



**INSTITUTO POLITÉCNICO NACIONAL**  
**ESCUELA SUPERIOR DE CÓMPUTO**



## **Actividad 14: Configuración de VPN**

### **NOMBRES:**

- MACÍAS CASTILLO JOSUÉ
- OCHOA MONROY JOSÉ LUIS

**GRUPO:** 4CV3

**UNIDAD DE APRENDIZAJE:** ADMINISTRACIÓN DE SERVICIOS EN RED

**PERIODO:** 20-21/1

**FECHA:** 18/01/2021

## **INTRODUCCIÓN**

### **VPN**

La interconexión de dispositivos mediante una red LAN representa una manera muy eficiente y segura de transmitir información (que puede ser sensible) entre los miembros de una organización. Sin embargo, durante los últimos años ha crecido exponencialmente la necesidad de que los miembros de una misma organización se mantengan interconectados a pesar de estar distanciados geográficamente, y muchos medios de comunicación por medio de Internet no manejan el nivel de seguridad suficiente o las políticas adecuadas para la información que se debe transmitir.

“Las organizaciones utilizan las VPN para crear una conexión de red privada de extremo a extremo a través de redes externas como Internet o las extranets. El túnel elimina la barrera de distancia y permite que los usuarios remotos accedan a los recursos de red del sitio central. Una VPN es una red privada creada mediante tunneling a través de una red pública, generalmente Internet. Una VPN es un entorno de comunicaciones en el que el acceso se controla de forma estricta para permitir las conexiones de peers dentro de una comunidad de interés definida. Para implementar las VPN, se necesita un gateway VPN. El gateway VPN puede ser un router, un firewall o un dispositivo de seguridad adaptable (ASA) de Cisco.” (ITESA, s.f.).

### **IPSec**

Por la propia naturaleza de la Internet, la información transmitida entre dos dispositivos que se comunican por este medio viaja por varios nodos intermedios. Esto representa una importante brecha de seguridad cuando se transmite información que debe tratarse con confidencialidad.

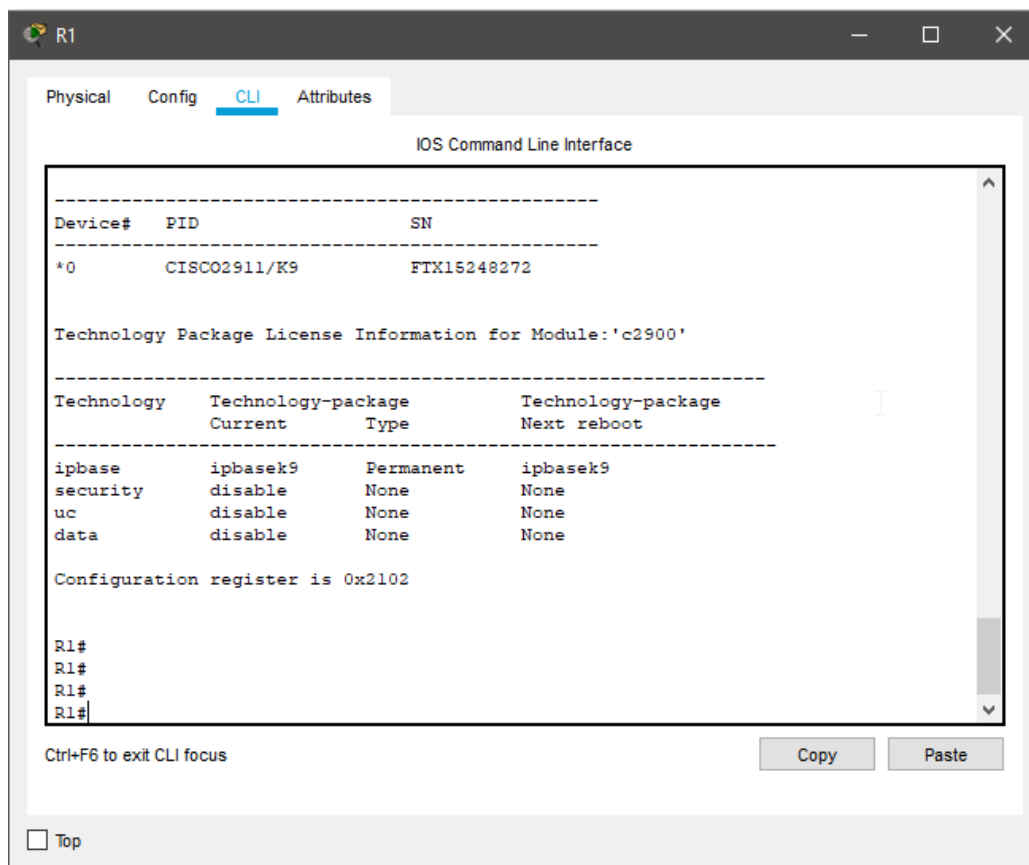
“IPsec es un marco de estándares abiertos que detalla las reglas para las comunicaciones seguras. IPSec no se limita a ningún tipo específico de cifrado, autenticación, algoritmo de seguridad ni tecnología de creación de claves. En realidad, IPsec depende de algoritmos existentes para implementar

comunicaciones seguras. IPsec permite que se implementen nuevos y mejores algoritmos sin modificar los estándares existentes de IPsec. IPsec funciona en la capa de red, por lo que protege y autentica los paquetes IP entre los dispositivos IPsec participantes, también conocidos como “peers”. IPsec protege una ruta entre un par de gateways, un par de hosts o un gateway y un host. Como resultado, IPsec puede proteger prácticamente todo el tráfico de una aplicación, dado que la protección se puede implementar desde la capa 4 hasta la capa 7.” (ITESA, s.f.).

## SOLUCIÓN DE LA ACTIVIDAD

### Parte 1: Habilitar las características de seguridad

#### Paso 1: Activar el módulo securityk9.



```
R1(config)# license boot module c2900 technology-package securityk9  
R1(config)# end  
R1# copy running-config startup-config  
R1# reload
```

Technology Package License Information for Module:'c2900'

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

Configuration register is 0x2102

The screenshot shows a window titled 'R3' with tabs for 'Physical', 'Config', 'CLI', and 'Attributes'. The 'CLI' tab is active, displaying the 'IOS Command Line Interface'. The interface shows the following output:

```
Device# PID SN
-----
*0 CISCO2911/K9 FTX1524R5X7

Technology Package License Information for Module:'c2900'

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

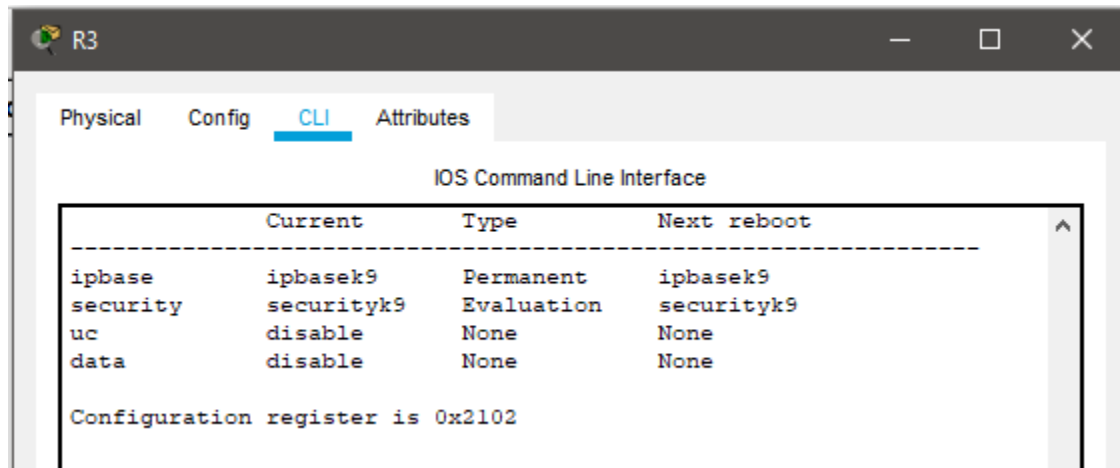
Configuration register is 0x2102

R3#
R3#
R3#
R3#
R3#
```

At the bottom of the CLI window, there is a prompt 'Ctrl+F6 to exit CLI focus' and two buttons: 'Copy' and 'Paste'. Below the CLI window, there is a checkbox labeled 'Top'.

Enter configuration commands, one per line. End with CNTL/Z.  
R3(config)#license boot module c2900 technology-package securityk9

```
R3#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R3#reload
Proceed with reload? [confirm]
```



## Parte 2: Configurar los parámetros de IPsec en el R1

### Paso 1: Probar la conectividad.

Haga ping de la **PC-A** a la **PC-C**.

```
C:\>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Reply from 192.168.3.3: bytes=32 time=3ms TTL=125
Reply from 192.168.3.3: bytes=32 time=2ms TTL=125
Reply from 192.168.3.3: bytes=32 time=10ms TTL=125
Reply from 192.168.3.3: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 10ms, Average = 4ms

C:\>
```

### Paso 2: Identificar el tráfico interesante en el R1.

```
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#
R1(config)#access-list 110 permit ip 192.168.1.0 0.0.0.255
192.168.3.0 0.0.0.255
```

### Paso 3: Configurar las propiedades de la fase 1 de ISAKMP en el R1.

```
R1(config)#  
R1(config)#crypto isakmp policy 10  
R1(config-isakmp)#encryption aes  
R1(config-isakmp)#authentication pre-share  
R1(config-isakmp)#group 2  
R1(config-isakmp)#exit  
R1(config)#  
R1(config)#crypto isakmp key cisco address 10.2.2.2
```

### Paso 4: Configurar las propiedades de la fase 2 de ISAKMP en el R1.

```
R1(config)#crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac  
R1(config)#crypto map VPN-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)#description VPN connection to R3  
R1(config-crypto-map)#set peer 10.2.2.2  
R1(config-crypto-map)#set transform-set VPN-SET  
R1(config-crypto-map)#match address 110  
R1(config-crypto-map)#exit  
R1(config)#
```

### Paso 5: Configurar la asignación criptográfica en la interfaz de salida.

```
R1(config)#int S0/0/0  
R1(config-if)#crypto map VPN-MAP  
*Jan 3 07:16:26.785: %CRYPTO-6-ISA_KMP_ON_OFF: ISAKMP is ON  
R1(config-if)#
```

## Parte 3: Configurar los parámetros de IPsec en el R3

### Paso 1: Configurar el router R3 para admitir una VPN de sitio a sitio con el R1.

```
R3(config)#access-list 110 permit ip 192.168.3.0 0.0.0.255  
192.168.1.0 0.0.0.255  
R3(config)#
```

### Paso 2: Configurar las propiedades de la fase 1 de ISAKMP en el R3.

```
R3(config)#  
R3(config)#crypto isakmp policy 10  
R3(config-isakmp)#encryption aes  
R3(config-isakmp)#authentication pre-share  
R3(config-isakmp)#group 2  
R3(config-isakmp)#exit  
R3(config)#crypto isakmp key cisco address 10.1.1.2  
R3(config)#
```

### Paso 3: Configurar las propiedades de la fase 2 de ISAKMP en el R1.

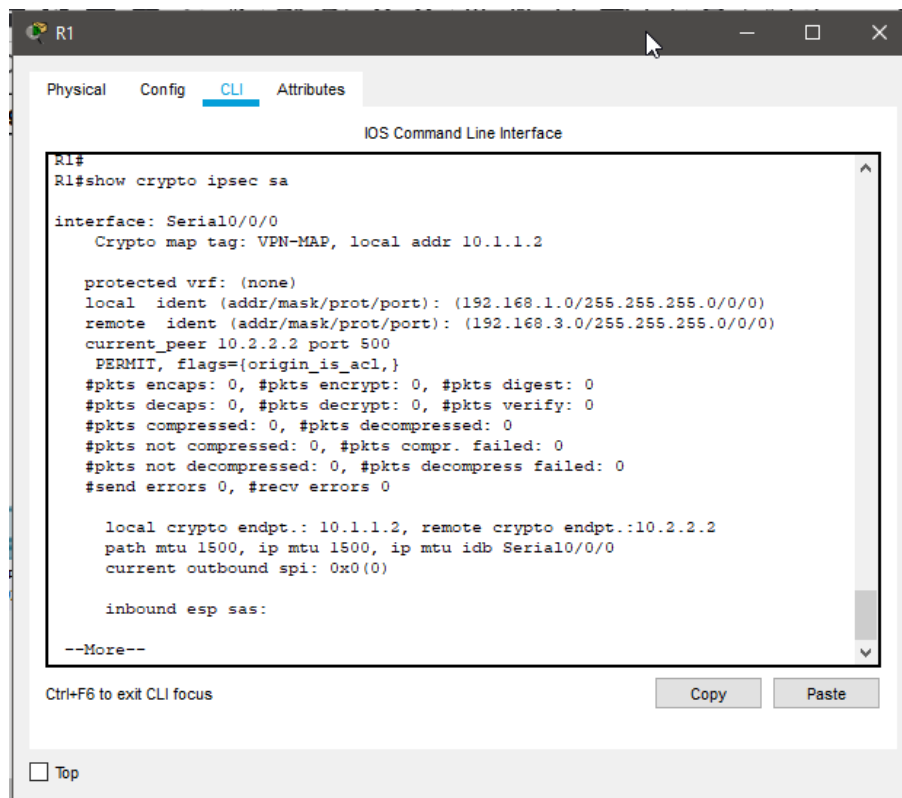
```
R3(config)#
R3(config)#crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
R3(config)#crypto map VPN-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R3(config-crypto-map)#description VPN connection to R1
R3(config-crypto-map)#set peer 10.1.1.2
R3(config-crypto-map)#set transform-set VPN-SET
R3(config-crypto-map)#match address 110
R3(config-crypto-map)#exit
R3(config)#
```

### Paso 4: Configurar la asignación criptográfica en la interfaz de salida.

```
R3(config)#int S0/0/1
R3(config-if)#crypto map VPN-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R3(config-if)#
```

## Parte 4: Verificar la VPN con IPsec

### Paso 1: Verificar el túnel antes del tráfico interesante.



## Paso 2: Crear el tráfico interesante.

Haga ping de la PC-A a la PC-C.

```
C:\>ping 192.168.3.3

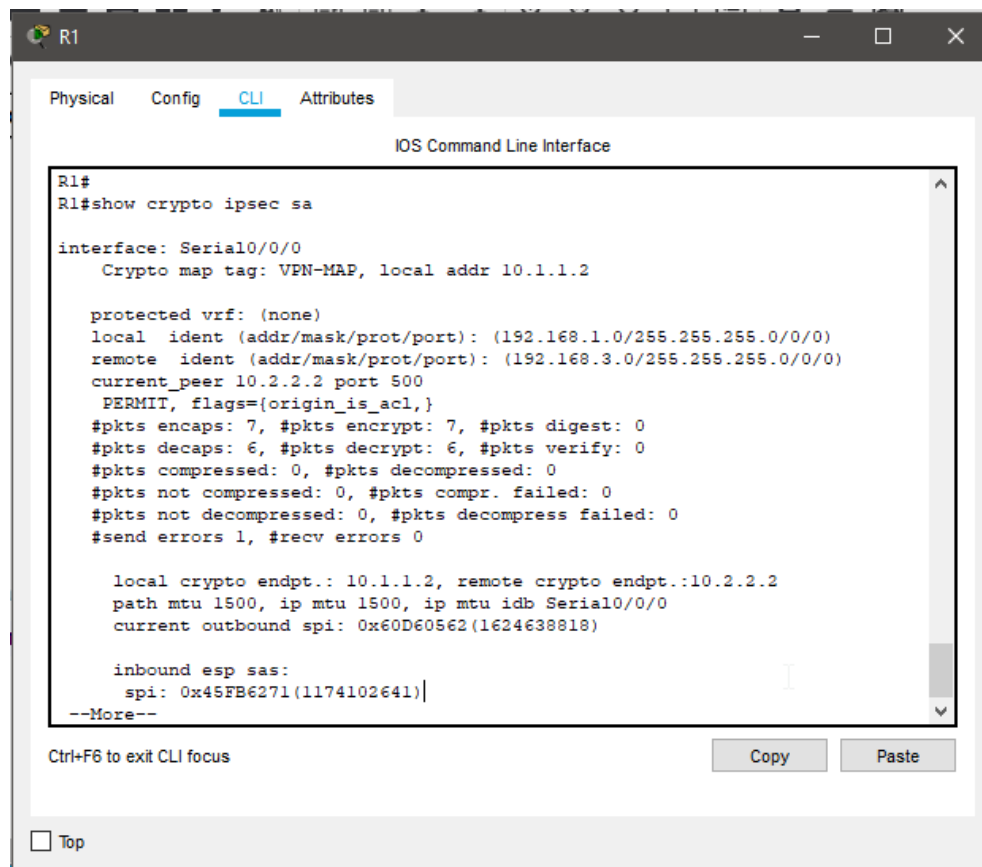
Pinging 192.168.3.3 with 32 bytes of data:

Reply from 192.168.3.3: bytes=32 time=3ms TTL=125
Reply from 192.168.3.3: bytes=32 time=2ms TTL=125
Reply from 192.168.3.3: bytes=32 time=10ms TTL=125
Reply from 192.168.3.3: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 10ms, Average = 4ms

C:\>
```

## Paso 3: Verificar el túnel después del tráfico interesante.





#### Paso 4: Crear el tráfico no interesante.

Haga ping de la PC-A a la PC-B.

```
C:\>ping 192.168.2.3

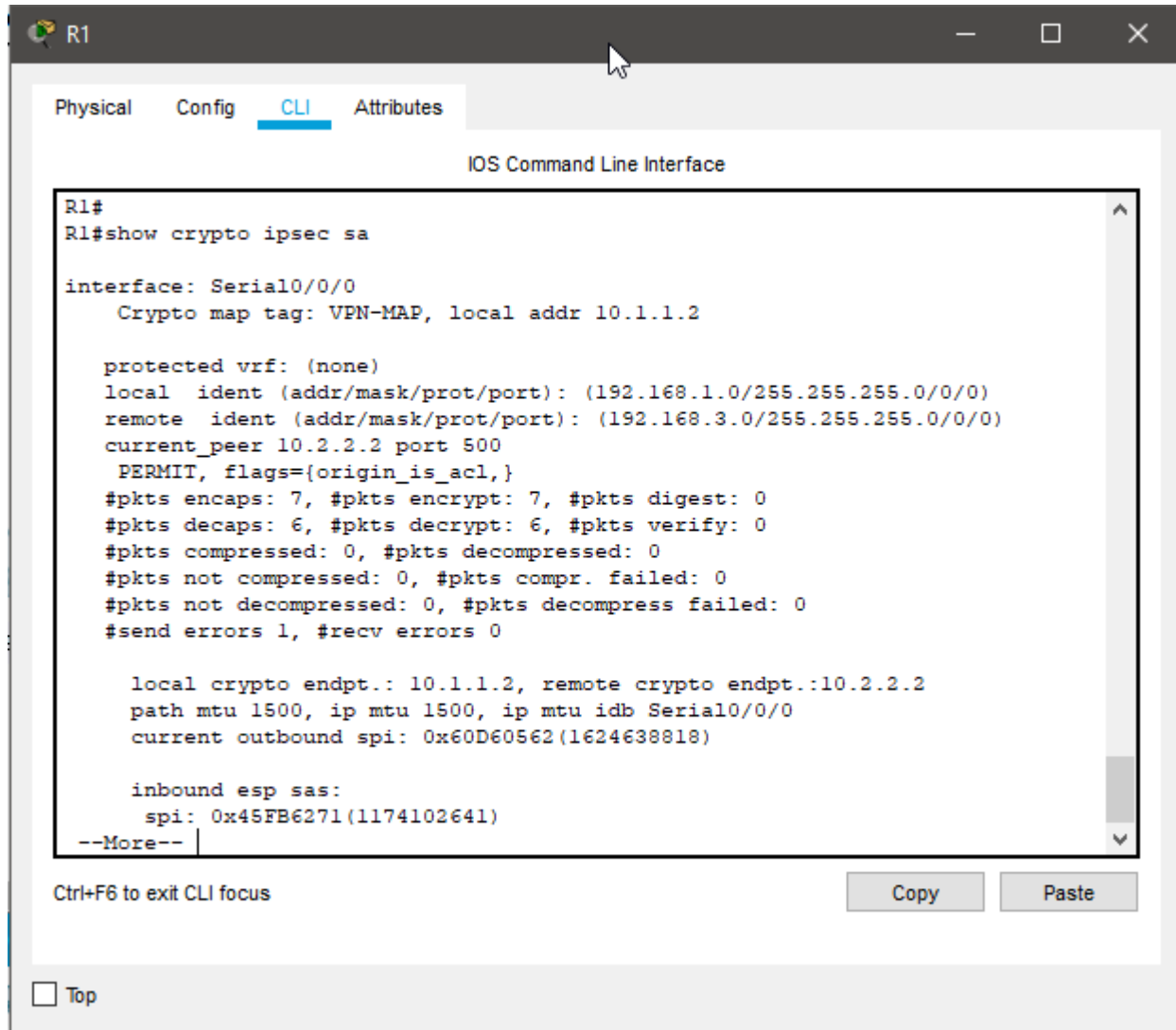
Pinging 192.168.2.3 with 32 bytes of data:

Reply from 192.168.2.3: bytes=32 time=2ms TTL=126
Reply from 192.168.2.3: bytes=32 time=1ms TTL=126
Reply from 192.168.2.3: bytes=32 time=1ms TTL=126
Reply from 192.168.2.3: bytes=32 time=6ms TTL=126

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 6ms, Average = 2ms

C:\>
```

#### Paso 5: Verificar el túnel.



The screenshot shows a network device (R1) CLI window with the following content:

```
R1#
R1#show crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: VPN-MAP, local addr 10.1.1.2

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 10.2.2.2 port 500
    PERMIT, flags={origin_is_acl,}
#pkts encaps: 7, #pkts encrypt: 7, #pkts digest: 0
#pkts decaps: 6, #pkts decrypt: 6, #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.: 10.1.1.2, remote crypto endpt.:10.2.2.2
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
current outbound spi: 0x60D60562(1624638818)

inbound esp sas:
    spi: 0x45FB6271(1174102641)
--More--
```

At the bottom of the CLI window, there is a status bar with the text "Ctrl+F6 to exit CLI focus" and two buttons: "Copy" and "Paste". Below the CLI window, there is a checkbox labeled "Top".

## **CONCLUSIONES**

### **MACÍAS CASTILLO JOSUÉ**

En esta práctica se pudo conocer cómo se configura una VPN desde un router con los comandos mostrados en la práctica algo que me llamó la atención fue que se estaba utilizando el algoritmo de cifrado llamado AES, yo en el pasado he trabajado con él en otra materia y conozco bien cómo funciona ya que tuve la dicha de hacer una práctica donde lo programe, algo que me llamó la atención es el uso de las Access-list para armar el túnel de la VPN y a su vez encriptarlo con el algoritmo AES, cuando se realiza el ping de una PC a otra se nota como toma en cuenta solo a los dispositivos que están dentro de la VPN como por ejemplo la PC-A y PC-C mientras que ignora cualquier tráfico de la PC-B.

### **OCHOA MONROY JOSÉ LUIS**

En esta práctica, considero que tuvimos la oportunidad de aprender un tema bastante relevante para la época actual dentro de la administración de redes. Con la evolución tecnológica y por las circunstancias que hemos vivido como humanidad, cada día se vuelve más importante que los miembros de una organización puedan trabajar desde diferentes ubicaciones geográficas en un medio de comunicación eficiente a la vez que seguro. Además, hay contenido en Internet al que únicamente es posible acceder desde ciertas regiones, e incluso existen aún países con políticas represivas muy fuertes en cuanto a la navegación por la Internet. En ambos casos, las VPN juegan un papel fundamental, lo cual a su vez requiere administradores de red con dominio en la construcción de este tipo de infraestructura.

## **REFERENCIAS**

- ITESA, Cisco Networking Academy. (s.f.). Aspectos básicos de las VPN. Recuperado el 14 de enero de 2021, de:  
<https://www.itesa.edu.mx/netacad/networks/course/module7/index.html#7.3.1.1>

- ITESA, Cisco Networking Academy. (s.f.). Seguridad de protocolo de Internet. Recuperado el 14 de enero de 2021, de:  
<https://www.itesa.edu.mx/netacad/networks/course/module7/index.html#7.3.1.1>