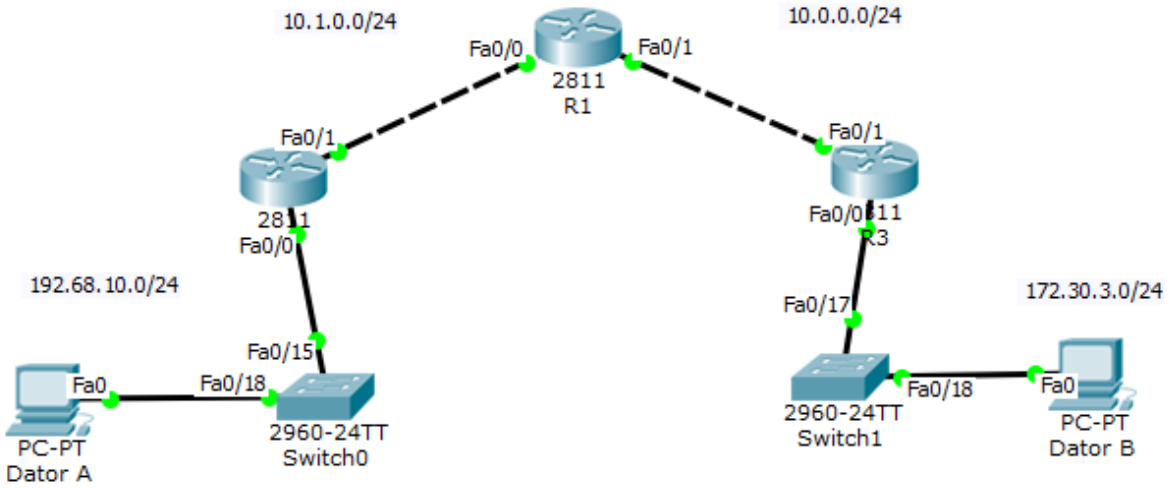
# Laboration CISCO IOS Site-2-Site VPN

I denna laboration kommer ni att konfigurera två stycken routrar till att tunnla trafik via en Site-to-site VPN-tunnel som använder IPSec.

**Gruppstorlek:** Arbete i grupp om 2 eller individuellt

**Material:** Packet Tracer är enklast då det krävs en ”enterprise” version av CISCO IOS för krypteringskommandona. **Det finns en förkonfigurerad projektfil till labben.**




**IP-konfiguration**

| Enhet | Interface | IP-adress | Nätmask | Default GW |
|---|---|---|---|---|
| R1 | Fa0/0 | 10.1.0.2 | 255.255.255.0 | - |
| | Fa0/1 | 10.0.0.1 | 255.255.255.0 | - |
| R2 | Fa0/0 | 192.168.10.1 | 255.255.255.0 | - |
| | Fa0/1 | 10.1.0.1 | 255.255.255.0 | - |
| R3 | Fa0/0 | 172.30.3.1 | 255.255.255.0 | - |
| | Fa0/1 | 10.0.0.2 | 255.255.255.0 | - |
| Dator-A | NIC | 192.168.10.2 | 255.255.255.0 | 192.168.10.1 |
| Dator-B | NIC | 172.30.3.2 | 255.255.255.0 | 172.30.3.1 |

Till laborationen finns en förkonfigurerad packet tracer fil där alla anslutningar är gjorda och alla interface har konfigurerats med IP-adresser.

1. Vi börjar med att se till så att alla enheter kan kommunicera med varandra. Då behöver vi lägga till lite statiska routes (OBS vi kommer ej att köra någon NAT för våra nätverk bakom R2 och R3).
   **På R2:**
   **`ip route 0.0.0.0 0.0.0.0 10.1.0.2`**
   (Skapar default route)
   På R3:
   **`ip route 0.0.0.0 0.0.0.0 10.0.0.1`**
   (Skapar default route)
   På R1:

**ip route 192.168.10.0 255.255.255.0 10.1.0.1**
**ip route 172.30.3.0 255.255.255.0 10.0.0.2**
(Skapar routes så att R1 kan vidarebefordra paketen rätt)

2. Kontrollera att alla enheter kan kommunicera med varandra genom att pinga Dator-B från Dator-A (eller tvärt om).
3. Skapa Site-to-Site VPN mellan R3 och R2. Poängen är att trafik mellan näten 192.168.10.0/24 och 172.30.3.0/24 ska tunnlas och krypteras mellan R3 och R2 med en VPN-tunnel som använder IP-sec.

**Vi börjar med att konfigurera R3:**

| | |
|---|---|
| **crypto isakmp enable** | Aktiverar IKE |
| **crypto isakmp policy 1** | Skapar en ISAKMP Policy |
| **authentication pre-share** | ISAKMP Policy ska använda en delad nyckel |
| **encryption 3des** | ISAKMP Policy ska använda 3des-kryptering |
| **hash sha** | ISAKMP Policy hash algoritm sha |
| **group 2** | DH group key exchange no 2 |
| **exit** | Tillbaka till global configuration mode |

**crypto isakmp key 1234 address 10.1.0.1**
Anger att delade nyckeln *1234* ska användas vid kommunikation med R2
**crypto ipsec transform-set TRANS esp-3des esp-sha-hmac**
Konfigurerar IPsec transform set och kallar den för *TRANS*
**access-list 101 permit ip 172.30.3.0 0.0.0.255 192.168.10.0 0.0.0.255**
Skapar en ACL som identifierar ”intressant” trafik. I detta fall all kommunikation från vårt lokala nät 172.30.3.0/24 som går till nätet 192.168.10.0/24. Observera att ”omvända” nätmasker används. Denna access-lista kommer vi att använda för att ange vilken trafik som ska genom vår VPN-tunnel.

| | |
|---|---|
| **crypto map CMAP 1 ipsec-isakmp** | Skapar en crypto map med namn *CMAP* |
| **match address 101** | Anger intressant trafik (access-lista 101) |
| **set peer 10.1.0.1** | Anger R2 som *peer* |

**set transform-set TRANS**
Anger transform-set till *TRANS* som definierats tidigare.

| | |
|---|---|
| **int fa 0/1** | Välj interface fa 0/1 (utgående interface) |
| **crypto map CMAP** | Applicera vår crypto map på fa 0/1 |

Nu gör vi samma sak på R2:

| | |
|---|---|
| **crypto isakmp enable** | Aktiverar IKE |
| **crypto isakmp policy 1** | Skapar en ISAKMP Policy |
| **authentication pre-share** | ISAKMP Policy ska använda en delad nyckel |
| **encryption 3des** | ISAKMP Policy ska använda 3des-kryptering |
| **hash sha** | ISAKMP Policy hash algoritm sha |
| **group 2** | DH group key exchange no 2 |
| **exit** | Tillbaka till global configuration mode |

**crypto isakmp key 1234 address 10.0.0.2**
Anger att delade nyckeln *1234* ska användas vid kommunikation med R3
**crypto ipsec transform-set TRANS esp-3des esp-sha-hmac**
Konfigurerar IPsec transform set och kallar den för *TRANS*
**access-list 101 permit ip 192.168.10.0 0.0.0.255 172.30.3.0 0.0.0.255**
Skapar en ACL som identifierar ”intressant” trafik. I detta fall all kommunikation från vårt lokala nät 192.168.10.0/24 som går till nätet 172.30.3.0/24. Observera att ”omvända”

nätmasker används. Denna access-lista kommer vi att använda för att ange vilken trafik som ska genom vår VPN-tunnel.

| | |
|---|---|
| **crypto map CMAP 1 ipsec-isakmp** | Skapar en crypto map med namn *CMAP* |
| **match address 101** | Anger intressant trafik (access-lista 101) |
| **set peer 10.0.0.2** | Anger R3 som *peer* |

**set transform-set TRANS**

Anger transform-set till *TRANS* som definierats tidigare.

| | |
|---|---|
| **int fa 0/1** | Välj interface fa 0/1 (utgående interface) |
| **crypto map CMAP** | Applicera vår crypto map på fa 0/1 |

4. Kontrollera att trafiken tunnlas.
   Först måste vi generera ”intressant” trafik. Detta gör vi genom att pinga Dator-B från Dator-A (eller tvärt om). Detta bör fungera.
   För att kontrollera att paketen verkligen kapslats in och krypterats så kör vi följande kommando på R2 eller R3:
   **show crypto ipsec sa**
   Detta kommando visar alla security associations. Och vi bör nu se ifall vi har upprättat en VPN-tunnel mellan R2 och R3 samt hur många paket som passerats. Prova att låta datorerna pinga varandra igen och upprepa show-kommandot för att se att fler paket krypterats.

**Detta skall du kunna efter genomförd labb:**

✓ Skapa site-to-site VPN mellan två routrar