IMPLEMENTACIÓN DE UNA IPSEC VPN EN PACKET TRACER

CNO V – SEGURIDAD INFORMATICA

Juan Alejandro Pérez Ventura
180370@upslp.edu.mx

Contenido

1. Objetivo

El objetivo de esta práctica fue configurar una VPN Site-to-Site con el protocolo IPSec en routers Cisco 1941, con la finalidad de permitir una comunicación segura entre dos redes locales a través de Internet, protegiendo la información mediante cifrado.

Se buscó que los equipos de la red 192.168.1.0/24 y 192.168.3.0/24 pudieran intercambiar información sin riesgo de ser interceptados.

2. Descripción de la Topología

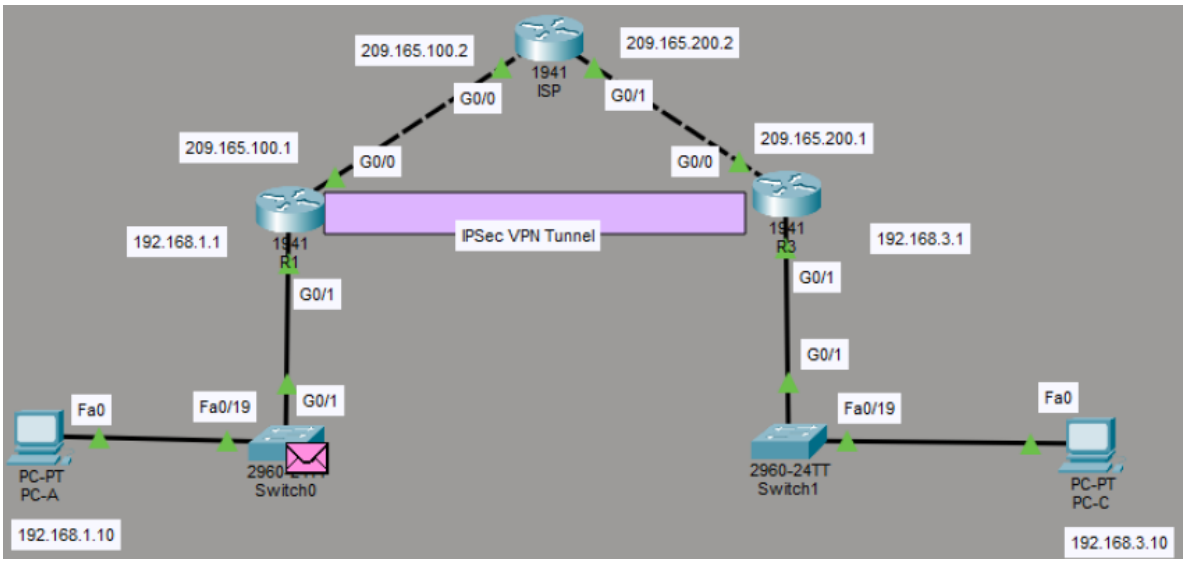
La topología implementada está conformada por tres routers:

- R1 (Red local izquierda)
- ISP (Simulación de Internet)
- R3 (Red local derecha)

Cada router cuenta con una interfaz LAN y una interfaz WAN, conectadas de la siguiente forma:

Router	Red LAN	Red WAN
R1	192.168.1.0/24	209.165.100.0/24
R3	192.168.3.0/24	209.165.200.0/24

El router ISP se utilizó como intermediario para simular el acceso a Internet.



3. Habilitación del Módulo de Seguridad

Antes de configurar la VPN, fue necesario habilitar el paquete de seguridad en los routers Cisco 1941, ya que este no se encuentra activo por defecto.
Para ello se utilizó el siguiente comando:

1. *license boot module c1900 technology-package securityk9*
2. *reload*

```
Router>enable
Router#conf
Router#configure te
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#license boot module c1900 technology-package securityk9
```

Este comando permitió activar las funciones necesarias para el uso de IPSec.

4. Configuración Básica de Red

4.1 Configuración de R1

Se configuraron las interfaces LAN y WAN, además de una ruta por defecto para permitir el acceso a Internet.

1. *interface g0/1*
2. *ip address 192.168.1.1 255.255.255.0*
3. *no shutdown*
4. *interface g0/0*
5. *ip address 209.165.100.1 255.255.255.0*
6. *no shutdown*
7. *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
```

4.2 Configuración del ISP

El router ISP se configuró únicamente para enrutar tráfico entre R1 y R3.

1. *interface g0/1*
2. *ip address 209.165.200.2 255.255.255.0*
3. *no shutdown*
4. *interface g0/0*
5. *ip address 209.165.100.2 255.255.255.0*
6. *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
```

4.3 Configuración de R3

La configuración de R3 es similar a la de R1, cambiando las direcciones IP.

1. *interface g0/1*
2. *ip address 192.168.3.1 255.255.255.0*
3. *no shutdown*
4. *interface g0/0*
5. *ip address 209.165.200.1 255.255.255.0*
6. *no shutdown*
7. *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
```

```
Router(config)#int g0/1
Router(config-if)#ip add
Router(config-if)#ip address 192.168.3.1 255.255.255.0
Router(config-if)#no sh
Router(config-if)#no shutdown

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

5. Configuración de IPSec en R1

5.1 Política ISAKMP (Fase 1)

Se definieron los parámetros de autenticación y cifrado.

1. *crypto isakmp policy 10*
2. *encryption aes 256*
3. *authentication pre-share*
4. *group 5*

5.2 Clave Precompartida

1. *crypto isakmp key secretkey address 209.165.200.1*

Esta clave permite autenticar ambos extremos del túnel.

5.3 Transform Set (Fase 2)

1. *crypto ipsec transform-set R1-R3 esp-aes 256 esp-sha-hmac*

5.4 Crypto Map

1. *crypto map IPSEC-MAP 10 ipsec-isakmp*
2. *set peer 209.165.200.1*
3. *set pfs group5*
4. *set security-association lifetime seconds 86400*
5. *set transform-set R1-R3*
6. *match address 100*

5.5 Aplicación en la Interfaz WAN

1. *interface g0/0*
2. *crypto map IPSEC-MAP*

5.6 Lista de Control de Acceso (ACL)

1. *access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255*

Esta ACL define el tráfico que será cifrado.

```
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
R1(config-crypto-map)#
```

6. Configuración de IPSec en R3

La configuración de R3 es equivalente a la de R1, modificando direcciones IP y nombres.
Incluye:

- Política ISAKMP
- Clave precompartida
- Transform set
- Crypto map
- ACL
- Aplicación en interfaz WAN

Esto garantiza compatibilidad entre ambos routers.

7. Verificación del Túnel VPN

Para comprobar el funcionamiento del túnel se utilizaron los siguientes comandos:

1. *show crypto isakmp sa*
2. *show crypto ipsec sa*

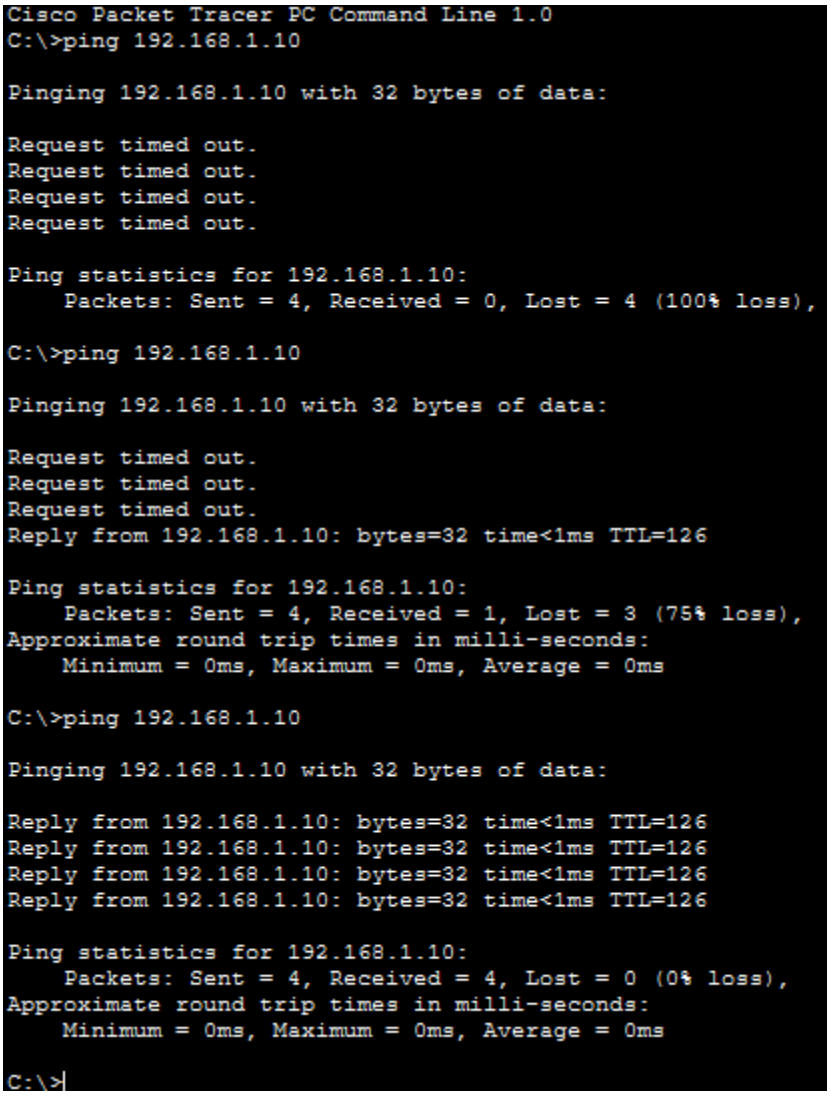
Si el estado es QM_IDLE, significa que la VPN está activa.
También se realizaron pruebas con ping entre equipos.

8. Resultados Obtenidos

Después de realizar la configuración:

- Se logró comunicación entre ambas redes
- El tráfico viajó cifrado
- El túnel se estableció correctamente
- No se presentaron pérdidas de información

Esto confirma el funcionamiento exitoso del VPN.



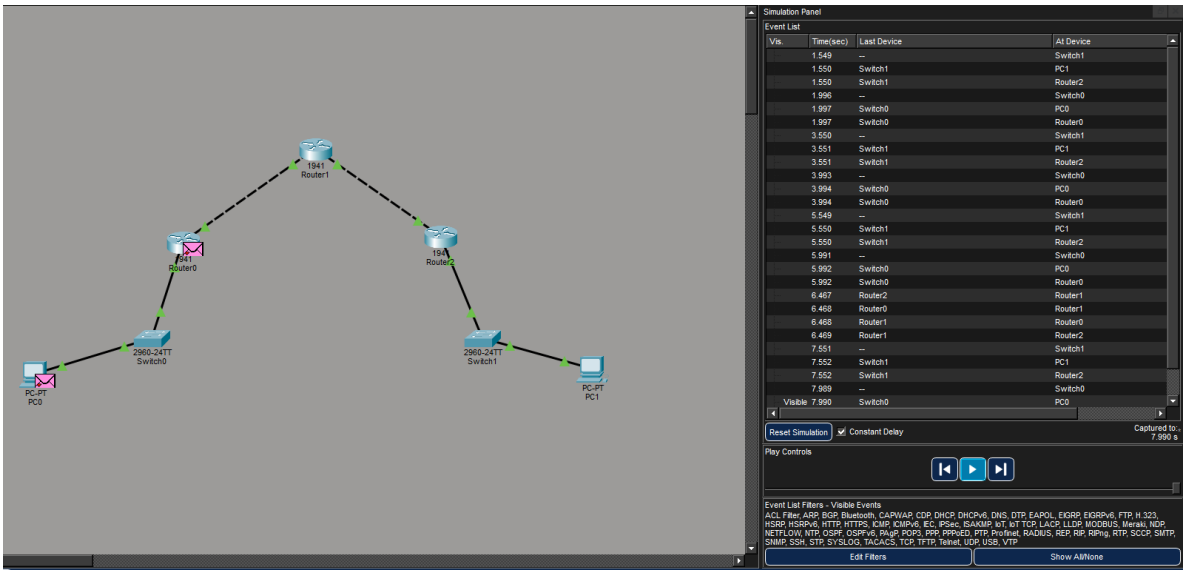
9. Conclusiones

Mediante esta práctica se comprendió el funcionamiento de una VPN Site-to-Site usando IPSec.

Se aprendió a:

- Activar funciones de seguridad
- Configurar fases de VPN
- Aplicar ACL
- Verificar túneles

IPSec es una herramienta confiable para proteger información en redes empresariales.



10. Recomendaciones

- Utilizar contraseñas más seguras
- Implementar certificados digitales
- Realizar respaldos antes de configurar
- Documentar cambios
- Probar la red antes y después del VPN