COURSE: CLOUD AND NETWORK SECURITY

NAME: DENISE SOPHY ONDISO MUTAYI

STUDENT NO: CS-CN09-25047

CONFIGURING SITE-TO-SITE VPNS

Table of contents

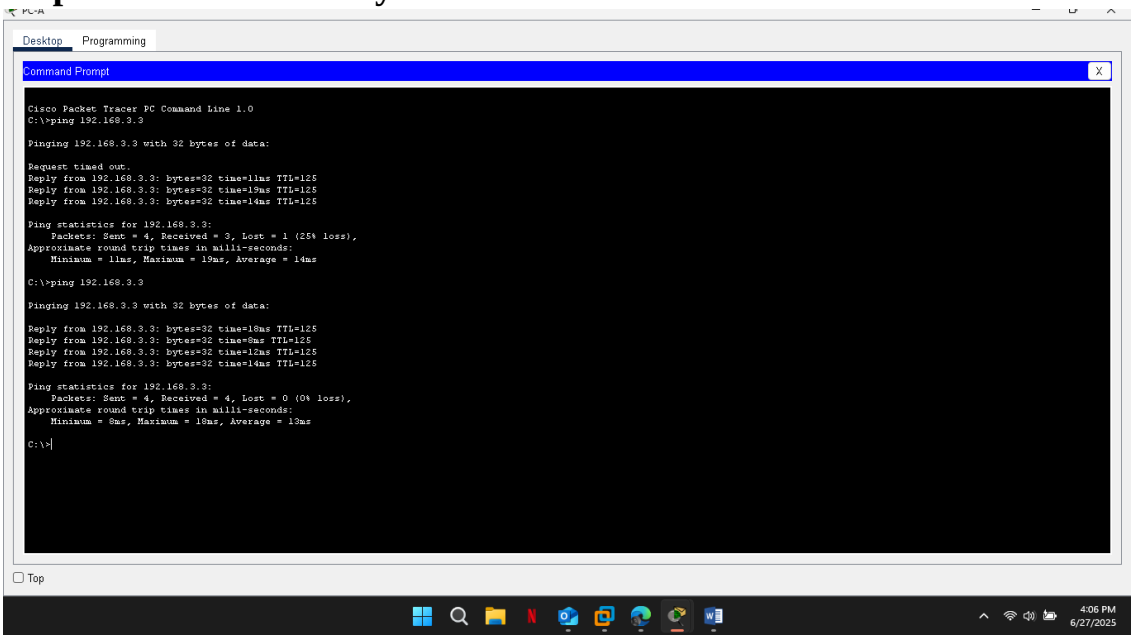
INTRODUCTION

This Packet Tracer activity involved the configuration and verification of a site-to-site IPsec VPN between two routers, R1 and R3, which were connected through an intermediary router, R2, acting as a simple pass-through with no VPN awareness. The primary goal was to secure communication between the LANs of R1 (192.168.1.0/24) and R3 (192.168.3.0/24) by using IPsec to encrypt traffic across the untrusted transit network.

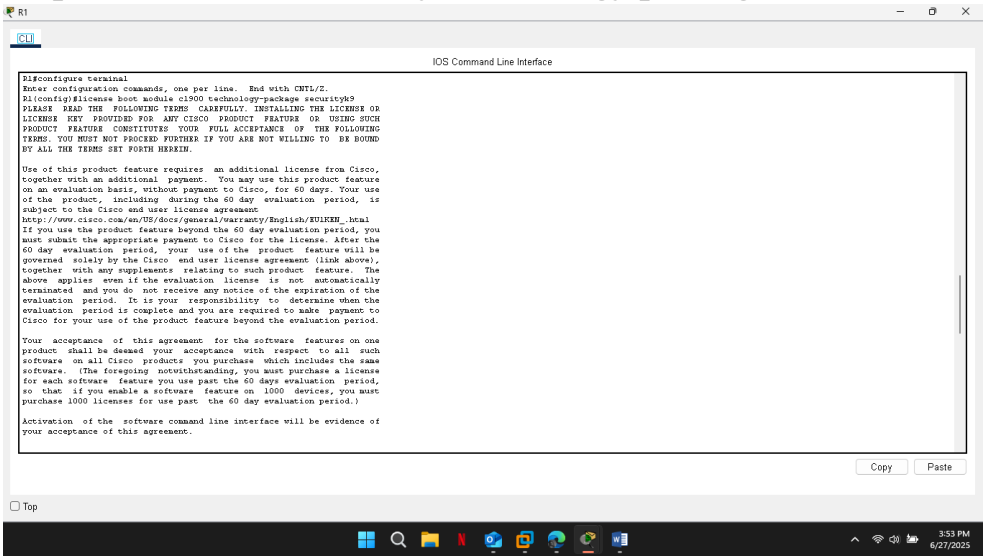
The task included enabling the securityk9 license package on both R1 and R3, defining interesting traffic using ACL 110, configuring IKE Phase 1 (ISAKMP) policies with AES-256 encryption and DH Group 5 key exchange, and setting up IPsec Phase 2 with ESP using AES and SHA-HMAC for authentication. The VPN configuration was finalized using crypto maps, which were applied to the appropriate serial interfaces. Throughout the process, commands such as show crypto isakmp sa and show crypto ipsec sa were used to verify tunnel establishment and packet encryption.

PART 1: CONFIGURE IPSEC PARAMETERS ON R1

Step 1: Test connectivity.

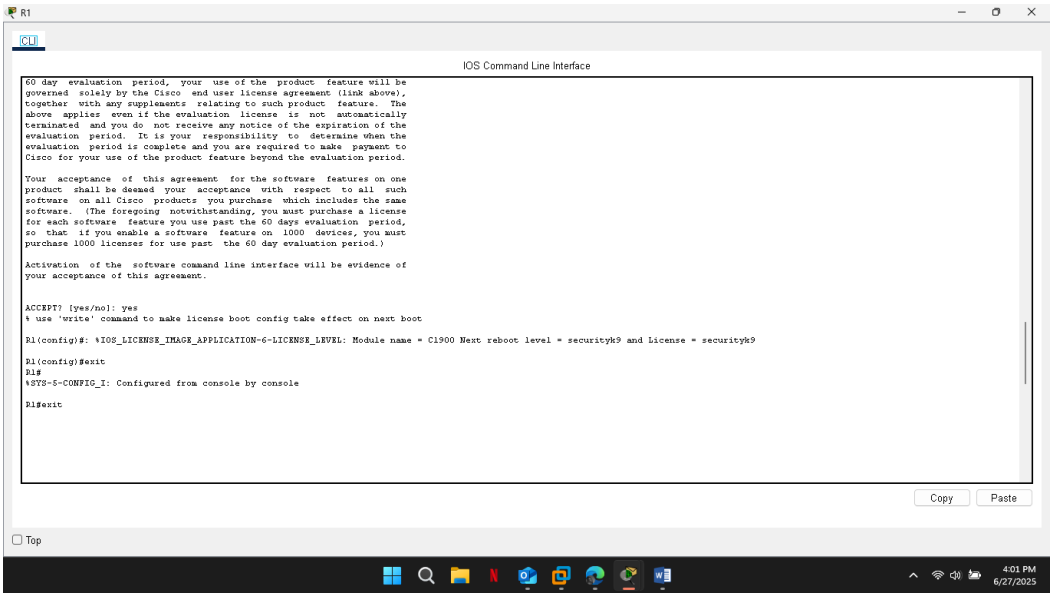


Step 2: Enable the Security Technology package.

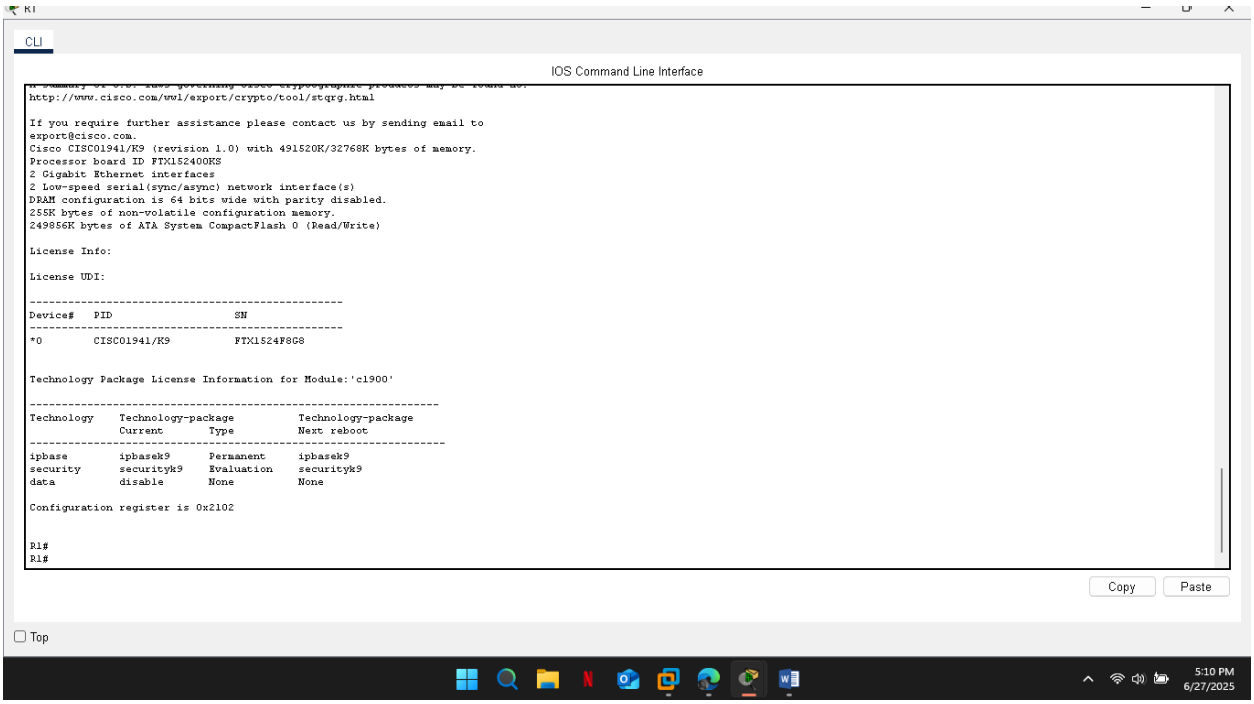


Enable the security technology package by using the following command to enable the package.

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

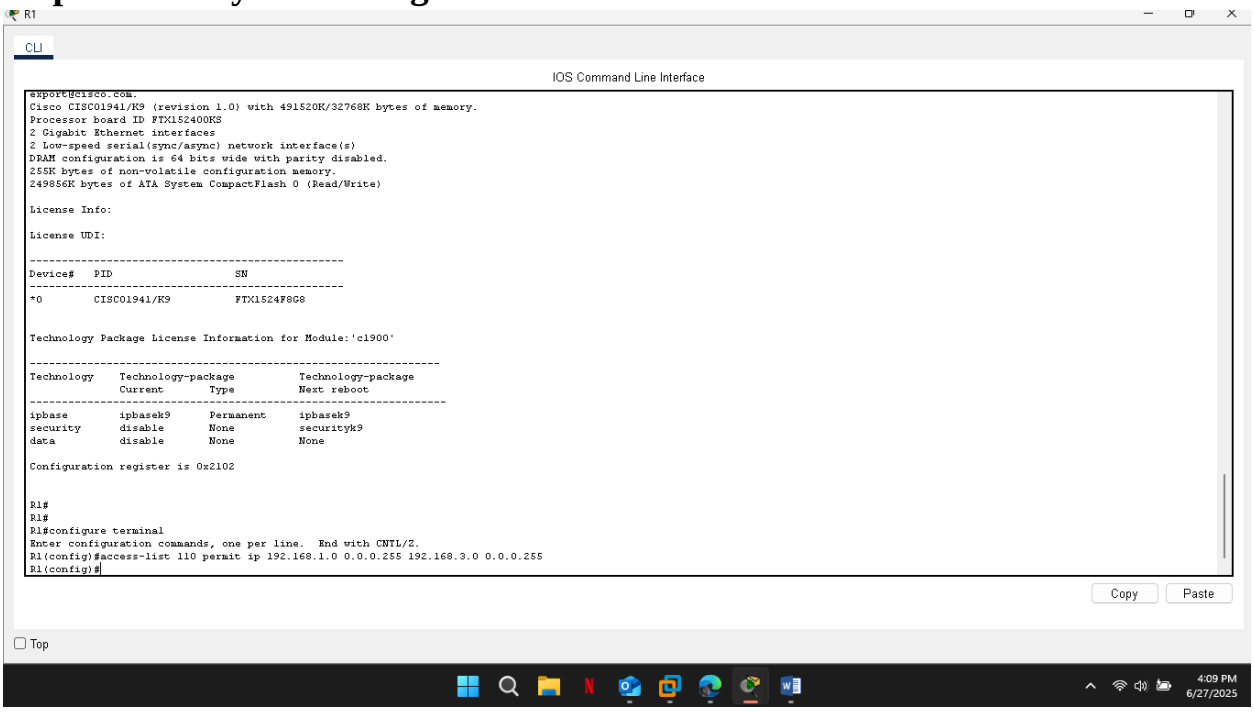


Accept the end-user license agreement.

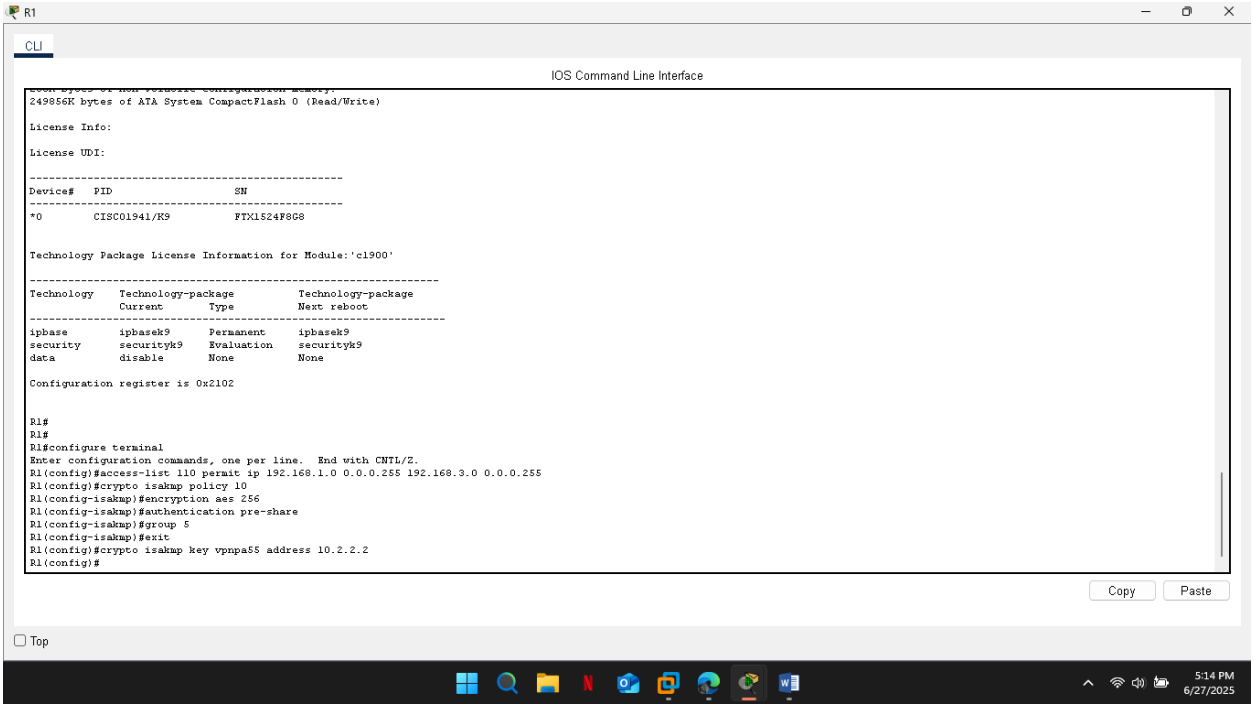


Verified that the Security Technology package has been enabled by using the show version command

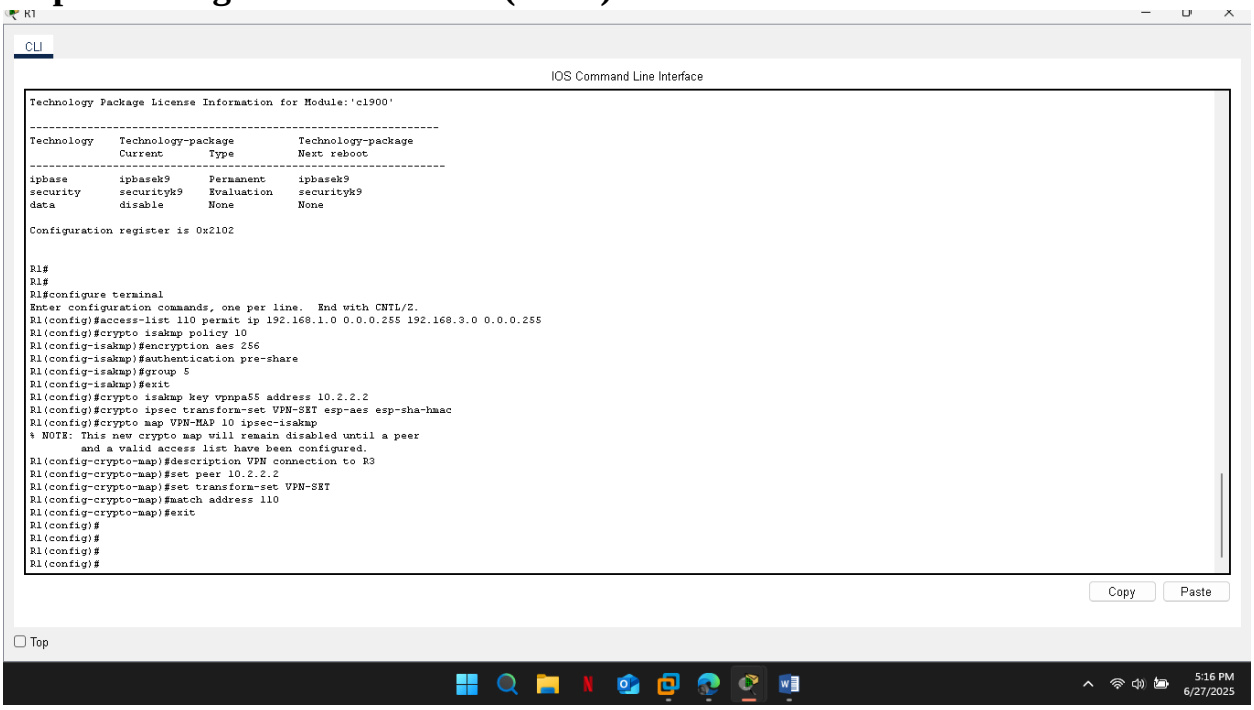
Step 3: Identify interesting traffic on R1.



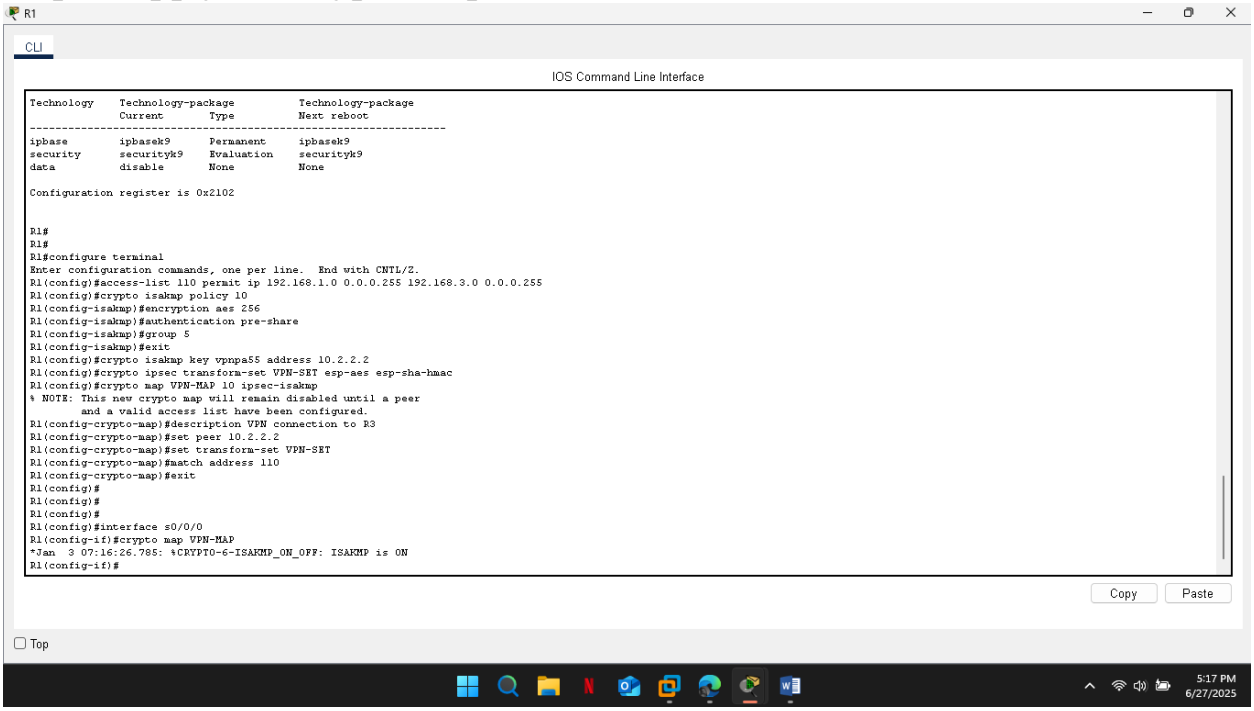
Step 4: Configure IKE Phase 1 (ISAKMP) on R1



Step 5: Configure IKE Phase 2 (IPsec) on R1



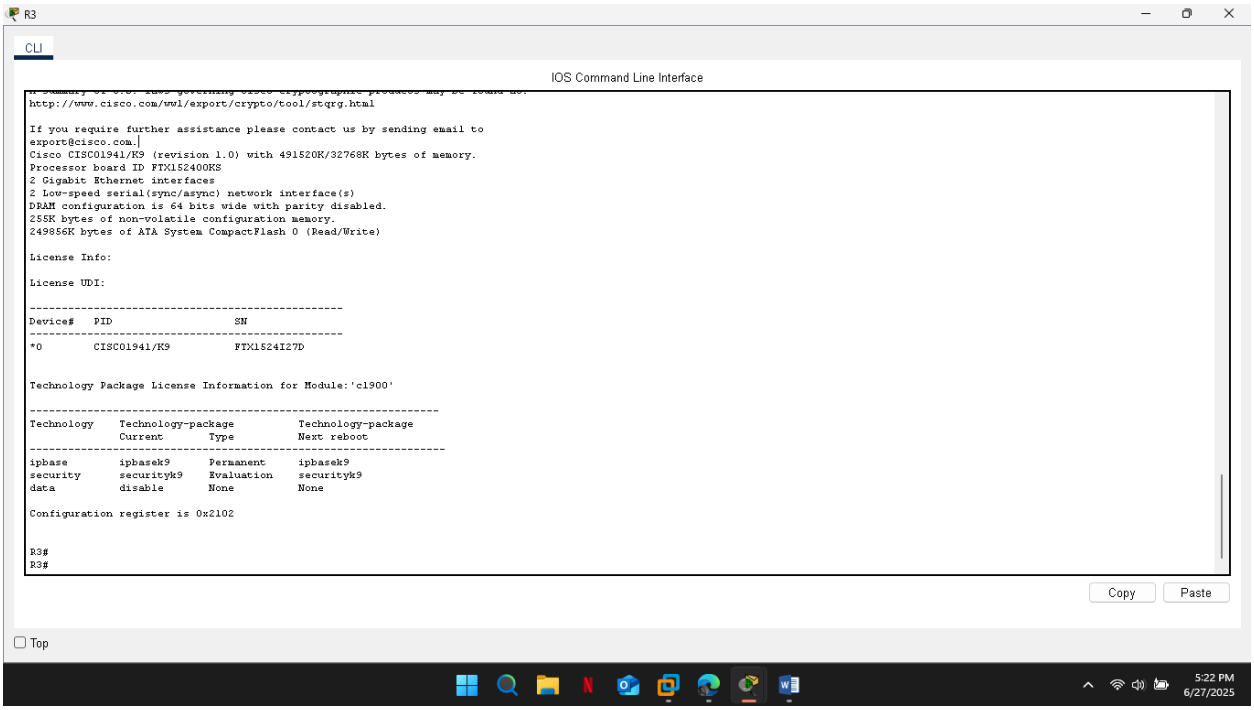
Step 6: Apply the Crypto Map to the Interface



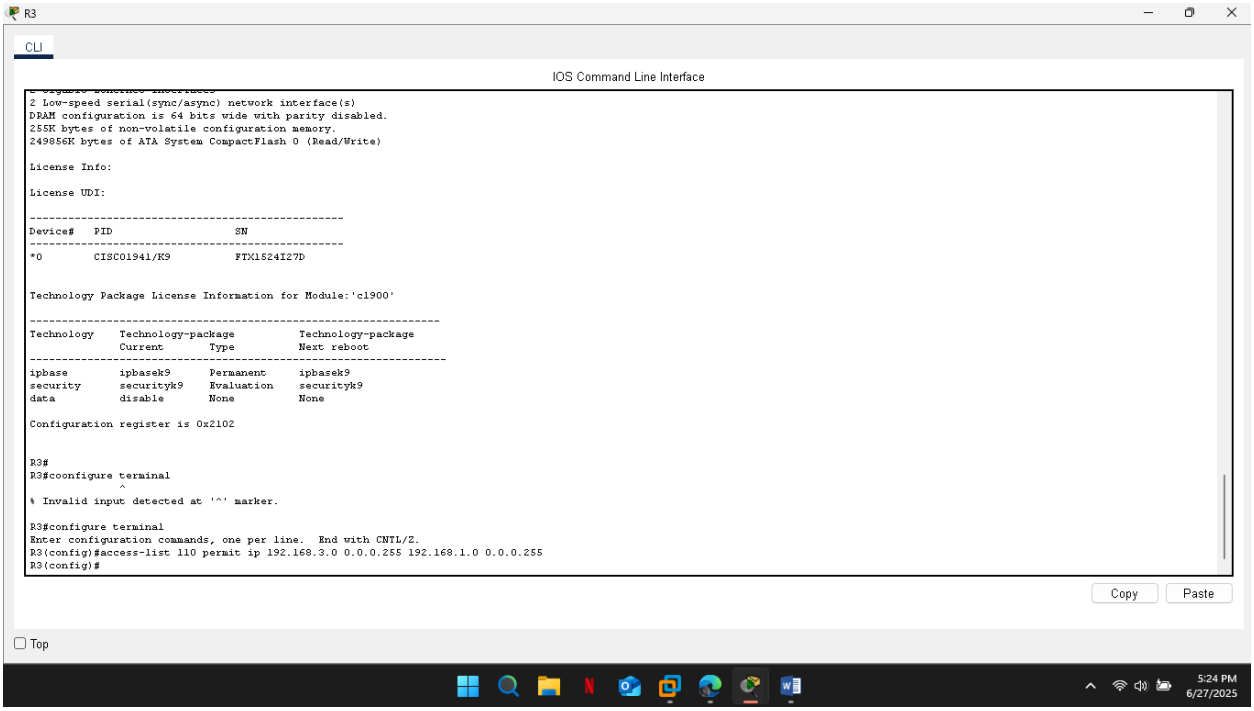
Part 2: Configure IPsec on R3

Step 1: Enable the Security Technology package.

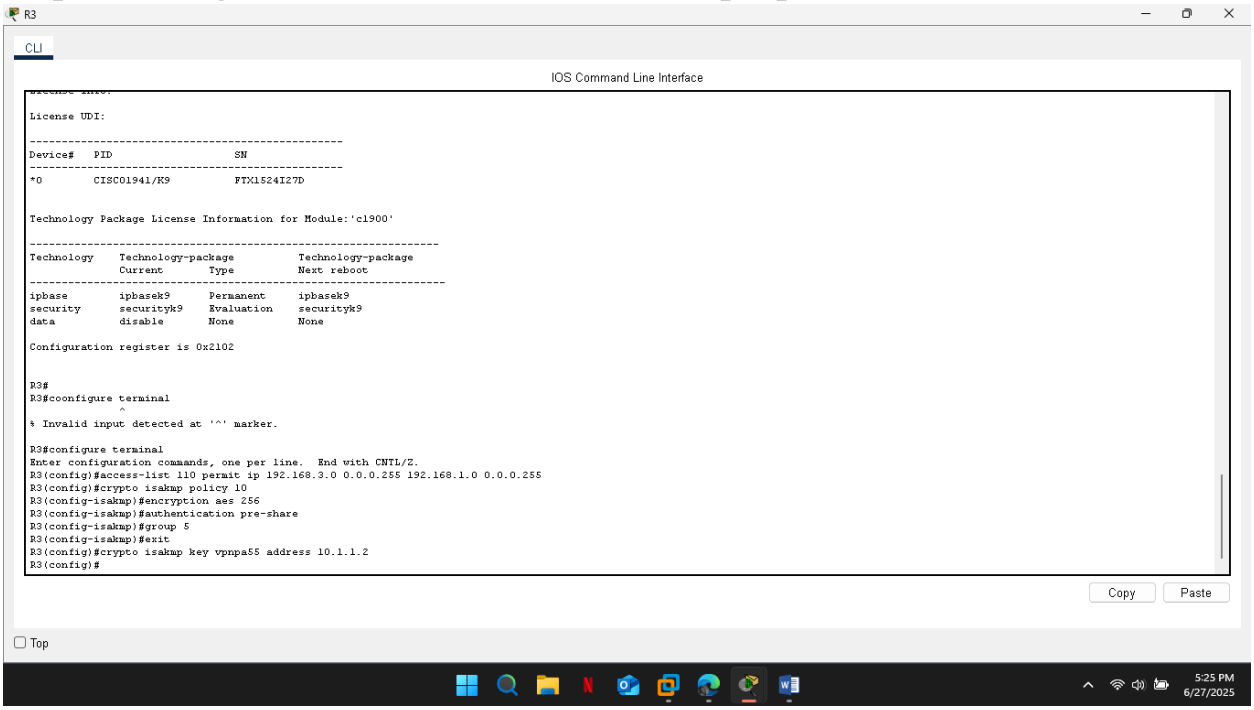
it's enabled and fully operational for your site-to-site IPsec VPN



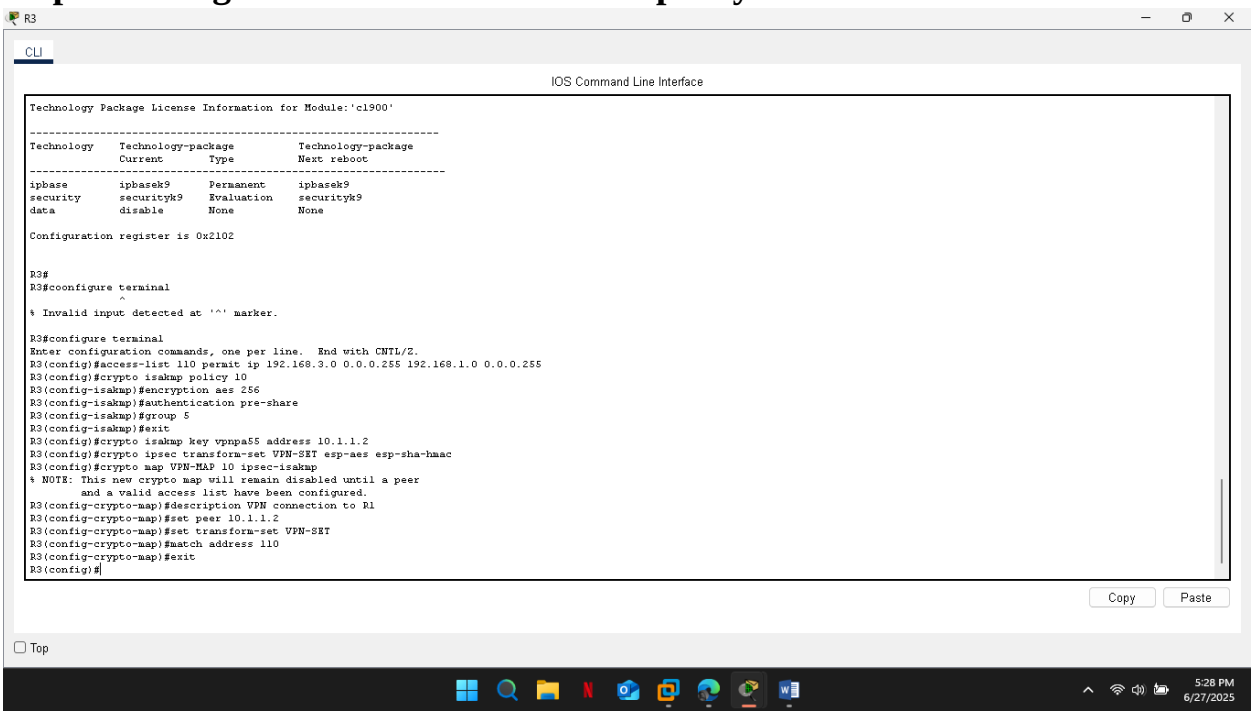
Step 2: Configure router R3 to support a site-to-site VPN with R1.



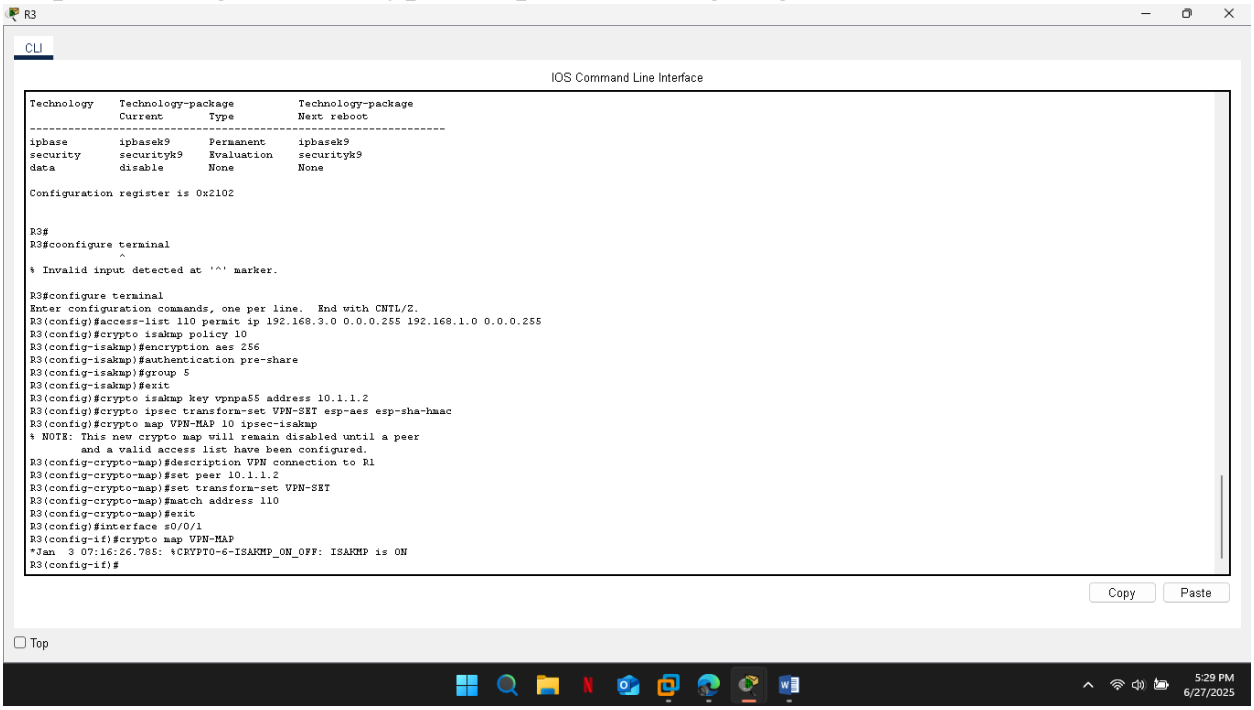
Step 3: Configure the IKE Phase 1 ISAKMP properties on R3.



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

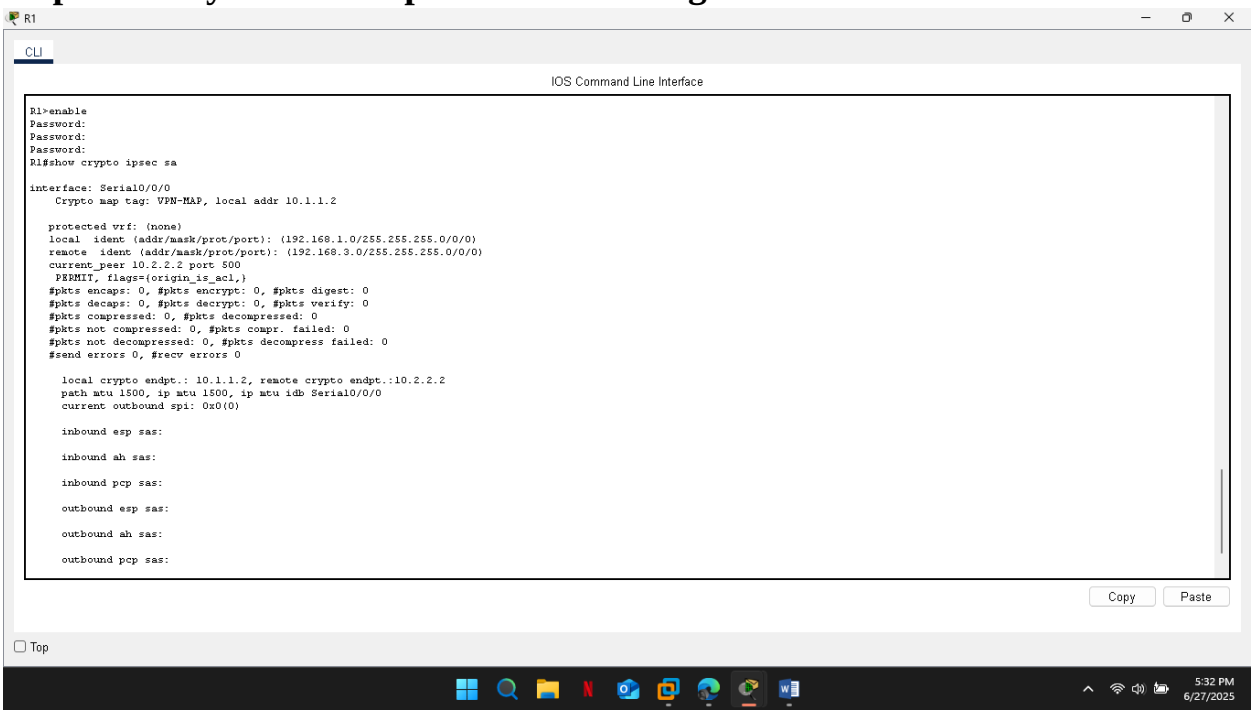


Step 5: Configure the crypto map on the outgoing interface.

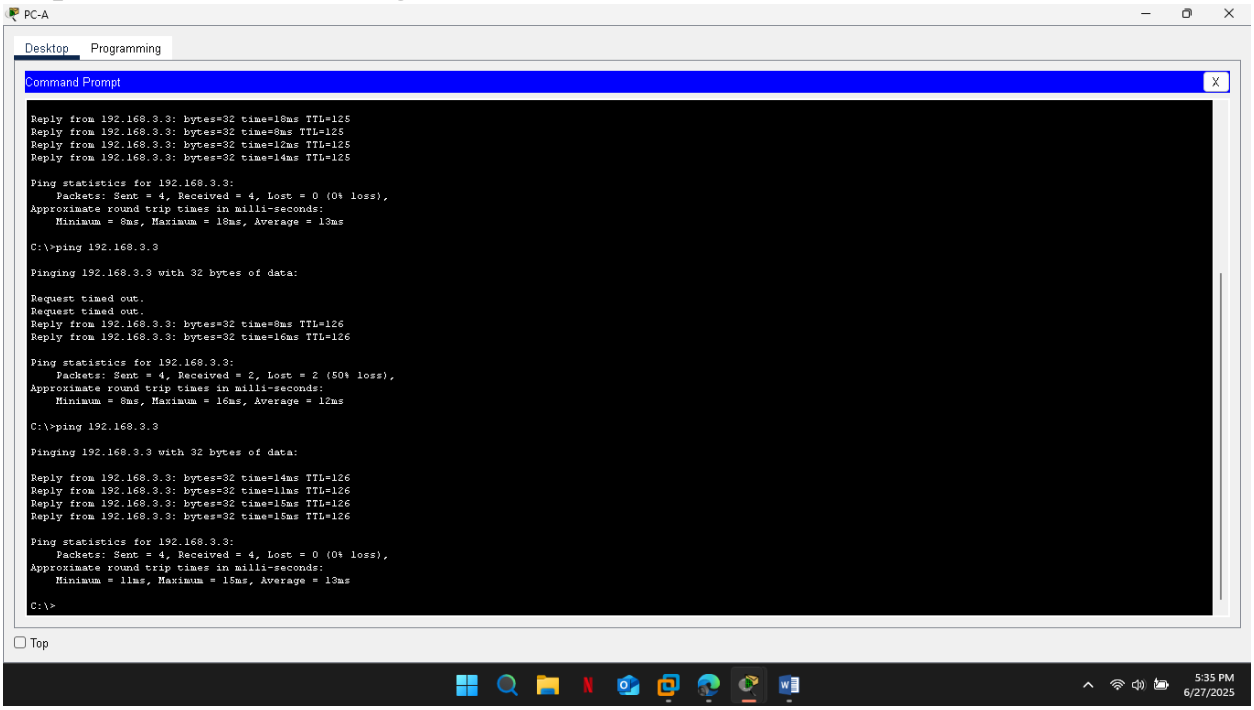


Part 3: Verify the IPsec VPN

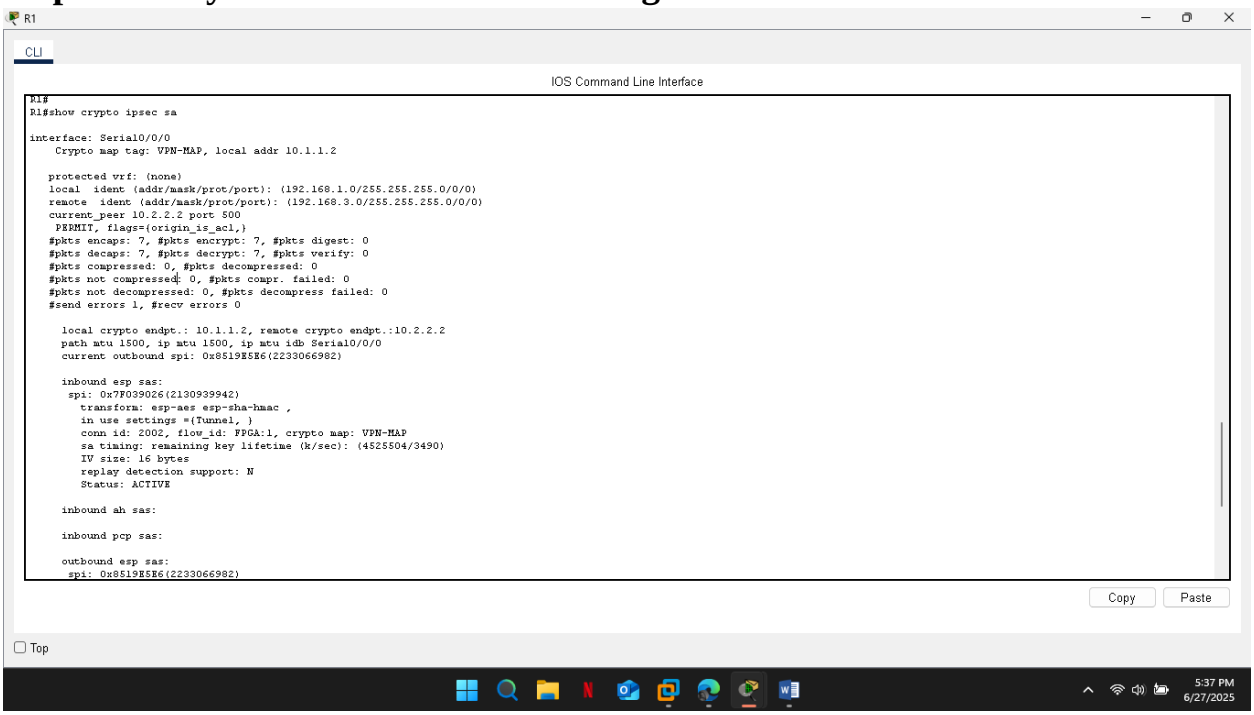
Step 1: Verify the tunnel prior to interesting traffic.



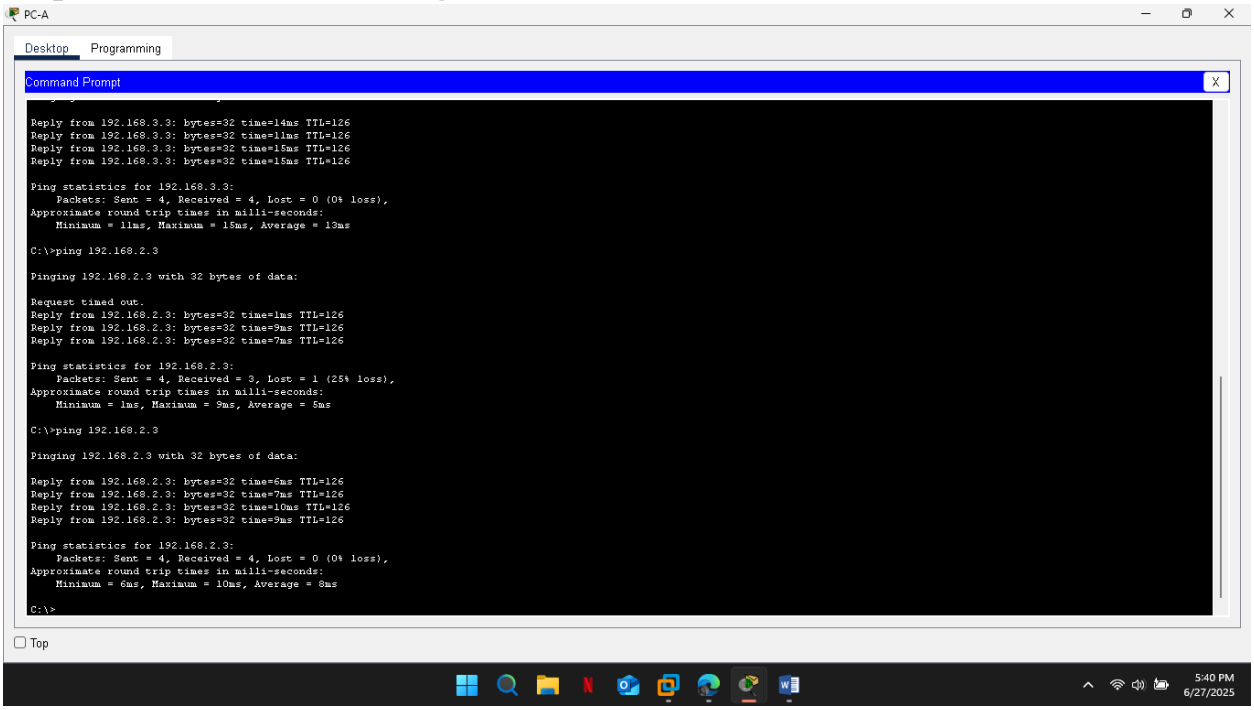
Step 2: Create interesting traffic.



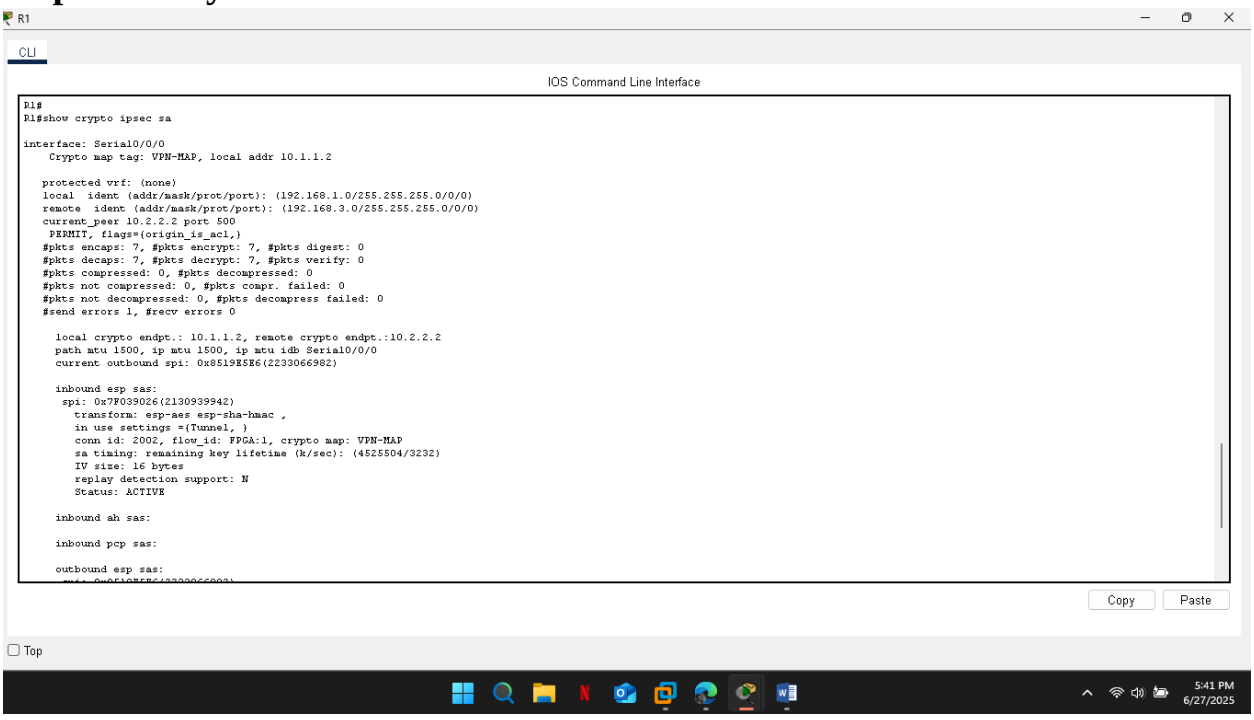
Step 3: Verify the tunnel after interesting traffic.



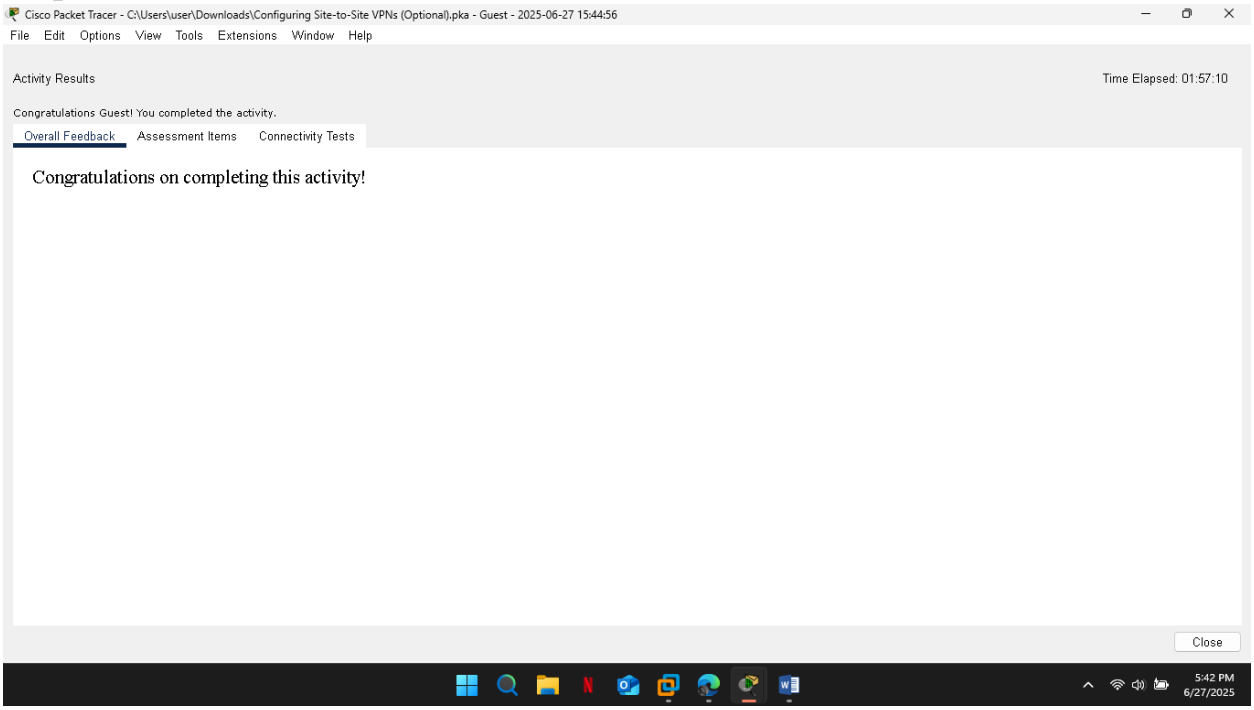
Step 4: Create uninteresting traffic.



Step 5: Verify the tunnel.



Step 6: Check results.



CONCLUSION

Upon completion of this activity, the IPsec VPN tunnel between R1 and R3 was successfully established and verified. Encrypted communication was confirmed by observing increased encapsulation and encryption counters following a successful ping from PC-A (192.168.1.3) to PC-C (192.168.3.3), which matched the defined interesting traffic. Uninteresting traffic, such as pings to PC-B, bypassed the VPN as expected.

This activity reinforced the foundational steps of creating a secure site-to-site VPN using Cisco IOS CLI, including license activation, access-list definition, ISAKMP and IPsec configuration, and crypto map application. By simulating a secure inter-branch communication scenario, it highlighted the importance of IPsec in protecting sensitive data over insecure networks and deepened understanding of VPN tunnel negotiation and maintenance in a routed network environment.