

Actividad 06 – Implementación IPSec VPN

Jorge Alejandro Cabrera Meza – 181591

CNO V – Seguridad informática

Ing. Tecnologías de la información

Mto Servando López Contreras

Índice

1. ¿Qué es una VPN IPSec?
2. Marco Teórico: El Protocolo IPSec
 - 2.1. Protocolos de Seguridad: AH y ESP
 - 2.2. Modos de Funcionamiento: Transporte y Túnel
 - 2.3. El Proceso IKE (Internet Key Exchange)
3. Descripción de la Topología
4. Conexión del Puente VPN
5. Configuración Inicial
6. Configuración Real de los Routers (R1 y R2)
 - 6.1. Configuración R1
 - 6.2. Configuración R2
7. Explicación Detallada de los Comandos de Configuración
8. Verificación del Túnel
9. Conclusión

1. ¿Qué es una VPN IPSec?

IPSec (Internet Protocol Security) es un conjunto de protocolos que proporcionan seguridad a nivel de red (capa 3 del modelo OSI) mediante cifrado, autenticación e integridad de los datos. Una VPN (Virtual Private Network) IPSec permite crear un túnel seguro a través de una red pública (como Internet), conectando dos redes locales (LAN) de forma transparente y segura, como si estuvieran en el mismo espacio físico.

2. El Protocolo IPSec

Para comprender la configuración, es esencial entender los componentes y el proceso que sigue IPSec para establecer una comunicación segura.

2.1. Protocolos de Seguridad: AH y ESP

IPSec utiliza dos protocolos principales para proteger los datos:

- AH (Authentication Header): Proporciona autenticación e integridad de los datos, pero no ofrece cifrado. Su función es garantizar que los datos provengan de un origen legítimo y que no hayan sido modificados en tránsito. Hoy en día, es poco utilizado en favor de ESP, que ofrece un espectro de seguridad más completo.
- ESP (Encapsulating Security Payload): Es el protocolo más común. Ofrece un paquete completo de seguridad: cifrado (confidencialidad), autenticación e integridad. Como se observa en la configuración (`esp-aes 256` `esp-sha-hmac`), ESP es el protocolo elegido para el túnel.

2.2. Transporte y Túnel

- Modo Transporte: En este modo, solo la carga útil (los datos) del paquete IP es cifrada y/o autenticada. La cabecera IP original permanece intacta. Se utiliza principalmente para comunicaciones de extremo a extremo, como entre un cliente y un servidor.
- Modo Túnel: Aquí, el paquete IP completo (cabecera y carga útil) es cifrado y autenticado. Luego, este paquete se encapsula dentro de un nuevo paquete IP con una nueva cabecera. Este es el modo estándar para las VPNs site-to-site, ya que protege toda la información de las redes privadas y permite el enrutamiento a través de Internet.

2.3. El Proceso IKE (Internet Key Exchange)

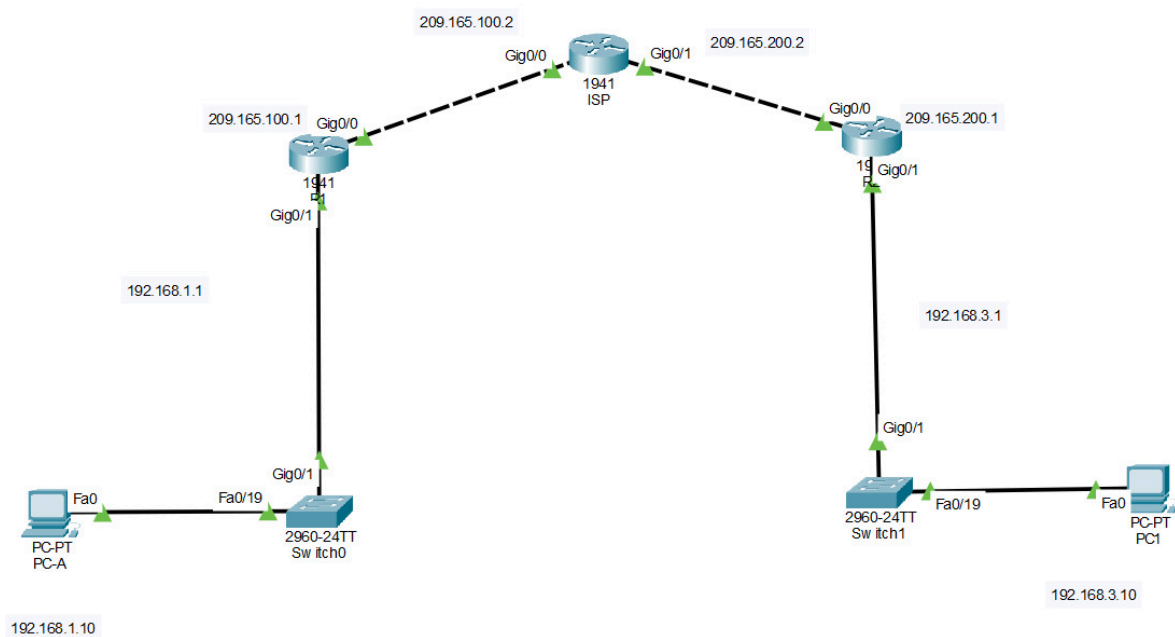
El establecimiento de un túnel IPSec no es instantáneo. Sigue un proceso negociado en dos fases, conocido como IKE:

- **Fase 1 (IKE / ISAKMP):** El objetivo de esta fase es establecer un canal seguro de control entre los dos peers (R1 y R2). En esta negociación inicial, los routers se autentican mutuamente (usando una clave precompartida, como secretkey) y acuerdan los parámetros de seguridad para el canal de control, como el algoritmo de cifrado (aes 256), el de autenticación (pre-share), y el grupo Diffie-Hellman (group 5) para el intercambio seguro de claves. Al final de esta fase, se crea un ISAKMP SA (Security Association), que es el acuerdo que define el canal seguro de control.
- **Fase 2 (IPSec):** Una vez que el canal de control es seguro, se procede a negociar el túnel de datos. En esta fase se acuerdan los parámetros para proteger el tráfico de datos real (el "tráfico interesante" definido en la ACL). Aquí se negocia el protocolo (ESP), los algoritmos de cifrado y autenticación para los datos (esp-aes 256 esp-sha-hmac), y si se usará PFS (Perfect Forward Secrecy). Al finalizar, se crean las IPSec SAs, que son un par de acuerdos (uno para cada dirección del tráfico) que definen cómo se cifran y descifran los datos del usuario.

3. Descripción de la Topología

Interconexión de dos LAN remotas a través de un ISP.

- R1: 192.168.1.0/24 (Red Local)
- R2: 192.168.3.0/24 (Red Remota)
- ISP: Actúa como la red pública de transporte.



4. Conexión del Puente VPN

El túnel IPsec encapsula y cifra el tráfico entre ambas redes, creando un puente seguro sobre la infraestructura del ISP.

5. Configuración Inicial

Configuración base de direccionamiento y rutas estáticas aplicada a ISP, R1 y R2 para garantizar la conectividad IP de extremo a extremo antes de construir el túnel.

Router ISP

Enable

conf t

hostname ISP

interface G0/0

ip address 209.165.100.2 255.255.255.0

no shut

interface G0/1

```
ip address 209.165.200.2 255.255.255.0
```

```
no shut
```

```
ip route 0.0.0.0 0.0.0.0 209.165.100.2
```

R1

```
enable
```

```
conf t
```

```
hostname R1
```

```
interface G0/1
```

```
ip address 192.168.1.1 255.255.255.0
```

```
no shut
```

```
interface G0/0
```

```
ip address 209.165.100.1 255.255.255.0
```

```
no shut
```

```
ip route 0.0.0.0 0.0.0.0 209.165.100.2
```

R2

```
enable
```

```
configure terminal
```

```
hostname R2
```

```
interface g0/1
```

```
ip address 192.168.3.1 255.255.255.0
```

```
no shutdown
```

```
interface g0/0
```

```
ip address 209.165.200.1 255.255.255.252
```

```
no shutdown
```

```
ip route 0.0.0.0 0.0.0.0 209.165.200.2
```

6. Configuración Real de los Routers (R1 y R2)

6.1 Configuración R1

```
R1
R1>en
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#
R1(config)#
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)#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->R2 esp-aes 256 esp-sha-hmac
R1(config)#crypto map IPSEC-MAP 10 ipsec-isakmp
R1(config-crypto-map)#set peer 209.165.200.1
R1(config-crypto-map)#set pfs group5
R1(config-crypto-map)#set transform-set R1->R2
R1(config-crypto-map)#match address 100
R1(config-crypto-map)#exit
R1(config)#int g0/0
R1(config-if)#crypto map IPSEC-MAP

R1(config-if)#
```

6.2 Configuración R2

```
text
R2
R2>en
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#access-list 100 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
R2(config)#crypto isakmp policy 10
R2(config-isakmp)#encryption aes 256
```

```
R2(config-isakmp)#authentication pre-share
R2(config-isakmp)#group 5
R2(config-isakmp)#exit
R2(config)#crypto isakmp key secretkey address 209.165.100.1
R2(config)#crypto ipsec transform-set R2->R1 esp-aes 256 esp-sha-hmac
R2(config)#crypto map IPSEC-MAP 10 ipsec-isakmp
R2(config-crypto-map)#set peer 209.165.100.1
R2(config-crypto-map)#set pfs group5
R2(config-crypto-map)#set transform-set R2->R1
R2(config-crypto-map)#match address 100
R2(config-crypto-map)#exit
R2(config)#int g0/0
R2(config-if)#crypto map IPSEC-MAP

R2(config-if)#
```

7. Explicación Detallada de los Comandos de Configuración

Comando	Contexto	Explicación
access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255	Configuración Global (ACL)	Define el "tráfico interesante". Esta ACL extendida número 100 le indica al router qué tráfico debe ser cifrado y enviado a través del túnel. En este caso, todo el tráfico IP proveniente de la red 192.168.1.0/24 con destino a la red 192.168.3.0/24 será protegido por IPSec.

crypto isakmp policy 10	Configuración Global (IKE)	Crea y entra al modo de configuración de una política IKE (Fase 1) con prioridad 10. El número 10 es la prioridad; cuanto más bajo el número, mayor prioridad tiene la política.
encryption aes 256	Configuración ISAKMP	Especifica el algoritmo de cifrado para la Fase 1. Aquí se utiliza AES (Advanced Encryption Standard) con una clave de 256 bits, el estándar más seguro y recomendado actualmente.
authentication pre-share	Configuración ISAKMP	Define el método de autenticación para la Fase 1. Se utilizará una clave precompartida (PSK), que es una contraseña que ambos routers conocen y que usarán para validar su identidad mutua.
group 5	Configuración ISAKMP	Especifica el grupo Diffie-Hellman (DH) a utilizar para el intercambio de claves en la Fase 1. El grupo 5 utiliza una clave de 1536 bits. Un grupo DH más alto (como 14, 19, etc.) ofrece mayor seguridad pero requiere más

		recursos computacionales.
crypto isakmp key secretkey address 209.165.200.1	Configuración Global (IKE)	Configura la clave precompartida (secretkey) que se usará con el peer de IPSec en la dirección IP 209.165.200.1. Este comando vincula la clave con el router remoto específico.
crypto ipsec transform-set R1->R2 esp-aes 256 esp-sha-hmac	Configuración Global (IPSec)	Crea un transform-set para la Fase 2. Es como un "menú" de opciones de seguridad que el router ofrecerá para proteger los datos. En este caso, se define el protocolo ESP, con cifrado AES 256 y autenticación HMAC-SHA(un algoritmo hash seguro).
crypto map IPSEC-MAP 10 ipsec-isakmp	Configuración Global (Crypto Map)	Crea una entidad de crypto map llamada IPSEC-MAP con una secuencia número 10. Esta entidad actúa como un "contrato" que une todos los elementos de la VPN: qué tráfico proteger (ACL), con quién (peer), cómo negociar (ISAKMP) y con qué métodos (transform-set).

A continuación, se desglosa el propósito de cada comando utilizado en las configuraciones de R1 y R2:

8. Verificación del Túnel

Comandos utilizados para verificar el estado de la VPN:

- `show crypto isakmp sa`: Muestra el estado de las Asociaciones de Seguridad (SA) de la Fase 1 (IKE). Un estado `QM_IDLE` o `ACTIVE` indica que la Fase 1 se estableció correctamente.
- `show crypto ipsec sa`: Muestra las SA de la Fase 2 (IPSec). Es el comando más importante para verificar el túnel de datos. Muestra el número de paquetes cifrados/descifrados, los `spi` (Security Parameter Index) y si el túnel está activo (`inbound esp sas, outbound esp sas`).
- `show ip route`: Verifica que las rutas estáticas o dinámicas a las redes locales y remotas existan y sean correctas.

9. Conclusión

La implementación de una VPN site-to-site con IPSec es un proceso que integra a la perfección la teoría de redes con la práctica de configuración. Como se ha demostrado, no se trata solo de introducir comandos, sino de comprender el diálogo estructurado en dos fases (IKE) que establecen los routers para ponerse de acuerdo en cómo protegerse mutuamente (Fase 1) y cómo proteger los datos sensibles de las organizaciones (Fase 2).

Cada elemento de la configuración, desde la definición del tráfico interesante mediante una ACL hasta la aplicación del crypto map en la interfaz, cumple un rol específico y crítico. Parámetros como el grupo Diffie-Hellman, el algoritmo de cifrado AES-256 o la activación de PFS no son meros detalles técnicos, sino decisiones de diseño que determinan la robustez y la seguridad del túnel frente a ataques y vulnerabilidades.

Este ejercicio práctico permite concluir que el dominio de tecnologías como IPSec es indispensable para el diseño y administración de infraestructuras de red modernas. La capacidad de interconectar sedes de forma segura, garantizando la confidencialidad, integridad y autenticidad de la información, es un pilar fundamental para la continuidad y seguridad operativa de cualquier organización en un entorno digital interconectado y, a menudo, hostil.