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

Go to R1/2/3

R1(config)#enable secret enpa40

R1(config)#line console 0

R1(config-line)#password conpa40

R1(config-line)#login

R1(config-line)#exit

R1(config)#ip domain-name ccnasecurity.com

R1(config)#username admin secret adminpa55

R1(config)#line vty 0 4

R1(config-line)#login local

R1(config-line)#exit

R1(config)#crypto key generate rsa

How many bits in the modulus [512]: 1024

Now, Enable OSPF Routing in all Routers:

Steps:

Go to R1 🡪 R1(config)#

R1(config)#router ospf 1

R1(config-router)#network 192.168.1.0 0.0.0.255 area 0

R1(config-router)#network 10.1.1.0 0.0.0.3 area 0

Go to R2 🡪 R2(config)#

R2(config)#router ospf 2

R2(config-router)#network 192.168.2.0 0.0.0.255 area 0

R2(config-router)#network 10.2.2.0 0.0.0.3 area 0

R2(config-router)#network 10.1.1.0 0.0.0.3 area 0

Go to R3 🡪 R3(config)#

R3(config)#router ospf 3

R3(config-router)#network 192.168.3.0 0.0.0.255 area 0

R3(config-router)#network 10.2.2.0 0.0.0.3 area 0

2. Enable Security Technology Package on R1 & R3.

R1# show version

R1# conf t

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

R1(config)# ex

R1# reload

R1# show version

Create an ACL & configure the IKE Phase 1 ISAKMP policy on R1 & R3

Steps: ( For R1 )

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

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 vpnpa40 address 10.2.2.2

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

R1(config)#crypto map VPN-MAP 10 ipsec-isakmp

% NOTE: This new crypto map will remain disabled until a peer

and a valid access list have been configured.

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

R1(config)#interface se0/0/0

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

\*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP\_ON\_OFF: ISAKMP is ON

Steps: ( For R3 )

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

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 vpnpa40 address 10.1.1.2

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

R3(config)#crypto map VPN-MAP 10 ipsec-isakmp

% NOTE: This new crypto map will remain disabled until a peer

and a valid access list have been configured.

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

R3(config)#interface se0/0/1

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

\*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP\_ON\_OFF: ISAKMP is ON

R1 & R3 🡪 cmd

show crypto ipsec sa

PC A 🡪 cmd Ping 192.168.3.3

PC B 🡪 cmd Ping 192.168.1.3