Gre tunnel over IPSec

Introduction

This document deals with configuration of GRE tunnel over IPSEC.

What is GRE?

Generic Routing Encapsulation (GRE), is a simple IP packet encapsulation protocol. A GRE tunnel is used when IP packets need to be sent from one network to another, without being parsed or treated like IP packets by any intervening routers.

For example, in Mobile IP, a mobile node registers with a Home Agent. When the mobile node roams to a new network, it registers with a Foreign Agent there. Whenever IP packets addressed to the mobile node are received by the Home Agent, they can be relayed over a GRE tunnel to the Foreign Agent for delivery. It does not matter how the Home Agent and Foreign Agent communicate with each other -- hops in between just pass along the GRE packet. Only the GRE tunnel endpoints -- the two Agents -- actually route the encapsulated IP packet.

What is IPSEC?

The IP Security (IPsec) Encapsulating Security Payload (ESP), also encapsulates IP packets. However, it does so for a different reason: to secure the encapsulated payload using encryption. IPsec ESP is used when IP packets need to be exchanged between two systems while being protected against eavesdropping or modification along the way.

For example, in a site-to-site VPN, a source host in network "A" transmits an IP packet. When that packet reaches the edge of network "A," it hits a VPN gateway. VPN gateway "A" encrypts the private IP packet and relays it over an ESP tunnel to a peer VPN gateway at the edge of network "B." VPN gateway "B" then decrypts the packet and delivers it to the destination host. Like GRE, it doesn't really matter how the two VPN gateways communicate with each other -- hops in between just pass along the ESP packet. But unlike GRE, someone at those hops could not possibly look at or change the encapsulated IP packet, even if they wanted to. That's because cryptographic algorithms have been applied to scramble the IP packet and detect any modification or replay.

In summary, use a GRE tunnel where IP tunneling without privacy is required -- it's simpler and thus faster. But use IPsec ESP where IP tunneling and data privacy are required -- it provides security features that are not even attempted by GRE.

Gre tunnel over IPSec

To **configure Generic Routing Encapsulation (GRE) over an IPSec tunnel between two routers**, you can refer to these steps as follows:

Gre IP-Subnet:192.168.16.0 /30
RT01:
Se0/0/0: 10.10.10.1 (source set fra RT01)
Gre tunnel adresse: 192.168.16.1 255.255.255.252
RT02:
Se0/0/1: 10.20.10.1 (Destination set fra RT01)
Gre tunnel adresse: 192.168.16.2 255.255.255.252

RT01 (Source og destination skal byttes om på RT02):
1. Create a tunnel interface *(the IP address of tunnel interface on both routers must be in the same subnet),* and configure a tunnel source and tunnel destination under tunnel interface configuration, as shown:

```
interface Tunnel0
ip address 192.168.16.1 255.255.255.252
tunnel source 10.10.10.1
tunnel destination 10.20.10.1
```

2. Configure isakmp policies, as shown:

```
crypto isakmp policy 1
authentication pre-share
```

3. Configure pre share keys, as shown:

```
crypto isakmp key cisco123 address 10.20.10.1 (Remote outside interface IP with 32 bit subnet mask)
```

4. Configure transform set, as shown:

```
crypto ipsec transform-set STRONG esp-3des esp-md5-hmac
```

5. Creat crypto ACl that permits GRE traffic from the outside interface of the local router to the outside interface of the remote router, as shown:

```
access-list 120 permit gre host 10.10.10.1 (local outside interface ip) host 10.20.10.1 (Remote outside
interface IP)
```

6. Configure crypto map and bind transform set and crypto Access Control List (ACL) to crypto map. Define peer IP address under crypto map, as shown:

```
crypto map IPSEC_MAP 10 ipsec-isakmp
set peer 10.20.10.1
set transform-set STRONG
match address 120
```

7. Bind crypto map to the physical (outside) interface if you are running **Cisco IOS Software Release 12.2.15** or later. If not, then the crypto map must be applied to the tunnel interface as well as the physical interace, as shown:

```
interface seriel0/0/0
ip address 10.10.10.1
crypto map IPSEC_MAP
```

Gre tunnel over IPSec

Test af ISAKMP og IPsec:

- **show crypto isakmp sa**
  Nedenstående vises (kun et eksempel):

  ```
  IPv4 Crypto ISAKMP SA
  dst src state conn-id slot status
  203.0.0.6 203.0.0.2 QM_IDLE 1001 0 ACTIVE
  IPv6 Crypto ISAKMP SA
  ```

- **show crypto ipsec sa**
  Nedenstående vises (kun et eksempel):

  ```
  interface: Serial0/0
  Crypto map tag: IPSEC_MAP, local addr 203.0.0.2
  protected vrf: (none)
  local ident (addr/mask/prot/port): (203.0.0.2/255.255.255.255/47/0)
  remote ident (addr/mask/prot/port): (203.0.0.6/255.255.255.255/47/0)
  current_peer 203.0.0.6 port 500
  PERMIT, flags={origin_is_acl,}
     #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
     #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
  #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
  ```