CONFIGURING VPN REPORT

PACKET TRACER LAB

BY

YUNIS MOHAMED

Contents

Introduction

This packet tracer lab involves configuring a site to site ipsec VPN to help enhance security in the network. To set it up one has to configure routers in the network to create a VPN tunnel, generate a shared key that will be used to authenticate the routers and encrypt the traffic flowing through the tunnels. Protocols such as Internet Security Association and Key Management Protocol (ISAKMP) was used to establish secure communication channels and manage cryptographic keys in the network.

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	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	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	R3
Key distribution method	Manual or **ISAKMP**	ISAKMP	ISAKMP
Encryption algorithm	**DES**, 3DES, or AES	AES	AES
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		cisco	cisco

IPsec 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

Part 1: Enable Security Features

Activate securityk9 module.

To activate the securityk9 module for the next boot of the router, accept the license, save the configuration, and reboot. Use of the following command: **license boot module c2900 technology-package securityk9.**

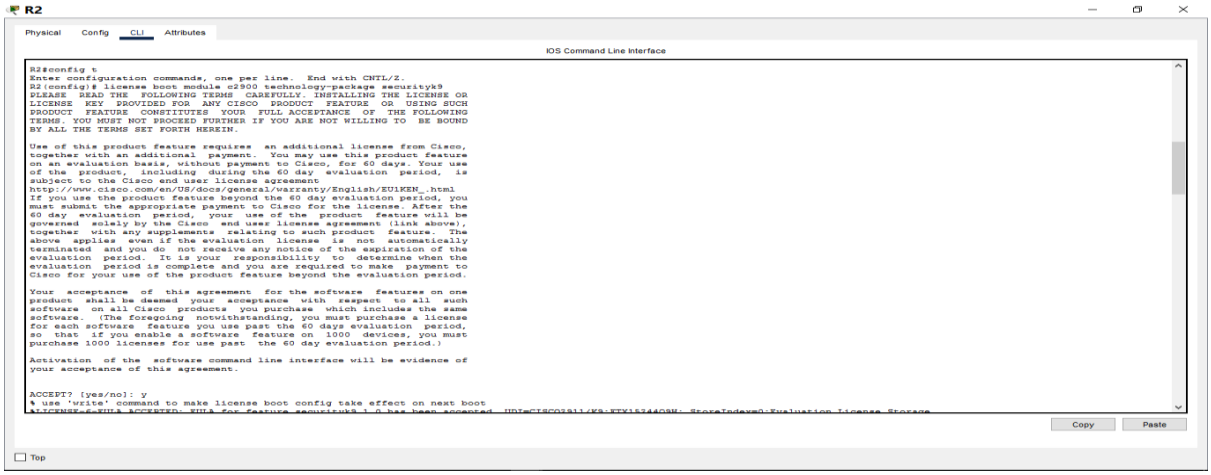


Figure 1 R2 security activation

Verify activation package licence.

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

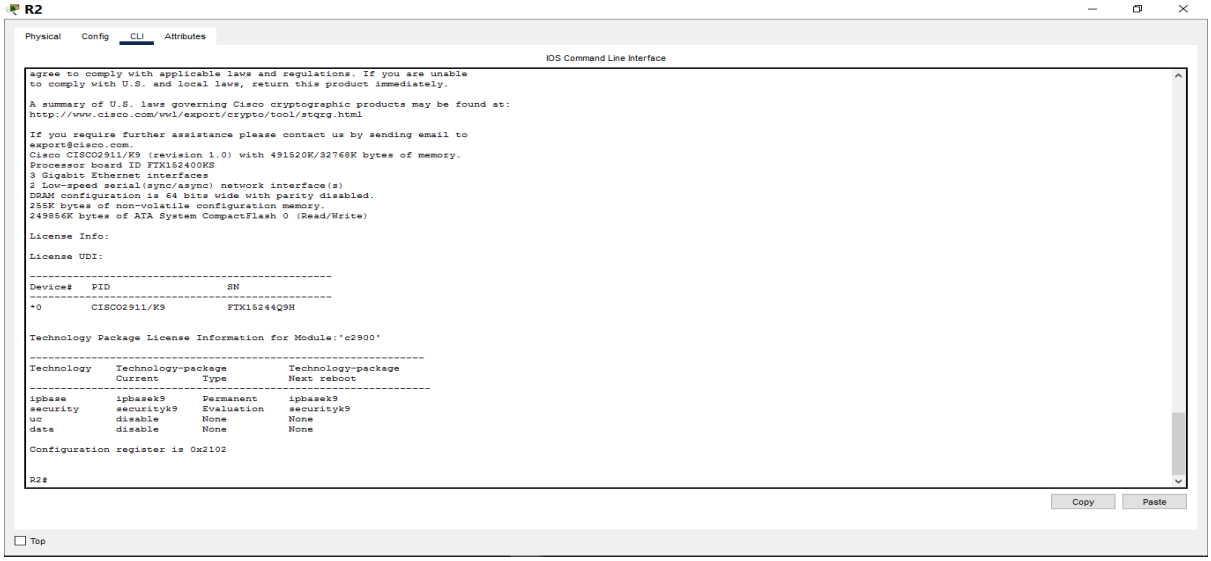


Figure 2verify activation

Part 2: Configure IPsec Parameters on R1

Test connectivity by performing a ping from PC-A to PC-C.

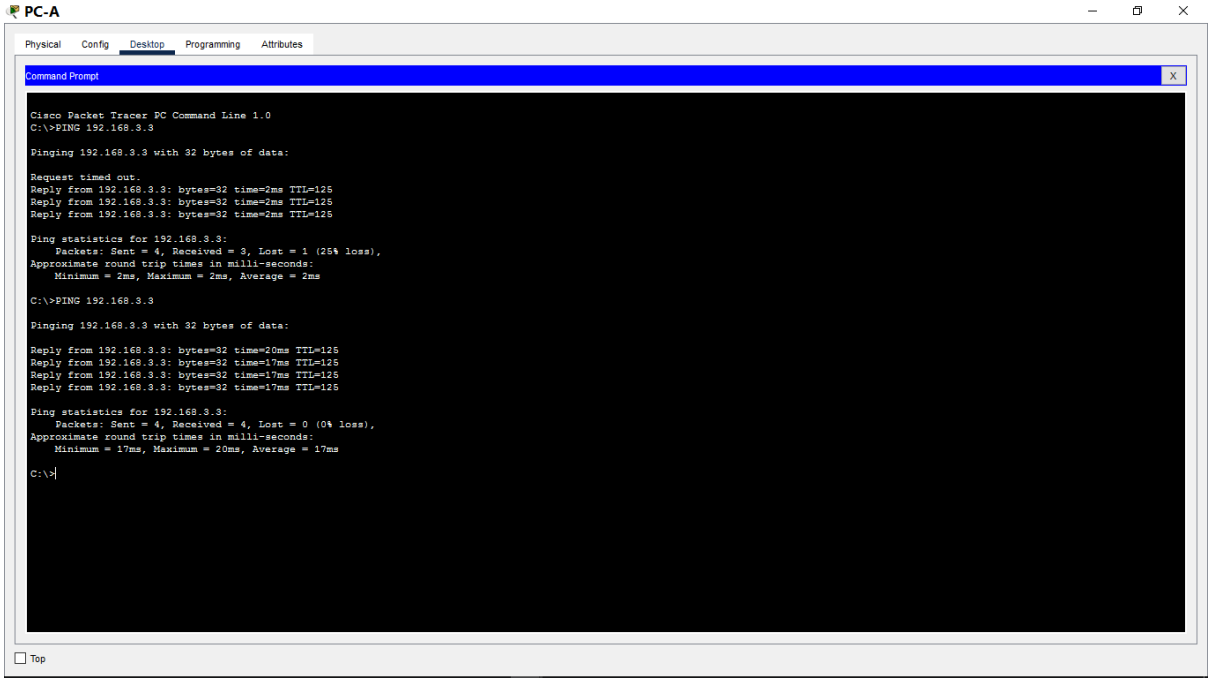


Figure 3ping PC-A to PC-C

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.

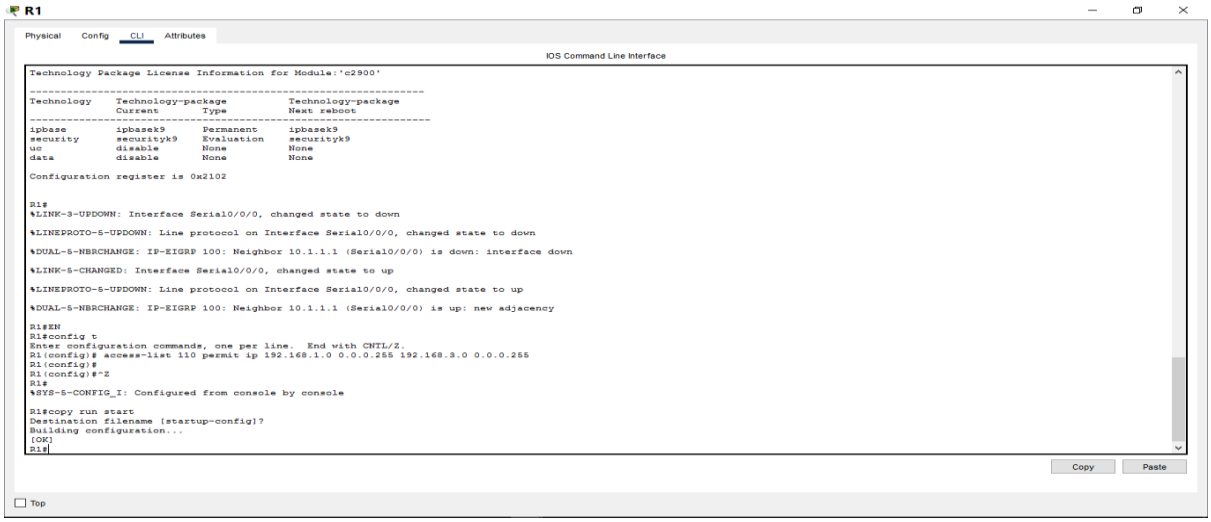


Figure 4 identify interesting traffic

Configure the ISAKMP Phase 1 properties on R1.

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.

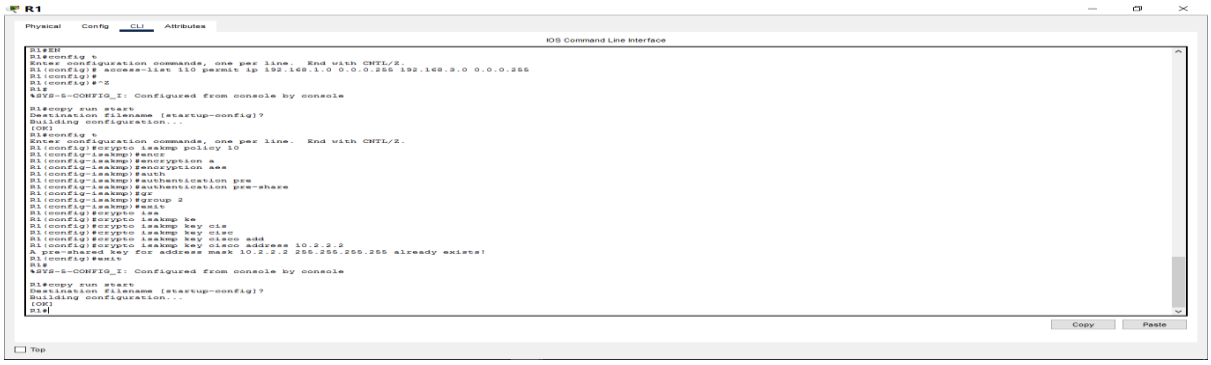


Figure 5 ISAKMP phase 1 on R1

Configure the ISAKMP Phase 2 properties on R1.

Create the transform-set VPN-SET to use esp-3des and esp-sha-hmac. Then create the crypto map VPNMAP that binds all of the Phase 2 parameters together. Use sequence number 10 and identify it as an ipsec-isakmp map.

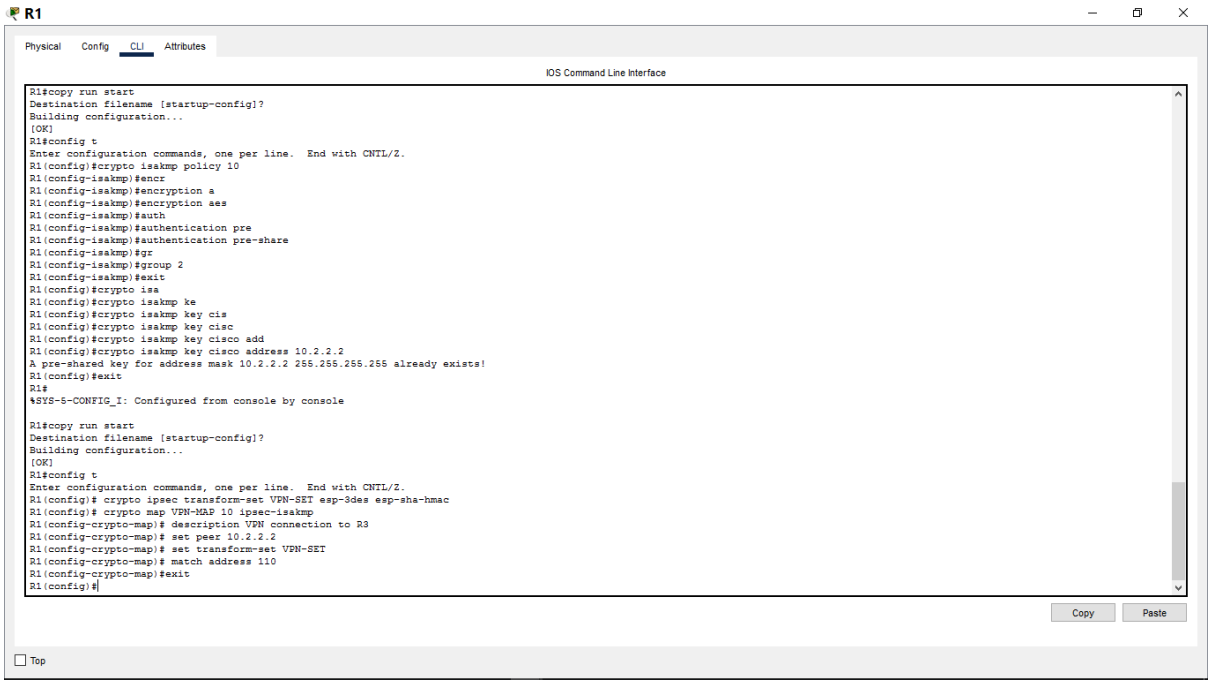


Figure 6 ISAKMP phase 2 R1

Configure the crypto map on the outgoing interface.

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

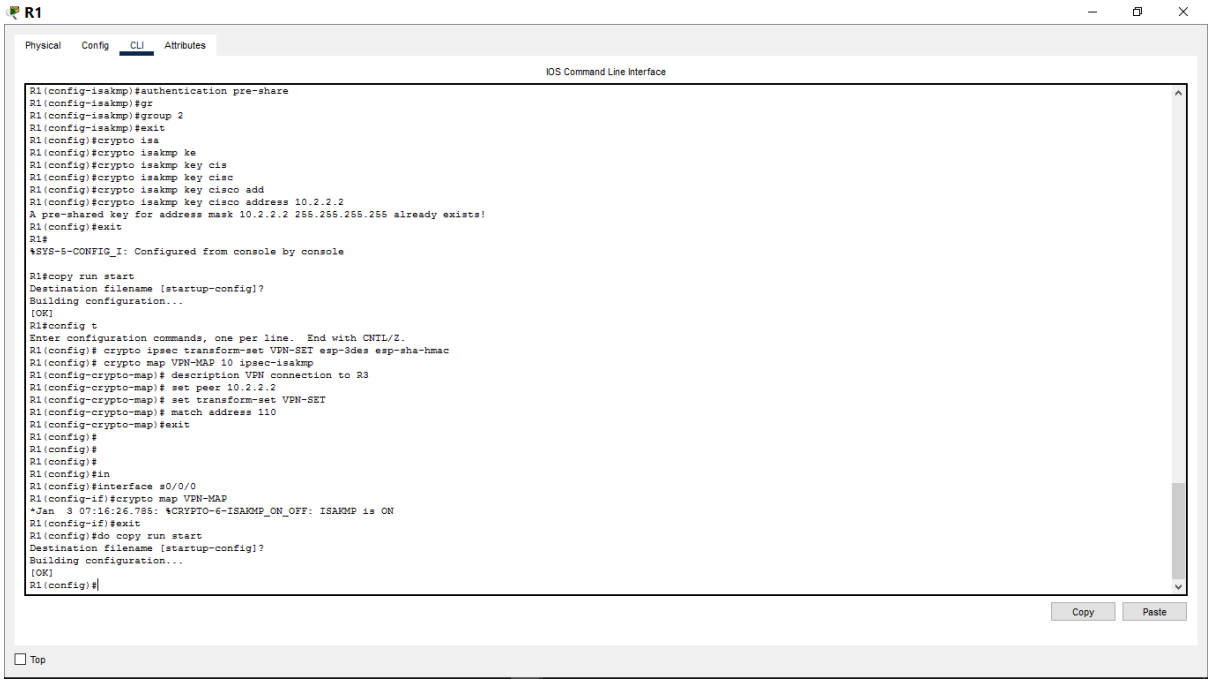


Figure 7crypto map R1

Part 3: Configure IPsec Parameters on R3

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

Figure 8 site to site vpn R3

Configure the ISAKMP Phase 1 properties on R3.

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

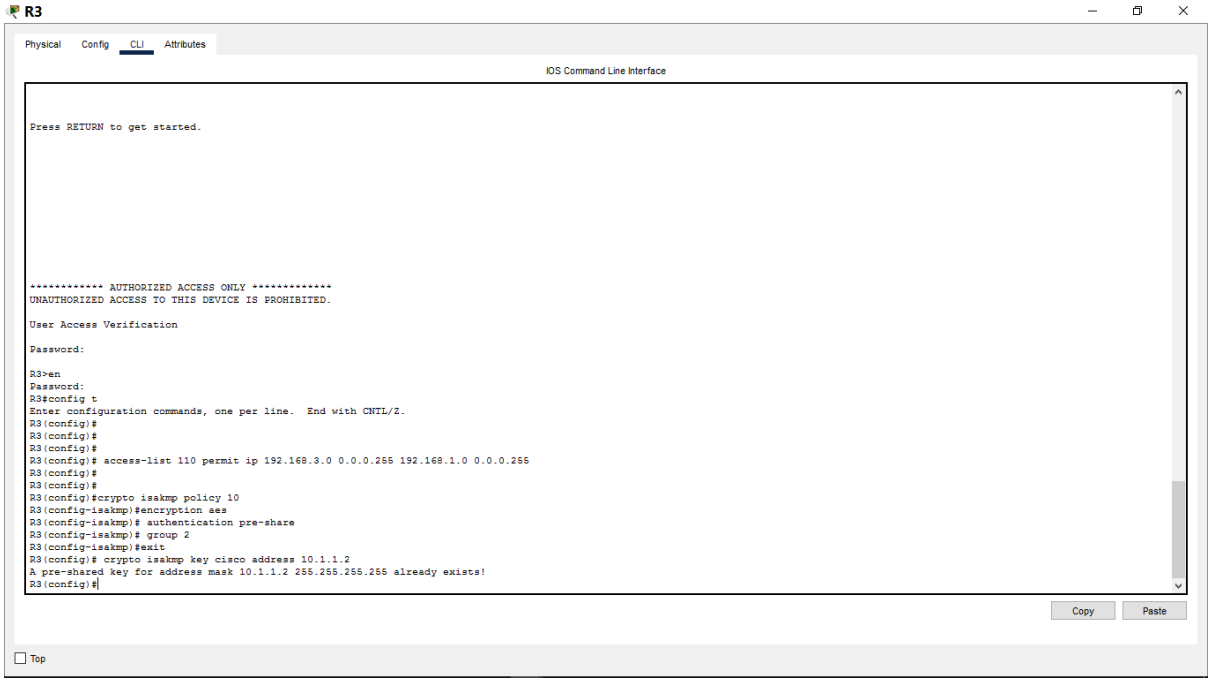


Figure 9 ISAKMP policy R3

Configure the ISAKMP Phase 2 properties 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.

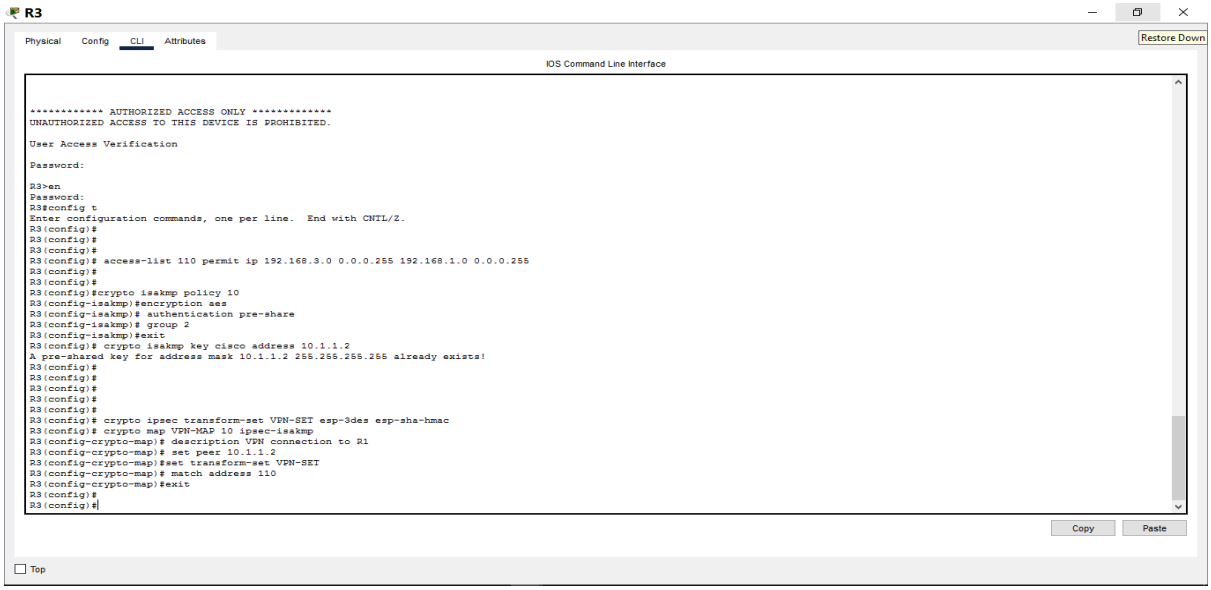


Figure 10 ISAKMP phase R3

Configure the crypto map on the outgoing interface.

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

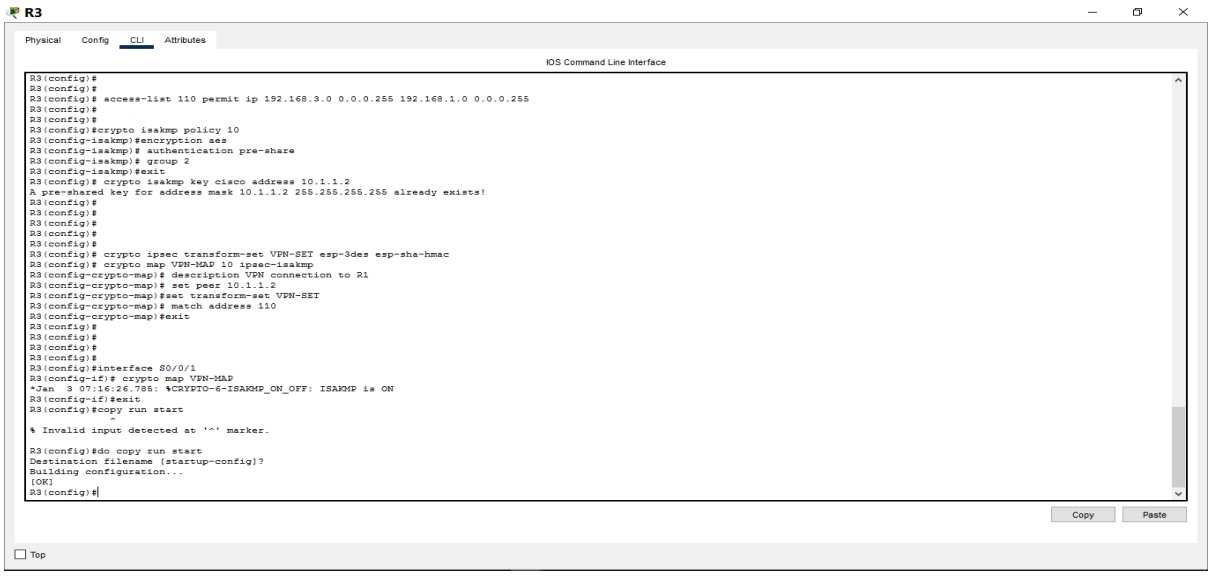


Figure 11 crypto map R3

Part 4: Verify the IPsec VPN

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.

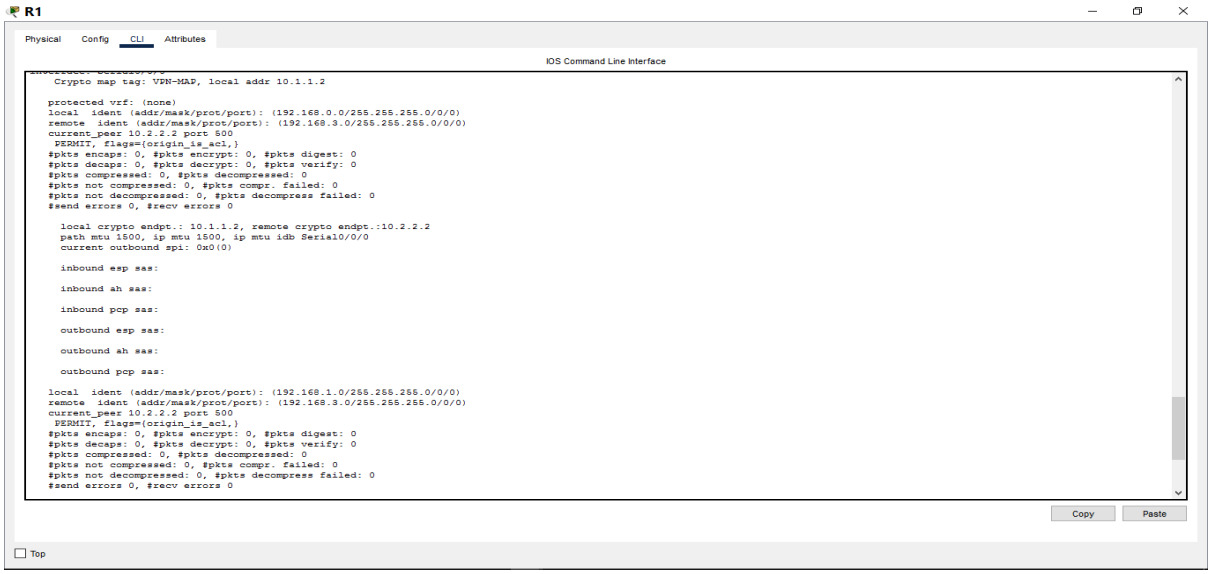


Figure 12 verify tunnel prior to traffic

Create interesting traffic.

Ping PC-C from PC-A.

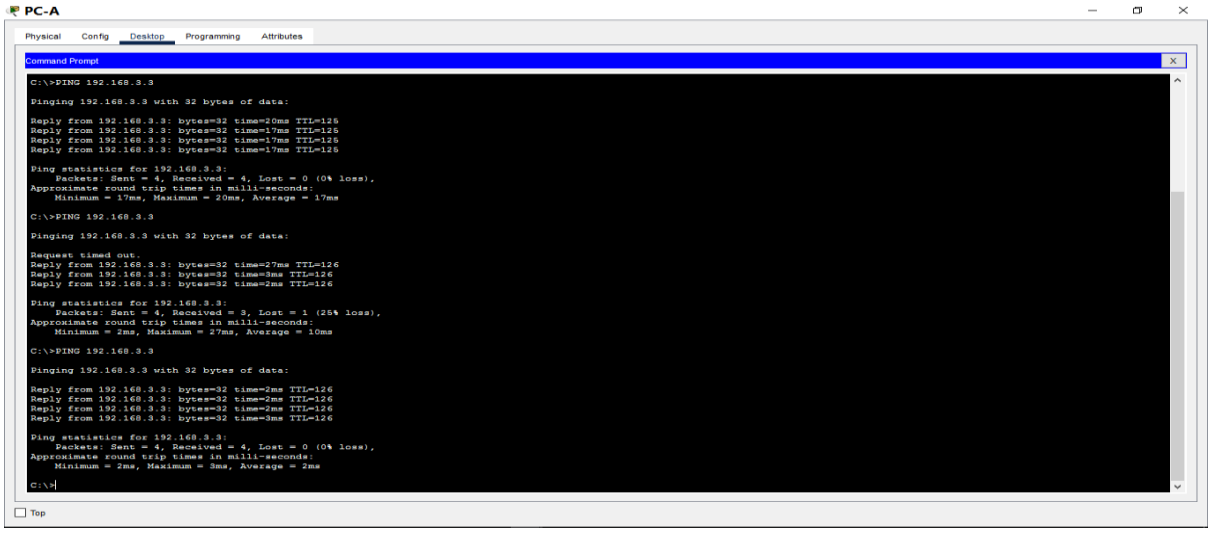
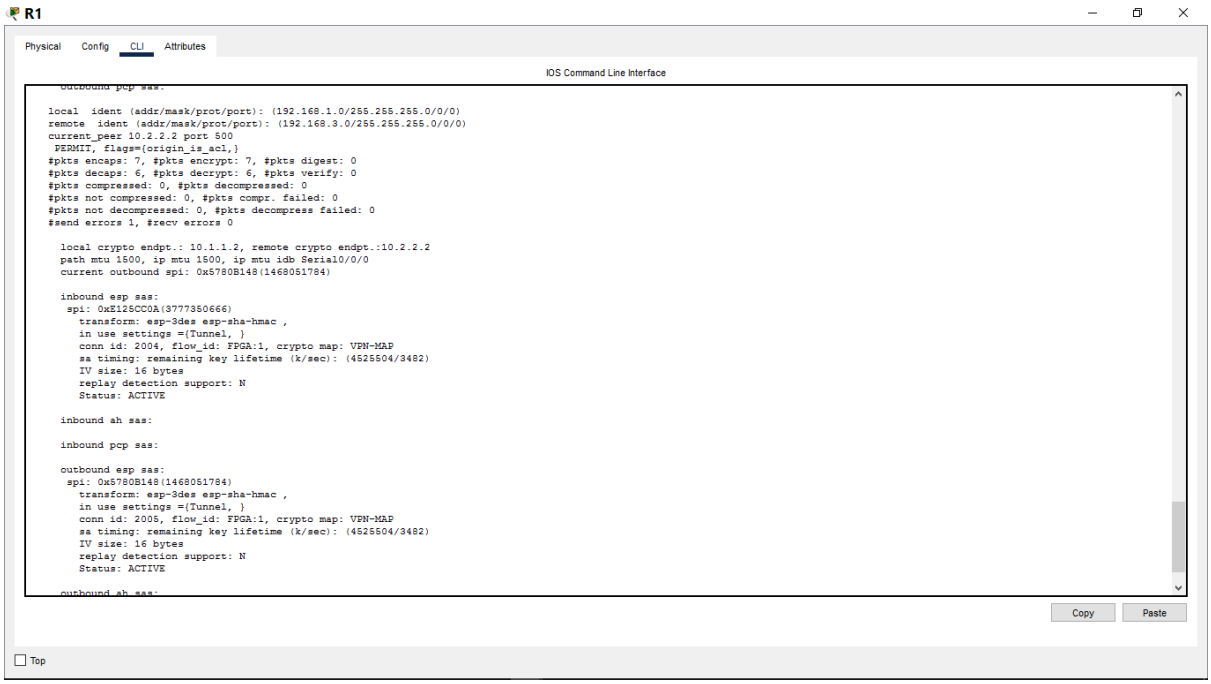


Figure 13 ping PC-C from PC-A

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 indicating that the IPsec VPN tunnel is working.



Create uninteresting traffic.

Ping PC-B from PC-A.

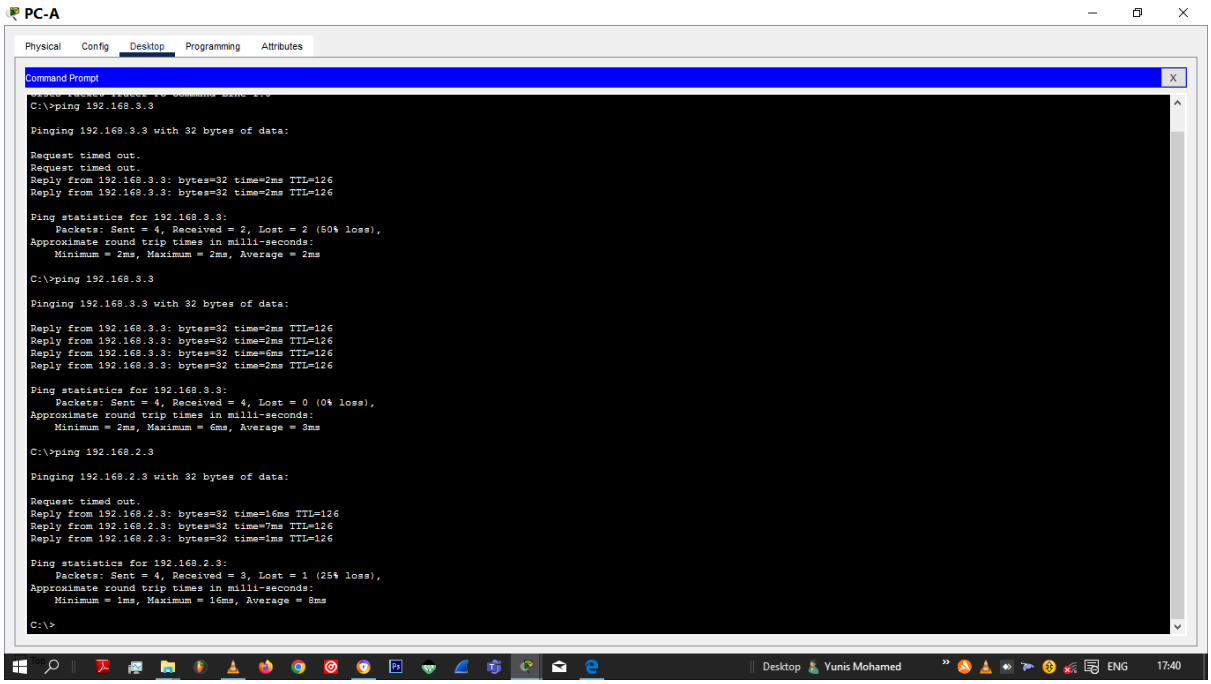
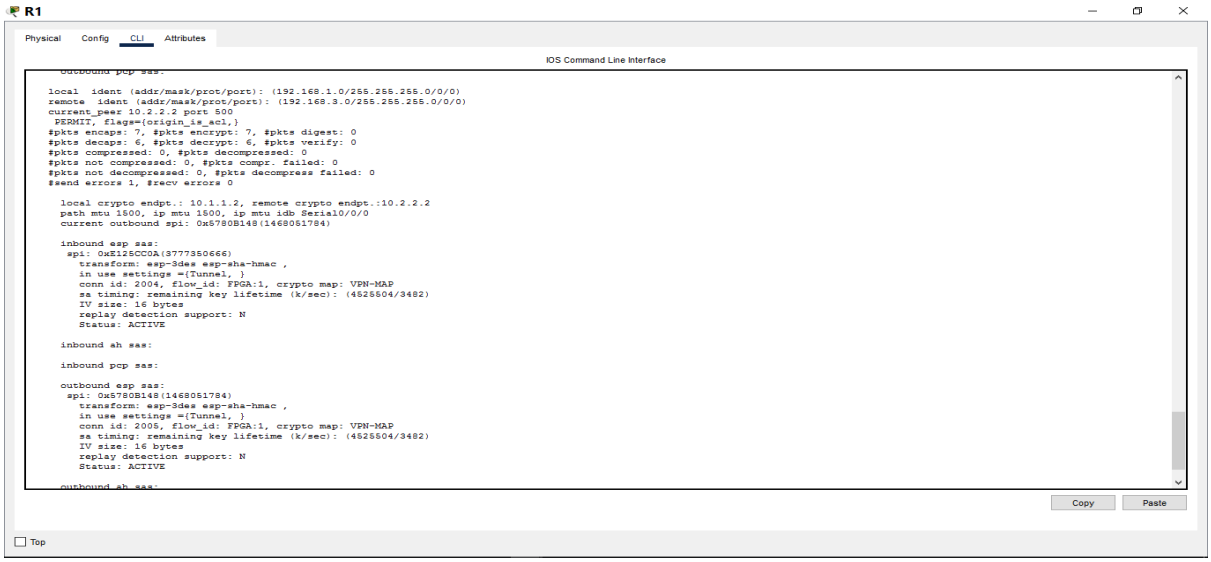


Figure 14 uninteresting traffic

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.



Conclusion

In conclusion, Site-to-site IPsec VPN is a secure connection between two or more remote sites over the Internet. It uses IPsec protocols to encrypt and authenticate data, ensuring the confidentiality, integrity, and authenticity of traffic between the connected sites. This type of VPN is commonly used by organizations to securely connect geographically dispersed sites or branch offices. Through the ISAKMP protocol, data is encrypted and authenticated making it difficult for unauthorized parties to access or intercept. I was able to gain and apply hands-on skills in configuring and implementing site to site Ipsec VPN. The configuration syntax and commands was overwhelming at first, but with more practice I will be able to be more comfortable and apply.