UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

15-2-2026

CNO V: Seguridad Informática

Hernández Fernández Diego Osvaldo – 182217

Mtro. Servando López Contreras

ACTIVIDAD 05

IPSec VPN

IPSec VPN

Un Site-to-Site IPSec VPN actúa como un puente seguro entre distintas sedes, utilizando protocolos diseñados para proteger el intercambio de datos en redes IP. Su propósito esencial es establecer un canal privado y cifrado entre dos routers, garantizando que la información viaje protegida de extremo a extremo.

La operatividad de este sistema se fundamenta en tres garantías esenciales para el tráfico de red:

- Confidencialidad.
- Integridad.
- Autenticación.

A continuación, se realizará dicha conexión con ayuda de la herramienta de Cisco Packet Tracer en donde se usará lo siguiente:

Infraestructura del Sitio Local (Red 192.168.1.0/24)

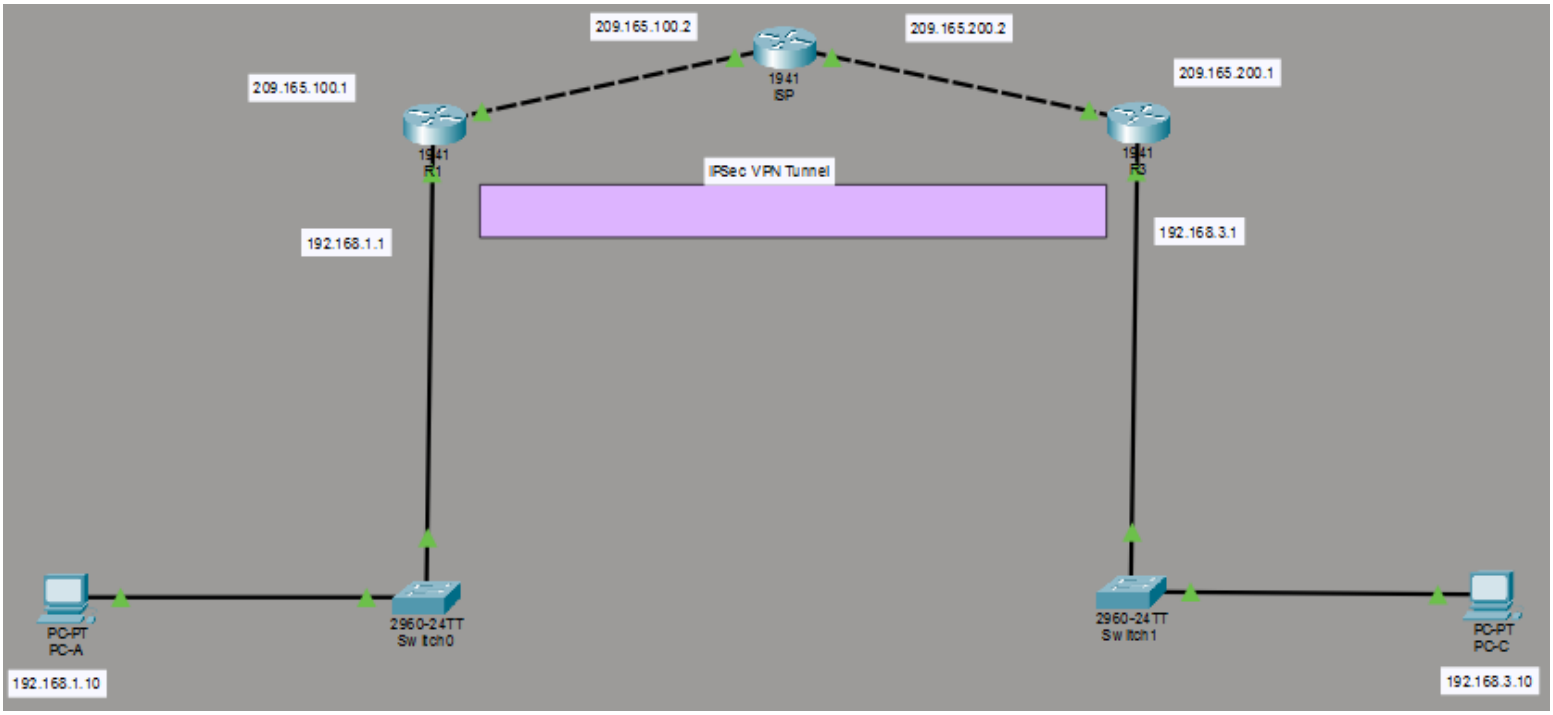
- Host Final: PC-A (IP: 192.168.1.10).
- Interconexión LAN: Switch0.
- Gateway de Seguridad: Router R1.
    - *Interfaz Interna:* 192.168.1.1.
    - *Interfaz Externa:* 209.165.100.1.

Infraestructura de Transporte

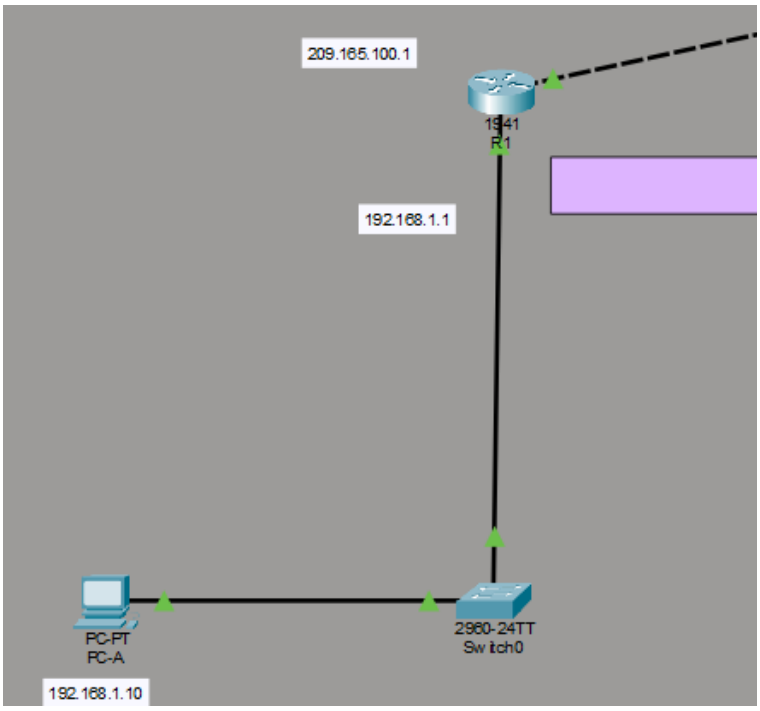
- Nodo Intermedio: Router ISP.
    - *Enlace hacia R1:* 209.165.100.2.
    - *Enlace hacia R3:* 209.165.200.2.

Infraestructura del Sitio Remoto (Red 192.168.3.0/24)

- Terminación de Túnel: Router R3.
    - *Interfaz Externa:* 209.165.200.1.
    - *Interfaz Interna:* 192.168.3.1.
- Interconexión LAN: Switch1.
- Host Destino: PC-C (IP: 192.168.3.10).



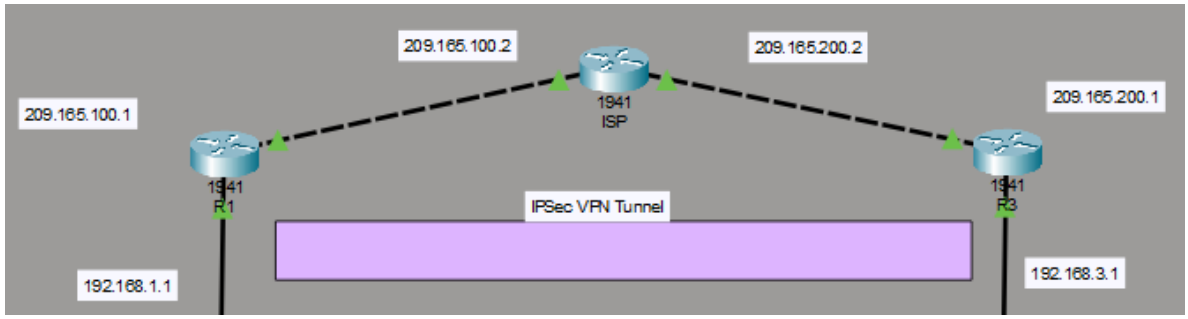
Topología



Sitio Local (Red 192.168.1.10)

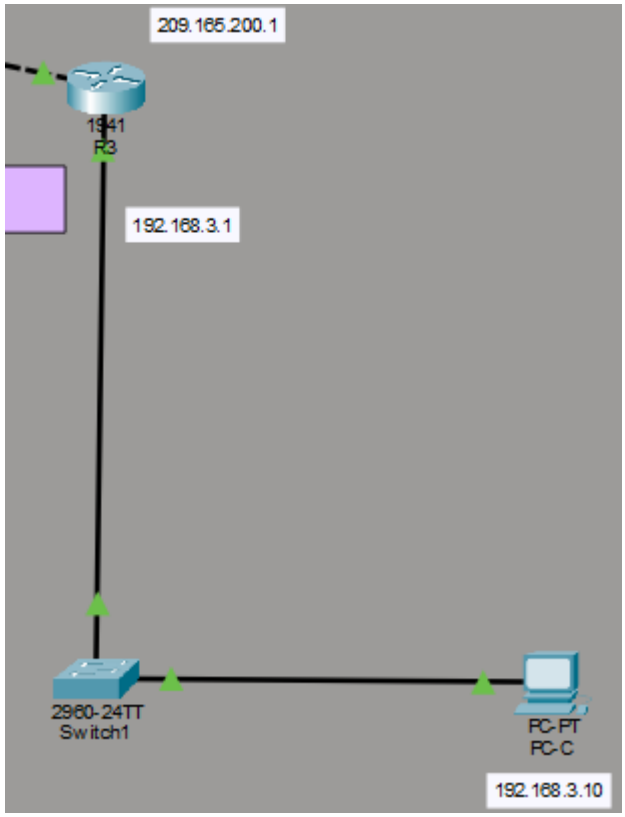
- **PC-A (192.168.1.10):** Es el host final que originará el tráfico.
- **Switch0:** Conecta los dispositivos locales.
- **Router R1:** Es el Gateway (Puerta de enlace).
    - Su interfaz interna tiene la IP 192.168.1.1.
    - Su interfaz externa tiene la IP pública 209.165.100.1.

- R1 será el encargado de cifrar el tráfico que vaya hacia la red del PC-C.



La Nube / Proveedor.

- **Router ISP:** Representa la infraestructura de Internet.
  - Recibe tráfico de R1 por la IP 209.165.100.2.
  - Envía tráfico hacia R3 por la IP 209.165.200.2.
  - El ISP no sabe qué hay dentro del túnel VPN él solo se encarga de mover los paquetes de una IP pública a otra.



El Sitio Remoto (Red 192.168.3.0)

- **Router R3:** Es el otro extremo del túnel.
    - Su interfaz externa tiene la IP pública 209.165.200.1.
    - Su interfaz interna tiene la IP 192.168.3.1.
- **Switch1:** Distribuye la conexión en el sitio remoto.
- **PC-C (192.168.3.10):** El destino final. Para este PC, los datos llegan como si vinieran de una red local, gracias a que R3 los descifra al recibirlos.

Configuración de los Routers

Configuración Inicial del Router R1

Modo privilegiado y asignación de nombre:

```
R1>enable
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#hostname R1
R1(config)#
```

- enable: Permite pasar del modo de usuario básico al modo de ejecución privilegiada.
- configure terminal: Entra en el modo de configuración global, donde los cambios afectan a todo el dispositivo.
- hostname R1: Define el nombre único del router en la red.

Configuración de la Interfaz LAN (Red Local):

```
R1(config)#interface g0/1
R1(config-if)#
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#
R1(config-if)#no shutdown
```

- interface g0/1: Accede a la configuración de la interfaz GigabitEthernet que conecta al switch interno.
- ip address 192.168.1.1 255.255.255.0: Asigna la dirección IP privada que servirá como Gateway para los dispositivos de la red interna.
- no shutdown: Activa administrativamente la interfaz para que comience a transmitir datos.

Configuración de la Interfaz WAN (Conexión Pública):

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

- interface g0/0: Selecciona la interfaz que conecta hacia el ISP (Internet).

- ip address 209.165.100.1 255.255.255.0: Asigna la dirección IP pública necesaria para establecer la comunicación externa.
- no shutdown: Habilita la interfaz, permitiendo que el router sea visible para el siguiente salto (ISP).

Configuración del Router R3

Modo privilegiado y asignación de nombre:

```
R2>enable
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#hostname R2
```

- enable: Eleva los privilegios del usuario.
- configure terminal: Abre el editor de configuración global del router.
- hostname R2: Asigna un nombre al dispositivo.

Configuración de la Interfaz LAN (Red de Destino):

```
R2(config)#interface g0/1
R2(config-if)#ip address 192.168.3.1 255.255.255.0
R2(config-if)#no shutdown
```

- interface g0/1: Selecciona el puerto GigabitEthernet que comunica con el Switch1.
- ip address 192.168.3.1 255.255.255.0: Establece la dirección IP privada que servirá como Gateway para la PC-C y otros dispositivos en esa ubicación.
- no shutdown: Cambia el estado del puerto a "Up" (encendido), permitiendo el flujo de paquetes locales.

Configuración de la Interfaz WAN (Salida a Internet):

```
R2(config-if)#interface g0/0
R2(config-if)#ip address 209.165.200.1 255.255.255.0
R2(config-if)#no shutdown
```

- interface g0/0: Accede a la interfaz física conectada hacia el proveedor de servicios (ISP).
- ip address 209.165.200.1 255.255.255.0: Define la dirección IP pública del sitio remoto. Esta dirección será el "punto de destino" que el Router R1 buscará para levantar el túnel IPSec.
- no shutdown: Habilita el enlace físico hacia la red externa.

Configuración del Router ISP

Este dispositivo actúa como el puente de comunicación entre las dos oficinas. Su función es puramente de transporte: recibe los paquetes cifrados de un router y los entrega al otro basándose en sus direcciones IP públicas.

Ingreso a la consola y personalización:

```
ISP>enable
ISP#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ISP(config)#hostname ISP
```

- enable: Accede al modo de ejecución con privilegios elevados.
- configure terminal: Entra al modo de configuración global para modificar los parámetros del sistema.
- hostname ISP: Identifica al dispositivo como el Proveedor de Servicios.

Configuración del Enlace hacia la Sede R1:

```
ISP(config)#interface g0/0
ISP(config-if)#ip address 209.165.100.2 255.255.255.0
ISP(config-if)#no shutdown
```

- interface g0/0: Selecciona el puerto físico que se conecta directamente con el Router R1.
- ip address 209.165.100.2 255.255.255.0: Asigna la dirección IP que completa el segmento de red con R1.
- no shutdown: Enciende la interfaz, estableciendo el enlace físico y lógico con R1.

Configuración del Enlace hacia la Sede R3 (Remota):

```
ISP(config-if)#interface g0/1
ISP(config-if)#ip address 209.165.200.2 255.255.255.0
ISP(config-if)#no shutdown
```

- interface g0/1: Selecciona el puerto físico conectado al Router R3.
- ip address 209.165.200.2 255.255.255.0: Establece la dirección IP en el segmento público del sitio remoto.
- no shutdown: Activa la interfaz para permitir el flujo de datos.

Configuración de Enrutamiento (Rutas Estáticas)

Router R1 (Sede Local)

```
R1(config)#ip route 0.0.0.0 0.0.0.0 209.165.100.2
```

- ip route 0.0.0.0 0.0.0.0 209.165.100.2

Con esta instrucción, definimos el camino que debe seguir cualquier tráfico que no pertenezca a nuestra red local. Básicamente, le indicamos al Router R1 que, si no conoce el destino interno de un paquete (ya sea que vaya hacia internet o a la oficina remota), debe entregarlo a la dirección 209.165.100.2. Esta IP del ISP funciona como nuestra puerta de salida obligatoria hacia el mundo exterior.

Router R3 (Sede Remota)

```
R2(config)#ip route 0.0.0.0 0.0.0.0 209.165.200.2
```

- ip route 0.0.0.0 0.0.0.0 209.165.200.2

Siguiendo la misma lógica que en el sitio local, hemos definido una ruta en el router remoto para garantizar la bidireccionalidad de los datos. Al establecer la IP 209.165.200.2 como su puerta de enlace, aseguramos que R2 pueda devolver el tráfico y responder a las peticiones externas. Este ajuste es crítico para cerrar el ciclo de comunicación entre ambos puntos de la infraestructura.

Router ISP (El Núcleo)

```
ISP(config)#ip route 0.0.0.0 0.0.0.0 209.165.200.1
```

- ip route 0.0.0.0 0.0.0.0 209.165.200.1

Esta instrucción es fundamental para la visibilidad de la red ya que básicamente, estamos definiendo que el router R2 es el destino final para los paquetes que transitan por la interfaz 209.165.200.1.

Activación de la Licencia de Seguridad (Security K9)

Para que un router Cisco de la serie 1900 pueda procesar túneles IPSec, es obligatorio activar el paquete de tecnología de seguridad. Por defecto, estos routers vienen con una licencia básica (IP Base), y el comando ejecutado realiza lo siguiente:

- license boot module c1900 technology-package securityk9:

Con el comando instruimos al sistema operativo para que cargue los protocolos criptográficos necesarios (como AES y 3DES) en el siguiente arranque. Sin este paso, el equipo no tendría la 'inteligencia' necesaria para procesar el cifrado de los túneles IPSec.

Para garantizar que ambos extremos del túnel hablen el mismo 'lenguaje' de seguridad, es fundamental aplicar esta configuración de manera idéntica tanto en el Router R1 como en el R3.

```
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.

Use of this product feature requires  an additional license from Cisco,
together with an additional  payment.  You may use this product feature
on an evaluation basis, without payment to Cisco, for 60 days. Your use
of the  product,  including  during the 60 day  evaluation  period,  is
subject to the Cisco end user license agreement
http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html
If you use the product feature beyond the 60 day evaluation period, you
must submit the appropriate payment to Cisco for the license. After the
60 day  evaluation  period,  your  use of the  product  feature will be
governed  solely by the Cisco  end user license agreement (link above),
together  with any supplements  relating to such product  feature.  The
above  applies  even if the evaluation  license  is  not  automatically
terminated  and you do  not receive any notice of the expiration of the
evaluation  period.  It is your  responsibility  to  determine when the
evaluation  period is complete and you are required to make  payment to
Cisco for your use of the product feature beyond the evaluation period.

Your  acceptance  of  this agreement  for the software  features on one
product  shall be deemed  your  acceptance  with  respect  to all  such
software  on all Cisco  products  you purchase  which includes the same
software.  (The foregoing  notwithstanding, you must purchase a license
for each software  feature you use past the 60 days evaluation  period,
so  that  if you enable a software  feature on  1000  devices, you must
purchase 1000 licenses for use past  the 60 day evaluation period.)

Activation  of the  software command line interface will be evidence of
your acceptance of this agreement.


ACCEPT? [yes/no]: yes
% use 'write' command to make license boot config take effect on next boot
```

Continuación de la Configuración

Una vez que hemos activado la licencia de seguridad en ambos routers, vamos a realizar una serie de pasos administrativos para que los cambios tengan efecto y se mantengan de forma permanente.

exit:

```
R1(config)#exit
R1#
```

- **Función:** Regresa un nivel en la jerarquía de la línea de comandos.

copy run start:

```
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

- Guarda la configuración actual que está en la RAM (volátil) hacia la memoria NVRAM (no volátil).

Es necesario ya que, si el router se apaga o se reinicia sin este comando, podríamos perder toda la configuración de las IPs, el hostname y la activación de la licencia.

reload:

```
R1#reload
Proceed with reload? [confirm]
System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO1941/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 64/-1(On-board/DIMM0) bit mode with ECC disabled

Readonly ROMMON initialized

program load complete, entry point: 0x80803000, size: 0x1b340
program load complete, entry point: 0x80803000, size: 0x1b340

IOS Image Load Test
___________________
Digitally Signed Release Software
program load complete, entry point: 0x81000000, size: 0x2bb1c58
Self decompressing the image :
################################################################################ [OK]
Smart Init is enabled
smart init is sizing iomem
                    TYPE      MEMORY_REQ
     Onboard devices &
          buffer pools      0x01E8F000
------------------------------------------------
                TOTAL:      0x01E8F000
Rounded IOMEM up to: 32Mb.
Using 6 percent iomem. [32Mb/512Mb]

              Restricted Rights Legend
Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.
           cisco Systems, Inc.
           170 West Tasman Drive
           San Jose, California 95134-1706
```

- Reinicia físicamente el router.

show version:

```
R1>show version
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.1(4)M4, RELEASE
SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 23-Feb-11 14:19 by pt_team

ROM: System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
cisco1941 uptime is 16 seconds
System returned to ROM by power-on
System image file is "flash0:c1900-universalk9-mz.SPA.151-1.M4.bin"
Last reload type: Normal Reload

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.
Cisco CISCO1941/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
2 Gigabit Ethernet interfaces
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

License Info:

License UDI:

------------------------------------------------

License Info:

License UDI:

------------------------------------------------
Device#   PID                   SN
------------------------------------------------
*0        CISCO1941/K9          FTX152482R6-


Technology Package License Information for Module:'c1900'

-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      securityk9    Evaluation    securityk9
data          disable       None          None

Configuration register is 0x2102
```

- Muestra un resumen del hardware, el software (IOS) y el estado de las licencias.

Es fundamental que estos comandos se repliquen de forma exacta tanto en R1 como en R3

Configuración de la Fase 1 (IKEv1 / ISAKMP)

En esta fase, nos enfocamos en configurar el protocolo ISAKMP, cuya función principal es establecer un marco de confianza antes del envío de datos. Más que transportar información de usuario, este protocolo crea un canal de control privado y seguro. En este espacio, ambos routers pueden negociar 'en secreto' los parámetros de seguridad que regirán la conexión posterior. Es un paso que requiere una simetría exacta entre R1 y R3 para que la comunicación inicial sea exitosa.

crypto isakmp policy 10:

```
R1(config)#crypto isakmp policy 10
```

Crea una política de seguridad con el número de prioridad 10. Los routers compararán sus políticas y usarán la primera que coincida.

encryption aes 256:

```
R1(config-isakmp)#encryption aes 256
```

Define que el algoritmo de cifrado será AES con una llave de 256 bits.

authentication pre-share:

```
R1(config-isakmp)#authentication pre-share
```

Indica que los routers se identificarán entre sí mediante una contraseña compartida previamente.

group 5:

```
R1(config-isakmp)#group 5
```

Utiliza el grupo 5 de Diffie-Hellman (1536 bits) para intercambiar las llaves de cifrado de forma segura.

crypto isakmp key secretkey address [XXX.XXX.XXX.XXX]:

Aquí es donde colocamos la "contraseña" (secretkey).

- En **R1**, se apunta a la IP pública de **R3** (209.165.200.1).

```
R1(config-isakmp)#crypto isakmp key secretkey address 209.165.200.1
```

- En **R3**, se apunta a la IP pública de **R1** (209.165.100.1).

```
R2(config-isakmp)#crypto isakmp key secretkey address 209.165.100.1
```

Tráfico de interés y Transform-Set

Una vez que los routers han establecido un canal de confianza, el siguiente paso es definir las reglas específicas para proteger la información real de los usuarios.

Definición del Tráfico de interés (ACL)

Aquí usamos una Lista de Acceso (ACL) para identificar qué datos deben entrar al túnel.

En R1:

```
R1(config)#access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
```

- access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255

Este comando establece el criterio de selección para el túnel. Al configurar esta regla, el router identifica automáticamente la comunicación entre ambas sedes (de la red 1.0 a la 3.0) y activa los protocolos de seguridad. De esta manera, aseguramos que solo los datos que viajan entre sucursales sean encapsulados, permitiendo que el resto del tráfico de internet siga su curso normal.

En R3:

```
R2(config)#access-list 100 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
```

- access-list 100 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255

Para que la VPN sea en modo espejo, configuramos en R3 el criterio de retorno. Este comando instruye al router para que capture y cifre cualquier paquete que viaje desde la sede remota hacia la red local. Esto con el fin de asegurar que las respuestas y los datos de vuelta también viajen de forma privada por el enlace.

Conjunto de Transformación (Transform-Set)

Es el método de cifrado para los datos reales

En R1:

```
R1(config)#crypto ipsec transform-set R1-R3 esp-aes 256 esp-sha-hmac
```

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

En R3:

```
R2(config)#crypto ipsec transform-set R3-R1 esp-aes 256 esp-sha-hmac
```

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

Para ambos casos:

- **crypto ipsec transform-set [NOMBRE]**: Crea un grupo de configuraciones de seguridad. El nombre es local, pero los parámetros internos deben ser **idénticos** en ambos routers.
- **esp-aes 256**: Utiliza el protocolo ESP con cifrado AES de 256 bits para garantizar la confidencialidad.
- **esp-sha-hmac**: Utiliza el algoritmo SHA para asegurar la integridad (que nadie cambie los datos en el camino).

El Crypto Map y Activación en la Interfaz

Configuración del Crypto Map y Aplicación en Interfaz

En esta etapa final, creamos el mapa criptográfico. Este componente es el que organiza la Fase 1 (política), la Fase 2 (transform-set) y la selección de datos (ACL) para que trabajen juntos.

Este comando define el perfil de seguridad que el router seguirá.

```
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.
```

- crypto map IPSEC-MAP 10 ipsec-isakmp

crypto map [NOMBRE] 10 ipsec-isakmp: Crea el mapa de seguridad con el nombre "IPSEC-MAP". El número "10" indica la prioridad y "ipsec-isakmp" especifica que este mapa usará el protocolo de intercambio de llaves que configuramos al principio.

Aquí le decimos al router a quién debe enviarle los datos cifrados.

En R1:

```
R1(config-crypto-map)#set peer 209.165.200.1
```

- set peer 209.165.200.1

En R2:

```
R2(config-crypto-map)#set peer 209.165.100.1
```

- set peer 209.165.100.1

set peer [IP_PUBLICA]: Establece la dirección IP del router remoto. En R1 apuntamos a la IP pública de R2, y en R2 apuntamos a la IP pública de R1.

Aquí activamos una función para que las llaves de cifrado se regeneren de forma segura y no dependan de llaves anteriores.

```
R2(config-crypto-map)#set pfs group5
```

- set pfs group5

Activa la función Perfect Forward Secrecy usando el grupo 5 de Diffie-Hellman. Esto añade una capa de seguridad extra al asegurar que, si una llave de sesión se llegara a comprometer, no afectará a las llaves de sesiones pasadas ni futuras.

En este comando establecemos cuánto tiempo durarán las llaves de seguridad antes de que el router cree unas nuevas automáticamente.

```
R2(config-crypto-map)#set security-association lifetime seconds 86400
```

- set security-association lifetime seconds 86400

Define el tiempo de vida de la conexión segura. En este caso, configuramos 86,400 segundos (equivalente a 24 horas). Pasado este tiempo, los routers regenerarán automáticamente nuevas llaves de cifrado para mantener la conexión protegida.

Vinculamos el conjunto de algoritmos (AES/SHA)

R1:

```
R1(config-crypto-map)#set transform-set R1-R3
```

- set transform-set R1-R3

R2:

```
R2(config-crypto-map)#set transform-set R3-R1
```

- set transform-set R3-R1

Vincula el conjunto de algoritmos de cifrado (AES y SHA) con este mapa.

Aquí se selecciona que tráfico debemos proteger

```
R2(config-crypto-map)#match address 100
```

- match address 100

Esta línea llama a la Lista de Acceso 100 que creamos antes. Le indica al mapa que solo debe cifrar los paquetes que coincidan con el origen y destino especificados en la ACL. Todo lo demás pasará por la interfaz sin ser cifrado.

Por último, activamos el final en la interfaz

```
R2(config-crypto-map)#interface g0/0
```

- interface g0/0

```
R2(config-if)#crypto map IPSEC-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

- crypto map IPSEC-MAP

Finalmente, entramos a la interfaz física que conecta con el ISP (Internet) y aplicamos el mapa. A partir de este segundo, el router empieza a vigilar el tráfico de salida: si detecta datos que van hacia la otra oficina, los cifra y los envía por el túnel.

Verificación

```
C:\>ping 192.168.3.10

Pinging 192.168.3.10 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 192.168.3.10: bytes=32 time=13ms TTL=126
Reply from 192.168.3.10: bytes=32 time=11ms TTL=126

Ping statistics for 192.168.3.10:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
Approximate round trip times in milli-seconds:
    Minimum = 11ms, Maximum = 13ms, Average = 12ms
```

Para poner en marcha el túnel, lanzamos un ping persistente desde la PC-A hacia la dirección 192.168.3.10. Este flujo de datos funcionó como el 'tráfico de interes' necesario para despertar la conexión; al detectar estos paquetes, los routers iniciaron automáticamente la negociación de las fases ISAKMP e IPsec para establecer el canal seguro.

```
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           1068    0 ACTIVE


IPv6 Crypto ISAKMP SA

R1#
```

Para confirmar que todo estaba en orden, ejecutamos el comando show crypto isakmp sa. Al obtener el estado QM_IDLE, validamos que la asociación de seguridad se completó con éxito; esto nos indica que ambos routers se han reconocido y autenticado correctamente, dejando el túnel listo para el tráfico de datos.

```
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: 3, #pkts encrypt: 3, #pkts digest: 0
   #pkts decaps: 2, #pkts decrypt: 2, #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 1, #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: 0x2DBDFACC(767425228)

     inbound esp sas:
      spi: 0xC3923917(3281139991)
        transform: esp-aes 256 esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2008, flow_id: FPGA:1, crypto map: IPSEC-MAP
        sa timing: remaining key lifetime (k/sec): (4525504/3454)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x2DBDFACC(767425228)
        transform: esp-aes 256 esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2009, flow_id: FPGA:1, crypto map: IPSEC-MAP
```

```
     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x2DBDFACC(767425228)
        transform: esp-aes 256 esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2009, flow_id: FPGA:1, crypto map: IPSEC-MAP
        sa timing: remaining key lifetime (k/sec): (4525504/3454)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:
```

Para asegurarnos de que el tráfico realmente estaba protegido, revisamos las estadísticas con show crypto ipsec sa. Al observar cómo aumentaban los contadores de paquetes encapsulados y decapsulados, confirmamos que el tráfico ICMP no solo estaba fluyendo, sino que viajaba cifrado y de forma totalmente privada a través del túnel.

```
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#

R2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R2#
```

Como paso final, guardamos los cambios con el comando copy running-config startup-config en ambos routers. De esta manera, nos aseguramos de que toda la configuración de la VPN sea permanente; así, ante cualquier reinicio o fallo eléctrico, el equipo cargará automáticamente los parámetros de seguridad y enrutamiento sin necesidad de intervención manual.