Week 5 Assignment 2

Course: Cloud and Network Security - C1-2026

Student Name: Bussllus Bertrand

Student Number: CS-CNS11-26004

Wednesday, February 25, 2026

Class Exercise: Configuring Site-to-Site VPNs

Contents

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

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 **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

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	**86400**	**86400**
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**

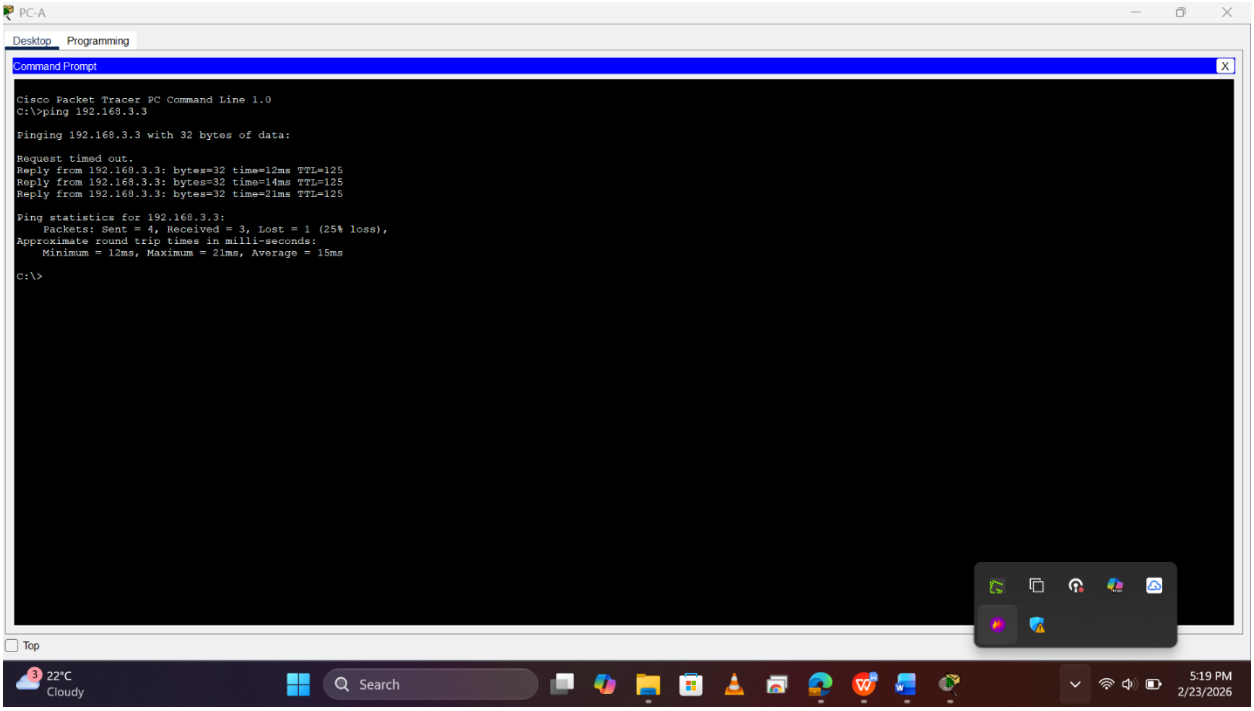
- Enable password: **ciscoenpa55**
- SSH username and password: **SSHadmin** / **ciscosshpa55**
- OSPF 101

Instructions

Part 1: Configure IPsec Parameters on R1

Step 1: Test connectivity.

Ping from PC-A to PC-C.

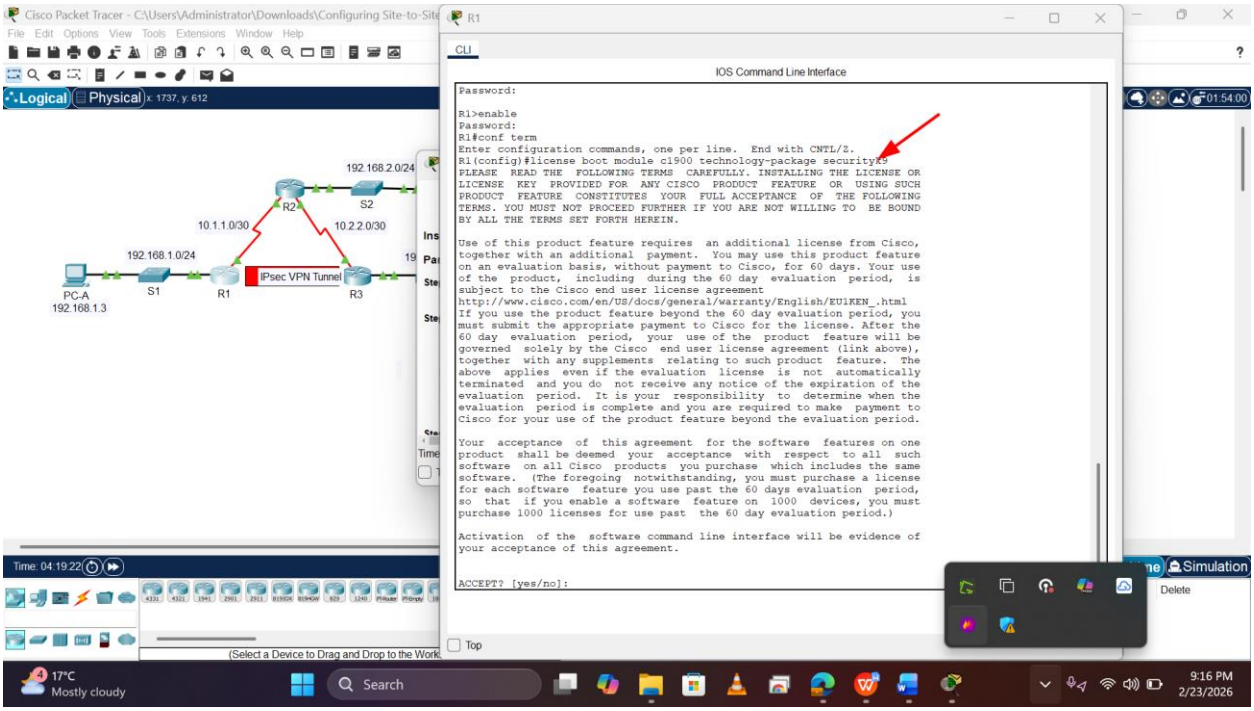


Step 2: Enable the Security Technology package.

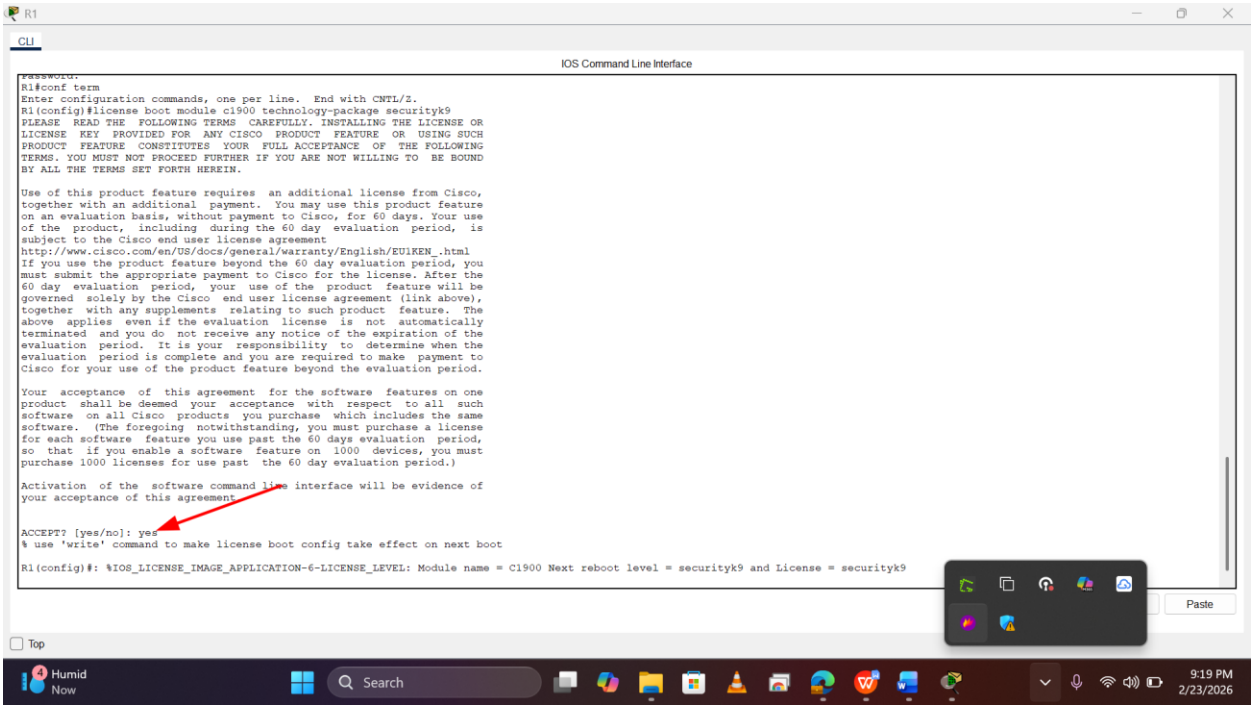
a. Enable the security technology package by using the following command to enable the package.

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

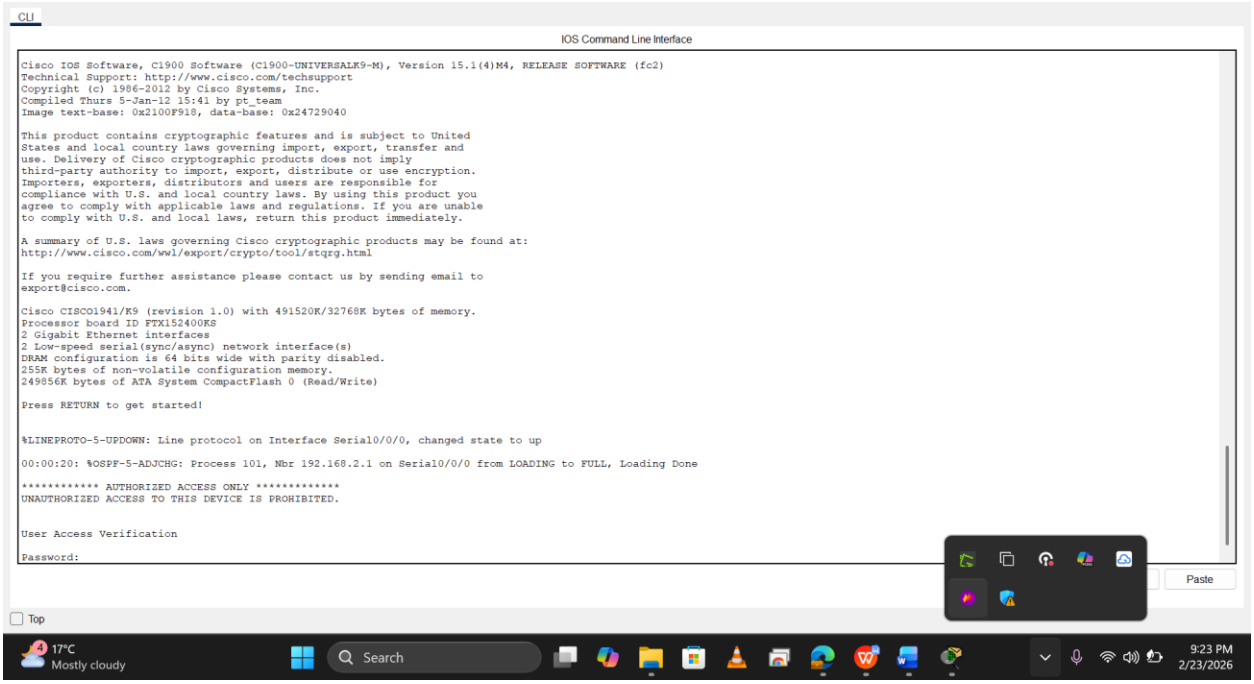
Week 5 Assignment 2



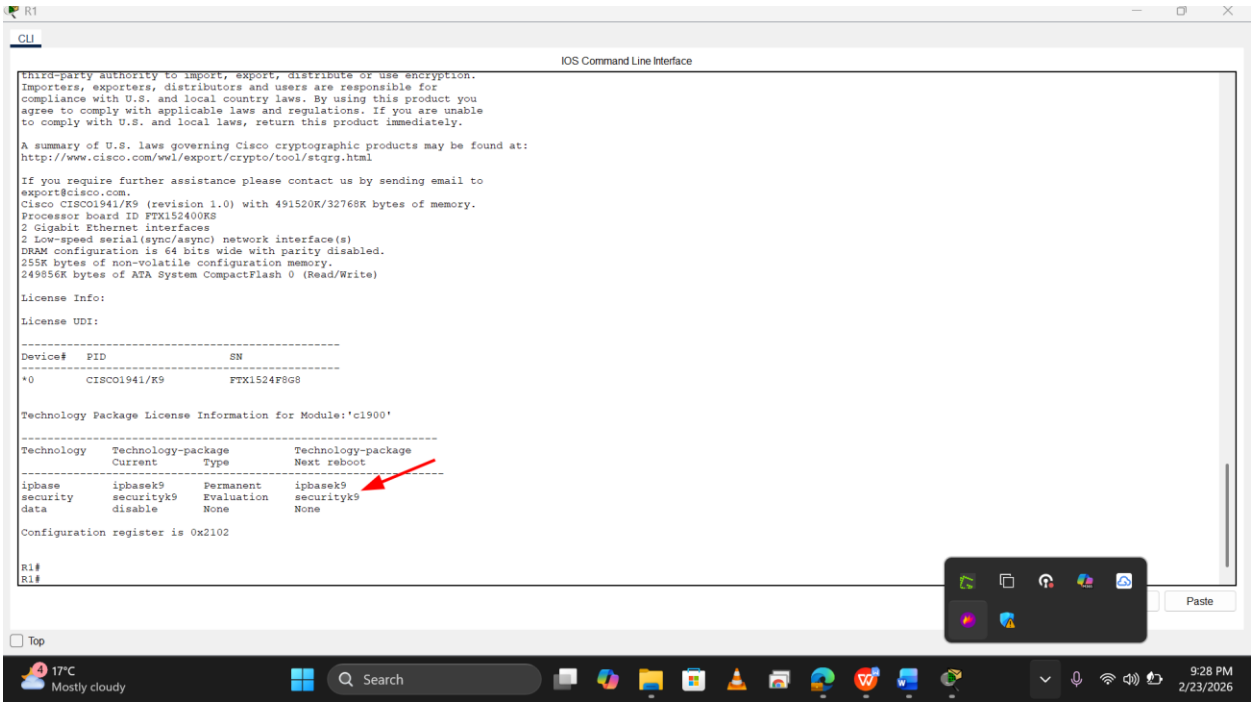
b. Accept the end-user license agreement.



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



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

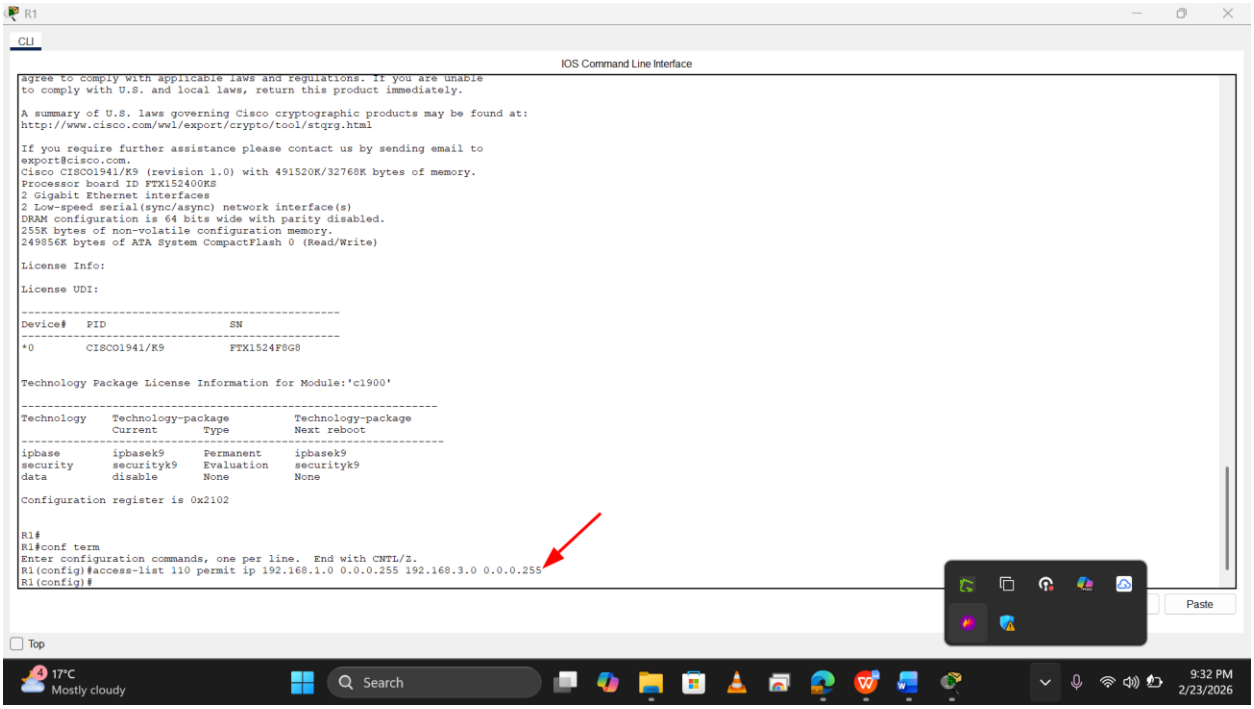


Step 3: Identify interesting traffic on R1.

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

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

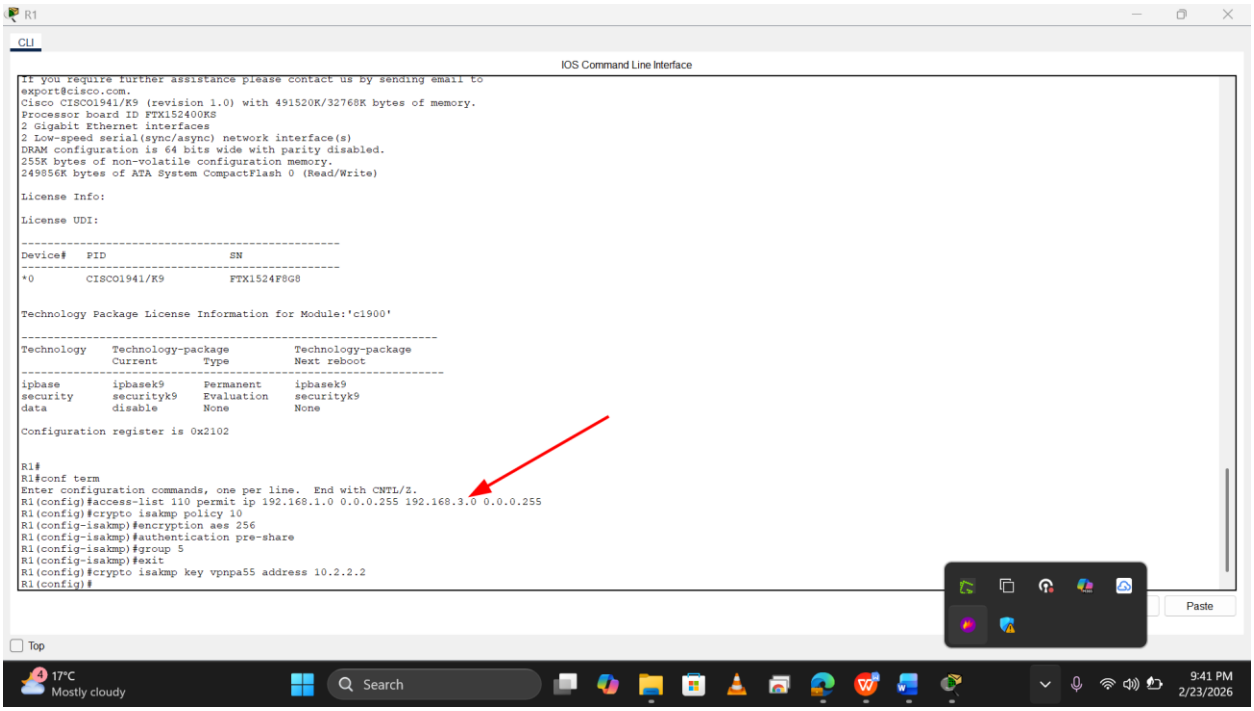
R1(config-isakmp)# encryption aes 256

R1(config-isakmp)# authentication pre-share

R1(config-isakmp)# group 5

R1(config-isakmp)# exit

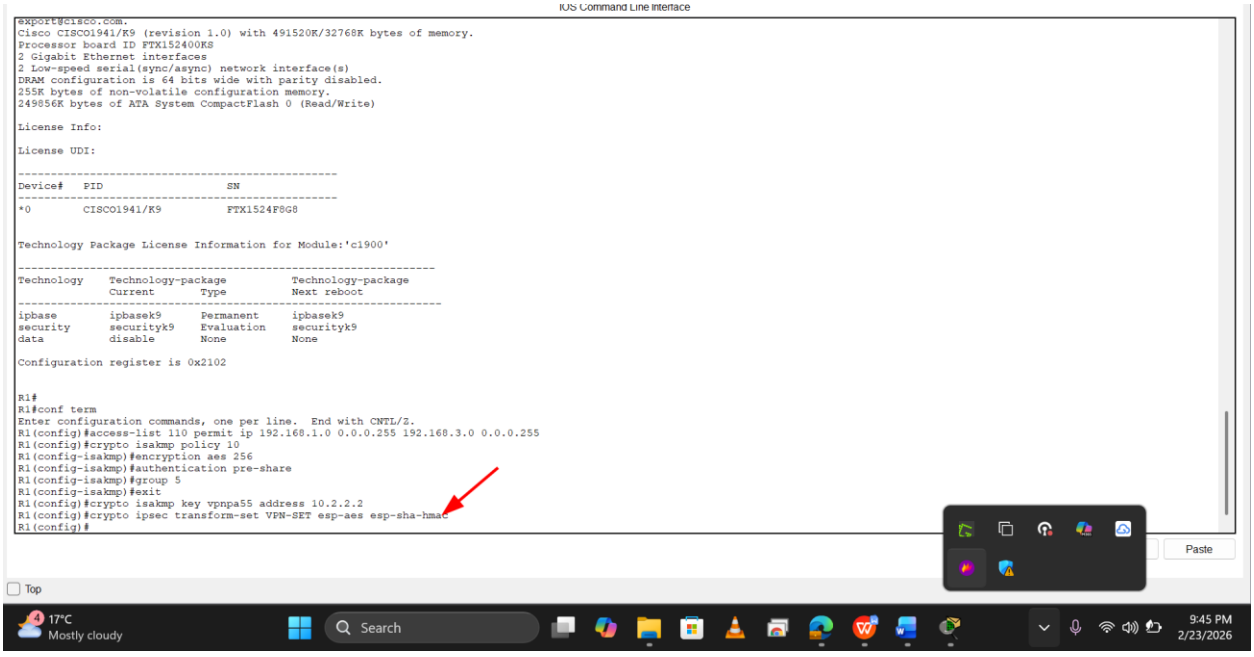
R1(config)# crypto isakmp key vpnpa55 address 10.2.2.2



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



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

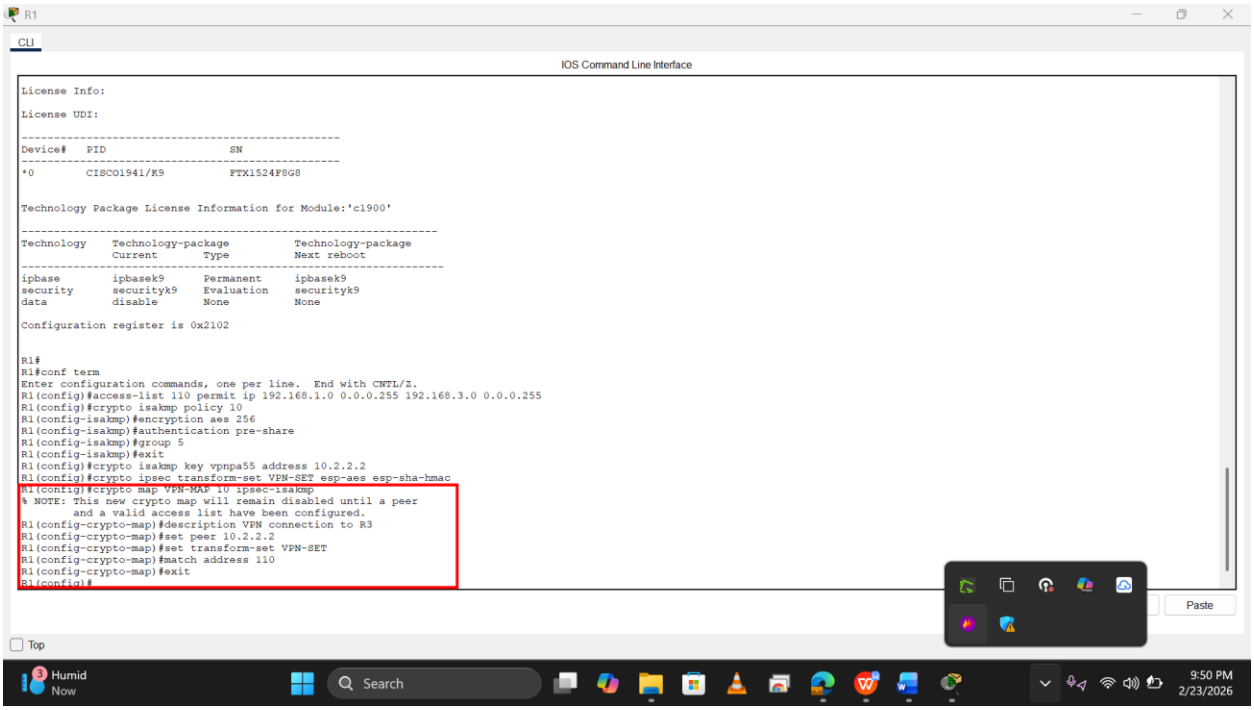
R1(config-crypto-map)# description VPN connection to R3

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

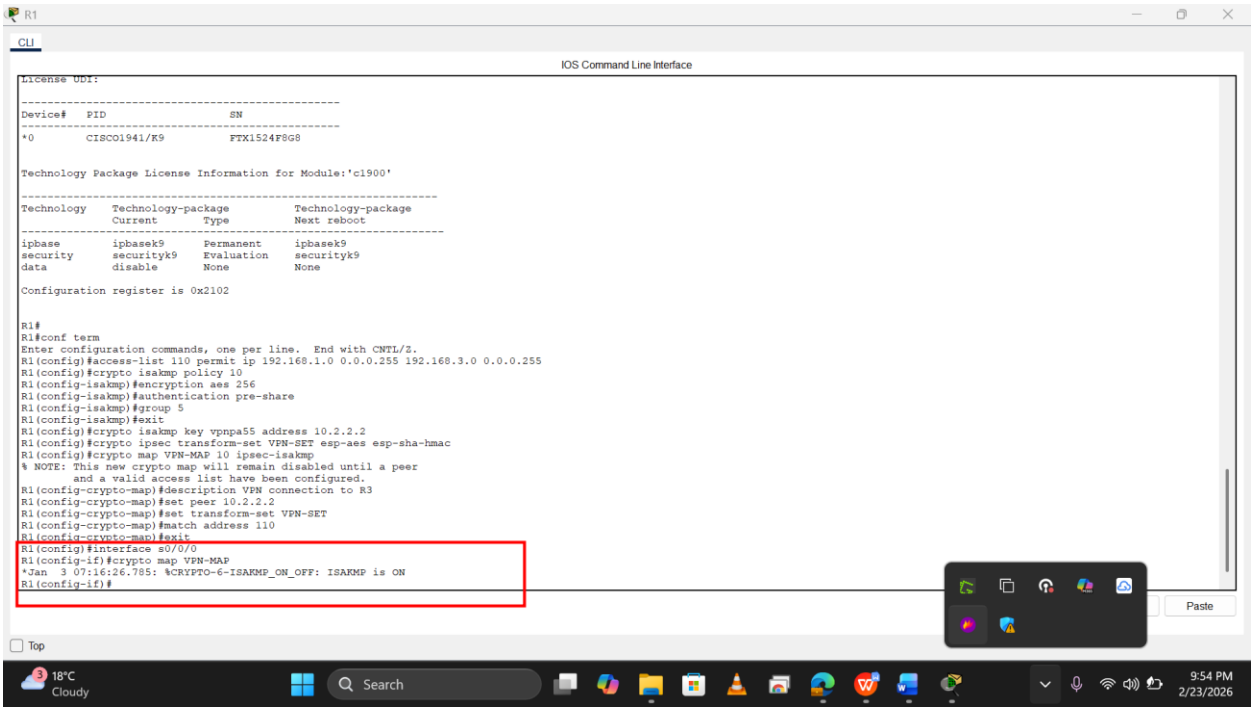


Step 6: Configure the crypto map on the outgoing interface.

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

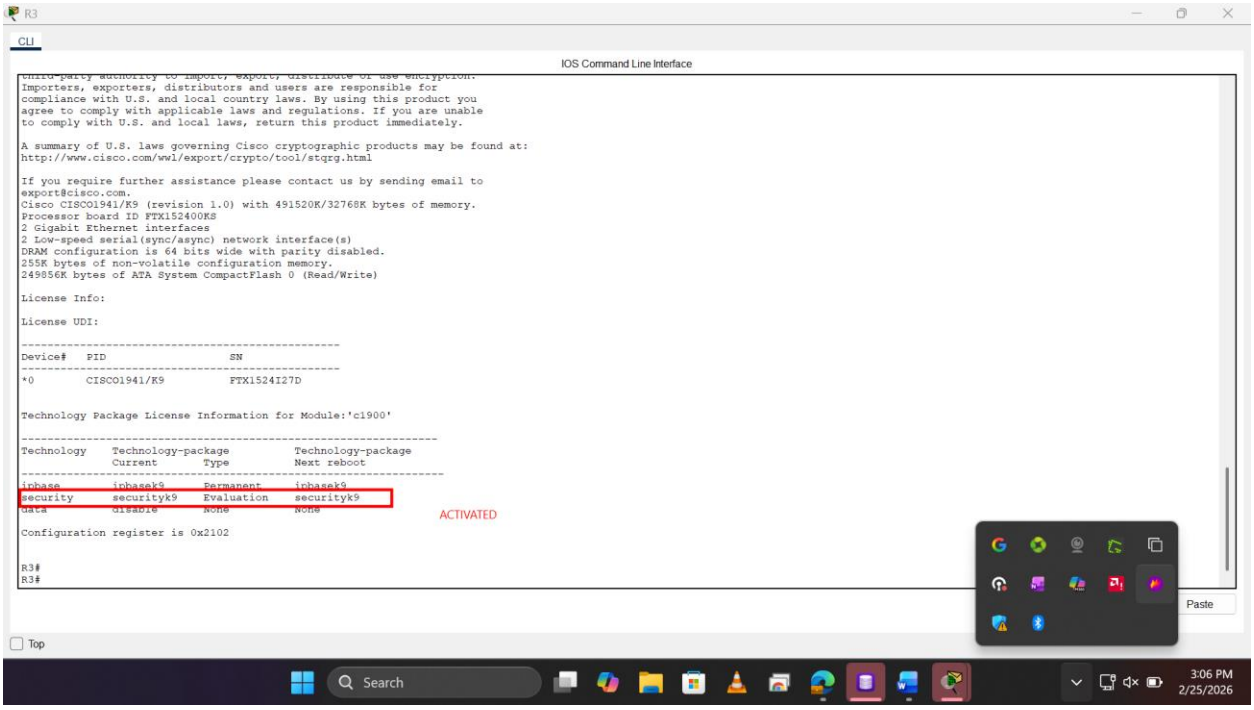


Part 2: Configure IPsec Parameters on R3

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.

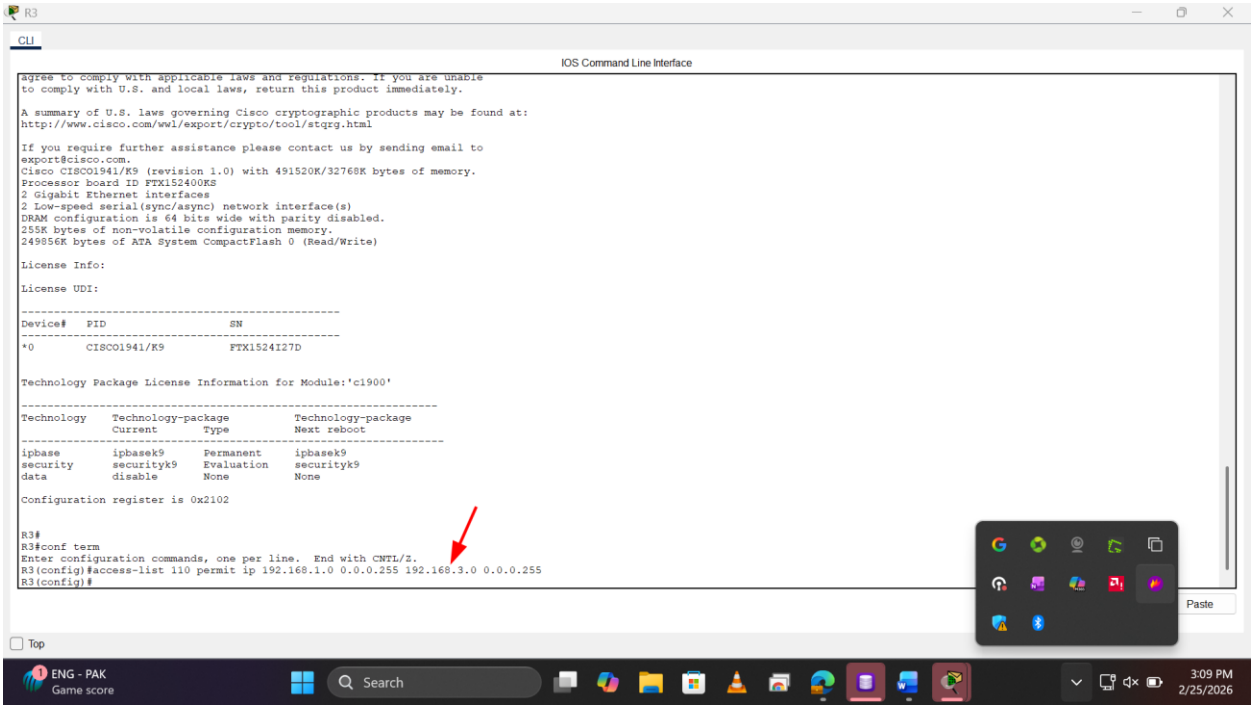
b. If the security technology package has not been enabled, enable the package and reload R3.



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

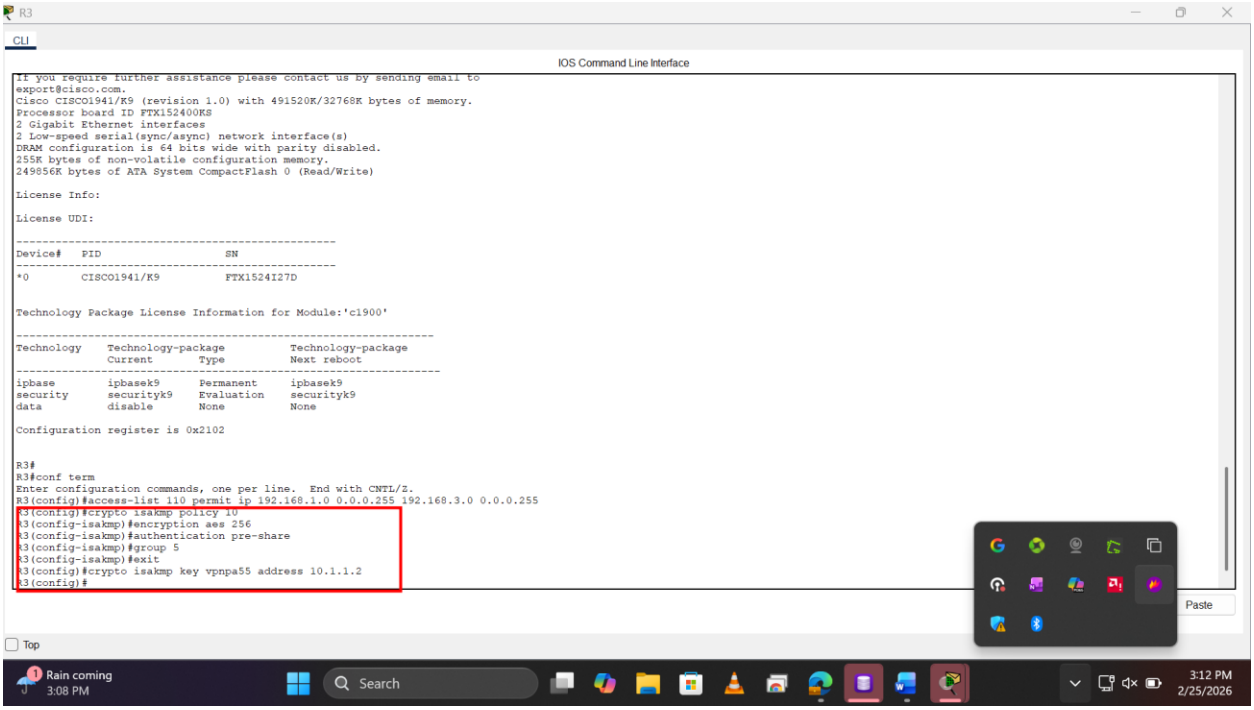
R3(config-isakmp)# encryption aes 256

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



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

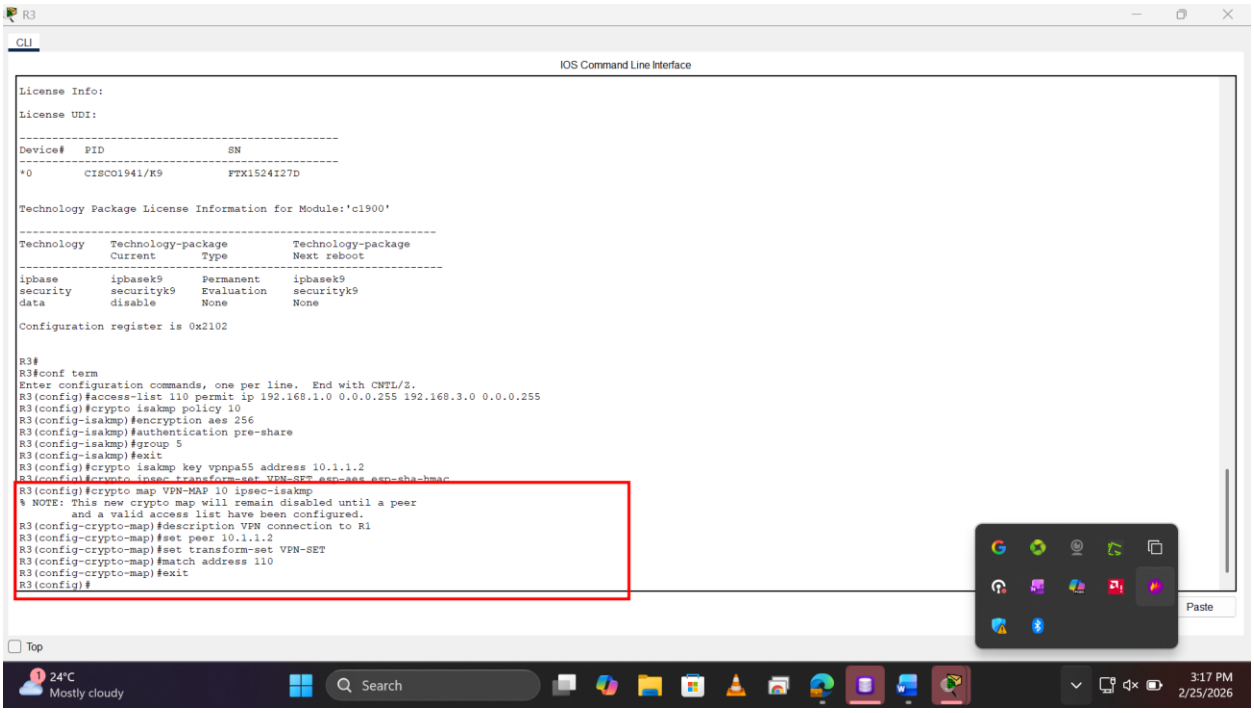
R3(config-crypto-map)# description VPN connection to R1

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

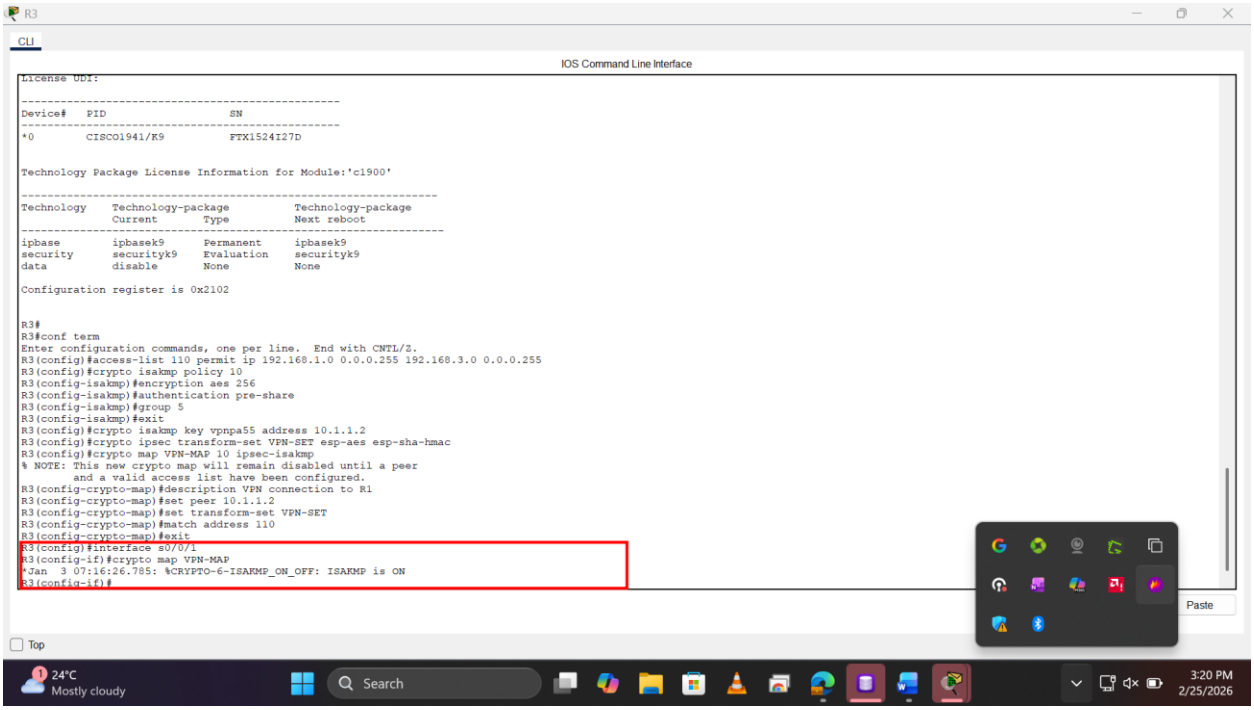


Step 5: Configure the crypto map on the outgoing interface.

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

R3(config)# interface s0/0/1

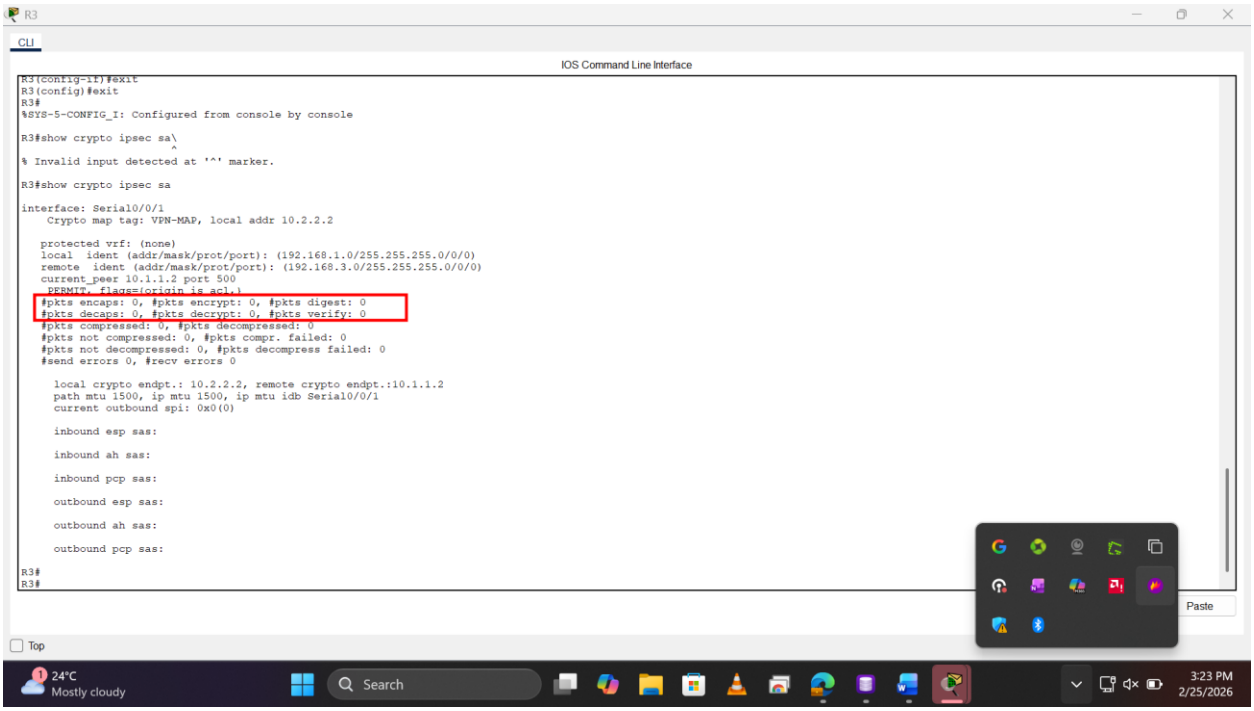
R3(config-if)# crypto map VPN-MAP



Part 3: Verify the IPsec VPN

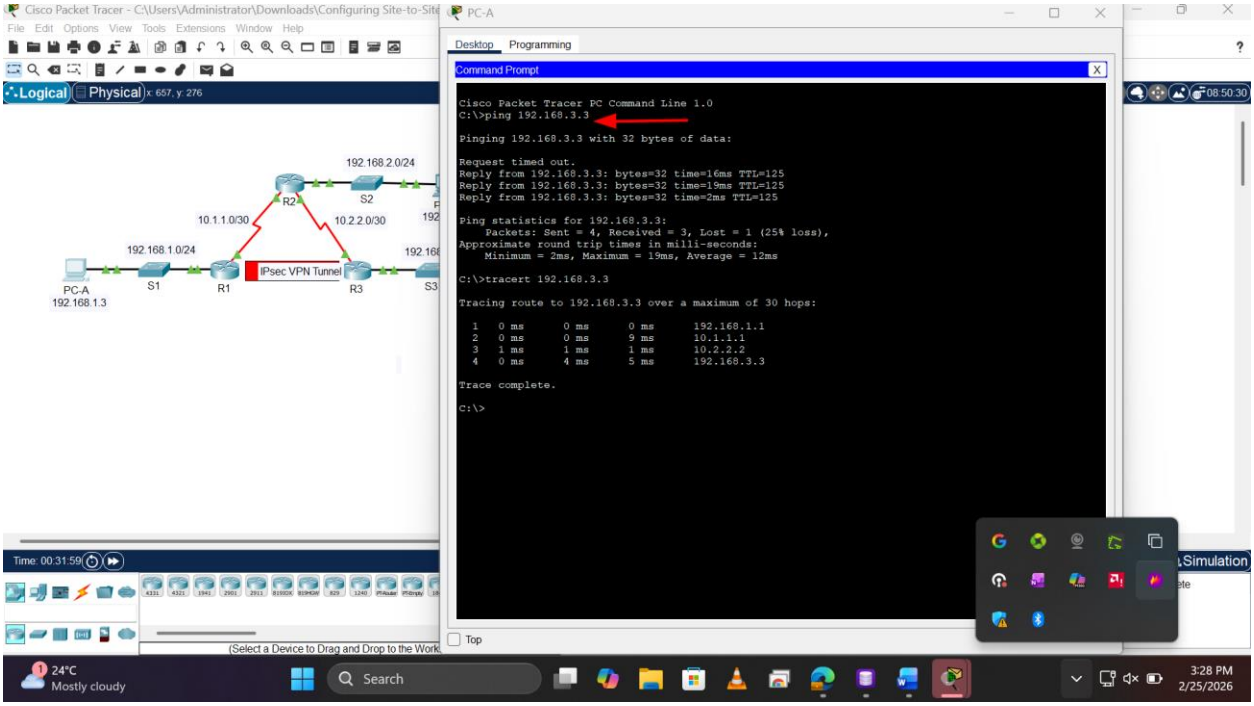
Step 1: Verify the tunnel prior to interesting traffic.

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.



Step 2: Create interesting traffic.

Ping PC-C from PC-A.

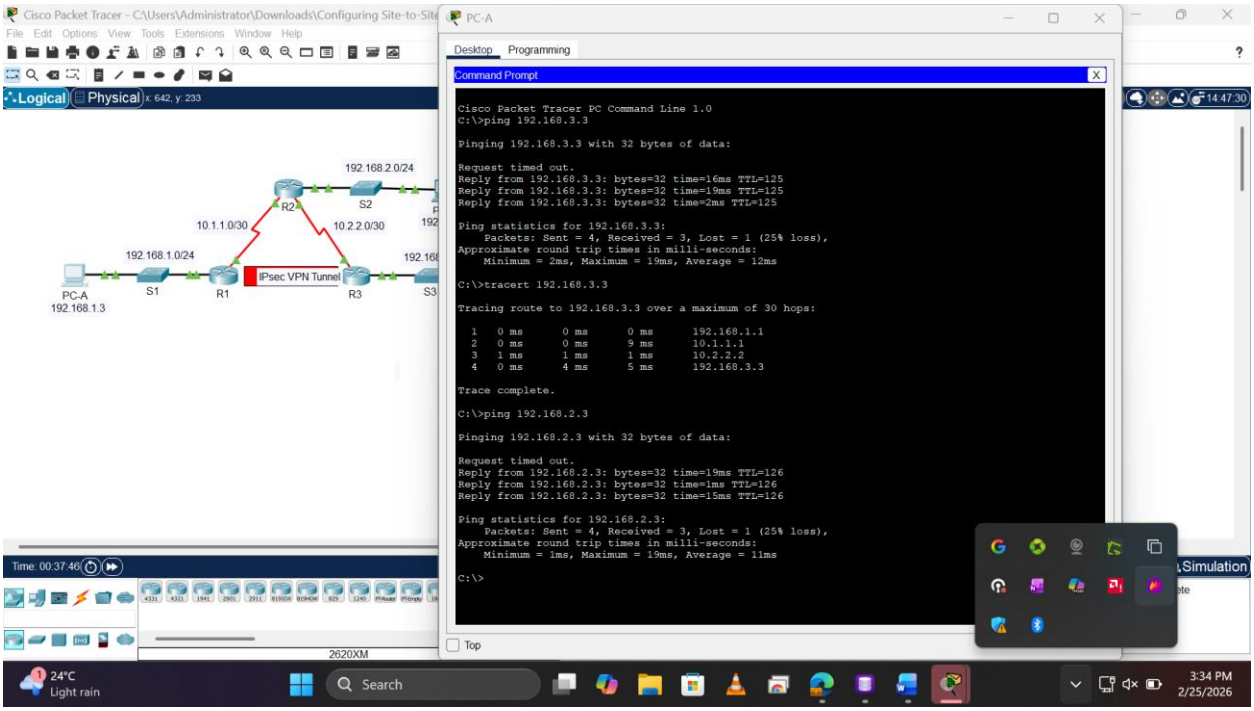


Step 3: Verify the tunnel after interesting traffic.

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.



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.