UNIVERSIDAD POLITÉCNICA
DE SAN LUIS POTOSÍ

Actividad 06

Implementación IPSec VPN

Alan Gilberto Sánchez Zavala

177263

Universidad Politécnica de
San Luis Potosi

Ciberseguridad

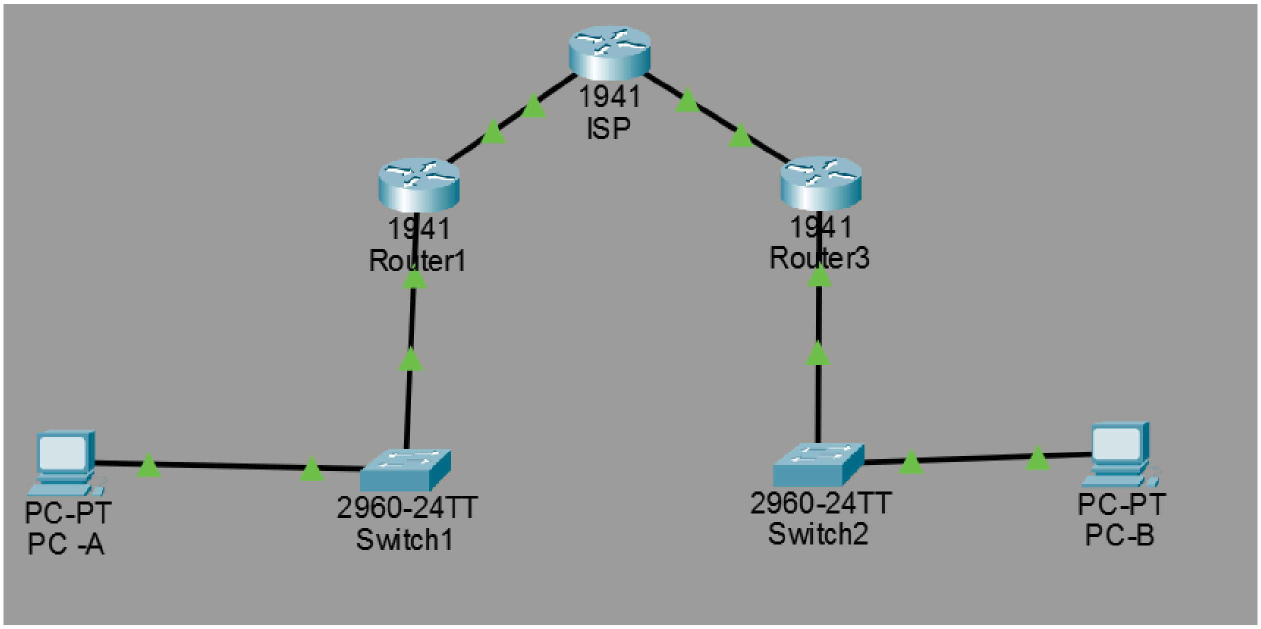
Contents

Introducción

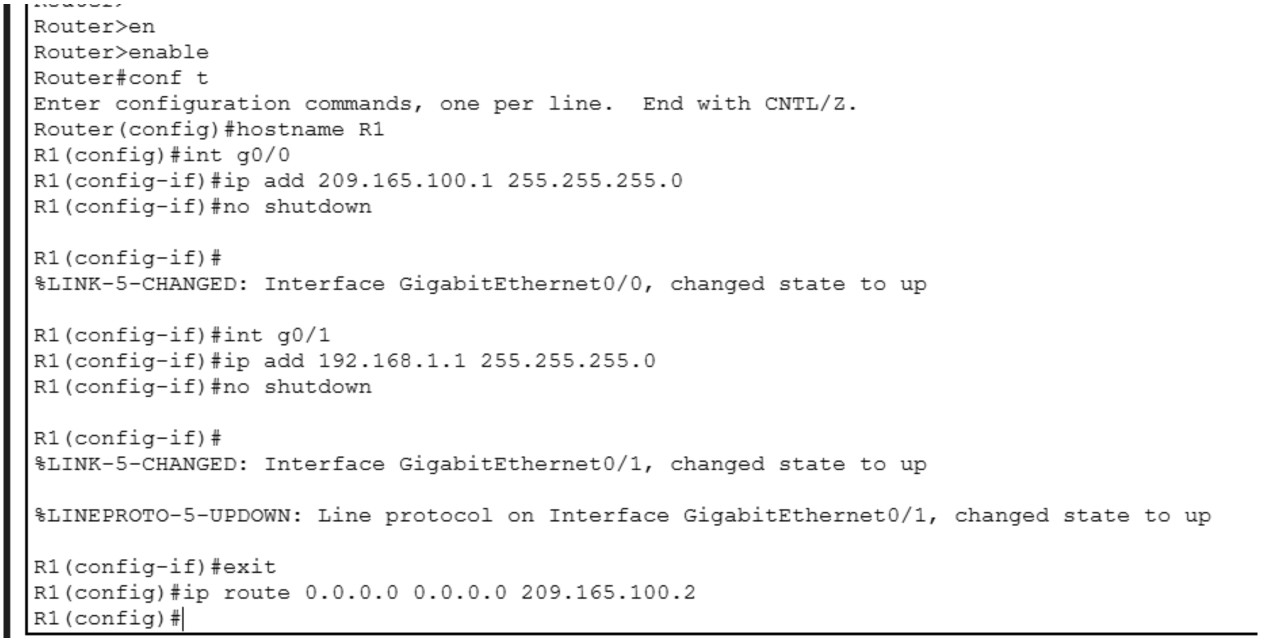
La interconectividad de redes a través de infraestructuras públicas como Internet plantea desafíos críticos de seguridad, especialmente cuando se trata de comunicar sucursales geográficamente distantes que manejan datos sensibles. Una de las soluciones más robustas para este problema es la implementación de Redes Privadas Virtuales (VPN) punto a punto utilizando el protocolo IPSec (Internet Protocol Security).

En esta actividad, se ha diseñado una topología que simula una conexión empresarial donde dos redes locales (LAN) se comunican a través de un router ISP. El objetivo principal es la configuración del protocolo ISAKMP (Internet Security Association and Key Management Protocol) para establecer una asociación de seguridad (SA) que permita el cifrado de datos mediante algoritmos avanzados como AES-256. Esta configuración asegura que el tráfico entre los dispositivos finales sea invisible para actores externos, garantizando la integridad, confidencialidad y autenticidad de la información

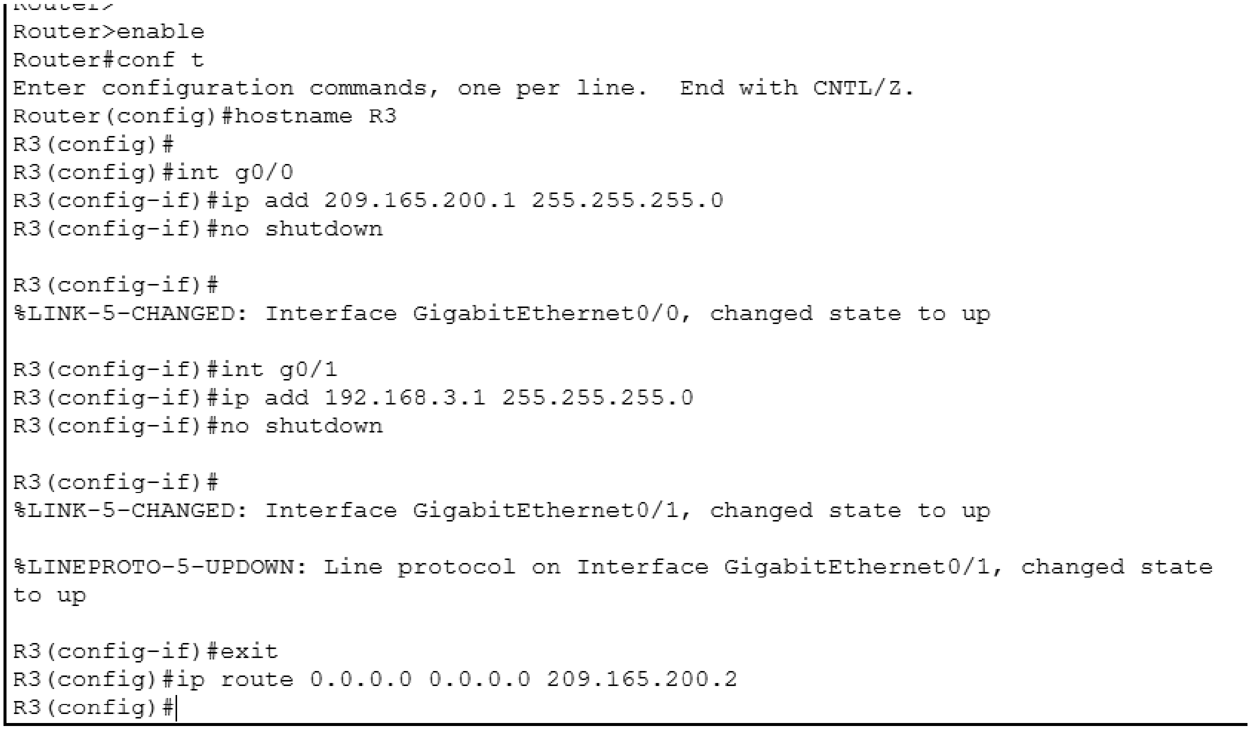
Desarrollo



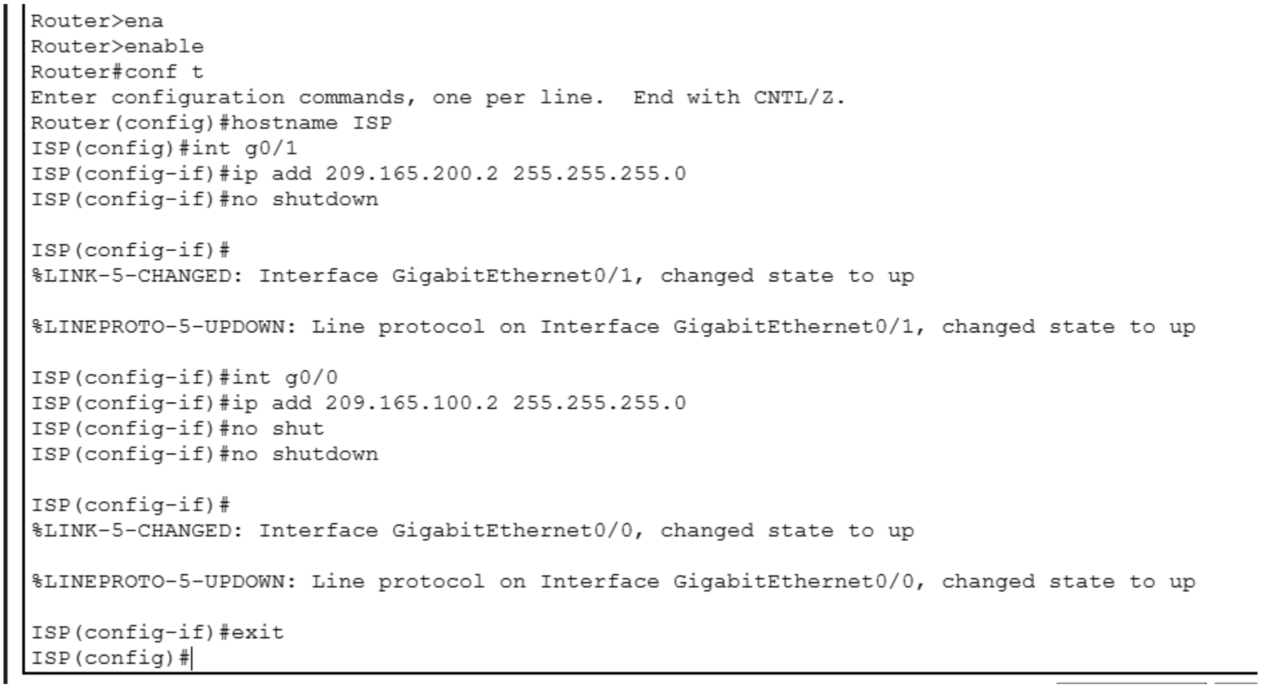
Configuración de las interfaces y la ruta predeterminada



```
Router>en
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#int g0/0
R1(config-if)#ip add 209.165.100.1 255.255.255.0
R1(config-if)#no shutdown

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

R1(config-if)#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)#ip route 0.0.0.0 0.0.0.0 209.165.100.2
R1(config)#
```

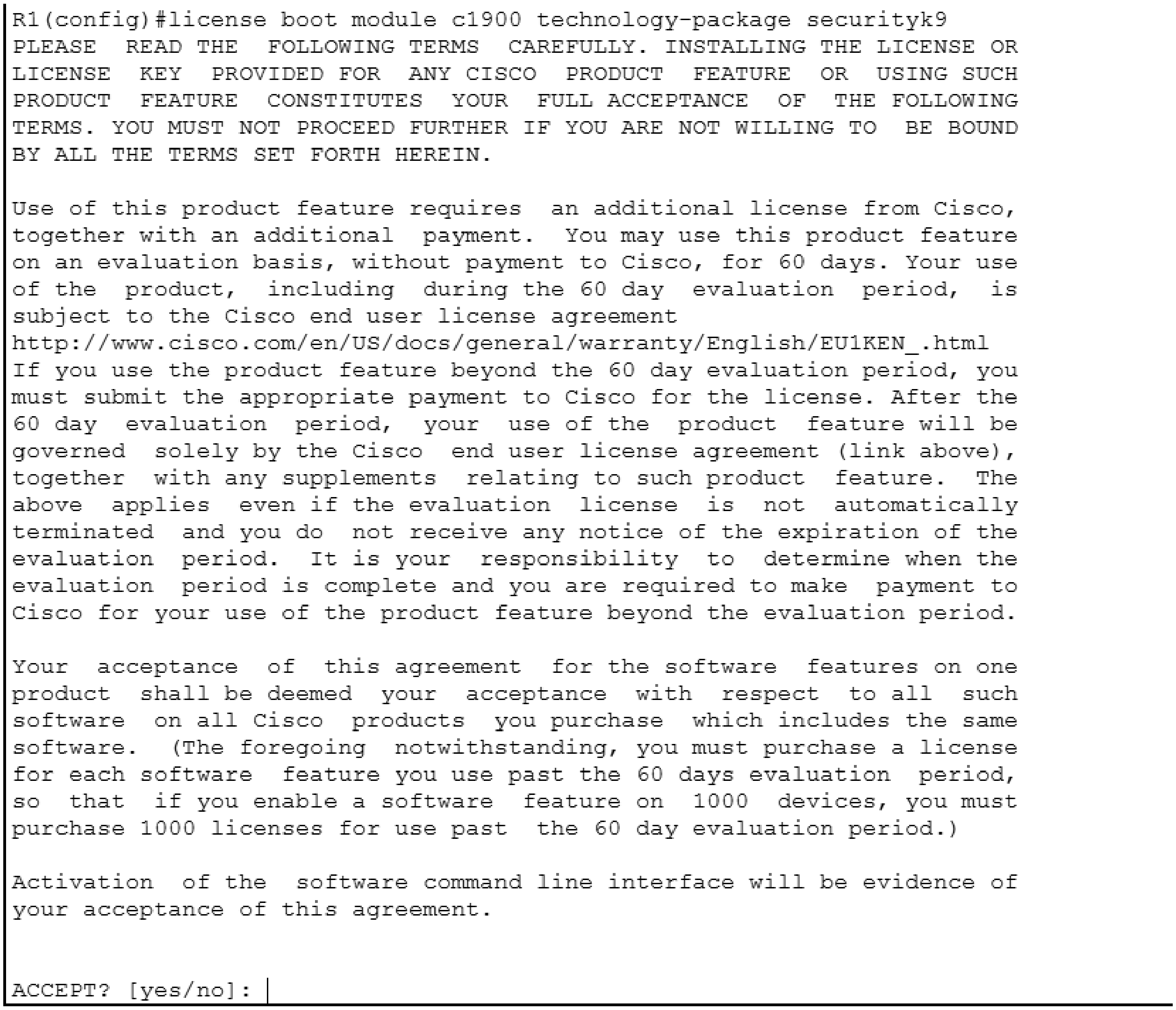


```
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R3
R3(config)#
R3(config)#int g0/0
R3(config-if)#ip add 209.165.200.1 255.255.255.0
R3(config-if)#no shutdown

R3(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

R3(config-if)#int g0/1
R3(config-if)#ip add 192.168.3.1 255.255.255.0
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)#exit
R3(config)#ip route 0.0.0.0 0.0.0.0 209.165.200.2
R3(config)#
```

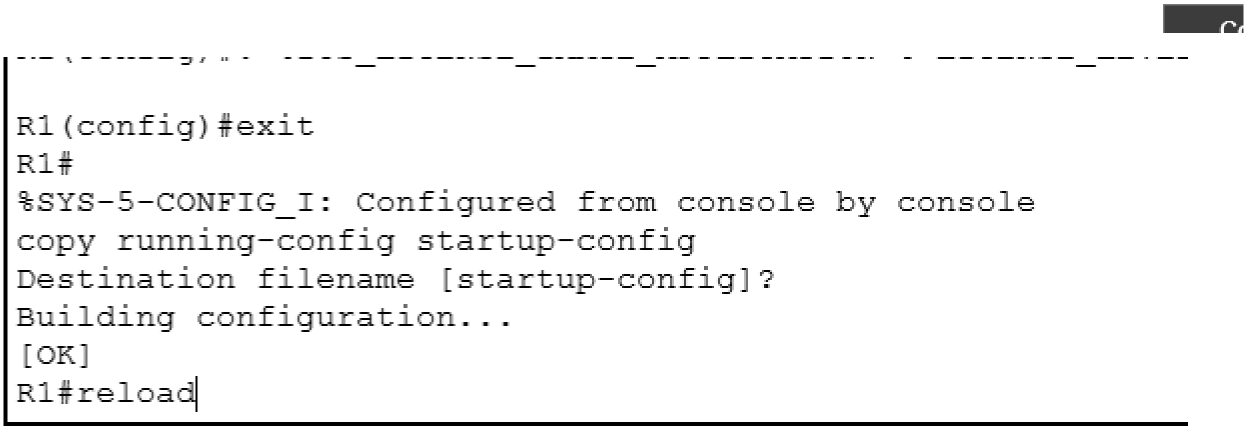


```
Router>ena
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname ISP
ISP(config)#int g0/1
ISP(config-if)#ip add 209.165.200.2 255.255.255.0
ISP(config-if)#no shutdown

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)#int g0/0
ISP(config-if)#ip add 209.165.100.2 255.255.255.0
ISP(config-if)#no shut
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)#exit
ISP(config)#
```

Activar el paquete de tecnología securityk9, Para habilitar los comandos de seguridad (crypto isakmp, crypto map, etc.)



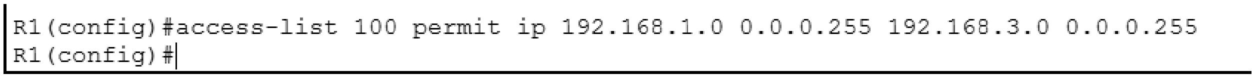
```
R1(config)#license boot module c1900 technology-package securityk9
PLEASE  READ THE  FOLLOWING TERMS  CAREFULLY. INSTALLING THE LICENSE OR
LICENSE  KEY  PROVIDED FOR  ANY CISCO  PRODUCT  FEATURE  OR  USING SUCH
PRODUCT  FEATURE  CONSTITUTES  YOUR  FULL ACCEPTANCE  OF  THE FOLLOWING
TERMS. YOU MUST 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]:
```



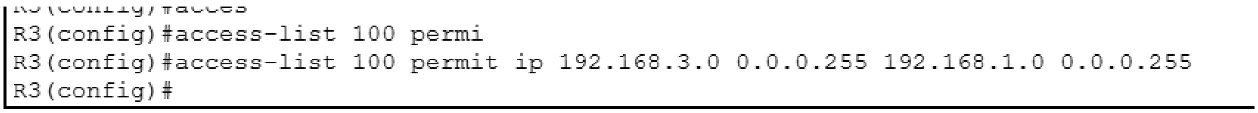
```
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#reload
```

Hacerlo en R1y R3

Lista de acceso

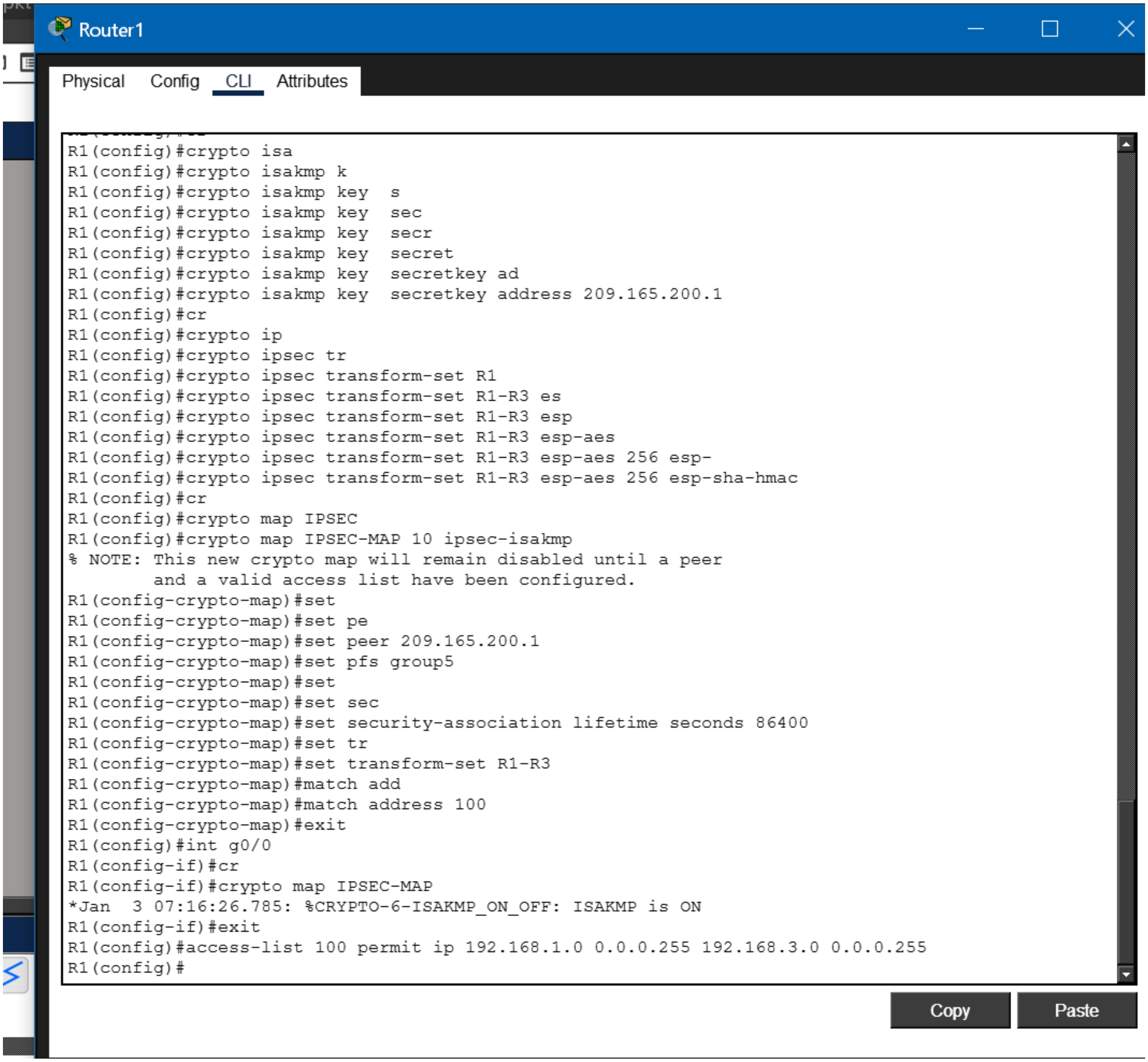


```
R1(config)#access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
R1(config)#
```

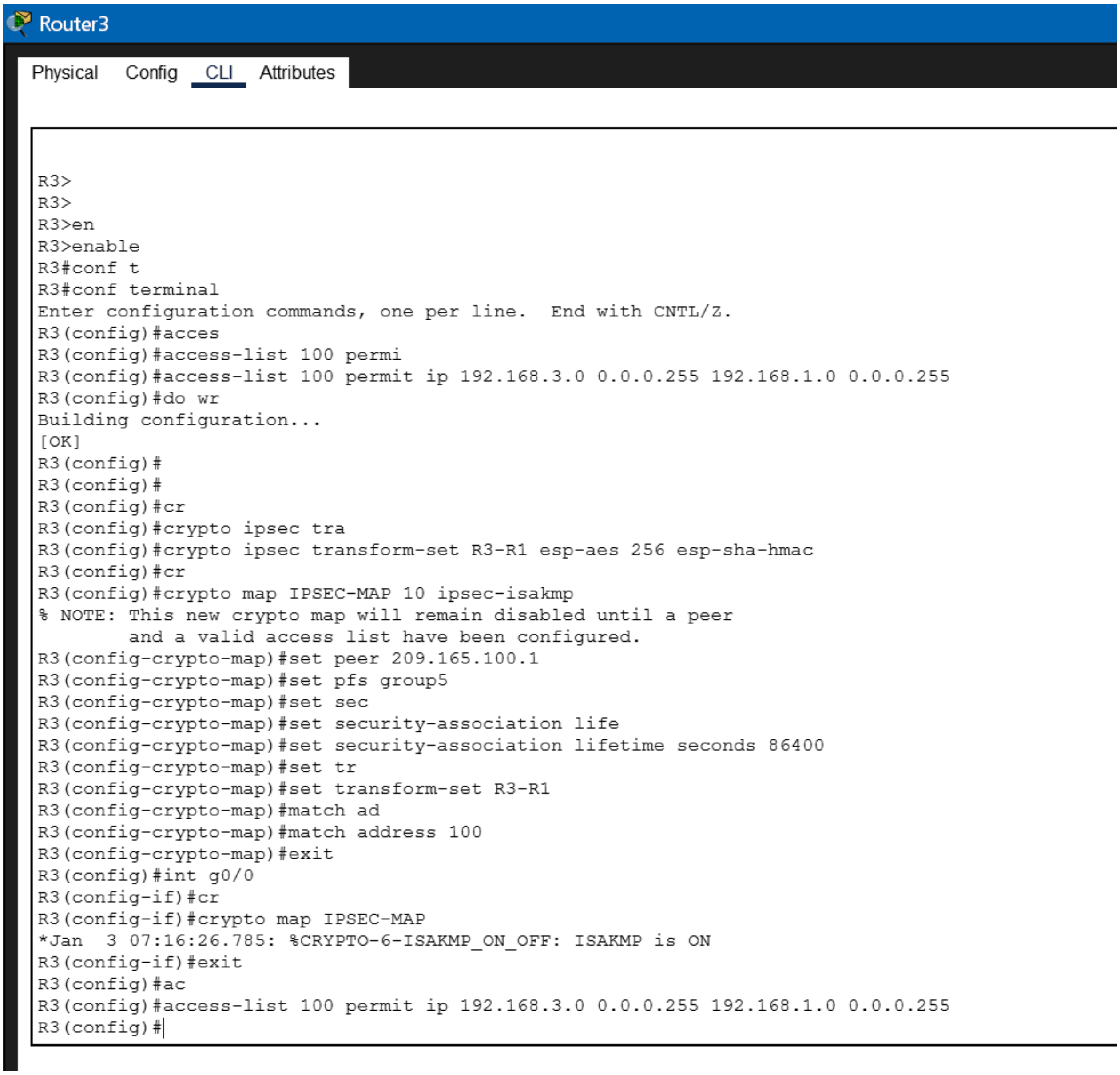


```
R3(config)#acces
R3(config)#access-list 100 permi
R3(config)#access-list 100 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
R3(config)#
```

Configuracion de llave, el transform-set, el crypto map y la ACL



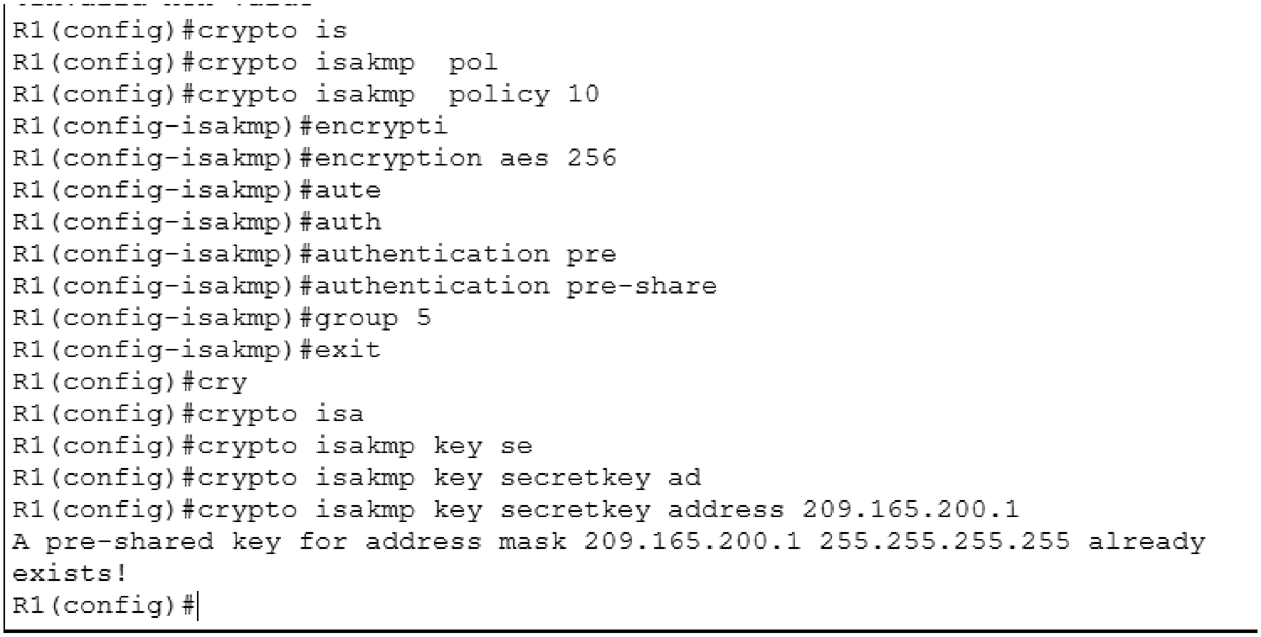
```
R1(config)#cr
R1(config)#crypto isa
R1(config)#crypto isakmp k
R1(config)#crypto isakmp key  s
R1(config)#crypto isakmp key  sec
R1(config)#crypto isakmp key  secr
R1(config)#crypto isakmp key  secret
R1(config)#crypto isakmp key  secretkey ad
R1(config)#crypto isakmp key  secretkey address 209.165.200.1
R1(config)#cr
R1(config)#crypto ip
R1(config)#crypto ipsec tr
R1(config)#crypto ipsec transform-set R1
R1(config)#crypto ipsec transform-set R1-R3 es
R1(config)#crypto ipsec transform-set R1-R3 esp
R1(config)#crypto ipsec transform-set R1-R3 esp-aes
R1(config)#crypto ipsec transform-set R1-R3 esp-aes 256 esp-
R1(config)#crypto ipsec transform-set R1-R3 esp-aes 256 esp-sha-hmac
R1(config)#cr
R1(config)#crypto map 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
R1(config-crypto-map)#set pe
R1(config-crypto-map)#set peer 209.165.200.1
R1(config-crypto-map)#set pfs group5
R1(config-crypto-map)#set
R1(config-crypto-map)#set sec
R1(config-crypto-map)#set security-association lifetime seconds 86400
R1(config-crypto-map)#set tr
R1(config-crypto-map)#set transform-set R1-R3
R1(config-crypto-map)#match add
R1(config-crypto-map)#match address 100
R1(config-crypto-map)#exit
R1(config)#int g0/0
R1(config-if)#cr
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 0.0.0.255 192.168.3.0 0.0.0.255
R1(config)#
```



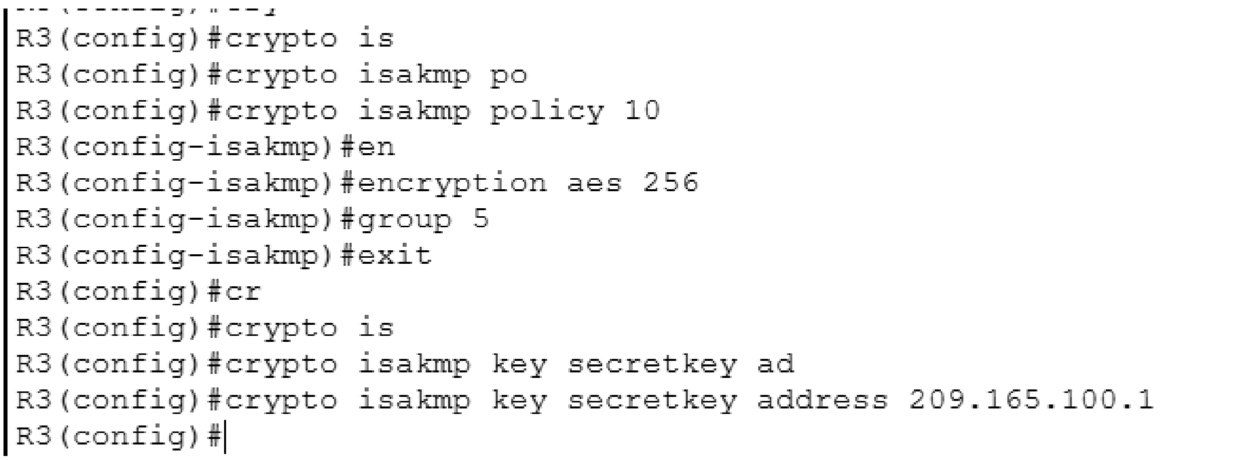
```
R3>
R3>
R3>en
R3>enable
R3#conf t
R3#conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#acces
R3(config)#access-list 100 permi
R3(config)#access-list 100 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
R3(config)#do wr
Building configuration...
[OK]
R3(config)#
R3(config)#
R3(config)#cr
R3(config)#crypto ipsec tra
R3(config)#crypto ipsec transform-set R3-R1 esp-aes 256 esp-sha-hmac
R3(config)#cr
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 sec
R3(config-crypto-map)#set security-association life
R3(config-crypto-map)#set security-association lifetime seconds 86400
R3(config-crypto-map)#set tr
R3(config-crypto-map)#set transform-set R3-R1
R3(config-crypto-map)#match ad
R3(config-crypto-map)#match address 100
R3(config-crypto-map)#exit
R3(config)#int g0/0
R3(config-if)#cr
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)#ac
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)#
```

Hacerlo en R1 y R3.

Política ISAKMP

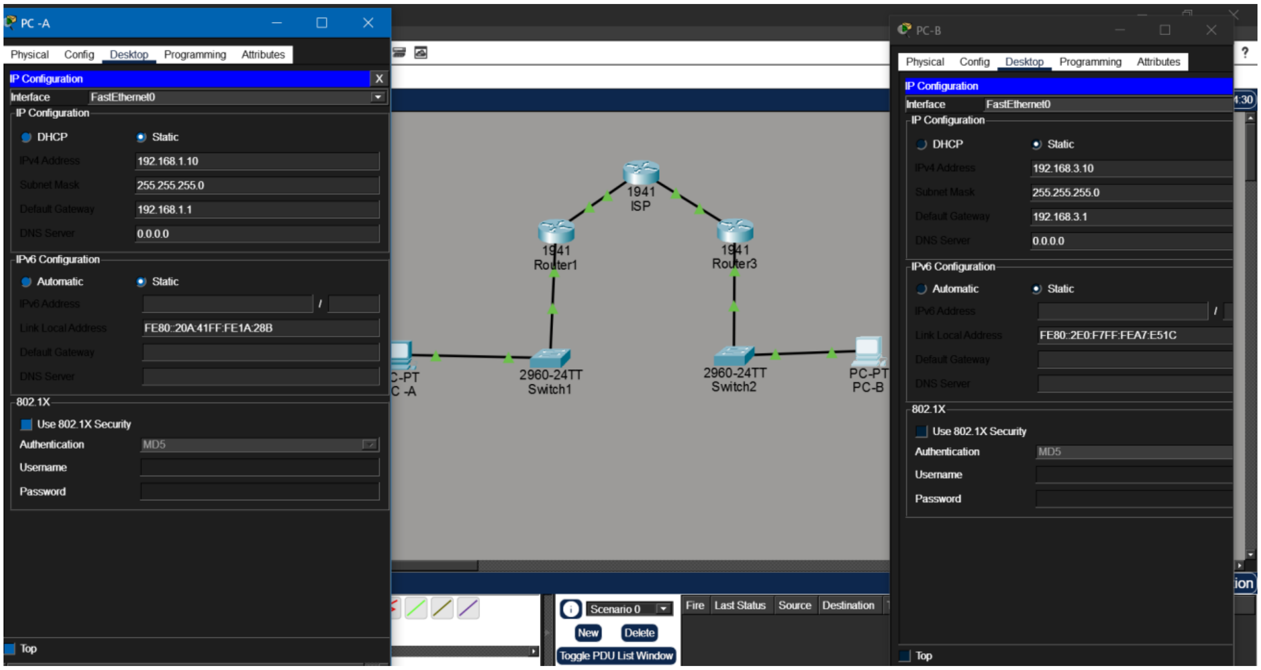


```
R1(config)#crypto is
R1(config)#crypto isakmp  pol
R1(config)#crypto isakmp  policy 10
R1(config-isakmp)#encrypti
R1(config-isakmp)#encryption aes 256
R1(config-isakmp)#aute
R1(config-isakmp)#auth
R1(config-isakmp)#authentication pre
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 5
R1(config-isakmp)#exit
R1(config)#cry
R1(config)#crypto isa
R1(config)#crypto isakmp key se
R1(config)#crypto isakmp key secretkey ad
R1(config)#crypto isakmp key secretkey address 209.165.200.1
A pre-shared key for address mask 209.165.200.1 255.255.255.255 already
exists!
R1(config)#
```



```
R3(config)#crypto is
R3(config)#crypto isakmp po
R3(config)#crypto isakmp policy 10
R3(config-isakmp)#en
R3(config-isakmp)#encryption aes 256
R3(config-isakmp)#group 5
R3(config-isakmp)#exit
R3(config)#cr
R3(config)#crypto is
R3(config)#crypto isakmp key secretkey ad
R3(config)#crypto isakmp key secretkey address 209.165.100.1
R3(config)#
```

Configuración ip



PC -A

Physical | Config | Desktop | Programming | Attributes

IP Configuration

Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address: 192.168.1.10
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.1.1
DNS Server: 0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /
Link Local Address: FE80::20A:41FF:FE1A:28B
Default Gateway:
DNS Server:

802.1X

□ Use 802.1X Security
Authentication: MD5
Username:
Password:

PC-B

Physical | Config | Desktop | Programming | Attributes

IP Configuration

Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address: 192.168.3.10
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.3.1
DNS Server: 0.0.0.0

IPv6 Configuration

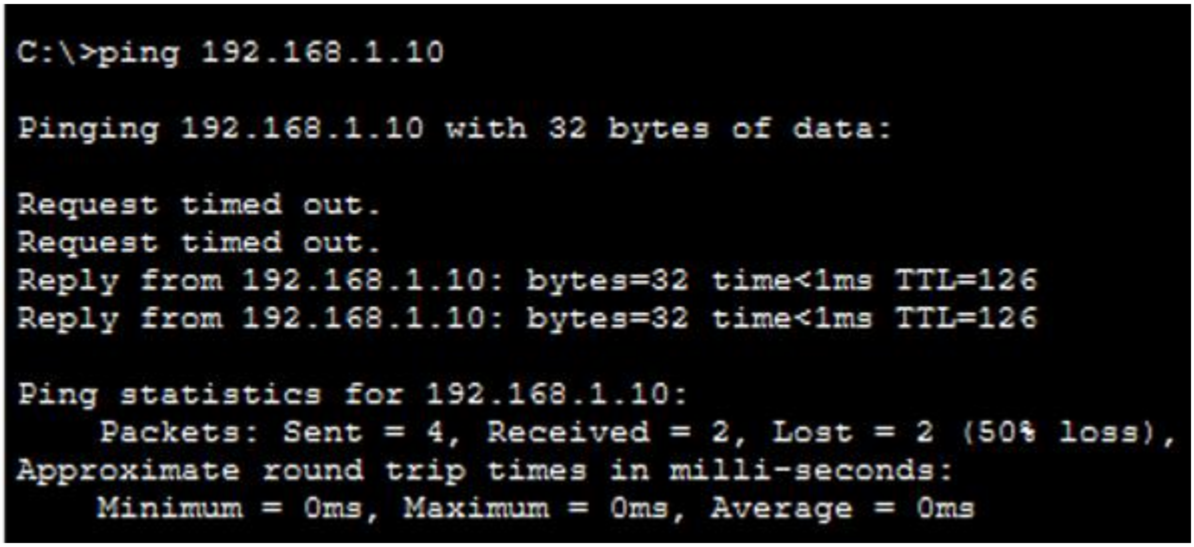
○ Automatic ● Static

IPv6 Address: /
Link Local Address: FE80::2E0:F7FF:FEA7:E51C
Default Gateway:
DNS Server:

802.1X

□ Use 802.1X Security
Authentication: MD5
Username:
Password:

Prueba de ping



```
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 = 0ms, Maximum = 0ms, Average = 0ms
```

e

Conclusión

La implementación exitosa de un túnel VPN IPSec demuestra que es posible extender una red privada de forma segura sobre una infraestructura pública no confiable. A través de este laboratorio, se validó que la correcta sincronización de las políticas de cifrado, la gestión de llaves compartidas (Pre-Shared Keys) y la definición precisa del "tráfico interesante" mediante Listas de Control de Acceso (ACL) son fundamentales para la estabilidad del túnel.

Bibliografía

- Cisco Systems. (2026). Cisco Packet Tracer (Versión 9.x) [Software de computación]. Disponible en https://www.netacad.com/