SITE TO SITE VPN

VPN ALAGÚT

- A VPN-t (Virtual Private Network) azért találták ki, hogy a különböző helyeken lévő egy szervezethez tartozó internet kapcsolattal rendelkező felhasználók biztonságosan tudjanak egymással információt cserélni.
- Nem kell ezért drága külön vonallal összekötni a végpontokat, tetszőleges internetkapcsolattal működik
- Biztonságos, mert a kapcsolódáskor hitelesítés történik és az összes átküldött adat titkosítva van
- Az átküldött adatok módosítás ellen is védve vannak, minden üzenetre lehet tenni hitelesítést (pecsét)

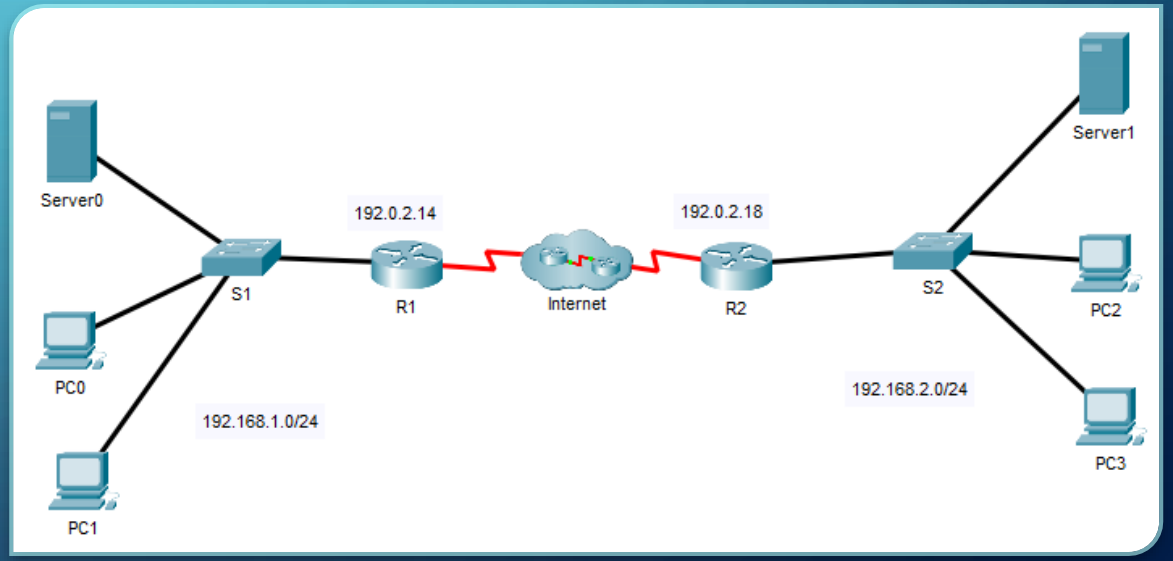
SITE TO SITE VPN

- Ez a típusú VPN két telephelyt köt össze.
- Itt nem úgy épül fel az alagút, mint a GRE estében, itt nem jelenik meg logikai kapcsolat az alagúttal. Az alagút teljesen láthatatlan lesz a hálózat számára. Olyan lesz mintha a két végpont összeolvadna és egy eszköz interfészei lennének az összekötött hálózatok. Ez problémát jelenthet az IP irányításában. Úgy lehet kiküszöbölni, hogy egy GRE alagút forgalmát tesszük be a VPN alagútba.

SITE TO SITE VPN BEÁLLÍTÁSA

Az ábrán a két összekötendő telephely látható. A bal oldali telephely (192.168.1.0/24 hálózat) és a jobb oldali (192.168.2.0/24). Mindkettőnek van beállított internetkapcsolata. R1 és R2 között hozzuk létre a VPN alagutat a felettük lévő két IP cím a publikus IP címük.

Ez a két cím lesz az alagút két végpontja. Fontos, hogy mivel most nem lesz összekötő logikai link a két végpont között, az alapértelmezett útvonal fogja az internet felé elindítani az üzeneteket és ezek közül kell kiválasztani az alagútba kerülőket.



SITE TO SITE VPN JELMAGYARÁZAT

- Piros szöveg: fix CLI parancsok
- Sárga szöveg: szabadon választható, vagy adott, de utána azt kell használni (többször előfordul!), a másikon újra szabadon elnevezhető
- Sötétkék szöveg: választható, vagy adott, és a két routeren meg kell egyeznie!
- Zöld szöveg/lila szöveg: adott feladat egyedi paraméterei (általában változtatni kell)

SITE TO SITE VPN BEÁLLÍTÁSA (BAL OLDAL)

- Először a végpontok hitelesítését kell beállítani. Létre kell hozni a túlsó végpontnak egy jelszót (itt jelszo lesz a jelszó):

```
R1(config)# crypto isakmp key jelszo address 192.0.2.18
```

- Majd be kell állítani, hogy ezt a jelszót használja:

```
R1(config)# crypto isakmp policy 1
R1(config-isakmp)# authentication pre-share
```

- Itt a hitelesítés típusának is egyeznie kell a két routeren, de a Packet Tracer csak pre-share-t tud ezért fix

SITE TO SITE VPN BEÁLLÍTÁSA (BAL OLDAL)

- Ez után meg kell adni a kapcsolatban használt titkosítást (itt AES 256 bites kulccsal) és ha akarunk akkor a csomagok hitelesítését (itt: SHA) is:

```
R1(config)# crypto ipsec transform-set TSET esp-aes 256 esp-sha-hmac
```

- Majd létre kell hozni egy ACL-t amellyel megadjuk, hogy milyen forgalmat akarunk beleterelni az alagútba (melyik hálózatból hová):

```
R1(config)# ip access-list extended S2SVPN
R1(config-ext-nacl)#permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
```

SITE TO SITE VPN BEÁLLÍTÁSA (BAL OLDAL)

- Ez után össze kell rakni az alagút tulajdonságait (az előző dián megadott ACL-t és titkosításokat rendeljük össze a végponti kapcsolattal):
- `R1(config)# crypto map CMAP 1 ipsec-isakmp`
- `R1(config-crypto-map)# set peer 192.0.2.18`
- `R1(config-crypto-map)# set transform-set TSET`
- `R1(config-crypto-map)# match address S2SVPN`

SITE TO SITE VPN BEÁLLÍTÁSA (BAL OLDAL)

- Végül az egészet hozzárendeljük a alagút kiindulópontját jelentő interfészhez:

```
R1(config)# interface Serial0/0/0
R1(config-if)# crypto map CMAP
```

- Ekkor kiírja, hogy bekapcsolt az interfészen a VPN végpont. Még nincs ekkor kapcsolat, annak kiépüléséhez az alagúton áthaladó forgalom kell. Ekkor automatikusan felveszi a kapcsolatot a túlsó végponttal.

SITE TO SITE VPN BEÁLLÍTÁSA (JOBB OLDAL)

- Először a végpontok hitelesítését kell beállítani. Létre kell hozni a túlsó végpontnak egy jelszót (meg kell egyeznie a túloldali jelszóval):

```
R2(config)# crypto isakmp key jelszo address 192.0.2.14
```

- Majd be kell állítani, hogy ezt a jelszót használja:

```
R2(config)# crypto isakmp policy 1
R2(config-isakmp)# authentication pre-share
```

- Itt a hitelesítésnek is egyeznie kell a két routeren, de a Packet Tracer csak pre-share-t tud ezért fix

SITE TO SITE VPN BEÁLLÍTÁSA (JOBB OLDAL)

- Ez után meg kell adni a kapcsolatban használt titkosítást és ha akarunk akkor a csomagok hitelesítését is (itt mindegyik lehetőség működik, de ugyanaz kell mint a másik végponton):

```
R2(config)# crypto ipsec transform-set TSET esp-aes 256 esp-sha-hmac
```

- Majd létre kell hozni egy ACL-t amellyel megadjuk, hogy milyen forgalmat akarunk beleterelni az alagútba (melyik hálózatból hová):

```
R2(config)# ip access-list extended S2SVPN
R2(config-ext-nacl)#permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
```

- Vigyázz! Ez az ACL nem azonos az előzővel! A forrás- és a célhálózatot fel kell cserélni!

SITE TO SITE VPN BEÁLLÍTÁSA (JOBB OLDAL)

- Ez után össze kell rakni az alagút tulajdonságait (az előző dián megadott ACL-t és titkosításokat rendeljük össze a végponti kapcsolattal):

```
R2(config)# crypto map CMAP 1 ipsec-isakmp
R2(config-crypto-map)# set peer 192.0.2.14
R2(config-crypto-map)# set transform-set TSET
R2(config-crypto-map)# match address S2SVPN
```

SITE TO SITE VPN BEÁLLÍTÁSA (JOBB OLDAL)

- Végül az egészet hozzárendeljük a alagút kiindulópontját jelentő interfészhez:

```
R2(config)# interface Serial0/0/0
R2(config-if)# crypto map CMAP
```

- A kapcsolat csak forgalom hatására alakul ki. Ha pinggel teszteled 4 sikertelen próbálkozás után gyanakodj csak problémára!