16 DE FEBERO DE 2026

IMPLEMENTACIÓN IPSEC VPN

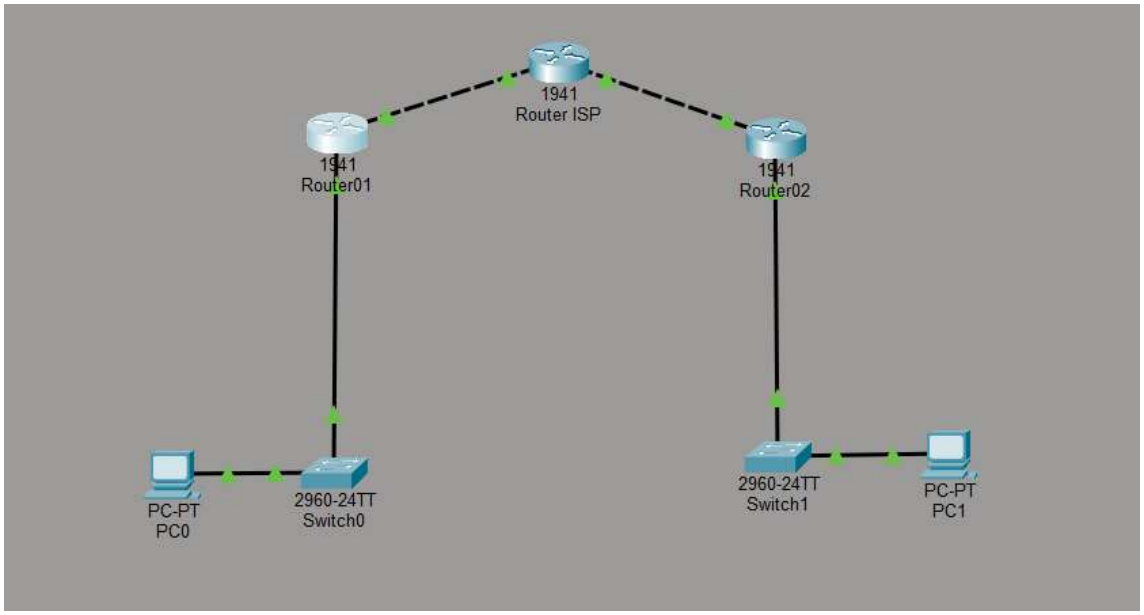
ACT 06

CAVAZOS ZACARÍAS RODOLFO 178823
UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ
CNO V: Seguridad Informática

Índice

1. Topología utilizada

- 3 routers 1941
- 2 switch 2960
- 2 PC



2. Configuración inicial

- Router 01
  - Enable
  - Conf t
  - Hostname R1
  - Interface g0/0
  - Ip address 192.168.1.1 255.255.255.0
  - No shut
  - Ip route 0.0.0.0 0.0.0.0 209.165.100.2
- Router 02
  - Enable
  - Conf t
  - Hostname R2
  - Ip address 192.168.3.1 255.255.255.0
  - No shut
  - Interface g0/0
  - Ip address 209.165.200.1 255.255.255.0
  - No shut
  - Ip route 0.0.0.0 0.0.0.0 209.165.100.2
- Router ISP
  - ENABLE
  - CONF T
  - HOSTNAME isp

- Interface g0/0
- Ip address 209.165.100.2 255.255.255.0
- No shut
- Ip rout 0.0.0.0 0.0.0.0 209.165.100.2

3. Licencia de seguridad

Para cada router:

- License boot technology-package securityk9
- Exit
- Copy run start
- Reload
- En
- Show version

4. Implementación ACL

Las ACL en implementaciones IPSec cumplen un rol fundamental al identificar el tráfico interesante que debe ser protegido mediante encapsulación y cifrado.

Para R1 (config): Access-list 100 permit ip 192.168.1 0.0.0.255 192.168.3.0 0.0.0.255

Para R2 (config): access –list 100 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255

5. Phase 01: ISAKMP policy

Para R1(config):

- Crypto isakmp policy 10
- Encryption aes 256
- Authentication pre-share
- Grpu5
- Exit
- Crypto isakmp key secretkey address 209.165.200.1

Para R2 (config):

- Crypto isakmp policy 10
- Encryption aes 256
- Authentication pre-share
- Grpu5
- Exit
- Crypto isakmp key secretkey address 209.165.200.1

6. Phase 02: IPSec transform-set

Para R1(config): crypto ipsec transform-set R1->R2 esp-aes 256 esp-sha-hmac

Para R1(config): crypto ipsec transform-set R2->R1 esp-aes 256 esp-sha-hmac

7. Mapa criptográfico

Para R1:

- R1(config)#crypto map IPSEC-MAP 10 ipsec-isakmp
- R1(config-crypto-map)#set peer 209.165.200.1
- R1(config-crypto-map)#set pfs group5

Para R2:

- R2(config)# crypto map IPSEC-MAP 10 ipsec-isakmp
- R2(config-crypto-map)# set peer 209.165.100.1 R2(config-crypto-map)#set pfs group5
- R2(config-crypto-map)#set security-association lifetime seconds 86400
- R2(config-crypto-map)#set transform-set R2->R1
- R2(config-crypto-map)#match address 100

8. Aplicación de mapa criptográfico

Para R1:

- R1(config-crypto-map)#exit
- R1(config)#int g0/0
- R1(config-if)#crypto map IPSEC-MAP

Para R2:

- R2(config-crypto-map)#exit
- R2(config)#int g0/0
- R2(config-if)#crypto map IPSEC-MAP