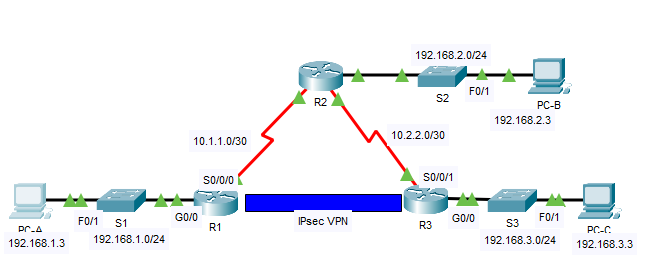
****

**Part 1:     Enable Security Features**

R1(config)# **license boot module c2900 technology-package securityk9**

R1(config)# **end**

R1# **copy running-config startup-config**

R1# **reload**

c.

d.    Repeat Steps 1a to 1c with **R3**.

**Part 2:     Configure IPsec Parameters on R1**

**Step 1:     Test connectivity.**

Ping from **PC-A** to **PC-C**.

**Step 2:     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 3:     Configure the ISAKMP Phase 1 properties on R1.**

R1(config)# **crypto isakmp policy 10**

R1(config-isakmp)# **encryption aes**

R1(config-isakmp)# **authentication pre-share**

R1(config-isakmp)# **group 2**

R1(config-isakmp)# **exit**

R1(config)# **crypto isakmp key cisco address 10.2.2.2**

**Step 4:     Configure the ISAKMP Phase 2 properties on R1.**

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

.

R1(config)# **interface S0/0/0**

R1(config-if)# **crypto map VPN-MAP**

**Part 3:     Configure IPsec Parameters on R3**

**Step 1:     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 2:     Configure the ISAKMP Phase 1 properties on R3.**

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**

**Step 3:     Configure the ISAKMP Phase 2 properties on R1.**

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**

**Step 4:     Configure the crypto map on the outgoing interface.**

R3(config)# **interface S0/0/1**

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.**

Ping **PC-C** from **PC-A**.

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

R1# **show crypto ipsec sa**

**Step 4:     Create uninteresting traffic.**

Ping **PC-B** from **PC-A**.