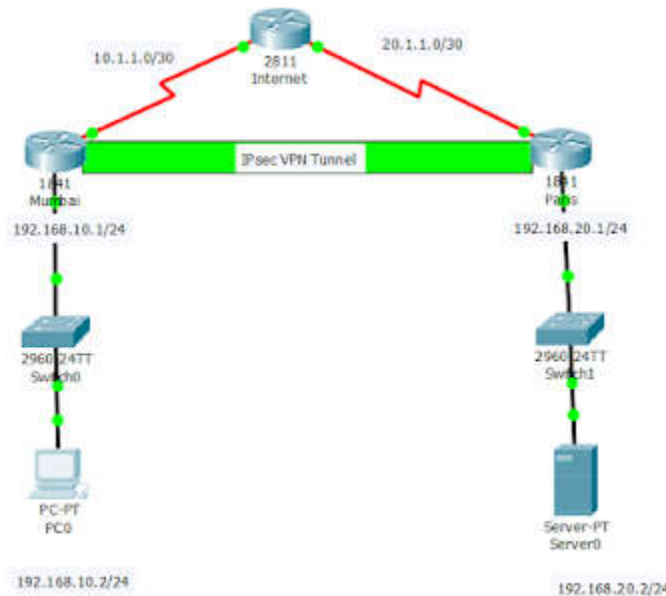


TP 05 : Configure Site-to-site IPsec VPN

When you finish this LAB, you will be able to configure the Site 2 Site IP sec VPN on cisco Devices.

Network topology

Network figure showing site-to-site IPsec Tunnel between **Paris** and **Mumbai** Routers. The Cisco 2811 router was used as the Internet router, while the 1841 security router was deployed in Mumbai and Paris offices. We have an https server in Paris that needs to be securely accessed from Mumbai. To make sure that https request from Mumbai to the server in Paris remain secure, we need to set up site-to-site IPsec VPN between Mumbai and Paris.



Configurations Tasks:

Task 1: build the network topology as shown in the figure.

Task 2: On Internet router make the following configuration

```
Router>en
Router#conf t
Router(config)#hostname Internet
Internet(config)#int s0/0/0
Internet(config-if)#clock rate 64000
Internet(config-if)#ip add 10.1.1.1 255.255.255.252
Internet(config-if)#desc connection to Mumbai
Internet(config-if)#no shut
Internet(config-if)#int s0/0/1
Internet(config-if)#clock rate 64000
Internet(config-if)#ip add 20.1.1.1 255.255.255.252
Internet(config-if)#desc connection to Paris
Internet(config-if)#no shut
Internet(config-if)#
Internet(config-if)#exit
Internet(config)#exit
Internet#
Internet#copy run start
```

Task 3: On Mumbai router make the following configuration

```
Router>en
Router#conf t
Router(config)#hostname Mumbai
Mumbai(config)#int s0/1/0
Mumbai(config-if)#ip add 10.1.1.2 255.255.255.252
Mumbai(config-if)#desc connection to Internet
Mumbai(config-if)#no shut
Mumbai(config-if)#int f0/0
Mumbai(config-if)#ip add 192.168.10.1 255.255.255.0
Mumbai(config-if)#desc connection to LAN
Mumbai(config-if)#no shut
Mumbai(config-if)#exit
Mumbai(config)#ip route 0.0.0.0 0.0.0.0 10.1.1.1
Mumbai(config)#
```

Task 4: On Paris Router make the following configuration

```
Router>en
Router#conf t
Router(config)#hostname Paris
Paris(config)#int s0/0/0
Paris(config-if)#ip add 20.1.1.2 255.255.255.252
Paris(config-if)#desc connection to Internet
Paris(config-if)#no shut
Paris(config-if)#int f0/0
Paris(config-if)#ip add 192.168.20.1 255.255.255.0
Paris(config-if)#desc connection to LAN
Paris(config-if)#no shut
Paris(config-if)#exit
Paris(config)#ip route 0.0.0.0 0.0.0.0 20.1.1.1
Paris(config)#
```

Task 5: set up an access-list on the Mumbai router to be used as VPN Traffic

First, set up an access-list to match the traffics to be allowed through the VPN tunnel.

```
Mumbai(config)#ip access-list extended VPN
Mumbai(config-ext-nacl)#permit ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
Mumbai(config-ext-nacl)#exit
Mumbai(config)#
```

Now, configure IPsec VPN to use the access-list named VPN. Authentication mode is pre-share key (Sofiane). The key must be the same on both routers. See below.

```
Mumbai(config)#crypto isakmp policy 1
Mumbai(config-isakmp)#authentication pre-share
Mumbai(config-isakmp)#crypto isakmp key Sofiane address 20.1.1.2 (The public IP address of Paris router)
Mumbai(config-isakmp)#exit
Mumbai(config)#crypto ipsec transform-set ASSET esp-aes esp-sha-hmac
Mumbai(config)#crypto map ASMAP 1 ipsec-isakmp
Mumbai(config-crypto-map)#set peer 20.1.1.2
Mumbai(config-crypto-map)#set transform-set ASSET
Mumbai(config-crypto-map)#match address VPN
```

Finally, on the Mumbai router, we MUST apply the crypto map to the interface connecting to the ISP.

```
Mumbai(config)#int s0/0/0
Mumbai(config-if)#crypto map ASMAP
```

Task 6: set up an access-list on the Paris router to be used as VPN Traffic

Now, repeat the process on the Paris router, making sure the IP address of the peer router matches the public IP address configured on the Paris router. Remember, this IP must be reachable from the Mumbai router. First, the ACL.

```
Paris(config)#ip access-list extended VPN
Paris(config-ext-nacl)#permit ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255
Paris(config-ext-nacl)#exit
Paris(config)#
```

Next, the VPN configuration proper.

```
Paris(config)#crypto isakmp policy 1
```

```
Paris(config-isakmp)#authentication pre-share
Paris(config-isakmp)#crypto isakmp key Sofiane address 10.1.1.2 (The public IP address of Paris
router)
Paris(config-isakmp)#exit
Paris(config)#crypto ipsec transform-set ASSET esp-aes esp-sha-hmac
Paris(config)#crypto map ASMAP 1 ipsec-isakmp
Paris(config-crypto-map)#set peer 10.1.1.2
Paris(config-crypto-map)#set transform-set ASSET
Paris(config-crypto-map)#match address VPN
```

Finally, apply the crypto-map to the WAN interface.

```
Paris(config)#int s0/0/0
Paris(config-if)#crypto map ASMAP
```

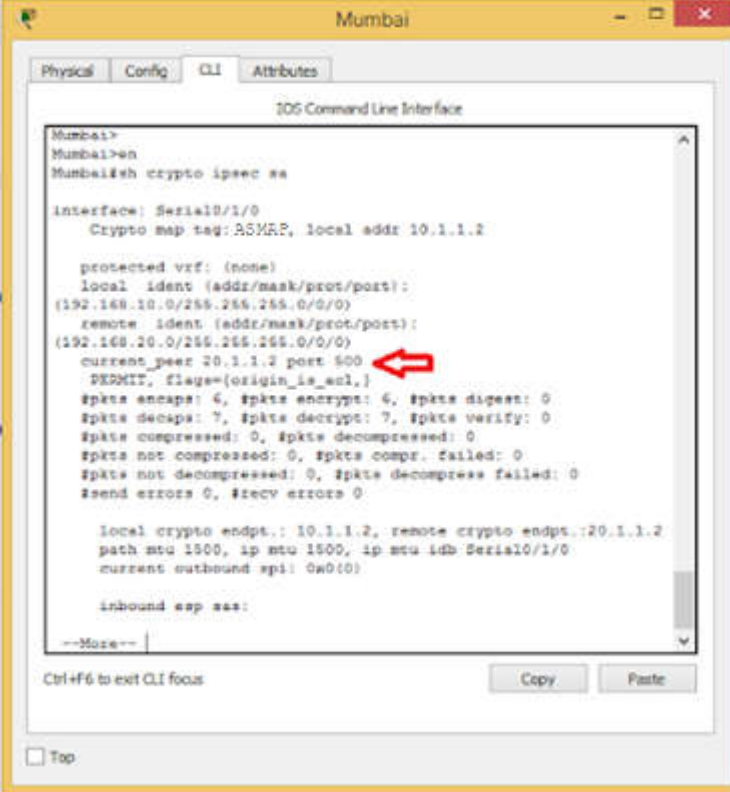
Note:

The IPsec VPN configuration will be in 4 phases.

1. Configuration of the access-list to match allowed traffics.
2. Configuration of the authentication phase which in this case makes use of pre-share key named Sofiane.
3. Configuration of the encryption phase which in this case uses esp-aes esp-sha-hmac
4. The placement of the crypto-map on the connecting interface. This must be the interface with the public IP used in the VPN configuration.

VERIFICATION:

To see the status of IPSEC authentication, use the command `#sh crypto ipsec sa` command. See output below



```
Mumbai>
Mumbai#en
Mumbai#sh crypto ipsec sa

interface: Serial0/1/0
Crypto map tag: ASMARP, local addr 10.1.1.2

protected vrf: (none)
local ident (addr/mask/prot/port):
(192.168.10.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port):
(192.168.20.0/255.255.255.0/0/0)
current_peer 20.1.1.2 port 500 ←
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 6, #pkts encrypt: 6, #pkts digest: 0
#pkts decaps: 7, #pkts decrypt: 7, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

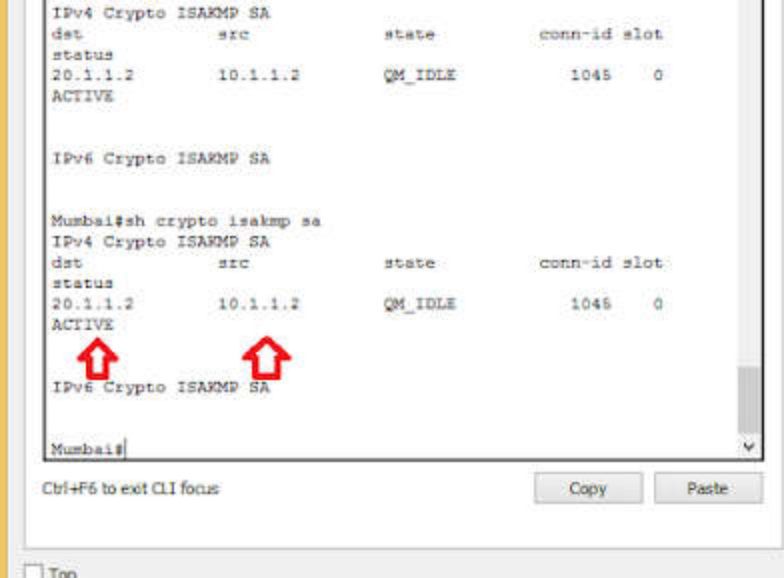
local crypto endpt.: 10.1.1.2, remote crypto endpt.:20.1.1.2
path mtu 1500, ip mtu 1500, ip mtu idb: Serial0/1/0
current outbound spi: 0a000

inbound esp sas:

--More--
Ctrl+F6 to exit CLI focus
```

Result of `#sh crypto ipsec sa`

The show crypto isakmp sa command will show encryption status.



```
IPv4 Crypto ISAKMP SA
dst      src      state      conn-id slot
status
20.1.1.2 10.1.1.2 QM_IDLE    1045  0
ACTIVE

IPv6 Crypto ISAKMP SA

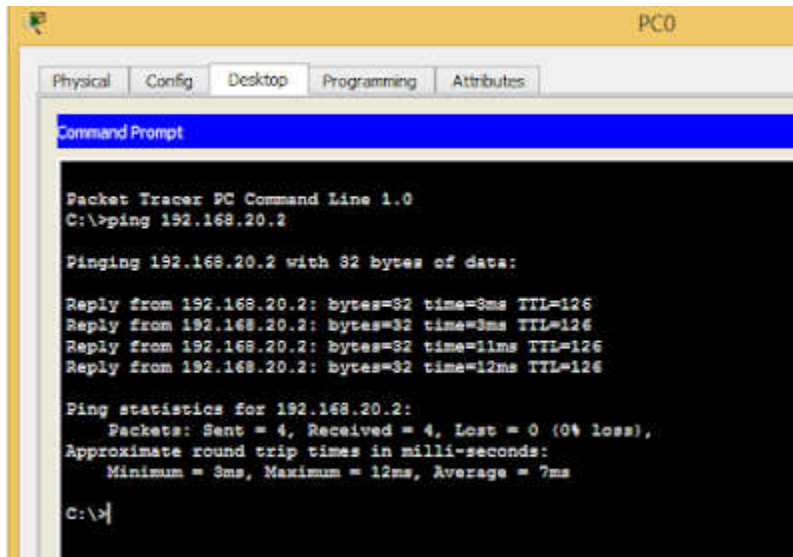
Mumbai#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst      src      state      conn-id slot
status
20.1.1.2 10.1.1.2 QM_IDLE    1045  0
ACTIVE
↑
IPv6 Crypto ISAKMP SA
↑
Mumbai#

Ctrl+F6 to exit CLI focus
```

Result of `#sh crypto isakmp sa`

TESTING THE CONNECTIVITY:

Finally, you must try to access the server in Paris from the PC in Mumbai.



Ping result from PC0 to server0

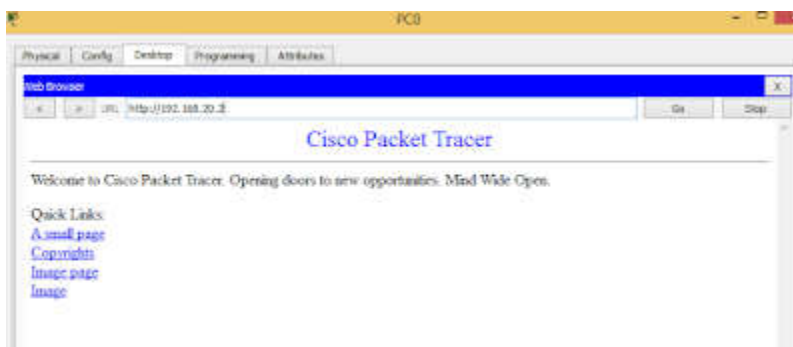


Image showing web access to server0 from PC0