16 DE FEBRERO DE 2026

ACTIVIDAD 06

IMPLEMENTACIÓN DE UNA IPSEC VPN EN PACKET TRACER

CAROL ELIZABETH CORTES BELTRAN
UNIVERSIDAD POLITECNICA DE SAN LUIS POTOSI
Seguridad Informática

Contenido

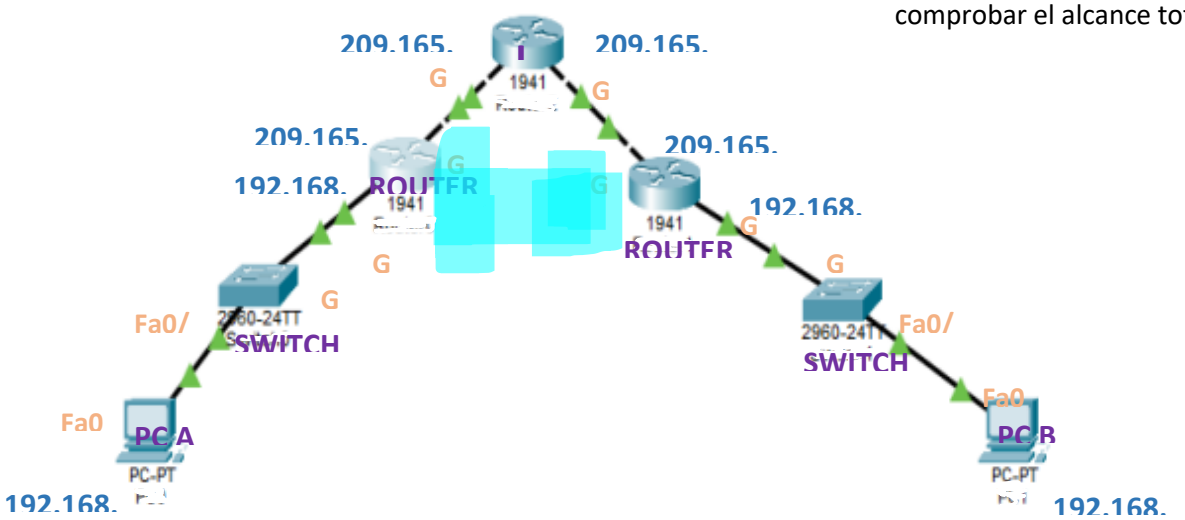
Objetivo de la Práctica

El objetivo principal de esta práctica es diseñar e implementar una **VPN (Red Privada Virtual) de sitio a sitio (Site-to-Site)** empleando el protocolo **IPSec** sobre routers Cisco 1941. El fin es establecer un túnel seguro y cifrado que permita la comunicación transparente y confidencial entre dos redes locales (192.168.1.0/24 y 192.168.3.0/24) a través de una red pública insegura (simulada por un router ISP). De esta manera, se busca garantizar la integridad y confidencialidad de los datos transmitidos, replicando un escenario corporativo real donde se interconectan sedes remotas de forma protegida.

Topología implementada

El enrutador del proveedor actuó como puente para emular la conexión a la red pública.

- **Equipos de red**: R2 (Sede Principal), R3 (Sede Secundaria) e ISP (Proveedor).
- **Dos switches**: Para el tendido de las redes internas.
- **Dos terminales**: PC-A y PC-B para comprobar el alcance total.



Desarrollo

Configuración Primaria y Protocolos de Enrutamiento

Inicialmente, se realizó la configuración básica de cada router, asignando direcciones IP a las interfaces GigabitEthernet y estableciendo rutas estáticas por defecto para simular el acceso a la red pública.

Configuración de R1:

interface g0/1

ip address 192.168.1.1 255.255.255.0

no shutdown

interface g0/0

ip address 209.165.100.1 255.255.255.0

no shutdown

ip route 0.0.0.0 0.0.0.0 209.165.100.2

```
Router>enable
Router#conf
Router#configure
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int g0/0
Router(config-if)#ip address 209.165.100.1 255.255.255.0
Router(config-if)#no sh
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
Router(config)#int g0/1
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shu
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)#exit
Router(config)#ip route 0.0.0.0 0.0.0.0 209.165.100.2
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

Configuración del ISP:

interface g0/0

ip address 209.165.100.2 255.255.255.0

no shutdown

interface g0/1

ip address 209.165.200.2 255.255.255.0

no shutdown

```
Router>enable
Router#conf t
Router#conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int g0/1
Router(config-if)#ip address 209.165.200.2 255.255.255.0
Router(config-if)#no sh
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
exit
Router(config)#int te
Router(config)#int g0/0
Router(config-if)#ip address 209.165.100.2 255.255.255.0
Router(config-if)#no shut
Router(config-if)#no shutdown

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

Configuración de R3:

interface g0/1

ip address 192.168.3.1 255.255.255.0

no shutdown

interface g0/0

ip address 209.165.200.1 255.255.255.0

no shutdown

ip route 0.0.0.0 0.0.0.0 209.165.200.2

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int g0/0
Router(config-if)#ip add
Router(config-if)#ip address 209.165.200.1 255.255.255.0
Router(config-if)#no sh
Router(config-if)#no shutdown

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

Verificación de Conectividad Básica

Antes de proceder con la configuración VPN, se verificó la conectividad entre extremos:

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

Configuración de IPSec

Política ISAKMP (Fase 1)

Se definieron los parámetros para el establecimiento del canal seguro:

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

```
Router#conf
Router#configure
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
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
R1(config)#crypto ipsec transform-set R1-R3 esp-aes 256 esp-sha-hmac
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
R1(config-crypto-map)# set security-association lifetime seconds 86400
R1(config-crypto-map)# set transform-set R1-R3
R1(config-crypto-map)# match address 100
```

Conectividad

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.3.10

Pinging 192.168.3.10 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.3.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.3.10

Pinging 192.168.3.10 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Reply from 192.168.3.10: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.3.10:
    Packets: Sent = 4, Received = 1, Lost = 3 (75% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

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
```

Verificación del túnel IPSec

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#sho
R1(config)#show cr
R1(config)#show crypto isakmp sa
          ^
% Invalid input detected at '^' marker.

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

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

R1(config)#is
R1(config)#cr
R1(config)#show cr
R1(config)#show crypto isakmp
          ^
% Invalid input detected at '^' marker.

R1(config)#show cr
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
ss
% Incomplete command.
R1#sho
R1#show cr
R1#show crypto isa
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           1026    0 ACTIVE


IPv6 Crypto ISAKMP SA
```

```
R1#
%SYS-5-CONFIG_I: Configured from console by console
##
% Incomplete command.
R1#sho
R1#show cr
R1#show crypto isa
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           1026    0 ACTIVE


IPv6 Crypto ISAKMP SA


R1#show cr
R1#show crypto is
R1#show crypto ipse
R1#show crypto ipsec sa

interface: GigabitEthernet0/0
    Crypto map tag: IPSEC-MAP, local addr 209.165.100.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
   current_peer 209.165.200.1 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 2, #pkts encrypt: 2, #pkts digest: 0
   #pkts decaps: 3, #pkts decrypt: 3, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

     local crypto endpt.: 209.165.100.1, remote crypto endpt.:209.165.200.1
     path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
     current outbound spi: 0x5C14F0C7(1544876231)
```

Conclusión

La implementación de una VPN Site-to-Site con IPSec permitió comprender el proceso completo para establecer comunicaciones seguras entre dos redes locales a través de Internet. Se aprendió a configurar las dos fases de IPSec: Fase 1 (ISAKMP) para la autenticación y establecimiento del canal seguro, y Fase 2 (IPSec) para el cifrado de los datos mediante transform sets.

Un aspecto fundamental fue la activación de las licencias securityk9 en los routers, sin las cuales no es posible utilizar funcionalidades criptográficas. También se enfrentaron y resolvieron problemas prácticos como la modificación de crypto maps activos, siguiendo el procedimiento correcto de removerlos de la interfaz antes de realizar cambios.

Las pruebas de conectividad y verificación confirmaron que el tráfico entre las redes 192.168.1.0/24 y 192.168.3.0/24 viajó cifrado (paquetes ESP), garantizando confidencialidad e integridad de la información. En conclusión, IPSec es una solución confiable y ampliamente adoptada para proteger comunicaciones en entornos empresariales, y esta práctica proporcionó las bases para su correcta implementación y diagnóstico.