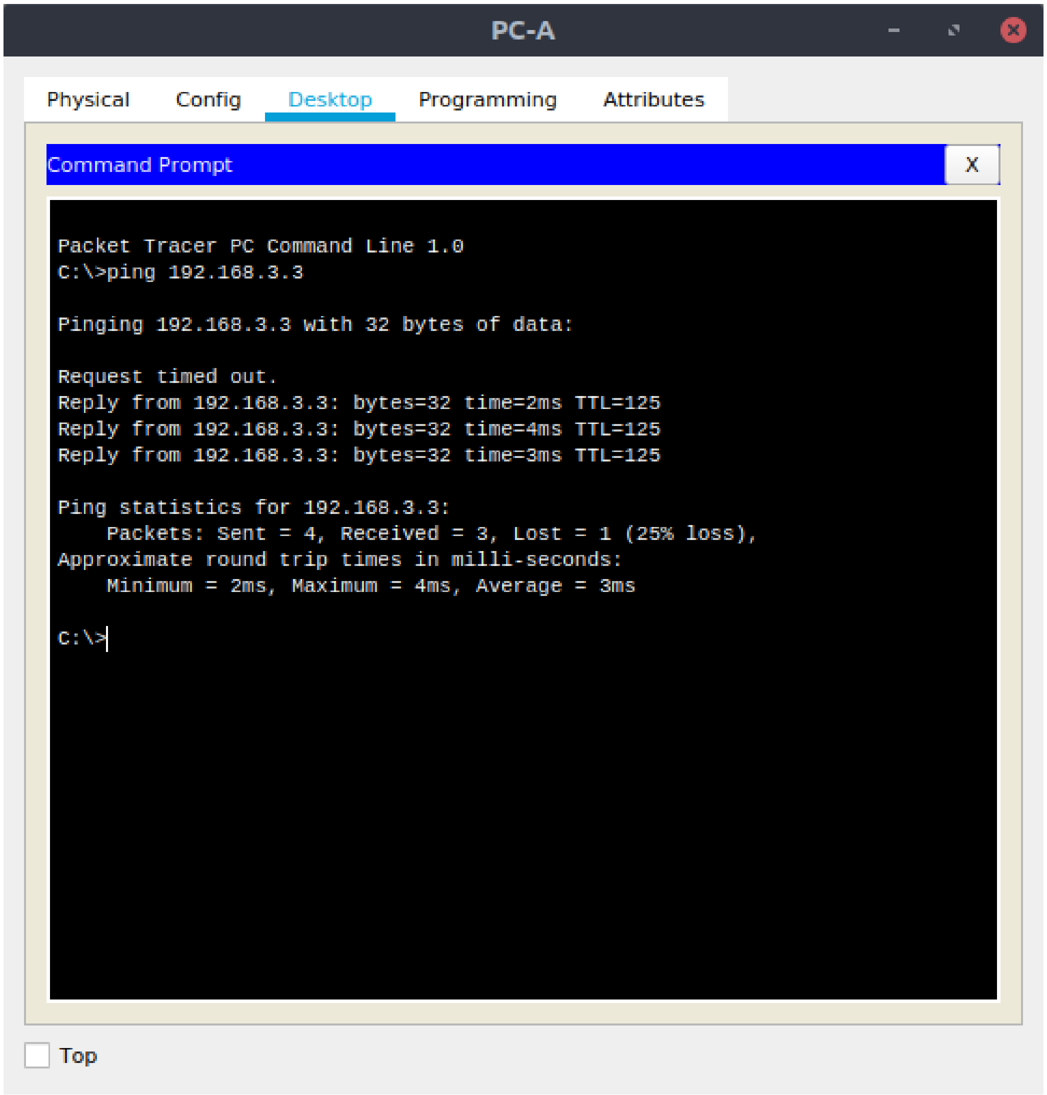
Lab 5: Configure and Verify a Site-to-Site IPsec VPNUsing CLI

Alexander Hoffmann

January 27, 2020

1 Configure IPsec Parameters on R1

1.1 Test connectivity

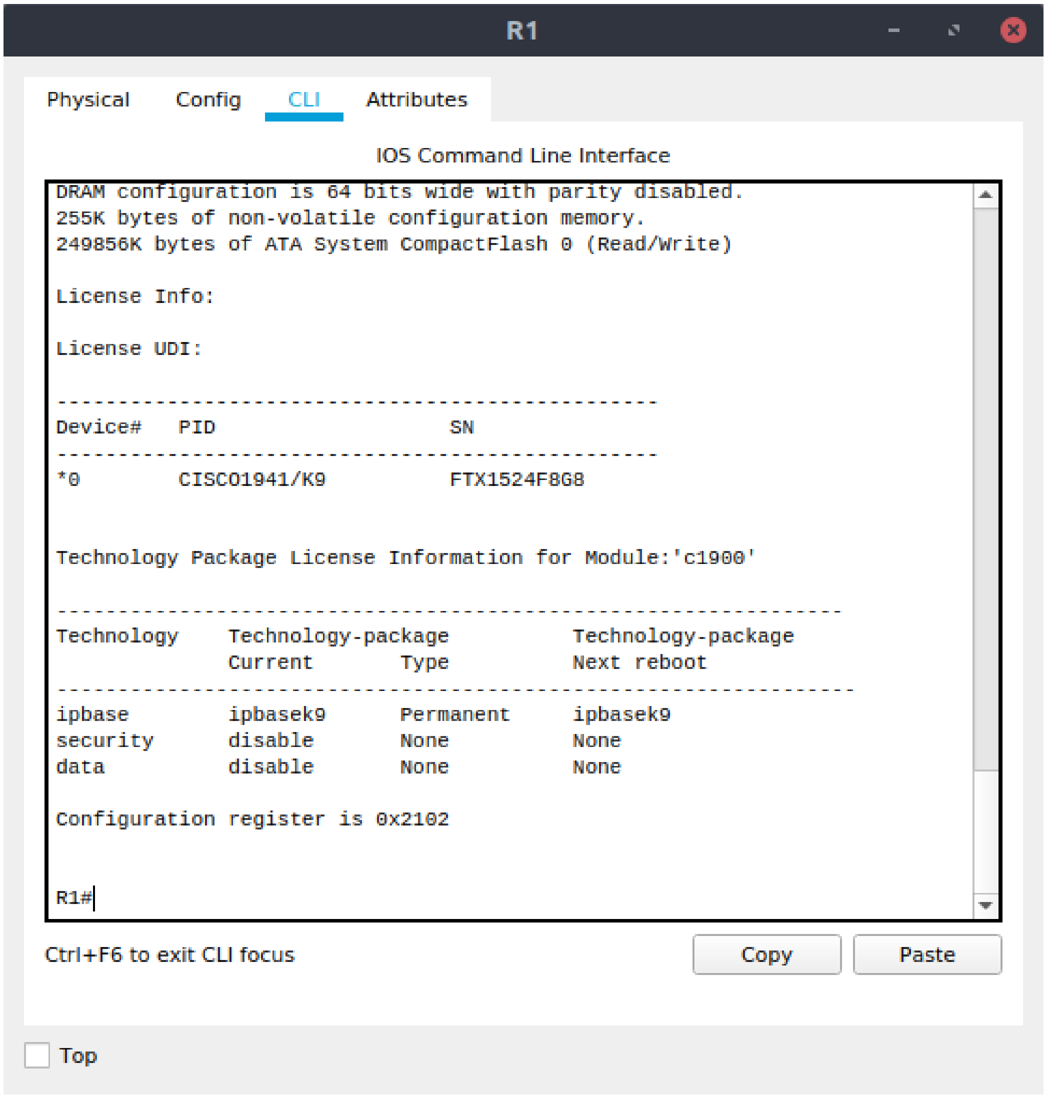


```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.3.3: bytes=32 time=2ms TTL=125
Reply from 192.168.3.3: bytes=32 time=4ms TTL=125
Reply from 192.168.3.3: bytes=32 time=3ms TTL=125

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 4ms, Average = 3ms

C:\>
```

Figure 1: PC-A ping PC-C

1.2 Enable the Security Technology package

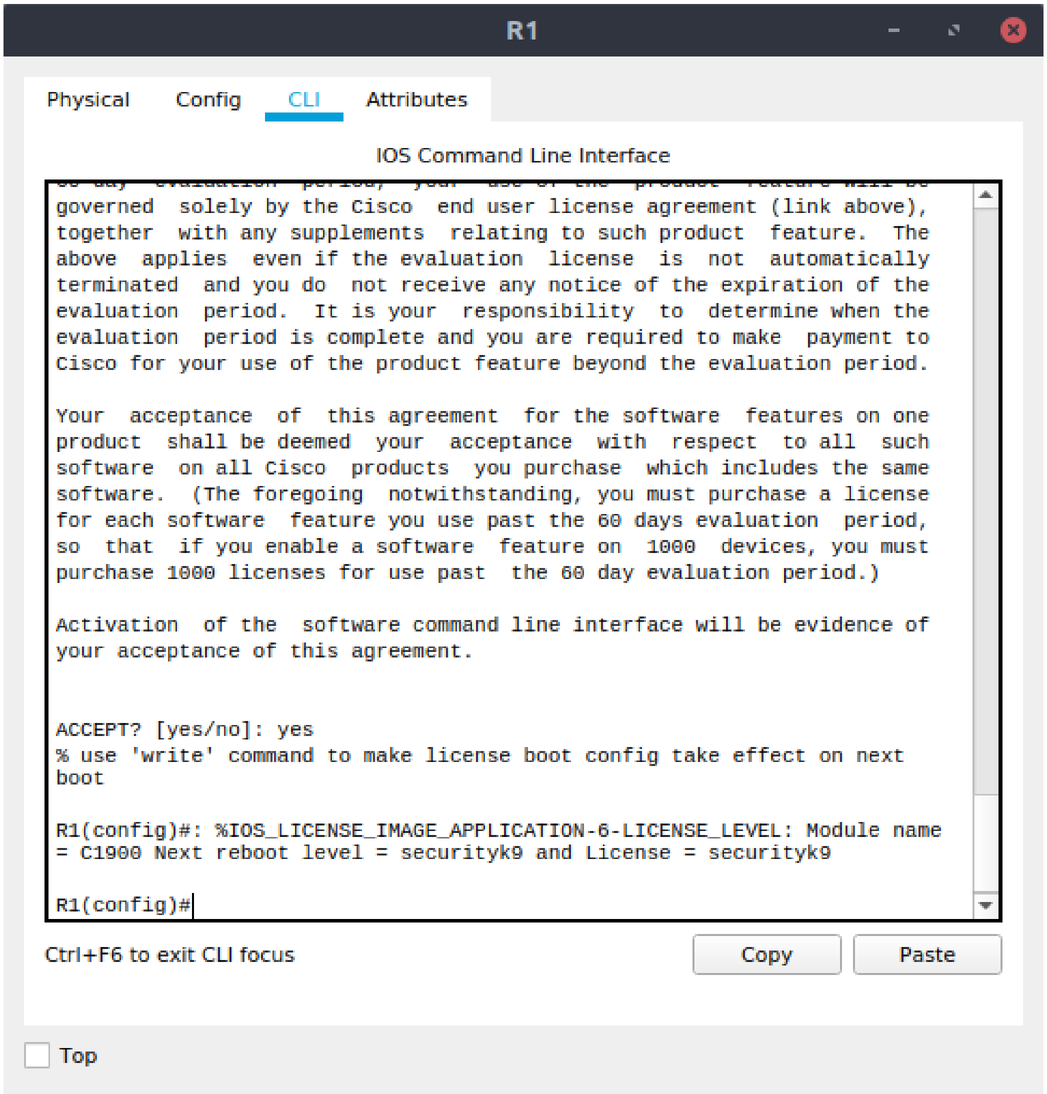
a. On R1, issue the show versioncommand to view the Security Technology package license information.



```
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)

License Info:

License UDI:

-------------------------------------------------
Device#   PID                   SN
-------------------------------------------------
*0        CISCO1941/K9          FTX1524F8G8


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


R1#
```

Figure 2: show versioncommand

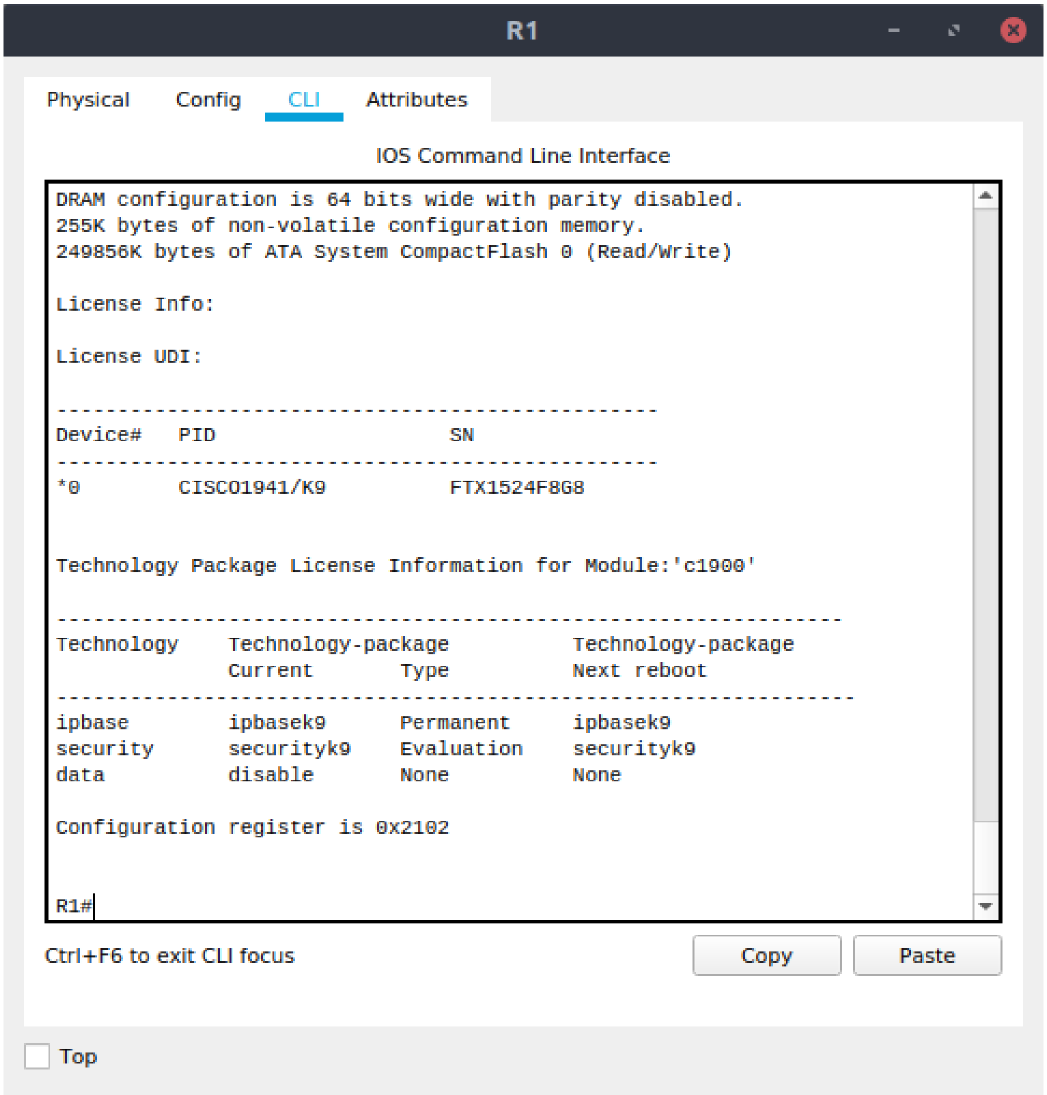
b. If the Security Technology package has not been enabled, use the following command to enable the package.



```
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)#
```

Figure 3: enable Security Technology package

e. Verify that the Security Technology package has been enabled by using the show versioncommand.



```
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)

License Info:

License UDI:

-------------------------------------------------
Device#   PID                   SN
-------------------------------------------------
*0        CISCO1941/K9          FTX1524F8G8


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


R1#
```

Figure 4: show versioncommand

1.3 Identify interesting traffic on R1

Configure ACL 110to identify the traffic from the LAN on R1to the LAN on R3as interesting. This interesting traffic will trigger the IPsec VPN to be implemented when there is traffic betweentheR1to R3LANs. All other traffic sourced from the LANs will not be encrypted.Because ofthe implicit deny all, there is no need to configure a deny ip any any statement.

1.4 Configure the IKE Phase 1 ISAKMP policy on R1

```
R1(config)# crypto isakmp policy 10
R1(config-isakmp)# encryption aes 256
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# group 5
R1(config-isakmp)# exit
R1(config)# crypto isakmp key vpnpa55 address 10.2.2.2
```

1.5 Configure the IKEPhase 2 IPsec policyon R1

```
R1(config)# crypto map VPN-MAP 10 ipsec-isakmp
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
```

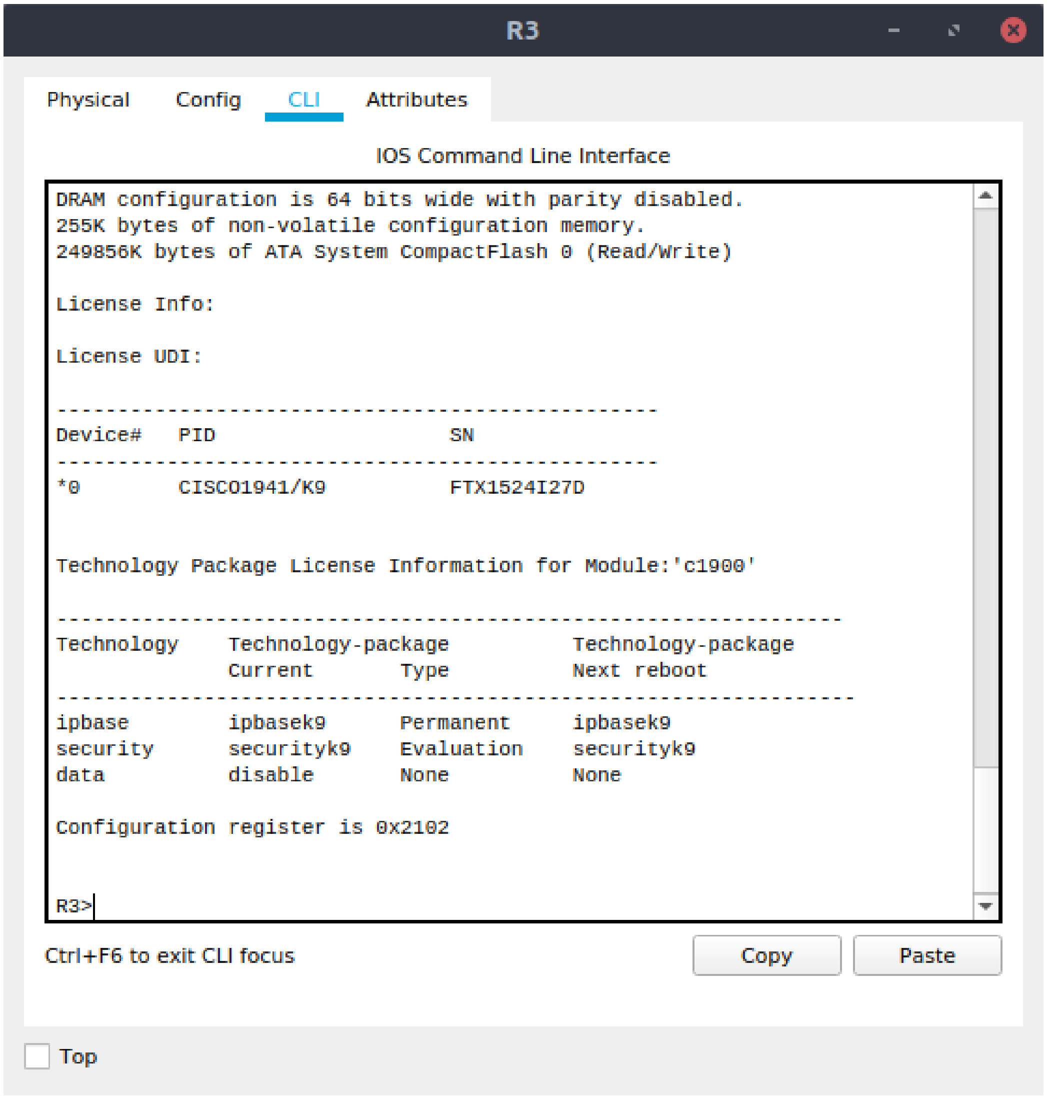
1.6 Configure the crypto map on the outgoing interface

```
R1(config)# interface s0/0/0
R1(config-if)# crypto map VPN-MAP
```

2 Configure IPsec Parameters on R3

2.1 Enable the Security Technology package

b. Verify that the Security Technology package has been enabled by using the show versioncommand after setting it up.



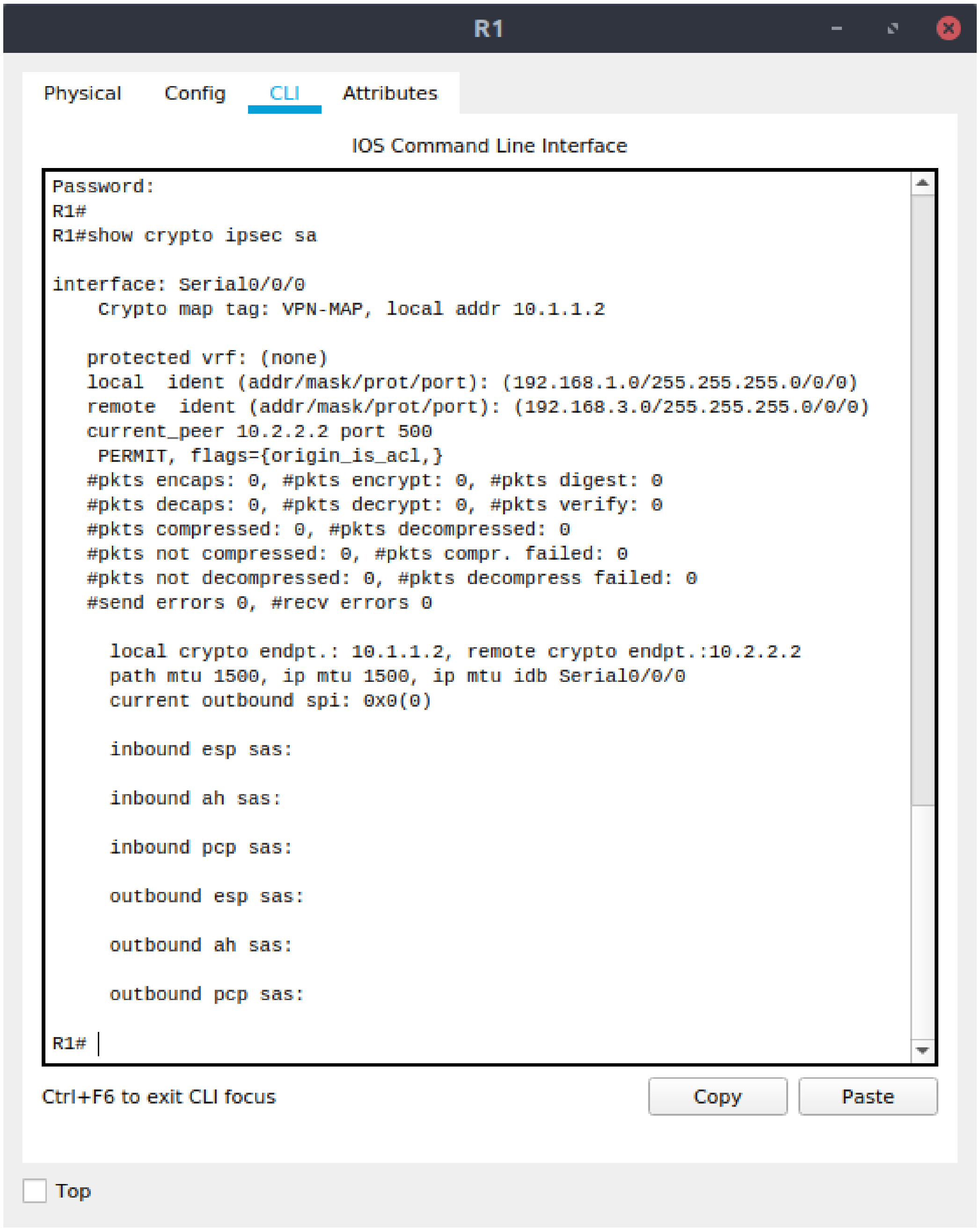
```
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

License Info:

License UDI:

-------------------------------------------------
Device#   PID                   SN
-------------------------------------------------
*0        CISCO1941/K9          FTX1524I27D


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


R3>
```

Figure 5: show versioncommand

After this, the configuration is similar to the one in the first part. We skip ahead to part 3.

3 Verify the IPsec VPN

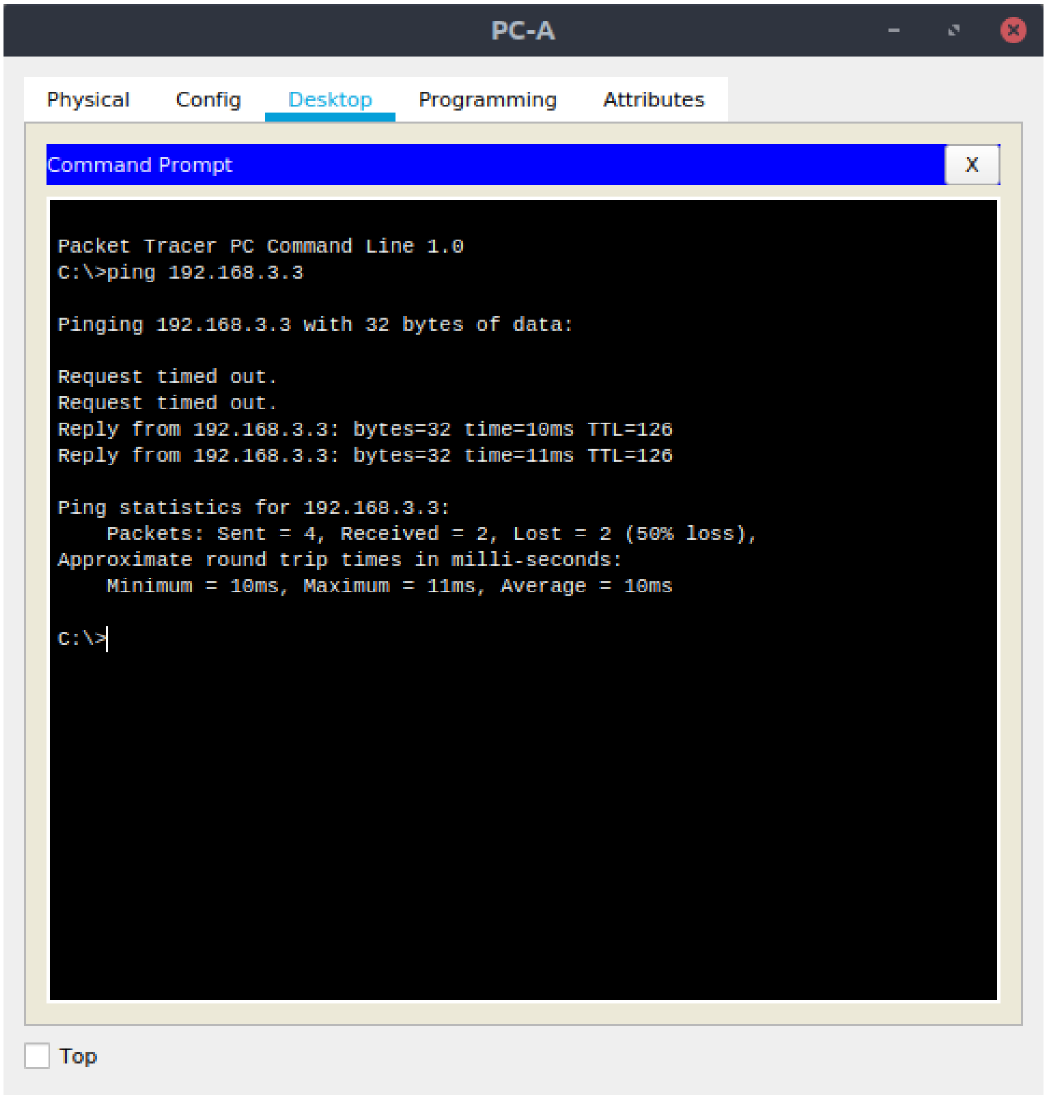
3.1 Verify the tunnel prior to interesting traffic



```
Password:
R1#
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:

R1# 
```

Figure 6: show crypto ipsec sa

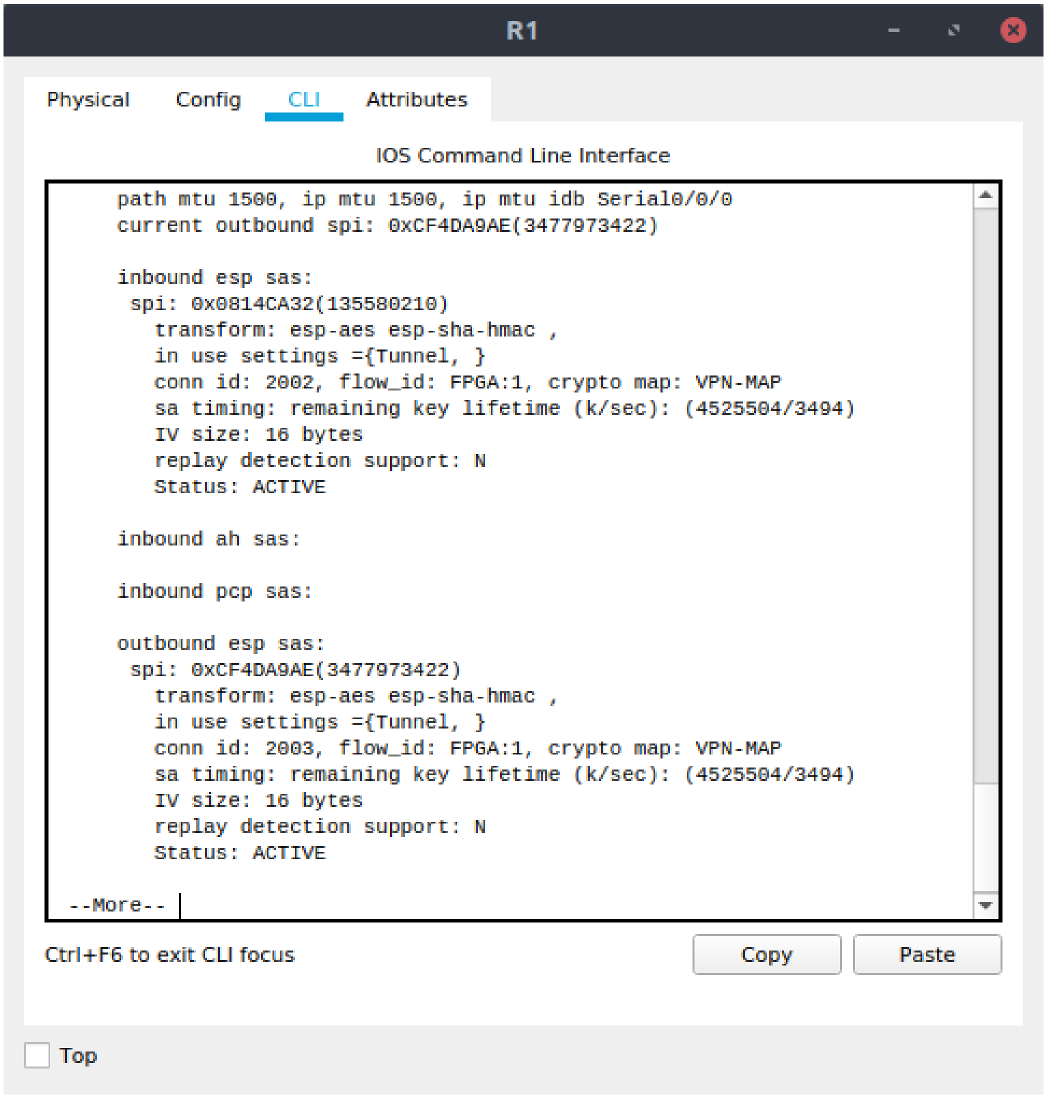
3.2 Create interesting traffic



```
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.
Request timed out.
Reply from 192.168.3.3: bytes=32 time=10ms TTL=126
Reply from 192.168.3.3: bytes=32 time=11ms TTL=126

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 11ms, Average = 10ms

C:\>
```

Figure 7: Ping PC-C from PC-A

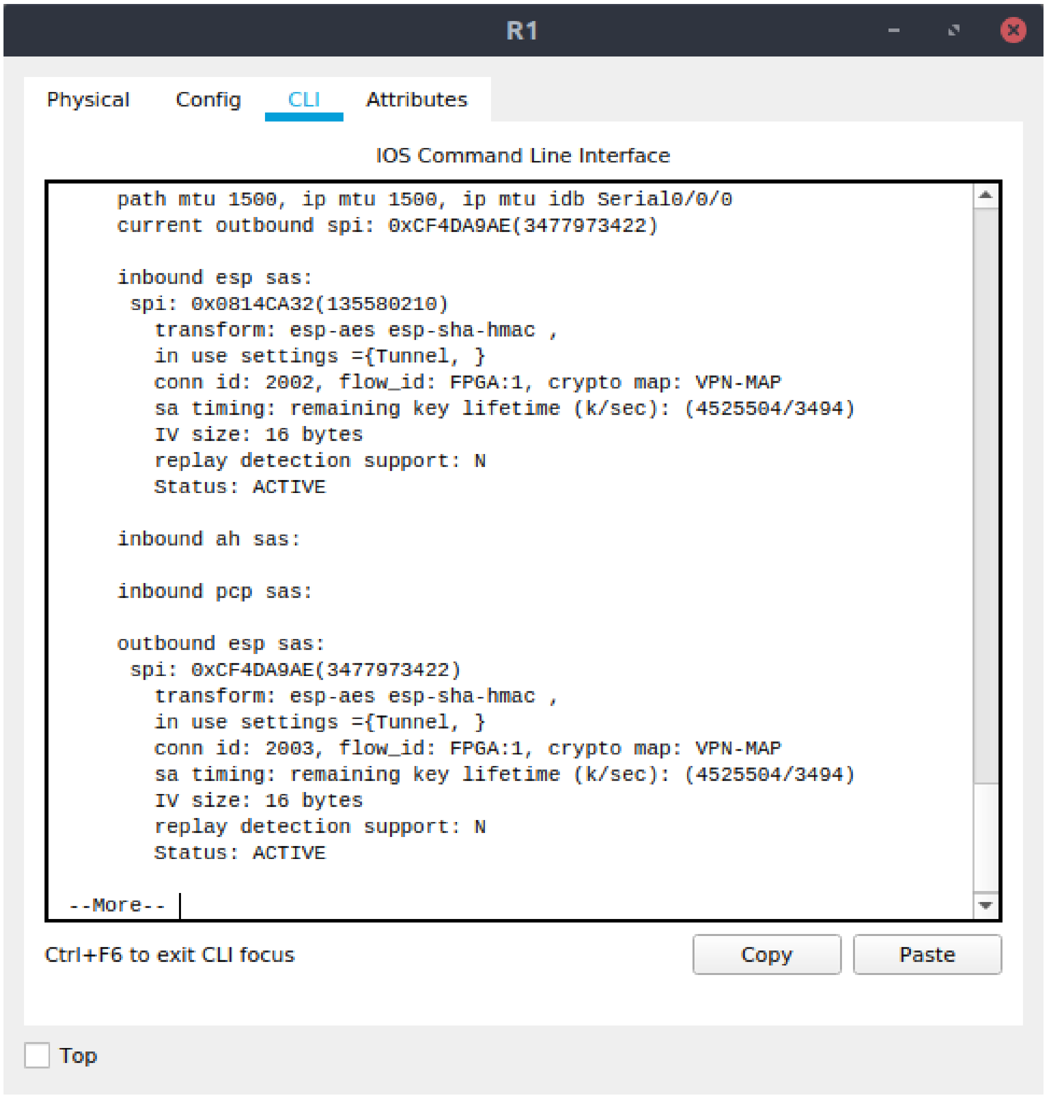
3.3 Verify the tunnel after interesting traffic



```
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0xCF4DA9AE(3477973422)

     inbound esp sas:
      spi: 0x0814CA32(135580210)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2002, flow_id: FPGA:1, crypto map: VPN-MAP
        sa timing: remaining key lifetime (k/sec): (4525504/3494)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xCF4DA9AE(3477973422)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2003, flow_id: FPGA:1, crypto map: VPN-MAP
        sa timing: remaining key lifetime (k/sec): (4525504/3494)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE

 --More--
```

Figure 8: show crypto ipsec sa

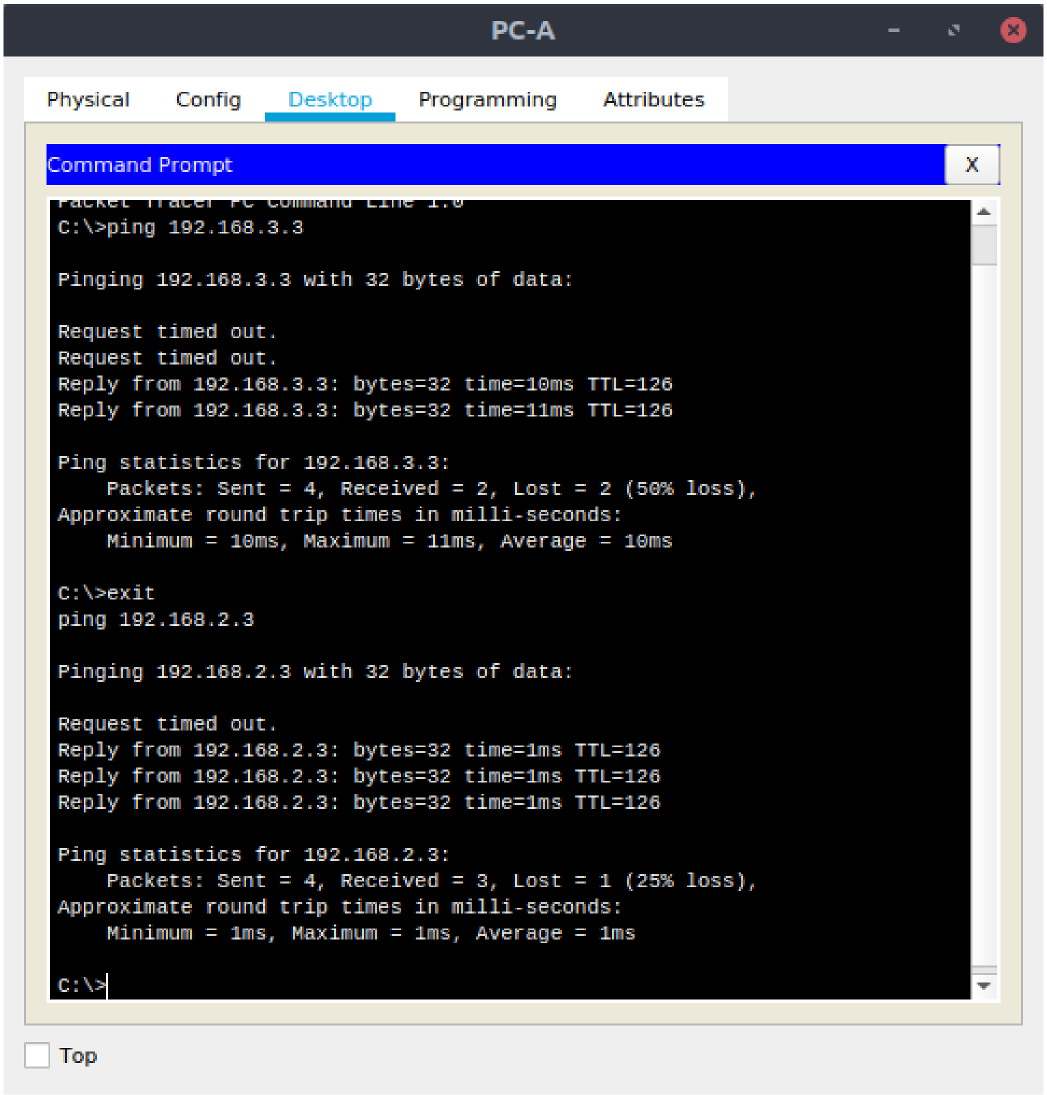
3.4 Create uninteresting traffic



```
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0xCF4DA9AE(3477973422)

     inbound esp sas:
      spi: 0x0814CA32(135580210)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2002, flow_id: FPGA:1, crypto map: VPN-MAP
        sa timing: remaining key lifetime (k/sec): (4525504/3494)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xCF4DA9AE(3477973422)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2003, flow_id: FPGA:1, crypto map: VPN-MAP
        sa timing: remaining key lifetime (k/sec): (4525504/3494)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE

 --More--
```

Figure 9: show crypto ipsec sa

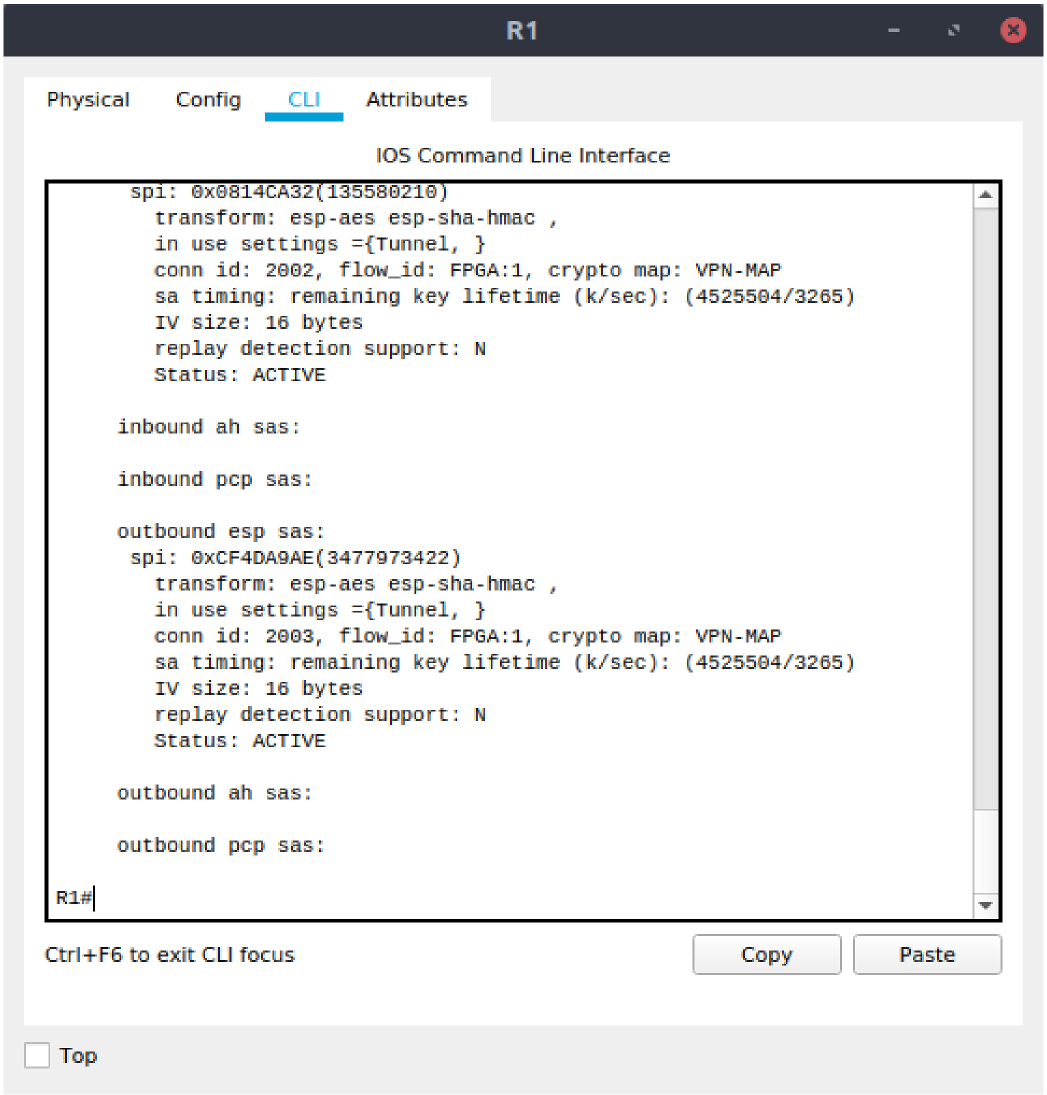
3.5 Create uninteresting traffic



```
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.
Request timed out.
Reply from 192.168.3.3: bytes=32 time=10ms TTL=126
Reply from 192.168.3.3: bytes=32 time=11ms TTL=126

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 11ms, Average = 10ms

C:\>exit
ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.3: bytes=32 time=1ms TTL=126
Reply from 192.168.2.3: bytes=32 time=1ms TTL=126
Reply from 192.168.2.3: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\>
```

Figure 10: Ping PC-B from PC-A

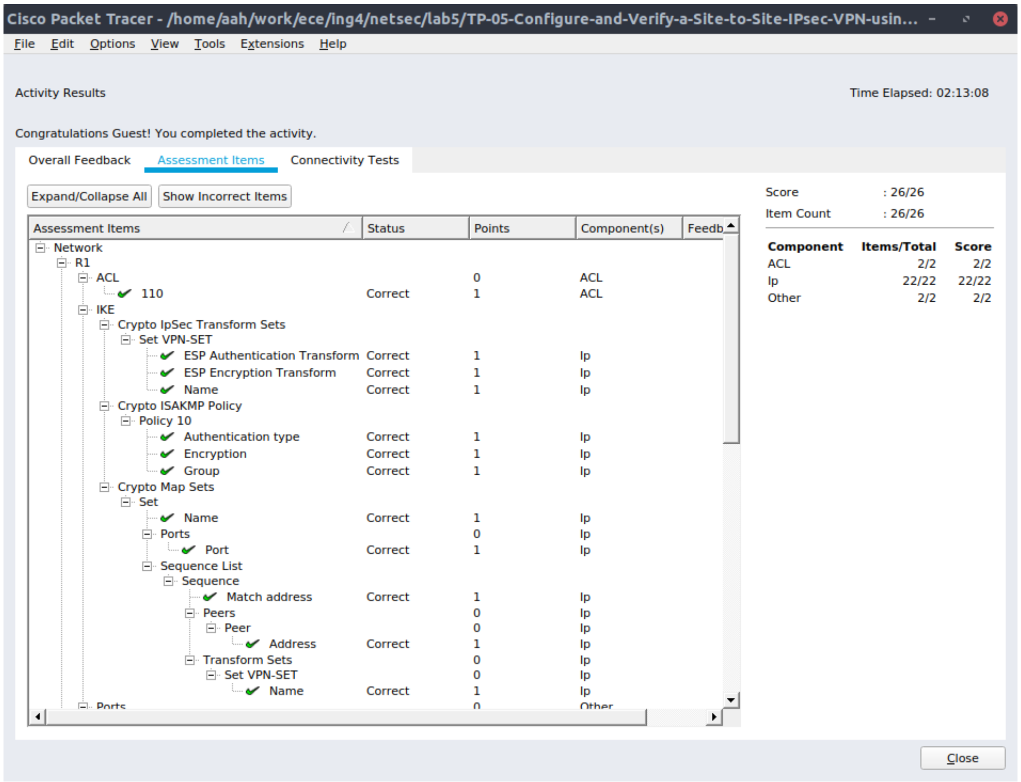
3.6 Verify the tunnel



```
       spi: 0x0814CA32(135580210)
         transform: esp-aes esp-sha-hmac ,
         in use settings ={Tunnel, }
         conn id: 2002, flow_id: FPGA:1, crypto map: VPN-MAP
         sa timing: remaining key lifetime (k/sec): (4525504/3265)
         IV size: 16 bytes
         replay detection support: N
         Status: ACTIVE

      inbound ah sas:

      inbound pcp sas:

      outbound esp sas:
       spi: 0xCF4DA9AE(3477973422)
         transform: esp-aes esp-sha-hmac ,
         in use settings ={Tunnel, }
         conn id: 2003, flow_id: FPGA:1, crypto map: VPN-MAP
         sa timing: remaining key lifetime (k/sec): (4525504/3265)
         IV size: 16 bytes
         replay detection support: N
         Status: ACTIVE

      outbound ah sas:

      outbound pcp sas:

R1#
```

Figure 11: show crypto ipsec sa

3.7 Check results


Cisco Packet Tracer - /home/aah/work/ece/ing4/netsec/lab5/TP-05-Configure-and-Verify-a-Site-to-Site-IPsec-VPN-usin...
File Edit Options View Tools Extensions Help
Overall Feedback
Assessment Items
Connectivity Tests
Expand/Collapse All
Show Incorrect Items
Close

Activity Results

Time Elapsed: 02:13:08

Congratulations Guest! You completed the activity.

Score : 26/26

Item Count : 26/26

Component	Items/Total	Score
ACL	2/2	2/2
Ip	22/22	22/22
Other	2/2	2/2

Assessment Items	Status	Points	Component(s)	Feedb
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	
Peers		0	Ip	
Peer		0	Ip	
✓ Address	Correct	1	Ip	
Transform Sets		0	Ip	
Set VPN-SET		0	Ip	
✓ Name	Correct	1	Ip	
Ports		0	Other	

Figure 12: Check results