Az **IPsec GRE tunnelen** történő konfigurálása Cisco routeren több lépésből áll. Az alábbiakban egy részletes konfigurációs példán keresztül mutatjuk be két router (R1 és R2) között a beállítását, ahol egy **GRE tunnel** lesz titkosítva **IPsec** segítségével.

---

1. A Hálózati topológia: `[R1] ---- (Internet) ---- [R2]`

- **R1 publikus IP:** 192.0.2.1
- **R2 publikus IP:** 192.0.2.2
- **GRE tunnel IP-k:**
  - R1: 10.10.10.1
  - R2: 10.10.10.2

---

2. GRE Tunnel konfiguráció

A GRE tunnelt először létre kell hozni mindkét routeren.

R1 konfigurációja:

```
interface Tunnel0
ip address 10.10.10.1 255.255.255.252
tunnel source Se0/0/0
tunnel destination 192.0.2.2
```

R2 konfigurációja:

```
interface Tunnel0
ip address 10.10.10.2 255.255.255.252
tunnel source Se0/0/0
tunnel destination 192.0.2.1
```

Ezzel létrejött a GRE tunnel, de még nem titkosított.

---

3. IPsec konfiguráció GRE tunnelre

3.1. SecurityK9 modul engedélyezése a routereken:

```
license boot module c2900 technology-package securityk9
```

3.2. IKE (Internet Key Exchange) Phase 1 beállítása: (Ez az IPsec kapcsolat létrehozásának első szakasza.)

R1 konfigurációja

```
crypto isakmp policy 10
 encryption aes 256      (titkosítási algoritmus)
 hash sha                (üzenetek integritás ellenőrzése)
 authentication pre-share       (előre megosztott kulcs alapú hitelesítés)
 group 5           (kulcsgenerálási módszer: Diffie-Hellman Group 5)
 lifetime 86400          (kapcsolat érvényességi ideje)
```

Előre megosztott kulcs létrehozása: a másik végpontnak is ismernie kell (192.0.2.2)

```
crypto isakmp key MYSECRETKEY address 192.0.2.2 (előre megosztott kulcs)
```

R2 konfigurációja

```
crypto isakmp policy 10
 encryption aes 256
 hash sha
 authentication pre-share
 group 5
 lifetime 86400
```

Előre megosztott kulcs létrehozása: a másik végpontnak is ismernie kell (192.0.2.1)

```
crypto isakmp key MYSECRETKEY address 192.0.2.1
```

3.3. IKE Phase 2 (IPsec transform set létrehozása)

A transform set meghatározza, hogy az IPsec milyen titkosítási és hitelesítési algoritmusokat használjon a forgalom védelmére.

R1 konfigurációja:

```
crypto ipsec transform-set MYSET esp-aes 256 esp-sha-hmac
```

R2 konfigurációja:

```
crypto ipsec transform-set MYSET esp-aes 256 esp-sha-hmac
```

3.4 ACL létrehozása az IPsec forgalomhoz

Egy ACL-t kell létrehozni, amely meghatározza, hogy mely forgalmat titkosítsa az IPsec.

```
access-list 100 permit ip 10.1.1.0 0.0.0.255 10.2.2.0 0.0.0.255
```

- **10.1.1.0/24** (belső hálózat R1 oldalán)
- **10.2.2.0/24** (belső hálózat R2 oldalán)
- Csak ezek között a hálózatok között haladó forgalom lesz titkosítva.

3.5. Crypto Map létrehozása

A crypto map beállítása, amely tartalmazza a partner IP-címét és a transform set-et:

R1 konfigurációja:

```
crypto map MYMAP 10 ipsec-isakmp
 set peer 192.0.2.2
 set transform-set MYSET
 match address 100
```

R2 konfigurációja:

```
crypto map MYMAP 10 ipsec-isakmp
 set peer 192.0.2.1
 set transform-set MYSET
 match address 100
```

- `MYMAP 10` → Létrehoz egy crypto map-et MYMAP néven, 10-es prioritással.
- `set peer 192.0.2.2` → Az IPsec VPN távoli végpontja (R2 IP-címe).
- `set transform-set MYSET` → Az előzőleg létrehozott transform set-et használja.
- `match address 100` → Csak a 100-as hozzáférési listával megjelölt forgalom kerül titkosításra.

3.6 Crypto Map alkalmazása az interfészre

A crypto map-et hozzá kell rendelni a külső interfészhez (pl. Serial0/0/0).

```
interface Serial0/0/0
 crypto map MYMAP
```

---

4. Ellenőrzés és hibaelhárítás

Miután a konfiguráció elkészült, ellenőrizhetjük az IPsec kapcsolat állapotát.

1. GRE tunnel állapotának ellenőrzése

```
show ip interface brief
show interface Tunnel0
```

2. IPsec állapotának ellenőrzése

```
show crypto isakmp sa
show crypto ipsec sa
```

Ha az IPsec kapcsolat sikeresen létrejött, akkor a kimenetben az IPsec SA (Security Association) aktív állapotban lesz.
