UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

ACTIVIDAD 06: Implementación IPSec VPN

Carrera: ITI

Asignatura: CNO V Seguridad informática

Pablo de Jesús Salazar Hernández - 171580

Mtro. Servando López Contreras

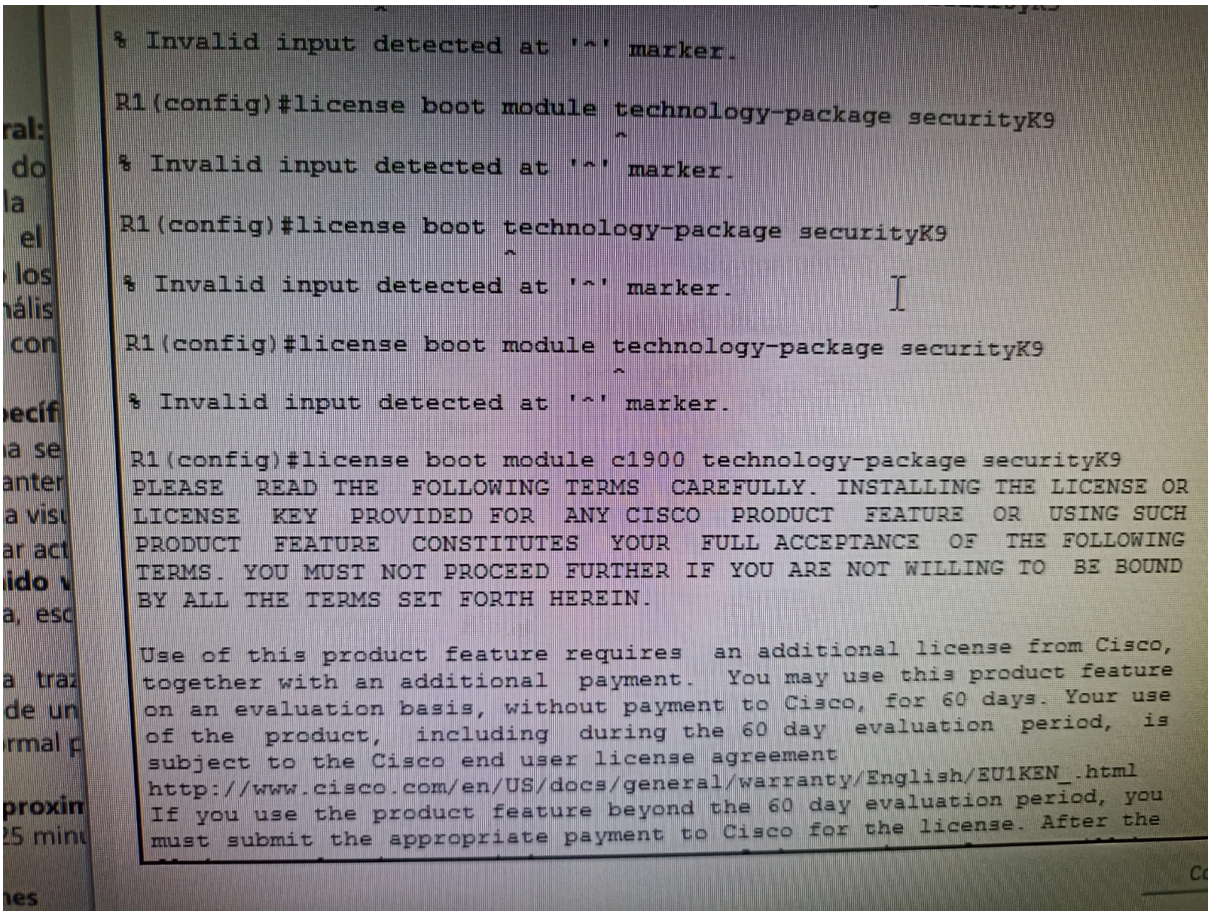
16/02/2026

1. Configuración inicial

Se configuraron los parámetros básicos de los routers (hostname, direcciones IP en interfaces LAN y WAN, rutas estáticas o por defecto y activación de interfaces). Esto permitió la conectividad entre las redes antes de implementar la VPN.

2. Licencia de seguridad habilitada

Se habilitó la licencia de seguridad (Security/K9) en los routers para permitir el uso de funciones criptográficas necesarias para configurar IPSec VPN.



```
R1>show version
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.1(4)M4, RELEASE
SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 23-Feb-11 14:19 by pt_team

ROM: System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
cisco1941 uptime is 18 seconds
System returned to ROM by power-on
System image file is "flash0:c1900-universalk9-mz.SPA.151-1.M4.bin"
Last reload type: Normal Reload

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
 --More--
```

3. Implementación de ACL

Se creó una lista de control de acceso (ACL) extendida para definir el tráfico interesante que será cifrado. Esta ACL permite el tráfico entre la red 192.168.1.0/24 y 192.168.3.0/24.

```
R1>enable
R1#conf 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
```

4. Phase 01: ISAKMP policy

Se configuró la política ISAKMP para establecer el canal seguro inicial. Se definieron parámetros como el método de autenticación (pre-shared key), algoritmo de encriptación, hash y grupo Diffie-Hellman.

```
R2(config)#crypto isa
R2(config)#crypto isakmp key secr address 209.165.100.1
R2(config)#crypto ipsec transform-set R2->R1 esp-aes 256 esp-sha-hmac
R2(config)#
```

5. Phase 02: IPSec transform-set

Se creó el transform-set para definir cómo se protegerán los datos, especificando el protocolo de cifrado (AES) y el algoritmo de integridad.

```
R1(config-if)#ip address 209.165.100.1 255.255.255.0
R1(config-if)#exit
R1(config)#crypt
R1(config)#crypto ips
R1(config)#crypto ipsec trams
R1(config)#crypto ipsec trans
R1(config)#crypto ipsec transform-set R1
R1(config)#crypto ipsec transform-set R1->R2 es
R1(config)#crypto ipsec transform-set R1->R2 esp
R1(config)#crypto ipsec transform-set R1->R2 esp
R1(config)#crypto ipsec transform-set R1->R2 esp
R1(config)#crypto ipsec transform-set R1->R2 esp
R1(config)#crypto ipsec transform-set R1->R2 esp
R1(config)#crypto ipsec transform-set R1->R2 esp
R1(config)#crypto ipsec transform-set R1->R2 esp
R1(config)#crypto ipsec transform-set R1->R2 esp-ae
R1(config)#crypto ipsec transform-set R1->R2 esp-aes 256 esp
R1(config)#crypto ipsec transform-set R1->R2 esp-aes 256 esp-sh
R1(config)#crypto ipsec transform-set R1->R2 esp-aes 256 esp-sha-hmac
R1(config)#crypto map
R1(config)#crypto map IPS
R1(config)#crypto map IPSEC-MAP 10 I
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)#
```

6. Crear el mapa criptográfico

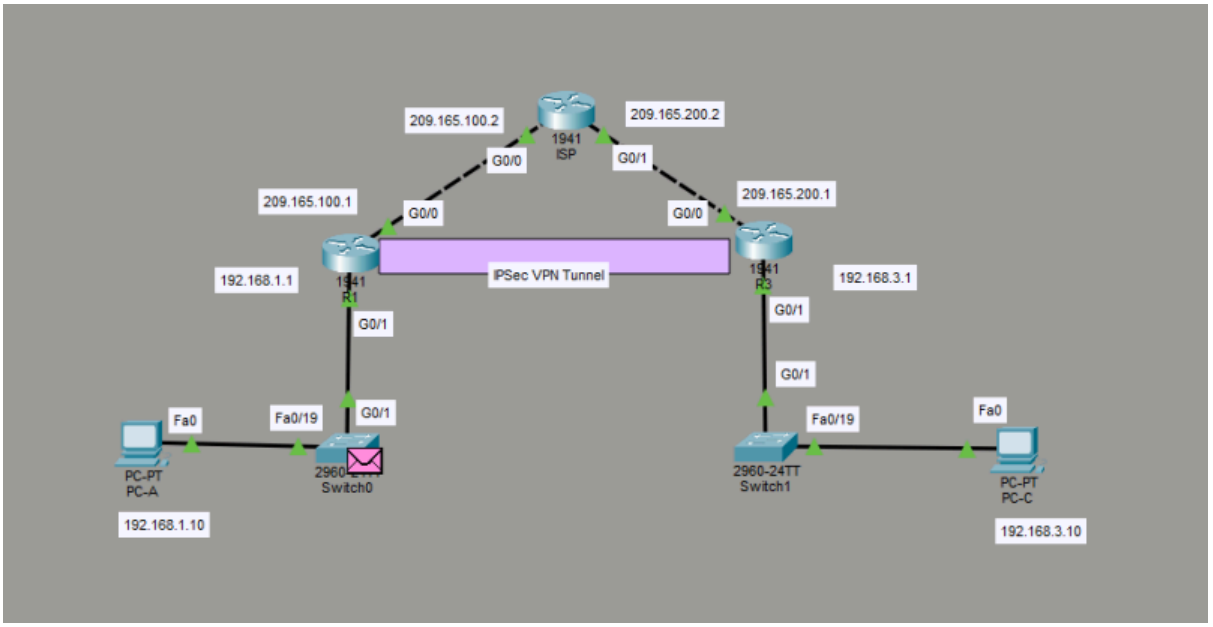
Se configuró el crypto map asociando la ACL, el peer remoto (IP pública del otro router) y el transform-set. Esto une todos los parámetros de seguridad definidos previamente.

```
R2(config)#crypto map IPSE
R2(config)#crypto map IPSEC-MAP 10 i
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 gr
R2(config-crypto-map)#set pfs group5
R2(config-crypto-map)#set secir
R2(config-crypto-map)#set secur
R2(config-crypto-map)#set security-association lof
R2(config-crypto-map)#set security-association lif
R2(config-crypto-map)#set security-association lifetime sec
R2(config-crypto-map)#set security-association lifetime seconds 86400
R2(config-crypto-map)#set trans
R2(config-crypto-map)#set transform-set R2->R1
R2(config-crypto-map)#match add
R2(config-crypto-map)#match address 100
R2(config-crypto-map)#
```

7. Aplicar el mapa criptográfico

Finalmente, el crypto map se aplicó a la interfaz WAN del router (G0/0). Esto activa el túnel IPSec para el tráfico que coincida con la ACL.

```
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
R2(config-if)#
```


209.165.100.2
1941
ISP
209.165.200.2
G0/0
G0/1
209.165.100.1
G0/0
G0/0
209.165.200.1
192.168.1.1
1941
R1
IPSec VPN Tunnel
1941
R3
192.168.3.1
G0/1
G0/1
G0/1
Fa0
Fa0/19
G0/1
Fa0/19
Fa0
PC-PT
PC-A
2960-24TT
Switch0
2960-24TT
Switch1
PC-PT
PC-C
192.168.1.10
192.168.3.10