**IPSec VPN Tunneling CLI Commands**

A VPN is a private network that uses a public network to connect two or more remote sites. Instead of using dedicated connections between networks, VPNs use virtual connections routed (tunneled) through public networks. IPsec VPN is a protocol, consists of set of standards used to establish a VPN connection.

**1. In the start, we set all the starting configurations for Routers R1, ISP, and R3.**

**2. Make sure routers have the security license enabled:**

license boot module c1900 technology-package securityk9

(licenses limit all encrypted tunnel counts to 225 tunnel maximum for IP security)

Then do **copy run start** followed by router **reload**

**i.** access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255

(To permit specific IP from the one network to another network)

**3.Configure IPsec on the routers at each end of the tunnel (R1 and R3)**

!**R1** (ISAKMP-Internet Security Association and Key Management Protocol)

**ii.** crypto isakmp policy 10

(is a policy that creates unique ISAKMP/IKE management connection policy on the router)

encryption aes 256 (aes-Advanced Encryption Standard)

authentication pre-share

group 5

(Diffie–Hellman key exchange is a method of securely exchanging cryptographic keys over a public channel)

!

**iii.** crypto isakmp key secretkey(password) address 209.165.200.1(address of peer router)

!

**iv.** crypto ipsec transform-set R1->R3 esp-aes(encryption) 256(bit) esp-sha-hmac(keyed hash)

!

**v.** crypto map IPSEC-MAP 10 ipsec-isakmp

set peer 209.165.200.1

set pfs group5 (pfs-perfect forward secrecy)

set security-association lifetime seconds 86400

set transform-set R1-R3

match address 100

!

**vi.** interface GigabitEthernet0/0

crypto map IPSEC-MAP

!

!**R3**

crypto isakmp policy 10

encryption aes 256

authentication pre-share

group 5 ("key exchange")

!

crypto isakmp key secretkey address 209.165.100.1

!

crypto ipsec transform-set R3-R1 esp-aes 256 esp-sha-hmac

!

crypto map IPSEC-MAP 10 ipsec-isakmp

set peer 209.165.100.1

set pfs group5

set security-association lifetime seconds 86400

set transform-set R3-R1

match address 100

!

interface GigabitEthernet0/0

crypto map IPSEC-MAP

!

access-list 100 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255

**To test if it is working correctly:**

->R1#show crypto ipsec sa

->R1#show crypto ?

->R1#show version

To paste in CLI

1. Starting configurations for R1, ISP, and R3. Paste to global config mode :

hostname R1

interface g0/1

ip address 192.168.1.1 255.255.255.0

no shut

interface g0/0

ip address 209.165.100.1 255.255.255.0

no shut

exit

ip route 0.0.0.0 0.0.0.0 209.165.100.2

hostname ISP

interface g0/1

ip address 209.165.200.2 255.255.255.0

no shut

interface g0/0

ip address 209.165.100.2 255.255.255.0

no shut

exit

hostname R3

interface g0/1

ip address 192.168.3.1 255.255.255.0

no shut

interface g0/0

ip address 209.165.200.1 255.255.255.0

no shut

exit

ip route 0.0.0.0 0.0.0.0 209.165.200.2

2. Make sure routers have the security license enabled:

license boot module c1900 technology-package securityk9

3. Configure IPsec on the routers at each end of the tunnel (R1 and R3)

!R1

crypto isakmp policy 10

encryption aes 256

authentication pre-share

group 5

!

crypto isakmp key secretkey address 209.165.200.1

!

crypto ipsec transform-set R1-R3 esp-aes 256 esp-sha-hmac

!

crypto map IPSEC-MAP 10 ipsec-isakmp

set peer 209.165.200.1

set pfs group5

set security-association lifetime seconds 86400

set transform-set R1-R3

match address 100

!

interface GigabitEthernet0/0

crypto map IPSEC-MAP

!

access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255

!R3

crypto isakmp policy 10

encryption aes 256

authentication pre-share

group 5

!

crypto isakmp key secretkey address 209.165.100.1

!

crypto ipsec transform-set R3-R1 esp-aes 256 esp-sha-hmac

!

crypto map IPSEC-MAP 10 ipsec-isakmp

set peer 209.165.100.1

set pfs group5

set security-association lifetime seconds 86400

set transform-set R3-R1

match address 100

!

interface GigabitEthernet0/0

crypto map IPSEC-MAP

!

access-list 100 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255

For Remote Access VPN

Initially, the PC in China cannot access the server in USA. When we try to enter IP address of server in the web browser of the PC in China it doesn’t show up.

Then, to set up VPN, we go to the PC in China and select the VPN option and enter the following details:

GroupName: GroupVPN

Group Key: ciscogroupvpn

Host IP: 209.165.200.230

Username: uservpn

Password: ciscovpn

Now, if we connect to the VPN successfully, we are able to access the webpage of the server in USA by typing the IP address of the server(192.168.2.254) in the web browser of the PC in China.