



CONFIGURING VPN REPORT

PACKET TRACER LAB



BY
YUNIS MOHAMED

Contents

Introduction	2
Part 1: Enable Security Features	2
Activate securityk9 module	3
Verify activation package licence.	4
Part 2: Configure IPsec Parameters on R1	4
Test connectivity by performing a ping from PC-A to PC-C.	4
Identify interesting traffic on R1.....	5
Configure the ISAKMP Phase 1 properties on R1.	5
Configure the ISAKMP Phase 2 properties on R1.	5
Configure the crypto map on the outgoing interface.	6
Part 3: Configure IPsec Parameters on R3	7
Configure ACL 110 identifying the traffic from the LAN on R3 to the LAN on R1 as interesting. R3.	7
Configure the ISAKMP Phase 1 properties on R3.	7
Configure the ISAKMP Phase 2 properties on R1.	8
Configure the crypto map on the outgoing interface.	8
Part 4: Verify the IPsec VPN.....	9
Verify the tunnel prior to interesting traffic.....	9
Create interesting traffic.	9
Verify the tunnel after interesting traffic.	10
Create uninteresting traffic.....	10
Verify the tunnel.	11
Conclusion	11

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**.

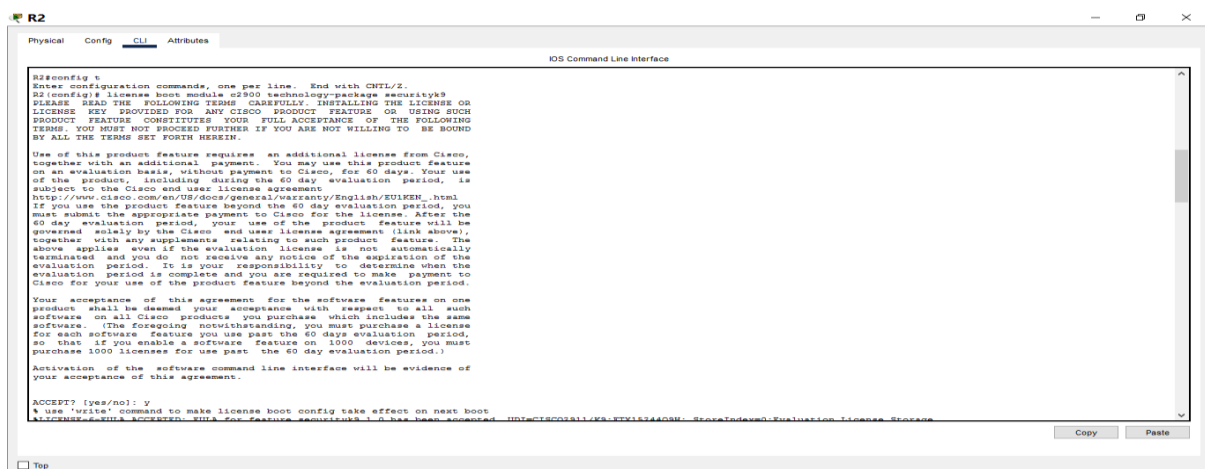


Figure 1 R2 security activation

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.

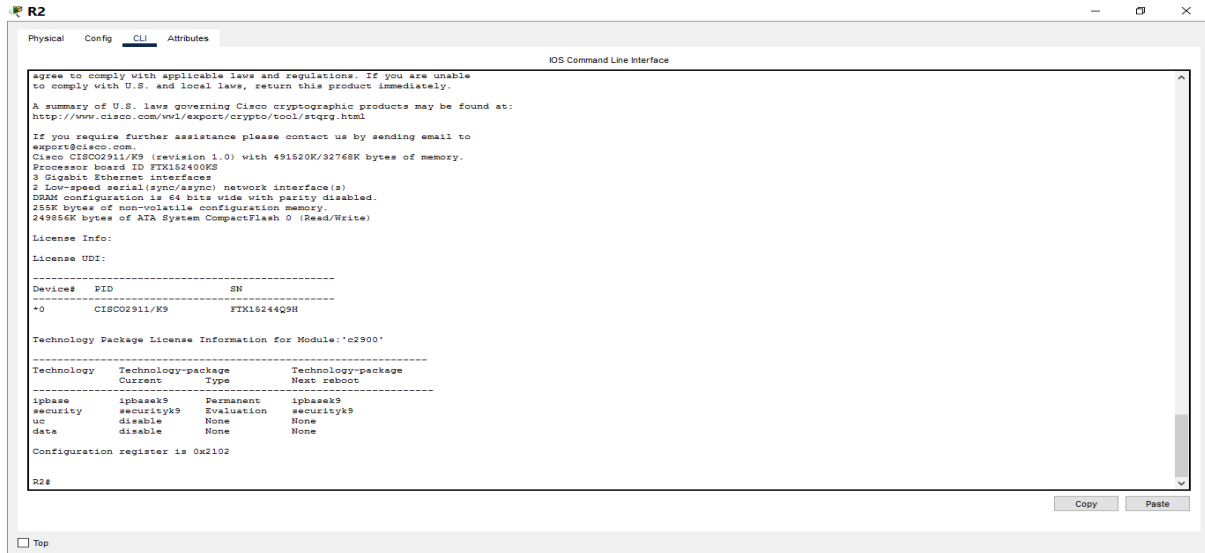


Figure 2verify activation

Part 2: Configure IPsec Parameters on R1

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

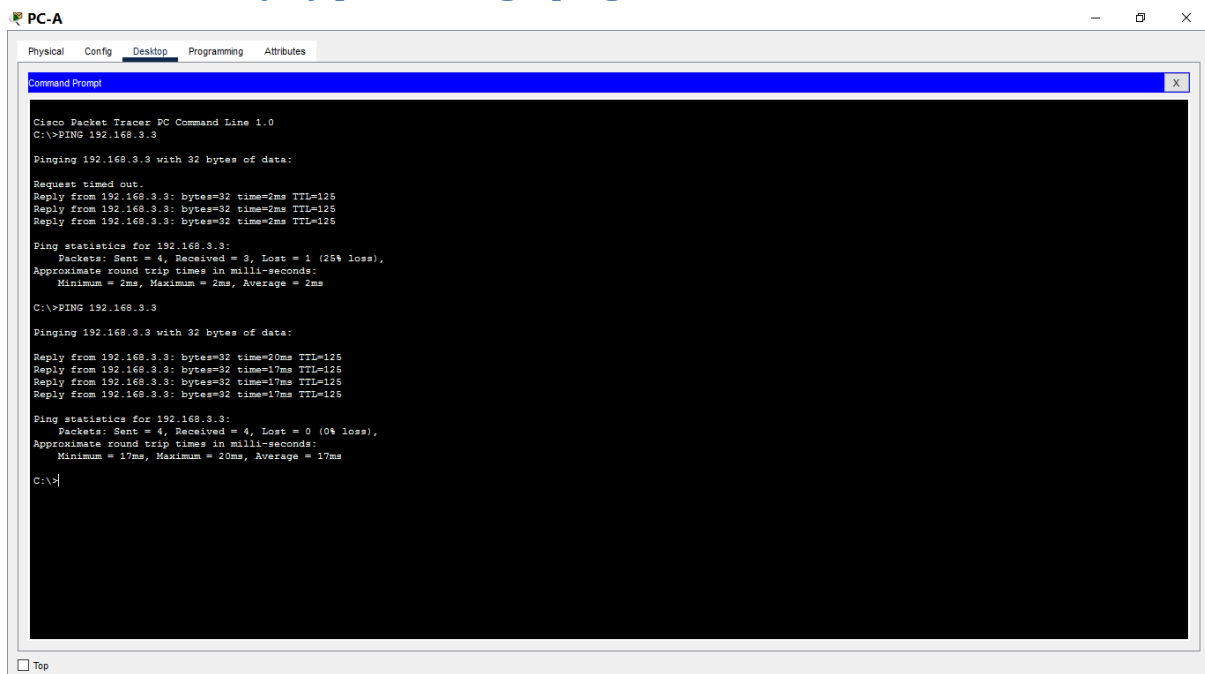


Figure 3ping PC-A to PC-C

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.

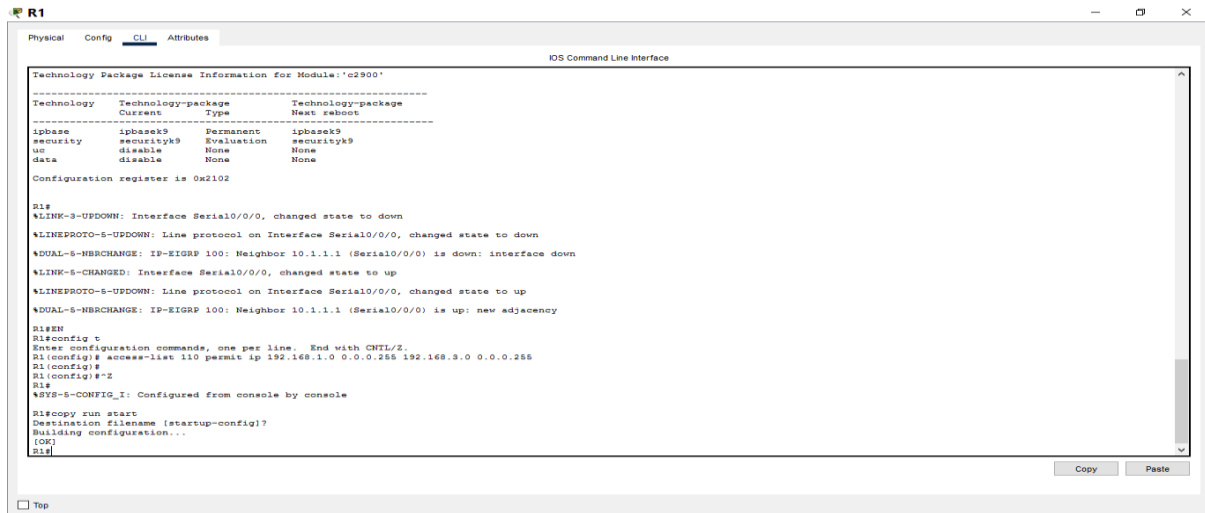


Figure 4 identify interesting traffic

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.

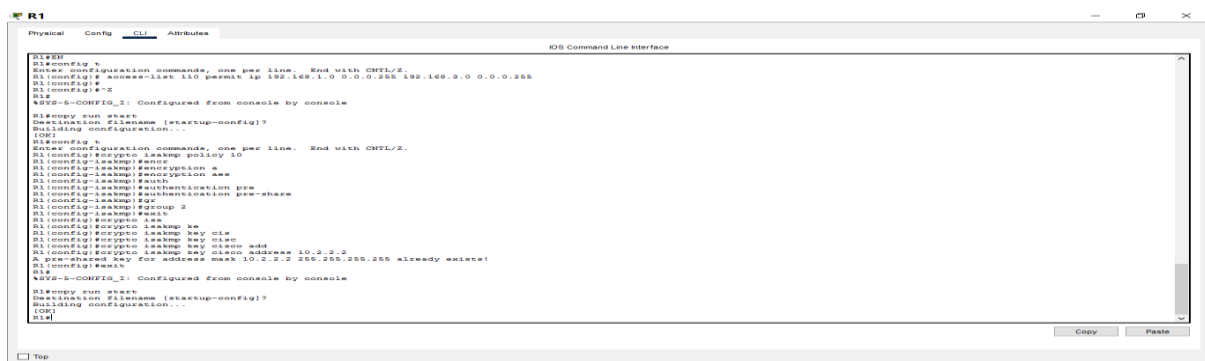
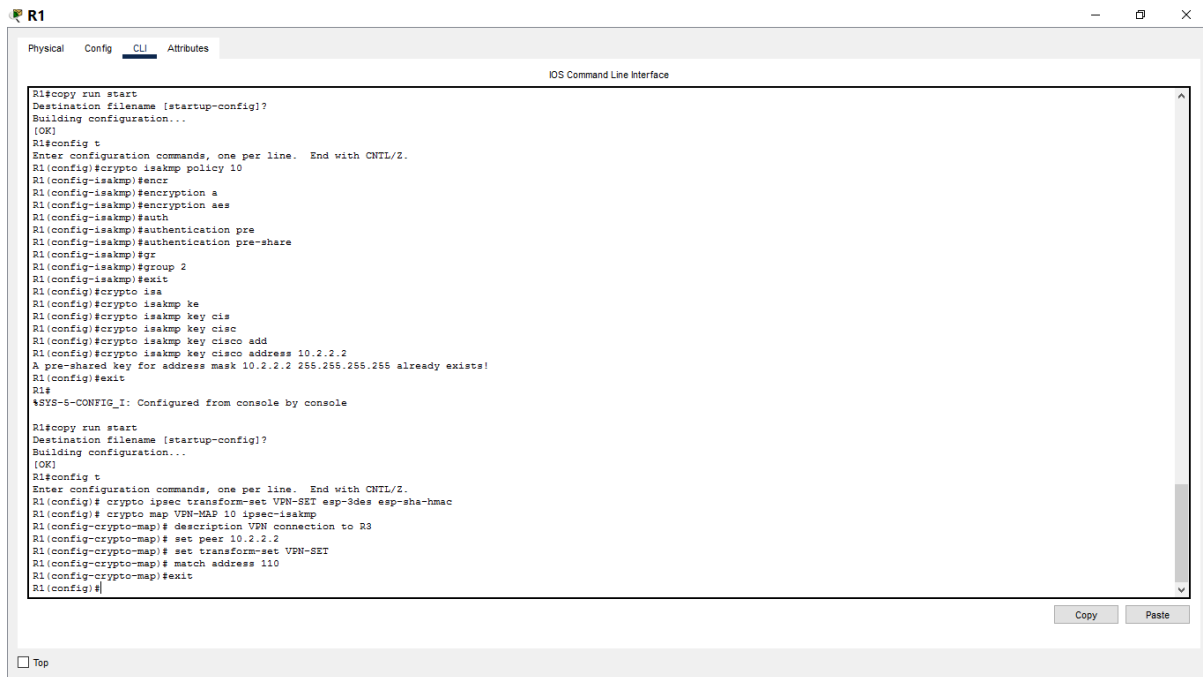


Figure 5 ISAKMP phase 1 on R1

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.



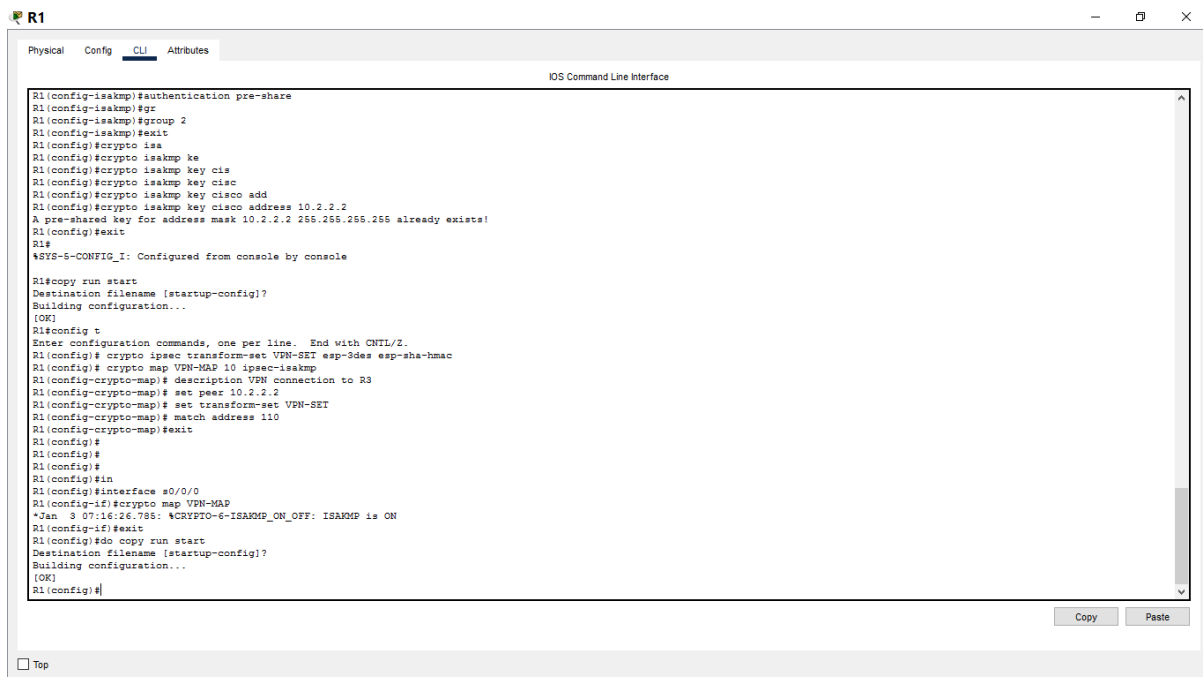
```
R1#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#encr
R1(config-isakmp)#encryption a
R1(config-isakmp)#encryption aes
R1(config-isakmp)#auth
R1(config-isakmp)#authentication pre
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#gr
R1(config-isakmp)#group 2
R1(config-isakmp)#exit
R1(config)#crypto isa
R1(config)#crypto isakmp ke
R1(config)#crypto isakmp key cis
R1(config)#crypto isakmp key cisc
R1(config)#crypto isakmp key cisco add
R1(config)#crypto isakmp key cisco address 10.2.2.2
A pre-shared key for address mask 10.2.2.2 255.255.255.255 already exists!
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
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
R1(config)#
```

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.



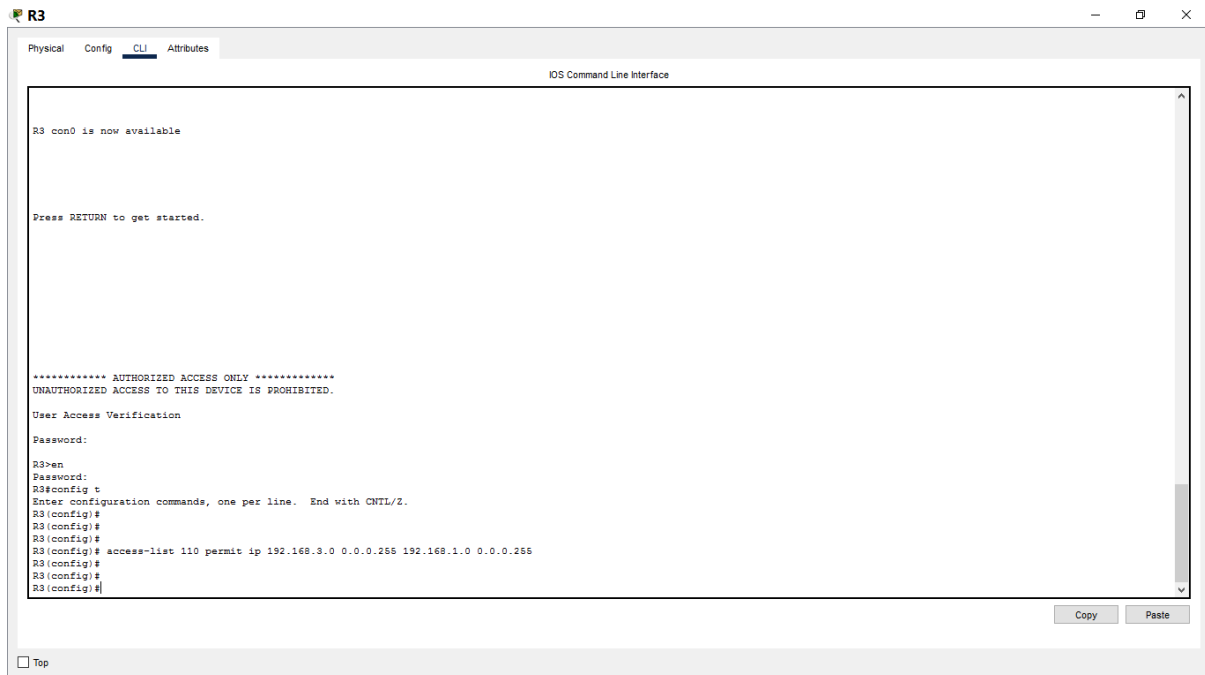
```
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#gr
R1(config-isakmp)#group 2
R1(config-isakmp)#exit
R1(config)#crypto isa
R1(config)#crypto isakmp ke
R1(config)#crypto isakmp key cis
R1(config)#crypto isakmp key cisc
R1(config)#crypto isakmp key cisco add
R1(config)#crypto isakmp key cisco address 10.2.2.2
A pre-shared key for address mask 10.2.2.2 255.255.255.255 already exists!
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
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
R1(config)#
R1(config)#
R1(config)#
R1(config)#in
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)#exit
R1(config)#do copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
R1(config)#
```

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.

A screenshot of the R3 router's CLI interface. The window title is 'R3' and the tab is 'CLI'. The interface shows the 'IOS Command Line Interface' with a scrollable text area. The text area contains the following commands and prompts:

```
R3 con0 is now available

Press RETURN to get started.

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

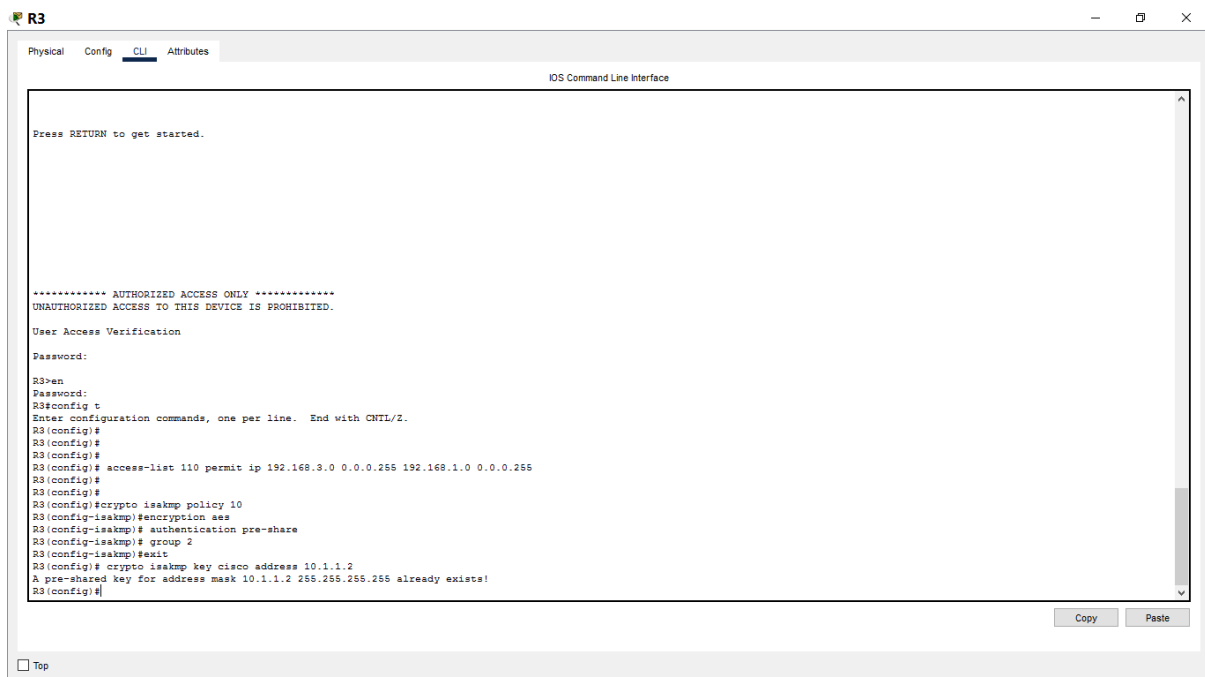
User Access Verification
Password:
R3>en
Password:
R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#
R3(config)#
R3(config)# access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
R3(config)#
R3(config)#
R3(config)#
```

At the bottom right of the text area are 'Copy' and 'Paste' buttons. At the bottom left is a 'Top' button.

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.

A screenshot of the R3 router's CLI interface, showing the continuation of the configuration. The window title is 'R3' and the tab is 'CLI'. The text area contains the following commands and prompts:

```
Press RETURN to get started.

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

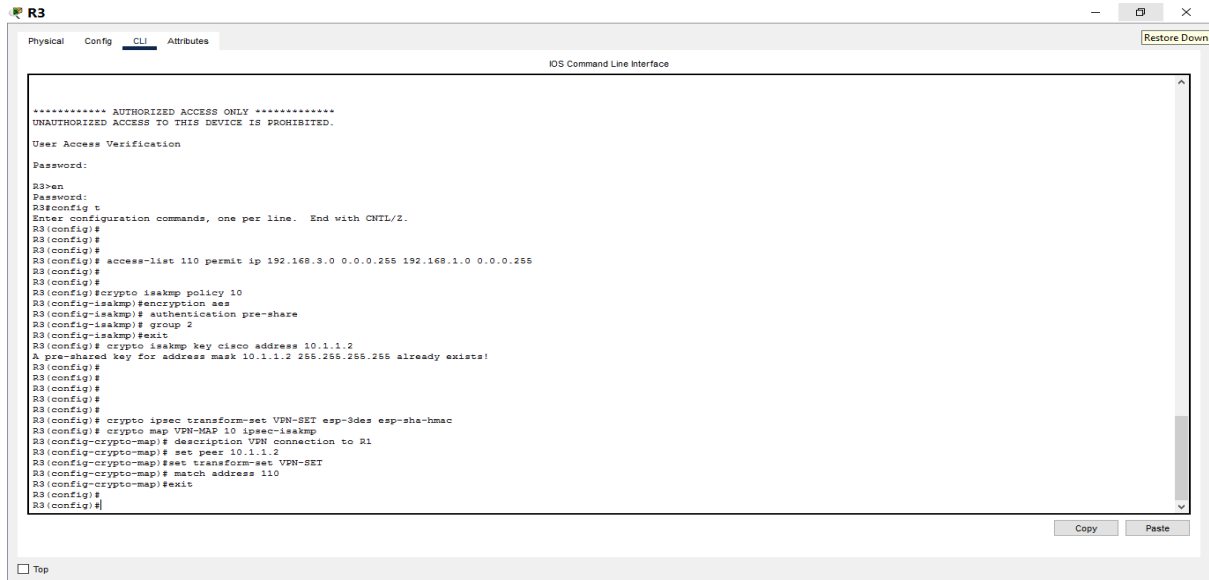
User Access Verification
Password:
R3>en
Password:
R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#
R3(config)#
R3(config)# access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
R3(config)#
R3(config)#
R3(config)# crypto isakmp policy 10
R3(config-isakmp)# 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
A pre-shared key for address mask 10.1.1.2 255.255.255.255 already exists!
R3(config)#
```

At the bottom right of the text area are 'Copy' and 'Paste' buttons. At the bottom left is a 'Top' button.

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.



```
R3
Physical Config CLI Attributes
IOS Command Line Interface

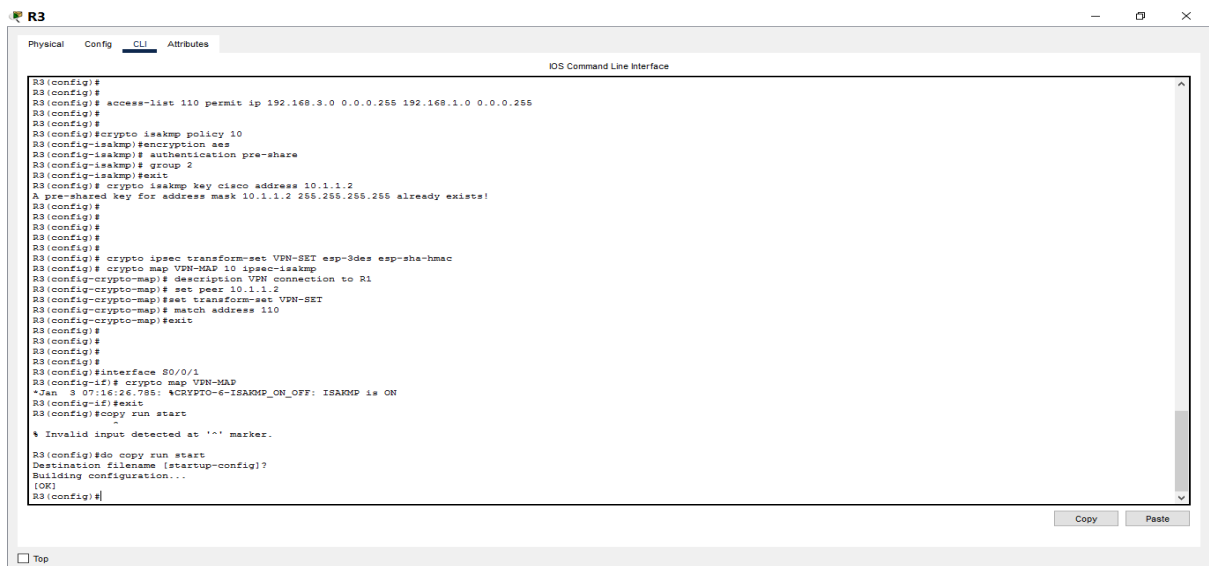
***** AUTHORIZED ACCESS ONLY *****
UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.

User Access Verification
Password:
R3>en
Password:
R3(config)#
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#
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)#
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
A pre-shared key for address mask 10.1.1.2 255.255.255.255 already exists!
R3(config)#
R3(config)#
R3(config)#
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
R3(config)#
R3(config)#
```

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.



```
R3
Physical Config CLI Attributes
IOS Command Line Interface

R3(config)#
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)#
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
A pre-shared key for address mask 10.1.1.2 255.255.255.255 already exists!
R3(config)#
R3(config)#
R3(config)#
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
R3(config)#
R3(config)#
R3(config)#
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)# exit
R3(config)# copy run start
R3(config)#

% Invalid input detected at '^' marker.

R3(config)#do copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
R3(config)#
```

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.

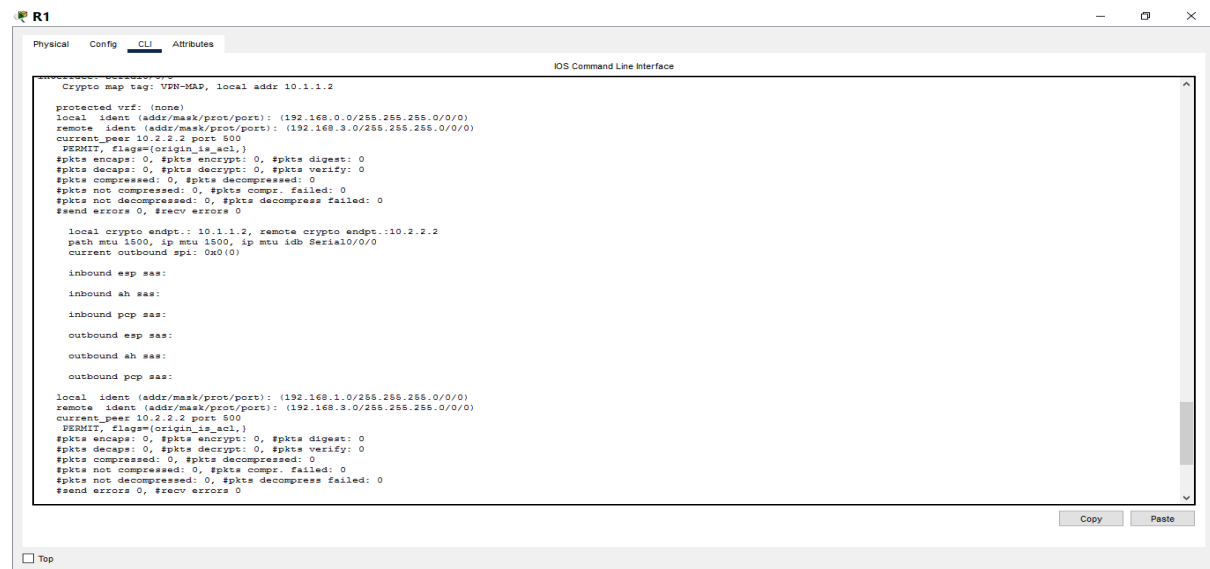


Figure 12 verify tunnel prior to traffic

Create interesting traffic.

Ping PC-C from PC-A.

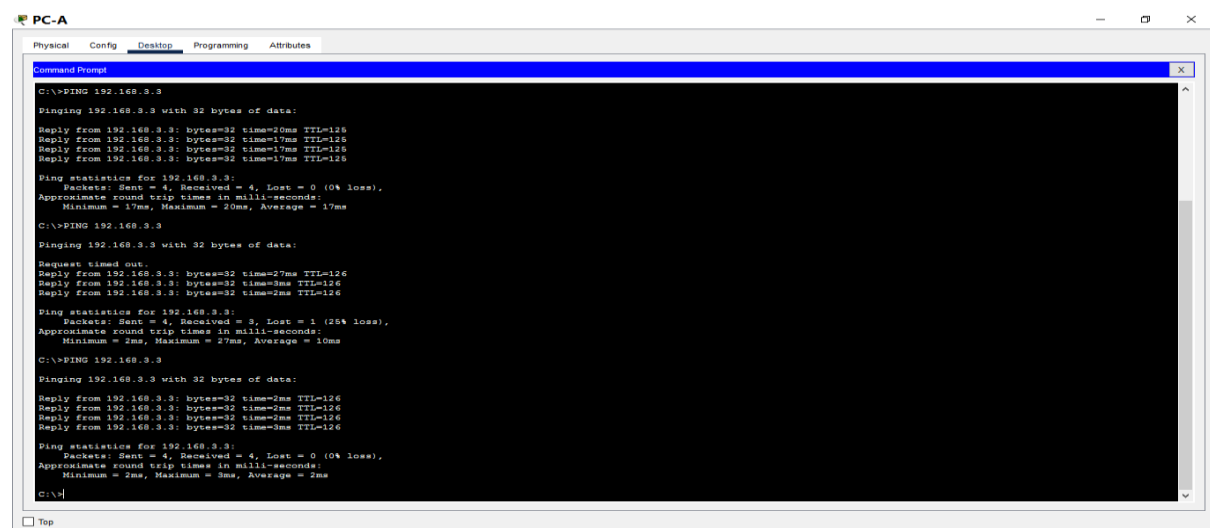
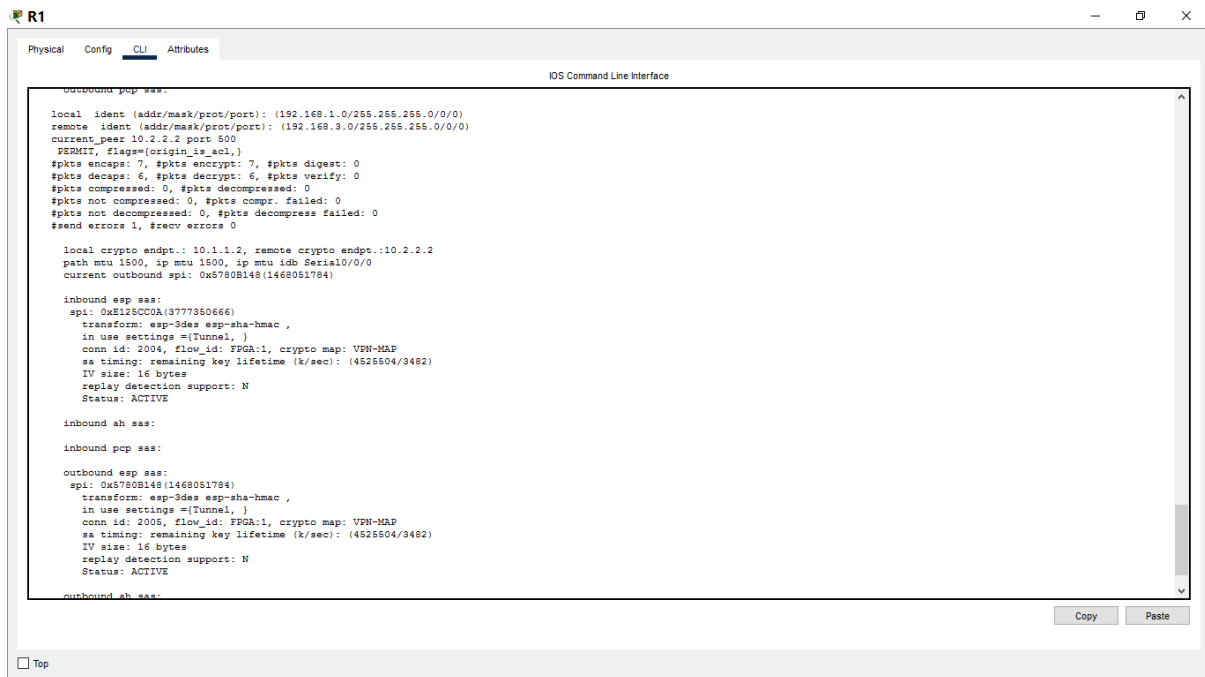


Figure 13 ping PC-C from PC-A

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.

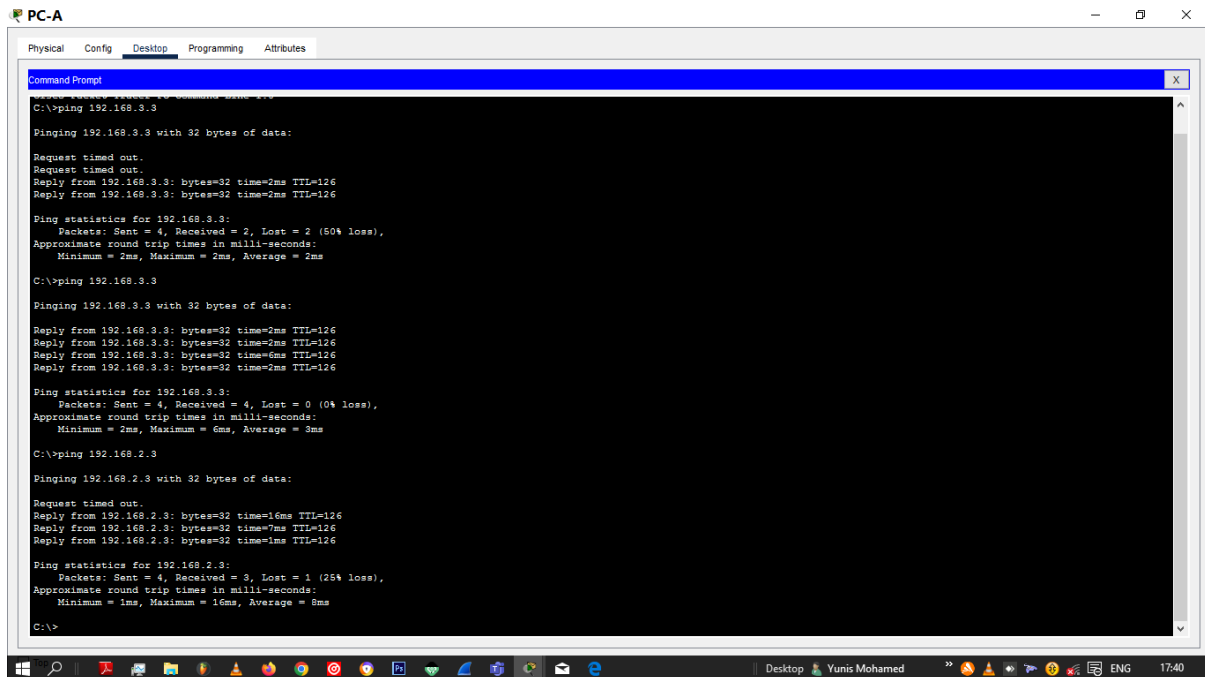
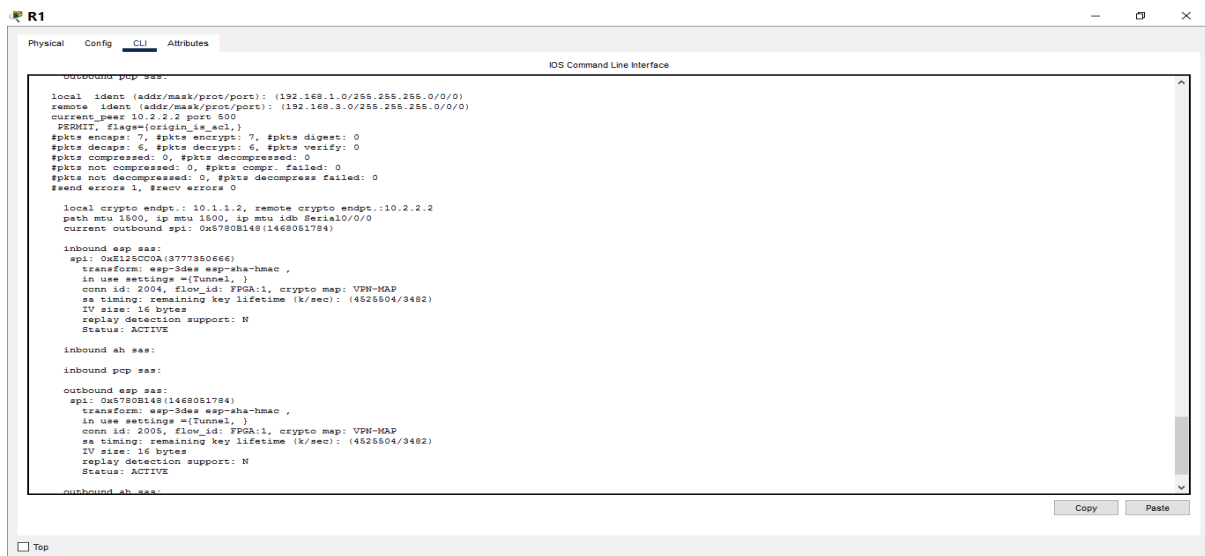


Figure 14 uninteresting traffic

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.



```

R1
Physical Config CLI Attributes
IOS Command Line Interface

show crypto ipsec sa:

local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
current_peer 10.2.2.2 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 7, #pkts encrypt: 7, #pkts digest: 0
  #pkts decaps: 6, #pkts decrypt: 6, #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: 0x5780B148(1468051784)

inbound esp sas:
  spi: 0x5125C0CA(3777380666)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Tunnel,}
    conn id: 2004, flow_id: FFD411, crypto map: VPN-MAP
    sa timing: remaining key lifetime (k/sec): (4525504/3482)
    IV size: 16 bytes
    replay detection support: N
    Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0x5780B148(1468051784)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Tunnel,}
    conn id: 2005, flow_id: FFD411, crypto map: VPN-MAP
    sa timing: remaining key lifetime (k/sec): (4525504/3482)
    IV size: 16 bytes
    replay detection support: N
    Status: ACTIVE

outbound ah sas:

```

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.