

ACTIVIDAD:
Implementación IPSec VPN

Institución: Universidad Politécnica de San Luis Potosí

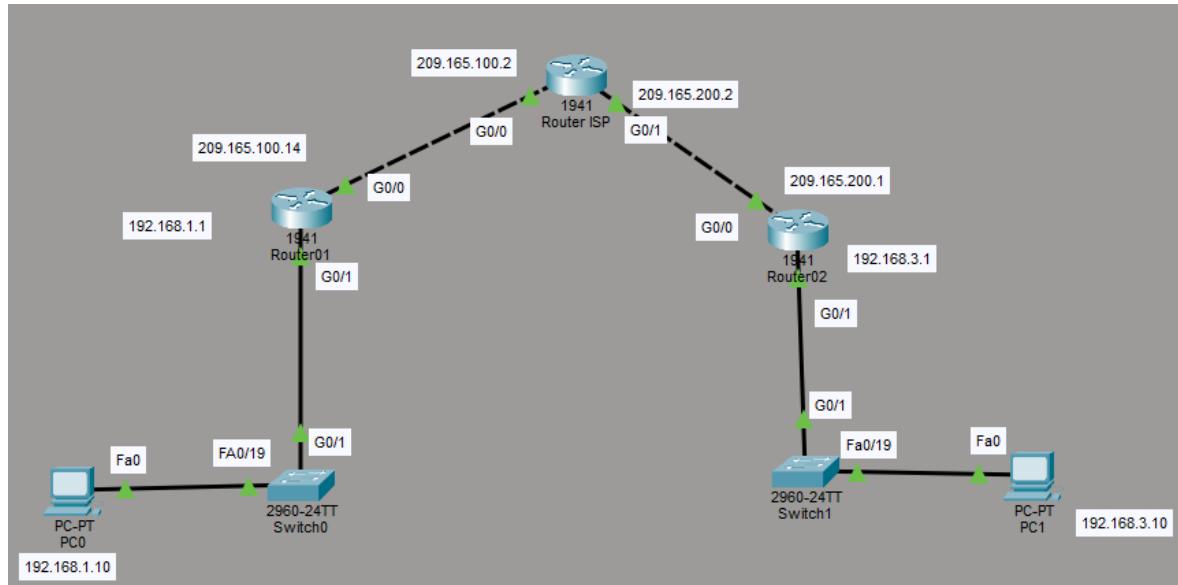
Materia:
CNO V – Seguridad Informática

Estudiante:
López Castro Diego – 182032

Profesor:
Mtro. Servando López Contreras

Fecha de entrega:
16 – Febrero – 2026

Configuración de la topología de red



Fases de la configuración

1. Configuración inicial

En la fase de configuración inicial se realiza la preparación básica de cada router. Primero se utiliza el comando `enable` (o `en`) para entrar al modo EXEC privilegiado, lo cual permite ejecutar comandos administrativos. Después se utiliza `configure terminal` para ingresar al modo de configuración global. Se asigna un nombre a cada router con el comando `hostname`, lo que facilita su identificación dentro de la red. Así mismo, se configuran las interfaces de red. Con el comando `interface GigabitEthernet` se accede a la configuración de cada interfaz física. Se asigna una dirección IP y una máscara de subred mediante el comando `ip address`, lo cual permite que el dispositivo pueda comunicarse dentro de su segmento de red. El comando `no shut` se utiliza para activar la interfaz, ya que por defecto estas se encuentran deshabilitadas administrativamente. Además, se configura una ruta estática por defecto utilizando el comando `ip route 0.0.0.0 0.0.0.0`, lo que permite que todo el tráfico destinado a redes desconocidas sea enviado hacia el siguiente salto correspondiente. Esto es fundamental para que los routers puedan comunicarse a través del ISP.

Router 01

```

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

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)#interface G0/0
^
% Invalid input detected at '^' marker.

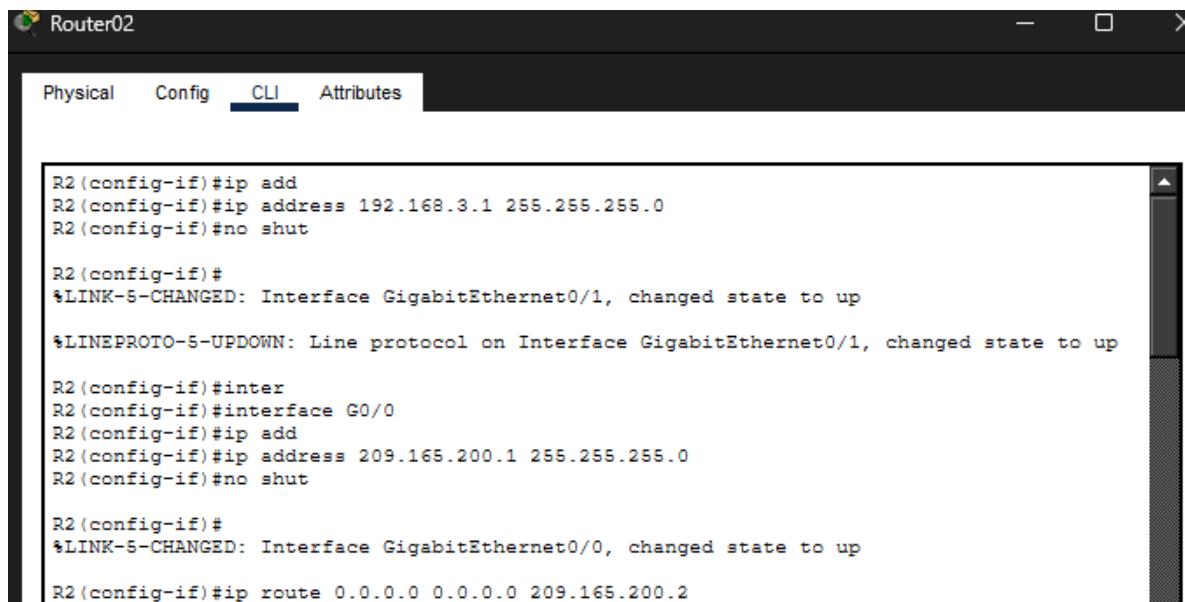
R1(config-if)#interface G0/0
R1(config-if)#ip add
R1(config-if)#ip address 209.165.100.1 255.255.255.0
R1(config-if)#no shut

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

R1(config-if)#ip rout 0.0.0.0 0.0.0.0 209.165.100.2
% Ambiguous command: "ip rout 0.0.0.0 0.0.0.0 209.165.100.2"
R1(config)#ip route 0.0.0.0 0.0.0.0 209.165.100.2
R1(config)#license boot module c1900 technology-package securityk9

```

Router 02



```

Router02

Physical Config CLI Attributes

R2(config-if)#ip add
R2(config-if)#ip address 192.168.3.1 255.255.255.0
R2(config-if)#no shut

R2(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

R2(config-if)#inter
R2(config-if)#interface G0/0
R2(config-if)#ip add
R2(config-if)#ip address 209.165.200.1 255.255.255.0
R2(config-if)#no shut

R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

R2(config-if)#ip route 0.0.0.0 0.0.0.0 209.165.200.2

```

Router ISP

```
-- you require technical assistance please contact us by sending email to  
export@cisco.com.  
  
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!  
  
Router>enable  
Router#conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
Router(config)#hostname ISP  
ISP(config)#interface G0/0  
ISP(config-if)#ip add  
ISP(config-if)#ip address 209.165.100.2 255.255.255.0  
ISP(config-if)#no shut  
  
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)#interface G0/1  
ISP(config-if)#ip add  
ISP(config-if)#ip address 209.165.200.2 255.255.255.0  
ISP(config-if)#no shut  
  
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)#ip route 0.0.0.0 0.0.0.0 209.165.200.1  
ISP(config)#
```

Copy Paste

2. Licencia de seguridad habilitada

En esta fase, básicamente, se habilita la licencia de seguridad. Para que el router pueda ejecutar funciones criptográficas como IPSec, es necesario activar el paquete tecnológico SecurityK9. Esto se realiza mediante el comando license boot technology-package securityK9. Después se guarda la configuración con copy running-config startup-config y se reinicia el dispositivo con reload para aplicar los cambios. Finalmente, el comando show version permite verificar que la licencia de seguridad está activa. Sin esta licencia, los comandos relacionados con crypto no estarían disponibles, por lo que la implementación de la VPN no sería posible.

Router 01

Router01

Physical Config **CLI** Attributes

```
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

R1(config)#

R1 con0 is now available
```

Router01

Physical Config **CLI** Attributes

```
Destination filename [startup-config]?  
Building configuration...  
[OK]  
R1#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 :  
#####
##### [OK]  
Smart Init is enabled  
smart init is sizing iomem  
    TYPE      MEMORY_REQ  
  Onboard devices &  
    buffer pools   0x01E8F000  
-----  
        TOTAL: 0x01E8F000  
Rounded IOMEM up to: 32Mb.  
Using 6 percent iomem. [32Mb/512Mb]  
  
Restricted Rights Legend  
Use, duplication, or disclosure by the Government is  
subject to restrictions as set forth in subparagraph  
(c) of the Commercial Computer Software - Restricted  
Rights clause at FAR sec. 52.227-19 and subparagraph  
(c) (1) (ii) of the Rights in Technical Data and Computer  
Software clause at DFARS sec. 252.227-7013.
```

Copy Paste

Router 02

Router02

Physical Config **ICL** Attributes

```
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

R2(config)#: %IOS_LICENSE_IMAGE_APPLICATION-6-LICENSE_LEVEL: Module name = C1900 Next reboot level = securityk9 and License = securityk9

R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
R2#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 DTM600 = 0 MB
```

Copy Paste

Router02

Physical Config **CLI** Attributes

```
Building configuration...
[OK]
R2#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 :
#####
Smart Init is enabled
smart init is sizing iomem
    TYPE      MEMORY_REQ
  Onboard devices &
    buffer pools 0x01E8F000
-----
    TOTAL: 0x01E8F000
Rounded IOMEM up to: 32Mb.
Using 6 percent iomem. [32Mb/512Mb]

    Restricted Rights Legend
Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.
cisco Systems, Inc.
```

Copy Paste

Router ISP

Router ISP

Physical Config **CLI** Attributes

```
IOS Image Load Test

Digitally Signed Release Software
program load complete, entry point: 0x81000000, size: 0x2bb1c58
Self decompressing the image :
#####
[OK]
Smart Init is enabled
smart init is sizing iomem
    TYPE      MEMORY_REQ
    Onboard devices &
    buffer pools   0x01E8F000
-----
    TOTAL: 0x01E8F000
Rounded IOMEM up to: 32Mb.
Using 6 percent iomem. [32Mb/512Mb]

Restricted Rights Legend
Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.
cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.1(4)M4, RELEASE
SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thurs 5-Jan-12 15:41 by pt_team
Image text-base: 0x2100F918, data-base: 0x24729040

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. laws and regulations regarding the export and import
of cryptographic products, as well as for all other aspects of
import, export, distribution and use of Cisco cryptographic products.
Cisco and the Cisco logo are trademarks of Cisco Systems, Inc. and/or its
subsidiaries and/or affiliates. All other trademarks belong to their
respective holders.
```

Copy Paste

```
Router>copy run start
^
* Invalid input detected at '^' marker.

Router>enable
Router#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Router#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 :
#####
[OK]
Smart Init is enabled
smart init is sizing iomem
      TYPE      MEMORY_REQ
  Onboard devices &
  buffer pools    0x01E8F000
-----
      TOTAL:    0x01E8F000
Rounded IOMEM up to: 32Mb.
Using 6 percent iomem. [32Mb/512Mb]

Restricted Rights Legend
```

Copy Paste

3. Implementación de ACLs

En la fase de implementación de ACL's se crean Listas de Control de Acceso extendidas. Una ACL es un conjunto de reglas que permiten o deniegan tráfico según criterios específicos como direcciones IP. En este caso se configura la ACL 100 en cada router. Esta ACL permite tráfico IP entre las redes privadas 192.168.1.0 y 192.168.3.0 utilizando una wildcard mask 0.0.0.255. La wildcard mask indica qué bits pueden variar dentro de la red, representando una red con máscara /24. Estas ACL no se utilizan para bloquear tráfico, sino para definir el tráfico interesante que será protegido por IPSec. Solo los paquetes que coincidan con esta ACL serán cifrados dentro del túnel VPN.

Router 01

```
R1#en
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#access-list 100 cpermit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
^
% Invalid input detected at '^' marker.

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

Router 02

```
R2>en
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#access-list 100 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
R2(config)#[
```

Copy

Paste

4. Phase 1: ISAKMP policy

En la Phase 01 se configura la política ISAKMP. ISAKMP es el protocolo encargado de negociar y establecer los parámetros de seguridad entre los peers antes de que se cifren los datos. Se crea una política con crypto isakmp policy indicando un número de prioridad. Dentro de esta política se especifica el algoritmo de cifrado mediante encryption aes 256, lo que indica que se utilizará AES con clave de 256 bits. Se define el método de autenticación con authentication pre-share, lo que significa que ambos routers utilizarán una clave precompartida para autenticarse mutuamente. También se configura el grupo 5 de Diffie-Hellman con group 5, el cual se encarga del intercambio seguro de claves. Finalmente, con crypto isakmp key se establece la clave precompartida asociada a la dirección IP del peer remoto. Esta fase crea la Security Association inicial que protege la negociación del túnel.

Router 01

```

R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#cry
R1(config)#crypto isakmp pol
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#encr
R1(config-isakmp)#encryption aes 256
R1(config-isakmp)#aunt
R1(config-isakmp)#aut
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group5
^
% Invalid input detected at '^' marker.

R1(config-isakmp)#group 5
R1(config-isakmp)#exit
R1(config)#cry
R1(config)#crypto is
R1(config)#crypto isakmp key se
R1(config)#crypto isakmp key secret
R1(config)#crypto isakmp key secretkey add
R1(config)#crypto isakmp key secretkey address 209.165.200.1
R1(config)#

```

[Copy](#)

[Paste](#)

Top

Router 02

```

R2>en
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#access-list 100 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
R2(config)#crypto is
R2(config)#crypto isakmp po
R2(config)#crypto isakmp policy 10
^
% Invalid input detected at '^' marker.

R2(config)#crypto isakmp policy 10
R2(config-isakmp)#encr
R2(config-isakmp)#encryption aes 256
R2(config-isakmp)#aut
R2(config-isakmp)#authentication pre
R2(config-isakmp)#authentication pre-share
R2(config-isakmp)#group 5
R2(config-isakmp)#exit
R2(config)#cry
R2(config)#crypto is
R2(config)#crypto isakmp key secretkey add
R2(config)#crypto isakmp key secretkey address 209.165.100.1
R2(config)#

```

[Copy](#)

[Paste](#)

5. Phase 2 ipsec transform set

En la Phase 2 se configura el IPSec transform-set. Esta fase define cómo se protegerán los datos reales que viajan por el túnel. El comando crypto ipsec transform-set crea un conjunto de transformaciones criptográficas. Se utiliza esp-aes 256, lo que indica que se emplea el protocolo Encapsulating Security Payload con cifrado AES de 256 bits. También se configura esp-sha-hmac, que proporciona autenticación e integridad de los datos mediante el algoritmo SHA con HMAC. A

diferencia de la Phase 01, en esta etapa se cifra tanto el encabezado como el contenido del paquete. Aquí se establece la Security Association de IPSec que protegerá el tráfico definido previamente por la ACL.

Router 01

```
R1(config)#cry
R1(config)#crypto ip
R1(config)#crypto ipsec trans
R1(config)#crypto ipsec transform-set R1->R2 esp
R1(config)#crypto ipsec transform-set R1->R2 esp-a
R1(config)#crypto ipsec transform-set R1->R2 esp-aes 256 esp-sha-hmac
R1(config)#

```

Router 02

```
R2(config)#cry
R2(config)#crypto ip
R2(config)#crypto ipsec trans
R2(config)#crypto ipsec transform-set R2->R1 esp-aes 256 esp-sha-hmac
R2(config)#

```

[Copy](#)

[Paste](#)

6. Crear el mapa criptográfico

En la creación del mapa criptográfico, se crea el mapa con el comando crypto map. El crypto map funciona como un contenedor que integra todos los elementos configurados anteriormente. Dentro del crypto map se define el peer remoto con set peer, se activa Perfect Forward Secrecy mediante set pfs group5, lo cual obliga a generar nuevas claves de sesión usando Diffie-Hellman para cada negociación, y se establece el tiempo de vida de la Security Association con set security-association lifetime seconds 86400, indicando que la asociación será válida por 24 horas. También se asocia el transform-set con set transform-set y se vincula la ACL mediante match address 100, especificando que el tráfico interesante será el definido en esa lista de acceso.

Router 01

```
R1(config)#crypto ipsec transform-set R1->R2 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 peer 209.165.200.1
R1(config-crypto-map)#set pfs group5
R1(config-crypto-map)#

```

[Copy](#)

[Paste](#)

Router 02

```
R2(config)#crypto ipsec transform-set R2->R1 esp-aes 256 esp-sha-hmac
R2(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.
R2(config-crypto-map)#set peer 209.165.100.1
R2(config-crypto-map)#set pfs group5
R2(config-crypto-map)#set security-association lifetime seconds 86400
R2(config-crypto-map)#set transform-set R2->R1
R2(config-crypto-map)#match address 100
R2(config-crypto-map)#

```

Copy

Paste

7. Aplicar el mapa criptográfico

En esta última fase, se aplica el mapa criptográfico a la interfaz que conecta hacia la red pública. Con el comando interface GigabitEthernet se accede a la interfaz externa y se aplica crypto map IPSEC-MAP. Esto activa la funcionalidad de IPSec en esa interfaz. A partir de ese momento, todo el tráfico que pase por dicha interfaz será evaluado según el crypto map, y si coincide con la ACL configurada, será cifrado automáticamente.

Router 01

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

```

Copy

Paste

Router 02

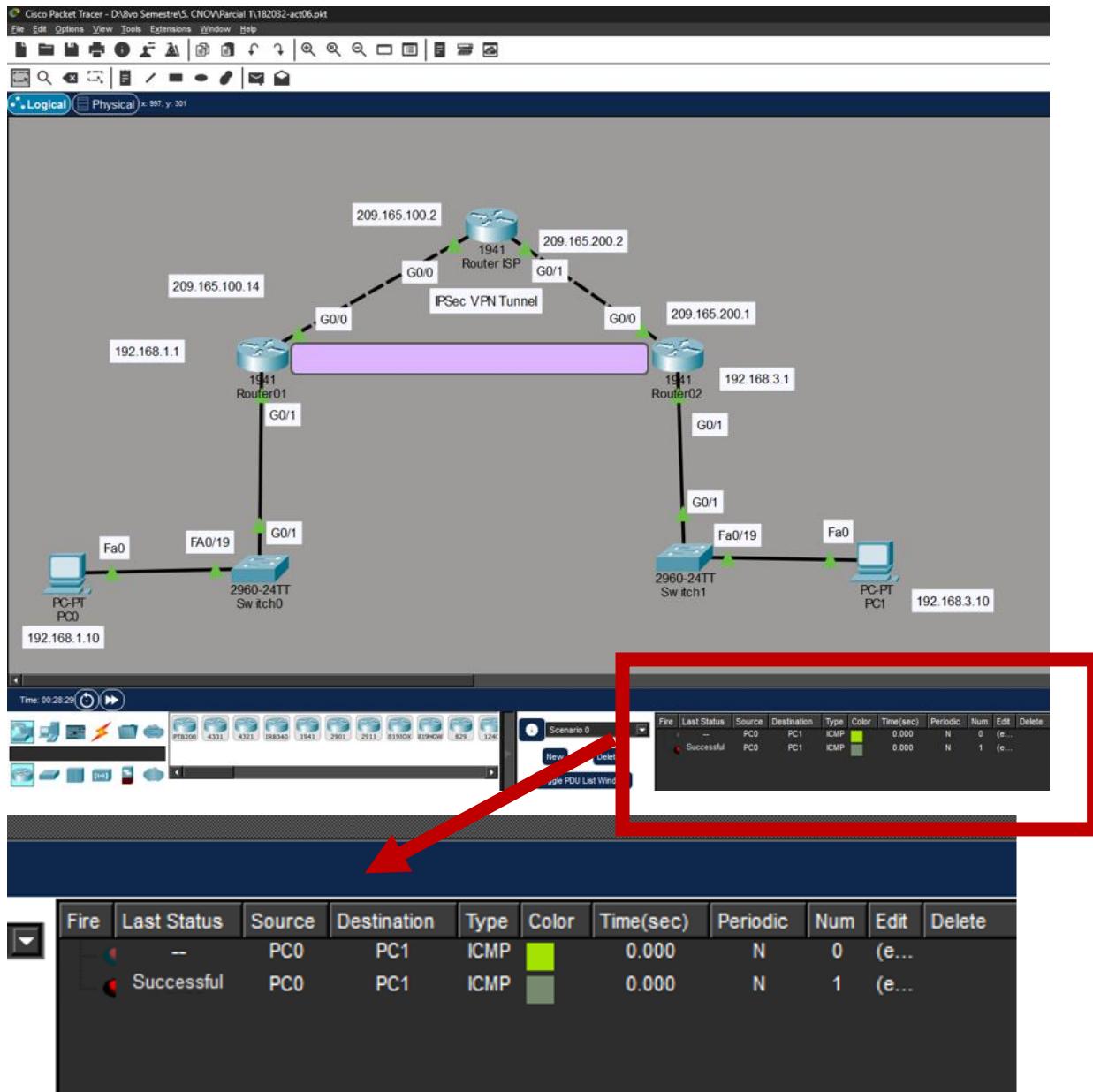
```
R2(config-crypto-map)#match address 100
R2(config-crypto-map)#
R2(config-crypto-map)#exit
R2(config)#int G0/0
R2(config-if)#crypto map IPSEC-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R2(config-if)#

```

Copy

Paste

Resultado final



Conclusión

En resumen, aplicar la VPN IPSec Tunnel en la topología propuesta, la seguridad en una red de tráfico de información necesita de una configuración ordenada y coherente en cada etapa. Primero se estableció el direccionamiento IP y las rutas estáticas para asegurar la conectividad básica. Después se habilitó la licencia SecurityK9 para activar las funciones criptográficas necesarias. Las ACL definieron el tráfico interesante que sería protegido, evitando cifrar información innecesaria.

En la Phase 01, la política ISAKMP permitió negociar los parámetros de seguridad como el cifrado AES 256, la autenticación pre-share y el grupo Diffie-Hellman 5, creando la Security Association inicial. En la Phase 2, el transform-set con ESP, AES 256 y SHA-HMAC garantizó la confidencialidad e integridad de los datos. El crypto map integró todos estos elementos y, al aplicarlo en la interfaz externa, se activó el túnel seguro.

Todo lo realizado con anterioridad puede ser usado, si no es que muchas empresas ya lo aplican, por compañías, organizaciones que conectan departamentos de forma remota o cualquier entorno que necesite proteger información a través de Internet. Al seguir correctamente cada paso y mantener coherencia en ambos routers, se logró establecer una conexión segura y funcional entre las dos redes privadas, asegurando autenticación, integridad y confidencialidad en la comunicación.