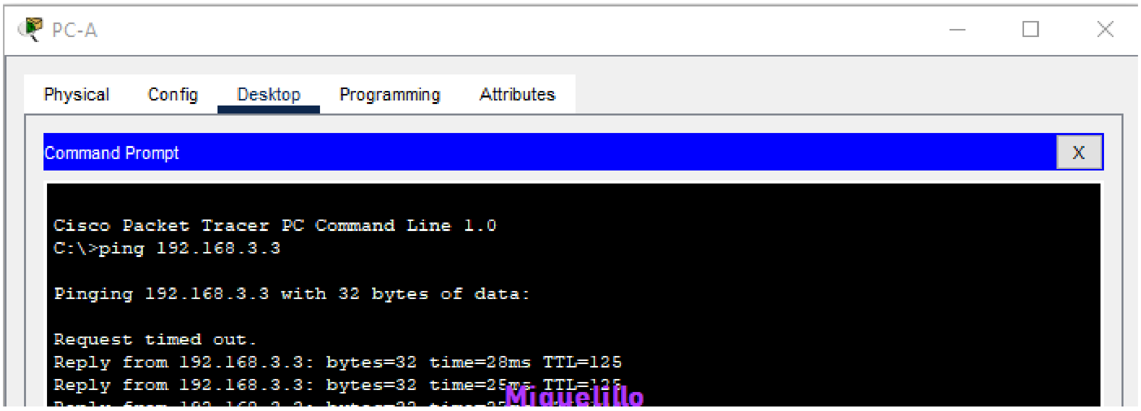
Índice:

Ejercicio 1 - Configurar y Verificar Site-to-Site IPsec VPN

a) Configurar parámetros de IPsec en R1

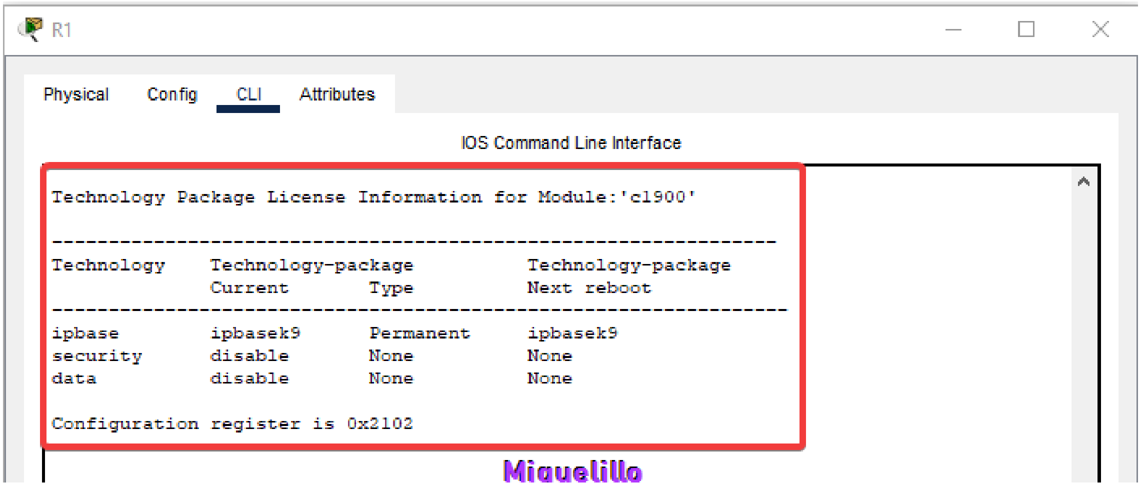
Solución:

Probamos a hacer un ping del PC-A al PC-C



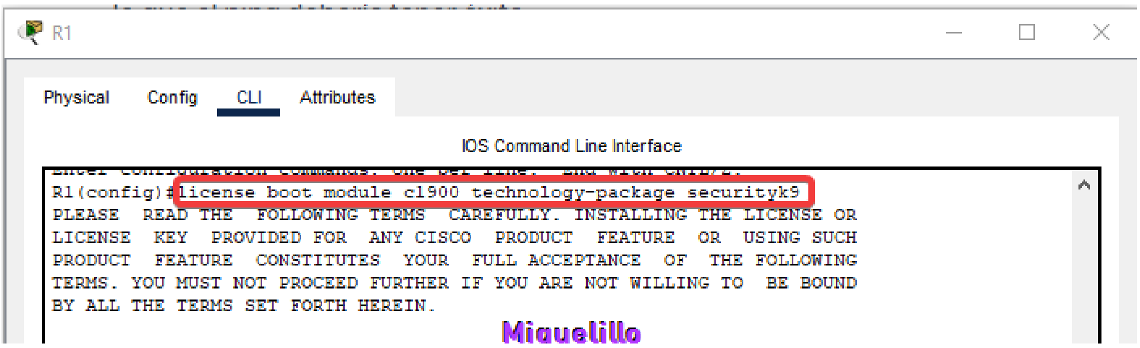
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.3.3: bytes=32 time=28ms TTL=125
Reply from 192.168.3.3: bytes=32 time=25ms TTL=125
```

Hago un show versión y veo información de la licencia del paquete de tecnología de seguridad.



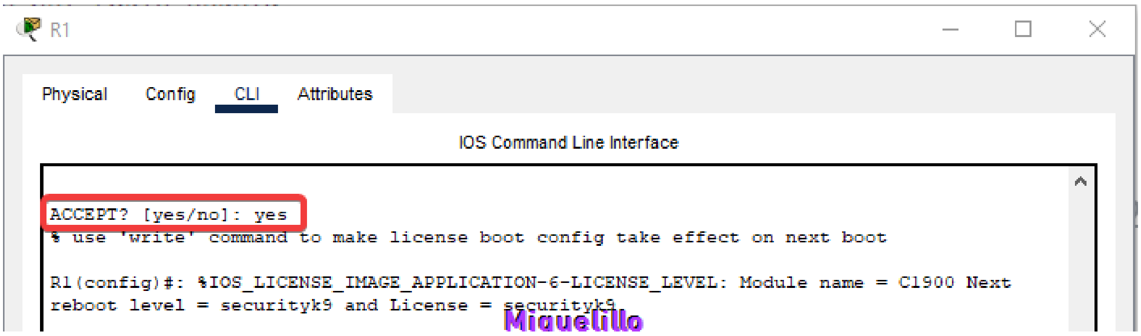
```
Technology Package License Information for Module:'c1900'

-----------------------------------------------------------------
Technology    Technology-package           Technology-package
              Current       Type           Next reboot
------------------------------------------------------------------
ipbase        ipbasek9      Permanent      ipbasek9
security      disable       None           None
data          disable       None           None

Configuration register is 0x2102
```

Lo habilitamos



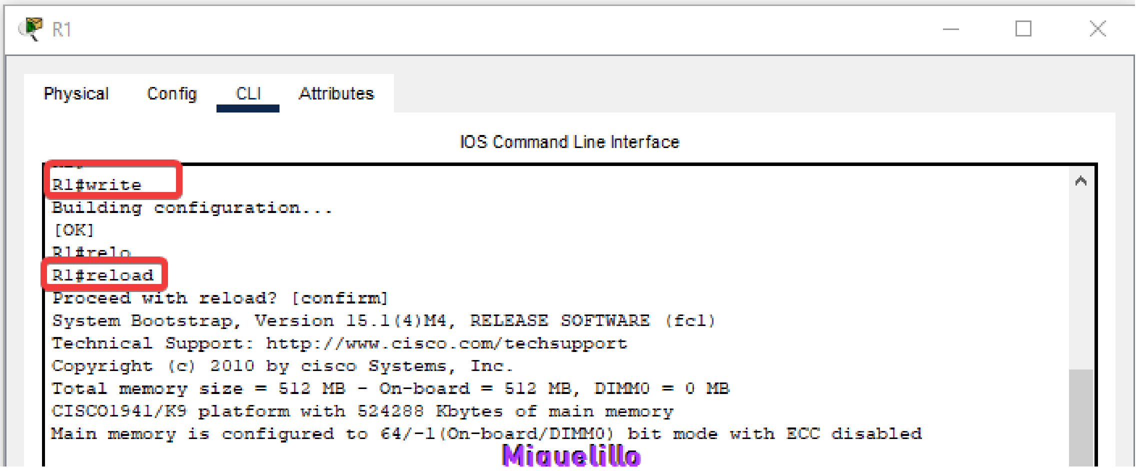
```
R1(config)#license boot module c1900 technology-package securityk9
PLEASE  READ THE  FOLLOWING TERMS  CAREFULLY. INSTALLING THE LICENSE OR
LICENSE  KEY  PROVIDED FOR  ANY CISCO  PRODUCT  FEATURE  OR  USING SUCH
PRODUCT  FEATURE  CONSTITUTES  YOUR  FULL ACCEPTANCE  OF  THE FOLLOWING
TERMS. YOU MUST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

Aceptamos los términos y condiciones



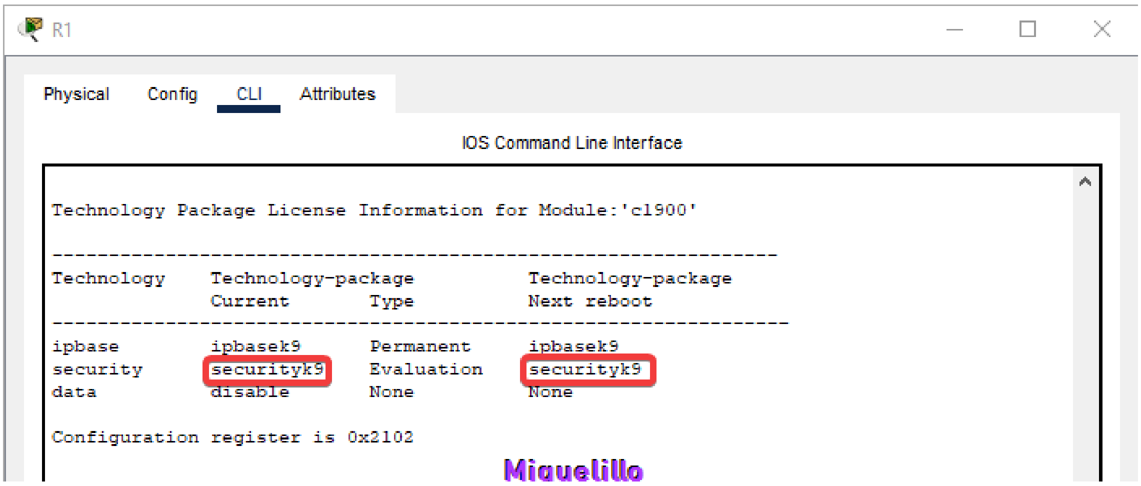
```
ACCEPT? [yes/no]: yes
% use 'write' command to make license boot config take effect on next boot

R1(config)#: %IOS_LICENSE_IMAGE_APPLICATION-6-LICENSE_LEVEL: Module name = C1900 Next
reboot level = securityk9 and License = securityk9
```

Guardamos la configuración y reiciamos



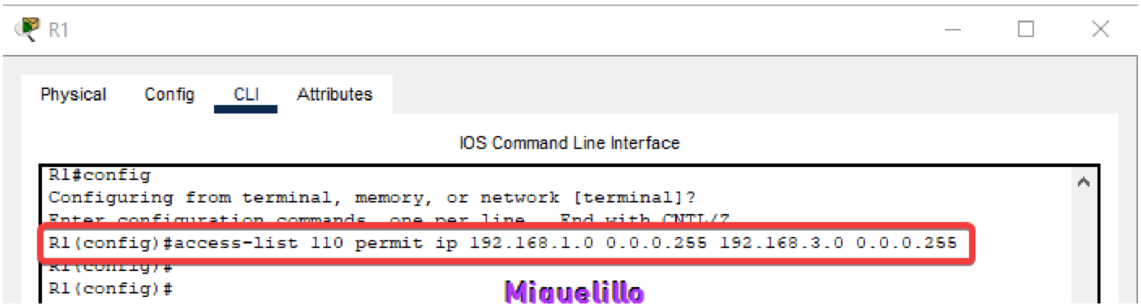
```
R1#write
Building configuration...
[OK]
R1#relo
R1#reload
Proceed with reload? [confirm]
System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 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
```

Vemos que securityk9 esta activado



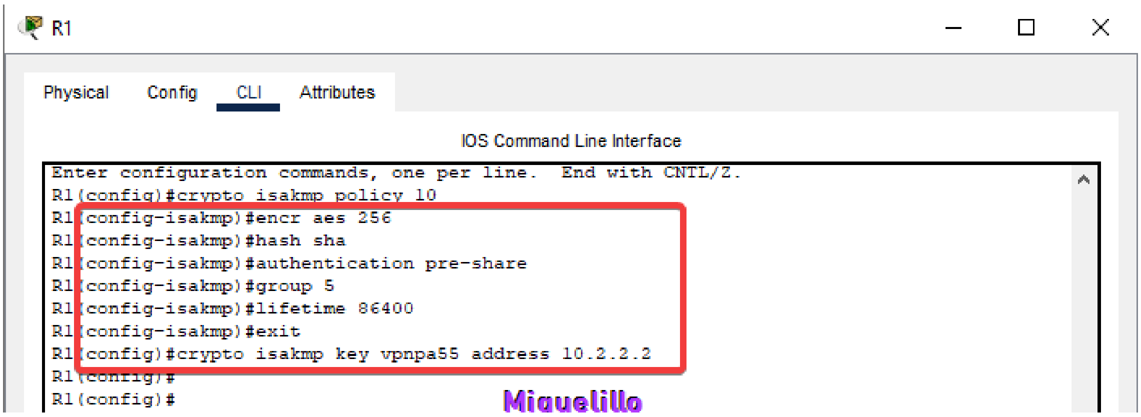
```
Technology Package License Information for Module:'c1900'

----------------------------------------------------------------
Technology    Technology-package           Technology-package
              Current       Type           Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent      ipbasek9
security      securityk9    Evaluation     securityk9
data          disable       None           None

Configuration register is 0x2102
```

Configuramos la ACL 110 para permitir el tráfico desde la LAN en R1 hacia la LAN en R3



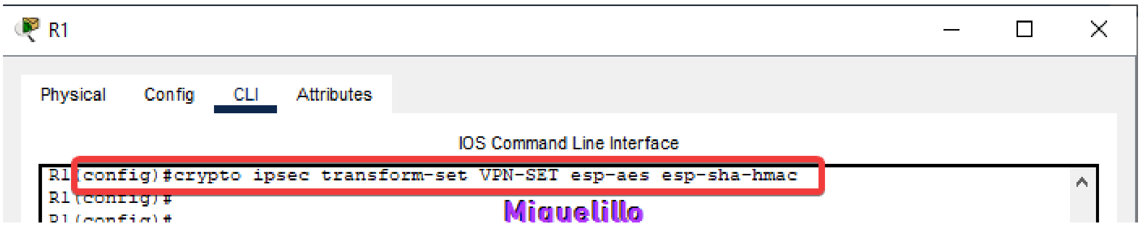
```
R1#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
R1(config)#
R1(config)#
```

Configuraramos los parámetros de la Fase 1 de ISAKMP en R1



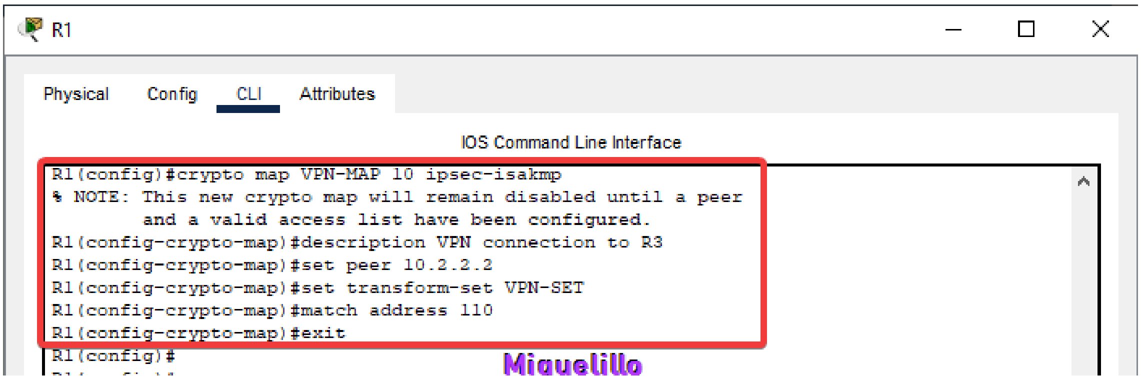
```
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#encr aes 256
R1(config-isakmp)#hash sha
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 5
R1(config-isakmp)#lifetime 86400
R1(config-isakmp)#exit
R1(config)#crypto isakmp key vpnpa55 address 10.2.2.2
R1(config)#
R1(config)#
```

Seleccionamos el Algoritmo de IPSEC en este caso ESP



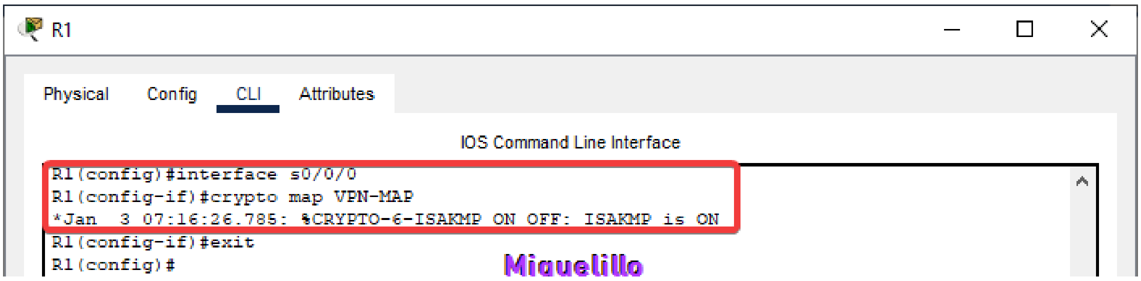
```
R1(config)#crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
R1(config)#
R1(config)#
```

Configura los parámetros de la Fase 2 de IPsec en R1



```
R1(config)#crypto map VPN-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)#description VPN connection to R3
R1(config-crypto-map)#set peer 10.2.2.2
R1(config-crypto-map)#set transform-set VPN-SET
R1(config-crypto-map)#match address 110
R1(config-crypto-map)#exit
R1(config)#
R1(config)#
```

Consiste en vincular el mapa criptográfico (crypto map) VPN-MAP a la interfaz saliente Serial 0/0/0 en R1

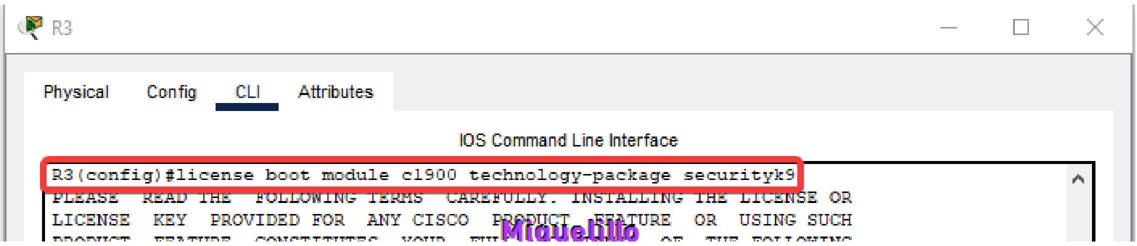


```
R1(config)#interface s0/0/0
R1(config-if)#crypto map VPN-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config-if)#exit
R1(config)#
```

b) Configurar parámetros de IPsec en R3

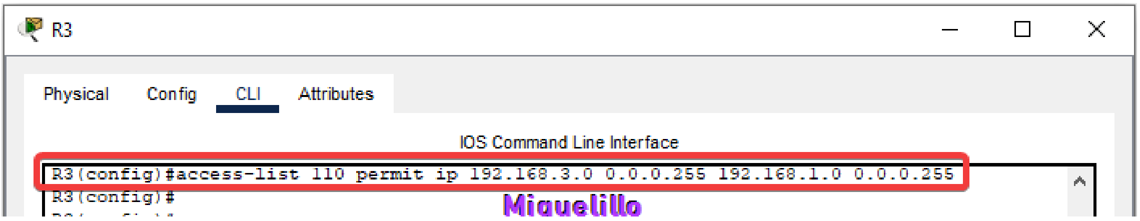
Solución:

Habilitamos el paquete de tecnología y reiniciamos R3



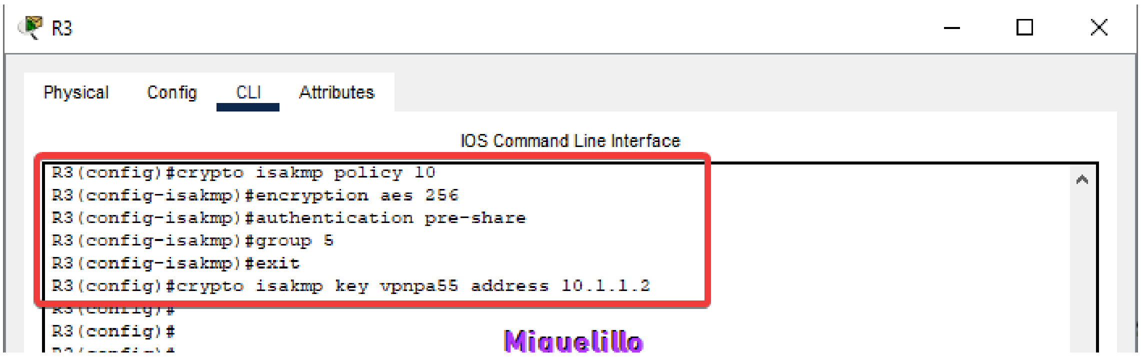
```
R3(config)#license boot module c1900 technology-package securityk9
PLEASE  READ THE  FOLLOWING TERMS  CAREFULLY. INSTALLING THE LICENSE OR
LICENSE  KEY  PROVIDED FOR  ANY CISCO  PRODUCT  FEATURE  OR  USING SUCH
```

Configuramos la ACL 110 para aceptar el tráfico de la LAN en R3 hacia la LAN en R1



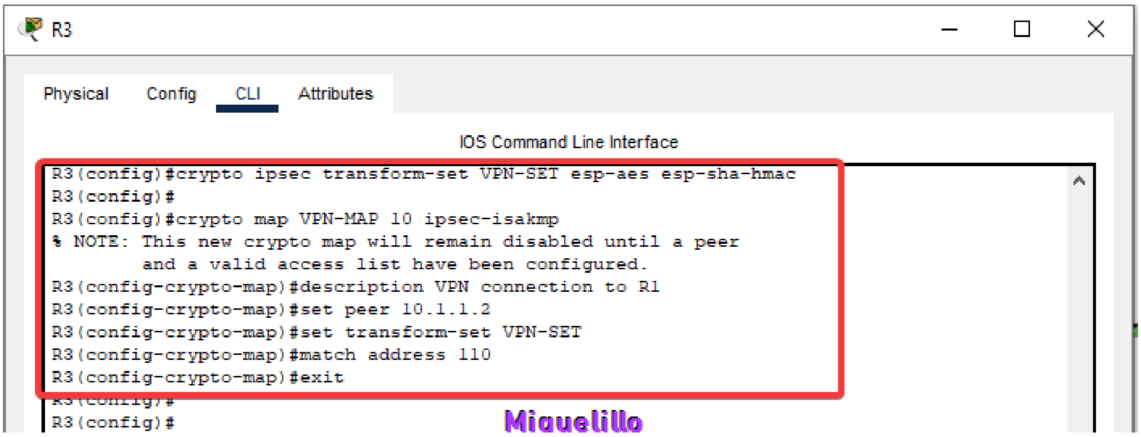
```
R3(config)#access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
R3(config)#
```

Configuramos las propiedades de la Fase 1 de ISAKMP en R3



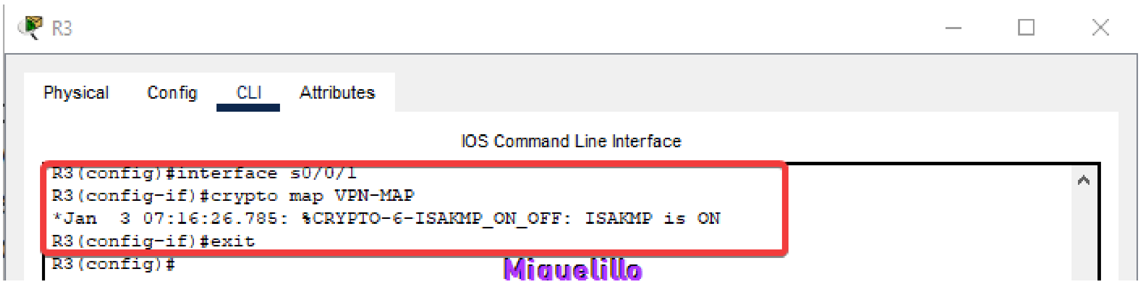
```
R3(config)#crypto isakmp policy 10
R3(config-isakmp)#encryption aes 256
R3(config-isakmp)#authentication pre-share
R3(config-isakmp)#group 5
R3(config-isakmp)#exit
R3(config)#crypto isakmp key vpnpa55 address 10.1.1.2
R3(config)#
R3(config)#
```

Crearamos el mapa criptográfico VPN-MAP que vincula todos los parámetros de la Fase 2



```
R3(config)#crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
R3(config)#
R3(config)#crypto map VPN-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)#description VPN connection to R1
R3(config-crypto-map)#set peer 10.1.1.2
R3(config-crypto-map)#set transform-set VPN-SET
R3(config-crypto-map)#match address 110
R3(config-crypto-map)#exit
R3(config)#
R3(config)#
```

Configurar el mapa criptográfico en la interfaz saliente

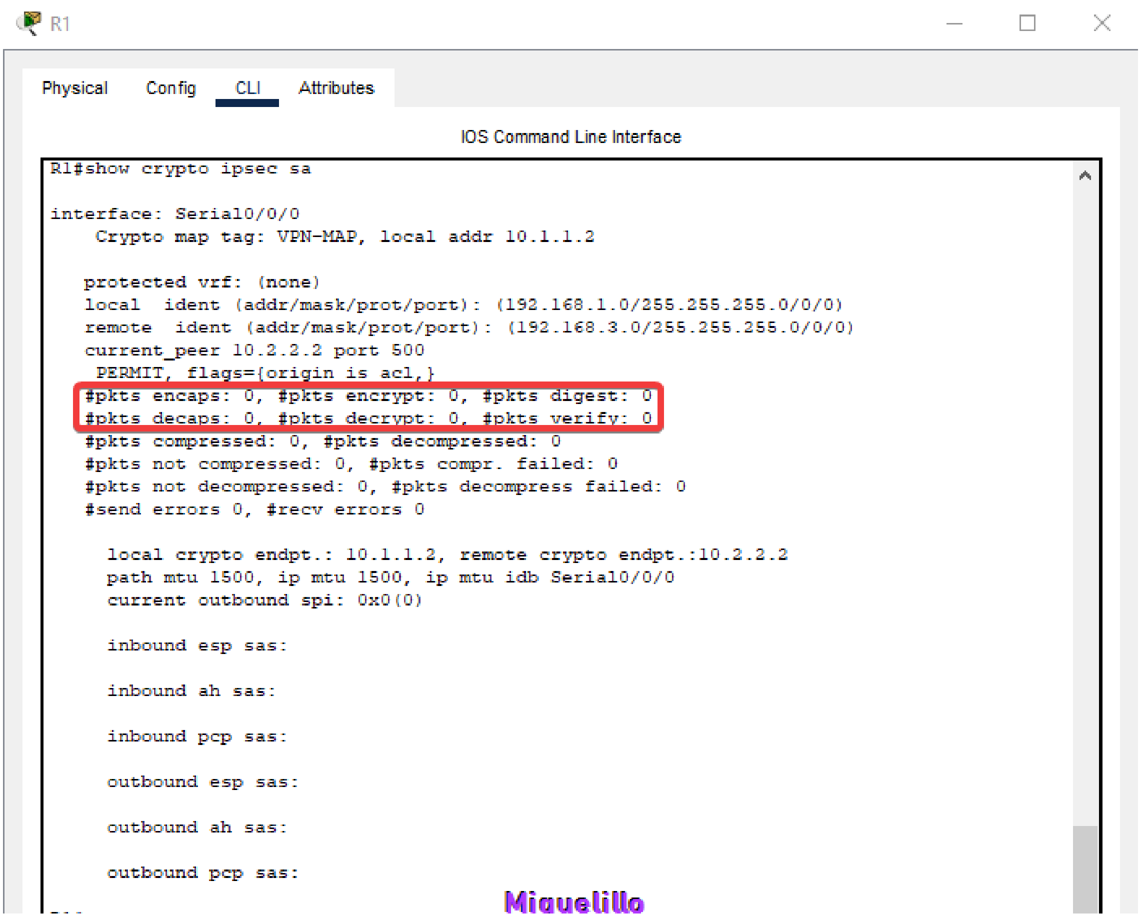


```
R3(config)#interface s0/0/1
R3(config-if)#crypto map VPN-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R3(config-if)#exit
R3(config)#
```

c) Probar IPsec VPN

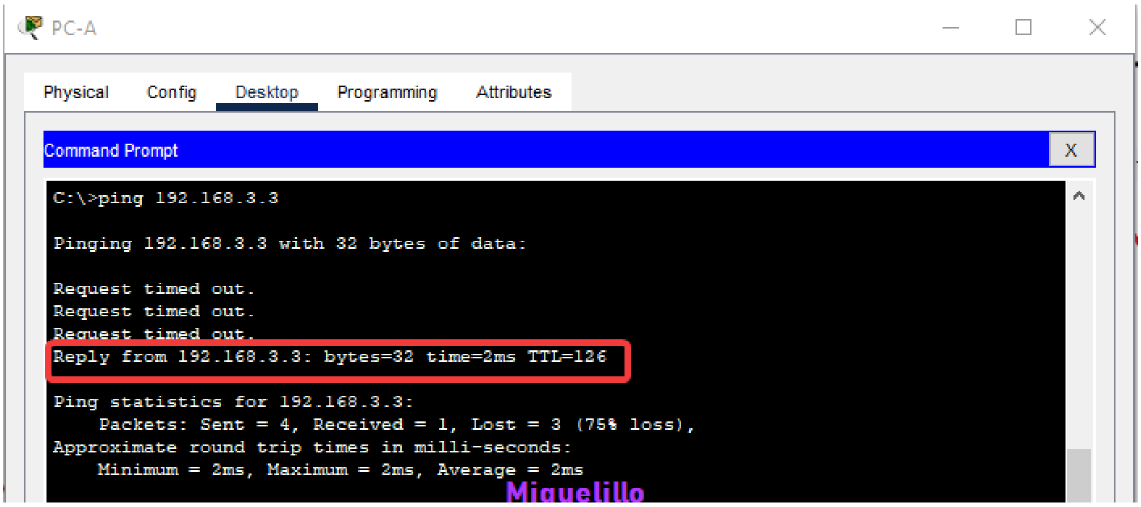
Solución:

Ejecuta el siguiente comando en R1 para verificar el estado del túnel antes de que se genere tráfico. Observa que el número de paquetes encapsulados, cifrados, desencapsulados y descifrados está establecido en 0.



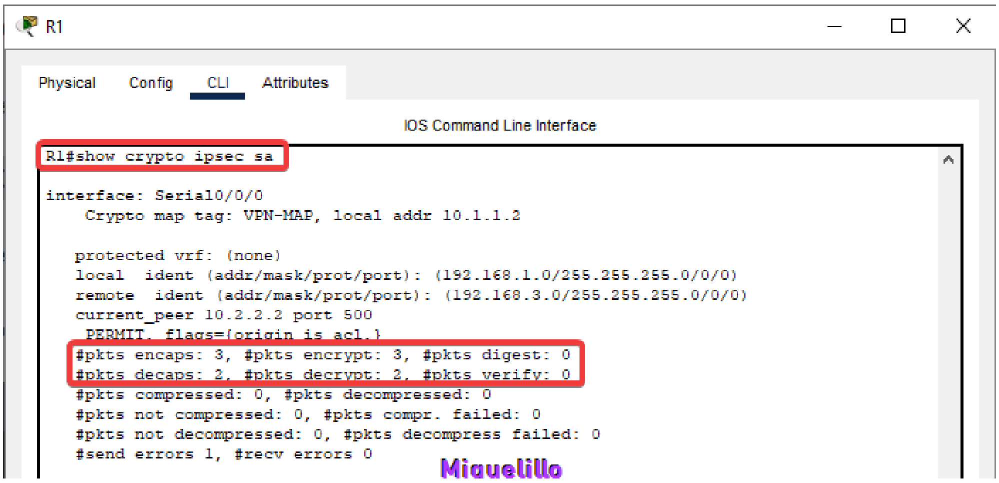
```
R1#show crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: VPN-MAP, local addr 10.1.1.2

   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 10.2.2.2 port 500
    PERMIT, flags={origin is acl,}
   #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
   #pkts decaps: 0, #pkts decrypt: 0, #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 0, #recv errors 0

     local crypto endpt.: 10.1.1.2, remote crypto endpt.:10.2.2.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0x0(0)

     inbound esp sas:

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:

     outbound ah sas:

     outbound pcp sas:
```

Desde PC-A, realiza un ping a PC-C para generar tráfico.



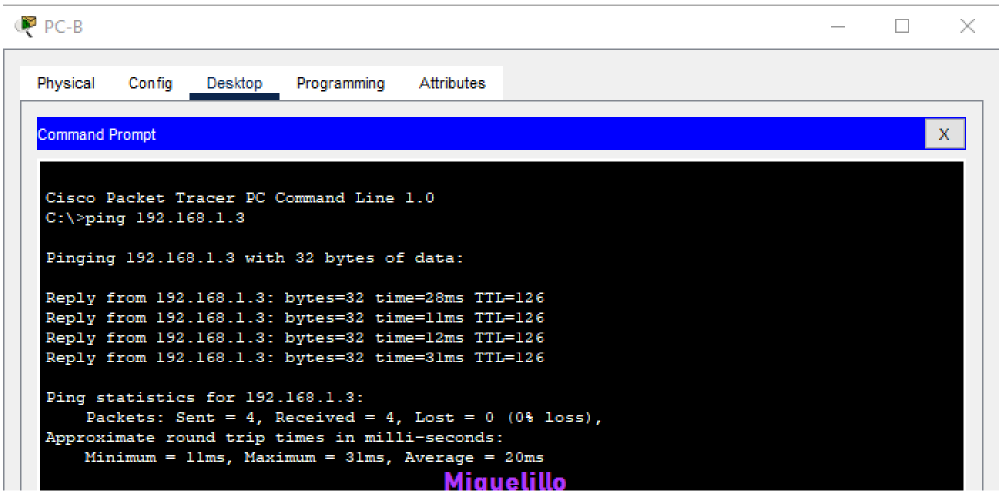
```
C:\>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Reply from 192.168.3.3: bytes=32 time=2ms TTL=126

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 1, Lost = 3 (75% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 2ms, Average = 2ms
```

Observamos que el número de paquetes ahora es mayor que 0, lo que indica que la VPN IPsec está funcionando.



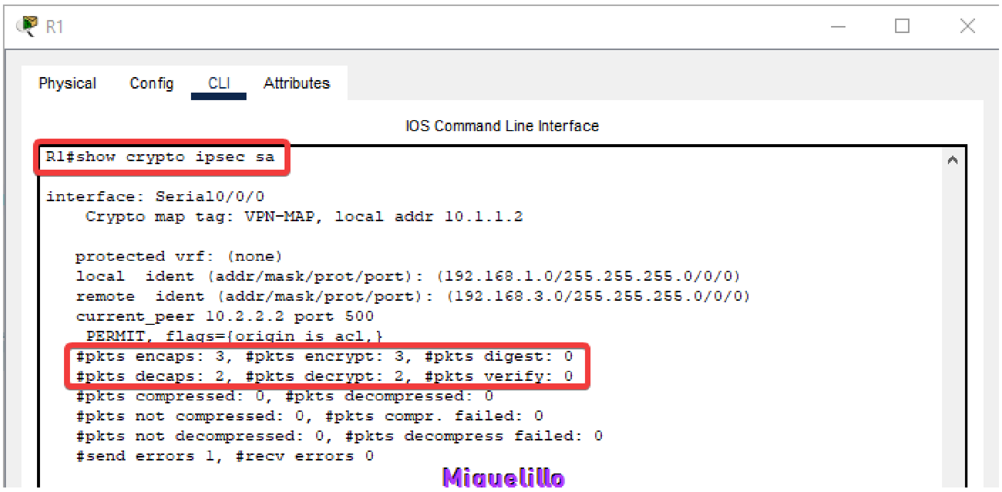
```
R1#show crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: VPN-MAP, local addr 10.1.1.2

   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 10.2.2.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 0
   #pkts decaps: 2, #pkts decrypt: 2, #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
```

Desde PC-A, realiza un ping a PC-B para generar tráfico



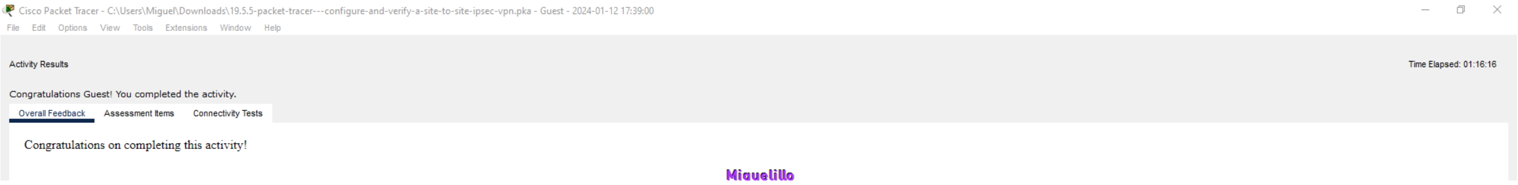
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=28ms TTL=126
Reply from 192.168.1.3: bytes=32 time=11ms TTL=126
Reply from 192.168.1.3: bytes=32 time=12ms TTL=126
Reply from 192.168.1.3: bytes=32 time=31ms TTL=126

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 11ms, Maximum = 31ms, Average = 20ms
```

Observa que el número de paquetes no ha cambiado, lo que verifica que el tráfico que no va por el túnel no se está cifrando.



```
R1#show crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: VPN-MAP, local addr 10.1.1.2

   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 10.2.2.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 0
   #pkts decaps: 2, #pkts decrypt: 2, #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
```

Clicamos en verificar los resultados



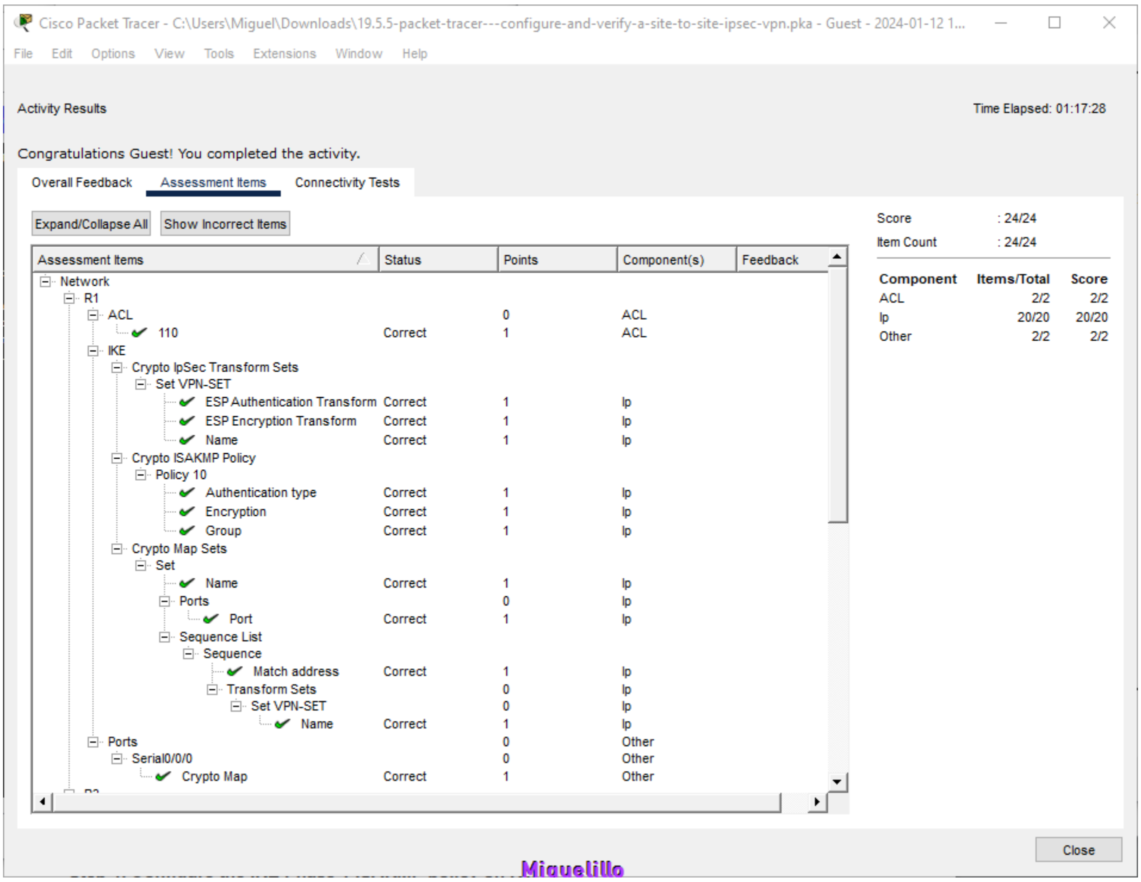
Cisco Packet Tracer - C:\Users\Miguel\Downloads\19.5.5-packet-tracer---configure-and-verify-a-site-to-site-ipsec-vpn.pka - Guest - 2024-01-12 17:39:00

Activity Results

Time Elapsed: 01:16:16

Congratulations Guest! You completed the activity.

Congratulations on completing this activity!



Cisco Packet Tracer - C:\Users\Miguel\Downloads\19.5.5-packet-tracer---configure-and-verify-a-site-to-site-ipsec-vpn.pka - Guest - 2024-01-12 1...

Activity Results

Time Elapsed: 01:17:28

Congratulations Guest! You completed the activity.

Assessment Items	Status	Points	Component(s)	Feedback
Network				
R1				
ACL		0	ACL	
✓ 110	Correct	1	ACL	
IKE				
Crypto IpSec Transform Sets				
Set VPN-SET				
✓ ESP Authentication Transform	Correct	1	Ip	
✓ ESP Encryption Transform	Correct	1	Ip	
✓ Name	Correct	1	Ip	
Crypto ISAKMP Policy				
Policy 10				
✓ Authentication type	Correct	1	Ip	
✓ Encryption	Correct	1	Ip	
✓ Group	Correct	1	Ip	
Crypto Map Sets				
Set				
✓ Name	Correct	1	Ip	
Ports		0	Ip	
✓ Port	Correct	1	Ip	
Sequence List				
Sequence				
✓ Match address	Correct	1	Ip	
Transform Sets		0	Ip	
Set VPN-SET		0	Ip	
✓ Name	Correct	1	Ip	
Ports		0	Other	
Serial0/0/0		0	Other	
✓ Crypto Map	Correct	1	Other	

Score : 24/24

Item Count : 24/24

Component	Items/Total	Score
ACL	2/2	2/2
Ip	20/20	20/20
Other	2/2	2/2