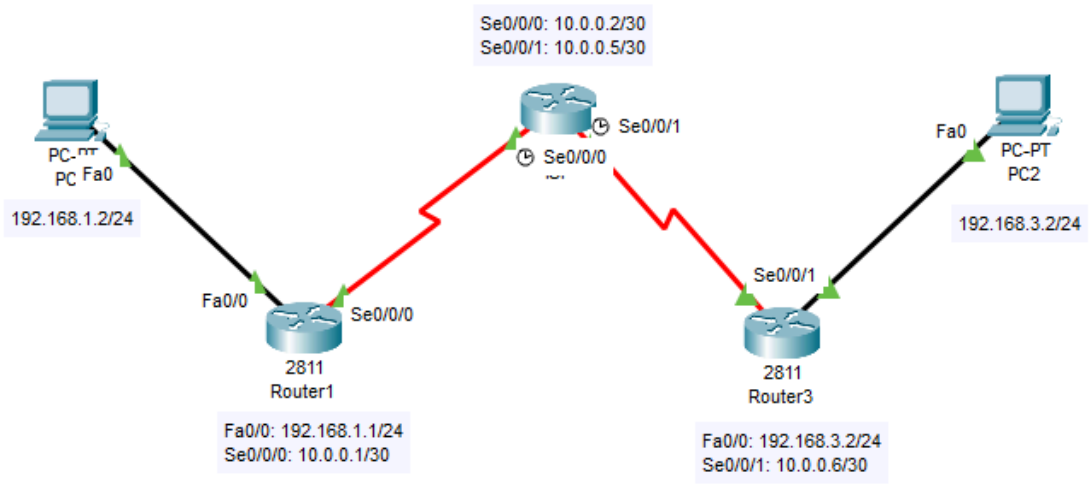
Eric Guzman 4/30/2025

Professor Cannistra Internet Security

Lab 5

Description: In this lab we will configure a site to site VPN between IOS routers on an ISP network.

Topology:



Syntax:

Command	Description	Mode of IOS
crypto isakmp key cisco123 address 10.0.0.6	Sets the pre shared key for ISAKMP	Global configuration mode
show crypto isakmp sa	Displays ISAKMP status	Privileged EXEC mode
show crypto ipsec sa	Displays information on IPsec security associations	Privileged EXEC mode

Verification:

```
C:\>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.3.2: bytes=32 time=9ms TTL=126
Reply from 192.168.3.2: bytes=32 time=10ms TTL=126
Reply from 192.168.3.2: bytes=32 time=11ms TTL=126

Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 9ms, Maximum = 11ms, Average = 10ms

C:\>
```

```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=11ms TTL=126
Reply from 192.168.1.2: bytes=32 time=12ms TTL=126
Reply from 192.168.1.2: bytes=32 time=25ms TTL=126
Reply from 192.168.1.2: bytes=32 time=10ms TTL=126

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 25ms, Average = 14ms

C:\>
```

These screenshots show that pings are successful from both PCs on the topology proving that the tunnel is successfully established and working properly.

```
Router1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
10.0.0.6        10.0.0.1        QM_IDLE           1019    0 ACTIVE


IPv6 Crypto ISAKMP SA
```

This screenshot shows the output from the “show crypto isakmp sa” command which indicates that the ISAKMP phase one tunnel has been established with Router3 (10.0.0.6).

```
Router1#show crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: VPN-MAP, local addr 10.0.0.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
   current_peer 10.0.0.6 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 7, #pkts encrypt: 7, #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 1, #recv errors 0

     local crypto endpt.: 10.0.0.1, remote crypto endpt.:10.0.0.6
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0x9D0B2FDF(2634756063)

     inbound esp sas:
      spi: 0xEAB05F21(3937427233)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2003, flow_id: FPGA:1, crypto map: VPN-MAP
        sa timing: remaining key lifetime (k/sec): (4525504/2690)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x9D0B2FDF(2634756063)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2004, flow_id: FPGA:1, crypto map: VPN-MAP
        sa timing: remaining key lifetime (k/sec): (4525504/2690)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:
```

This screenshot shows the output from the “show crypto ipsec sa” command confirming that IPsec phase two is active. You can see the encrypted and decrypted packet counters that prove that data is securely flowing through the active tunnel.

Conclusion:

This was a nice quick lab that I feel will be good to use in the challenge lab. I know I probably will copy at least the commands I used here to save time when configuring it.