# IPSec Site-to-Site VPN med OSPF - Labbrapport

## 1. Syfte

Syftet med denna labb var att konfigurera en site-to-site IPSec VPN-tunnel mellan två routers (R1 och R3) via en mellanliggande router (R2). OSPF användes som dynamiskt routingprotokoll för att möjliggöra automatisk nätverksupptäckt och ruttpropagering.

## 2. Topologi

Nätverkstopologin består av tre routrar:  
- R1 (lokalt nät 192.168.1.0/24)  
- R2 (mellanliggande router, endast vidarebefordrar trafik)  
- R3 (lokalt nät 192.168.3.0/24)  
R1 och R3 är VPN-ändpunkterna. Trafik mellan dessa nät krypteras med IPSec.

En bild som visar diagram, text, karta, linje

AI-genererat innehåll kan vara felaktigt.

## 3. Konfiguration

Nedan följer konfigurationerna från samtliga routrar.

### R1 - Running Configuration

crypto isakmp policy 10  
 encr aes 256  
 authentication pre-share  
 group 5  
 lifetime 3600  
crypto isakmp key cisco123 address 10.2.2.1  
crypto ipsec security-association lifetime seconds 1800  
crypto ipsec transform-set 50 esp-aes 256 esp-sha-hmac  
crypto map CMAP 10 ipsec-isakmp   
 set peer 10.2.2.1  
 set pfs group5  
 set security-association lifetime seconds 900  
 set transform-set 50   
 match address 101  
interface GigabitEthernet0/0/0  
 ip address 10.1.1.1 255.255.255.252  
 crypto map CMAP  
interface GigabitEthernet0/0/1  
 ip address 192.168.1.1 255.255.255.0  
router ospf 101  
 network 192.168.1.0 0.0.0.255 area 0  
 network 10.1.1.0 0.0.0.3 area 0  
access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255

### R2 - Running Configuration

interface GigabitEthernet0/0/0  
 ip address 10.1.1.2 255.255.255.252  
interface GigabitEthernet0/0/1  
 ip address 10.2.2.2 255.255.255.252  
router ospf 101  
 network 10.1.1.0 0.0.0.3 area 0  
 network 10.2.2.0 0.0.0.3 area 0

### R3 - Running Configuration

crypto isakmp policy 10  
 encr aes 256  
 authentication pre-share  
 group 5  
 lifetime 3600  
crypto isakmp key cisco123 address 10.1.1.1  
crypto ipsec security-association lifetime seconds 1800  
crypto ipsec transform-set 50 esp-aes 256 esp-sha-hmac  
crypto map CMAP 10 ipsec-isakmp   
 set peer 10.1.1.1  
 set pfs group5  
 set security-association lifetime seconds 900  
 set transform-set 50   
 match address 101  
interface GigabitEthernet0/0/0  
 ip address 10.2.2.1 255.255.255.252  
 crypto map CMAP  
interface GigabitEthernet0/0/1  
 ip address 192.168.3.1 255.255.255.0  
router ospf 101  
 network 192.168.3.0 0.0.0.255 area 0  
 network 10.2.2.0 0.0.0.3 area 0  
access-list 101 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255

## 4. Verifiering

För att verifiera VPN-tunneln användes följande kommandon:  
- show crypto isakmp sa (visar att SA är ACTIVE och i QM\_IDLE-läge)  
- show crypto ipsec sa (visar krypterade och dekrypterade paket)  
- ping mellan 192.168.1.3 och 192.168.3.3 lyckades när tunneln var uppe.

## 5. Problem och lösningar

Under labben uppstod följande problem:  
- Felmeddelande vid 'mode tunnel' i transform-set. Lösning: Ange hela kommandot på samma rad som transform-set.  
- Felaktig koppling av crypto map på fel interface (g0/0/1 istället för g0/0/0). Lösning: Ta bort från fel interface och lägg till på rätt.  
- SPI mismatch (%CRYPTO-4-RECVD\_PKT\_INV\_SPI). Lösning: Ta bort och lägga till crypto map igen för att tvinga ny SA-förhandling.

## 6. Slutsats

Labben lyckades efter att ovanstående problem lösts. VPN-tunneln är aktiv och trafik mellan 192.168.1.0/24 och 192.168.3.0/24 krypteras. OSPF gör att nätverken annonseras dynamiskt och routrarna behöver inte statiska rutter.