Instituto Tecnológico y de Estudios Superiores de Monterrey

Actividad 3.4. Configuración de VPNs basadas en IPSec

Nombre	Matrícula
Julio Avelino Amador Fernández	A01276513
Juan Pablo Echeagaray González	A00830646
Verónica Victoria García De la Fuente	A00830383
Erika Martínez Meneses	A01028621
Emily Rebeca Méndez Cruz	A00830768
Ana Paula Ruiz Alvaro	A01367467

Análisis de Criptografía y Seguridad

MA2002B.300

Dr. Alberto Francisco Martínez Herrera

10 de junio de 2022

Esta actividad consiste en configurar y verificar un VPN IPSec usando CLI, en otras palabras, se busca verificar la conectividad a través de la red así como configurar el router R1 para un VPN IPSec con R3.

En la topología de red dada se muestran tres routers, y se busca configurar el R1 y el R3 para el tráfico que fluye por los respectivos LANs. El túnel IPSec VPN sale de R1 y llega a R3 pasando por R2, y este último no sabe que hay un VPN. Entonces, lo que IPSec hace es básicamente ofrecer transmisión segura de datos e información sensible en redes no protegidas del Internet.

1. Parámetros de la conexión

Para configurar la conexión VPN se han seguido los siguientes parámetros especificados en el enunciado de la tarea:

Parámetros	R1	R3
Key Distribution Method	ISAKMP	ISAKMP
Encryption Algorithm	AES	AES
Hash Algorithm	SHA-1	SHA-1
Authentication method	Pre-share	Pre-share
Key Exchange	DH2	DH2
IKE SA Lifetime	86400	86400
ISAKMP key	vpnpa55	vpnpa55

Tabla 1: Parámetros de la política IPSec Fase 1

Parámetros	R1	R3
Transform set	VPN-SET	VPN-SET
Peer Hostname	R3	R1
Peer IP Address	10.2.2.2	10.1.1.2
Network to be encrypted	192.168.1.0/24	192.168.3.0/24
Crypto Map Name	VPN-MAP	VPN-MAP
SA establishment	ipsec-isakmp	ipsec-isakmp

Tabla 2: Parámetros de la política IPSec Fase 2

Aunado a estos parámetros, los routers cuentan con las siguientes pre-configuraciones:

- Password for console line: `ciscoconpa55`
- Password for vty lines: `ciscovtypa55`
- Enable password: `ciscoenpa55`
- RIP version 2

2. Procedimiento

2.1. Configuración de IPSec en Router 1

En esta primera sección se configurarán todos los parámetros de la conexión IPSec que el router 1 necesita, como referencia a los métodos seleccionados, por favor ver las tablas 1, 2.

2.1.1. Conectividad entre PC-C y PC-A

Primero se verifica el estado de la conexión en la red, se realizará un `ping` desde la PC-A hacia la PC-C para verificar que existe una conexión en buen estado antes de comenzar a trabajar; este paso se ilustra en la figura 1.

2.1.2. Identificación de tráfico a través de R1

Después se configura un `acces-list` que catalogue como interesante todo el tráfico entre R1 y R3. Para este paso se utilizan los IP proporcionados en la tabla 2. El comando usado para crear esta lista es `access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255` como demostramos en la figura 2.

2.1.3. Configuración de propiedades ISAKMP en R1. Fase 1

Ya que se ha definido el tráfico interesante a través de R1, se captura la cadena de comandos presentada en la figura 3 para aplicar todos los parámetros establecidos en la tabla 1.

2.1.4. Configuración de propiedades ISAKMP en R1. Fase 2

Una vez se han configurado los parámetros de la fase 1, se configuran los de la fase 2 descritos en la tabla 2 mediante los comandos mostrados en la imagen 4.

2.1.5. Configuración del crypto map en la interfaz de salida

Para finalizar la configuración de R1, accedemos a la interfaz `s0/0/0/0` y se aplica el `VPN-MAP` definido en el paso anterior, como se demuestra en la figura 5.

2.2. Configuración de IPSec en Router 3

Los pasos descritos en la sección anterior se repetirán para R3.

2.2.1. Configuración de R3 para soportar conexión VPN

En esta tarea se busca configurar los parámetros IPSec en R3, y lo primero que se debe hacer es configurar R3 para el VPN de R1. Esto se empieza por abrir la línea de comandos de R3, poner las respectivas contraseñas de acceso y agregar el `access-list` definido con anterioridad mediante el comando `access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255`. Esto lo demostramos en la figura 6.

2.2.2. Configuración de propiedades ISAKMP en R3. Fase 1

Una vez que se ha definido el tráfico interesante que puede pasar por R3, se configuran los parámetros de la conexión IPSec fase 1 descritos en la tabla 1, esto se realiza mediante la secuencia de comandos descrita en la figura 7.

2.2.3. Configuración de propiedades ISAKMP en R3. Fase 2

Ya que la configuración de los parámetros de la fase 1 ha surtido efecto, se configuran los de la fase 2 descritos en la tabla 2 mediante los comandos mostrados en la figura 8.

2.2.4. Configuración del crypto map en la interfaz de salida

Para finalizar la configuración de R1, accedemos a la interfaz `s1/0/0/0` y se aplica el `VPN-MAP` definido en el paso anterior, como se demuestra en la figura 9.

2.3. Verificar el IPSec del VPN

2.3.1. Estado del túnel antes del tráfico *interesante*

Para verificar que el `VPN` establecido funcione de manera correcta, se checará si es que hay paquetes que hayan fluido por R1 que fuesen encriptados. Desde R1 se ejecuta el comando `show crypto ipsec sa`; como no se han enviado paquetes por la red desde que comenzó el proceso de configuración, no debería de haber ningún paquete encriptado en el registro, esto lo comprobamos en la figura 10.

2.3.2. Creación de tráfico *interesante*

Ya que se comprueba que ningún paquete ha sido encriptado, generamos tráfico *interesante* entre PC-A y PC-C, el comando `ping` bastará para lograr esta faena. La conexión es exitosa como se muestra en la figura 11.

2.3.3. Estado del túnel después del tráfico *interesante*

Se repite el paso anterior en el que checamos si es que han habido mensajes encriptados. Vemos que ahora el número se ha incrementado como se demuestra en la figura 12.

2.3.4. Creación de tráfico no *interesante*

Ahora se crea un tráfico *no interesante* que pase por la red, desde PC-A se enviarán paquetes a la PC-B como se muestra en la figura 13.

2.3.5. Estado del túnel después del tráfico no *interesante*

Para finalizar el chequeo de la `VPN` implementada, se checa de nuevo que el conteo de paquetes encriptados que pasan por R1 no haya incrementado, ver figura 13.

Adjuntamos al final una captura de pantalla 15, como evidencia de haber completado esta actividad con éxito.

A. Evidencias de actividad

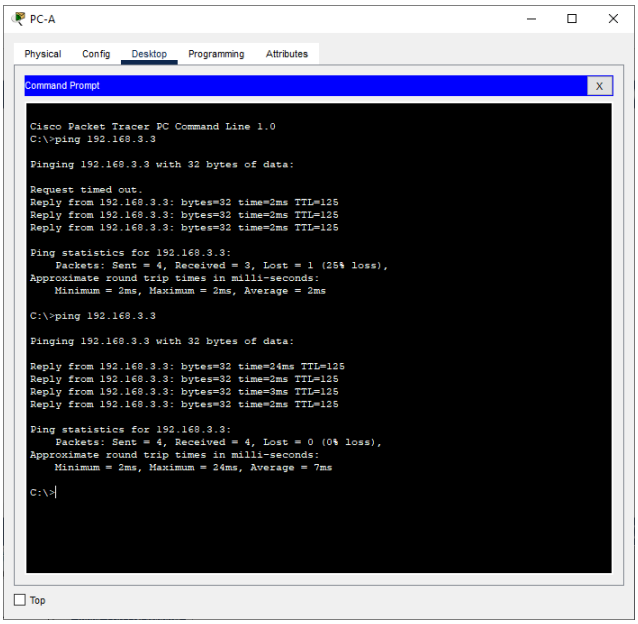

Figura 1: Prueba de conectividad entre PC-C y PC-A

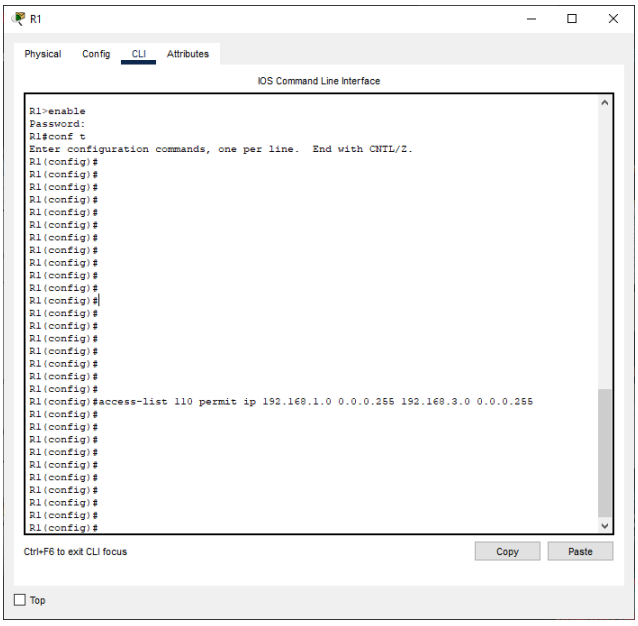

Figura 2: Identificación de tráfico interesante en Router 1

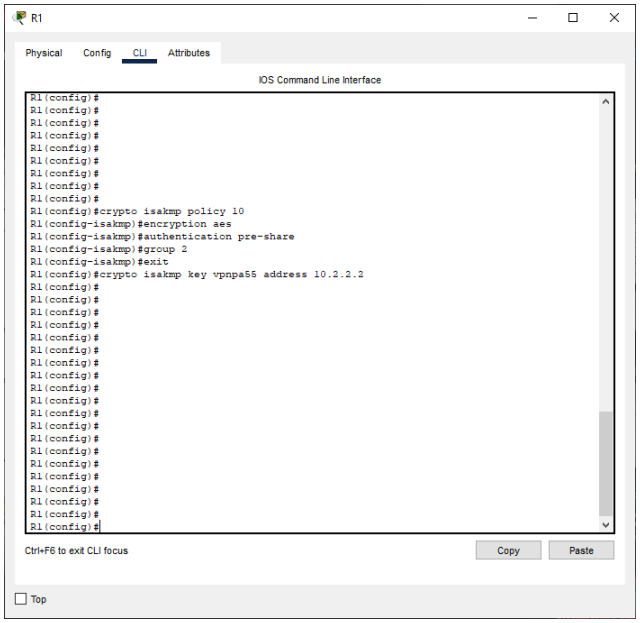

Figura 3: Configuración de parámetros IPSec Fase 1 en Router 1

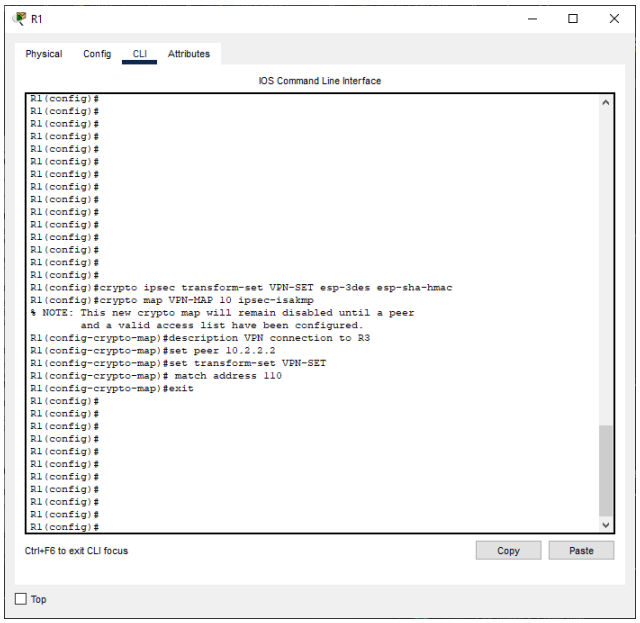

Figura 4: Configuración de parámetros IPSec Fase 2 en Router 1

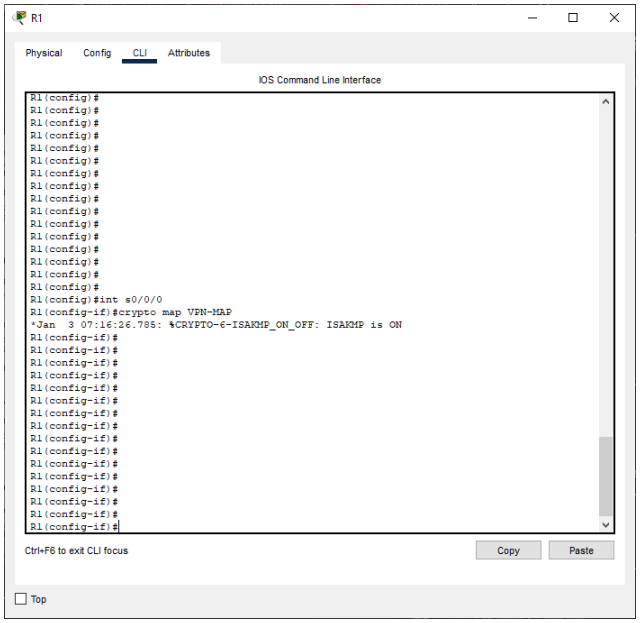

Figura 5: Aplicación del `VPN-MAP` en la interfaz de salida de R1

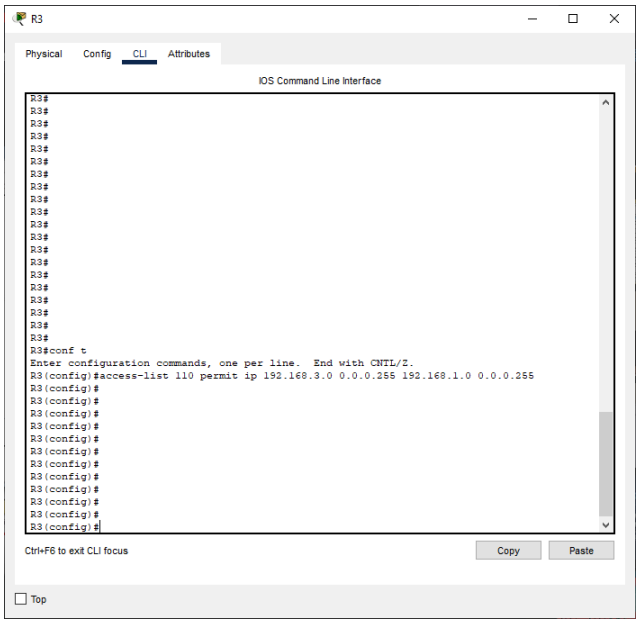

Figura 6: Creación del `access-list` para la conexión a R1

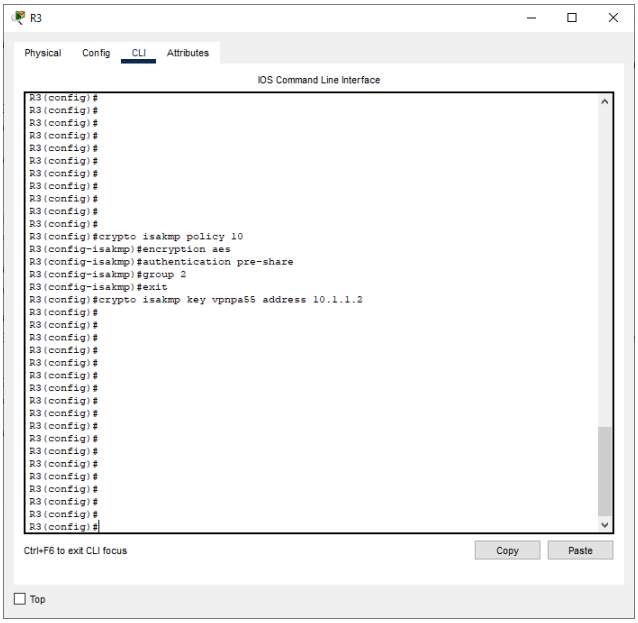

Figura 7: Configuración de parámetros IPSec Fase 1 en Router 3

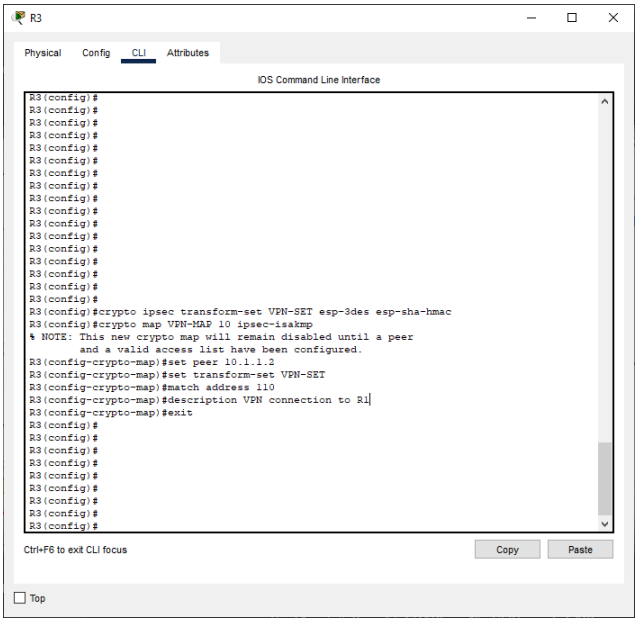

Figura 8: Configuración de parámetros IPSec Fase 2 en Router 3

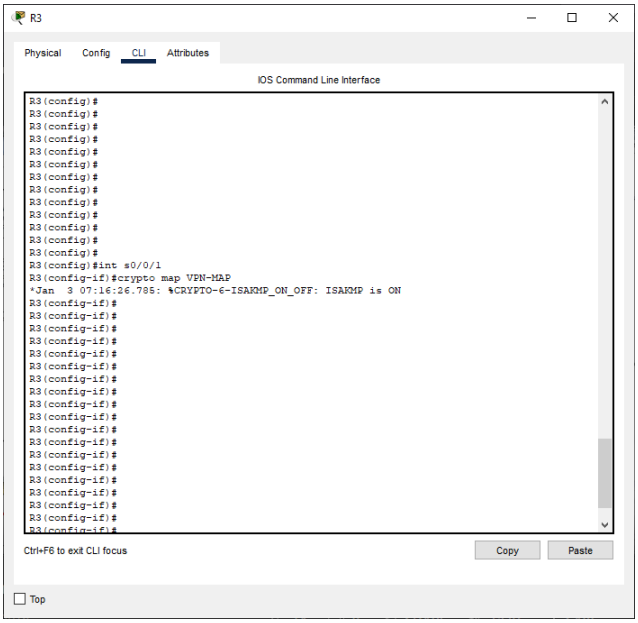

Figura 9: Aplicación del `VPN-MAP` en la interfaz de salida de R3

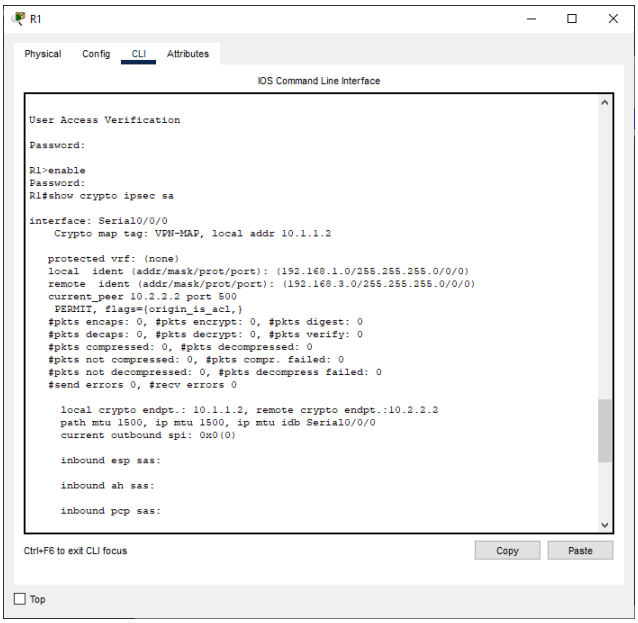

Figura 10: Verificación de paquetes encriptados que hayan fluido por R1

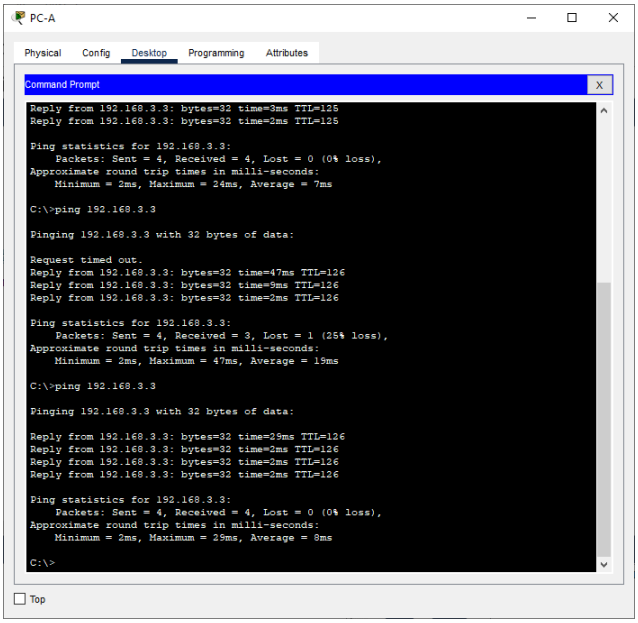

Figura 11: Creación de tráfico interesante por R1

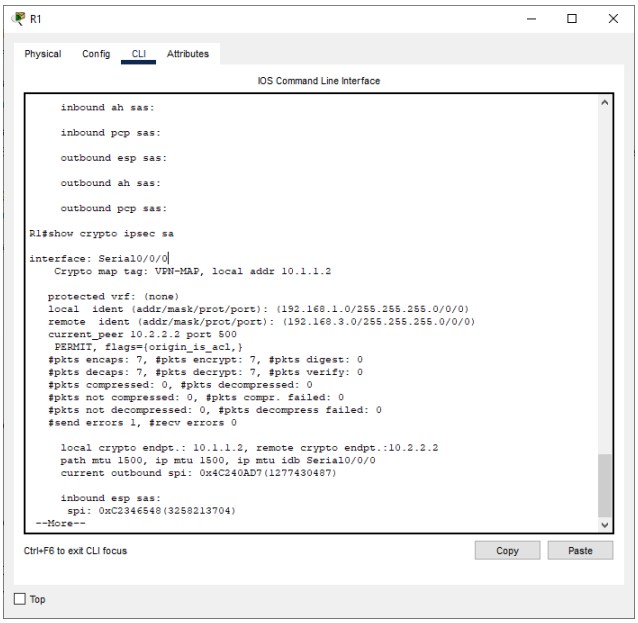

Figura 12: Verificación de paquetes interesantes a través de R1 después de tráfico interesante

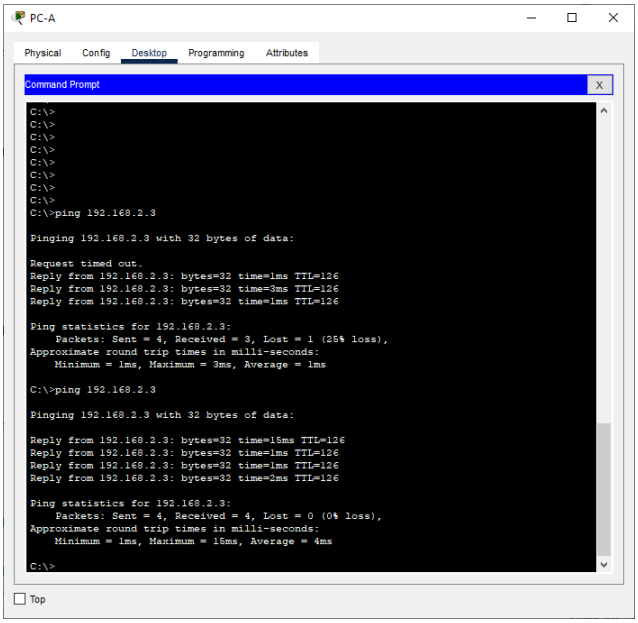

Figura 13: Creación de tráfico no interesante por R1

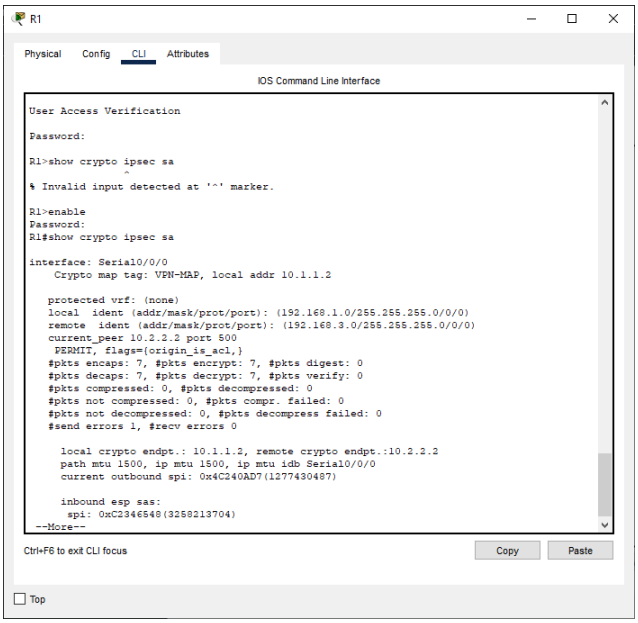

Figura 14: Verificación de paquetes interesantes a través de R1 después del tráfico no interesante

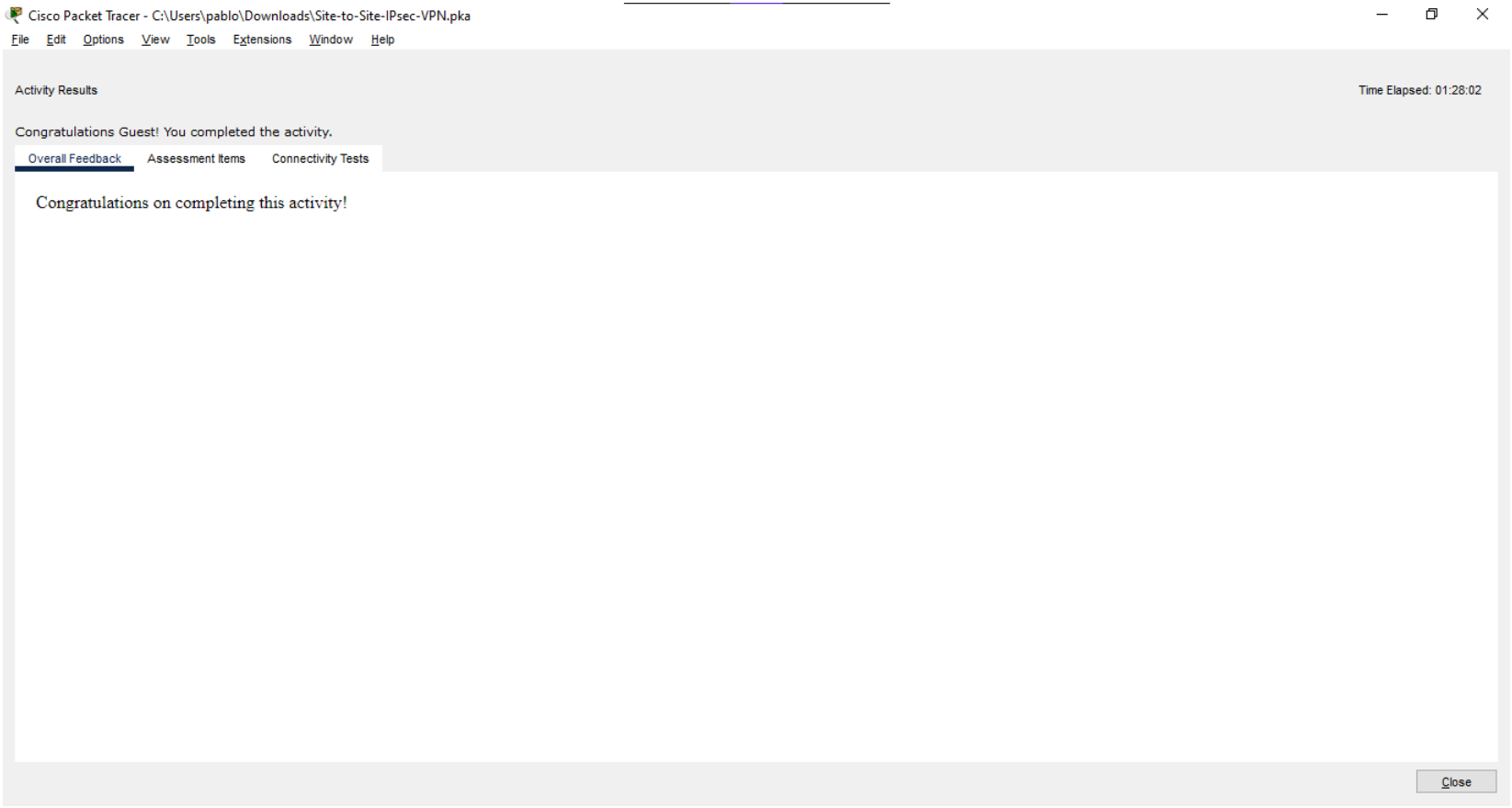

Figura 15: Evidencia de finalización de actividad