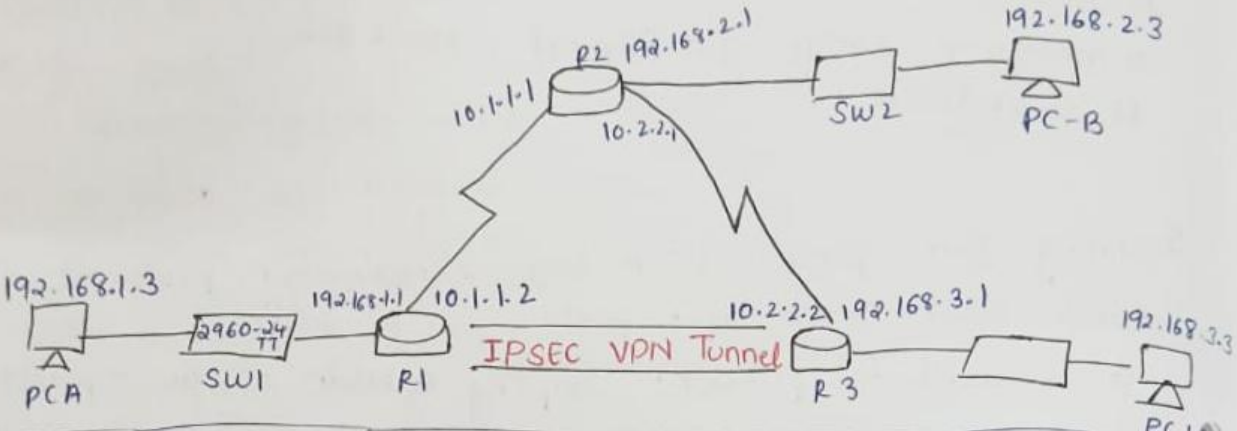
Practical # 9

Configure IPsec VPN using CLI



Steps: 1) Enable Security on Router
conpa55, enpa55 and SSH

2) Configure OSPF

On R1: router ospf 1
network 192.168.1.0 0.0.0.255 area 0
network 10.1.1.0 0.0.0.3 area 0
#ex

On R2: router ospf 1
network 192.168.2.0 0.0.0.255 area 0
network 10.2.2.0 0.0.0.3 area 0
network 10.1.1.0 0.0.0.3 area 0
#ex

On R3: router ospf 1
network 192.168.3.0 0.0.0.255 area 0
network 10.2.2.0 0.0.0.3 area 0
#ex

→ Test by ping cmd from PC-A to PC-C

3) Enable security package. (for both R1 & R3)

R1 → R1(config)# license boot module c1900 technology-package
security k9
-y
→ reload.

4/10/23 Identify the traffic of interest on R1

R1(config)# access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255

Configure ACL 110 to identify traffic from R1 to R3 (This traffic will trigger the IPsec VPN to be implemented when data flows betn R1 & R3)

5.) Configure the IKE phase 1 Ipsec policy on R1 → defines params for securing

→R1(config)# crypto isakmp policy 10

ISAKMP - Internet Security Association and Key Management Protocol.

The above command is used to configure cryptographic parameters included in ISAKMP policy 10, where 10 is the priority of the policy.

→ #encryption aes 256 → key-size

To configure encryption settings within Ipsec with algorithm AES (Adv encryption std). AES is an symmetric key alogorithms that works by using Block cipher.

→ #authentication pre-share

The authentication method is set to pre-shared keys. It means both devices should have same key.

→ # group 5

sets the Diffie-Hellman (DH) group to group 5 for the IKE negotiations. DH is a key exchange protocol used to establish a shared secret between two devices communicating over an insecure network

→ # ex

→ # crypto isakmp key VPNpa55 address 10.2.2.2

Specifies the pre-shared key to be used for IKE Phase 1 negotiation with R3.

IKE Phase 1: Internet Key Exchange Phase 1 is the 1st step in establishing a secure connect^n like VPN here, the device authenticate each other and negotiate security params such as encryption methods & authentication mechanisms. (Basically an agreement on how they will exchange the data)

Continue.....

6) Configure IKE phase 2 IPsec policy on R1.

In phase 2, devices establish the params for encrypting & authenticating the actual data to be transmitted betn them.

crypto ipsec transform-set VPN-SET esp-aes (encapsulating security payload) esp-sha-hmac (Hashed message authentication code) (secured Hash algorithm)

A transform set is collection of security parameters that define how data is encrypted, authenticate & protected during transmission.

→ The above command configures the router to use AES encryption with SHA-HMAC authentication for secure IPsec communication when using "VPN-SET" transform set.

crypto map VPN-MAP 10 ipsec-isakmp

→ creates a cryptomap named with a sequence number of & associates it with both IPsec & ISAKMP, meaning that this crypto map will handle both phase 1 & 2 negotiation.

→ Crypto maps are a config object used to define the policy for IPsec. They are applied to interfaces to determine which traffic should be encrypted and sent over the tunnel.

description VPN connection to R3

Adds a description to the crypto map

set peer 10.2.2.2

specifies the other device with which we communicate

set transform-set VPN-SET

Associates the VPN-SET with VPN-MAP

match address 110

specifies that ACL 110 determines which traffic should be protected by this crypto map. Only the traffic matching the condn in 110 will be encrypted & sent over the tunnel.

#

Configure cryptomap on the outgoing interface
interface s1/0/0 10
crypto map VPN-MAP.

Do the same for R3

Verify the IPsec VPN

→ show crypto ipsec sa
The no. of params should be zero.

→ Ping PC-C from PC-A

→ show crypto ipsec sa

→ create uninteresting traffic
ping PCB from PCA

→ show crypto ipsec sa
(The no. of packets should not change).