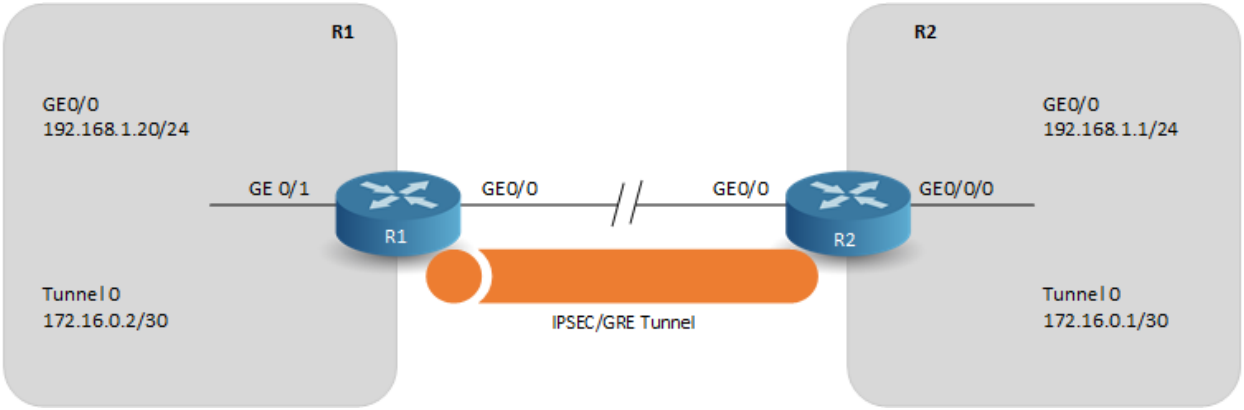
Create an IPsec Protected Tunnel



Lab Setup

- CML
- IOSv
    - Image: IOSv 15.8(3)

Establishing GRE Tunnel

```
R1(config)$interface tunnel 0
R1(config-if)#ip mtu 1400
R1(config-if)#ip address 172.16.0.2 255.255.255.252
R1(config-if)#tunnel source 192.168.1.20
R1(config-if)#tunnel destination 192.168.1.1
R1(config-if)#tunnel key 12345

R2(config)$interface tunnel 0
R2(config-if)#ip mtu 1400
R2(config-if)#ip address 172.16.0.1 255.255.255.252
R2(config-if)#tunnel source 192.168.1.1
```

```
R2(config-if)#tunnel destination 192.168.1.20
R2(config-if)#tunnel key 12345
```

R1 - IPsec Configuration

```
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#encryption aes 256
R1(config-isakmp)#hash sha256
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 16
R1(config-isakmp)#exit

R1(config)#crypto isakmp key CISCO_KEY address 192.168.1.1

R1(config)#crypto ipsec transform-set VPNset esp-aes 256 esp-sha256-hmac
R1(cfg-crypto-trans)#mode transport
R1(cfg-crypto-trans)#exit

R1(config)#crypto ipsec profile VPNprofile
R1(ipsec-profile)#set transform-set VPNset
R1(ipsec-profile)#exit

R1(config)#interface tunnel 0
R1(config-if)#tunnel protection ipsec profile VPNprofile
```

R2 - IPsec Configuration

```
R2(config)#crypto isakmp policy 10
R2(config-isakmp)#encryption aes 256
R2(config-isakmp)#hash sha256
R2(config-isakmp)#authentication pre-share
R2(config-isakmp)#group 16
R2(config-isakmp)#exit

R2(config)#crypto isakmp key CISCO_KEY address 192.168.1.20

R2(config)#crypto ipsec transform-set VPNset esp-aes 256 esp-sha256-hmac
R2(cfg-crypto-trans)#mode transport
R2(cfg-crypto-trans)#exit

R2(config)#crypto ipsec profile VPNprofile
R2(ipsec-profile)#set transform-set VPNset
R2(ipsec-profile)#exit
```

```
R2(config)#interface tunnel 0
R2(config-if)#tunnel protection ipsec profile VPNprofile
```

R1 - Verify

```
R1#show interfaces tunnel 0
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 172.16.0.2/30
  MTU 17870 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel linestate evaluation up
  Tunnel source 192.168.1.20, destination 192.168.1.1
  Tunnel protocol/transport GRE/IP
    Key 0x3039, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255, Fast tunneling enabled
  Tunnel transport MTU 1430 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Tunnel protection via IPSec (profile "VPNprofile")
  Last input 00:20:17, output 00:20:17, output hang never
  Last clearing of "show interface" counters 00:25:15
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     5 packets input, 620 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     5 packets output, 620 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
R1#

R1#sh cryto ipsec sa

interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 192.168.1.20

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.1.20/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/47/0)
   current_peer 192.168.1.1 port 500
```

```
      PERMIT, flags={origin_is_acl,}
     #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
     #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
     #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.: 192.168.1.20, remote crypto endpt.: 192.168.1.1
      plaintext mtu 1458, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
      current outbound spi: 0x4A2C1DB0(1244405168)
      PFS (Y/N): N, DH group: none

      inbound esp sas:
       spi: 0x4976134D(1232474957)
         transform: esp-256-aes esp-sha256-hmac ,
         in use settings ={Transport, }
         conn id: 1, flow_id: SW:1, sibling_flags 80000000, crypto map: Tunnel0-head-0
         sa timing: remaining key lifetime (k/sec): (4608000/3309)
         IV size: 16 bytes
         replay detection support: Y
         Status: ACTIVE(ACTIVE)
       spi: 0xEAEFDE5(246349285)
         transform: esp-256-aes esp-sha256-hmac ,
         in use settings ={Transport, }
         conn id: 3, flow_id: SW:3, sibling_flags 80004000, crypto map: Tunnel0-head-0
         sa timing: remaining key lifetime (k/sec): (4241526/3312)
         IV size: 16 bytes
         replay detection support: Y
         Status: ACTIVE(ACTIVE)

      inbound ah sas:

      inbound pcp sas:

      outbound esp sas:
       spi: 0x8B0E2E3F(2332962367)
         transform: esp-256-aes esp-sha256-hmac ,
         in use settings ={Transport, }
         conn id: 2, flow_id: SW:2, sibling_flags 80000000, crypto map: Tunnel0-head-0
         sa timing: remaining key lifetime (k/sec): (4608000/3309)
         IV size: 16 bytes
         replay detection support: Y
         Status: ACTIVE(ACTIVE)
       spi: 0x4A2C1DB0(1244405168)
         transform: esp-256-aes esp-sha256-hmac ,
         in use settings ={Transport, }
         conn id: 4, flow_id: SW:4, sibling_flags 80004000, crypto map: Tunnel0-head-0
         sa timing: remaining key lifetime (k/sec): (4241526/3312)
         IV size: 16 bytes
         replay detection support: Y
         Status: ACTIVE(ACTIVE)

      outbound ah sas:
```

```
     outbound pcp sas:
R1#


R1#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
192.168.1.1     192.168.1.20    QM_IDLE           1002 ACTIVE
192.168.1.20    192.168.1.1     QM_IDLE           1001 ACTIVE

IPv6 Crypto ISAKMP SA

R1#
```

R2 - Verify

```
R2#show interfaces tunnel 0
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 172.16.0.1/30
  MTU 17870 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel linestate evaluation up
  Tunnel source 192.168.1.1, destination 192.168.1.20
  Tunnel protocol/transport GRE/IP
    Key 0x3039, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255, Fast tunneling enabled
  Tunnel transport MTU 1430 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Tunnel protection via IPSec (profile "VPNprofile")
  Last input 00:18:08, output 00:18:10, output hang never
  Last clearing of "show interface" counters 00:23:40
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     5 packets input, 620 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     5 packets output, 620 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
```

```
     0 output buffer failures, 0 output buffers swapped out
R2#


R2#sh crypto ipsec sa

interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 192.168.1.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (192.168.1.20/255.255.255.255/47/0)
   current_peer 192.168.1.20 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
    #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
    #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.: 192.168.1.1, remote crypto endpt.: 192.168.1.20
     plaintext mtu 1458, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
     current outbound spi: 0xEAEFDE5(246349285)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0x8B0E2E3F(2332962367)
        transform: esp-256-aes esp-sha256-hmac ,
        in use settings ={Transport, }
        conn id: 1, flow_id: SW:1, sibling_flags 80004000, crypto map: Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4608000/3213)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)
      spi: 0x4A2C1DB0(1244405168)
        transform: esp-256-aes esp-sha256-hmac ,
        in use settings ={Transport, }
        conn id: 3, flow_id: SW:3, sibling_flags 80000000, crypto map: Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4272923/3216)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x4976134D(1232474957)
        transform: esp-256-aes esp-sha256-hmac ,
        in use settings ={Transport, }
        conn id: 2, flow_id: SW:2, sibling_flags 80004000, crypto map: Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4608000/3213)
```

```
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)
      spi: 0xEAEFDE5(246349285)
        transform: esp-256-aes esp-sha256-hmac ,
        in use settings ={Transport, }
        conn id: 4, flow_id: SW:4, sibling_flags 80000000, crypto map: Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4272923/3216)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     outbound ah sas:

     outbound pcp sas:
R2#

R2#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
192.168.1.20    192.168.1.1     QM_IDLE           1001 ACTIVE
192.168.1.1     192.168.1.20    QM_IDLE           1002 ACTIVE

IPv6 Crypto ISAKMP SA

R2#
```