UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

CNO V:Seguridad Informática

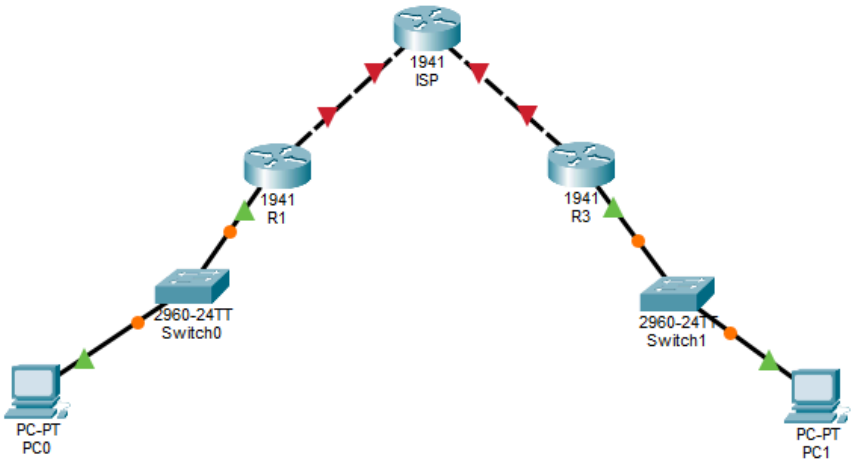
Implementación IPSec VPN

Josué Emiliano Rosales Ramírez
181760

16-02-2026

1-Topología

Para este paso, se hace uso de tres routers 1941, dos switches 2960-24TT y dos computadoras como se muestra en la siguiente imagen:



2-Configuración Inicial

Se configuran los routers por la terminal CLI, esto con el fin de utilizar comandos y permitirnos más versatilidad.

ISP

Para cada router se seguirá el mismo procedimiento, en este caso empezaremos con el ISP, que es el que estará funcionando como un puente de Internet para los demás routers.

Primero empezamos configurando desde la terminal con estos comandos *Enable* y *Config terminal*

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
```

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname ISP interface g0/1
                        ^
% Invalid input detected at '^' marker.

Router(config)#interface g0/1
Router(config-if)#ip address 209.165.200.2 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

Router(config-if)#interface g0/0
Router(config-if)#ip address 209.165.100.2 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
exit
```

Se configuran las salidas de los gigabit Ethernet g0/0 y g0/1 con sus respectivas IP's, estos serán las salidas para los otros dos routers R1 y R3.

R1

Se realizan los mismos procedimientos en R1

```
R1>enable
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#hostname R1
R1(config)#interface g0/1
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#interface g0/0
R1(config-if)#ip address 209.165.100.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#ip route 0.0.0.0 0.0.0.0 209.165.100.2
R1(config)#
```

R3

```
R3>enable
R3#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#hostname R3
R3(config)#interface g0/1
R3(config-if)#ip address 192.168.3.1 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#interface g0/0
R3(config-if)#ip address 209.165.200.1 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#ip route 0.0.0.0 0.0.0.0 209.165.200.2
R3(config)#
```

Configuración de VPN

Fase 1: Isakmp policy

Para este paso nos dirigimos a uno de los dos routers R1 y R3

El comando de la ultima linea sirve para crear una politica de seguridad de prioridad 10

```
R1>enable
R1#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#crypto isakmp policy 10
```

Se habilita la encriptación aes 256 y se habilita la autenticación pre-compartida.

```
R1(config-isakmp)#encryption aes 256
R1(config-isakmp)#authentication pre-share
```

escribimos el group 5 para el intercambio de claves de Diffie-Hellman

```
R1(config-isakmp)#authentic
R1(config-isakmp)#group 5
```

Finalmente asignamos una clave secreta compartida con su otro router R3

```
R1(config-isakmp)#exit
R1(config)#crypto isakmp key secretkey address 209.165.200.1
```

Fase 2: Ipsec transform set

Consecuentemente, definimos el conjunto de transformación de cifrado aes y autenticación sha

```
R1(config)#crypto ipsec transform-set R1-R3 esp-aes 256 esp-sha-hmac
```

Y creamos un mapa criptográfico con secuencia 10 que sirve para gestionar múltiples túneles VPN en un mismo router de manera organizada.

```
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.
```

Y definimos al peer del router que en este caso seria hacia R3

```
        and a valid access list have been conf
R1(config-crypto-map)#set peer 209.165.200.1
```

Establecemos el mismo conjunto de transformación para R3 con:

```
R1(config-crypto-map)#set transform-set R1-R3
```

Crear el mapa criptográfico

Y establecemos el mapa criptografico para g0/0

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

Se define el trafico que debe ser protegido (ACL)

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

Aplicar todo a R3

Terminado con R1, pasamos a R3.

Se realiza la misma serie de comandos pero cambiando la dirección IP para compartir las claves con su peer R1

```
R3(config)#crypto isakmp key secretkey address 209.165.100.1
```

Una vez llegado a este punto, hemos terminado y configurado el túnel VPN a través de IPSEC

```
R3(config-if)#exit
R3(config)#access-li
R3(config)#access-list 100 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
R3(config)#do wr
Building configuration...
[OK]
```

Pruebas y verificación

Para probar el funcionamiento hay de dos formas, una por un ping desde una computadora y otra con el comando *SHOW CRYPTO IPSEC SA*

Realizamos un ping de PC0 a PC1

Y se puede comprobar el funcionamiento del túnel pues todos los paquetes fueron recibidos correctamente.

```
C:\>ping 192.168.3.10

Pinging 192.168.3.10 with 32 bytes of data:

Reply from 192.168.3.10: bytes=32 time<1ms TTL=126
Reply from 192.168.3.10: bytes=32 time=1ms TTL=126
Reply from 192.168.3.10: bytes=32 time<1ms TTL=126
Reply from 192.168.3.10: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.3.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Al igual que podemos ver el STATUS activo del crypto

```
R1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
209.165.200.1   209.165.100.1   QM_IDLE           1038    0 ACTIVE


IPv6 Crypto ISAKMP SA
```

Conclusión

Como se pudo ver, hay un proceso para lograr un tráfico cifrado, con el fin de proteger los datos y de limitar los accesos.

Con esta pequeña práctica pude ver cómo se aplican los cifrados e intercambios de clave y como los Routers y switches responden.