Course:	Cloud and Network Security
Name:	Neville Ngothe Iregi
Student No.:	CS-CNS10-25054
Date:	Tuesday, 14th October 2025

Week 5 Assignment 2: Configuring Site-to-Site VPNs

Introduction

IPsec is an IETF standard that defines how a VPN can be secured across IP networks; It provides secure transmission of sensitive information over unprotected networks e.g. the Internet. Many corporations use it since it allows them to select security services according to internal security policies. IPsec operates at the network layer and protects and authenticates IP packets between participating IPsec devices (peers), such as Cisco routers. Some of the security functions provided are:

1. **Confidentiality -** Encryption algorithms to prevent cybercriminals from reading packet contents
2. **Integrity:** Hashing algorithms to ensure packets have not been altered between the source and destination.
3. **Internet Key Exchange (IKE) Protocol / Internet Security Association and Key Management Protocol (ISAKMP):** Handles negotiation and setup of the security parameters for the tunnel (Origin Authentication i.e source and destination).
4. **Key Exchange:** Diffie-Hellman used to secure.
5. **IPsec Protocol:** IPsec protocol encapsulates packets using Authentication Header (AH) and Encapsulation Security Protocol (ESP).

IPsec thus allows for easy integration of new security tech without updating existing IPsec standards.

Objectives

- Verify connectivity throughout the network.

- Configure R1 to support a site-to-site IPsec VPN with R3.

Scenario

In this activity, you will configure two routers to support a site-to-site IPsec VPN for traffic flowing from their respective LANs. The IPsec VPN traffic will pass through another router that has no knowledge of the VPN. 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.

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.1.1	255.255.255.0	N/A
	S0/0/0 (DCE)	10.1.1.2	255.255.255.252	N/A
R2	G0/0	192.168.2.1	255.255.255.0	N/A
	S0/0/0	10.1.1.1	255.255.255.252	N/A
	S0/0/1 (DCE)	10.2.2.1	255.255.255.252	N/A
R3	G0/0	192.168.3.1	255.255.255.0	N/A
	S0/0/1	10.2.2.2	255.255.255.252	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

PC-B	NIC	192.168.2.3	255.255.255.0	192.168.2.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

ISAKMP Phase 1 Policy Parameters

Parameters		R1	R2
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 2	DH 2
IKE SA Lifetime	86400 seconds or less	**86400**	**86400**
ISAKMP Key	Provided by user.	vpnpa55	vpnpa55

- **Bolded** parameters are defaults. Other defaults need to be explicitly configured.

ISAKMP Phase 2 Policy Parameters

Parameters	R1	R3
Transform Set	VPN-SET	VPN-SET
Peer Hostname	R3	R1
Peer IP Address	10.2.2.2	10.1.1.2
Network to be encrypted	192.168.1.0/24	192.168.3.0/24

Crypto Map name	VPN-MAP	VPN-MAP
SA Establishment	ipsec-isakmp	ipsec-isakmp

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

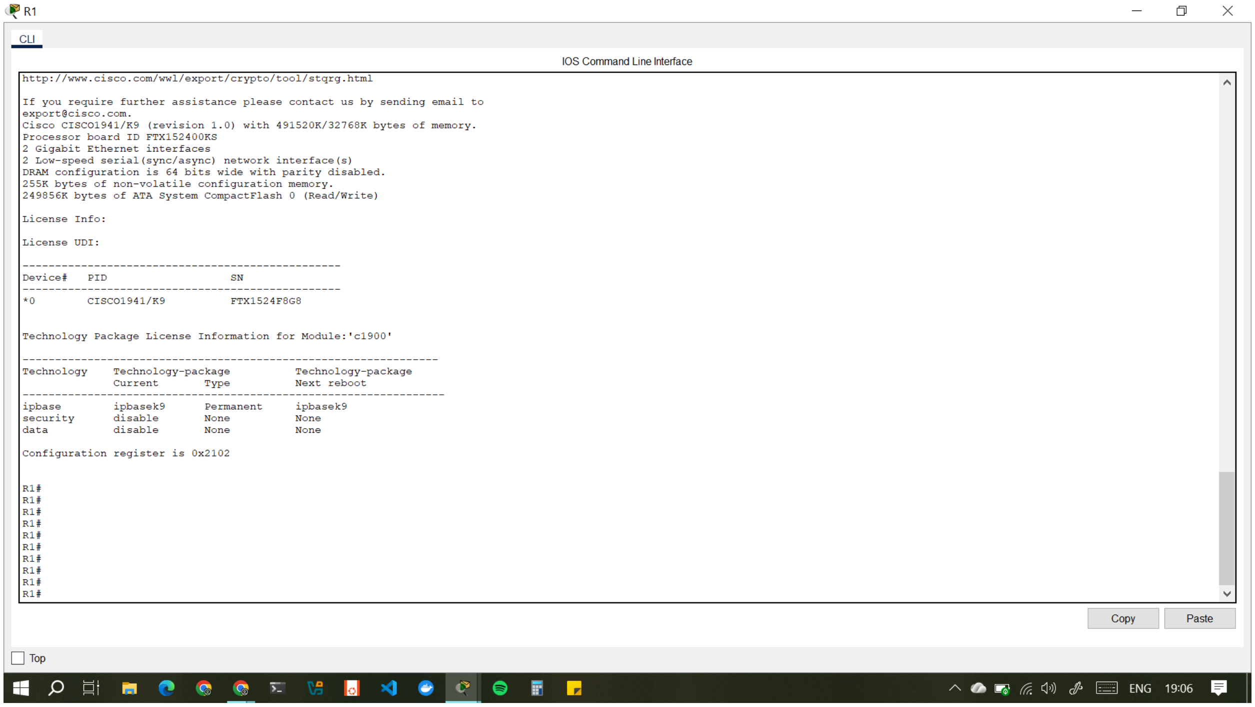
Part 1: Enable Security Features

Step 1: Activate securityk9 module.

The Security Technology Package license must be enabled to complete this activity.

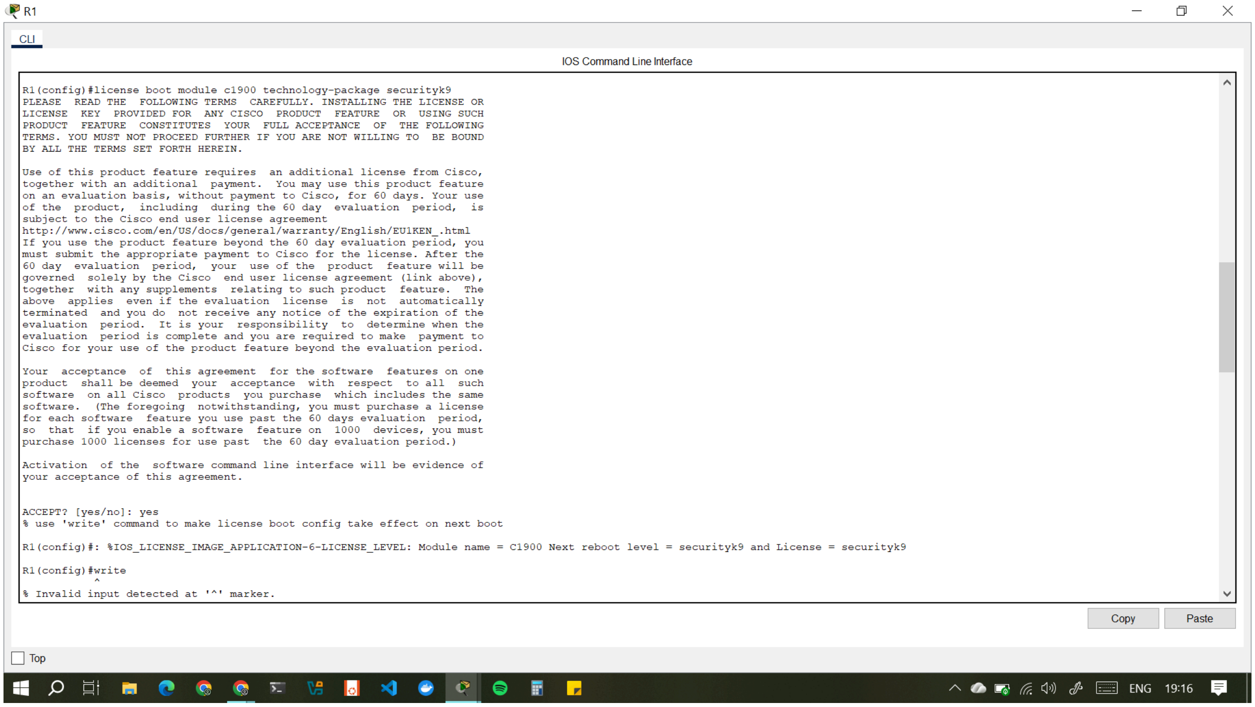
a. Issue the show version command in the user EXEC or privileged EXEC mode to verify that the Security Technology Package license is activated.

```
---------------------------------------------------------------------------------------------

Technology          Technology-package          Technology-package

                    Current      Type           Next reboot

---------------------------------------------------------------------------------------------

ipbase              ipbasek9     Permanent      ipbasek9

security            None         None           None

uc                  None         None           None

data                None         None           None


Configuration register is 0x2102
```

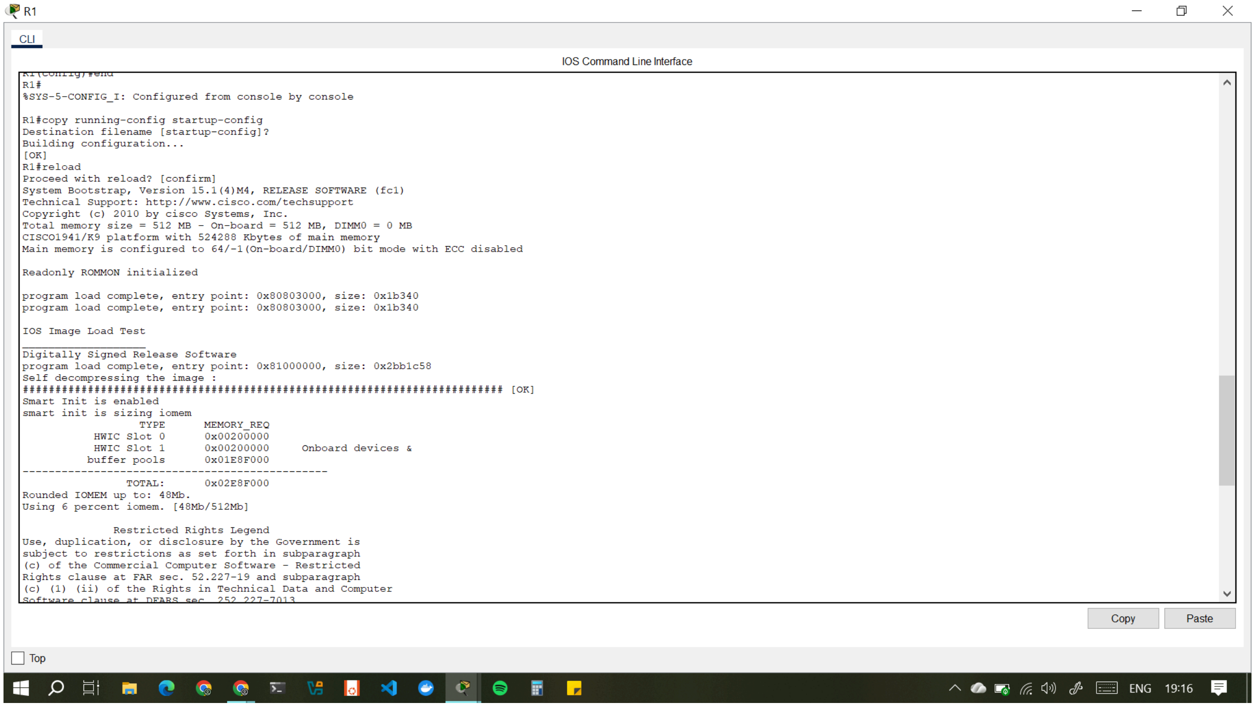


```
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.
Cisco CISCO1941/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
2 Gigabit Ethernet interfaces
2 Low-speed serial(sync/async) network interface(s)
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#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
```

b. If not, activate the **securityk9** module for the next boot of the router, accept the license, save the configuration, and reboot using **license boot module c2900 technology-package securityk9**

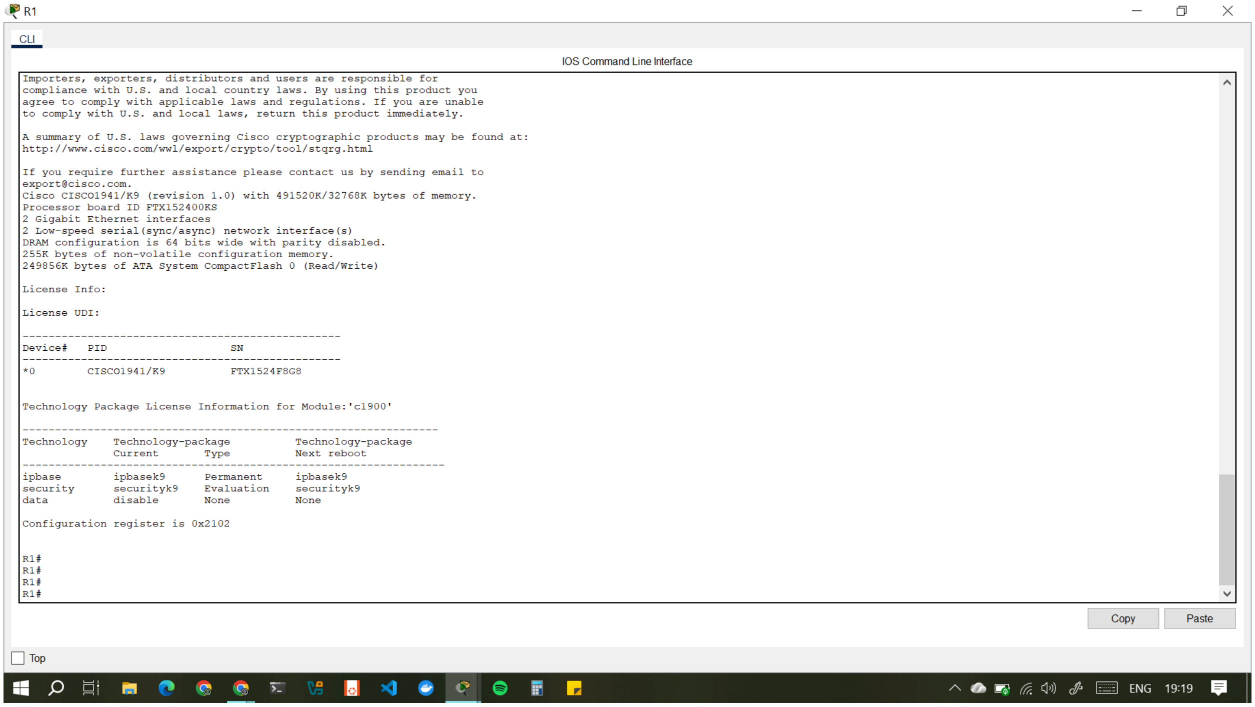


```
R1(config)#license boot module c1900 technology-package securityk9
PLEASE  READ THE  FOLLOWING TERMS  CAREFULLY. INSTALLING THE LICENSE OR
LICENSE  KEY  PROVIDED FOR  ANY CISCO  PRODUCT  FEATURE  OR  USING SUCH
PRODUCT  FEATURE  CONSTITUTES  YOUR  FULL ACCEPTANCE  OF  THE FOLLOWING
TERMS. YOU MUST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



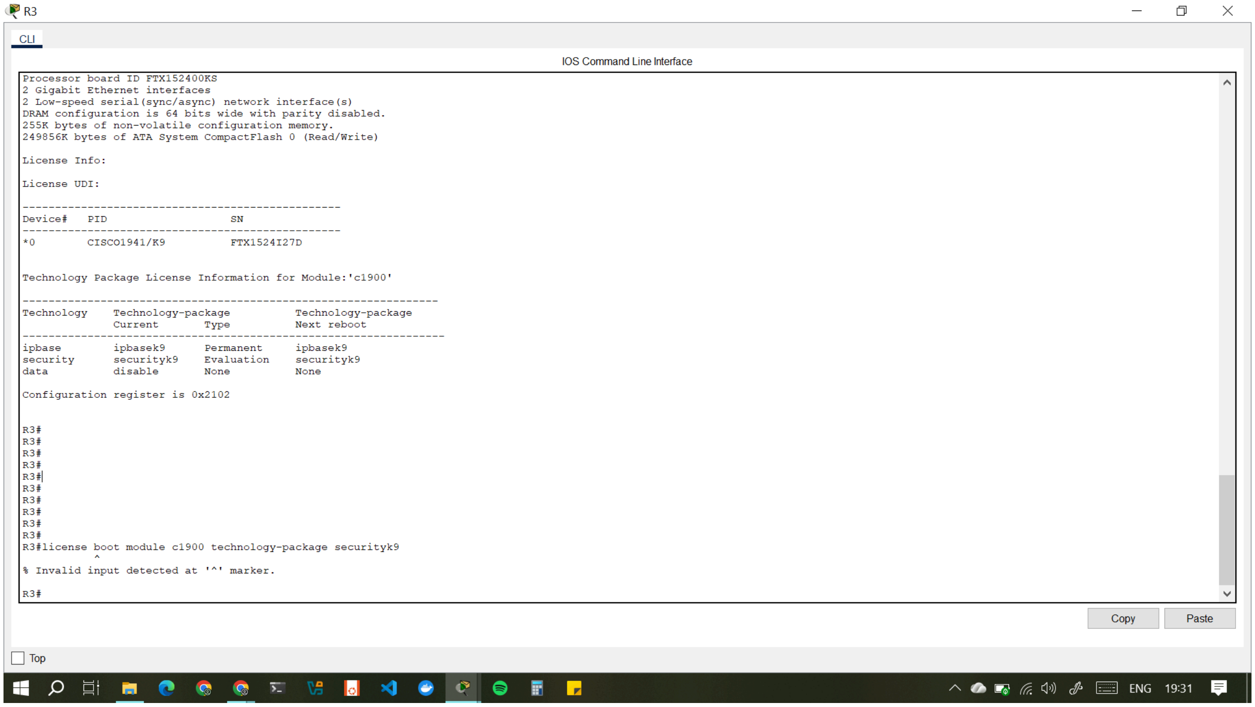
```
R1(config)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

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

Readonly ROMMON initialized

program load complete, entry point: 0x80803000, size: 0x1b340
program load complete, entry point: 0x80803000, size: 0x1b340

IOS Image Load Test
___________________
Digitally Signed Release Software
program load complete, entry point: 0x81000000, size: 0x2bb1c58
Self decompressing the image :
########################################################################## [OK]
Smart Init is enabled
smart init is sizing iomem
                  TYPE      MEMORY_REQ
           HWIC Slot 0      0x00200000
           HWIC Slot 1      0x00200000     Onboard devices &
          buffer pools      0x01E8F000
-----------------------------------------------
                TOTAL:      0x02E8F000
Rounded IOMEM up to: 48Mb.
Using 6 percent iomem. [48Mb/512Mb]

              Restricted Rights Legend
Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013
```

c. After the reloading is completed, issue the **show version** again to verify the Security Technology Package license activation.



```
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.
Cisco CISCO1941/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
2 Gigabit Ethernet interfaces
2 Low-speed serial(sync/async) network interface(s)
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#
R1#
R1#
R1#
```

d. Repeat Steps 1a to 1c with R3.



```
Processor board ID FTX152400KS
2 Gigabit Ethernet interfaces
2 Low-speed serial(sync/async) network interface(s)
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#
R3#
R3#
R3#
R3#
R3#
R3#
R3#
R3#
R3#
R3#license boot module c1900 technology-package securityk9
           ^
% Invalid input detected at '^' marker.

R3#
```

Part 2: Configure IPsec Parameters on R1

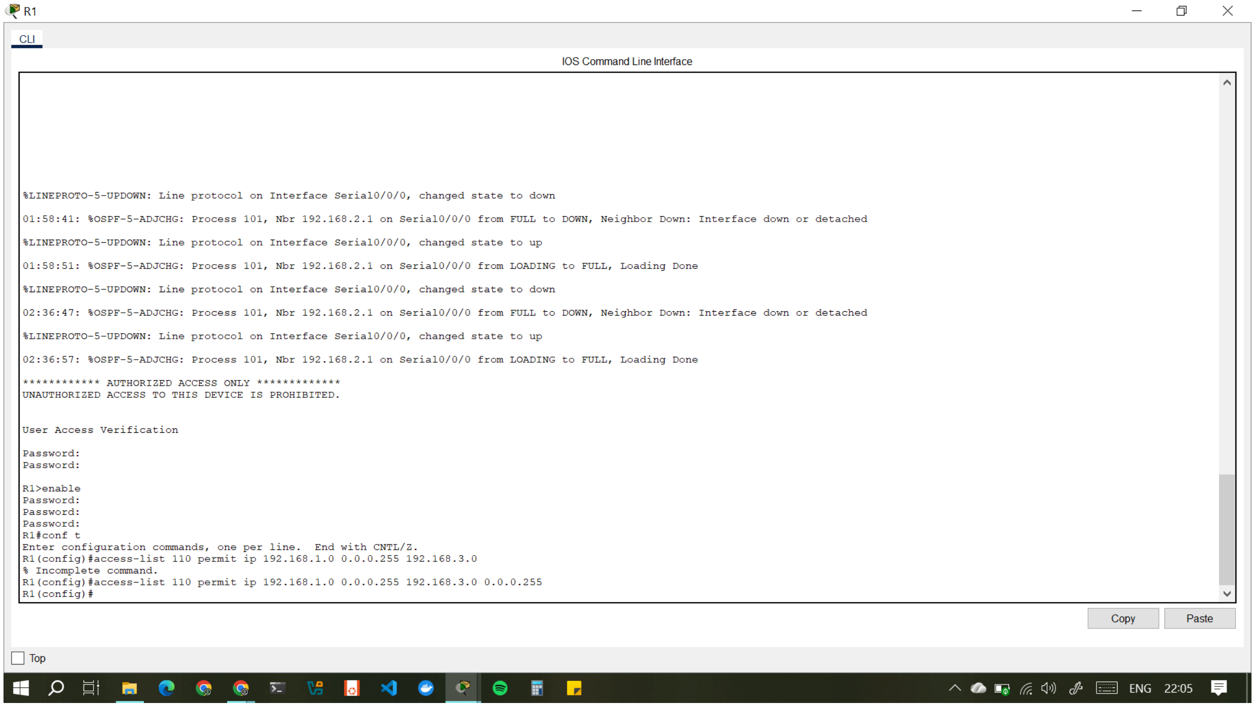
Step 1: Test connectivity.

Ping from PC-A to PC-C.

Step 2: 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 whenever there is traffic between R1 to R3 LANs. All other traffic sourced from the LANs will not be encrypted. Remember that due to the implicit deny any, there is no need to add the statement to the list.

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



```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down

01:58:41: %OSPF-5-ADJCHG: Process 101, Nbr 192.168.2.1 on Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or detached

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

01:58:51: %OSPF-5-ADJCHG: Process 101, Nbr 192.168.2.1 on Serial0/0/0 from LOADING to FULL, Loading Done

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down

02:36:47: %OSPF-5-ADJCHG: Process 101, Nbr 192.168.2.1 on Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or detached

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

02:36:57: %OSPF-5-ADJCHG: Process 101, Nbr 192.168.2.1 on Serial0/0/0 from LOADING to FULL, Loading Done

************ AUTHORIZED ACCESS ONLY *************
UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.


User Access Verification

Password:
Password:

R1>enable
Password:
Password:
Password:
R1#conf t
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
% Incomplete command.
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)#
```

Step 3: Configure the ISAKMP Phase 1 properties on R1.

- The goal of phase 1 is to create a secure, authenticated channel between the two VPN peers - like shaking hands before sending any sensitive data.

Configure the crypto ISAKMP policy **10** properties on R1 along with the shared crypto key **cisco**. 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, key exchange method, and DH method must be configured.

R1(config)# ***crypto isakmp policy 10***

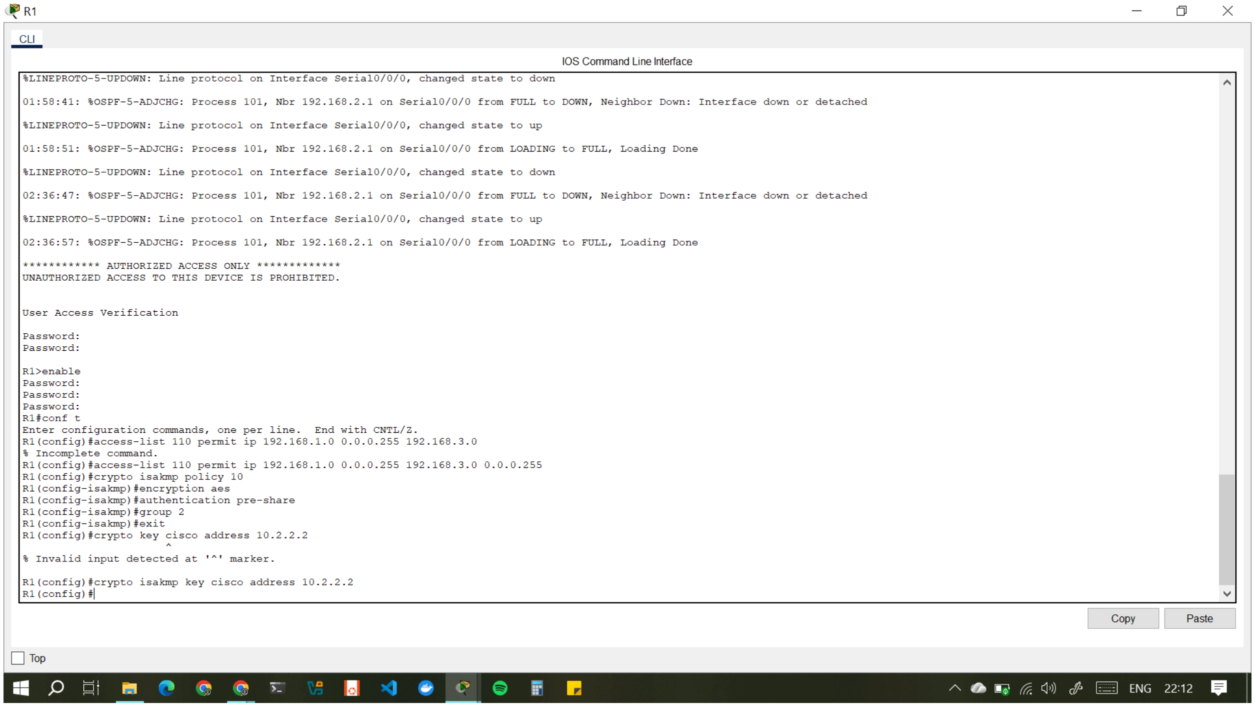
R1(config-isakmp)# ***encryption aes***

R1(config-isakmp)# ***authentication pre-share***

R1(config-isakmp)# ***group 2***

R1(config-isakmp)# ***exit***

R1(config)# ***crypto isakmp key cisco address 10.2.2.2***



```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down

01:58:41: %OSPF-5-ADJCHG: Process 101, Nbr 192.168.2.1 on Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or detached

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

01:58:51: %OSPF-5-ADJCHG: Process 101, Nbr 192.168.2.1 on Serial0/0/0 from LOADING to FULL, Loading Done

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down

02:36:47: %OSPF-5-ADJCHG: Process 101, Nbr 192.168.2.1 on Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or detached

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

02:36:57: %OSPF-5-ADJCHG: Process 101, Nbr 192.168.2.1 on Serial0/0/0 from LOADING to FULL, Loading Done

************ AUTHORIZED ACCESS ONLY *************
UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.


User Access Verification

Password:
Password:

R1>enable
Password:
Password:
Password:
R1#conf t
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
% Incomplete command.
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
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 2
R1(config-isakmp)#exit
R1(config)#crypto key cisco address 10.2.2.2
                      ^
% Invalid input detected at '^' marker.

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

Step 4: Configure the ISAKMP Phase 2 properties on R1.

Phase 2 uses the secure channel from Phase 1 to negotiate **how actual data traffic will be protected**.

Create the transform-set VPN-SET to use esp-3des and esp-sha-hmac. Then 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 ipsec transform-set VPN-SET esp-3des esp-sha-hmac***

*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***

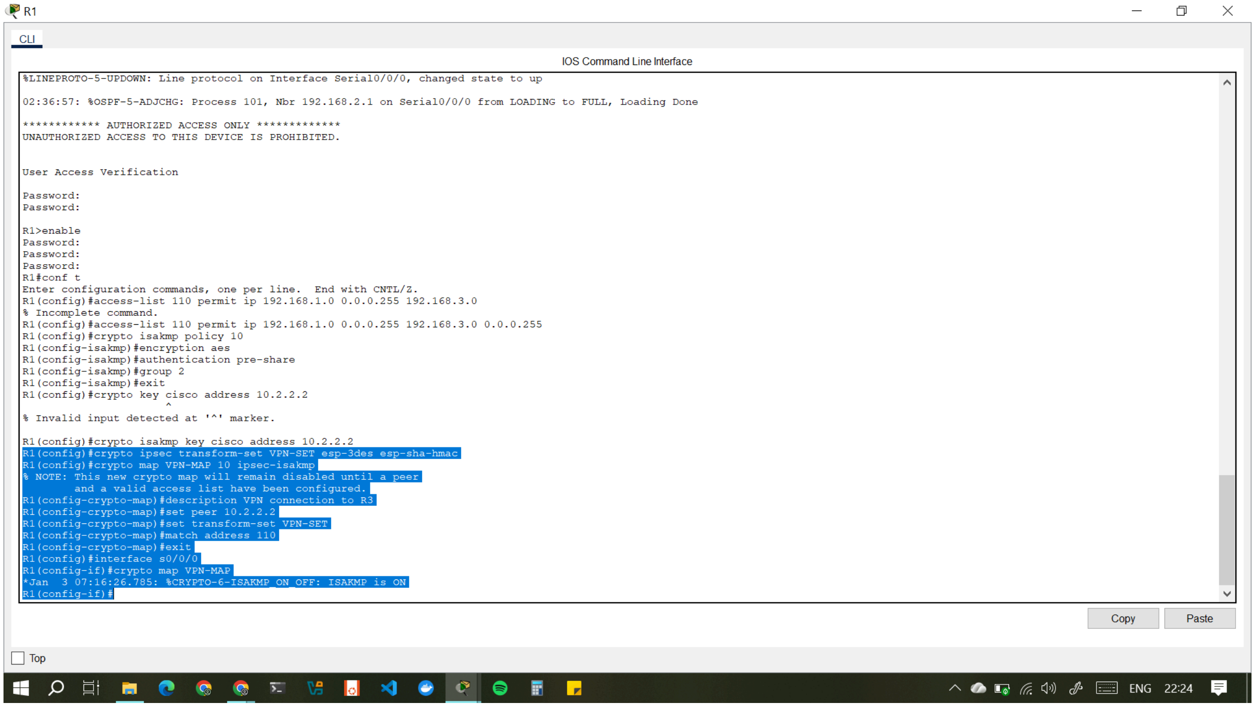
*R1(config-crypto-map)# **exit***

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

Finally, bind the VPN-MAP crypto map to the outgoing Serial 0/0/0 interface. Note: This is not graded.

*R1(config)# **interface S0/0/0***

*R1(config-if)# **crypto map VPN-MAP***



```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

02:36:57: %OSPF-5-ADJCHG: Process 101, Nbr 192.168.2.1 on Serial0/0/0 from LOADING to FULL, Loading Done

************ AUTHORIZED ACCESS ONLY *************
UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.


User Access Verification

Password:
Password:

R1>enable
Password:
Password:
Password:
R1#conf t
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
% Incomplete command.
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
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 2
R1(config-isakmp)#exit
R1(config)#crypto key cisco address 10.2.2.2
                      ^
% Invalid input detected at '^' marker.

R1(config)#crypto isakmp key cisco address 10.2.2.2
R1(config)#crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
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)#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)#
```

Part 3: Configure IPsec Parameters on R3

Step 1: Configure router R3 to support a site-to-site VPN with R1.

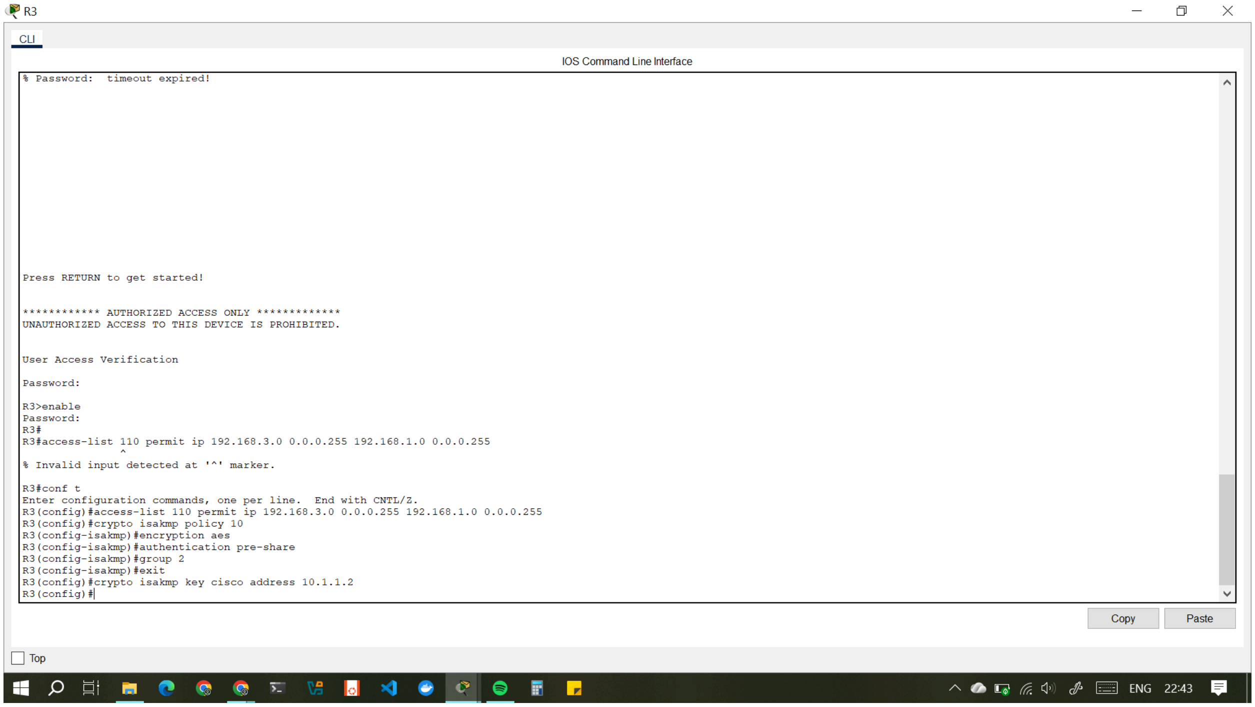
Now configure reciprocating parameters on R3. Configure ACL 110 identifying the traffic from the LAN on R3 to the LAN on R1 as interesting.

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

Step 2: Configure the ISAKMP Phase 1 properties on R3.

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

```
R3(config)# crypto isakmp policy 10

R3(config-isakmp)# encryption aes

R3(config-isakmp)# authentication pre-share

R3(config-isakmp)# group 2

R3(config-isakmp)# exit

R3(config)# crypto isakmp key cisco address 10.1.1.2
```



```
% Password:  timeout expired!









Press RETURN to get started!


************ AUTHORIZED ACCESS ONLY *************
UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.


User Access Verification

Password:

R3>enable
Password:
R3#
R3#access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
               ^
% Invalid input detected at '^' marker.

R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
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)#crypto isakmp policy 10
R3(config-isakmp)#encryption aes
R3(config-isakmp)#authentication pre-share
R3(config-isakmp)#group 2
R3(config-isakmp)#exit
R3(config)#crypto isakmp key cisco address 10.1.1.2
R3(config)#
```

Step 3: Configure the ISAKMP Phase 2 properties on R1.

Like you did on R1, create the transform-set **VPN-SET** to use **esp-3des** and **esp-sha-hmac**. Then 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 ipsec transform-set VPN-SET esp-3des esp-sha-hmac***

*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***

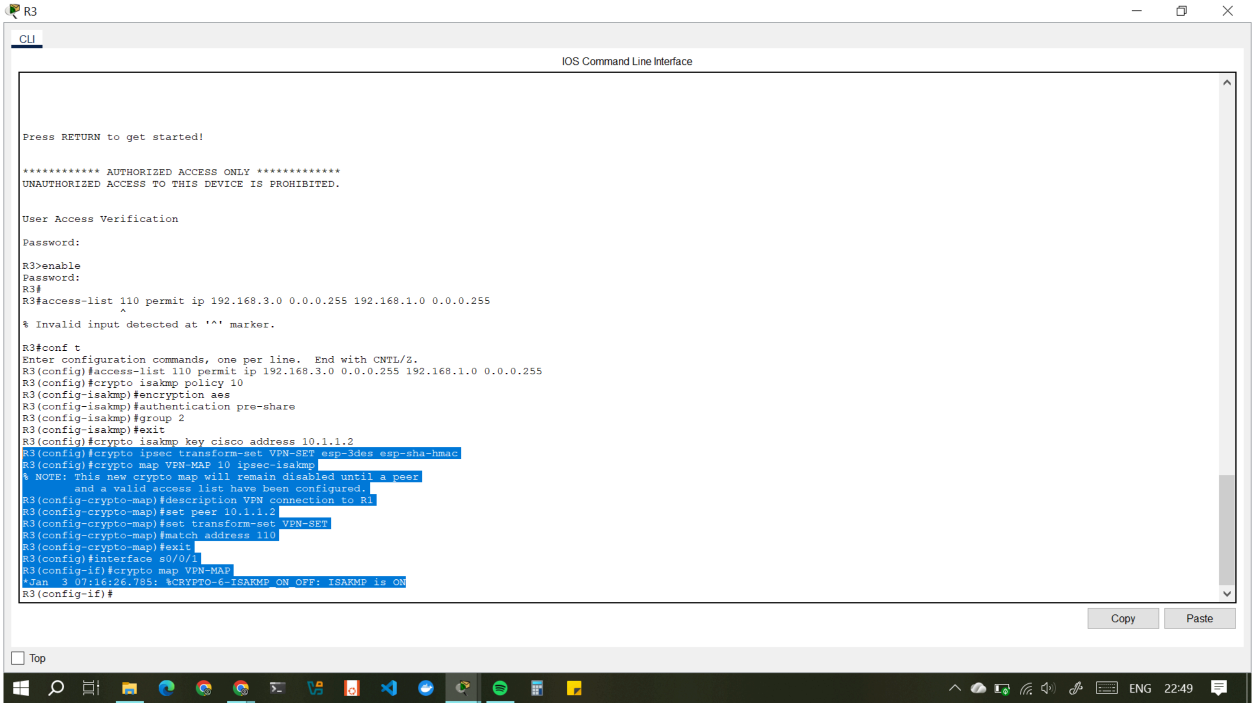
*R3(config-crypto-map)# **exit***

Step 4: Configure the crypto map on the outgoing interface.

Finally, 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***

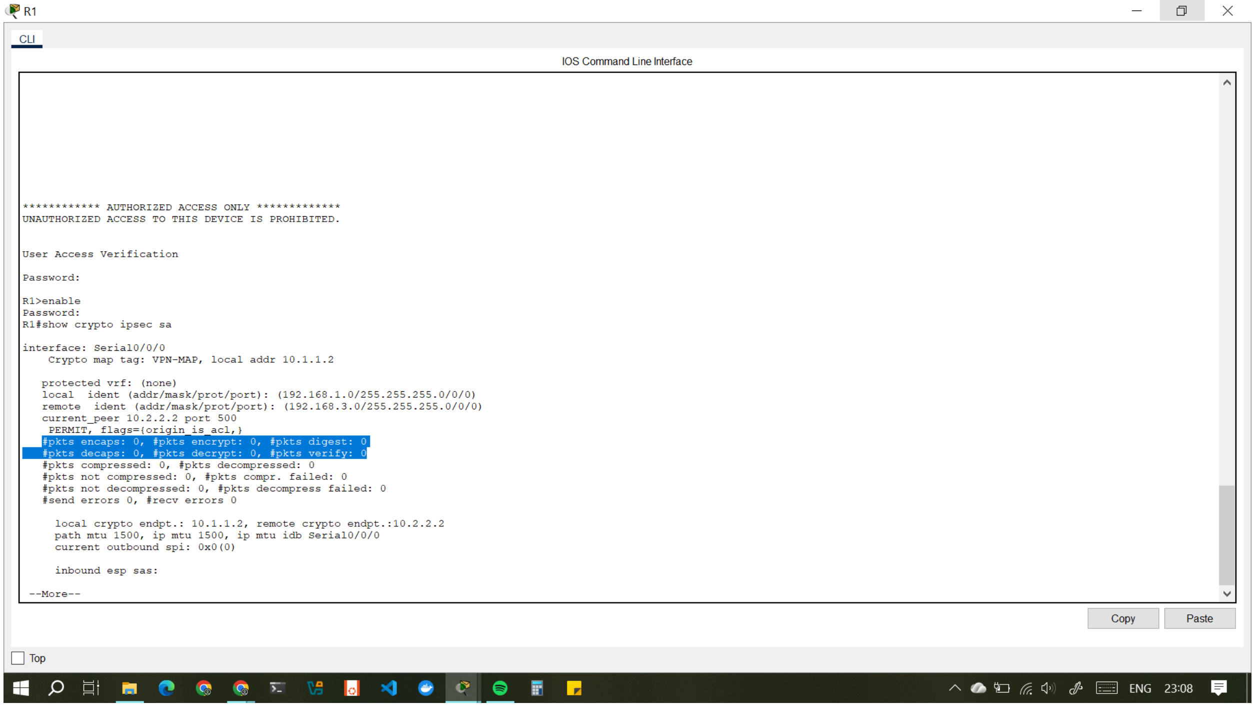


```
Press RETURN to get started!


************ AUTHORIZED ACCESS ONLY *************
UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.


User Access Verification

Password:

R3>enable
Password:
R3#
R3#access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
               ^
% Invalid input detected at '^' marker.

R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
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)#crypto isakmp policy 10
R3(config-isakmp)#encryption aes
R3(config-isakmp)#authentication pre-share
R3(config-isakmp)#group 2
R3(config-isakmp)#exit
R3(config)#crypto isakmp key cisco address 10.1.1.2
R3(config)#crypto ipsec transform-set VPN-SET esp-3des 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
R3(config-if)#
```

Part 4: Verify the IPsec VPN

Step 1: Verify the tunnel prior to interesting traffic.

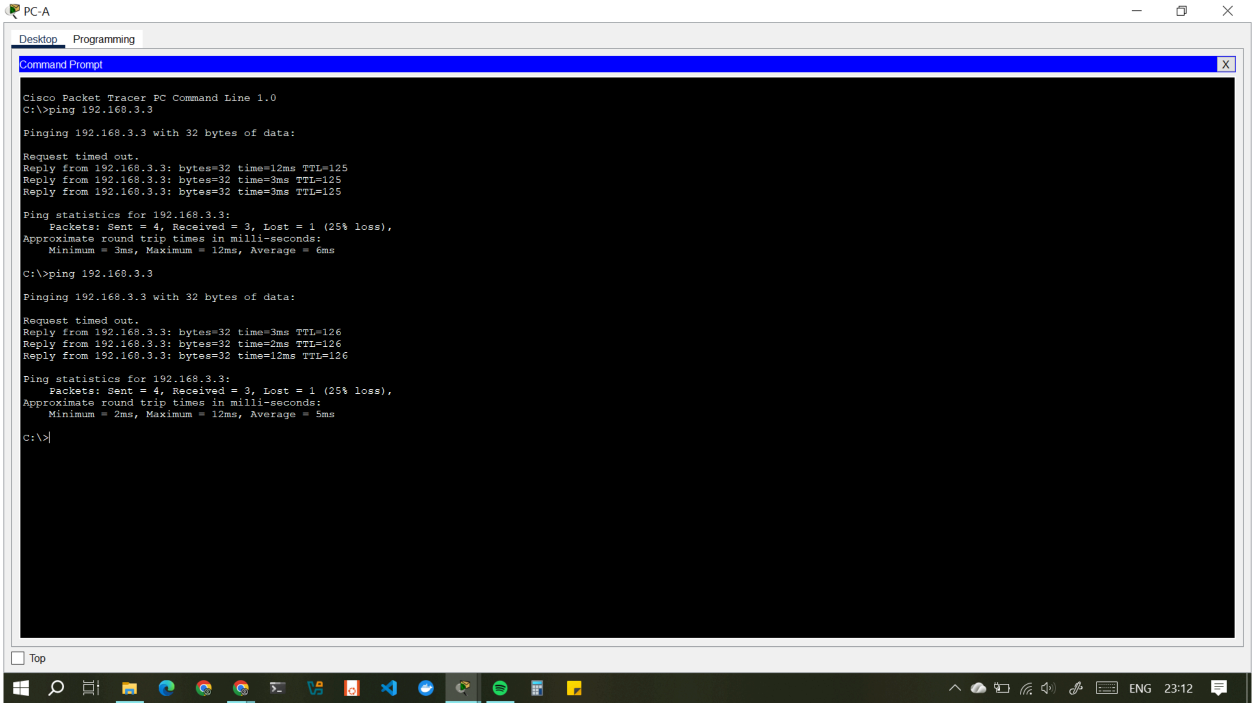
Issue the **show crypto ipsec sa** command on R1. Notice that the number of packets encapsulated, encrypted, decapsulated and decrypted are all set to 0.



```
************ AUTHORIZED ACCESS ONLY *************
UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.


User Access Verification

Password:

R1>enable
Password:
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:

 --More--
```

Step 2: Create interesting traffic.

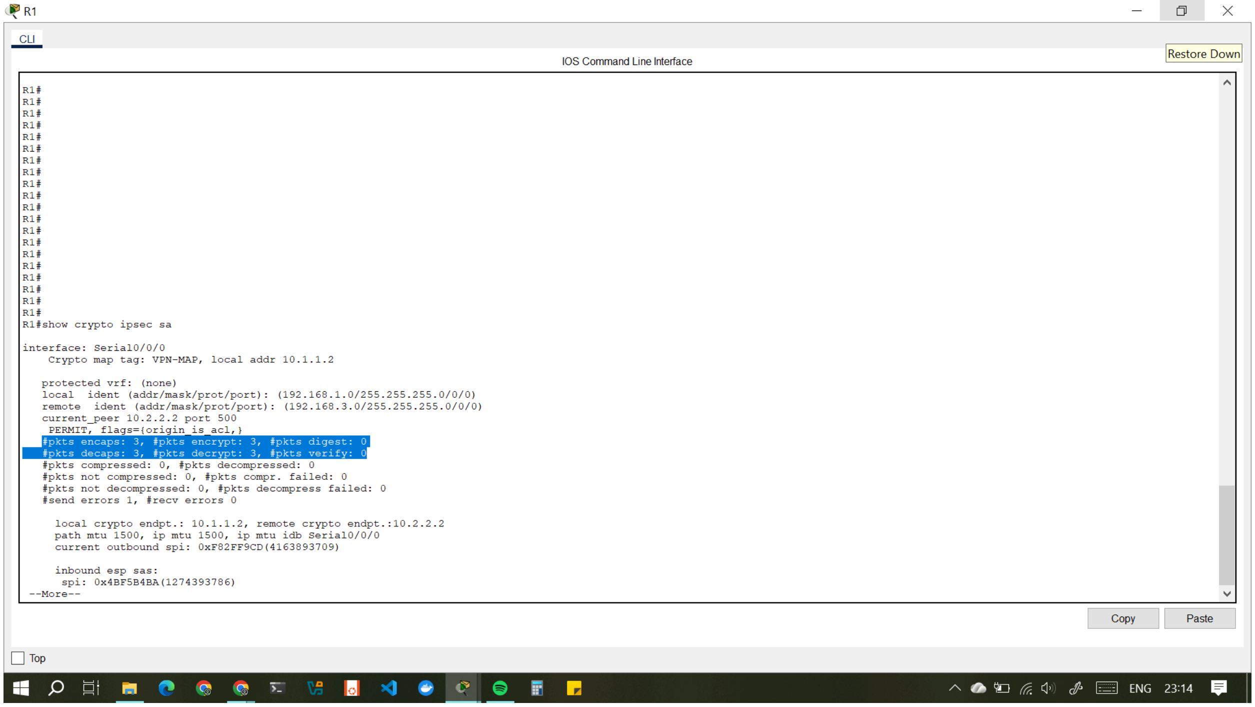
Ping PC-C from PC-A.



```
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=12ms TTL=125
Reply from 192.168.3.3: bytes=32 time=3ms 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 = 3ms, Maximum = 12ms, Average = 6ms

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=3ms TTL=126
Reply from 192.168.3.3: bytes=32 time=2ms TTL=126
Reply from 192.168.3.3: bytes=32 time=12ms TTL=126

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 = 12ms, Average = 5ms

C:\>
```

Step 3: Verify the tunnel after interesting traffic.

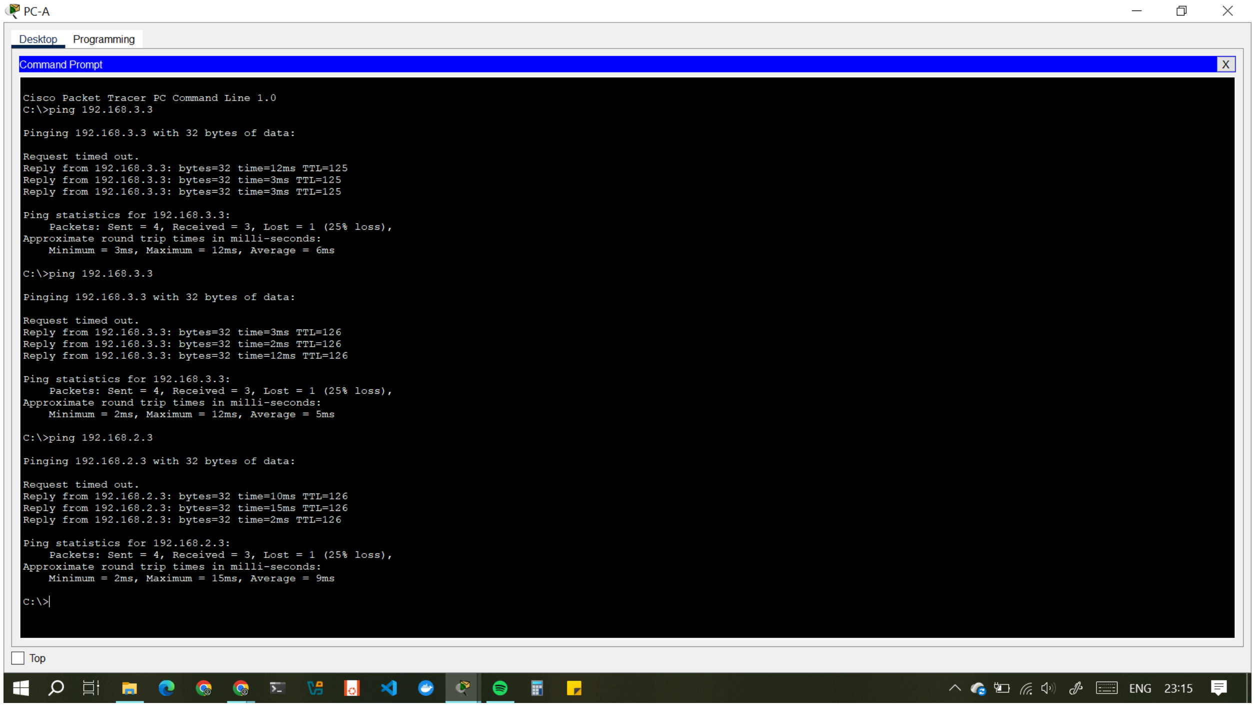
On R1, re-issue the **show crypto ipsec sa** command. Now notice that the number of packets is more than 0 (3) indicating that the IPsec VPN tunnel is working.



```
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
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: 3, #pkts encrypt: 3, #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 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: 0xF82FF9CD(4163893709)

     inbound esp sas:
      spi: 0x4BF5B4BA(1274393786)
 --More--
```

Step 4: Create uninteresting traffic.

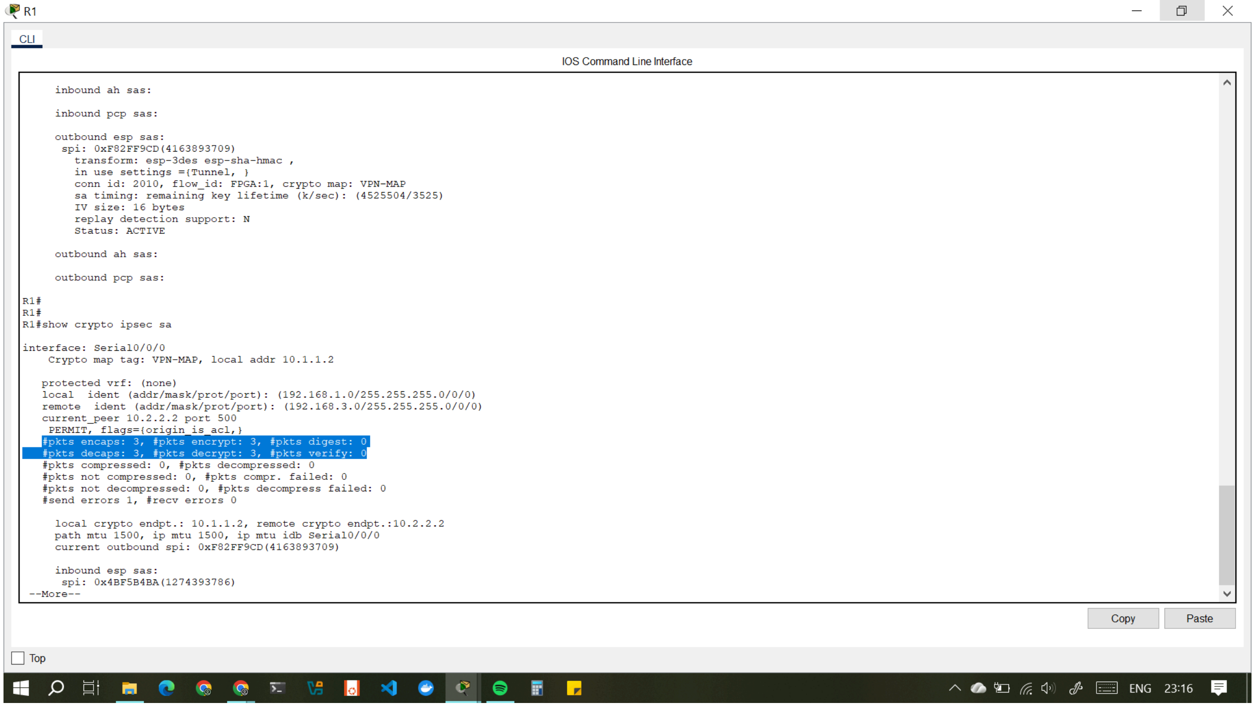
Ping PC-B from PC-A.



```
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=12ms TTL=125
Reply from 192.168.3.3: bytes=32 time=3ms 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 = 3ms, Maximum = 12ms, Average = 6ms

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=3ms TTL=126
Reply from 192.168.3.3: bytes=32 time=2ms TTL=126
Reply from 192.168.3.3: bytes=32 time=12ms TTL=126

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 = 12ms, Average = 5ms

C:\>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=10ms TTL=126
Reply from 192.168.2.3: bytes=32 time=15ms TTL=126
Reply from 192.168.2.3: bytes=32 time=2ms 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 = 2ms, Maximum = 15ms, Average = 9ms

C:\>
```

Step 5: Verify the tunnel.

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



```
    inbound ah sas:

    inbound pcp sas:

    outbound esp sas:
     spi: 0xF82FF9CD(4163893709)
       transform: esp-3des 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): (4525504/3525)
       IV size: 16 bytes
       replay detection support: N
       Status: ACTIVE

    outbound ah sas:

    outbound pcp sas:

R1#
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: 3, #pkts encrypt: 3, #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 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: 0xF82FF9CD(4163893709)

     inbound esp sas:
      spi: 0x4BF5B4BA(1274393786)
 --More--
```

Conclusion

This lab demonstrates the setting up of a secure site-to-site IPsec VPN tunnel between R1 and R3 to ensure encrypted communications between their respective LANs across an untrusted network. ISAKMP Phase 1 and Phase 2 configurations are used to ensure both routers established secure peer authentication, negotiated encryption and hashing algorithms, and exchanged keys for data protection. The use of ACLs effectively defined *interesting traffic*, ensuring that only designated packets were encrypted. Verification tests confirmed that packets sent between R1 and R3 LANs were successfully encapsulated and encrypted, while non-VPN traffic remained unencrypted. This exercise demonstrated the practical process of configuring, securing, and verifying a VPN tunnel, reinforcing the importance of IPsec in maintaining confidentiality, integrity, and authenticity in network communications.