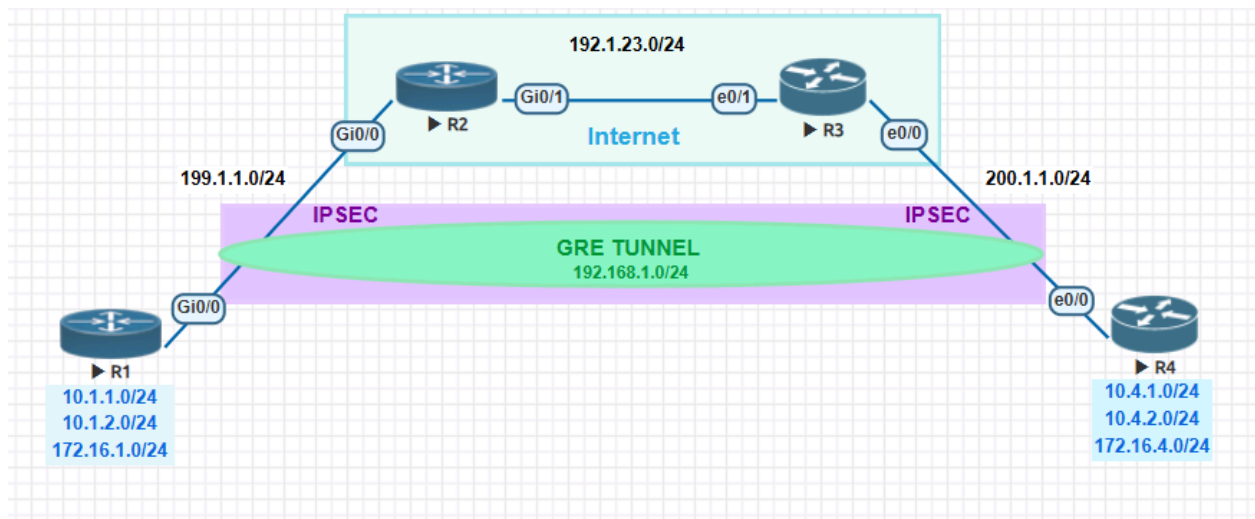



Goal: To encrypt all GRE tunnel traffic using IPsec.



In order to create GRE over IPsec, we have to follow the below steps:

Script:  GRE over IPSEC script.txt

IPsec P-cap:  GRE - IPsec to S-VTI.pcapng

Create a GRE tunnel.

Run an IGP.

Now for IPsec if we recall we needed below parameters:

! Phase#1

crypto isakmp policy 10

authentication pre-share

hash md5

encryption 3des

group 2

crypto isakmp key cisco123 address 200.1.1.4

Now for IPsec encryption, we need to create an IPsec profile and bind it with the tunnel.

Why are we not using crypto map with acl that matches interesting traffic?

- **Match traffic:** The ACL is used to Match traffic but our target is to encrypt all tunnel traffic.
- **Peer:** It's given in the tunnel as destination.
- **Transform Set:** IPsec profile is used to bind it to the interface tunnel.

! Phase#2

```
crypto ipsec transform-set TSET esp-3des esp-md5
```

```
! Create a profile to attach the transform set
```

```
crypto ipsec profile SECPROF
```

```
set transform-set TSET
```

```
! Configure the tunnel interface
```

```
interface tunnel 1
```

```
tunnel protection ipsec profile SECPROF
```

```
!
```

```
R4#
R4#
*Jul 29 03:31:27.606: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
*Jul 29 03:31:28.853: %CRYPTO-4-RECVD_PKT_NOT_IPSEC: Rec'd packet not an IPSEC packet. (ip) vrf/dest_addr= /200.1.1.4, src_addr= 199.1.1.1, prot=
47
R4#
R4#
R4#
R4#
*Jul 29 03:31:29.048: %SYS-5-CONFIG_I: Configured from console by console
R4#
R4#
R4#
R4#
*Jul 29 03:31:32.470: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnell, changed state to down
*Jul 29 03:31:32.470: %OSPF-5-ADJCHG: Process 1, Nbr 199.1.1.1 on Tunnell from FULL to DOWN, Neighbor Down: Interface down or detached
```

7	17.032815	192.168.1.1	224.0.0.5	OSPF	114 Hello Packet
8	17.690468	200.1.1.4	199.1.1.1	ISAKMP	206 Identity Protection (Main Mode)
9	17.693622	199.1.1.1	200.1.1.4	ICMP	70 Destination unreachable (Port unreachable)
10	18.335371	50:00:00:02:00:01	CDP/VTP/DTP/PAgP/UD...	CDP	402 Device ID: R2 Port ID: GigabitEthernet0/1
11	18.534785	aa:bb:cc:00:30:10	aa:bb:cc:00:30:10	LOOP	60 Reply
12	20.348657	50:00:00:02:00:01	50:00:00:02:00:01	LOOP	60 Reply
13	20.934480	aa:bb:cc:00:30:10	CDP/VTP/DTP/PAgP/UD...	CDP	373 Device ID: R3 Port ID: Ethernet0/1
14	26.417042	192.168.1.1	224.0.0.5	OSPF	114 Hello Packet
15	27.694766	200.1.1.4	199.1.1.1	ISAKMP	206 Identity Protection (Main Mode)
16	27.698518	199.1.1.1	200.1.1.4	ICMP	70 Destination unreachable (Port unreachable)
17	28.538946	aa:bb:cc:00:30:10	aa:bb:cc:00:30:10	LOOP	60 Reply

```
> Frame 7: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface -, id 0
> Ethernet II, Src: 50:00:00:02:00:01 (50:00:00:02:00:01), Dst: aa:bb:cc:00:30:10 (aa:bb:cc:00:30:10)
> Internet Protocol Version 4, Src: 199.1.1.1, Dst: 200.1.1.4
> Generic Routing Encapsulation (IP)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 224.0.0.5
> Open Shortest Path First
```

42	78.120861	199.1.1.1	200.1.1.4	ISAKMP	206 Identity Protection (Main Mode)
43	78.122282	200.1.1.4	199.1.1.1	ISAKMP	146 Identity Protection (Main Mode)
44	78.147600	199.1.1.1	200.1.1.4	ISAKMP	318 Identity Protection (Main Mode)
45	78.156342	200.1.1.4	199.1.1.1	ISAKMP	338 Identity Protection (Main Mode)
46	78.175861	199.1.1.1	200.1.1.4	ISAKMP	134 Identity Protection (Main Mode)
47	78.177253	200.1.1.4	199.1.1.1	ISAKMP	110 Identity Protection (Main Mode)
48	78.193473	199.1.1.1	200.1.1.4	ISAKMP	206 Quick Mode
49	78.195631	200.1.1.4	199.1.1.1	ISAKMP	206 Quick Mode
50	78.251023	199.1.1.1	200.1.1.4	ISAKMP	94 Quick Mode
51	78.254755	200.1.1.4	199.1.1.1	ISAKMP	206 Identity Protection (Main Mode)

112	162.700620	199.1.1.1	200.1.1.4	ESP	174 ESP (SPI=0x60338b0b)
113	164.810938	200.1.1.4	199.1.1.1	ESP	174 ESP (SPI=0x7f922877)

```

> Frame 112: 174 bytes on wire (1392 bits), 174 bytes captured (1392 bits) on interface -, id 0
> Ethernet II, Src: 50:00:00:02:00:01 (50:00:00:02:00:01), Dst: aa:bb:cc:00:30:10 (aa:bb:cc:00:30:10)
> Internet Protocol Version 4, Src: 199.1.1.1, Dst: 200.1.1.4
v Encapsulating Security Payload
  ESP SPI: 0x60338b0b (1613990667)
  ESP Sequence: 11

```

```

R1(config)#!Phase #1
R1(config)#
R1(config)#crypto isakmp policy 10
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# hash md5
R1(config-isakmp)# encryption 3des
R1(config-isakmp)# group 2
R1(config-isakmp)#
R1(config-isakmp)#crypto isakmp key cisco123 address 200.1.1.4
R1(config)#
R1(config)#!Phase #2
R1(config)#
R1(config)#crypto ipsec transform-set TSET esp-3des esp-md5
R1(cfg-crypto-trans)#
R1(cfg-crypto-trans)#! Create a profile to attach the transform set
R1(cfg-crypto-trans)#
R1(cfg-crypto-trans)#crypto ipsec profile SECROF
R1(ipsec-profile)# set transform-set TSET
R1(ipsec-profile)#
R1(ipsec-profile)#! Configure the tunnel interface
R1(ipsec-profile)#
R1(ipsec-profile)#interface tunnel 1
R1(config-if)# tunnel protection ipsec profile SECROF
Profile SECROF is not defined.
R1(config-if)# tunnel protection ipsec profile SECROF
R1(config-if)#
*Jul 29 03:33:04.518: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
*Jul 29 03:33:04.759: %OSPF-5-ADJCHG: Process 1, Nbr 200.1.1.4 on Tunnell from LOADING to FULL, Loading Done
*Jul 29 03:33:05.501: %LINEPROTO-5-UPDOWN: Line protocol on Interface NVI0, changed state to up
R1(config-if)#
R1(config-if)#

```

```

R1#show crypto ipsec sa | i in
interface: Tunnel1
  PERMIT, flags={origin_is_acl,}
  plaintext mtu 1446, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
  inbound esp sas:
    in use settings ={Tunnel, }
    conn id: 1, flow_id: SW:1, sibling_flags 80004040, crypto map: Tunnel1-head-0
    sa timing: remaining key lifetime (k/sec): (4608000/3336)
    in use settings ={Tunnel, }
    conn id: 3, flow_id: SW:3, sibling_flags 80000040, crypto map: Tunnel1-head-0
    sa timing: remaining key lifetime (k/sec): (4351778/3336)
  inbound ah sas:
  inbound pcp sas:
    in use settings ={Tunnel, }
    conn id: 2, flow_id: SW:2, sibling_flags 80004040, crypto map: Tunnel1-head-0
    sa timing: remaining key lifetime (k/sec): (4608000/3336)
    in use settings ={Tunnel, }
    conn id: 4, flow_id: SW:4, sibling_flags 80000040, crypto map: Tunnel1-head-0
    sa timing: remaining key lifetime (k/sec): (4351778/3336)
R1#

```

```

R1#show running-config | sec cryp
no service password-encryption
crypto isakmp policy 10
  encr 3des
  hash md5
  authentication pre-share
  group 2
crypto isakmp key cisco123 address 200.1.1.4
crypto ipsec transform-set TSET esp-3des esp-md5-hmac
  mode tunnel
crypto ipsec profile SECPROF
  set transform-set TSET
R1#

```

Transport Mode:

1. **Purpose:** Transport mode is primarily used for **point-to-point** tunnels, where endpoints need to communicate directly with each other.
2. **Encryption:** In transport mode, only the **payload** of the IP packet is encrypted and authenticated. The original IP headers remain unencrypted.
3. **Visibility:** Because the data is not fully encapsulated like tunnel mode, routers can still view the source and destination IP addresses.
4. **Use Case:** Historically, transport mode was used before IPsec became widespread. [It's suitable for specific endpoint communication¹](#).

Tunnel Mode:

5. **Purpose:** Tunnel mode is more versatile and commonly used. It's suitable for both **point-to-point** and **network-to-network** (site-to-site) communication.

6. **Encryption:** In tunnel mode, the entire IP packet (including the original IP header) is encapsulated within a new IP packet. This provides stronger security by encrypting both the payload and headers.
7. **Flexibility:** Tunnel mode can be used in any type of WAN environment, including scenarios involving NAT or PAT.
8. **Use Case:** [Ideal for securing connections over the Internet or private circuits like MPLS or VPLS².](#)

Transport:

112	162.700620	199.1.1.1	200.1.1.4	ESP	174	ESP (SPI=0x60338b0b)
113	164.810938	200.1.1.4	199.1.1.1	ESP	174	ESP (SPI=0x7f922877)

```

> Frame 112: 174 bytes on wire (1392 bits), 174 bytes captured (1392 bits) on interface -, id 0
> Ethernet II, Src: 50:00:00:02:00:01 (50:00:00:02:00:01), Dst: aa:bb:cc:00:30:10 (aa:bb:cc:00:30:10)
> Internet Protocol Version 4, Src: 199.1.1.1, Dst: 200.1.1.4
v Encapsulating Security Payload
  ESP SPI: 0x60338b0b (1613990667)
  ESP Sequence: 11

```

```

R4#show crypto ipsec sa | i in
interface: Tunnell
  PERMIT, flags={origin_is_acl,}
  plaintext mtu 1466, path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
  inbound esp sas:
    in use settings ={Transport, }
    conn id: 9, flow_id: SW:9, sibling_flags 80000000, crypto map: Tunnell-head-0
    sa timing: remaining key lifetime (k/sec): (4176052/3510)
  inbound ah sas:
  inbound pcp sas:
    in use settings ={Transport, }
    conn id: 10, flow_id: SW:10, sibling_flags 80000000, crypto map: Tunnell-head-0
    sa timing: remaining key lifetime (k/sec): (4176052/3510)
R4#

```

1304	2837.263034	199.1.1.1	200.1.1.4	ESP	150	ESP (SPI=0x819523bd)
1305	2840.280029	aa:bb:cc:00:30:10	aa:bb:cc:00:30:10	LOOP	60	Reply
1306	2840.899590	200.1.1.4	199.1.1.1	ESP	150	ESP (SPI=0xa31af465)

```

> Frame 1304: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits) on interface -, id 0
> Ethernet II, Src: 50:00:00:02:00:01 (50:00:00:02:00:01), Dst: aa:bb:cc:00:30:10 (aa:bb:cc:00:30:10)
> Internet Protocol Version 4, Src: 199.1.1.1, Dst: 200.1.1.4
v Encapsulating Security Payload
  ESP SPI: 0x819523bd (2174034877)
  ESP Sequence: 38

```

```
R4#  
R4#show runn interface tunnel 1  
Building configuration..  
  
Current configuration : 159 bytes  
!  
interface Tunnell  
  ip address 192.168.1.4 255.255.255.0  
  tunnel source 200.1.1.4  
  tunnel destination 199.1.1.1  
  tunnel protection ipsec profile SECPROF  
end
```