FEBRUARY 16, 2026

IMPLEMENTACIÓN IPSEC VPN

ACTIVIDAD 6

BRUNO AXEL PUENTE LUNA 177876
UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Contenido

Introducción

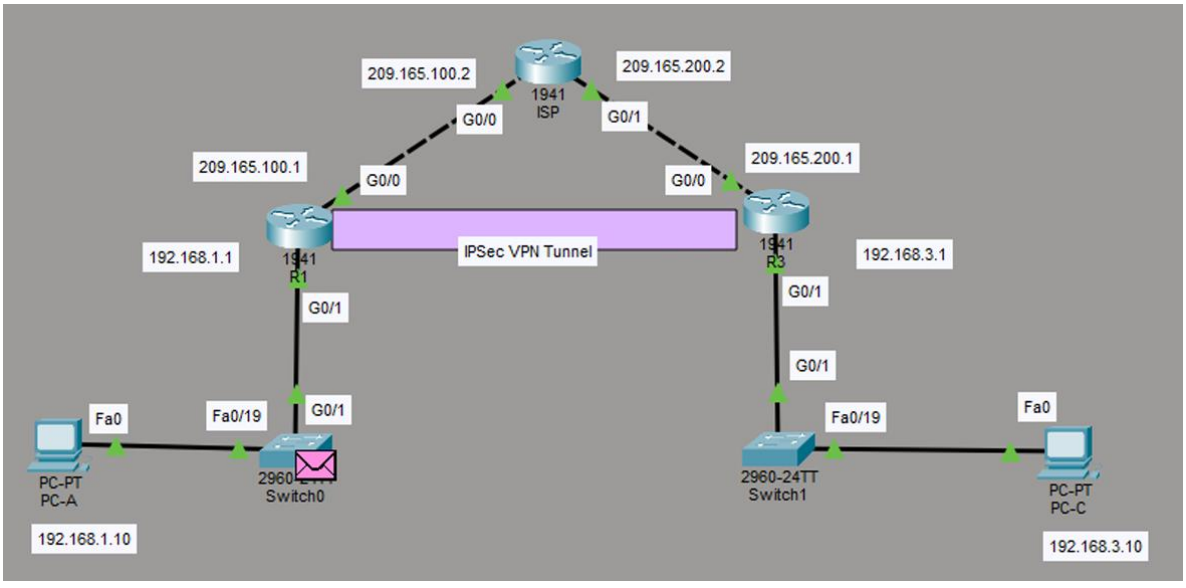
La protección de datos en redes públicas suele ser complicado por el libre acceso a este tipo de redes, los datos pueden ser modificados y/o suplantados durante su tránsito. Una opción para la protección de estos es IPSec (Internet Protocol Security), un conjunto de protocolos que opera en la capa de 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

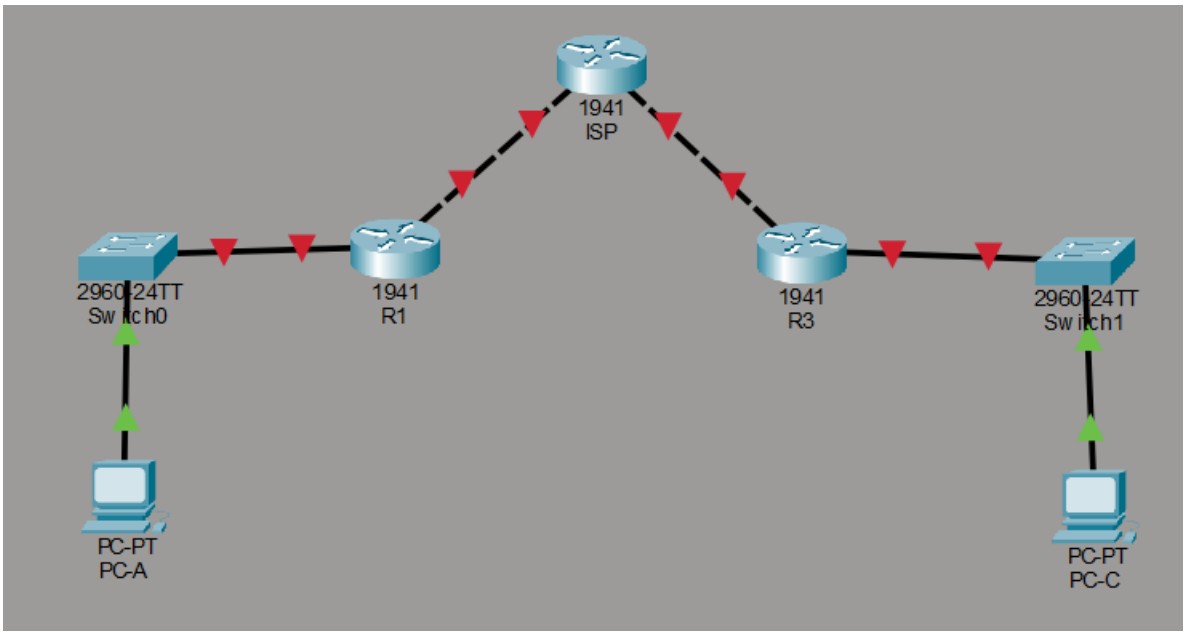
Gateway: 192.168.1.1

PC-C

IP: 192.168.3.10

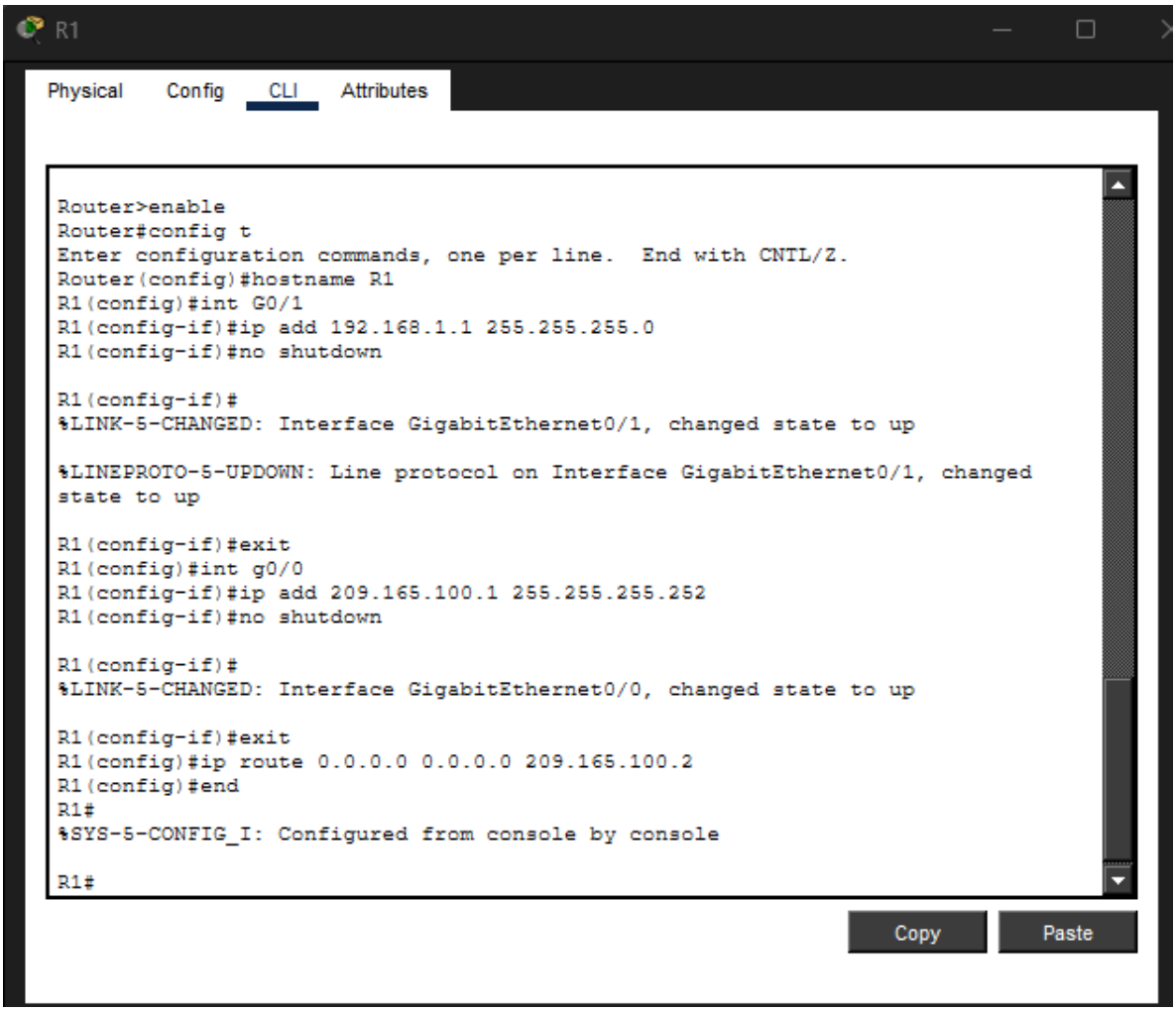
Mask: 255.255.255.0

Gateway: 192.168.3.1



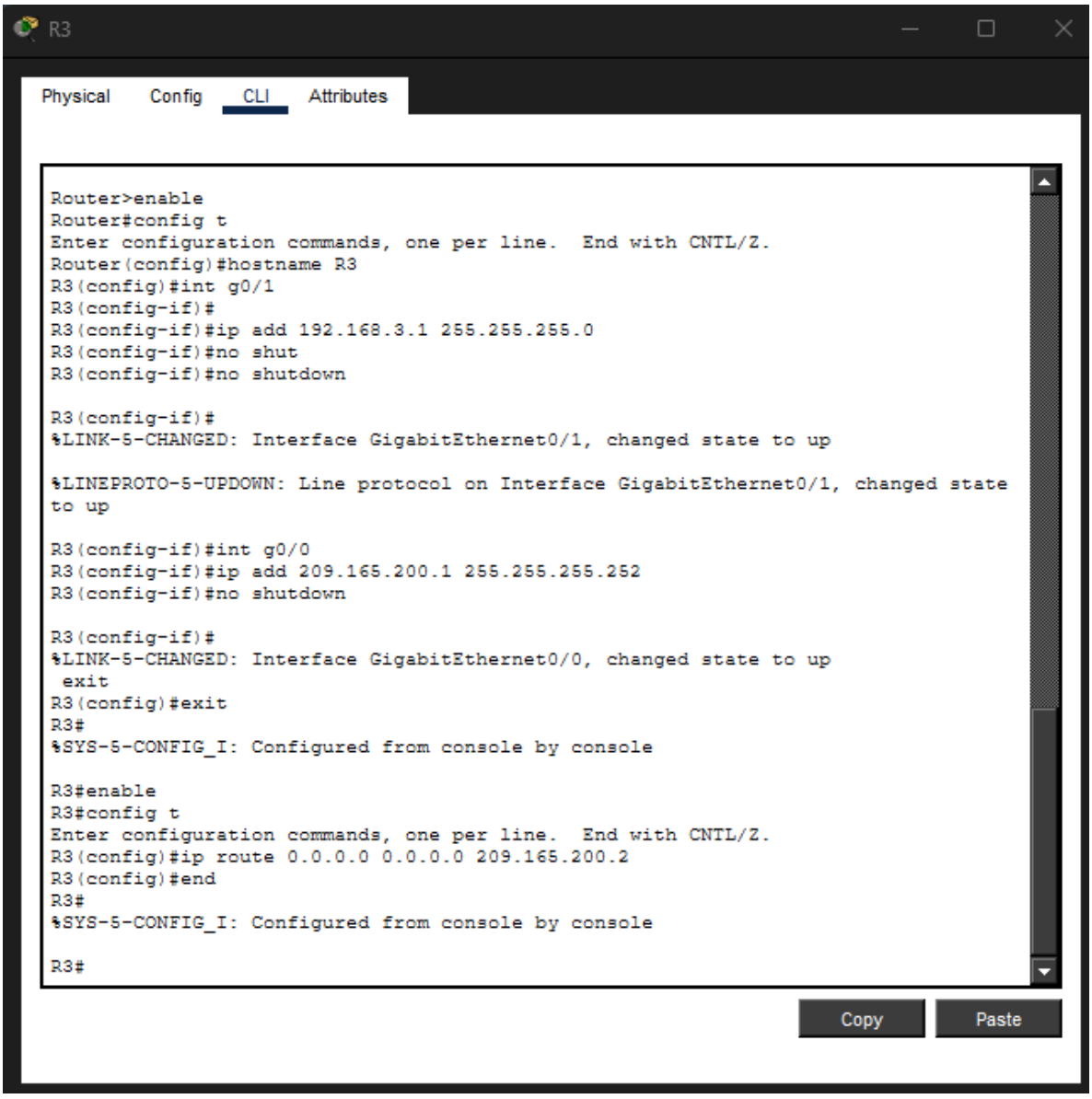
Proseguimos configurando el Router 1, con los siguientes comandos, esto para indicar las direcciones de entrada y salida, creando un correcto direccionamiento:

- 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



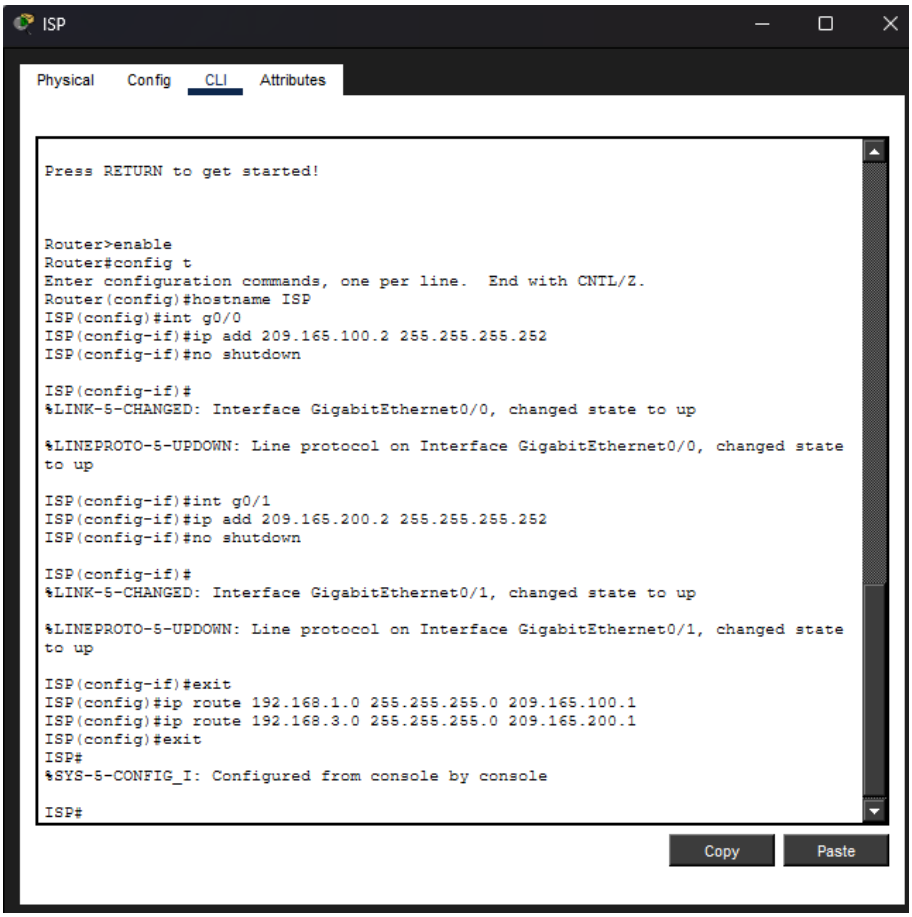
Se realizaron los mismos pasos para R3:

- 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

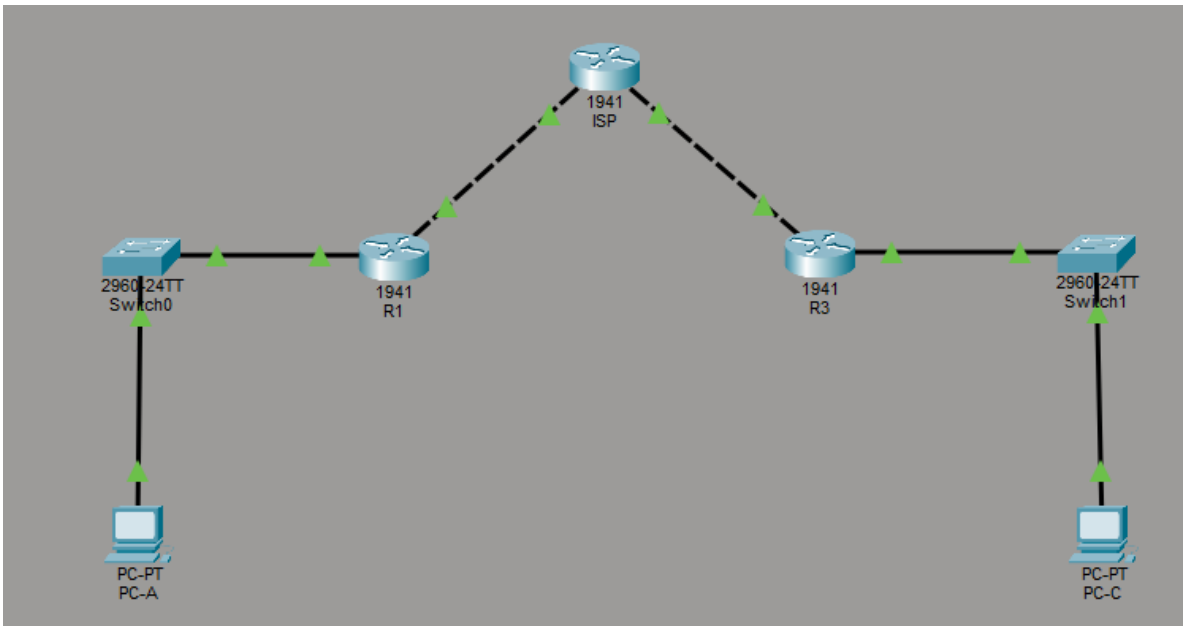


Después se realizó la configuración para el ISP, el cual cuenta con comandos similares:

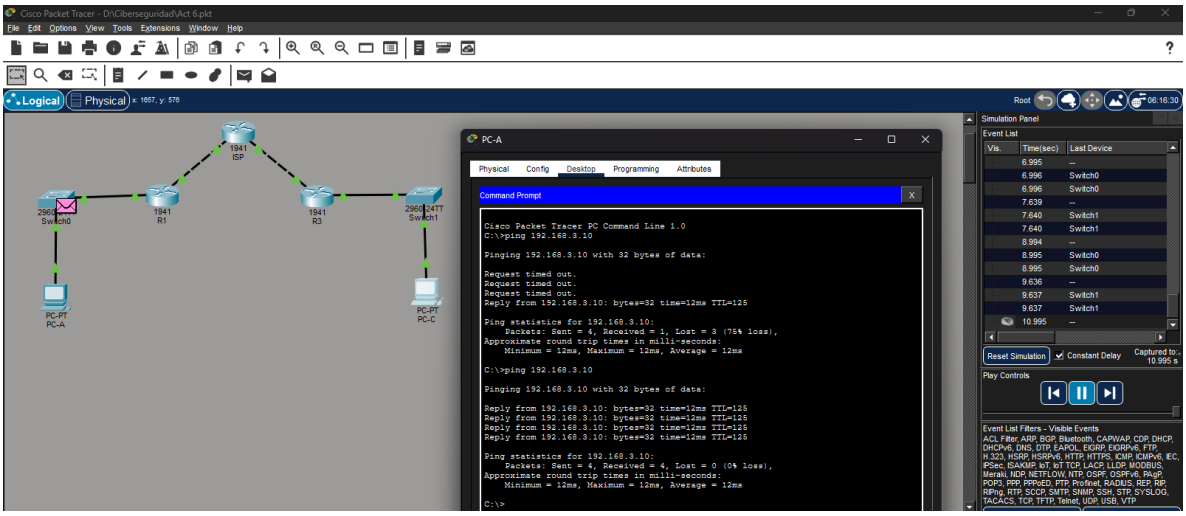
- Enable
- config t
- hostname ISP
- int g0/0
- ip add 209.165.100.2 255.255.255.252
- no shutdown
- int g0/1
- ip add 209.165.200.2 255.255.255.252
- no shutdown
- exit
- ip route 192.168.1.0 255.255.255.0 209.165.100.1
- ip route 192.168.3.0 255.255.255.0 209.165.200.1



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.



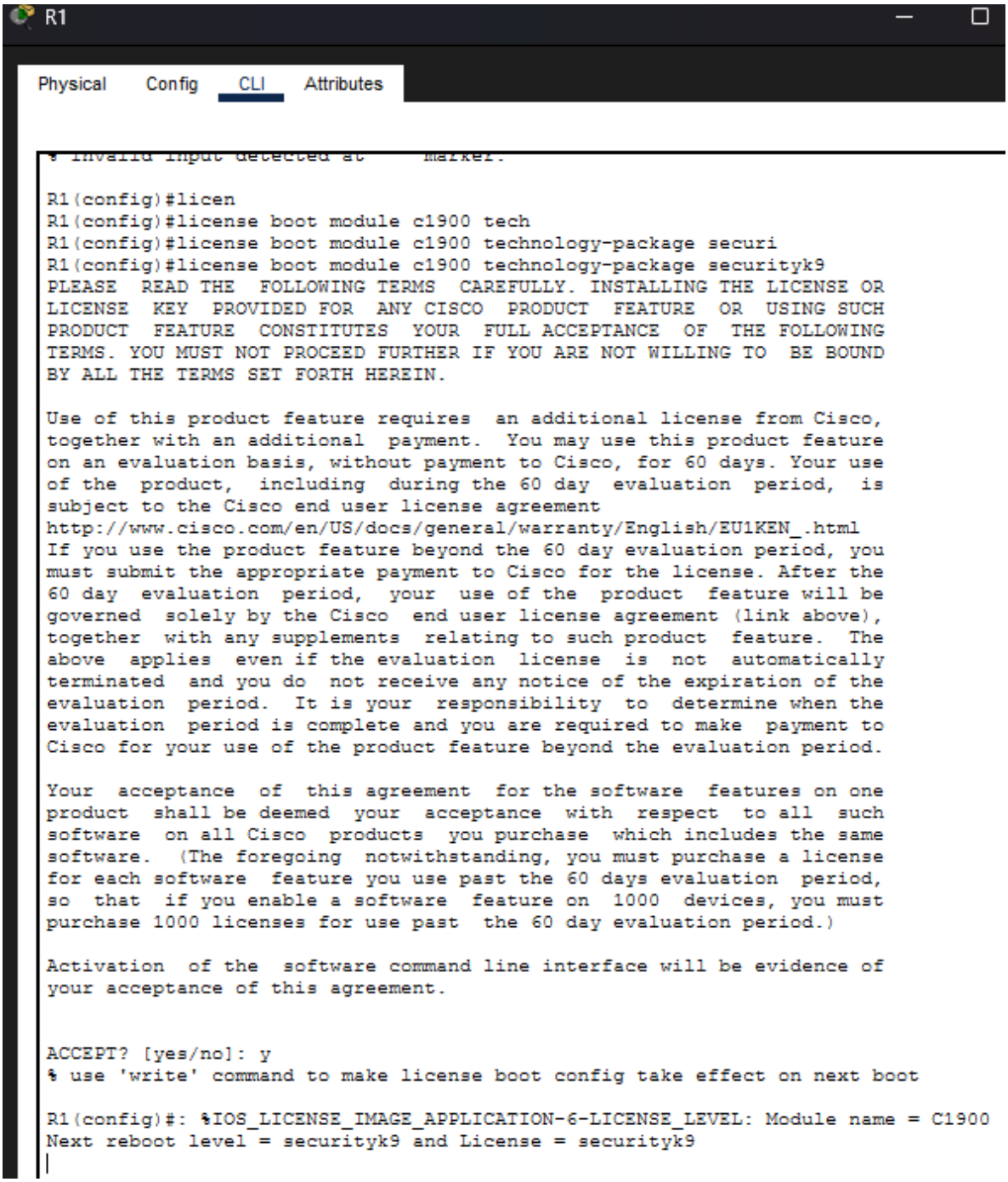
Con la topología concluida, avanzamos al siguiente paso que es habilitar las licencias de seguridad.

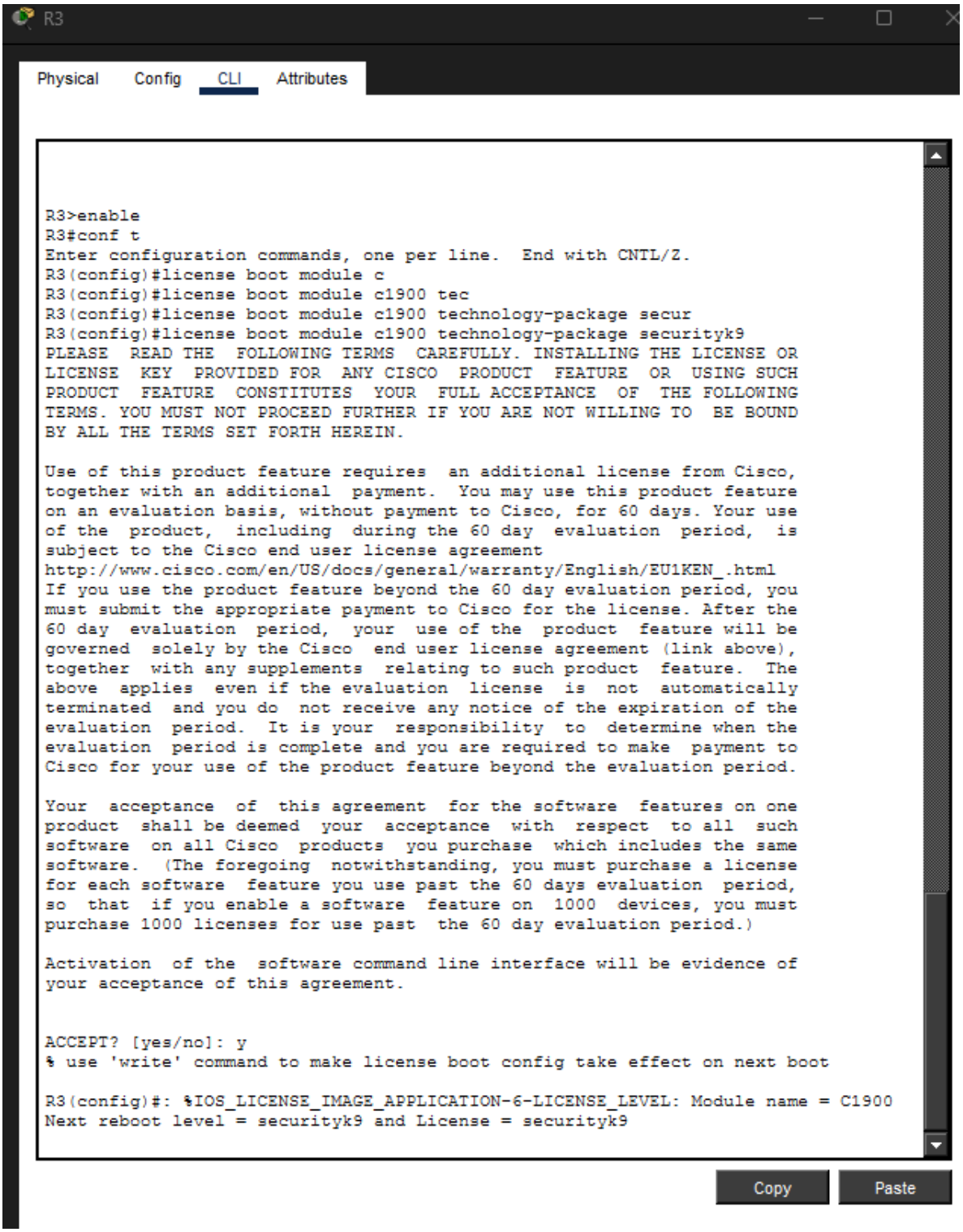
Habilitar licencia de seguridad

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

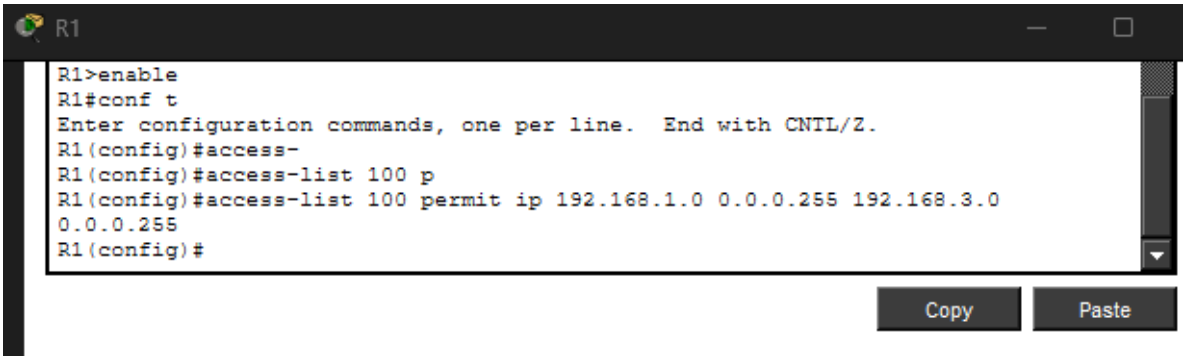

R3
Physical
Config
CLI
Attributes
R3>enable
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#license boot module c
R3(config)#license boot module c1900 tec
R3(config)#license boot module c1900 technology-package secur
R3(config)#license boot module c1900 technology-package 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

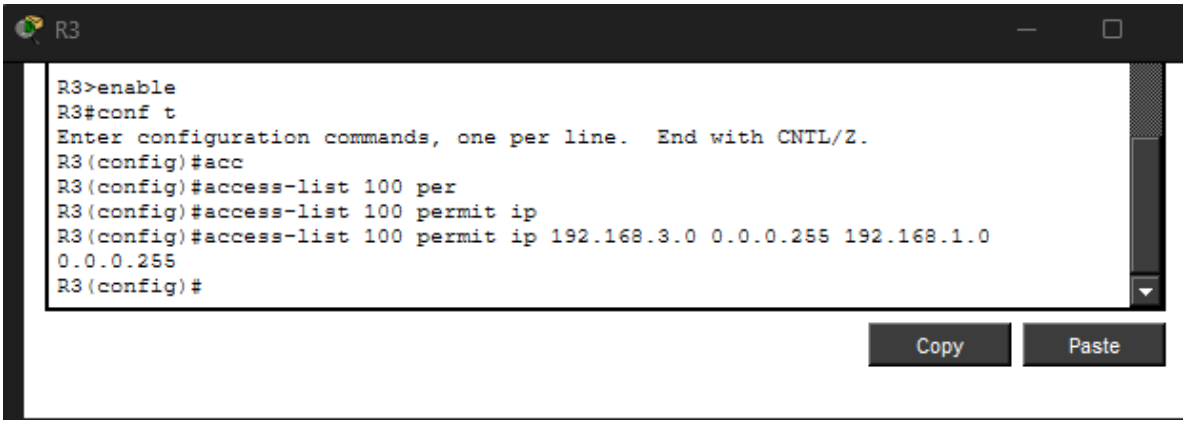
Trafico interesante

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



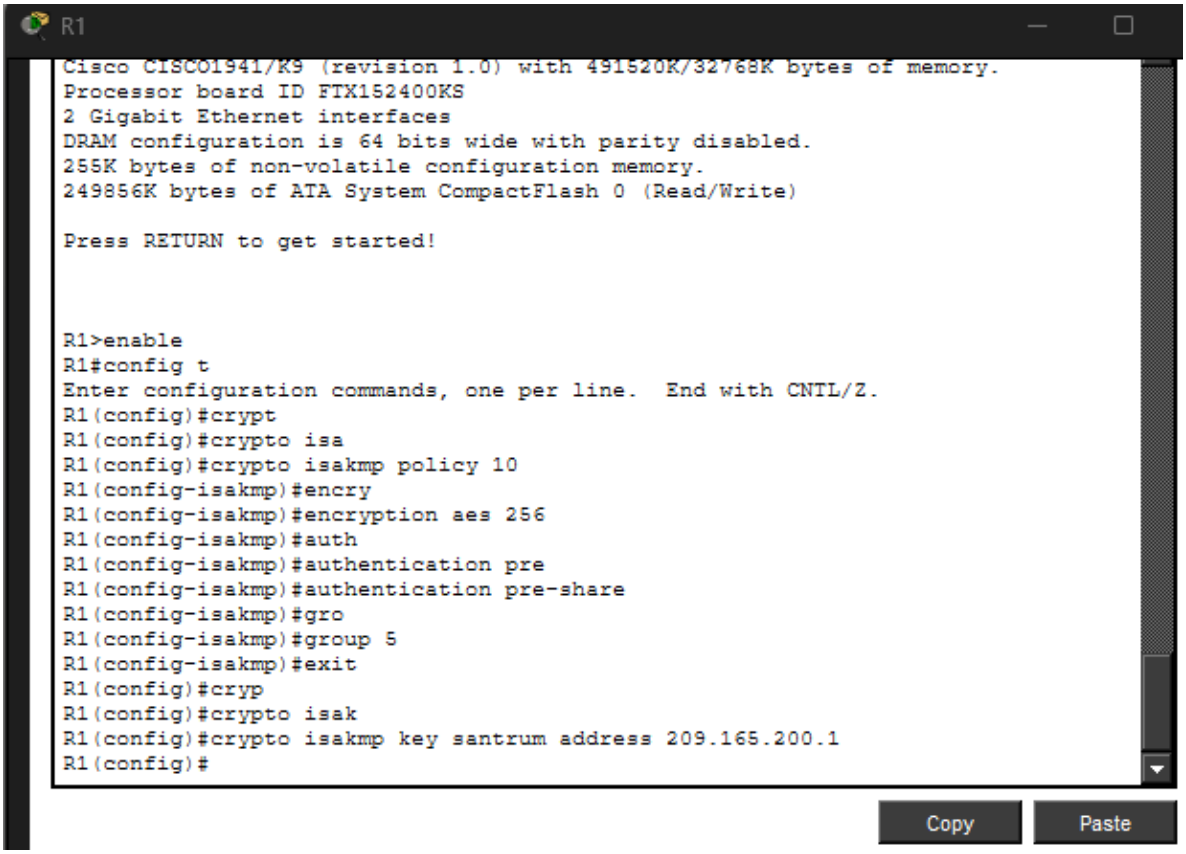


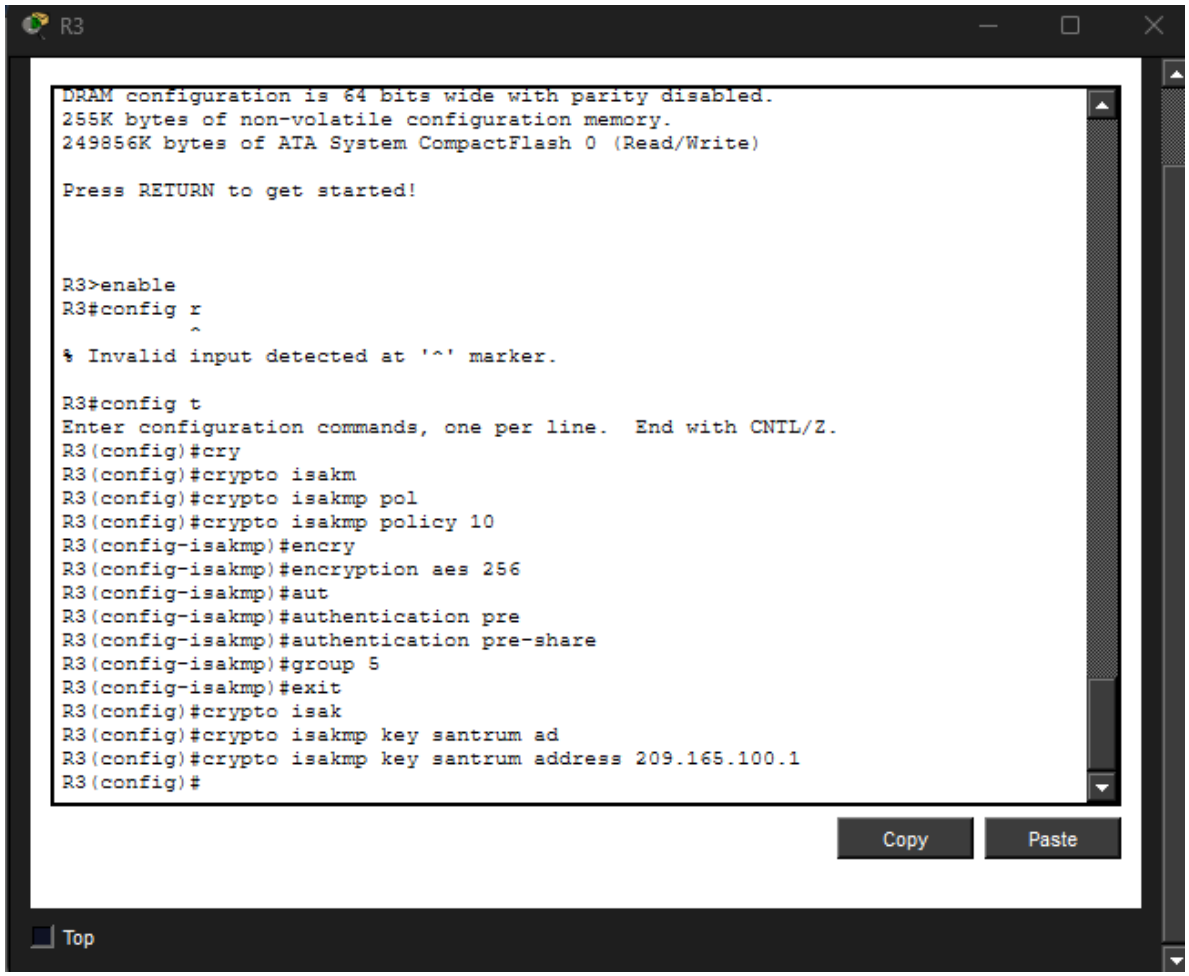
FASE 1 – ISAKMP (negociación)

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



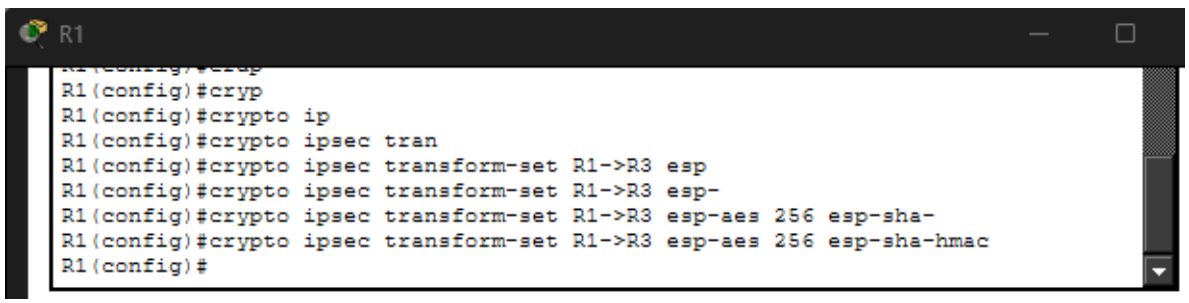


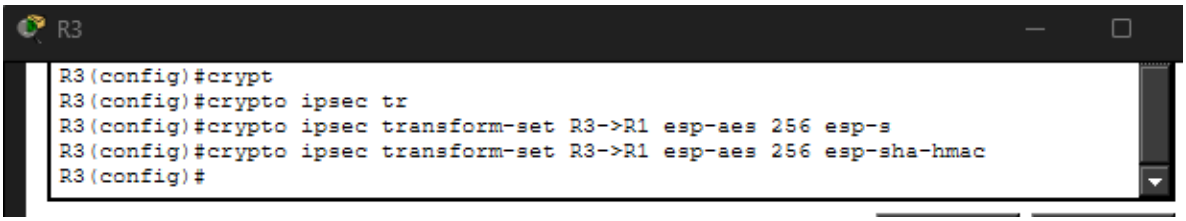
FASE 2 – Transform Set (cómo se protegerán los datos)

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



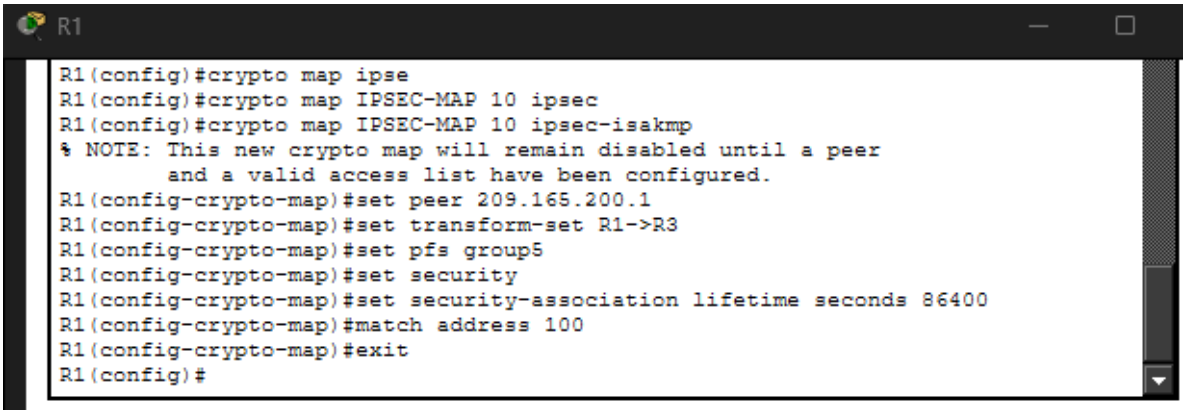


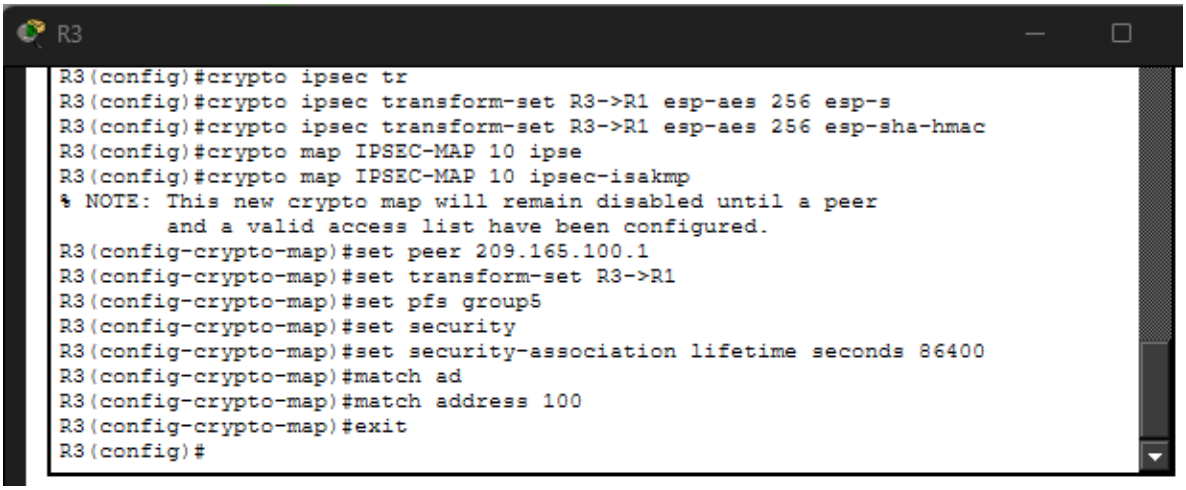
FASE 3 – Crypto Map

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



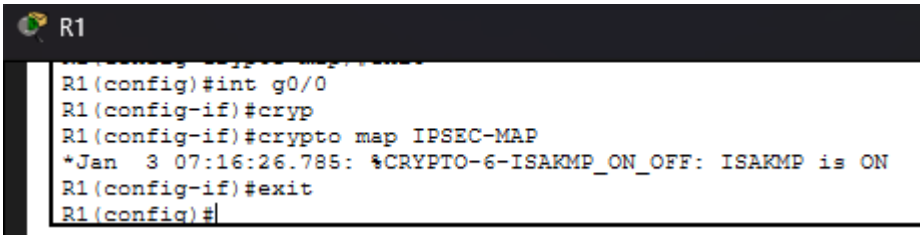


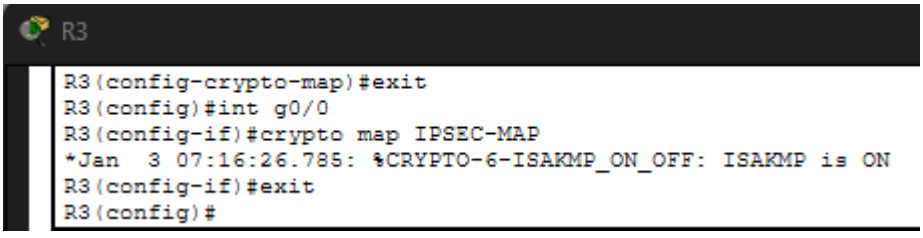
FASE 4 – Aplicar a la interfaz WAN (la que va al ISP)

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.

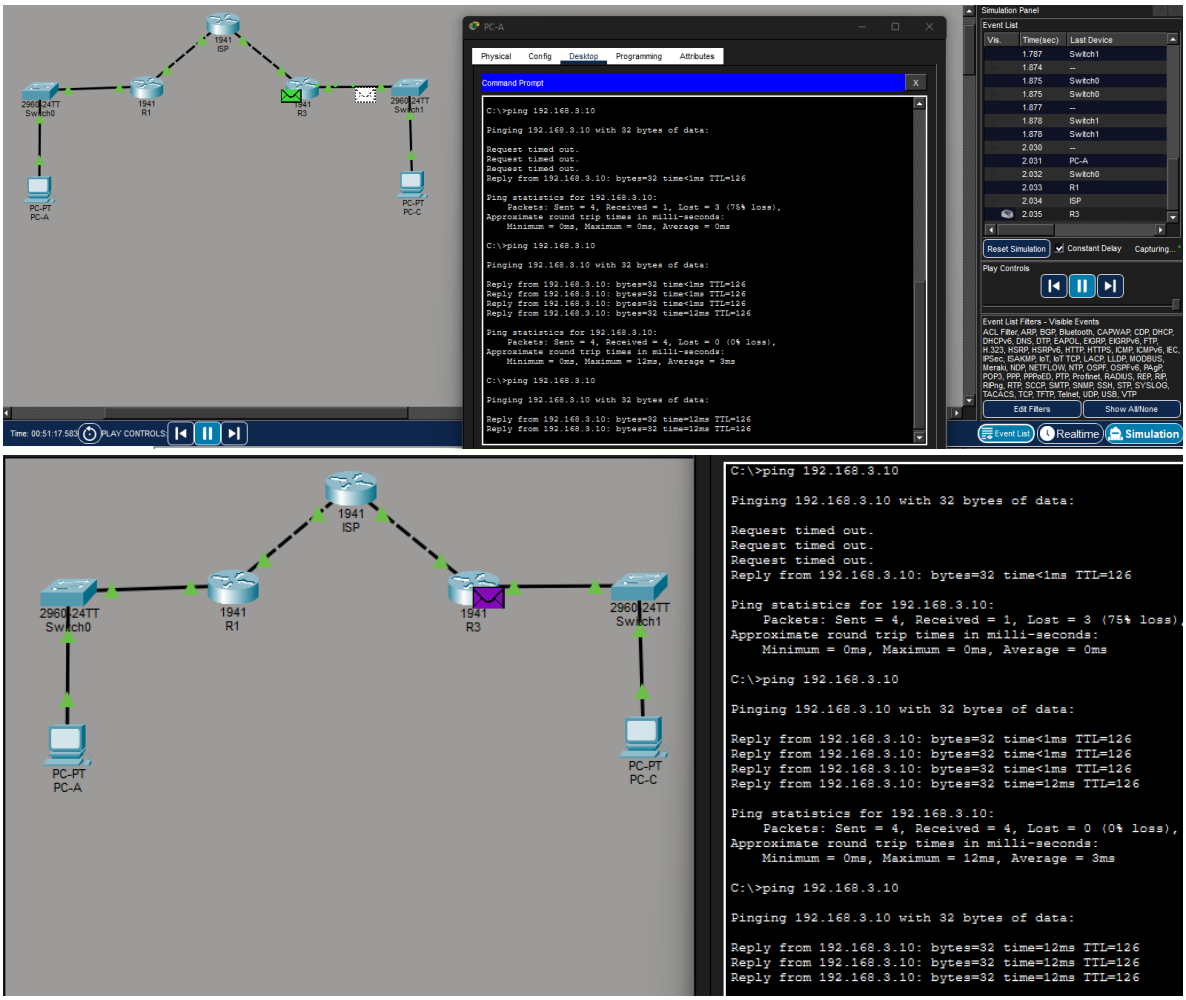
Se implementaron en cada interfaz con los siguientes comandos (Con variantes en cada IP del dispositivo a configurar):

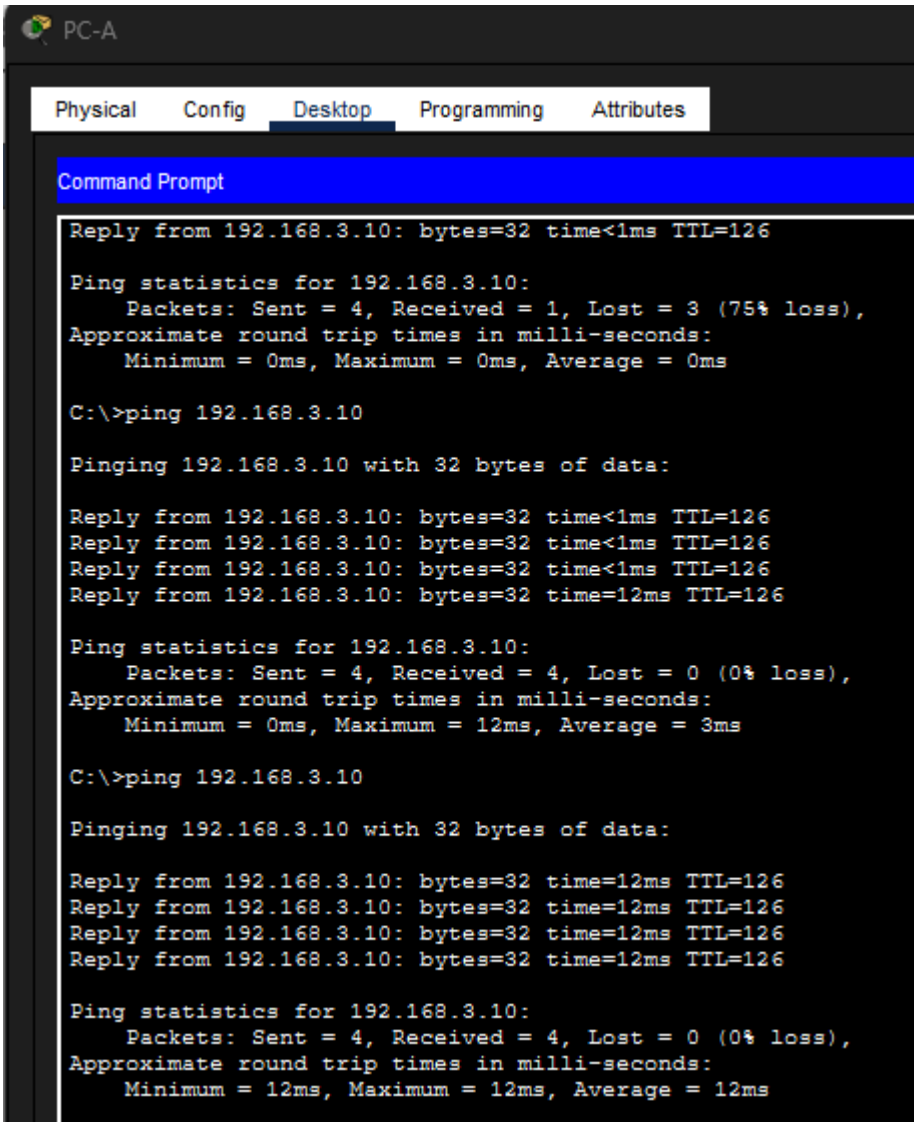
- interface g0/0
- crypto map IPSEC-MAP
- exit





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.





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.