Practical 10: Configure and Verify a Site-to-Site IPsec VPN Using CLI

The routers have been pre-configured with the following:

• Password for console line: ciscoconpa55

• Password for vty lines: ciscovtypa55

• Enable password: ciscoenpa55

• SSH username and password: SSHadmin / ciscosshpa55

• OSPF 101

Part 1: Configure IPsec Parameters on R1

Step 1: Test connectivity. Ping from PC-A to PC-C.

Step 2: Enable the Security Technology package.

Write the commands for this step.

Step 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

Step 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

Step 5: Configure the IKE Phase 2 IPsec policy on R1.

1. 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
2. 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

Step 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

Step 1: Enable the Security Technology package.

Step 2: Configure router R3 to support a site-to-site VPN with R1. Configure reciprocating parameters on R3. Configure ACL 110 identifying the traffic from the LAN on R3 to the LAN on R1 as interesting.

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

Step 3: Configure the IKE Phase 1 ISAKMP properties on R3. Configure the crypto ISAKMP policy 10 properties on R3 along with the shared crypto key vpnpa55.

R3(config)# crypto isakmp policy 10

R3(config-isakmp)# encryption aes 256

3(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 4: Configure the IKE Phase 2 IPsec policy on R3.

1. Create the transform-set VPN-SET to use esp-aes and esp-sha-hmac. R3(config)# crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
2. 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(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 5: Configure the crypto map on the outgoing interface. Bind the VPN-MAP crypto map to the outgoing Serial 0/0/1 interface. Note: This is not graded.

R3(config)# interface s0/0/1

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

Part 3: Verify the IPsec VPN

Step 1: 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.

Step 2: Create interesting traffic.

Ping PC-C from PC-A.

Step 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.

Step 4: Create uninteresting traffic.

Ping PC-B from PC-A. Note: Issuing a ping from router R1 to PC-C or R3 to PC-A is not interesting traffic. Step 5: Verify the tunnel. On R1, re-issue the show crypto ipsec sa command.