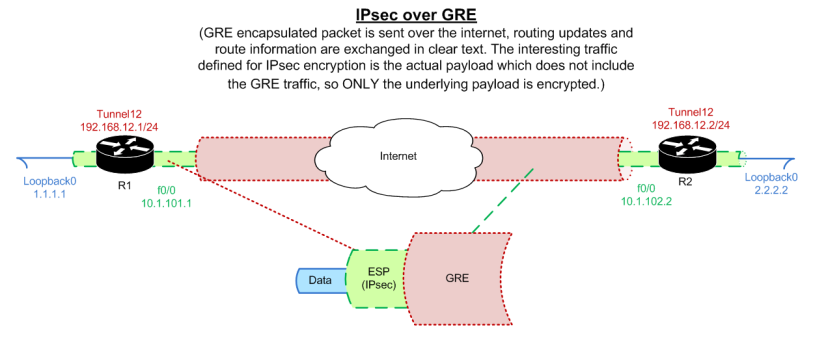
**IPsec over GRE – Configuration and Explanation**

As GRE does not have its own mechanism to encrypt traffic it depends on IPsec for getting the encryption job done. As opposed to GRE over IPsec, which encrypts anything that is encapsulated by GRE, IPsec over GRE encrypts only the payload and not the routing protocols running over a GRE tunnel.

In IPsec over GRE, the GRE tunnel is established over the internet, neighborship is formed and routes are exchanged and all of this is in clear text. We are only concerned with encrypting the interesting traffic flowing between the two peers. When securing the routing updates and routes isn’t a requirement and the major concern is to encrypt the information/payload flowing between the peers we use IPsec over GRE.

IPsec over GRE eliminates the additional overhead of encrypting the GRE header.



### Configuration on R1:

interface FastEthernet0/0

ip address 10.1.101.1 255.255.255.0

!

interface Loopback0

ip address 1.1.1.1 255.255.255.0

!

interface Tunnel12

ip address 192.168.12.1 255.255.255.0

tunnel source 10.1.101.1

tunnel destination 10.1.102.2

crypto map out\_map

!

router eigrp 34

network 1.1.1.1 0.0.0.0

network 192.168.12.0

!

access-list 130 permit ip host 1.1.1.1 host 2.2.2.2

!

crypto isakmp key cisco123 address 10.1.101.1

crypto isakmp policy 10

authentication pre-shared-key

encryption des

hash sha

group 1

!

crypto ipsec transform-set esp-3des esp-3des esp-sha-hmac

!

crypto map out\_map local-address Loopback0

crypto map out\_map 30 ipsec-isakmp

set peer 2.2.2.2

set transform-set esp-des

match address 130

### Configuration on R2:

interface FastEthernet0/0

ip address 10.1.102.2 255.255.255.0

!

interface Loopback0

ip address 2.2.2.2 255.255.255.0

!

interface Tunnel12

ip address 192.168.12.2 255.255.255.0

tunnel source 10.1.102.2

tunnel destination 10.1.101.1

crypto map out\_map

!

router eigrp 34

network 2.2.2.2 0.0.0.0

network 192.168.12.0

!

access-list 130 permit ip host 2.2.2.2 host 1.1.1.1

!

crypto isakmp key cisco123 address 10.1.101.1

crypto isakmp policy 10

authentication pre-shared-key

encryption des

hash sha

group 1

!

crypto ipsec transform-set esp-3des esp-3des esp-sha-hmac

!

crypto map out\_map local-address Loopback0

crypto map out\_map 30 ipsec-isakmp

set peer 1.1.1.1

set transform-set esp-des

match address 130

**Notes:-**

– IPsec over GRE encrypts the Payload and not the GRE encapsulated packets.

**– Interface for IPsec tunnel** – The IPsec tunnel should be formed using the loopback interface IP. When using loopbacks, you need to make sure the peer endpoints have a route for the loopback. This can be achieved by running another routing protocol to advertise the loopbacks and then forming an IPsec tunnel using the loopback IP address. ‘**crypto map out\_map local-address loopback 0**‘ needs to be configured so that when the tunnel is being negotiated it sources from its loopback address and the same is to be done on the other end peer.

**– Encryption Domain** – The encryption domain specified is always between the source and destination subnets that are to be encrypted and not the GRE tunnel source/destination IPs which is the case with GRE over IPsec. In the above example, we are specifying the encryption domain for all IP traffic between 1.1.1.1 and 2.2.2.2. So your GRE tunnel will not be encapsulated and only the traffic flowing through it will be encapsulated. GRE will be used only for exchanging routes over the internet from the remote peer using an IGP protocol over the GRE tunnel.

**– Application of Crypto Map** – The crypto map has to be applied on the interface where the route for the destination encryption domain is learnt. In our case the destination encryption domains of 1.1.1.1 and 2.2.2.2 are learnt via the Tunnel12 interface on R2 and R1 respectively, so the crypto map will be applied on Tunnel12 interface.

**– In the verification section below**, note the proxy identities in the IPsec SA. The encrypted traffic is for the remote subnets for IP traffic only. If it were GRE traffic, the proxy identities would have shown**protocol number 47** being encrypted.

### Verification on R1 and R2:

R1#show crypto ipsec sa peer 2.2.2.2

interface: Tunnel12

Crypto map tag: out\_map, local addr 1.1.1.1

protected vrf: (none)

local ident (addr/mask/prot/port): (1.1.1.1/255.255.255.255/**0**/0)

remote ident (addr/mask/prot/port): (2.2.2.2/255.255.255.255/**0**/0)

current\_peer 2.2.2.2 port 500

PERMIT, flags={origin\_is\_acl,}

#pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9

#pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9

R1#telnet 2.2.2.2 /source-interface loopback 0

Trying 2.2.2.2 ... Open

User Access Verification

Password:

R2>

R2#show crypto ipsec sa peer 1.1.1.1

interface: Tunnel12

Crypto map tag: out\_map, local addr 2.2.2.2

protected vrf: (none)

local ident (addr/mask/prot/port): (2.2.2.2/255.255.255.255/**0**/0)

remote ident (addr/mask/prot/port): (1.1.1.1/255.255.255.255/**0**/0)

current\_peer 1.1.1.1 port 500

PERMIT, flags={origin\_is\_acl,}

#pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9

#pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9

R2#telnet 1.1.1.1 /source-interface loopback 0

Trying 1.1.1.1 ... Open

User Access Verification

Password:

R1>

### Captures:-

To capture traffic I ran a ping from 1.1.1.1 to 2.2.2.2 and below is the wireshark capture showing the traffic being encrypted for the pings but the EIGRP hellos are not encrypted. With this we can conclude that in an IPsec over GRE VPN, only the defined interesting traffic is encrypted and the GRE traffic flows in clear text.

