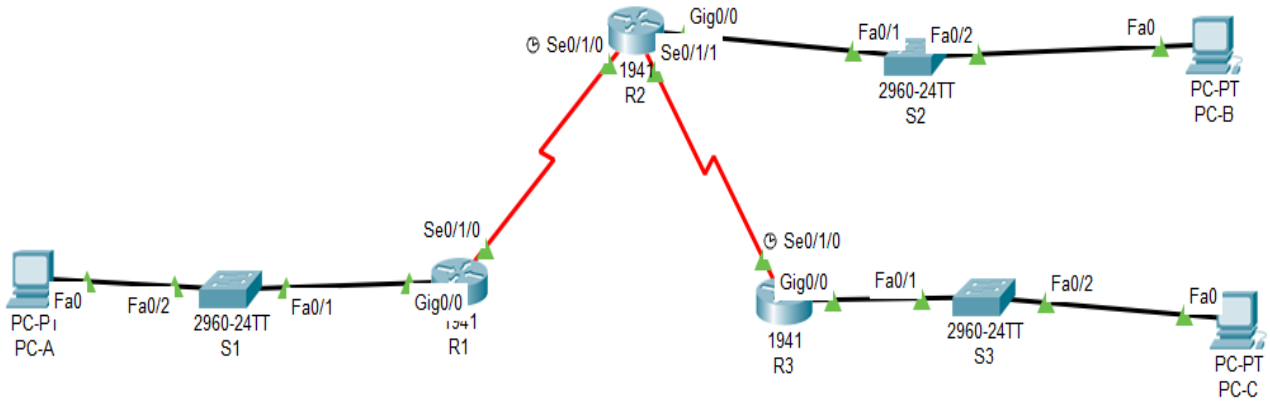
# Security In Computing Practical's

## Practical 9: Configure and Verify a Site-to-Site IPsec VPN Using CLI

### Topology:




### Addressing Table:

| Device | Interface | IP Address | Subnet Mask | Default Gateway |
|---|---|---|---|---|
| R1 | gig0/0 | 192.168.1.1 | 255.255.255.0 | N/A |
| | Se0/1/0 | 10.1.1.2 | 255.255.255.252 | N/A |
| R2 | gig0/0 | 192.168.2.1 | 255.255.255.0 | N/A |
| | Se0/1/0 | 10.1.1.1 | 255.255.255.252 | N/A |
| | Se0/1/1 | 10.2.2.1 | 255.255.255.252 | N/A |
| R3 | gig0/0 | 192.168.2.1 | 255.255.255.0 | N/A |
| | Se0/1/0 | 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 |

### Objectives:

- Verify connectivity throughout the network.
- Configure R1 to support a site-to-site IPsec VPN with R3.

# Security In Computing Practical's

## Part 1: Configure router

### Step 1: Configure secret on router

Execute command on all routers

R(config)# enable secret enpa55

### Step 2: Configure console password on router

Execute command on all routers

R(config)# line console 0

R(config-line)# password conpa55

R(config-line)# login

### Step 3: Configure SSH login on router

Execute command on all routers

R(config)# ip domain-name ccnasecurity.com

R(config)# username admin secret adminpa55

R(config)# line vty 0 4

R(config-line)# login local

R(config)# crypto key generate rsa

How many bits in the modulus [512]: 1024

### Step 4: Configure OSPF on routers

R1(config)# router ospf 1

R1(config)# network 192.168.1.0 0.0.0.255 area 0

R1(config)# network 10.1.1.0 0.0.0.3 area 0

R2(config)# router ospf 1

R2(config)# network 192.168.2.0 0.0.0.255 area 0

R2(config)# network 10.2.2.0 0.0.0.3 area 0

R2(config)# network 10.1.1.0 0.0.0.3 area 0

R3(config)# router ospf 1

R3(config)# network 192.168.3.0 0.0.0.255 area 0

R3(config)# network 10.2.2.0 0.0.0.3 area 0

## Part 2: Configure IPsec Parameters on R1

**Step 1: From PC-A, verify connectivity to PC-C and PC-B.**

PCA> ping 192.168.3.3

(Successful)

PCA> ping 192.168.2.3

(Successful)

PCB> ping 192.168.3.3

(Successful)



**Step 2: Check if the Security Technology package is enabled**

R1# show version

**Step 3: Enable the Security Technology package.**

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

**Step 4: Save the running config and reload the router to enable the security license**

R1# copy run start

R1# reload

# Security In Computing Practical's

**Step 5: Verify the Security Technology package is enabled**

R1# show version

**Step 6: Identify interesting traffic 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

**Step 7: Configure the IKE Phase 1 ISAKMP policy on R1.**

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 8: Configure the IKE Phase 2 IPsec policy on R1.**

R1(config)# crypto ipsec transform-set VPN-SET esp-aes 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

**Step 9: Configure the crypto map on the outgoing interface.**

R1(config)# int se0/1/0

R1(config-if)# crypto map VPN-MAP

## Part 3: Configure IPsec Parameters on R3

**Step 1: Check if the Security Technology package is enabled**

R3# show version

**Step 2: Enable the Security Technology package.**

R3(config)# license boot module c1900 technology-package securityk9

**Step 3: Save the running config and reload the router to enable the security license**

R3# copy run start

R3# reload



**Step 4: Verify the Security Technology package is enabled**

R3# show version

**Step 5: Configure router R3 to support a site-to-site VPN with R1.**

R3(config)# access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255

**Step 6: Configure the IKE Phase 1 ISAKMP properties on R3.**

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 7: Configure the IKE Phase 2 IPsec policy on R3.**

R3(config)# crypto ipsec transform-set VPN-SET esp-aes 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

**Step 8: Configure the crypto map on the outgoing interface.**

R3(config)# int se0/1/0

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



## Part 4: Verify the IPsec VPN

**Step 1: Verify the tunnel prior to interesting traffic.**

R1# show crypto ipsec sa

**Step 2: Create interesting traffic.**

PCC>ping 192.168.1.3

(Successful)

**Step 3: Verify the tunnel after interesting traffic.**

R1# show crypto ipsec sa

**Step 4: Create uninteresting traffic**

PCB>ping 192.168.1.3

(Successful)

R1#ping 192.168.3.3

(Successful)

R3#ping 192.168.1.3

(Successful)

**Step 5: Verify the tunnel.**

R1# show crypto ipsec sa