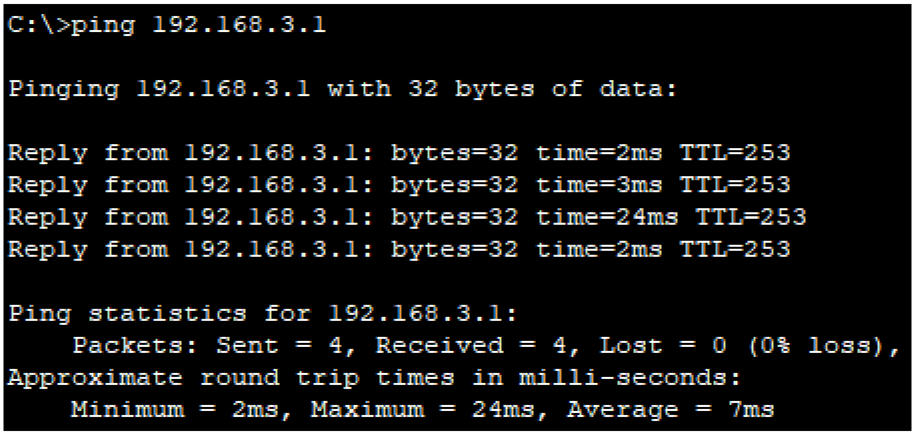
Jacques POLART
Jean-Baptiste ROUZÉ

LAB 1 : Configure and Verify a Site-to-Site IPsec VPN Using CLI

Part 1: Configure IPsec Parameters on R1

Step 1: Test connectivity.

Ping from PC-A to PC-C.



```
C:\>ping 192.168.3.1

Pinging 192.168.3.1 with 32 bytes of data:

Reply from 192.168.3.1: bytes=32 time=2ms TTL=253
Reply from 192.168.3.1: bytes=32 time=3ms TTL=253
Reply from 192.168.3.1: bytes=32 time=24ms TTL=253
Reply from 192.168.3.1: bytes=32 time=2ms TTL=253

Ping statistics for 192.168.3.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 24ms, Average = 7ms
```

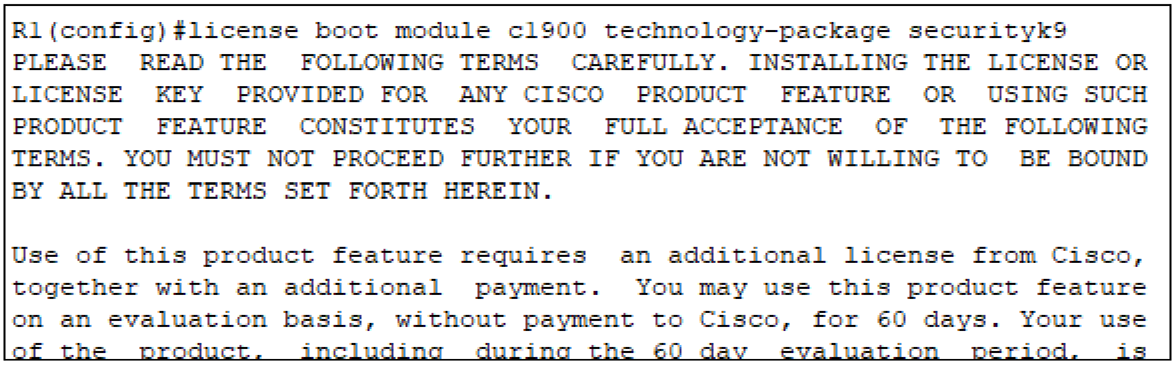
On obtient une réponse du PC C en pingant depuis le PC A

Step 2: Enable the Security Technology package.

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

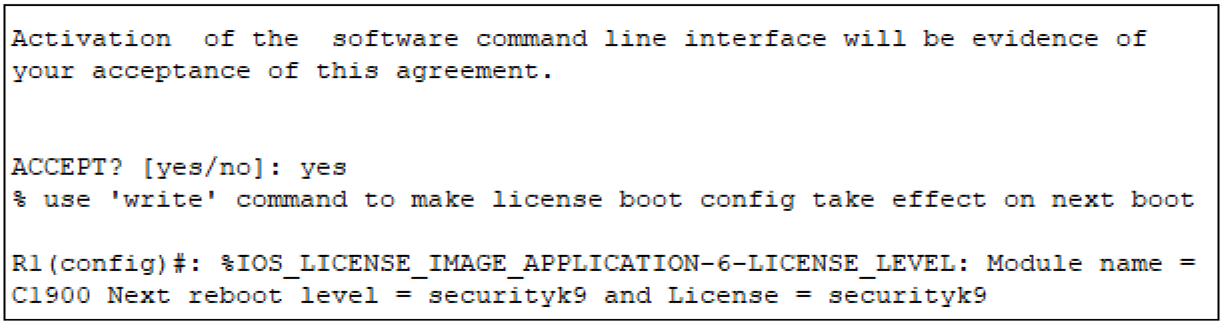
b. If the Security Technology package has not been enabled, use the following command to enable the
Package.

```
R1(config)# license boot module c1900 technology-package securityk9
```



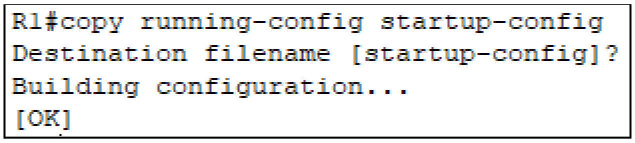
```
R1(config)#license boot module c1900 technology-package securityk9
PLEASE  READ THE  FOLLOWING TERMS  CAREFULLY. INSTALLING THE LICENSE OR
LICENSE  KEY  PROVIDED FOR  ANY CISCO  PRODUCT  FEATURE  OR  USING SUCH
PRODUCT  FEATURE  CONSTITUTES  YOUR  FULL ACCEPTANCE  OF  THE FOLLOWING
TERMS. YOU MUST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

c. Accept the end-user license agreement.

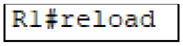


```
Activation  of the  software command line interface will be evidence of
your acceptance of this agreement.


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
```

d. Save the running-config and reload the router to enable the security license.



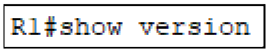
```
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```



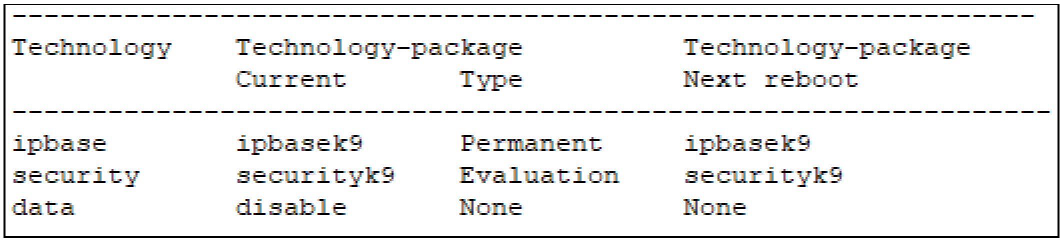
```
R1#reload
```

On sauvegarde la configuration du routeur 1.

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



```
R1#show version
```

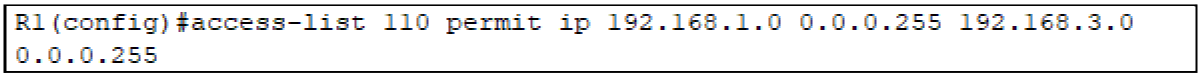


```
----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
------------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9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

Le paquet de sécurité est indiqué, il a bien été pris en compte.

Step 3: Identify interesting traffic on R1.

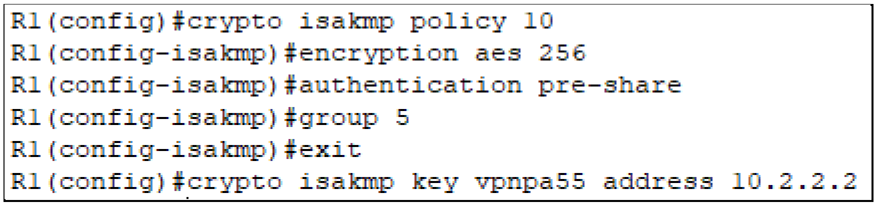
Because of the implicit deny all, there is no need to configure a deny ip any any statement.



```
R1(config)#access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0
0.0.0.255
```

Step 4: Configure the IKE Phase 1 ISAKMP policy on R1.

Configure the crypto ISAKMP policy 10 properties on R1 along with the shared crypto key vpnpa55



```
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
```

IKE (Internet Key Exchange) est également appelé ISAKMP (Internet Security Association and Key Management Protocol).
C’est le protocole de négociation qui permet à deux hôtes de convenir de la manière de construire une association de sécurité IPsec (Internet Protocol Security).

ISAKMP sépare la négociation en deux phases : Phase 1 et Phase 2.

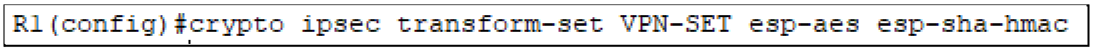
La phase 1 permet de créer le premier tunnel, ce dernier protège les messages de négociation ISAKMP.
La phase 2 est chargée de créer le tunnel qui protège les données.

Step 5 : Configure the IKE Phase 2 IPsec policy on R1.

a) Create the transform-set VPN-SET to use esp-aes and esp-sha-hmac.

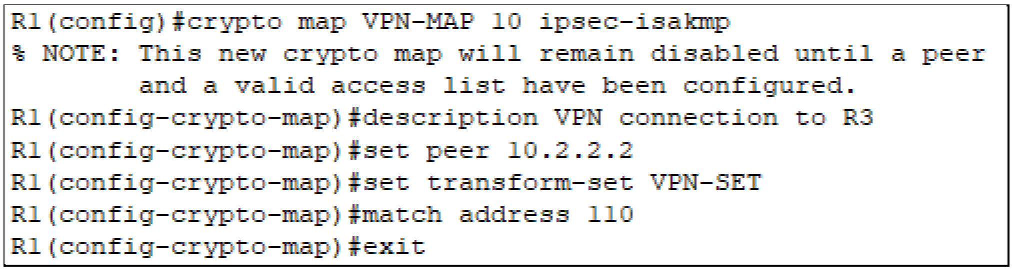
Esp-aes : **E**ncapsulating **S**ecurity **P**ayload
- Advanced **E**ncryption **S**tandard
Un algorithme cryptographique qui protège les informations sensibles et non classifiées.

Esp-sha-hmac : **E**ncapsulating **S**ecurity **P**ayload
-Secure **H**ash **A**lgorithm
- Hash-based **M**essage **A**uthentication **C**ode
HMAC est une variante de hachage à clé utilisée pour authentifier les données.



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

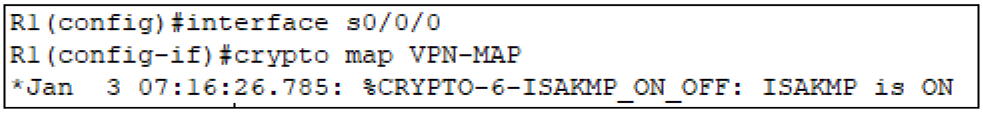
Create the crypto map VPN-MAP that binds all of the Phase 2 parameters together. Use sequence number 10 and identify it as an ipsec-isakmp map.



```
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
```

Step 6: Configure the crypto map on the outgoing interface.

Bind the VPN-MAP crypto map to the outgoing Serial 0/0/0 interface.



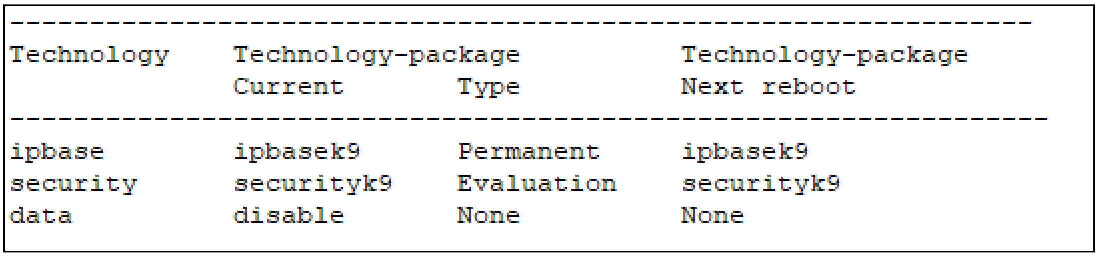
```
R1(config)#interface s0/0/0
R1(config-if)#crypto map VPN-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

Une crypto map est une entité de configuration logicielle qui remplit deux fonctions principales :
- Elle sélectionne les flux de données qui nécessitent un traitement de sécurité.
- Elle définit la politique pour ces flux et l' homologue cryptographique vers lequel ce trafic doit aller.

PART 2 : Configure IPsec Parameters on R3

Step 1: Enable the Security Technology package.

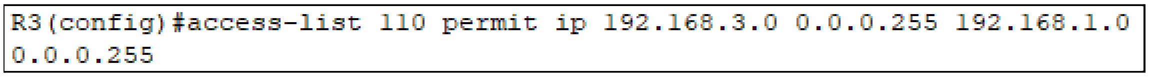
a. On R3, issue the show version command to verify that the Security Technology package license information has been enabled.



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

Le paquet de sécurité est bien activé.

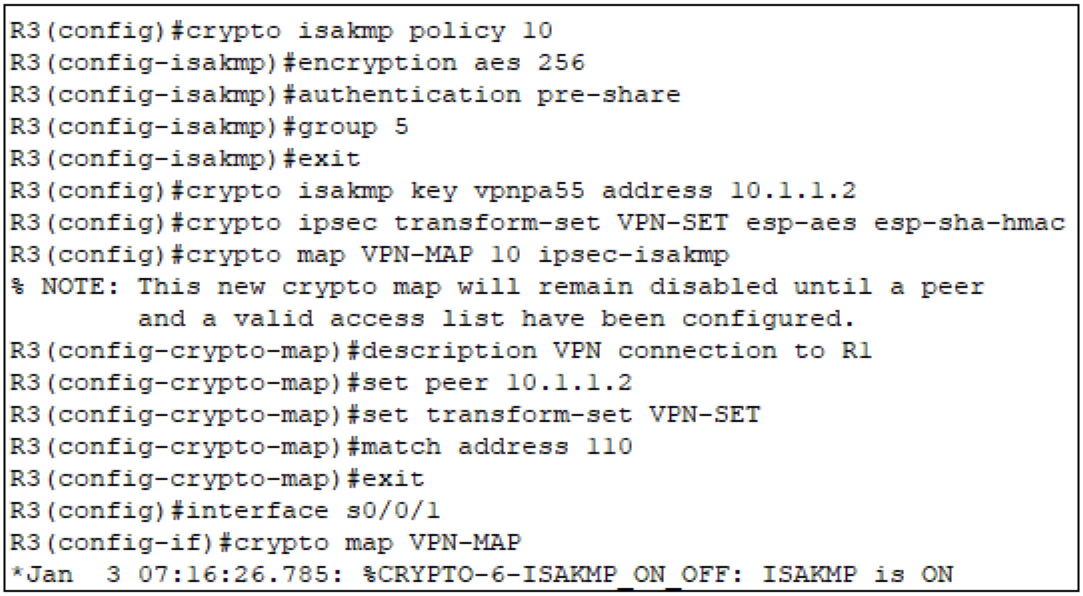
Step 2: Configure router R3 to support a site-to-site VPN with R1.



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

Step 3: Configure the IKE Phase 1 ISAKMP properties on R3.

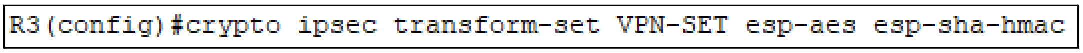
Configure the crypto ISAKMP policy 10 properties on R3 along with the shared crypto key vpnpa55.



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

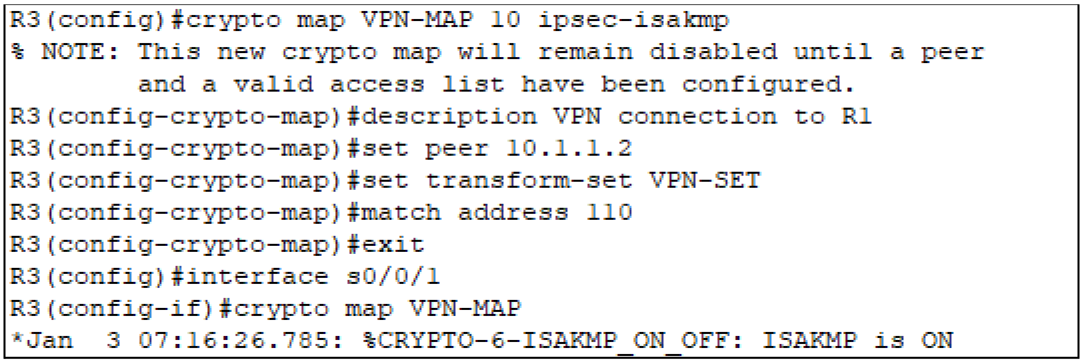
Step 4: Configure the IKE Phase 2 IPsec policy on R3.

a. Create the transform-set VPN-SET to use esp-aes and esp-sha-hmac.



```
R3(config)#crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
```

b. Create the crypto map VPN-MAP that binds all of the Phase 2 parameters together. Use sequence number 10 and identify it as an ipsec-isakmp map.

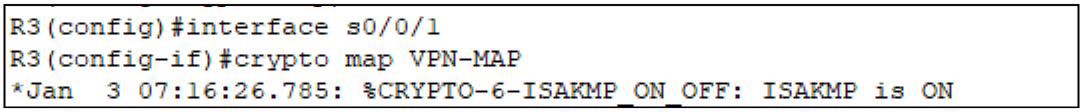


```
R3(config)#crypto map VPN-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R3(config-crypto-map)#description VPN connection to R1
R3(config-crypto-map)#set peer 10.1.1.2
R3(config-crypto-map)#set transform-set VPN-SET
R3(config-crypto-map)#match address 110
R3(config-crypto-map)#exit
R3(config)#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
```

Step 5: Configure the crypto map on the outgoing interface.

Bind the VPN-MAP crypto map to the outgoing Serial 0/0/1 interface. Note: This is not graded.

R3(config)# interface s0/0/1
R3(config-if)# crypto map VPN-MAP

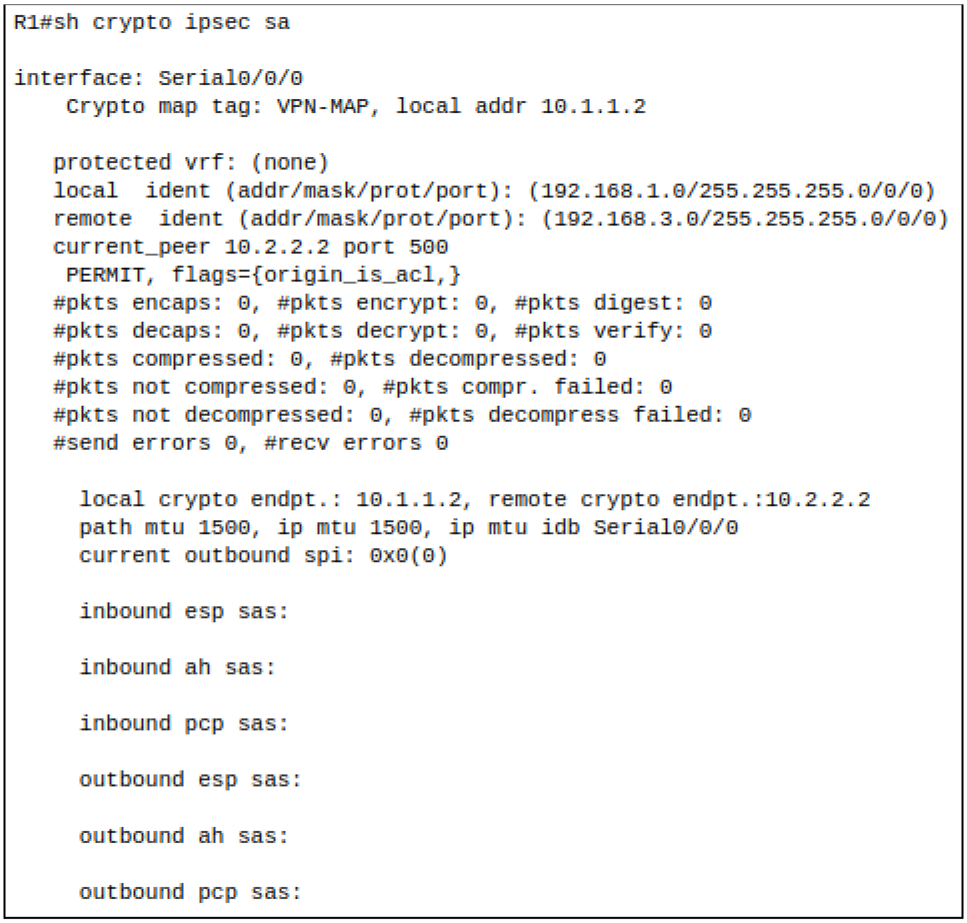


```
R3(config)#interface s0/0/1
R3(config-if)#crypto map VPN-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

Part 3: Verify the IPsec VPN

Step 1: Verify the tunnel prior to interesting traffic.

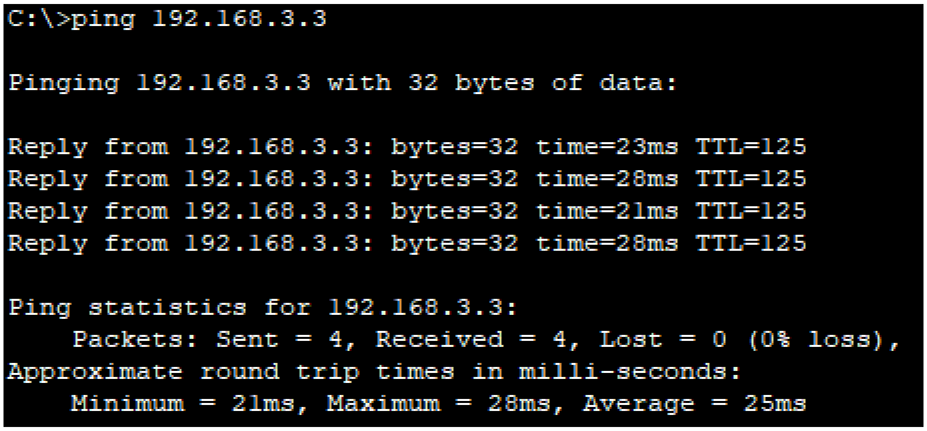
Issue the show crypto **ipsec sa** command on R1. Notice that the number of packets encapsulated, encrypted, decapsulated, and decrypted are all set to 0.



```
R1#sh 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:
```

Step 2: Create interesting traffic.

Ping PC-C from PC-A.

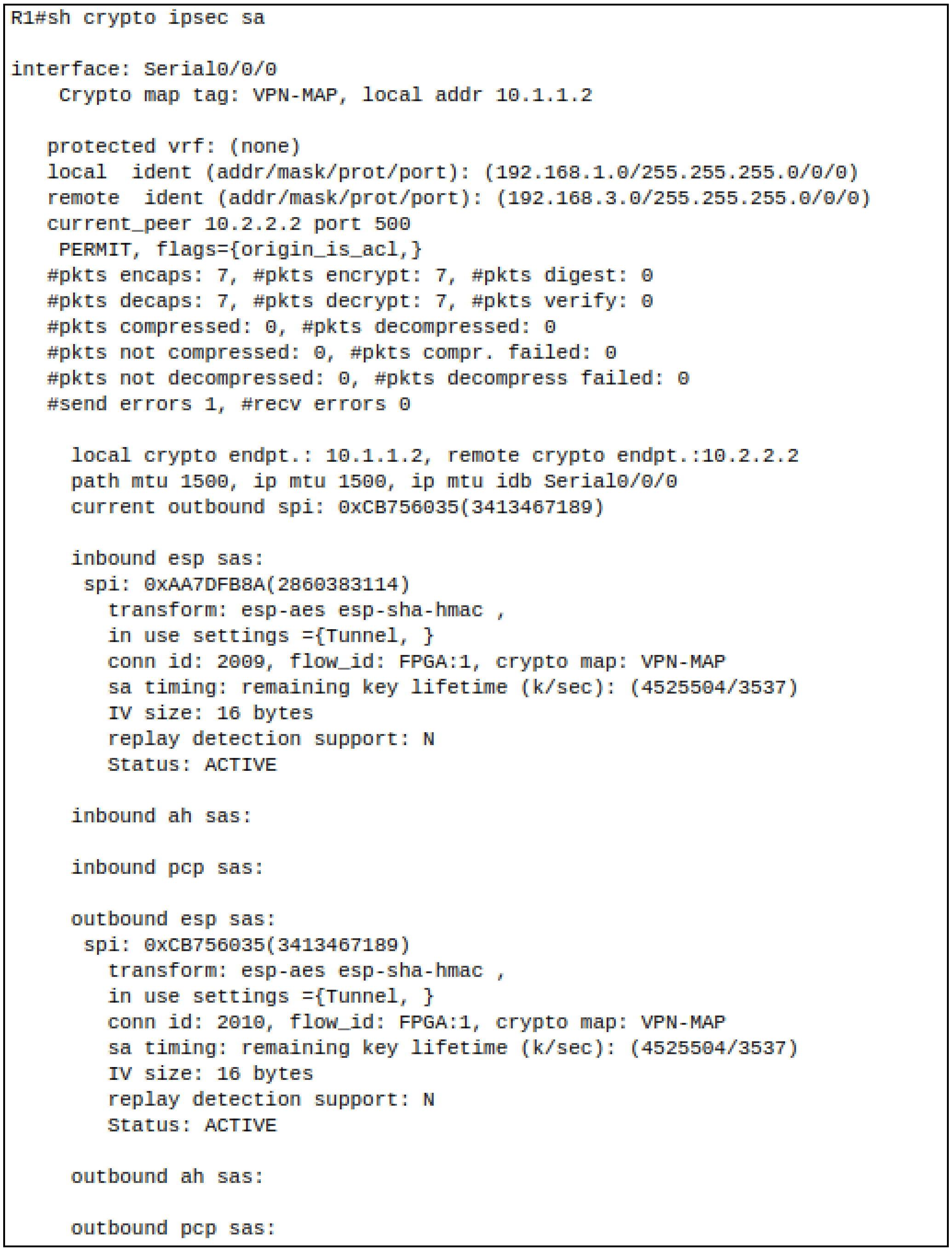


```
C:\>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Reply from 192.168.3.3: bytes=32 time=23ms TTL=125
Reply from 192.168.3.3: bytes=32 time=28ms TTL=125
Reply from 192.168.3.3: bytes=32 time=21ms TTL=125
Reply from 192.168.3.3: bytes=32 time=28ms TTL=125

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 21ms, Maximum = 28ms, Average = 25ms
```

Le PC C reçoit tous les paquets.

Step 3: Verify the tunnel after interesting traffic.

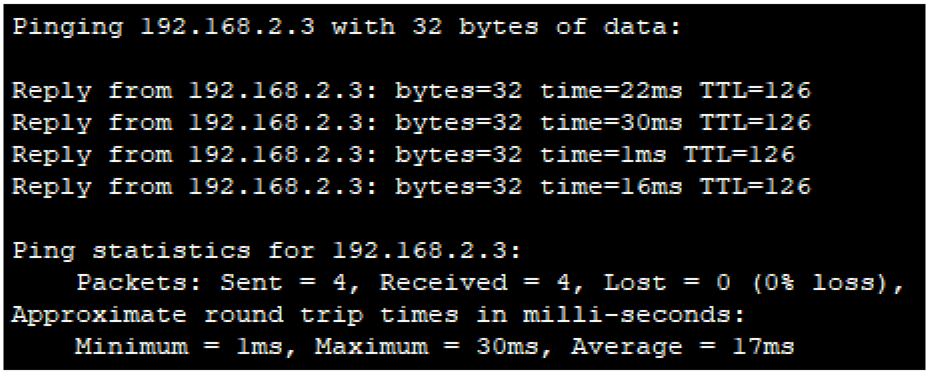
On R1, re-issue the show crypto ipsec sa command. Notice that the number of packets is more than 0, which indicates that the IPsec VPN tunnel is working.



```
R1#sh 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: 7, #pkts encrypt: 7, #pkts digest: 0
   #pkts decaps: 7, #pkts decrypt: 7, #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

     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: 0xCB756035(3413467189)

     inbound esp sas:
      spi: 0xAA7DFB8A(2860383114)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2009, flow_id: FPGA:1, crypto map: VPN-MAP
        sa timing: remaining key lifetime (k/sec): (4525504/3537)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xCB756035(3413467189)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2010, flow_id: FPGA:1, crypto map: VPN-MAP
        sa timing: remaining key lifetime (k/sec): (4525504/3537)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:
```

Step 4: Create uninteresting traffic.

Ping PC-B from PC-A. Note: Issuing a ping from router R1 to PC-C or R3 to PC-A is not interesting traffic.

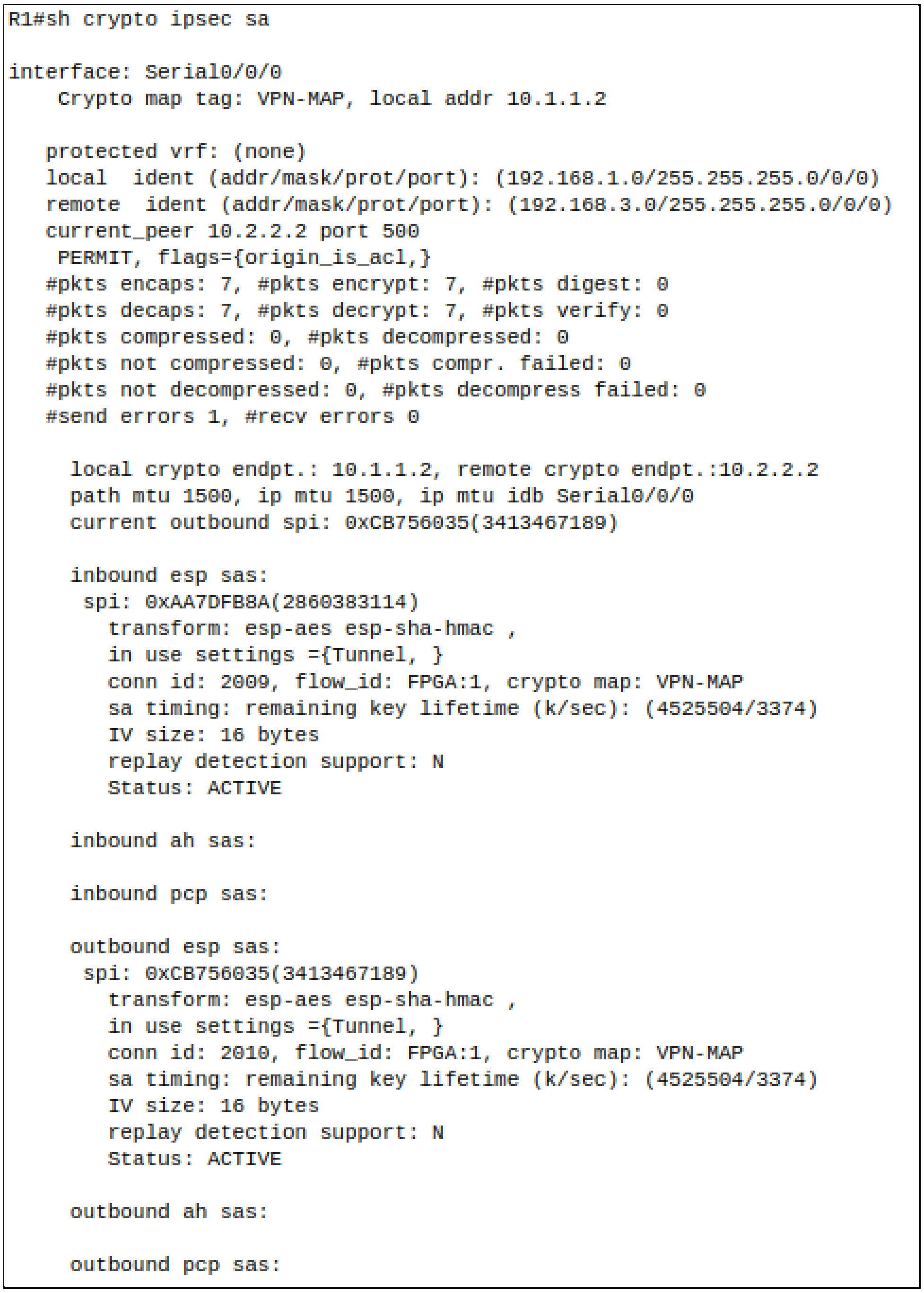


```
Pinging 192.168.2.3 with 32 bytes of data:

Reply from 192.168.2.3: bytes=32 time=22ms TTL=126
Reply from 192.168.2.3: bytes=32 time=30ms TTL=126
Reply from 192.168.2.3: bytes=32 time=1ms TTL=126
Reply from 192.168.2.3: bytes=32 time=16ms TTL=126

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 30ms, Average = 17ms
```

Le PC-B reçoit tous les paquets.

Step 5: Verify the tunnel.

On R1, re-issue the show crypto ipsec sa command. Notice that the number of packets has not changed, which verifies that uninteresting traffic is not encrypted.

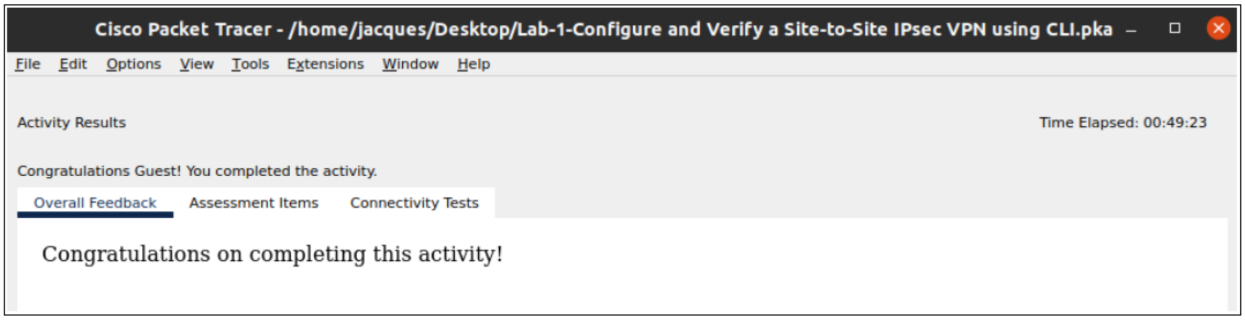


```
R1#sh crypto ipsec sa

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: 7, #pkts encrypt: 7, #pkts digest: 0
   #pkts decaps: 7, #pkts decrypt: 7, #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

     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: 0xCB756035(3413467189)

     inbound esp sas:
      spi: 0xAA7DFB8A(2860383114)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2009, flow_id: FPGA:1, crypto map: VPN-MAP
        sa timing: remaining key lifetime (k/sec): (4525504/3374)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xCB756035(3413467189)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2010, flow_id: FPGA:1, crypto map: VPN-MAP
        sa timing: remaining key lifetime (k/sec): (4525504/3374)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:
```

Tous les paquets encapsulés et cryptés peuvent être décapsulés et décryptés. Le trafic inintéressant n’est pas encrypté.

Step 6: Check results.

Your completion percentage should be 100%. Click Check Results to see feedback and verification of which required components have been completed.



Cisco Packet Tracer - /home/jacques/Desktop/Lab-1-Configure and Verify a Site-to-Site IPsec VPN using CLI.pka
File
Edit
Options
View
Tools
Extensions
Window
Help
Overall Feedback
Assessment Items
Connectivity Tests

Activity Results

Time Elapsed: 00:49:23

Congratulations Guest! You completed the activity.

Congratulations on completing this activity!