Aplicación de IPSec y VPN

Rodríguez Morin Estefano Alessandro

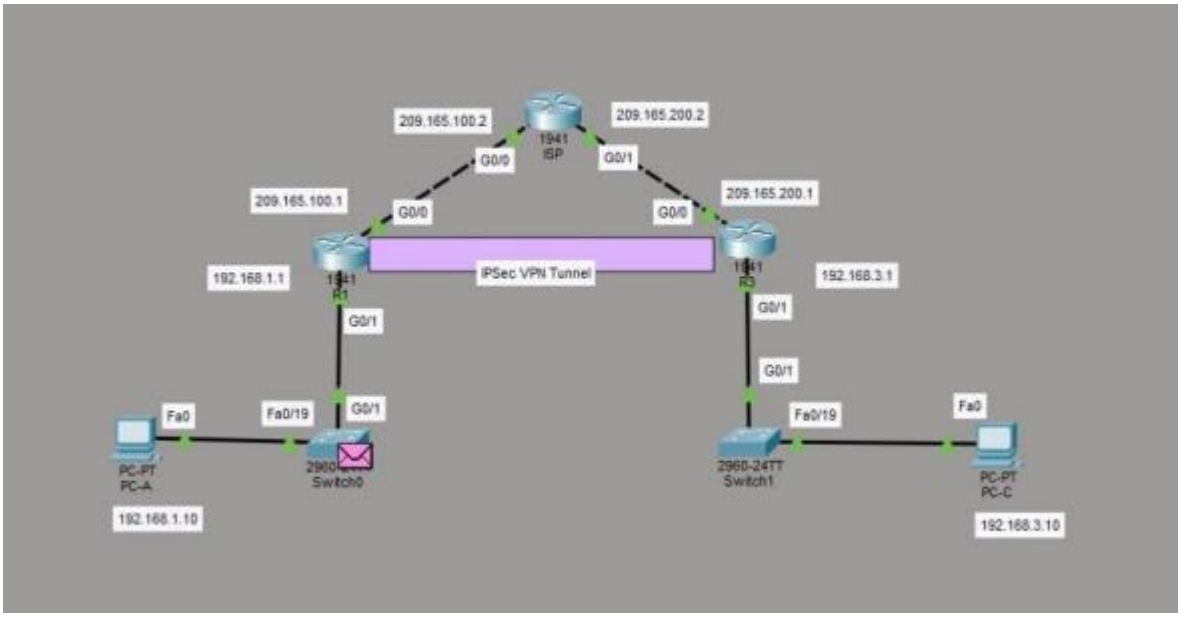
178584

CNO V: Seguridad Informática

16/02/2026

Introducción

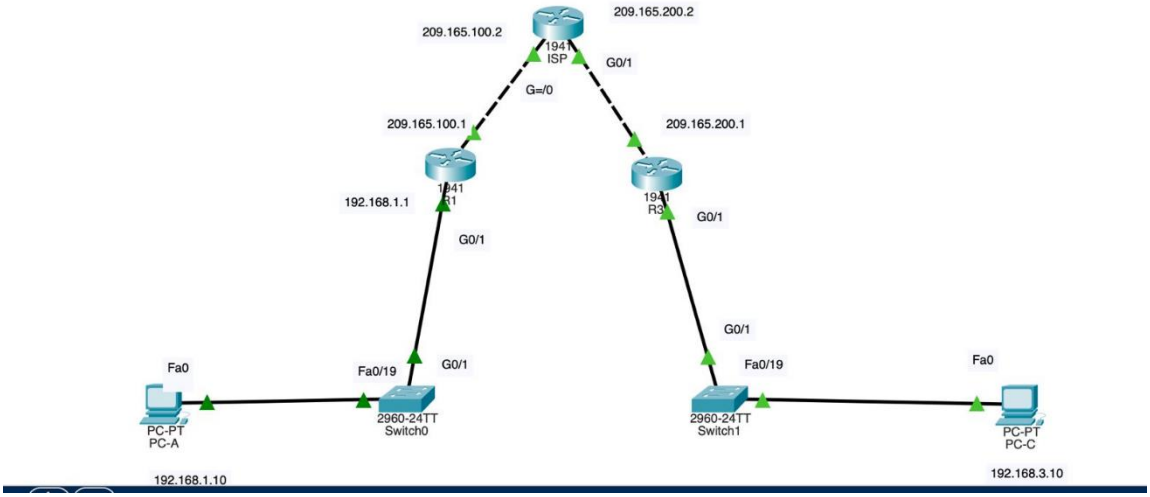
El objetivo de esta práctica es integrar los servicios de seguridad de Cisco para establecer un canal de comunicación protegido sobre una infraestructura pública. La metodología incluye la configuración de la **Fase 1 (ISAKMP)** y la **Fase 2 (IPsec)**, permitiendo una comprensión profunda de cómo los protocolos de seguridad transforman el tráfico ordinario en datos cifrados. Mediante la aplicación de **Transform Sets** y ACLs, el estudiante logrará dominar la protección de infraestructuras críticas en redes modernas.



Pasos a seguir

1. **Configuración inicial de equipo**
2. **Activar paquete de seguridad (licencia de seguridad habilitada)**
3. **Implementación de ACLS**
4. **4) Phase 01: ISAKMP POLICY**
5. **Phase 02: Ipsec transform set**
6. **Crear el mapa criptográfico**
7. **Aplicar el mapa criptográfico**

Topología


209.165.100.2
209.165.200.2
1941
ISP
G0/1
G=/0
209.165.100.1
209.165.200.1
192.168.1.1
1941
R1
1941
R3
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

Configuración para R1

Comandos utilizados:

1. Enable
2. Config T
3. Hostname R1
4. Int G0/1
    - Ip Add 192.168.1.1 255.255.255.0
    - No Shut Int G0/0
    - Ip Add 209.165.100.1 255.255.255.0
    - No Shut
    - Exit
5. Ip Route 0.0.0.0 0.0.0.0 209.165.100.2

```
ACCEPT? [yes/no]: yes
% use 'write' command to make license boot config take effect on next boot

R1(config)#: %IOS_LICENSE_IMAGE_APPLICATION-6-LICENSE_LEVEL: Module name = C1900 Next reboot l
License = securityk9

R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
reload
System configuration has been modified. Save? [yes/no]:yes
Building configuration...
[OK]
Proceed with reload? [confirm]c
R1#confirm
Translating "confirm"...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer address

R1#Enable
R1#Config T
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#Hostname R1
R1(config)#Int G0/1
R1(config-if)#Ip Add 192.168.1.1 255.255.255.0
R1(config-if)#No Shut

R1(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
Int G0/0
R1(config-if)#Ip Add 209.165.100.1 255.255.255.0
R1(config-if)#No Shut

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
Exit
R1(config)#Ip Route 0.0.0.0 0.0.0.0 209.165.100.2
```

ISP

Comandos utilizados:

1. hostname ISP
2. interface g0/1
3. ip address 209.165.200.2 255.255.255.0
4. no shutdown
5. interface g0/0
6. ip address 209.165.100.2 255.255.255.0
7. no shutdown
8. exit

```
Router(config-if)#Config T
%Invalid hex value
Router(config)#Hostname R3
R3(config)#Int G0/1
R3(config-if)#Hostname Isp
Isp(config)#Int G0/1
Isp(config-if)#Ip Add 209.165.200.2 255.255.255.0
Isp(config-if)#No Shut

Isp(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
Int G0/0
Isp(config-if)#Ip Add 209.165.100.2 255.255.255.0
Isp(config-if)#No Shut

Isp(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
```

Configuración para R2

Comandos utilizados:

6. Enable
7. Config T
8. Hostname R1
9. Int G0/1
    - Ip Add 192.168.1.1 255.255.255.0
    - No Shut Int G0/0
    - Ip Add 209.165.100.1 255.255.255.0
    - No Shut
    - Exit
10. Ip Route 0.0.0.0 0.0.0.0 209.165.100.2

```
Router(config-if)#Config T
%Invalid hex value
Router(config)#Hostname R3
R3(config)#Int G0/1
R3(config-if)#Ip Add 192.168.3.1 255.255.255.0
R3(config-if)#No Shut

R3(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
Int G0/0
R3(config-if)#Ip Add 209.165.200.1 255.255.255.0
R3(config-if)#No Shut

R3(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
R3(config)#Ip Route 0.0.0.0 0.0.0.0 209.165.200.2
R3(config)#Int G0/0
R3(config-if)#Ip Route 0.0.0.0 0.0.0.0 209.165.200.2
R3(config)#EXIT
```

Licencia de seguridad

Para utilizar el paquete securityk9, se tuvo que activar la licencia de seguridad mediante el uso del siguiente comando:
license boot module c1900 technology-package securityk9

Una vez hecho esto, se hizo un reinicio del sistema (reload) para la aplicación de los cambios.

Implementación de ACL's

Se configuró una lista de control de acceso (ACL) para identificar el tráfico interesante entre las redes LAN 192.168.1.0/24 y 192.168.3.0/24, el cual será protegido por IPSec.

Fase 1: ISAKMP policy

Para R1:

```
R1(config)#crypto isakmp  key secretkey address 209.165.200.1
R1(config)#cry
R1(config)#crypto ips
R1(config)#crypto ipsec tra
R1(config)#crypto ipsec transform-set R1-R3 esp-aes 256 esp-sha-hmac
R1(config)#cry
R1(config)#crypto map IPSEC-MAP 10 ipse
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
% Incomplete command.
R1(config-crypto-map)#set peer 209.165.200.1
R1(config-crypto-map)#set pfs grou
R1(config-crypto-map)#set pfs group5
R1(config-crypto-map)#set sec
R1(config-crypto-map)#set security-association life
R1(config-crypto-map)#set security-association lifetime seco
R1(config-crypto-map)#set security-association lifetime seconds 86400
R1(config-crypto-map)#set tra
R1(config-crypto-map)#set transform-set R1-R3
R1(config-crypto-map)#ma
R1(config-crypto-map)#match ad
R1(config-crypto-map)#match address 100
R1(config-crypto-map)#exit
R1(config)#int
R1(config)#interface gig
R1(config)#interface gigabitEthernet 0/0
R1(config-if)#cry
R1(config-if)#crypto ma
R1(config-if)#crypto map IPSEC-MAP
*Jan  3 07:16:26.786: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config-if)#exit
R1(config)#acc
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)#do wr
Building configuration...
[OK]
```

Para R3:

```
R3(config-crypto-map)#set peer 209.165.100.1
R3(config-crypto-map)#set pfs gro
R3(config-crypto-map)#set pfs group5
R3(config-crypto-map)#set sec
R3(config-crypto-map)#set security-association lifeti
R3(config-crypto-map)#set security-association lifetime second
R3(config-crypto-map)#set security-association lifetime seconds 86400
R3(config-crypto-map)#set tra
R3(config-crypto-map)#set transform-set R3-R1
R3(config-crypto-map)#mat
R3(config-crypto-map)#match ad
R3(config-crypto-map)#match address 100
R3(config-crypto-map)#exi
R3(config-crypto-map)#exit
R3(config)#inte
R3(config)#interface gi
R3(config)#interface gigabitEthernet 0/0
R3(config-if)#cry
R3(config-if)#crypto map IPSEC-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R3(config-if)#exi
R3(config-if)#exit
R3(config)#ac
R3(config)#access-list 100 pe
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]
```

Antes de que los datos puedan viajar cifrados, es necesario establecer un marco de confianza entre los extremos del túnel. Para ello, utilizamos una política de ISAKMP que estandariza el uso de claves pre-compartidas (PSK) y niveles de cifrado de grado industrial. Este proceso asegura que solo los dispositivos autorizados, en este caso el router con la IP 209.165.200.1, puedan negociar la asociación de seguridad (SA).

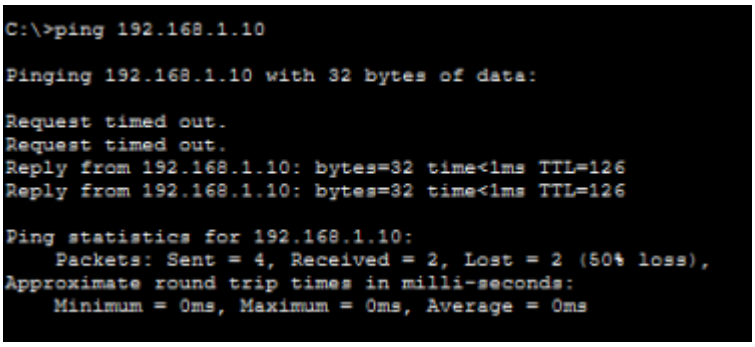
Configuración de mapa Criptográfico

```
R1#enable
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#no crypto map MAPA_VPN 10 ipsec-isakmp
Crypto-map mymap is in use by interface(s): Gig0/0,
Please remove the crypto map from the above interface(s) first
R1(config)#no crypto map MAPA_VPN 10 ipsec-isakmp
Crypto-map mymap is in use by interface(s): Gig0/0,
Please remove the crypto map from the above interface(s) first
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface g0/0
R1(config-if)#no crypto map MAPA_VPN
%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
R1(config-if)#exit
R1(config)#no crypto map MAPA_VPN 10 ipsec-isakmp
R1(config)#crypto map MAPA_VPN 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 transform-set MIS_DATOS_SEGUROS
R1(config-crypto-map)#match address 110
R1(config-crypto-map)#exit
R1(config)#interface g0/0
R1(config-if)#crypto map MAPA_VPN
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config-if)#exit
```

Esta secuencia de comandos es paso final para el armado de seguridad en el router R1. Lo que se hace aquí es crear el Crypto Map, donde le decimos a R1 a quién debe enviarle la información (el router R3), qué nivel de seguridad debe usar para encapsular los datos y, finalmente, qué archivos o mensajes específicos son los que deben viajar protegidos. Al terminar, entramos a la conexión física de internet y "encendemos" el mapa; en ese momento, el router nos confirma con un mensaje que el sistema de protección ya está activo y vigilando el tráfico. El mismo proceso se repite para R3.

Comprobación de resultados:



Esta imagen confirma que el túnel VPN funciona correctamente. Es normal que los primeros mensajes den error (Request timed out) mientras los routers “negocian” la seguridad y activan el cifrado; sin embargo, una vez establecida la conexión, los paquetes fluyen sin problemas hacia el destino. Este resultado es la prueba final de que toda nuestra configuración de seguridad está activa y protegiendo los datos en tránsito.

Conclusión

Esta actividad permite verificar como **ISAKMP** e **IPsec** transforman una red pública insegura en un canal privado y confiable para la comunicación con cifrado de datos. El éxito de la práctica no solo se refleja en la conectividad final lograda mediante el ping, sino en la correcta orquestación de la criptografía y las políticas de acceso para proteger la integridad de los datos. Este ejercicio refuerza que una VPN bien configurada es una herramienta fundamental en la ciberseguridad moderna para interconectar sedes remotas de forma eficiente y protegida.