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)#

```

Copy Paste



```
R3>enable
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#acc
R3(config)#access-list 100 per
R3(config)#access-list 100 permit ip
R3(config)#access-list 100 permit ip 192.168.3.0 0.0.0.255 192.168.1.0
0.0.0.255
R3(config)#

```

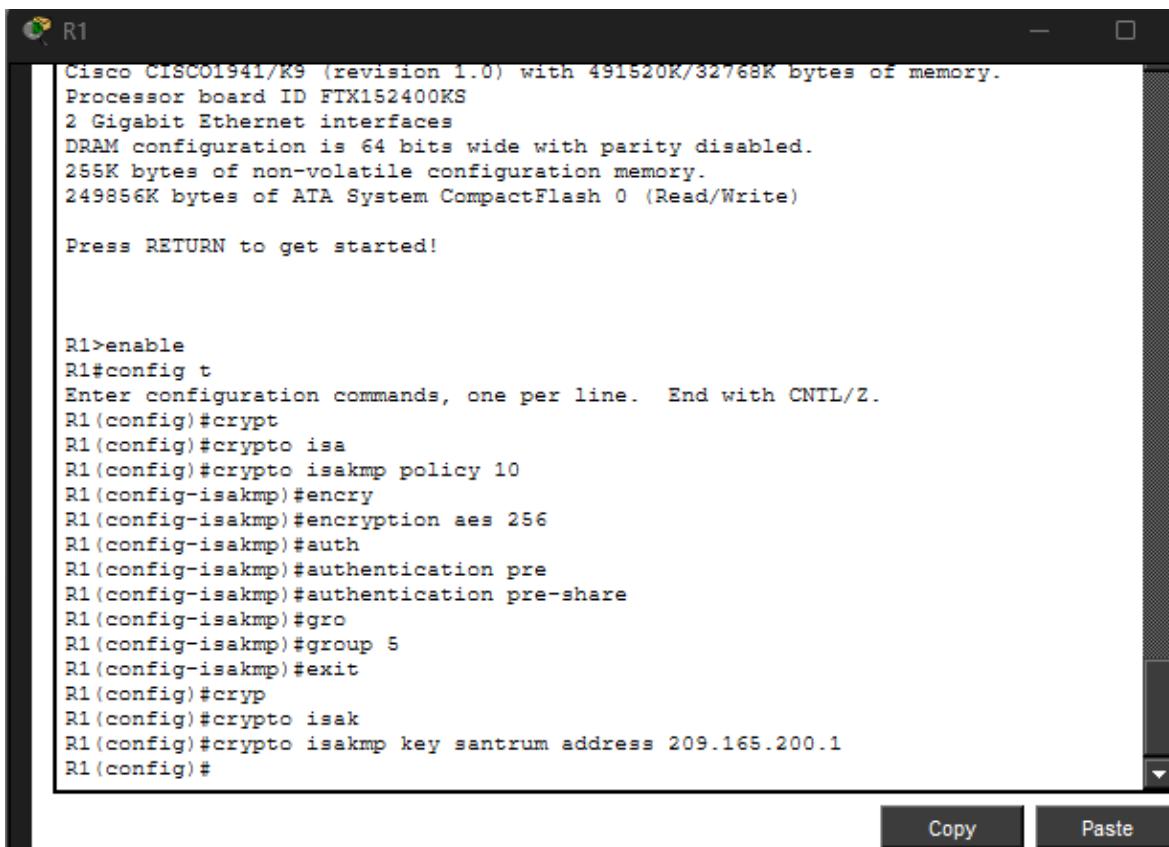
Copy Paste

## FASE 1 – ISAKMP (negociación)

En la Fase 1 (ISAKMP) los routers negocian y establecen un canal seguro intercambiando parámetros de cifrado y autenticación. No se cifran datos aún, solo se crea la base segura.

Se implementaron en cada interfaz con los siguientes comandos (Con variantes en cada IP del dispositivo a configurar)

- crypto isakmp policy 10
- encryption aes 256
- authentication pre-share
- group 5
- exit
- crypto isakmp key santrum address 209.165.200.1



R1

```
Cisco CISCO1941/K9 (revision 1.0) with 491520K/32768K bytes of memory.  
Processor board ID FTX152400KS  
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!  
  
R1>enable  
R1#config t  
Enter configuration commands, one per line. End with CNTL/Z.  
R1(config)#crypt  
R1(config)#crypto isa  
R1(config)#crypto isakmp policy 10  
R1(config-isakmp)#encry  
R1(config-isakmp)#encryption aes 256  
R1(config-isakmp)#auth  
R1(config-isakmp)#authentication pre  
R1(config-isakmp)#authentication pre-share  
R1(config-isakmp)#gro  
R1(config-isakmp)#group 5  
R1(config-isakmp)#exit  
R1(config)#cryp  
R1(config)#crypto isak  
R1(config)#crypto isakmp key santrum address 209.165.200.1  
R1(config)#

```

Copy Paste

```
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!  
  
R3>enable  
R3#config r  
^  
% Invalid input detected at '^' marker.  
  
R3#config t  
Enter configuration commands, one per line. End with CNTL/Z.  
R3(config)#cry  
R3(config)#crypto isakm  
R3(config)#crypto isakmp pol  
R3(config)#crypto isakmp policy 10  
R3(config-isakmp)#encry  
R3(config-isakmp)#encryption aes 256  
R3(config-isakmp)#aut  
R3(config-isakmp)#authentication pre  
R3(config-isakmp)#authentication pre-share  
R3(config-isakmp)#group 5  
R3(config-isakmp)#exit  
R3(config)#crypto isak  
R3(config)#crypto isakmp key santrum ad  
R3(config)#crypto isakmp key santrum address 209.165.100.1  
R3(config)#

```

Copy      Paste

## FASE 2 – Transform Set (cómo se protegerán los datos)

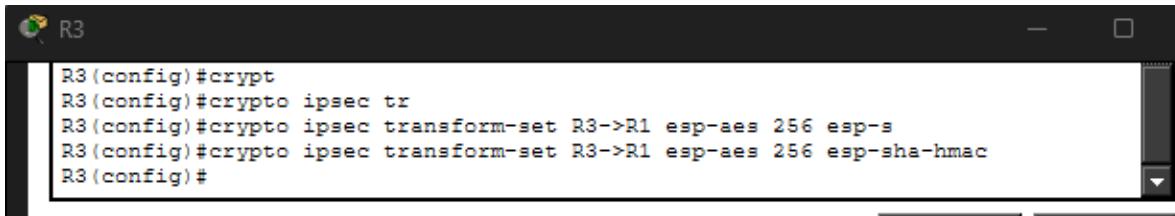
En la Fase 2 (IPSec) se establecen las asociaciones que realmente cifran y protegen los datos que coincidan con el tráfico interesante.

Se implementaron en cada interfaz con los siguientes comandos (Con variantes en cada IP del dispositivo a configurar)

- crypto ipsec transform-set R1-R3 esp-aes 256 esp-sha-hmac

```
R1#config t  
R1(config)#cryp  
R1(config)#crypto ip  
R1(config)#crypto ipsec tran  
R1(config)#crypto ipsec transform-set R1->R3 esp  
R1(config)#crypto ipsec transform-set R1->R3 esp-  
R1(config)#crypto ipsec transform-set R1->R3 esp-aes 256 esp-sha-  
R1(config)#crypto ipsec transform-set R1->R3 esp-aes 256 esp-sha-hmac  
R1(config)#

```



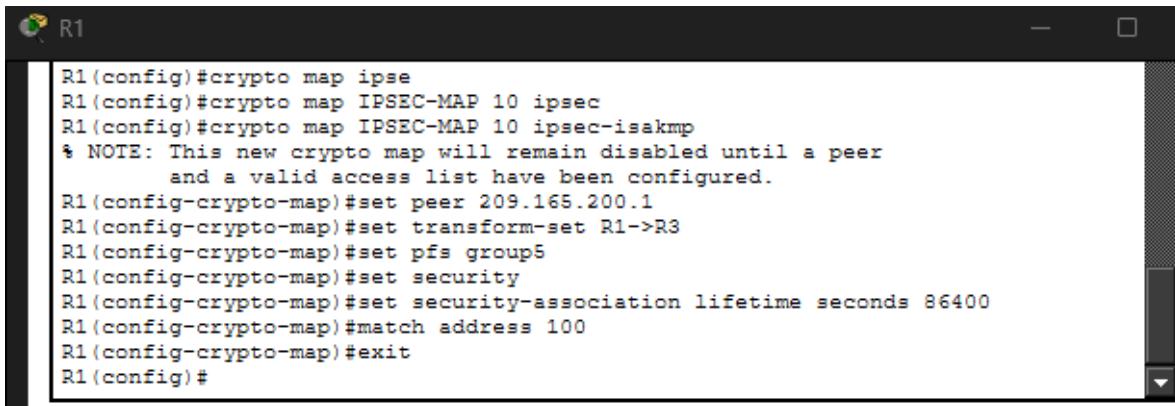
```
R3(config)#crypt
R3(config)#crypto ipsec tr
R3(config)#crypto ipsec transform-set R3->R1 esp-aes 256 esp-s
R3(config)#crypto ipsec transform-set R3->R1 esp-aes 256 esp-sha-hmac
R3(config)#+
```

## FASE 3 – Crypto Map

En la Fase 3 (Crypto Map) se vinculan el peer remoto, los algoritmos y la ACL para indicar cuándo debe activarse el cifrado.

Se implementaron en cada interfaz con los siguientes comandos (Con variantes en cada IP del dispositivo a configurar):

- crypto map IPSEC-MAP 10 ipsec-isakmp
- set peer 209.165.200.1
- set transform-set R1-R3
- set pfs group5
- set security-association lifetime seconds 86400
- match address 100
- exit



```
R1(config)#crypto map ipse
R1(config)#crypto map IPSEC-MAP 10 ipsec
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 peer 209.165.200.1
R1(config-crypto-map)#set transform-set R1->R3
R1(config-crypto-map)#set pfs group5
R1(config-crypto-map)#set security
R1(config-crypto-map)#set security-association lifetime seconds 86400
R1(config-crypto-map)#match address 100
R1(config-crypto-map)#exit
R1(config)#+
```

```
R3# R3
R3(config)#crypto ipsec tr
R3(config)#crypto ipsec transform-set R3->R1 esp-aes 256 esp-s
R3(config)#crypto ipsec transform-set R3->R1 esp-aes 256 esp-sha-hmac
R3(config)#crypto map IPSEC-MAP 10 ipse
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 transform-set R3->R1
R3(config-crypto-map)#set pfs group5
R3(config-crypto-map)#set security
R3(config-crypto-map)#set security-association lifetime seconds 86400
R3(config-crypto-map)#match ad
R3(config-crypto-map)#match address 100
R3(config-crypto-map)#exit
R3(config)#

```

## FASE 4 – Aplicar a la interfaz WAN (la que va al ISP)

En la Fase 4, el crypto map se aplica a la interfaz de salida hacia el ISP, permitiendo que el tráfico interesante que pase por ahí sea cifrado automáticamente.

Se implementaron en cada interfaz con los siguientes comandos (Con variantes en cada IP del dispositivo a configurar):

- interface g0/0
- crypto map IPSEC-MAP
- exit

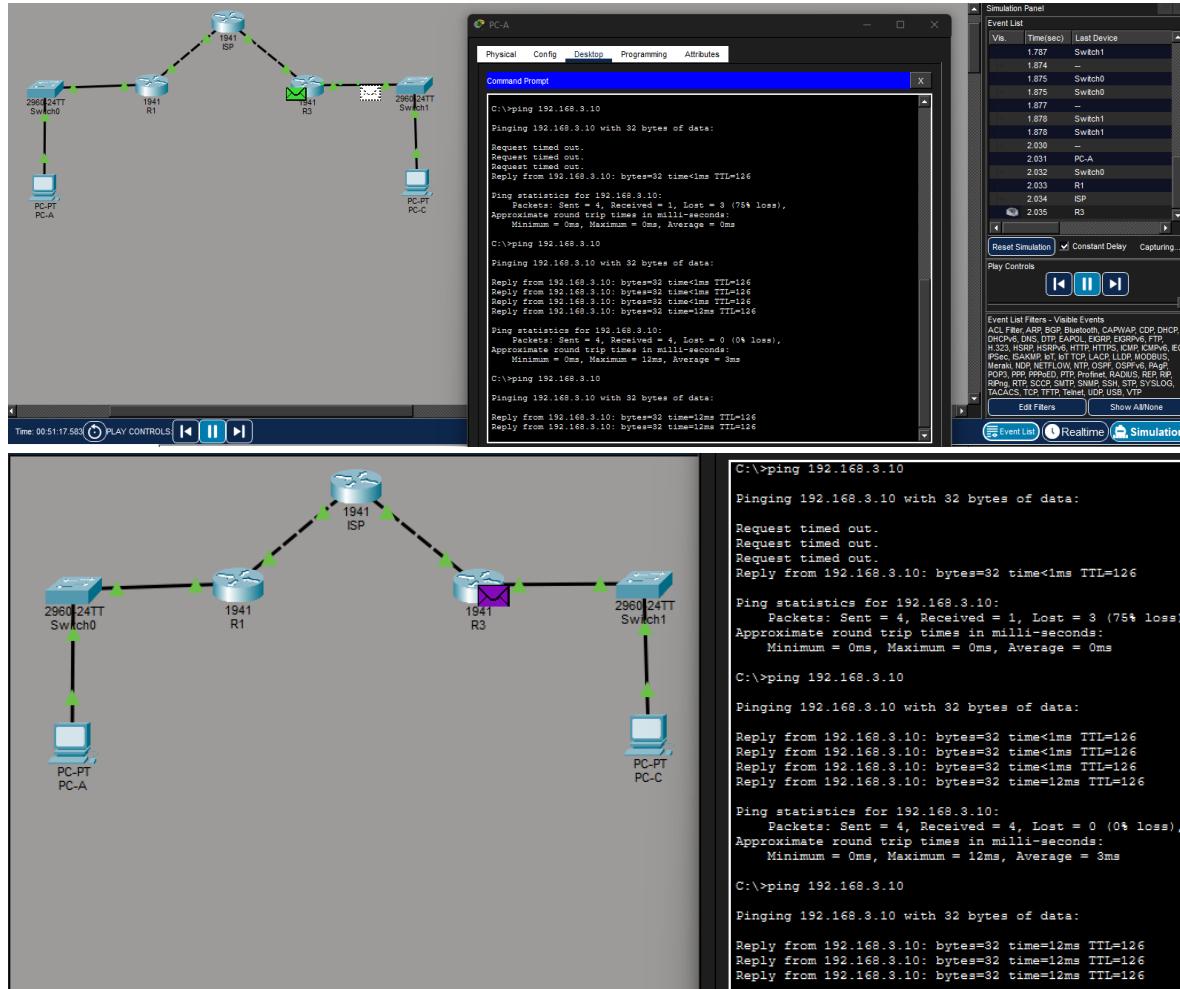
```
R1# R1
R1(config)#int g0/0
R1(config-if)#crypt
R1(config-if)#crypto map IPSEC-MAP
*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config-if)#exit
R1(config)#

```

```
R3# R3
R3(config-crypto-map)#exit
R3(config)#int g0/0
R3(config-if)#crypto map IPSEC-MAP
*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R3(config-if)#exit
R3(config)#

```

Con esto, se concluyó exitosamente la implementación del IPSec VPN, solo nos resta verificar la conexión entre PC-A y PC-C, de igual forma, nuestras tablas ARP fueron reiniciadas, por lo cual nuestro primer ping no fue exitoso, si no, hasta mandar un segundo comando con las tablas ya actualizadas y las claves verificadas.



PC-A

Physical Config Desktop Programming Attributes

Command Prompt

```
Reply from 192.168.3.10: bytes=32 time<1ms TTL=126
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 192.168.3.10

Pinging 192.168.3.10 with 32 bytes of data:

Reply from 192.168.3.10: bytes=32 time<1ms TTL=126
Reply from 192.168.3.10: bytes=32 time<1ms TTL=126
Reply from 192.168.3.10: bytes=32 time<1ms TTL=126
Reply from 192.168.3.10: bytes=32 time=12ms TTL=126

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 = 12ms, Average = 3ms

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=12ms TTL=126

Ping statistics for 192.168.3.10:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 12ms, Maximum = 12ms, Average = 12ms
```

## Conclusión

La implementación de la VPN IPSec permitió conectar ambas redes privadas a través del ISP como si fueran una sola red lógica, garantizando confidencialidad, integridad y autenticación del tráfico. A través de las fases de negociación, establecimiento de asociaciones y aplicación del crypto map, el túnel se construye dinámicamente cuando aparece tráfico interesante, demostrando cómo IPSec protege comunicaciones sobre infraestructura pública sin modificar el esquema de direccionamiento interno. Esto confirma que la seguridad en redes no solo depende del enrutamiento correcto, sino de mecanismos criptográficos que aseguren la información extremo a extremo.