# Lab 12

# Configure and Verify a Site-to-Site IPsec VPN

| Name: Syed Asghar Abbas Zaidi | Student ID: 07201 |
|---|---|

## 12.1 Objective

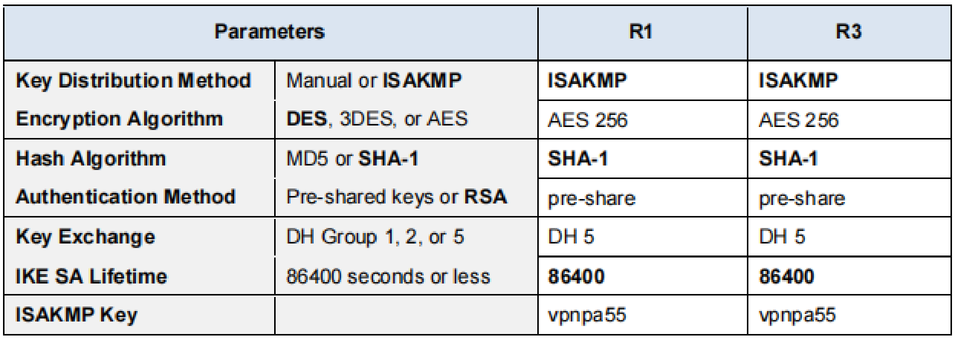
The Objectives of this lab are:

- Verify connectivity throughout the network.
- Configure R1 to support a site-to-site IPsec VPN with R3.

## 12.2 Background/Scenario

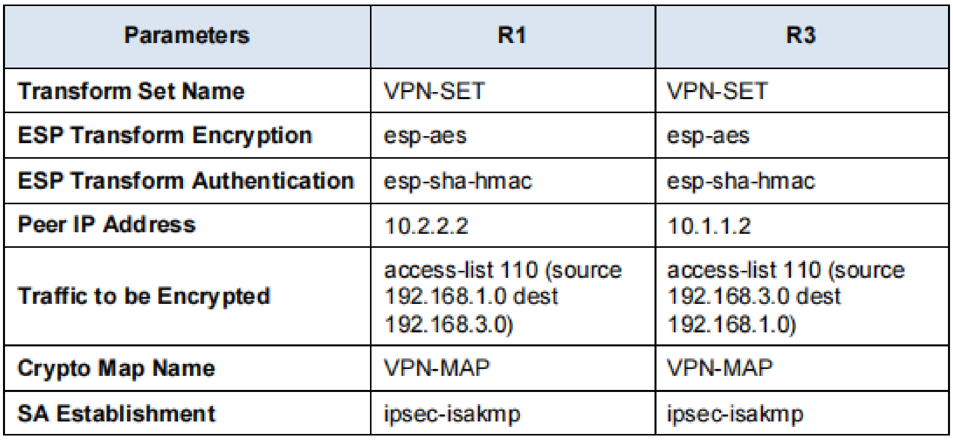
The network topology shows three routers. Your task is to configure R1 and R3 to support a site-to-site IPsec VPN when traffic flows between their respective LANs. The IPsec VPN tunnel is from R1 to R3 via R2. R2 acts as a pass-through and has no knowledge of the VPN. IPsec provides secure transmission of sensitive information over unprotected networks, such as the Internet. IPsec operates at the network layer and protects and authenticates IP packets between participating IPsec devices (peers), such as Cisco routers.

**ISAKMP Phase 1 Policy Parameters**



| Parameters | | R1 | R3 |
|---|---|---|---|
| **Key Distribution Method** | Manual or **ISAKMP** | **ISAKMP** | **ISAKMP** |
| **Encryption Algorithm** | **DES**, 3DES, or AES | AES 256 | AES 256 |
| **Hash Algorithm** | MD5 or **SHA-1** | **SHA-1** | **SHA-1** |
| **Authentication Method** | Pre-shared keys or **RSA** | pre-share | pre-share |
| **Key Exchange** | DH Group 1, 2, or 5 | DH 5 | DH 5 |
| **IKE SA Lifetime** | 86400 seconds or less | **86400** | **86400** |
| **ISAKMP Key** | | vpnpa55 | vpnpa55 |

**IPsec Phase 2 Policy Parameters**



| Parameters | R1 | R3 |
|---|---|---|
| **Transform Set Name** | VPN-SET | VPN-SET |
| **ESP Transform Encryption** | esp-aes | esp-aes |
| **ESP Transform Authentication** | esp-sha-hmac | esp-sha-hmac |
| **Peer IP Address** | 10.2.2.2 | 10.1.1.2 |
| **Traffic to be Encrypted** | access-list 110 (source 192.168.1.0 dest 192.168.3.0) | access-list 110 (source 192.168.3.0 dest 192.168.1.0) |
| **Crypto Map Name** | VPN-MAP | VPN-MAP |
| **SA Establishment** | ipsec-isakmp | ipsec-isakmp |

**Note:** Bolded parameters are defaults. Only unbolded parameters have to be explicitly configured.

The routers have been pre-configured with the following:

- Password for console line: **ciscoconpa55**
- Password for vty lines: **ciscovtypa55**
- Enable password: **ciscoenpa55**
- SSH username and password: **SSHadmin / ciscosshpa55**
- OSPF 101

## 12.3 Topology

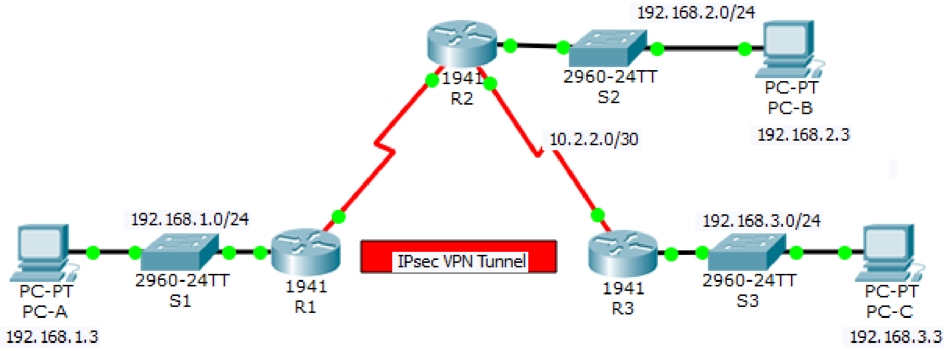
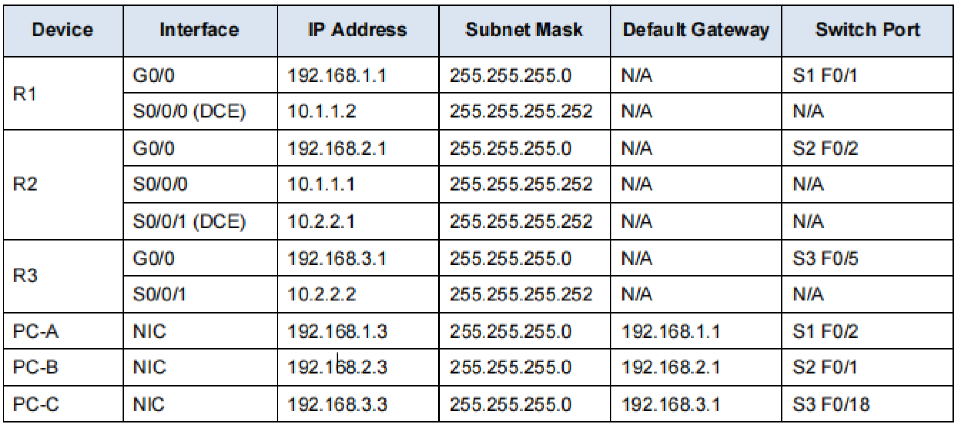


Figure 1: Topology

## 12.4 Addressing Table



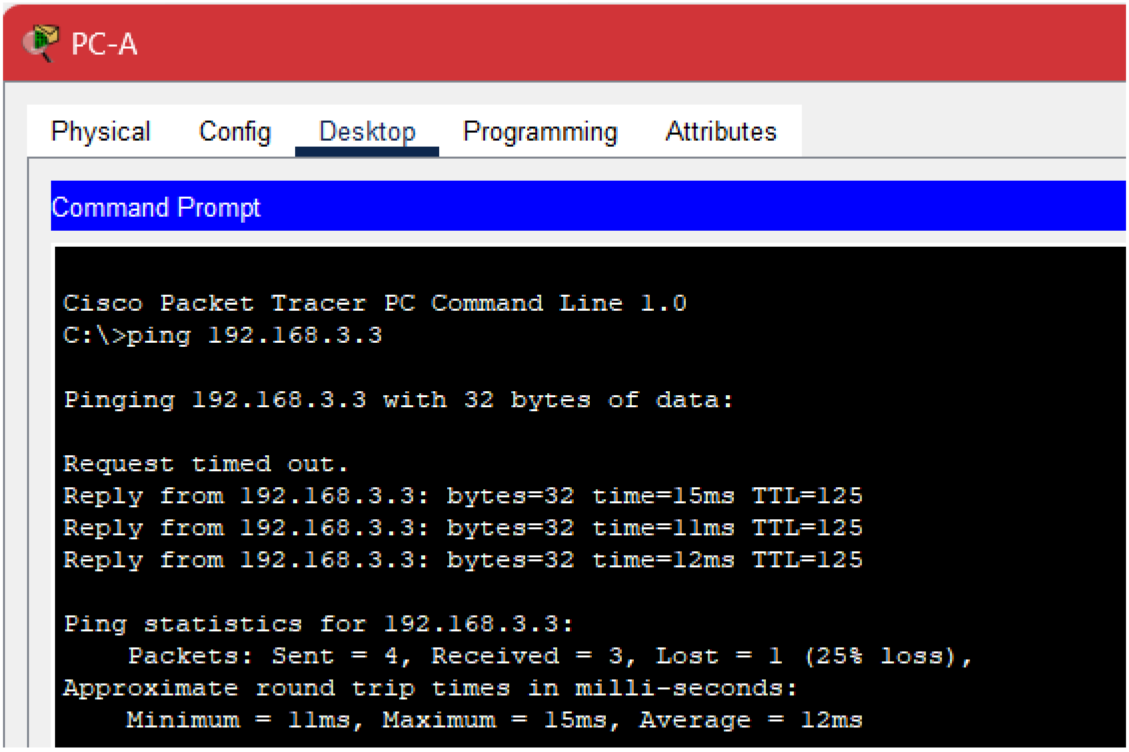
| Device | Interface | IP Address | Subnet Mask | Default Gateway | Switch Port |
|---|---|---|---|---|---|
| R1 | G0/0 | 192.168.1.1 | 255.255.255.0 | N/A | S1 F0/1 |
| | S0/0/0 (DCE) | 10.1.1.2 | 255.255.255.252 | N/A | N/A |
| R2 | G0/0 | 192.168.2.1 | 255.255.255.0 | N/A | S2 F0/2 |
| | S0/0/0 | 10.1.1.1 | 255.255.255.252 | N/A | N/A |
| | S0/0/1 (DCE) | 10.2.2.1 | 255.255.255.252 | N/A | N/A |
| R3 | G0/0 | 192.168.3.1 | 255.255.255.0 | N/A | S3 F0/5 |
| | S0/0/1 | 10.2.2.2 | 255.255.255.252 | N/A | N/A |
| PC-A | NIC | 192.168.1.3 | 255.255.255.0 | 192.168.1.1 | S1 F0/2 |
| PC-B | NIC | 192.168.2.3 | 255.255.255.0 | 192.168.2.1 | S2 F0/1 |
| PC-C | NIC | 192.168.3.3 | 255.255.255.0 | 192.168.3.1 | S3 F0/18 |

Figure 2: Addressing Table

## Task 1: Configure IPsec Parameters on R1

1. Test connectivity

   Ping from PC-A to 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=15ms TTL=125
Reply from 192.168.3.3: bytes=32 time=11ms TTL=125
Reply from 192.168.3.3: bytes=32 time=12ms 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 = 11ms, Maximum = 15ms, Average = 12ms
```

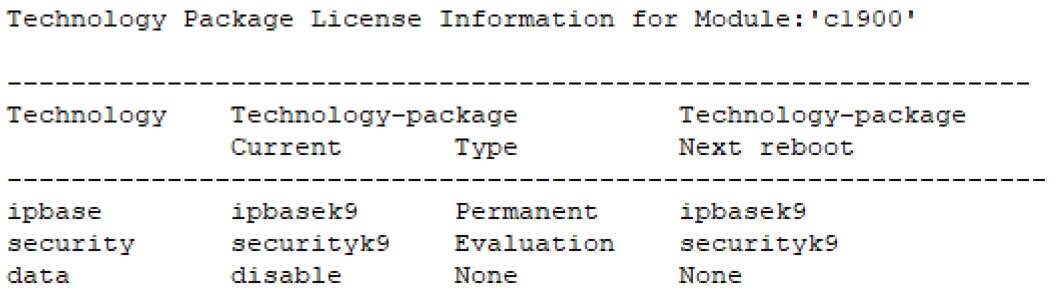
2. Enable the Security Technology Package
   a. On R1, issue the **show version** command to view the Security Technology package license information.
   b. If the Security Technology package has not been enabled, use the following command to enable the package.

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

   c. Accept the end-user license agreement
   d. Save the running-config and reload the router to enable the security license
   e. Verify that the Security Technology package has been enabled by using the **show version** command

```
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
```

It’s not enabled, enabling.
Loaded it, wrote it in the memory and then reloaded the device, I have already showcase how to do these steps in detail in lab 8
Proof that the package was loaded

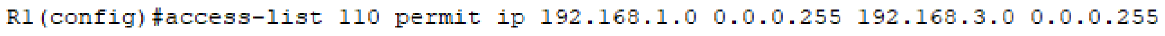


```
Technology Package License Information for Module:'c1900'

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

3. Identify Interesting traffic on R1

Configure ACL 110 to identify the traffic from the LAN on R1 to the LAN on R3 as interesting. This interesting traffic will trigger the IPsec VPN to be implemented when there is traffic between the R1 to R3 LANs. All other traffic sourced from the LANs will not be encrypted. 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
```



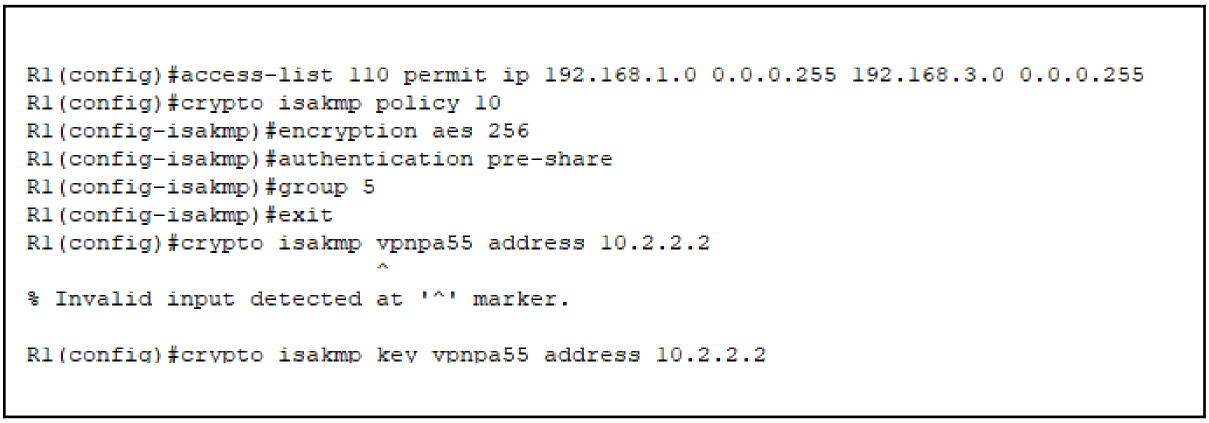
```
R1(config)#access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
```

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**. Refer to the ISAKMP Phase 1 table for the specific parameters to configure. Default values do not have to be configured. Therefore, only the encryption method, key exchange method, and DH method must be configured.

**Note:** The highest DH group currently supported by Packet Tracer is group 5. In a production network, you would configure at least DH 14.

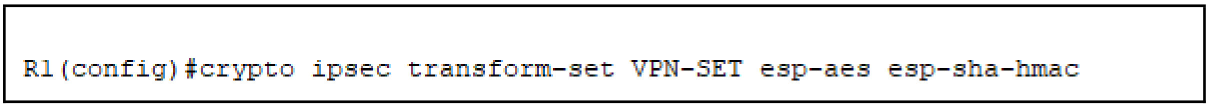
```
R1(config)# crypto isakmp policy 10
R1(config-isakmp)# encryption aes 256
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# group 5
R1(config-isakmp)# exit
R1(config)# crypto isakmp key vpnpa55 address 10.2.2.2
```



```
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)#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 vpnpa55 address 10.2.2.2
                         ^
% Invalid input detected at '^' marker.

R1(config)#crypto isakmp key vpnpa55 address 10.2.2.2
```

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.**

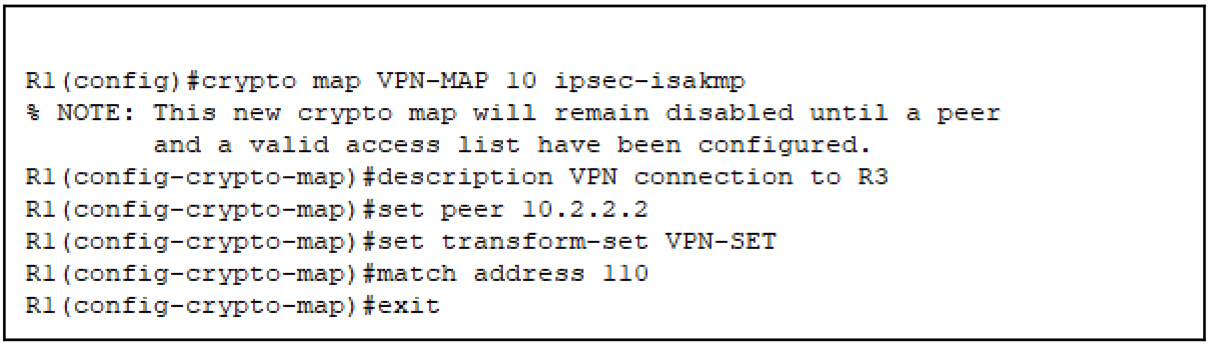
       R1(config)# **crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac**



```
R1(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.

       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**

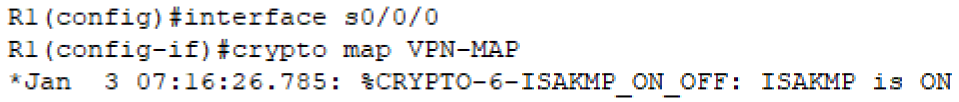


```
R1(config)#crypto map VPN-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R1(config-crypto-map)#description VPN connection to R3
R1(config-crypto-map)#set peer 10.2.2.2
R1(config-crypto-map)#set transform-set VPN-SET
R1(config-crypto-map)#match address 110
R1(config-crypto-map)#exit
```

6. Configure the crypto map on the outgoing interface

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

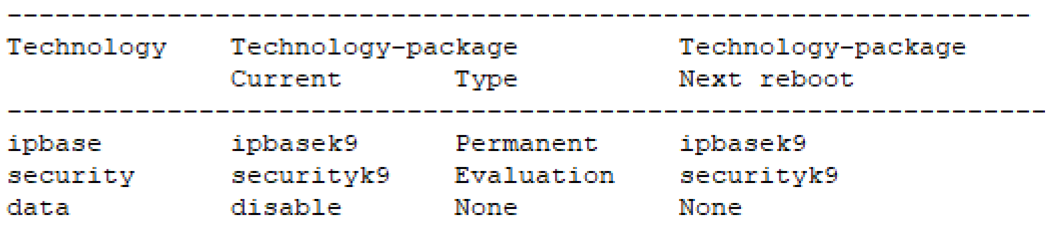
   `R1(config)#` **interface s0/0/0**
   `R1(config-if)#` **crypto map VPN-MAP**



```
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
```

## Task 2: Configure IPsec Parameters on R3

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
```

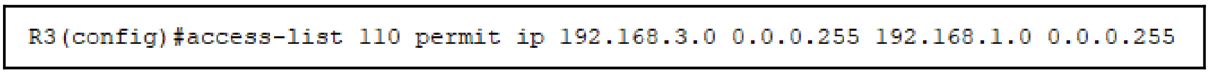
   b. If the Security Technology package has not been enabled, enable the package and reload R3.

It is already loaded

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

Configure reciprocating parameters on R3. Configure ACL 110 identifying the traffic from the LAN on R3 to the LAN on R1 as interesting.

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

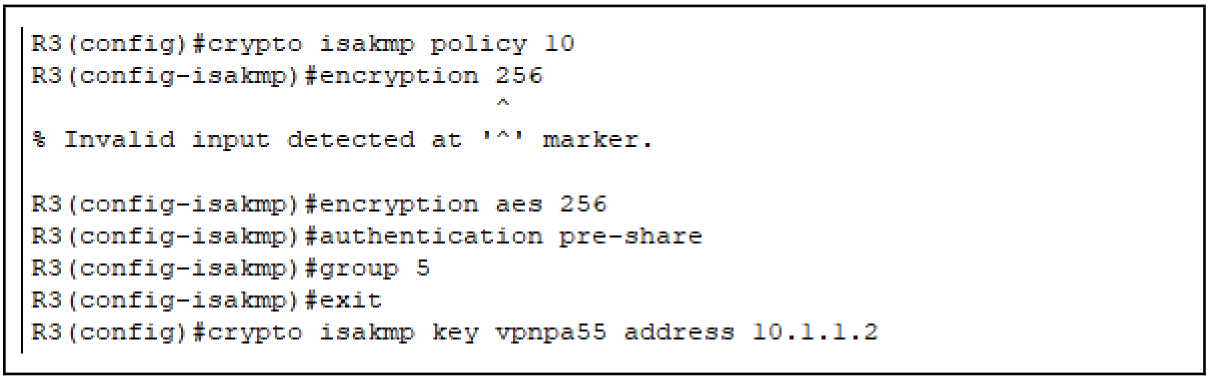


```
R3(config)#access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
```

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.

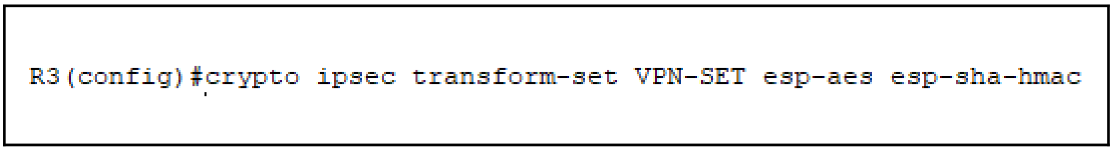
```
R3(config)# crypto isakmp policy 10
R3(config-isakmp)# encryption aes 256
R3(config-isakmp)# authentication pre-share
R3(config-isakmp)# group 5
R3(config-isakmp)# exit
R3(config)# crypto isakmp key vpnpa55 address 10.1.1.2
```



```
R3(config)#crypto isakmp policy 10
R3(config-isakmp)#encryption 256
                            ^
% Invalid input detected at '^' marker.

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
```

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**

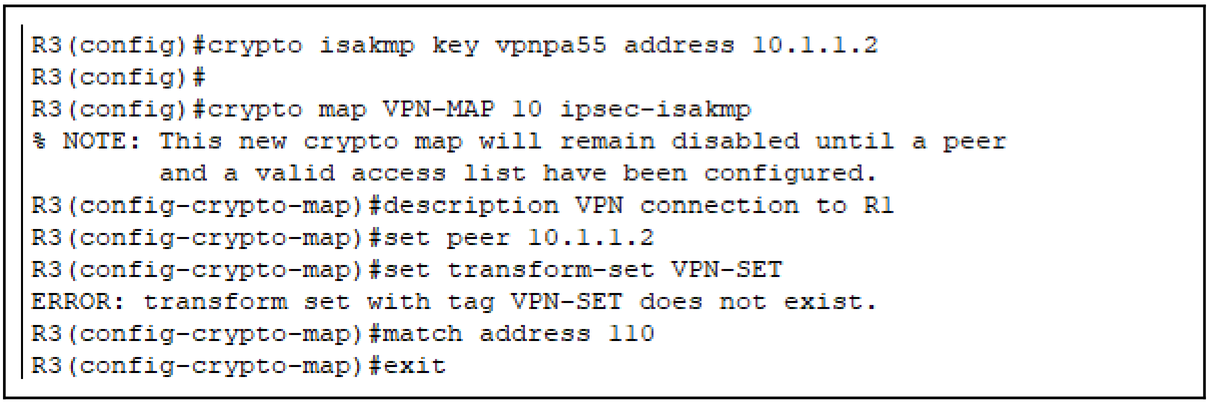
```
R3(config)# crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
```



```
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
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
```

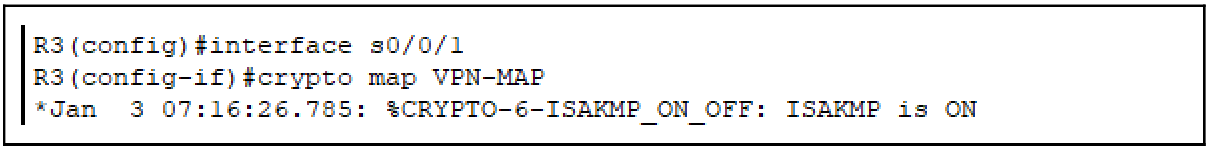


```
R3(config)#crypto isakmp key vpnpa55 address 10.1.1.2
R3(config)#
R3(config)#crypto map VPN-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R3(config-crypto-map)#description VPN connection to R1
R3(config-crypto-map)#set peer 10.1.1.2
R3(config-crypto-map)#set transform-set VPN-SET
ERROR: transform set with tag VPN-SET does not exist.
R3(config-crypto-map)#match address 110
R3(config-crypto-map)#exit
```

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
```

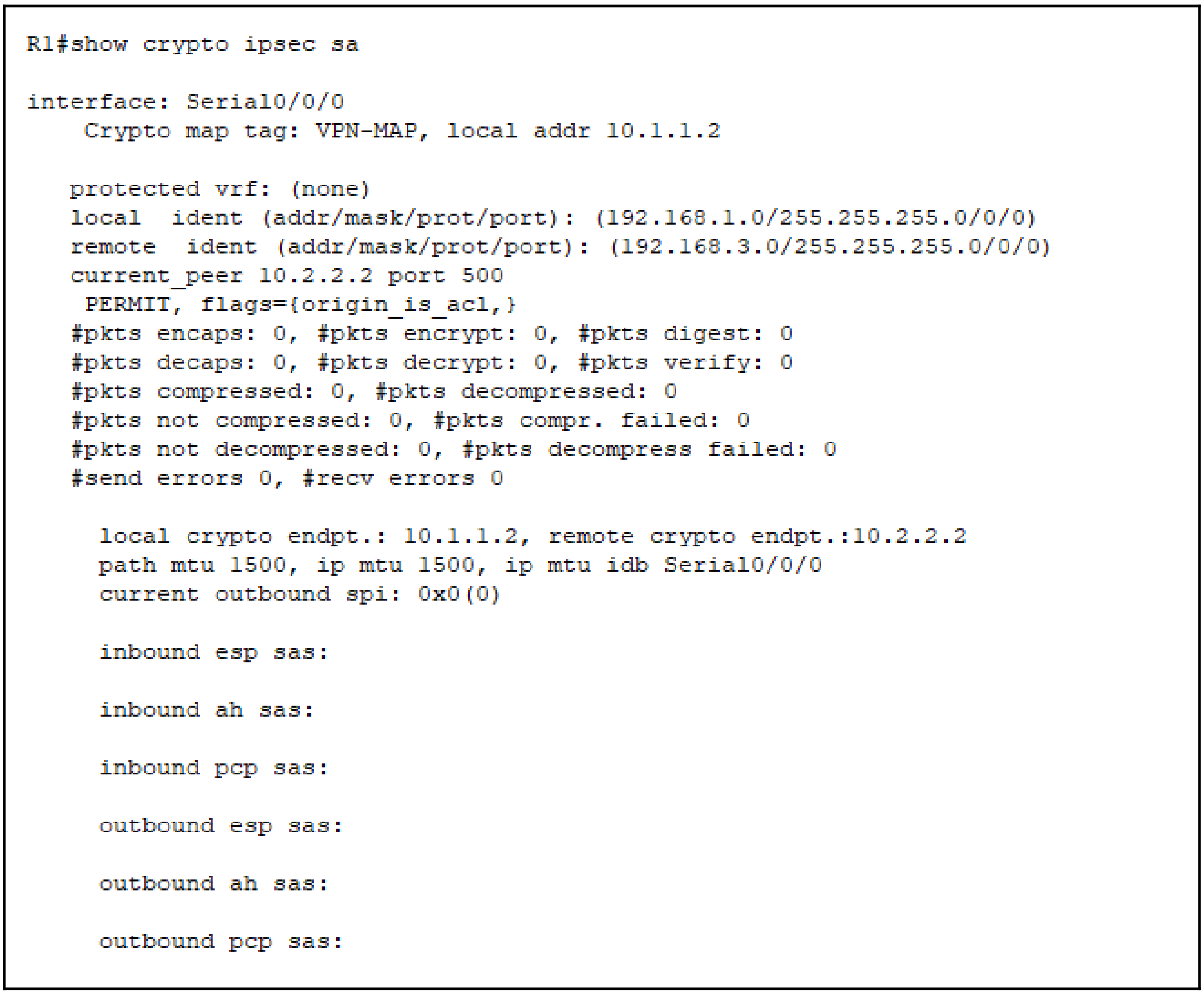


```
R3(config)#interface s0/0/1
R3(config-if)#crypto map VPN-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

## Task 3: Verify the IPsec VPN

1. Verify the tunnel prior to interesting traffic.

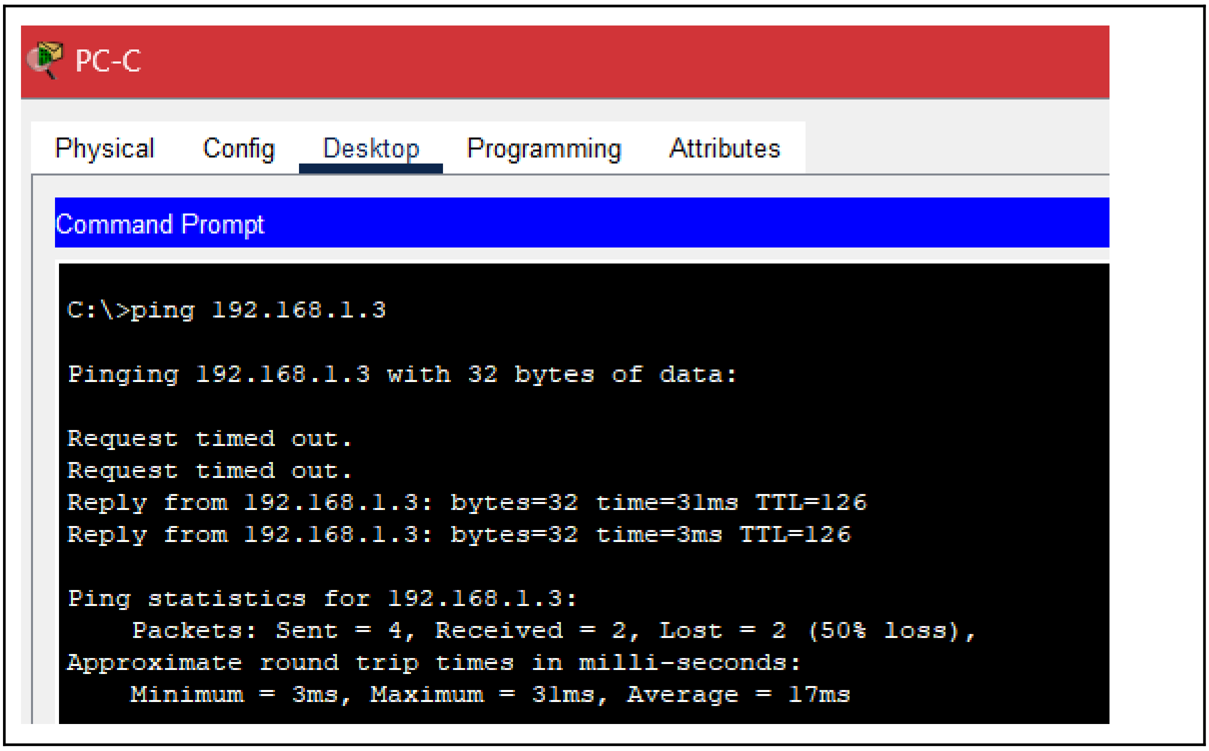
   Issue the **show crypto ipsec sa** command on R1. Notice that the number of packets encapsulated, encrypted, decapsulated, and decrypted are all set to 0.



```
R1#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:
```

2. Create interesting traffic.

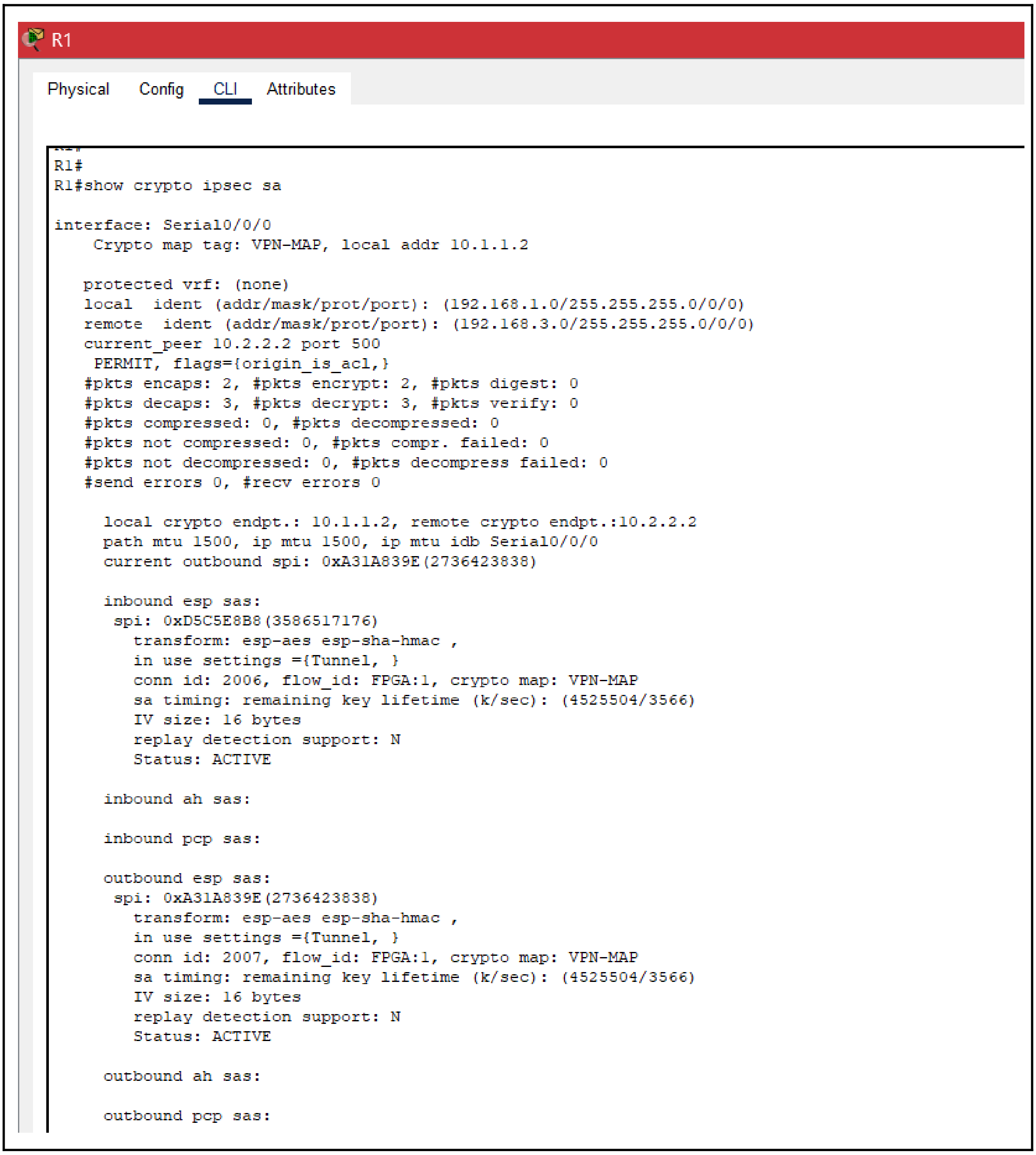
   Ping PC-C from PC-A.



```
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 192.168.1.3: bytes=32 time=31ms TTL=126
Reply from 192.168.1.3: bytes=32 time=3ms TTL=126

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 31ms, Average = 17ms
```

3. Verify the tunnel after interesting traffic

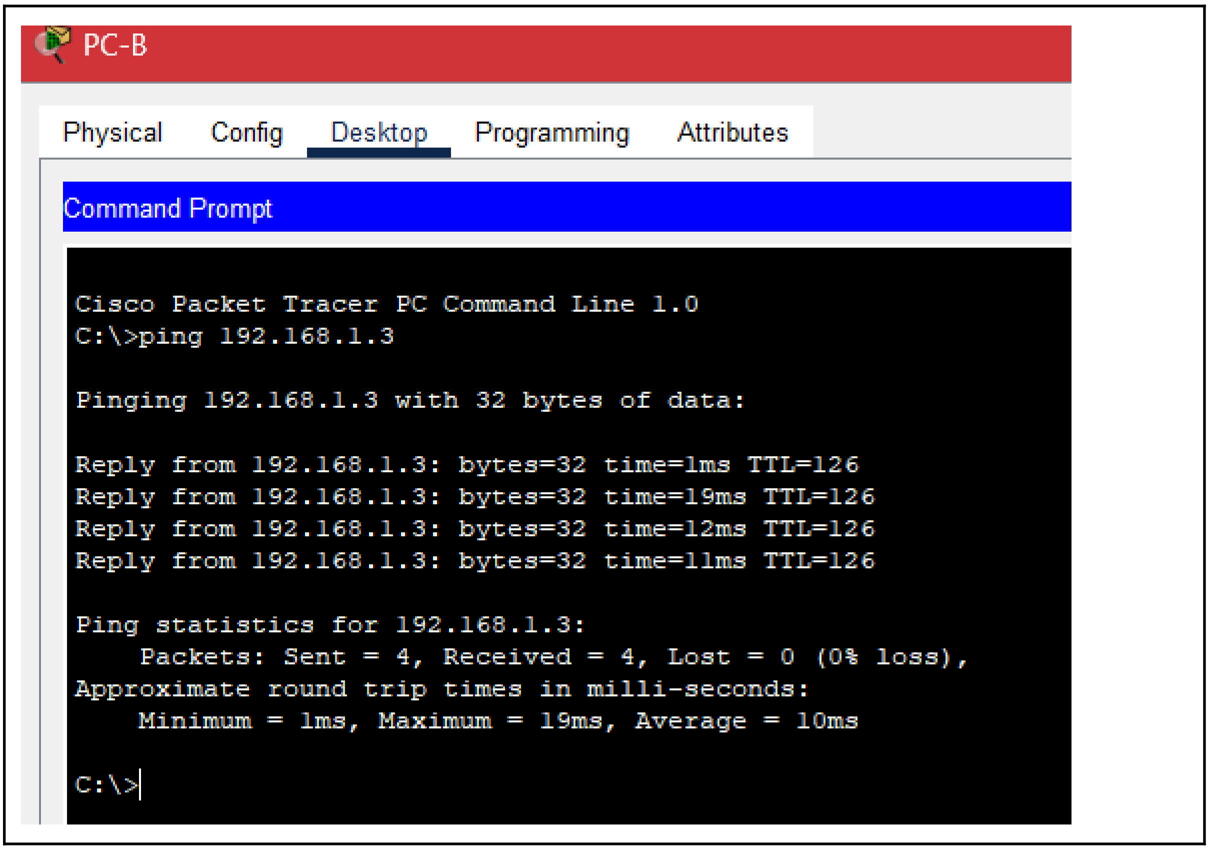
   On R1, re-issue the **show crypto ipsec sa** command. Notice that the number of packets is more than 0, which indicates that the IPsec VPN tunnel is working.



```
R1#
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: 2, #pkts encrypt: 2, #pkts digest: 0
   #pkts decaps: 3, #pkts decrypt: 3, #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: 0xA31A839E(2736423838)

     inbound esp sas:
      spi: 0xD5C5E8B8(3586517176)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2006, flow_id: FPGA:1, crypto map: VPN-MAP
        sa timing: remaining key lifetime (k/sec): (4525504/3566)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xA31A839E(2736423838)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2007, flow_id: FPGA:1, crypto map: VPN-MAP
        sa timing: remaining key lifetime (k/sec): (4525504/3566)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:
```

4. Create uninteresting traffic.

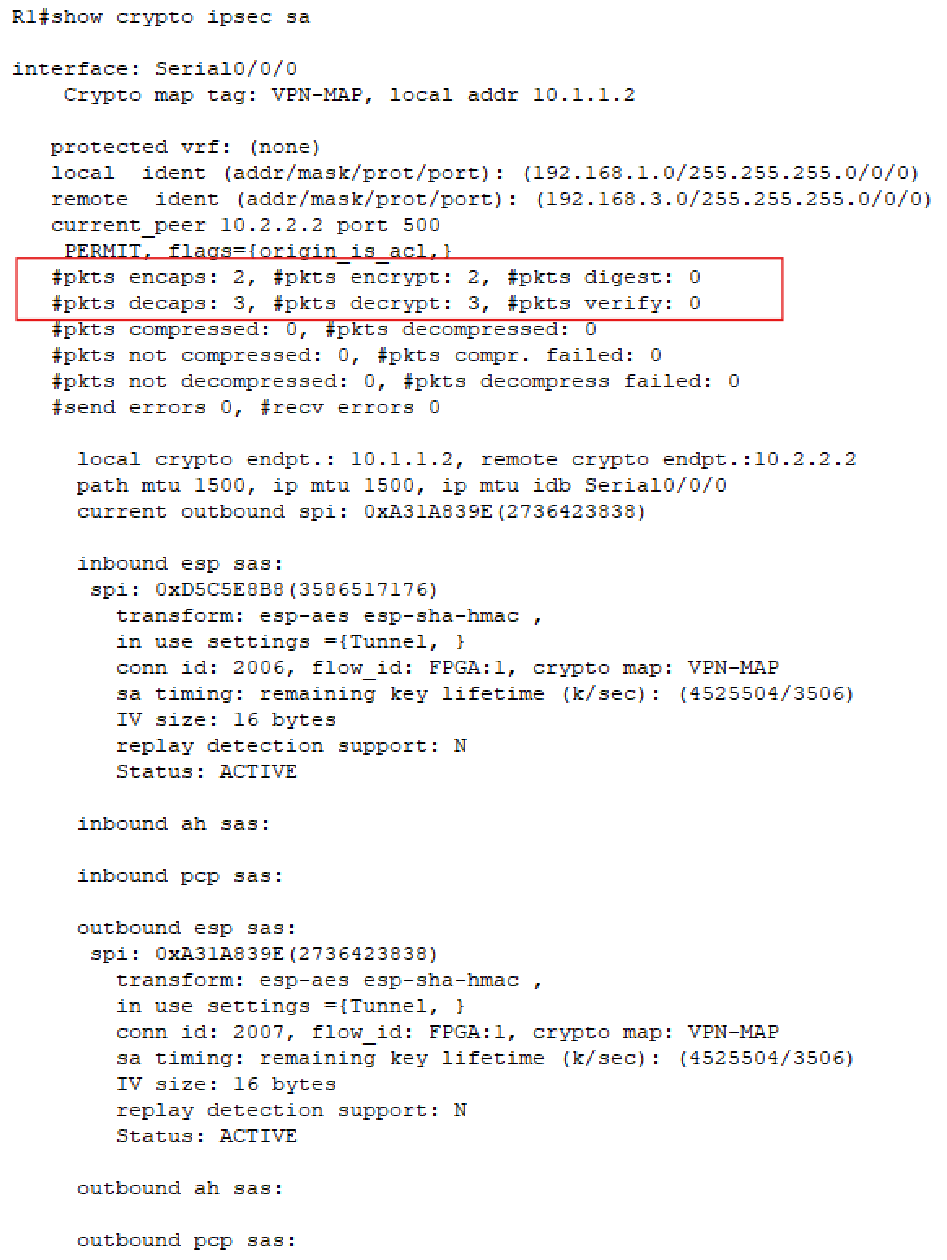
   Ping PC-B from PC-A. **Note:** Issuing a ping from router R1 to PC-C or R3 to PC-A is not interesting traffic.



```
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=1ms TTL=126
Reply from 192.168.1.3: bytes=32 time=19ms TTL=126
Reply from 192.168.1.3: bytes=32 time=12ms TTL=126
Reply from 192.168.1.3: bytes=32 time=11ms 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 = 1ms, Maximum = 19ms, Average = 10ms

C:\>
```

5. Verify the tunnel.

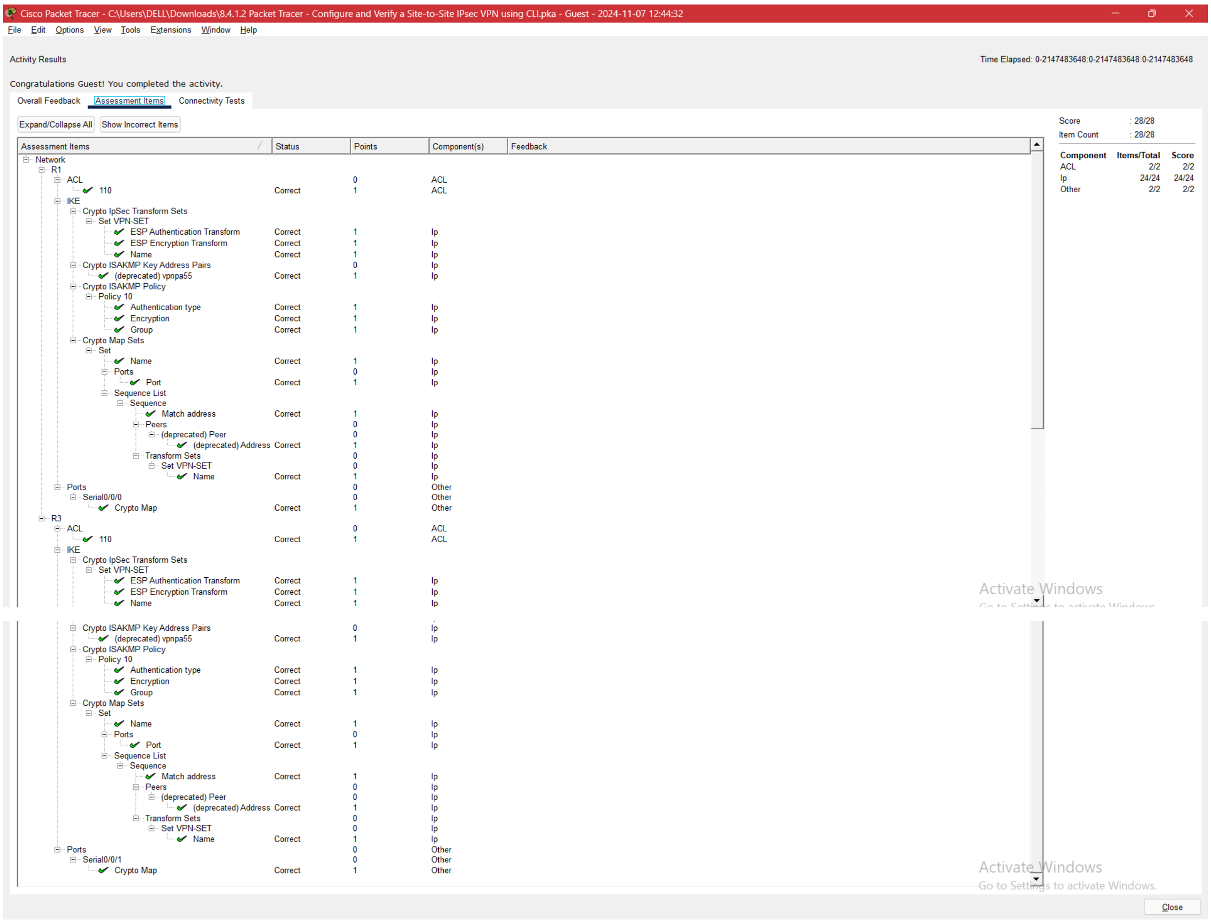
   On R1, re-issue the **show crypto ipsec sa** command. Notice that the number of packets has not changed, which verifies that uninteresting traffic is not encrypted.



```
R1#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: 2, #pkts encrypt: 2, #pkts digest: 0
   #pkts decaps: 3, #pkts decrypt: 3, #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: 0xA31A839E(2736423838)

     inbound esp sas:
      spi: 0xD5C5E8B8(3586517176)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2006, flow_id: FPGA:1, crypto map: VPN-MAP
        sa timing: remaining key lifetime (k/sec): (4525504/3506)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xA31A839E(2736423838)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2007, flow_id: FPGA:1, crypto map: VPN-MAP
        sa timing: remaining key lifetime (k/sec): (4525504/3506)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:
```

**As can be observed, the amount of packets encrypted and decrypted haven't changed thus verifying the packets were uninteresting.**

# PROOF OF COMPLETION OF THE LAB



Cisco Packet Tracer - C:\Users\DELL\Downloads\8.4.1.2 Packet Tracer - Configure and Verify a Site-to-Site IPsec VPN using CLI.pka - Guest - 2024-11-07 12:44:32
File Edit Options View Tools Extensions Window Help
Overall Feedback
Assessment Items
Connectivity Tests
Expand/Collapse All
Show Incorrect Items
Close

Activity Results

Time Elapsed: 0-2147483648:0-2147483648:0-2147483648

Congratulations Guest! You completed the activity.

Score : 28/28

Item Count : 28/28

| Component | Items/Total | Score |
|---|---|---|
| ACL | 2/2 | 2/2 |
| Ip | 24/24 | 24/24 |
| Other | 2/2 | 2/2 |

| 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 Key Address Pairs | | 0 | Ip | |
| ✓ (deprecated) vpnpa55 | 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 | |
| (deprecated) Peer | | 0 | Ip | |
| ✓ (deprecated) 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 | |
| R3 | | | | |
| 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 Key Address Pairs | | 0 | Ip | |
| ✓ (deprecated) vpnpa55 | 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 | |
| (deprecated) Peer | | 0 | Ip | |
| ✓ (deprecated) Address | Correct | 1 | Ip | |
| Transform Sets | | 0 | Ip | |
| Set VPN-SET | | 0 | Ip | |
| ✓ Name | Correct | 1 | Ip | |
| Ports | | 0 | Other | |
| Serial0/0/1 | | 0 | Other | |
| ✓ Crypto Map | Correct | 1 | Other | |

# Assessment Rubric

## Lab 12

## Configure and Verify a Site-to-Site IPsec VPN

| | |
|---|---|
| **Name: Syed Asghar Abbas Zaidi** | **Student ID: 07201** |

**Points Distribution**

| Task No. | LR 2<br>Simulation | LR5<br>Results/Plots | LR9<br>Report |
|---|---|---|---|
| Task 1 | 20 | - | |
| Task 2 | 20 | - | |
| Task 3 | 20 | 20 | |
| Total | /60 | /20 | /10 |
| **CLO Mapped** | CLO 4 | CLO 4 | CLO4 |
| | | | |

| Affective Domain Rubric | | Points | CLO Mapped |
|---|---|---|---|
| AR 7 | Report Submission | /10 | CLO 4 |

| CLO | Total Points | Points Obtained |
|---|---|---|
| 4 | 90 | |
| 4 | 10 | |
| **Total** | **100** | |

*For description of different levels of the mapped rubrics, please refer the provided Lab Evaluation Assessment Rubrics and Affective Domain Assessment Rubrics.*

# Lab Evaluation Assessment Rubric

| # | Assessment Elements | Level 1: Unsatisfactory Points 0-1 | Level 2: Developing Points 2 | Level 3:Good Points 3 | Level 4:Exemplary Points 4 |
|---|---|---|---|---|---|
| LR2 | Program/Code / Simulation Model/ Network Model | Program/code/simulation model/network model does not implement the required functionality and has several errors. The student is not able to utilize even the basic tools of the software. | Program/code/simulation model/network model has some errors and does not produce completely accurate results. Student has limited command on the basic tools of the software. | Program/code/simulation model/network model gives correct output but not efficiently implemented or implemented by computationally complex routine. | Program/code/simulation /network model is efficiently implemented and gives correct output. Student has full command on the basic tools of the software. |
| LR5 | Results & Plots | Figures/ graphs / tables are not developed or are poorly constructed with erroneous results. Titles, captions, units are not mentioned. Data is presented in an obscure manner. | Figures, graphs and tables are drawn but contain errors. Titles, captions, units are not accurate. Data presentation is not too clear. | All figures, graphs, tables are correctly drawn but contain minor errors or some of the details are missing. | Figures / graphs / tables are correctly drawn and appropriate titles/captions and proper units are mentioned. Data presentation is systematic. |
| LR9 | Report | All the in-lab tasks are not included in report and / or the report is submitted too late. | Most of the tasks are included in report but are not well explained. All the necessary figures / plots are not included. Report is submitted after due date. | Good summary of most the in-lab tasks is included in report. The work is supported by figures and plots with explanations. The report is submitted timely. | Detailed summary of the in-lab tasks is provided. All tasks are included and explained well. Data is presented clearly including all the necessary figures, plots and tables. |