UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Implementación IPSec VPN

CNO V – Seguridad Informática

Lunes 16 febrero, 2026

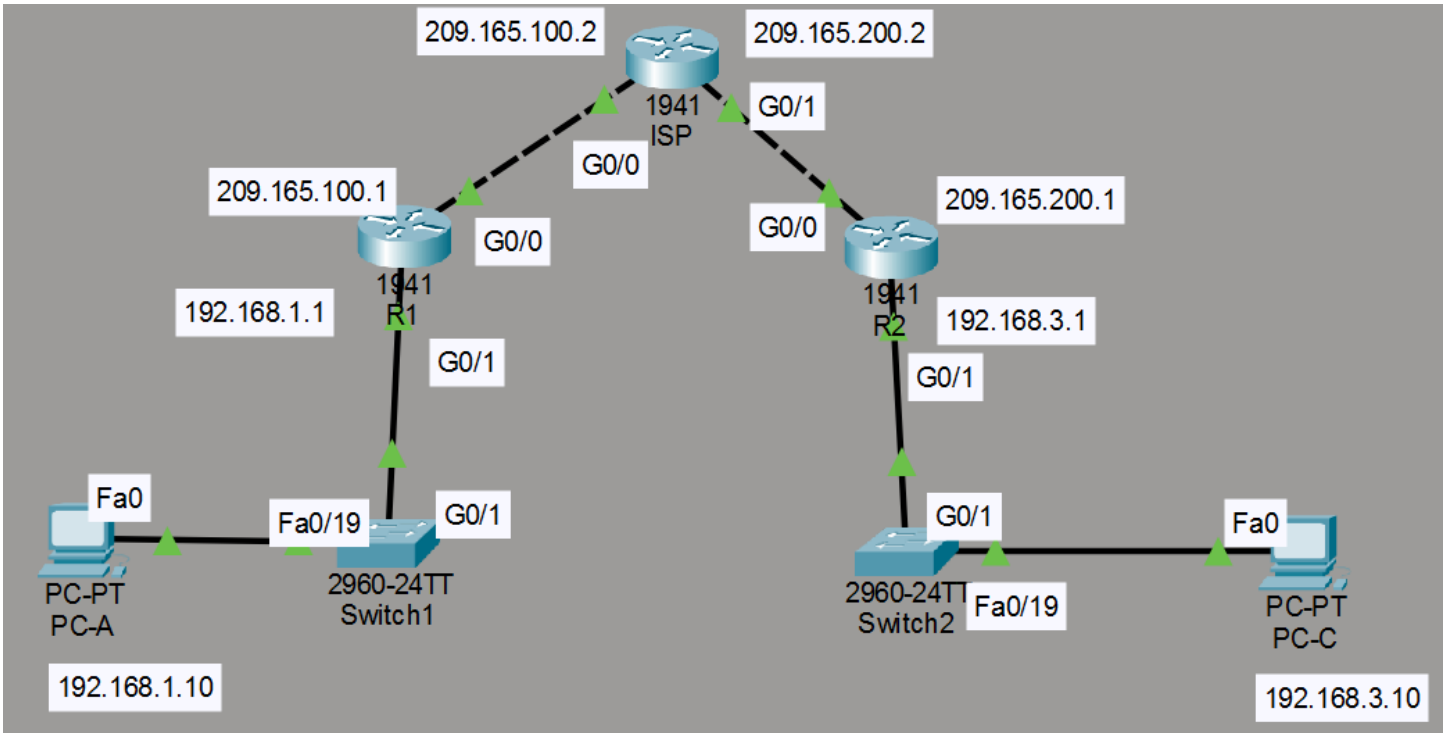
Elisa Alejandra Arellano Wratny

177339

Contenido

0. Topología

- Tres routers 1941 (ISP, R1, R2)
- Dos switch 2960 (S1, S2)
- Dos PC´s



1. Configuración inicial

Router ISP

- enable
- conf t
- hostname ISP
- interface G0/0
- ip address 209.165.100.2 255.255.255.0
- no shut
- interface G0/0
- ip address 209.165.200.2 255.255.255.0
- no shut
- ip route 0.0.0.0 0.0.0.0 209.165.100.2

Router 1

- enable
- conf t
- hostname R1
- interface G0/1
- ip address 192.168.1.1 255.255.255.0
- no shut
- interface G0/0
- ip address 209.165.100.1 255.255.255.0
- no shut
- ip route 0.0.0.0 0.0.0.0 209.165.100.2

Router 2

- enable
- conf t
- hostname R2
- interface G0/1
- 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

2. Licencia de seguridad habilitada

En cada Router:

- license boot technology-package securityK9
- exit
- copy run start
- reload
- en
- show versión

```
R2#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
R2#reload
Proceed with reload? [confirm]
System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO1941/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 64/-1(On-board/DIMM0) bit mode with ECC disabled
```

3. Implementación de ACL’s

Listas de Control de Acceso (ACL): son conjuntos de reglas de seguridad configuradas en routers, switches o firewalls que gestionan el tráfico de red permitiendo o denegando el paso de datos basándose en direcciones IP, protocolos y puertos.

R1 (config): access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255

```
R1>en
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
R1(config)#
```

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

```
R2>en
R2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#access-list 100 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
R2(config)#
```

4. Phase 01: ISAKMP policy

Cifra sólo encabezado.

R1 (config): crypto isakmp policy 10
encryption aes 256
authentication pre-share
group 5
exit
crypto isakmp key secretkey address 209.165.200.1

```
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#encryption aes 256
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 5
R1(config-isakmp)#exit
R1(config)#crypto isakmp key secretkey address 209.165.200.1
```

R2 (config): crypto isakmp policy 10
encryption aes 256
authentication pre-share
group 5
exit
crypto isakmp key secretkey address 209.165.100.1

```
R2(config)#crypto isakmp policy 10
R2(config-isakmp)#encryption aes 256
R2(config-isakmp)#authentication pre-share
R2(config-isakmp)#group 5
R2(config-isakmp)#exit
R2(config)#crypto isakmp key secretkey address 209.165.100.1
```

5. Phase 2: IPSec transform-set

Cifra encabezado y cuerpo del contenido.

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

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

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

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

6. Crear el mapa criptográfico

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

```
R1(config)#crypto map IPSEC-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R1(config-crypto-map)#set peer 209.165.200.1
R1(config-crypto-map)#set pfs group5
```

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

```
R2(config)#crypto map IPSEC-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
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
R2(config-crypto-map)#
```

7. Aplicar el mapa criptográfico

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

```
R1(config-crypto-map)#exit
R1(config)#int g0/0
R1(config-if)#crypto map IPSEC-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

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

```
R2(config-crypto-map)#exit
R2(config)#int g0/0
R2(config-if)#crypto map IPSEC-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```