

## Week 5 Assignment 2

Course: [Cloud and Network Security - C1-2026](#)

Student Name: [Bussilus Bertrand](#)

Student Number: [CS-CNS11-26004](#)

[Wednesday, February 25, 2026](#)

**[Class Exercise: Configuring Site-to-Site VPNs](#)**

## Week 5 Assignment 2

### Contents

Introduction .....	3
Addressing Table .....	3
Objectives .....	4
Background / Scenario .....	4
ISAKMP Phase 1 Policy Parameters .....	4
IPsec Phase 2 Policy Parameters .....	5
Instructions .....	6
Part 1: Configure IPsec Parameters on R1 .....	6
Part 2: Configure IPsec Parameters on R3 .....	12
Part 3: Verify the IPsec VPN .....	16
Conclusion .....	18

## Introduction

This lab report outlines the configuration and verification of a site-to-site IPsec Virtual Private Network (VPN) using the Command Line Interface (CLI). The primary objective of this exercise is to configure two end routers, R1 and R3, to securely transmit sensitive information between their respective Local Area Networks (LANs) over an unprotected network. In the provided topology, the IPsec VPN tunnel is established between R1 and R3 through an intermediate router, R2, which acts purely as a pass-through device with no knowledge of the VPN. Because IPsec operates at the network layer to protect and authenticate IP packets between participating peer devices, this exercise requires a multi-step configuration process. This includes enabling the necessary security technology packages, establishing ISAKMP Phase 1 policies for key exchange, setting up IPsec Phase 2 policies for data encryption, and creating Access Control Lists (ACLs) to properly identify the "interesting traffic" that will trigger the IPsec VPN.

## 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
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
	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	S3 F0/5

## Week 5 Assignment 2

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
	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	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

### Objectives

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

### 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	Parameter Options and Defaults	R1	R3
Key Distribution Method	Manual or <b>ISAKMP</b>	<b>ISAKMP</b>	<b>ISAKMP</b>
Encryption Algorithm	<b>DES</b> , 3DES, or AES	AES 256	AES 256
Hash Algorithm	MD5 or <b>SHA-1</b>	<b>SHA-1</b>	<b>SHA-1</b>
Authentication Method	Pre-shared keys or <b>RSA</b>	pre-share	pre-share

## Week 5 Assignment 2

Parameters	Parameter Options and Defaults	R1	R3
Key Exchange	DH Group 1, 2, or 5	DH 5	DH 5
IKE SA Lifetime	86400 seconds or less	<b>86400</b>	<b>86400</b>
ISAKMP Key	Provided by user.	vpnpa55	vpnpa55

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

### 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

The routers have been pre-configured with the following:

- Password for console line: **ciscoconpa55**
- Password for vty lines: **ciscovtypa55**

## Week 5 Assignment 2

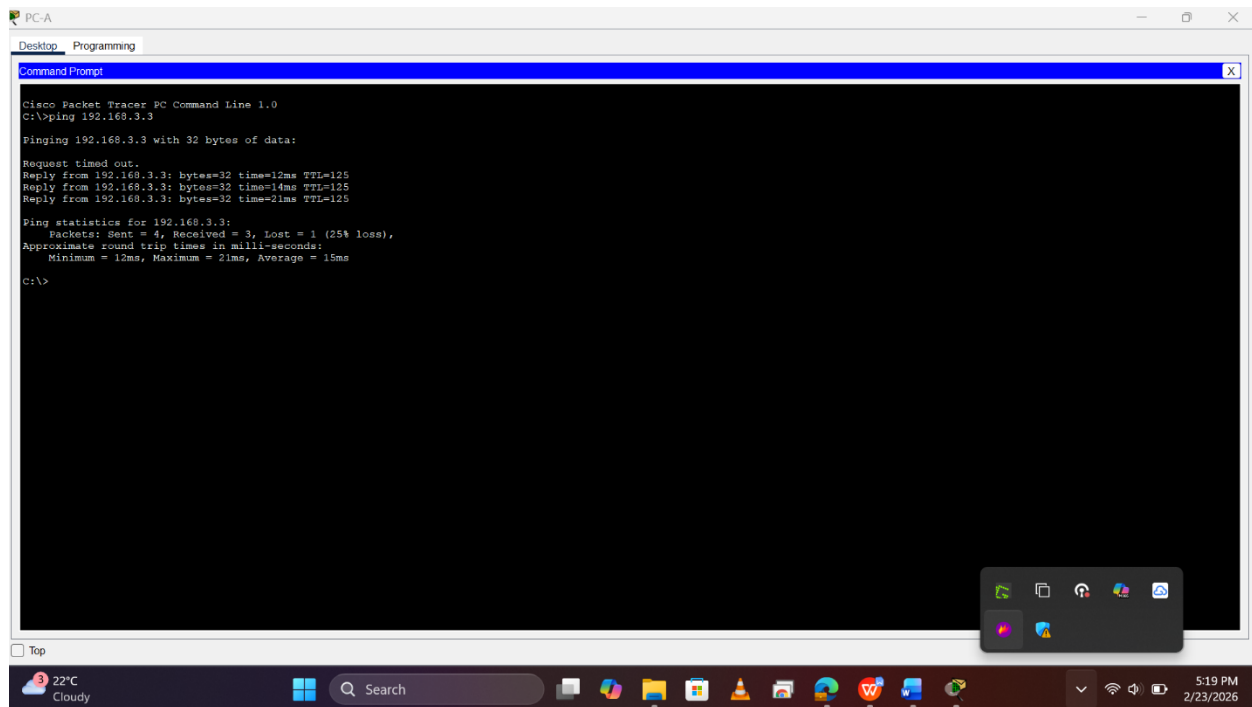
- Enable password: **ciscoenpa55**
- SSH username and password: **SSHadmin / ciscosshpa55**
- OSPF 101

### Instructions

#### Part 1: Configure IPsec Parameters on R1

##### *Step 1: Test connectivity.*

Ping from PC-A to PC-C.

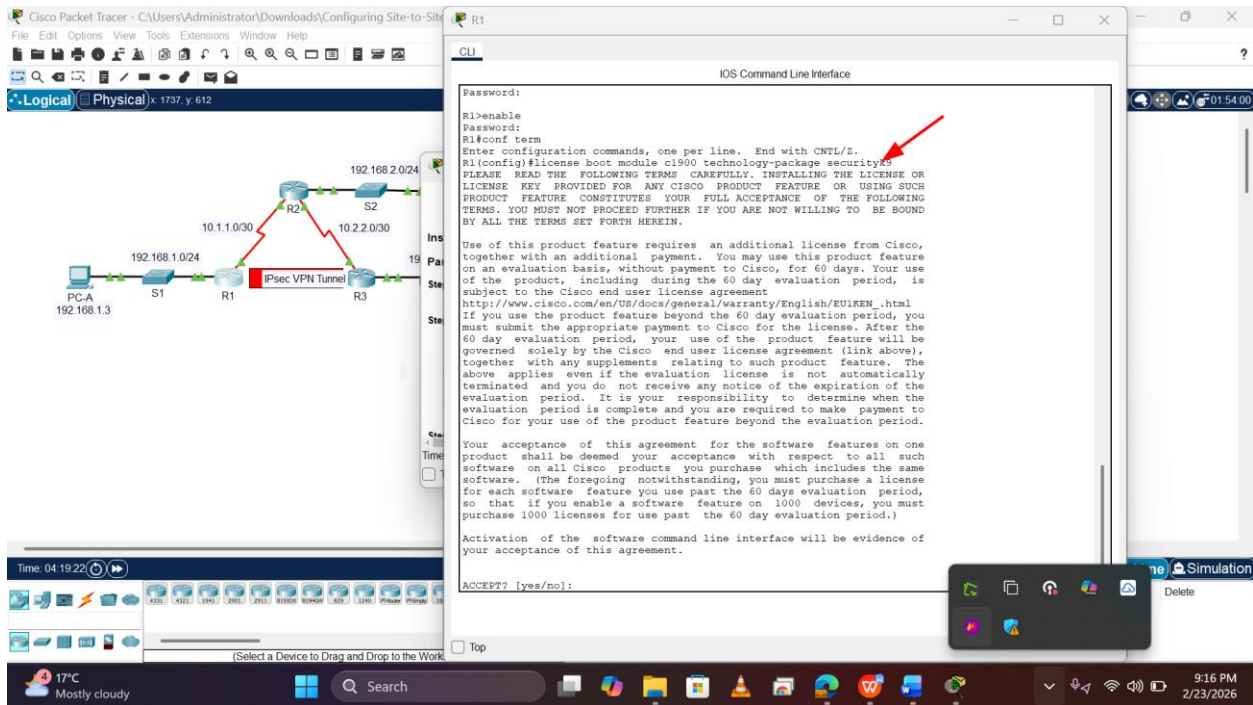


##### *Step 2: Enable the Security Technology package.*

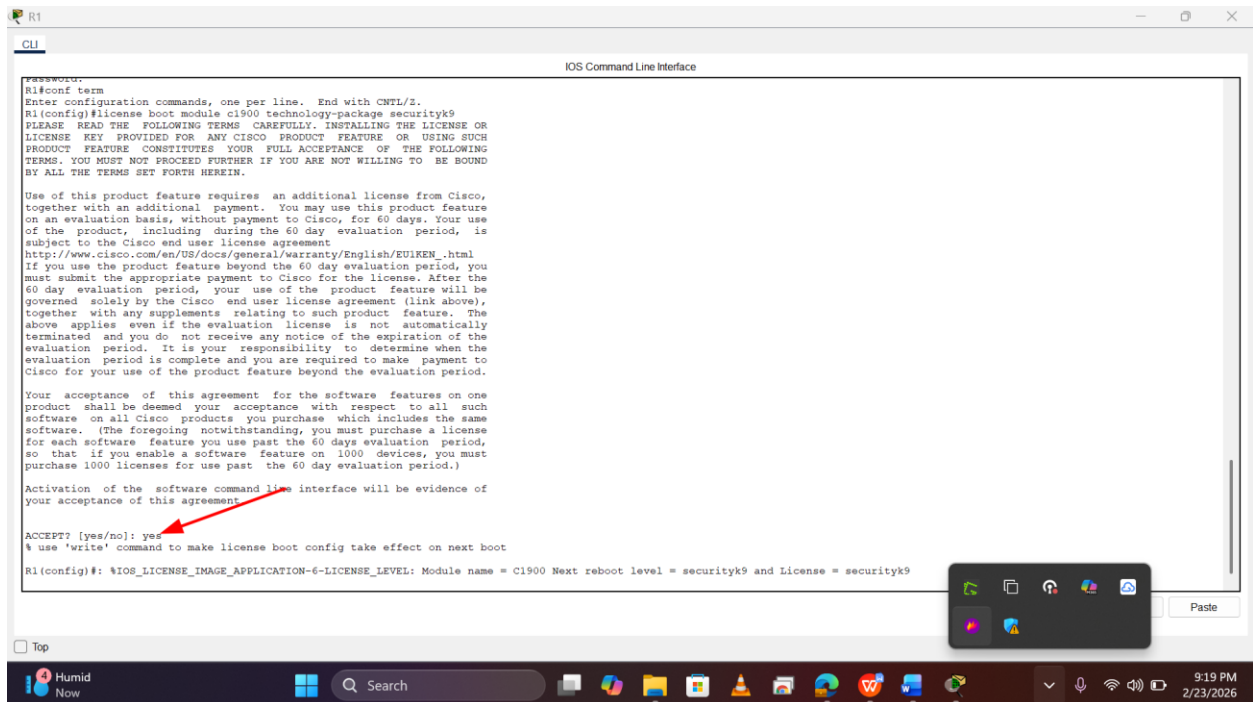
a. Enable the security technology package by using the following command to enable the package.

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

## Week 5 Assignment 2



b. Accept the end-user license agreement.



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

## Week 5 Assignment 2

```
CLI
IOS Command Line Interface

Cisco IOS Software, C1900 software (C1900-UNIVERSALK9-M), Version 15.1(4)M4, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thurs 5-Jan-12 13:41 by pt_team
Image text-base: 0x2100F910, data-base: 0x24729040

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
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/wvl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco CISC01941/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400K8
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)

Press RETURN to get started!

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
00:00:20: %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:
```

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

```
CLI
IOS Command Line Interface

third-party authority to import, export, distribute or use encryption.
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/wvl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco CISC01941/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400K8
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 CISC01941/K9 FTX1524F8G8

Technology Package License Information for Module: 'ci1900'
-----
Technology Technology-package Type Technology-package
Current Next reboot
-----
ipbase ipbasek9 Permanent ipbasek9
security securityk9 Evaluation securityk9
data disable None None

Configuration register is 0x2102

R1#
R1#
```

*Step 3: Identify interesting traffic on R1.*

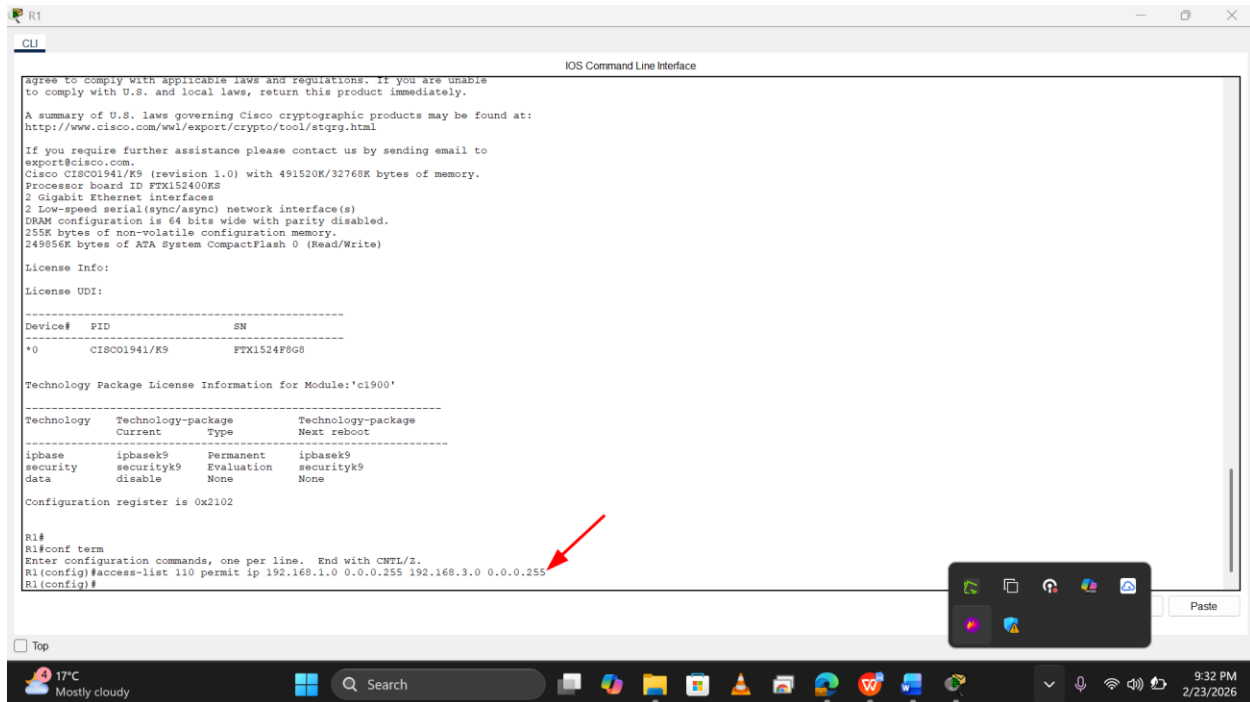
Configure ACL 110 to identify the traffic from the LAN on R1 to the LAN on R3 as interesting. This interesting traffic will trigger the IPsec VPN to be implemented when there is traffic



## Week 5 Assignment 2

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
```



### 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**. 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
```

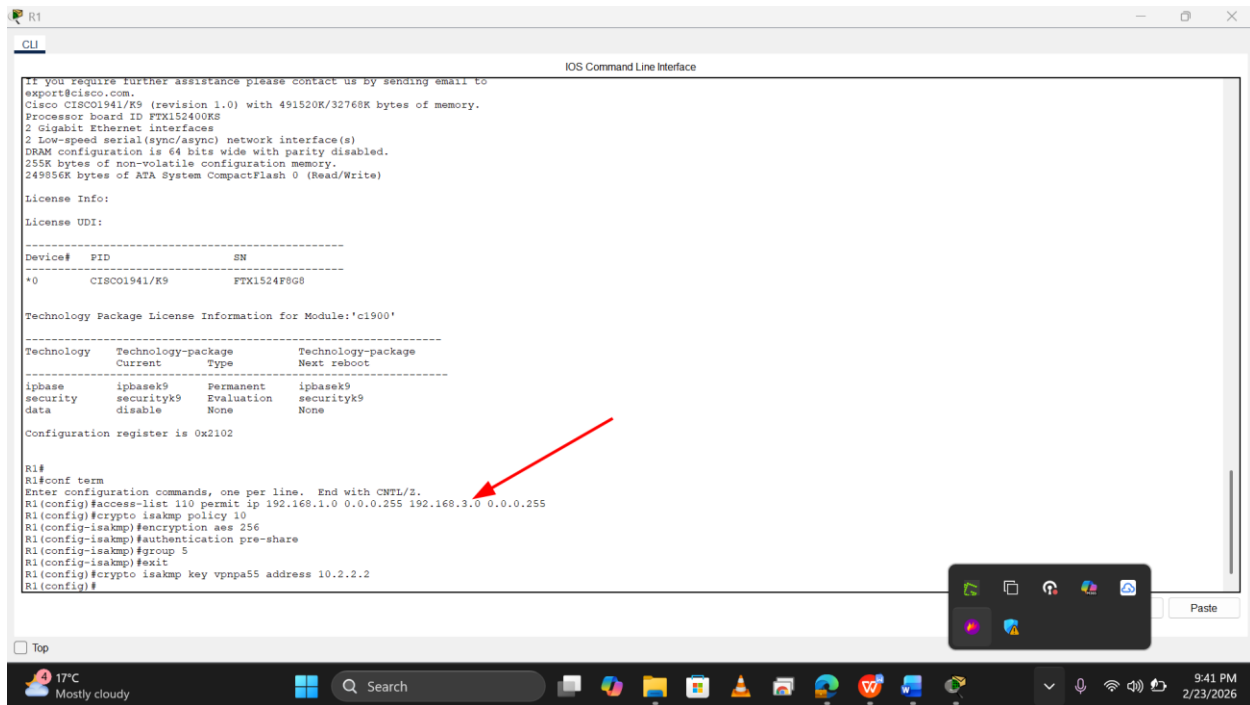
```
R1(config-isakmp)# authentication pre-share
```

```
R1(config-isakmp)# group 5
```

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

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

## Week 5 Assignment 2



```
if you require further assistance please contact us by sending email to
export@cisco.com.
Cisco IOS001941/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400K9
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 CISC001941/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

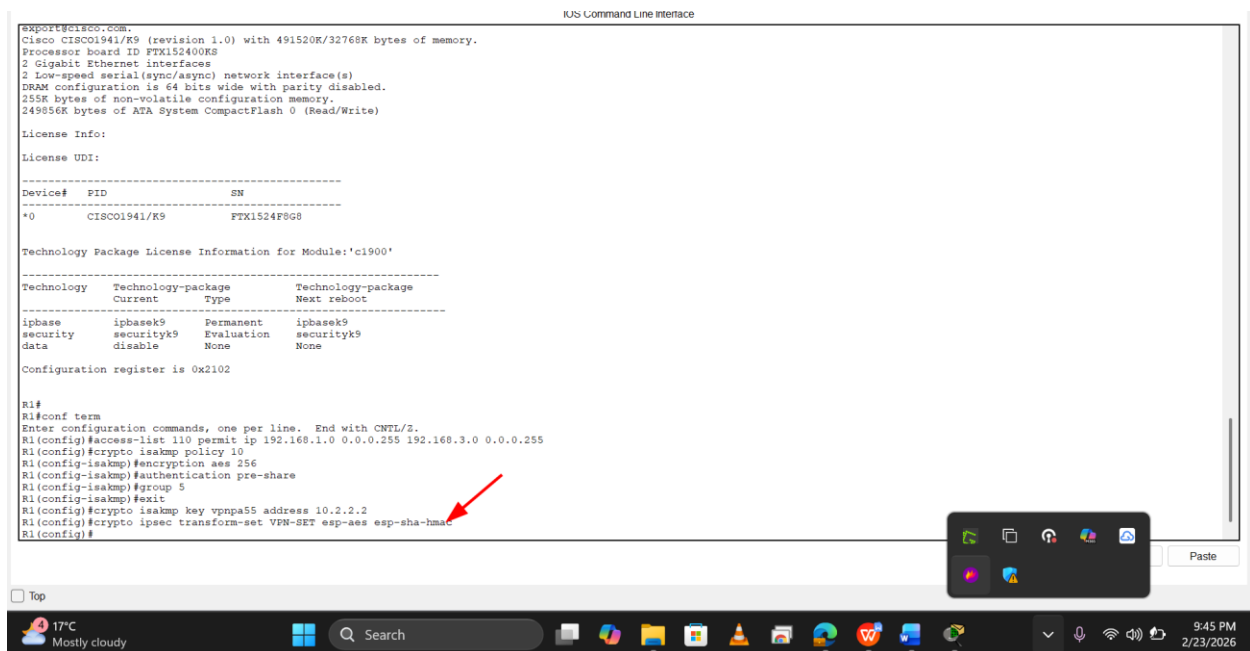
Configuration register is 0x2102

R1#
R1#conf term
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
R1(config)#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)#
```

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**.

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



```
export@cisco.com.
Cisco IOS001941/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400K9
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 CISC001941/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#conf term
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
R1(config)#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)#crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
R1(config)#
```

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.

## Week 5 Assignment 2

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

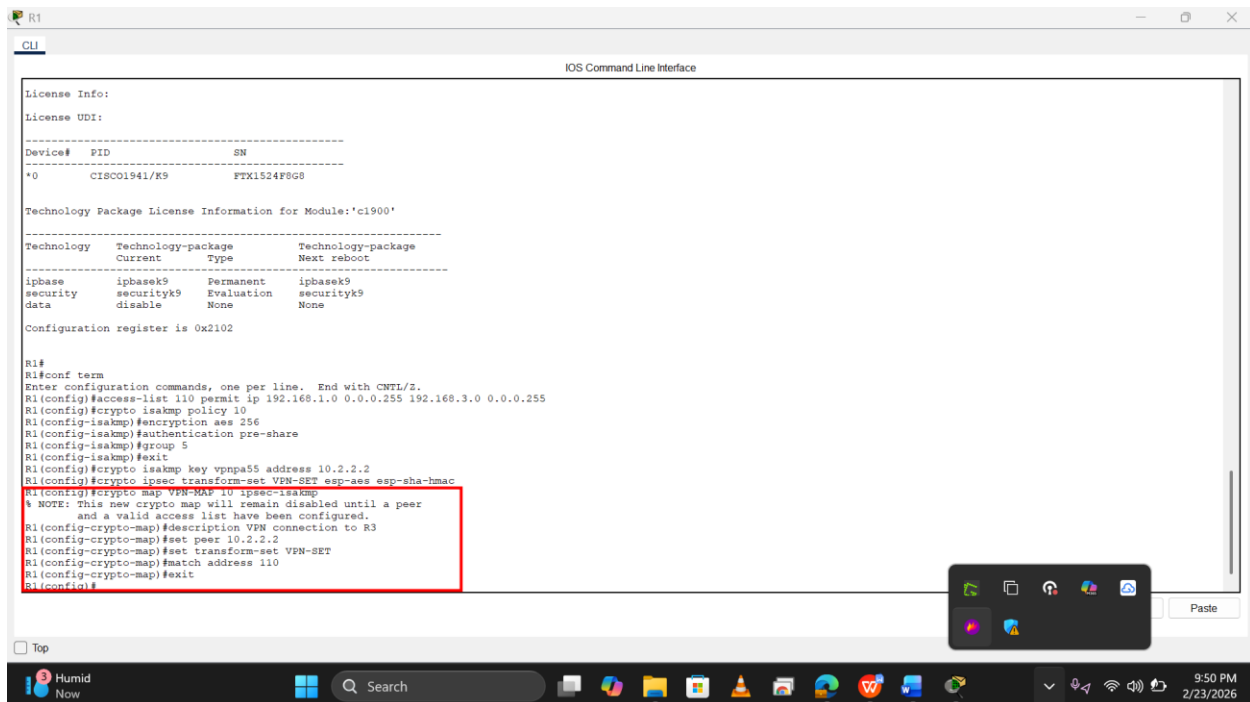
R1(config-crypto-map)# description VPN connection to R3

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
CLI
IOS Command Line Interface

License Info:
License UDI:
-----
Device# PID SN
*0 CISC01941/K9 FTX1524F6G8

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#conf term
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
R1(config)#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)#crypto ipsec transform-set VPN-SET esp-aes 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)#
```

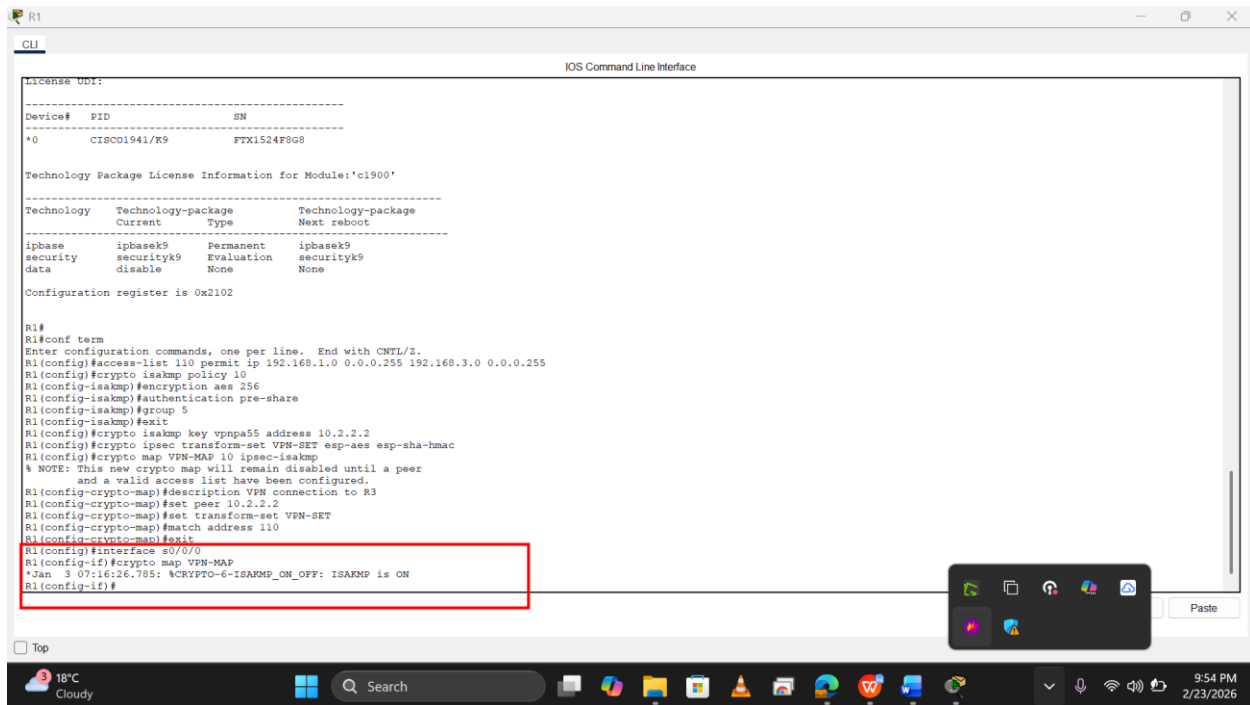
*Step 6: Configure the crypto map on the outgoing interface.*

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

## Week 5 Assignment 2



```
CLI
IOS Command Line Interface

License UDI:
-----
Device# PID SN
*0 CISCO1941/K9 FTX1524F8G8

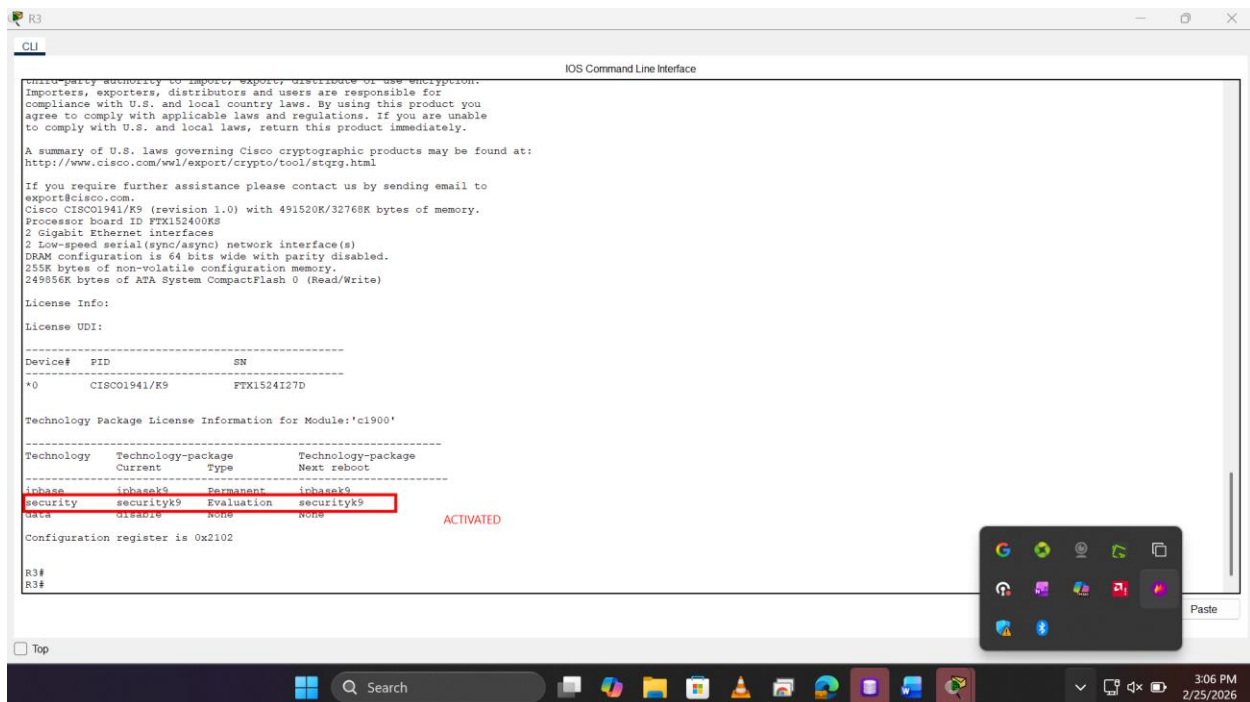
Technology Package License Information for Module:'c1900'
-----
Technology Technology-package Type Technology-package
Current Next reboot
-----
ipbase ipbasek9 Permanent ipbasek9
security securityk9 Evaluation securityk9
data disable None None
Configuration register is 0x2102

R1#
R1#conf term
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
R1(config)#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)#crypto ipsec transform-set VPN-SET esp-aes 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 2: Configure IPsec Parameters on R3

#### Step 1: Enable the Security Technology package.

- On R3, issue the show version command to verify that the Security Technology package license information has been enabled.
- If the security technology package has not been enabled, enable the package and reload R3.



```
CLI
IOS Command Line Interface

third-party technology to import, export, distribute or use encryption.
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/wurl/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 FTX15240UKS
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 Type Technology-package
Current Next reboot
-----
ipbase ipbasek9 Permanent ipbasek9
security securityk9 Evaluation securityk9
data disable None None
Configuration register is 0x2102

R3#
R3#
```

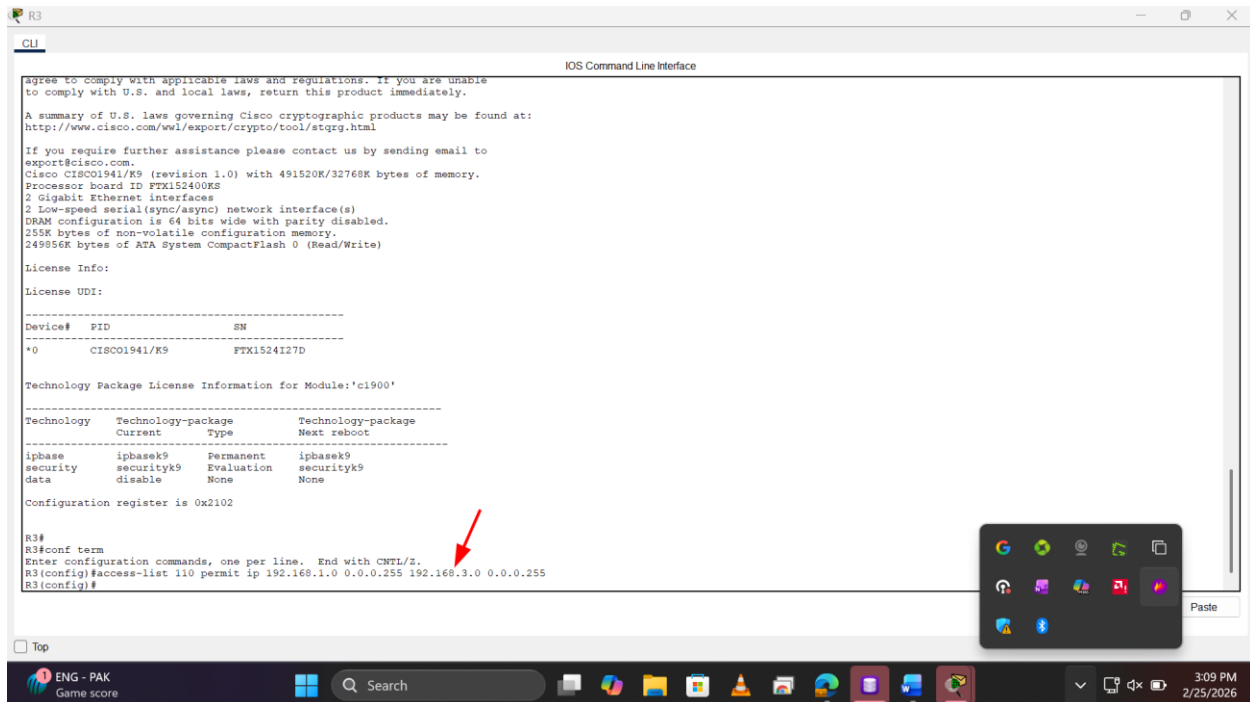
ACTIVATED

## Week 5 Assignment 2

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

Configure reciprocating parameters on R3. Configure ACL 110 to identify 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 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
```

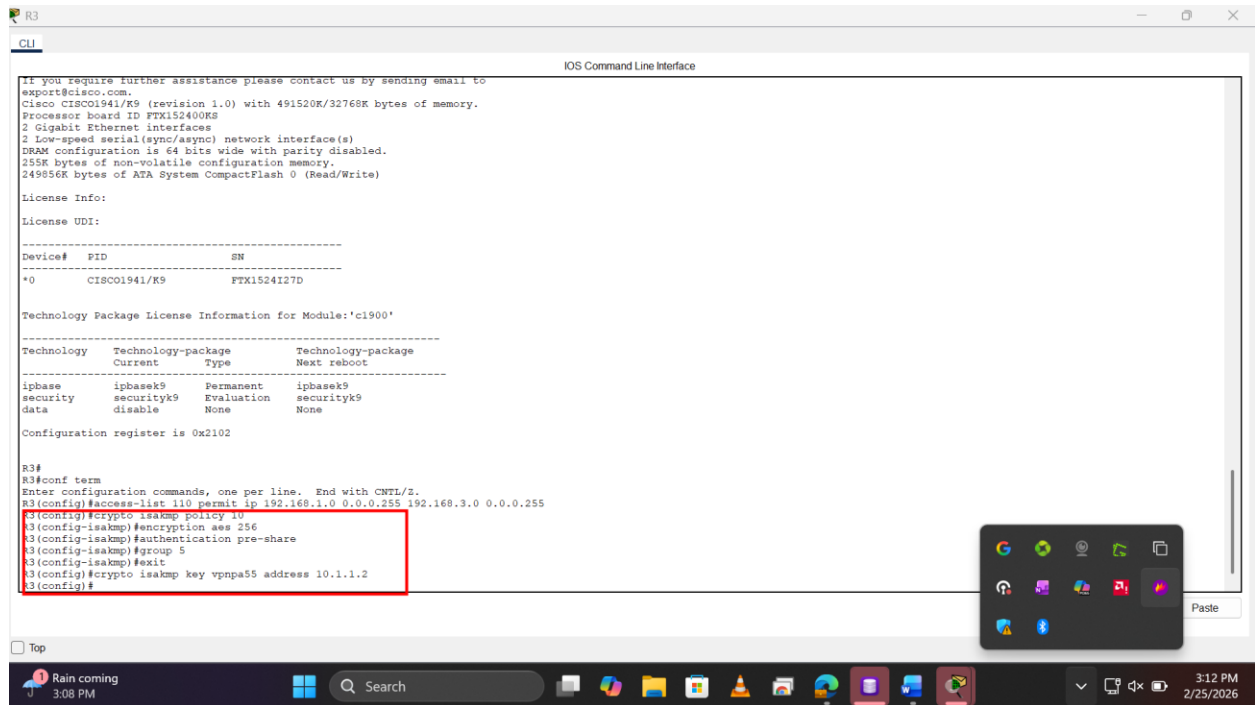
```
R3(config-isakmp)# authentication pre-share
```

```
R3(config-isakmp)# group 5
```

```
R3(config-isakmp)# exit
```

```
R3(config)# crypto isakmp key vpnpa55 address 10.1.1.2
```

## Week 5 Assignment 2



```
CLI
IOS Command Line Interface

If you require further assistance please contact us by sending email to
export@cisco.com.
Cisco CISC01941/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400K9
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 CISC01941/K9 FTX1524127D

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#conf term
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
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)#
```

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

c. 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
```

d. Create the crypto map VPN-MAP to bind 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
```

The image shows a Cisco IOS Command Line Interface (CLI) session. The top of the window displays the title "IOS Command Line Interface". The main content area shows the following text:

```
License Info:
License UDI:
-----
Device# PID SN
-----
*0 CISC01941/K5 FTK1524127D

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

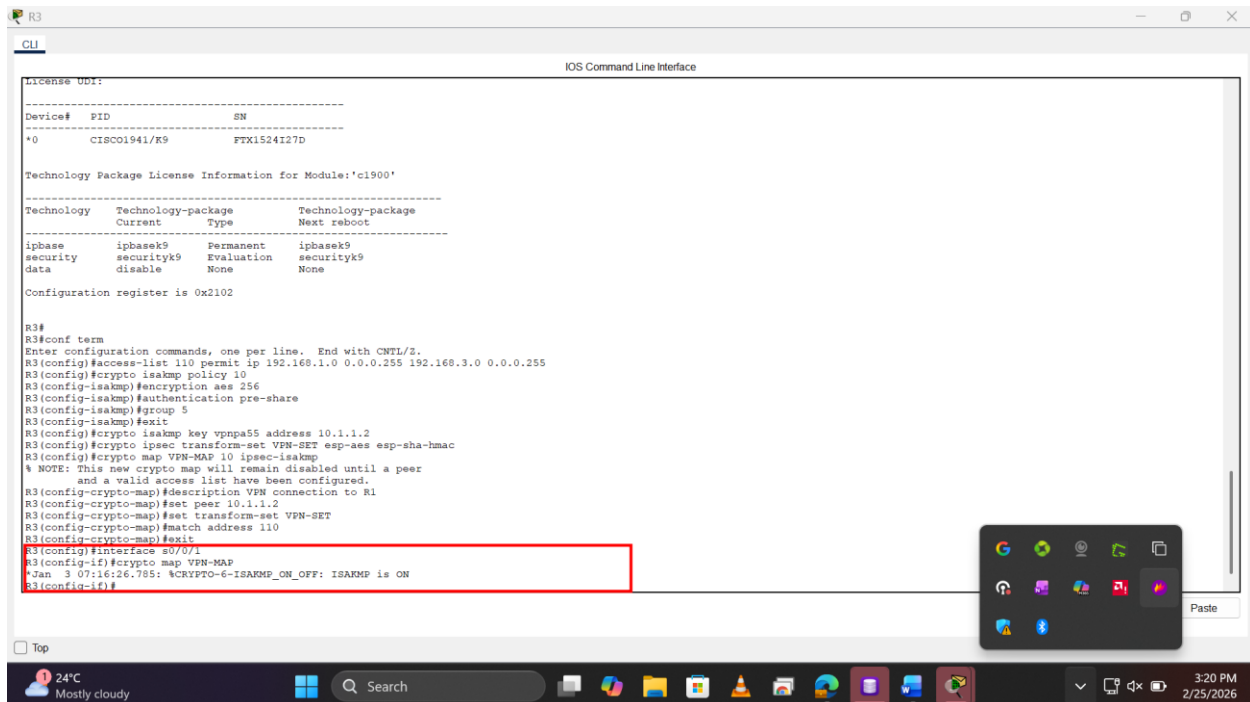
R3#
R3#conf term
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
R3(config)#crypto isakmp policy 10
R3(config-isakmp)#encryption aes 256
R3(config-isakmp)#authentication pre-share
R3(config-isakmp)#group 5
R3(config-isakmp)#exit
R3(config)#crypto isakmp key vpnpa55 address 10.1.1.2
R3(config)#crypto isakmp 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)#
```

A red rectangular box highlights the configuration commands starting from `R3(config)#crypto isakmp key vpnpa55 address 10.1.1.2` down to `R3(config)#`.

At the bottom of the window, there is a taskbar with various icons, including a clock showing 24°C, a search bar, and a system tray with icons for network, volume, and power. The date and time in the bottom right corner are 3:17 PM on 2/25/2026.

Bind the VPN-MAP crypto map to the outgoing Serial 0/0/1 interface.

```
R3(config-if)# crypto map VPN-MAP
```

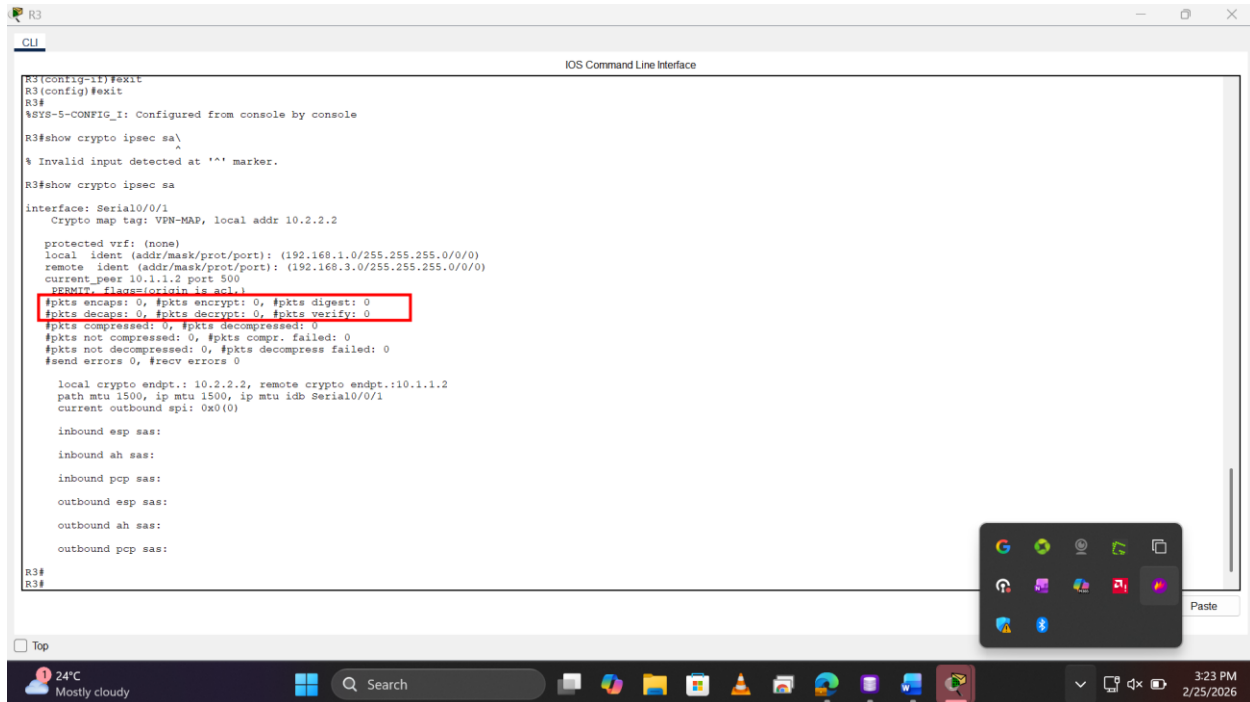


## Week 5 Assignment 2

### 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.



```
R3(config-if)#exit
R3(config)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console
R3#show crypto ipsec sa
% Invalid input detected at '^' marker.
R3#show crypto ipsec sa
interface: Serial0/0/1
  Crypto map tag: VPN-MAP, local addr 10.2.2.2

  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 10.1.1.2 port 500
    PERMIT, flags(origin-is-akl)
    #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.: 10.2.2.2, remote crypto endpt.: 10.1.1.2
  path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/1
  current outbound spi: 0x0(0)

inbound esp sas:

inbound ah sas:

inbound pcp sas:

outbound esp sas:

outbound ah sas:

outbound pcp sas:

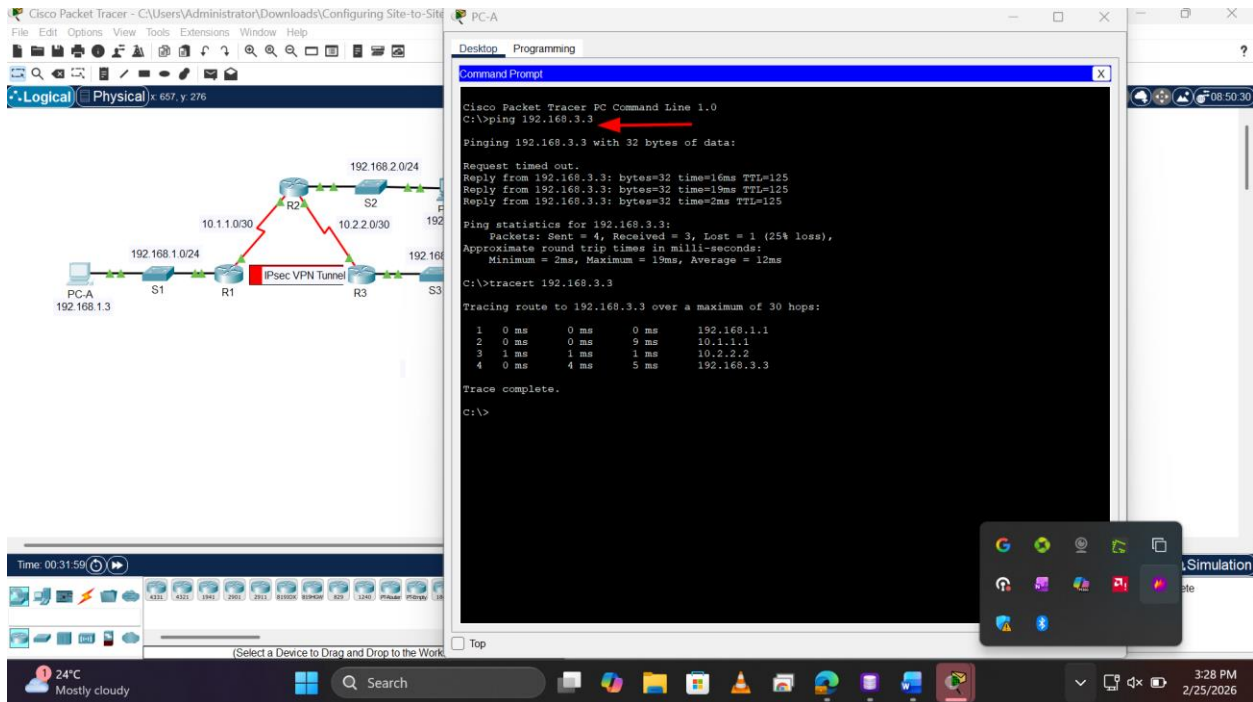
R3#
R3#
```

#### Step 2: Create interesting traffic.

Ping PC-C from PC-A.



## Week 5 Assignment 2



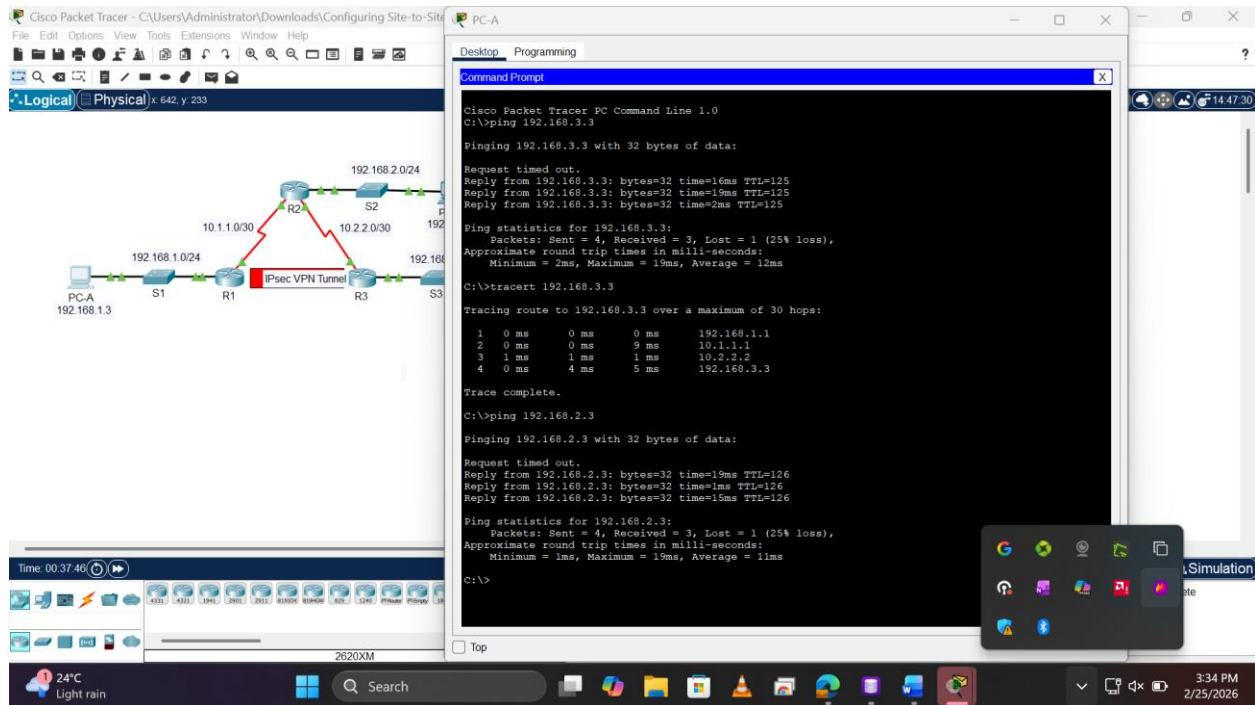
### *Step 3: Verify the tunnel after interesting traffic.*

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.

### *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.

## Week 5 Assignment 2



### 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.

### 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.

## Conclusion

In conclusion, this lab successfully demonstrates how to deploy, configure, and verify a functioning site-to-site IPsec VPN between two Cisco routers. After applying the required ISAKMP and IPsec policies to routers R1 and R3, the operation of the VPN tunnel was systematically tested. By generating interesting traffic (pinging from PC-A to PC-C) and analyzing the output of the `show crypto ipsec sa` command, it was confirmed that the tunnel actively encapsulated and encrypted the designated packets. Furthermore, the exercise validated that the VPN tunnel is highly selective; generating uninteresting traffic (such as pinging PC-B from PC-A) did not increase the encrypted packet count, verifying that non-targeted traffic bypassed the IPsec tunnel. Ultimately, the lab confirms that IPsec VPNs can successfully and selectively secure inter-LAN communication across unprotected networks.