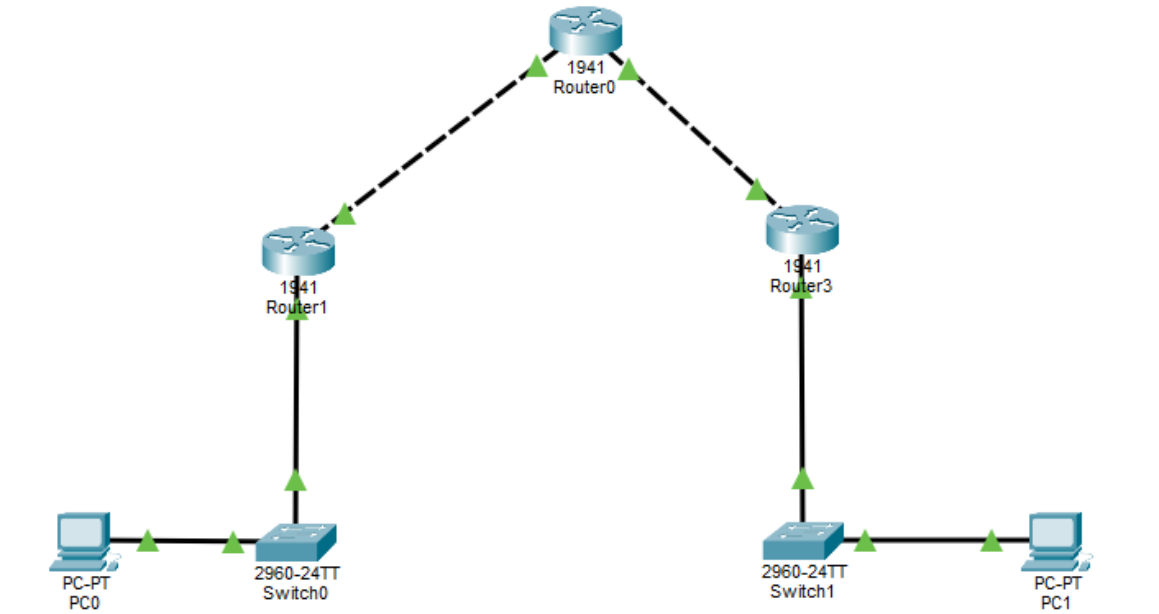
ACTIVIDAD 06

Implementación IPSec VPN

16 DE FEBRERO DE 2026

UPSLP
CNO V Seguridad Informática



Introducción

La seguridad en la transmisión de datos a través de infraestructuras públicas como Internet es un pilar fundamental de la ciberseguridad moderna. Este reporte detalla la implementación de una **VPN (Virtual Private Network**) IPSec Sitio a Sitio, basada en las prácticas de laboratorio realizadas para la asignatura de Seguridad Informática.

El objetivo primordial es establecer un túnel cifrado entre dos redes locales (LAN) remotas, garantizando la confidencialidad, integridad y autenticidad de la información mediante el uso de routers Cisco en un entorno simulado (Cisco Packet Tracer).Este método garantiza tres pilares fundamentales de la seguridad informática:

- **Confidencialidad:** Cifrado de los datos para que no sean legibles por terceros.
- **Integridad:** Asegurar que la información no haya sido alterada durante el tránsito.
- **Autenticidad:** Confirmar la identidad de los puntos finales (routers) antes de establecer la conexión.

Escenario y Topología

Basado en las prácticas analizadas, la infraestructura común en **Cisco Packet Tracer** incluye:

- **Dispositivos:** Tres routers (R1, ISP y R3/R2), dos switches y dos estaciones de trabajo (PCs).

- **Segmentos de Red:**
    - Red Local A (R1): 192.168.1.0/24
    - Red Local B (R2/R3): 192.168.3.0/24
    - Red de Transporte (ISP): Direccionamiento público (ej. 209.165.100.x y 209.165.200.x).

Proceso de Configuración Técnica

El proceso se divide en fases críticas para el establecimiento del túnel:

Paso 1: Preparación y Licenciamiento

Para que un router Cisco soporte funciones de seguridad, es necesario activar el paquete tecnológico:

Bash
```
R1(config)# license boot module c1900 technology-package securityk9
```

Nota: Requiere reinicio del dispositivo para aplicar cambios.

Paso 2: Definición del Tráfico Interesante (ACL)

Se utilizan Listas de Control de Acceso (ACL) para definir qué tráfico debe ser cifrado. Solo los paquetes que viajan de una LAN a otra activarán el túnel.

Bash
```
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-if)#ip address 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

R1(config-if)#interface g0/0
R1(config-if)#ip address 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

R1(config-if)#ip route
             ^
% Invalid input detected at '^' marker.

R1(config-if)#ip route 0.0.0.0 0.0.0.0 209.165.100.2
R1(config)#license boot module c1900 technology-package securityk9
PLEASE  READ THE  FOLLOWING TERMS  CAREFULLY. INSTALLING THE LICENSE OR
LICENSE  KEY  PROVIDED FOR  ANY CISCO  PRODUCT  FEATURE  OR  USING SUCH
PRODUCT  FEATURE  CONSTITUTES  YOUR  FULL ACCEPTANCE  OF  THE FOLLOWING
TERMS. YOU MUST NOT PROCEED FURTHER IF YOU ARE NOT WILLING TO  BE BOUND
BY ALL THE TERMS SET FORTH HEREIN.
```

Paso 3: Fase 1 - ISAKMP (IKE)

En esta fase, los routers negocian la política de seguridad para el canal de control.

- **Algoritmo de cifrado:** AES-256 (o AES).
- **Hash:** SHA o MD5.
- **Autenticación:** Pre-shared key (PSK).
- **Grupo Diffie-Hellman:** Grupo 5.

Bash
```
R1(config)# crypto isakmp policy 10
R1(config-isakmp)# encryption aes
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# group 5
R1(config)# crypto isakmp key vpn-p@ss address 209.165.200.1
```

Paso 4: Fase 2 - IPSec Transform-Set

Aquí se definen los parámetros para proteger los datos reales (tráfico de usuario).

Bash
```
R1(config)# crypto ipsec transform-set SET-NAME esp-aes esp-sha-hmac
```

Paso 5: Creación y Aplicación del Crypto Map

Se vinculan las configuraciones anteriores (ACL, Peer IP y Transform-Set) en un "Mapa Criptográfico" que se aplica a la interfaz de salida hacia internet (WAN).

Bash
```
R1(config)# crypto map VPN-MAP 10 ipsec-isakmp
R1(config-crypto-map)# set peer 209.165.200.1
R1(config-crypto-map)# set transform-set SET-NAME
R1(config-crypto-map)# match address 100
R1(config)# interface g0/0
R1(config-if)# crypto map VPN-MAP
```

```
R2(config)#!Fase 2
R2(config)#crypto ipsec transform-set R1->R2 esp-aes 256 esp-sha-hma
R2(config)#crypto ipsec transform-set R2->R1 esp-aes 256 esp-sha-hmac
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 109.165.100.1
R2(config-crypto-map)#set pfs group5
R2(config-crypto-map)#
R2(config-crypto-map)#
R2(config-crypto-map)#
R2(config-crypto-map)#set sec
R2(config-crypto-map)#set security-association lig
R2(config-crypto-map)#set security-association li
R2(config-crypto-map)#set security-association lifetime se
R2(config-crypto-map)#set security-association lifetime seconds 864000
                                                               ^
% Invalid input detected at '^' marker.

R2(config-crypto-map)#set security-association lifetime seconds 86400
R2(config-crypto-map)#tra
R2(config-crypto-map)#trans
R2(config-crypto-map)#set tra
R2(config-crypto-map)#set transform-set R2->R1
R2(config-crypto-map)#mat
R2(config-crypto-map)#match ad
R2(config-crypto-map)#match address 100
```

4. Verificación y Pruebas

Para confirmar que el túnel está operativo y el tráfico está siendo cifrado, se utilizan los siguientes comandos de diagnóstico:

1. **show crypto isakmp sa**: Muestra el estado de la Fase 1. El estado debe aparecer como QM_IDLE.
2. **show crypto ipsec sa**: Permite verificar el número de paquetes encapsulados y cifrados. Si los contadores aumentan al hacer un *ping* entre las PCs, el túnel es exitoso.
3. **Ping/Traceroute**: Verificación de conectividad extremo a extremo.

Conclusiones del Reporte

La implementación exitosa de una VPN IPSec permite a las organizaciones utilizar infraestructuras públicas económicas para interconectar sucursales de manera segura. Los documentos coinciden en que la precisión en los parámetros de ambas fases (IKE e IPSec) es vital; cualquier discrepancia en el cifrado o las llaves compartidas entre el Router 1 y el Router 2 impedirá el establecimiento de la comunicación.