



Configure OSPF on all routers

Commands

Enable secrete tyit1819

Hostname R1

Username admin1 secret adminit2019

AAA new-model

AAA authentication login default local

Line console 0

Login authentication default

End

Exit

En

Config t

Ip domain-nametyit.com

Crypto key generate RSA

AAA authentication login SSH-LOGIN local

Line vty 0 4

Login authenticationSSH-LOGIN

**Configure IPsec Parameters on R1**

1. test connectivity from PC-A TO PC-C

2. : Enable the Security Technology package.

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

Do copy run start

Reload

Config t

3. 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

4. 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

5 Configure the IKE Phase 2 IPsec policy on R1.

a. Create the transform-set VPN-SET to use esp-aes and esp-sha-hmac.

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

b. 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.

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-cryptomap)# exit

6. Configure the crypto map on the outgoing interface.

R1(config)# interface s0/0/0

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

Part 2: Configure IPsec Parameters on R3

1 Enable the Security Technology package.

On R3, issue the show version command to verify that the Security Technology package license information has been enabled. b. If the Security Technology package has not been enabled, enable the package and reload R3

R3(config)# license boot module c1900 technology-package securityk9 Do copy run start

Reload

Config t

2. 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

3. 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

4. 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

5. Configure the crypto map on the outgoing interface

R3(config)# interface s0/0/1

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

Part 3: Verify the IPsec VPN

1. Verify the tunnel prior to interesting traffic.

R1 show crypto ipsec sa

2. Ping PC-C from PC-A.

3. Verify the tunnel after interesting traffic

On R1, re-issue the show crypto ipsec sa command. Notice that the number of packets is more than 0, which indicates that the IPsec VPN tunnel is working.

4. Create uninteresting traffic.

Ping PC-B from PC-A.

5. Verify the tunnel.

On R1, re-issue the show crypto ipsec sa command.