Implementación de VPN IPSec

Mauricio Josafat Salinas Carrillo
Profesor: Servando López Contreras
15 de febrero de 2026

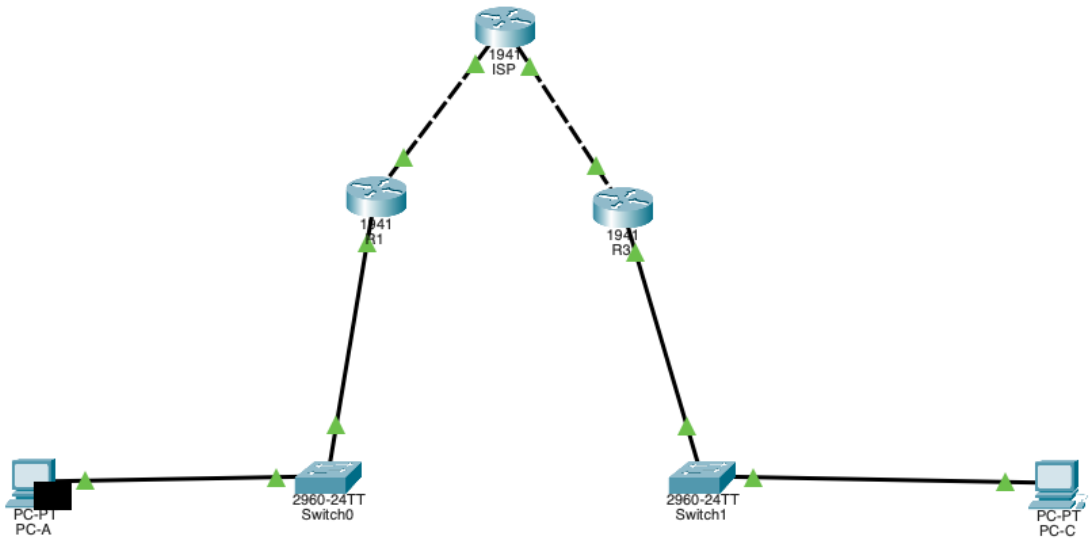
1. Objetivo de la Práctica

El objetivo principal de esta práctica fue configurar una red privada virtual (VPN) utilizando el protocolo IPSec entre dos sucursales simuladas (Router R1 y Router R3). La finalidad es permitir que dos redes LAN privadas (`192.168.1.0/24` y `192.168.3.0/24`) se comuniquen de manera segura y encriptada a través de una red pública insegura (simulada por el router ISP).

2. Topología de Red

Se diseñó una topología triangular compuesta por:

- **3 Routers:** R1 (Sucursal A), R3 (Sucursal B) e ISP (Internet).
- **2 Switches:** Para la distribución en las LAN.
- **2 PCs:** PC-A y PC-C para pruebas de conectividad de extremo a extremo.



3. Desarrollo de la Práctica

3.1 Configuración Base y Enrutamiento

Inicialmente, se configuraron las interfaces GigabitEthernet con direccionamiento IPv4 y se establecieron rutas estáticas predeterminadas (`ip route 0.0.0.0 0.0.0.0 [IP_ISP]`) para simular el acceso a Internet.

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(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)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

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

R1(config-if)#exit
R1(config)#interface g0/0
R1(config-if)#ip address 209.165.100.1 255.255.255.0
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

R1(config-if)#exit
R1(config)#ip route 0.0.0.0 0.0.0.0 209.165.100.2
R1(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

R1(config)#ping 209.165.200.1
          ^
% Invalid input detected at '^' marker.

R1(config)#do ping 209.165.200.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.1, timeout is 2 seconds:
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 0/3/10 ms

R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#ping 209.165.200.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
R1(config)#crypto map MAPA_VPN 10 ipsec-isk
```

3.2 Desafío Técnico: Activación de Licencias de Seguridad

Al intentar configurar los parámetros de la VPN, el router (modelo 1941) arrojó errores de "Invalid input" al ingresar comandos como `crypto map`.

Diagnóstico:

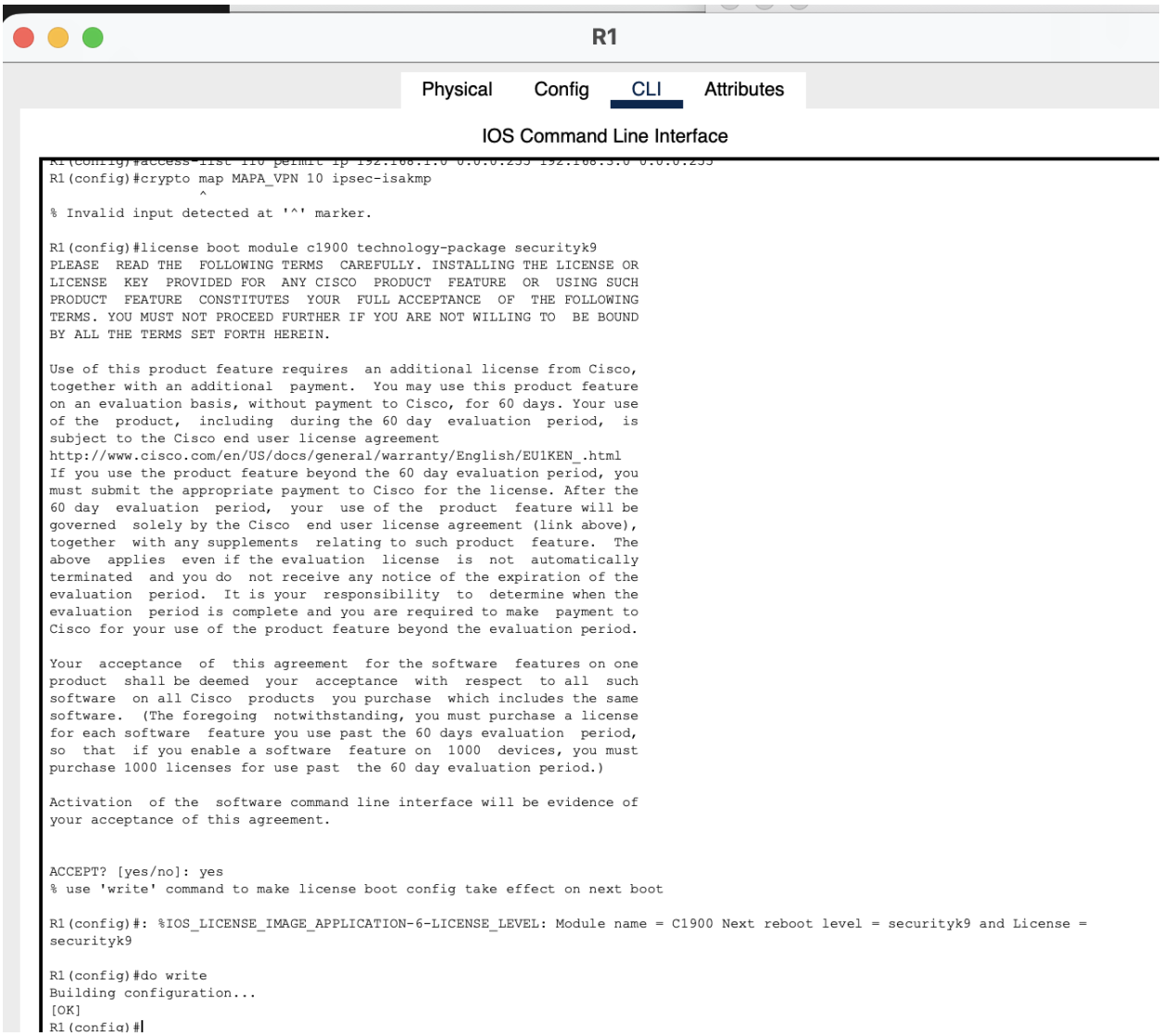
Se identificó que los routers venían con la licencia base (`ipbasek9`), la cual no incluye módulos de criptografía.

Solución:

Fue necesario activar el paquete de tecnología de seguridad mediante el comando:

license boot module c1900 technology-package securityk9

Posteriormente, se aceptaron los términos de licencia, se guardó la configuración y se reinició el equipo (`reload`) para aplicar los cambios.



3.3 Configuración de IPSec (Fase 1 y Fase 2)

Una vez activa la licencia, se procedió a la configuración criptográfica en ambos routers (R1 y R3):

1. **ACL (Lista de Acceso):** Se definió el tráfico "interesante" (de LAN a LAN).
2. **Política ISAKMP (Fase 1):** Encriptación AES, Hash SHA, Autenticación Pre-Shared, Grupo Diffie-Hellman 2.
3. **Transform Set (Fase 2):** Algoritmos para proteger los datos (ESP-AES, ESP-SHA-HMAC).
4. **Crypto Map:** Vinculación de la ACL, el peer remoto y el transform set a la interfaz WAN.

```
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)#
```

3.4 Resolución de Conflictos en R1

Durante la configuración de R1, se presentaron errores de sincronización y tipeo. Al intentar corregir el mapa criptográfico borrándolo, el sistema arrojó el error: "Crypto-map mymap is in use by interface..."

Solución Implementada: Se siguió el procedimiento correcto para modificación:

1. Ingresar a la interfaz `g0/0` y remover el mapa (`no crypto map...`).
2. Borrar el mapa globalmente.
3. Recrear el mapa con la sentencia `match address 110` correcta.
4. Reaplicar el mapa a la interfaz.

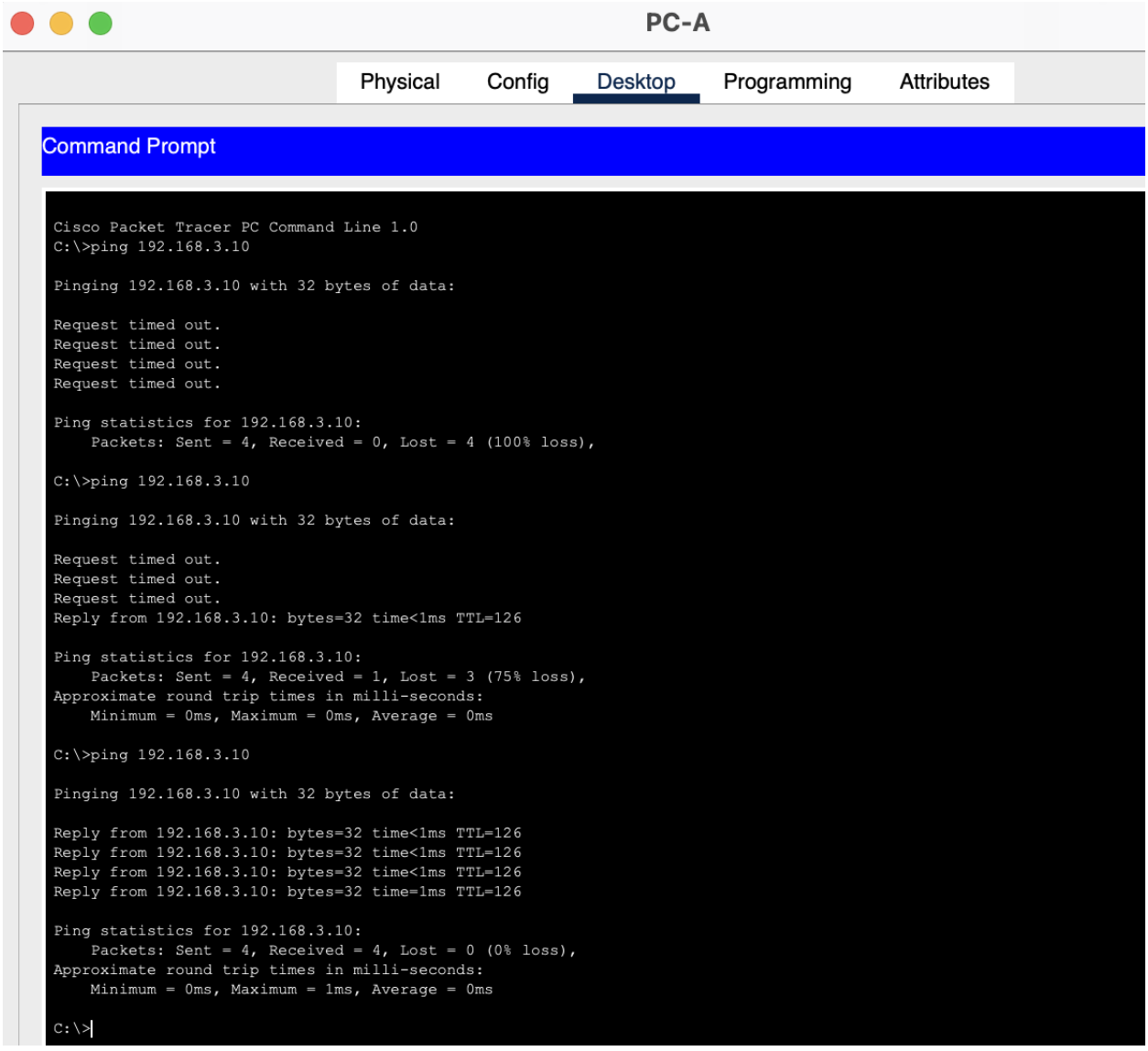
```
R1>enable
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

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
R1(config)#
```

4. Verificación y Resultados

4.1 Prueba de Conectividad (Ping)

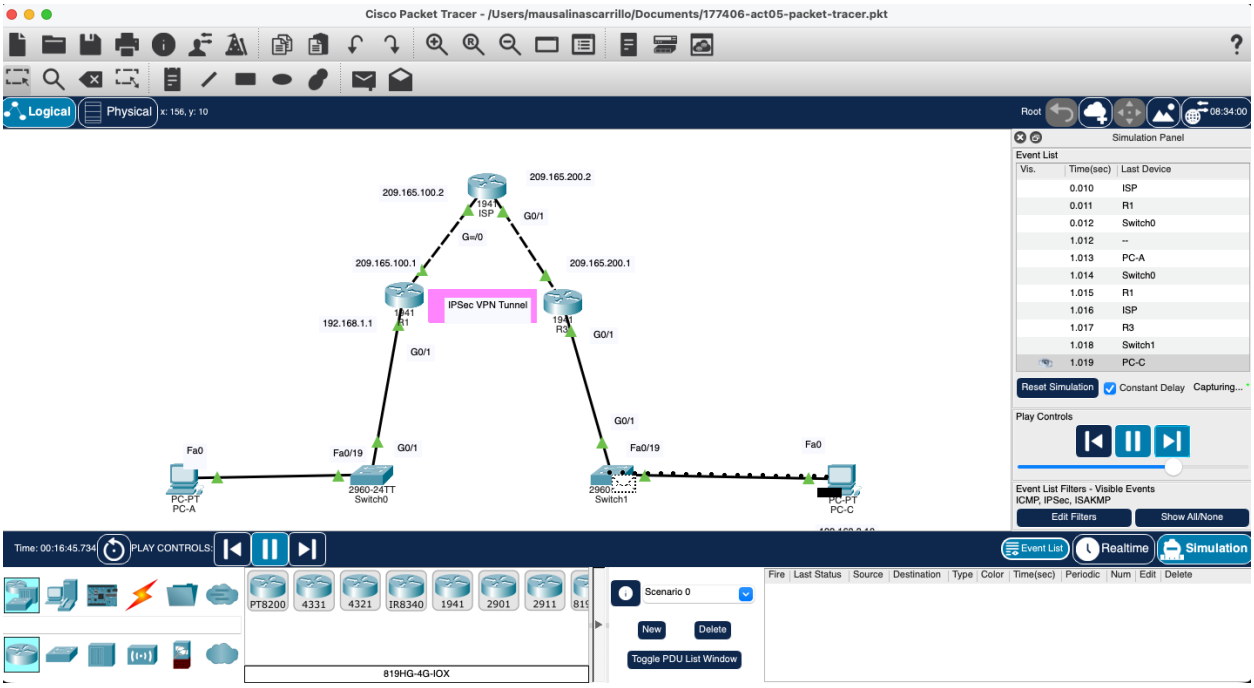
Se realizó un ping desde la PC-A (192.168.1.10) hacia la PC-C (192.168.3.10).

- **Observación:** Los primeros paquetes mostraron "Request timed out" debido al proceso de negociación de claves (IKE) y ARP.
- **Resultado:** A partir del tercer paquete, se obtuvo respuesta exitosa ("Reply from..."), confirmando el establecimiento del túnel.



4.2 Verificación Visual (Simulation Mode)

Utilizando el modo de simulación de Packet Tracer, se verificó visualmente el flujo de paquetes. Se observó cómo los paquetes ICMP eran encapsulados en paquetes ESP (IPSec) al transitar por el router ISP, garantizando que la información viajaba encriptada.



5. Conclusión

La práctica demostró exitosamente la implementación de una VPN Site-to-Site. Se aprendió la importancia de verificar las licencias del IOS (`securityk9`) antes de iniciar configuraciones avanzadas y la necesidad de seguir un orden estricto al modificar mapas criptográficos que están activos en interfaces. El túnel IPSec funciona correctamente, asegurando la confidencialidad de los datos entre las dos sucursales simuladas.