

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

CARRERA: Ingeniería en Tecnologías de la Información

MATERIA: CNO V: Seguridad Informática

TRABAJO: Actividad 06 IPSEC VPN

Grupo: T46A

PARCIAL 1

Donaldo Demián Gómez Arreguín 179822

I

Profesor: Servando Lopez

Contreras

Fecha de entrega: 16/02/202

Introducción

Las Redes Privadas Virtuales (VPN) basadas en IPSec constituyen una de las soluciones más utilizadas para asegurar la comunicación entre redes remotas a través de infraestructuras públicas como Internet.

IPSec proporciona mecanismos de cifrado, autenticación e integridad de datos que permiten proteger la información frente a accesos no autorizados, garantizando la confidencialidad durante su transmisión.

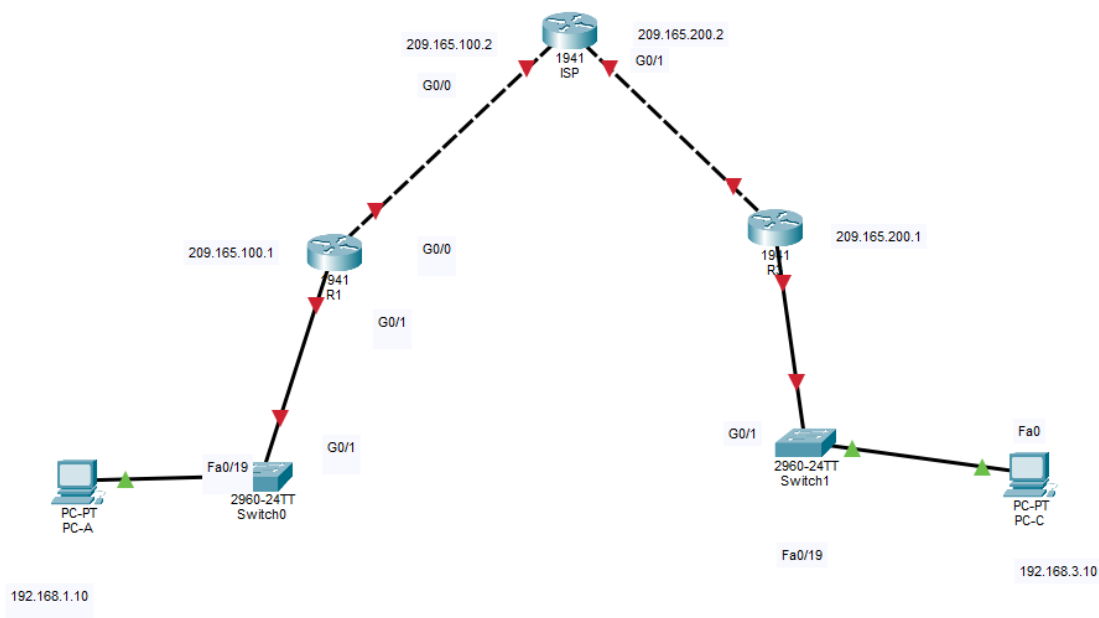
En la presente práctica se implementó una VPN Site-to-Site utilizando routers Cisco, estableciendo un túnel seguro entre dos redes LAN distintas interconectadas mediante un ISP simulado. Para ello se configuraron las fases de negociación ISAKMP e IPSec, listas de control de acceso y mapas criptográficos, verificando posteriormente el funcionamiento del túnel mediante pruebas de conectividad y monitoreo de asociaciones de seguridad.

Desarrollo

Es necesario brindar la estructura correcta entre los routers R1, R3 e ISP y los equipos finales, garantizando la conectividad básica antes de implementar seguridad, lo cual es un requisito indispensable para IPSec.

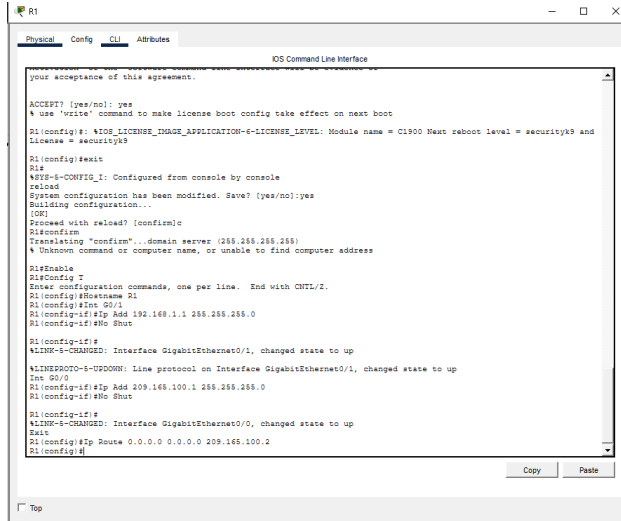
El router ISP únicamente enruta tráfico entre ambos routers sin aplicar cifrado, simulando una red pública.

Configuración inicial



Configuraciones iniciales

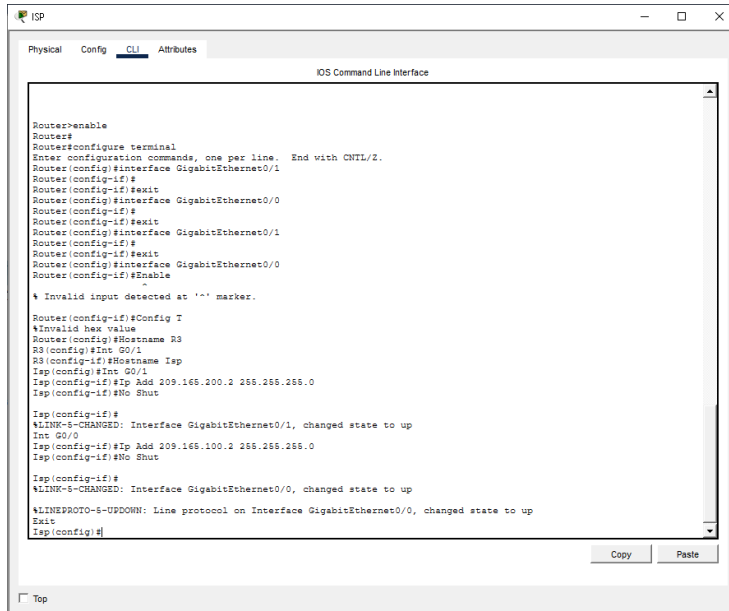
R1



```
your acceptance of this agreement.
ACCEPT? [yes/no]: yes
% use 'write' command to make license boot config take effect on next boot
R1(config): %IOS_LICENSE_IMAGE_APPLICATION-6-LICENSE_LEVEL: Module name = C1900 Next reboot level = security9 and
License = security9
R1(config)#exit
R1#
%SYS-5-CONFIG_1: Configured from console by console
reload
System configuration has been modified. Save? [yes/no]: yes
Building configuration...
[OK]
Proceed with reload? [confirm]:
R1confirm
Translating "confirm"...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer address
R1#enable
R1#configure t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#hostname R1
R1(config)#int G0/1
R1(config-if)#ip Add 192.168.1.1 255.255.255.0
R1(config-if)#no Shut
R1(config-if)#
%LINK-8-CHANGED: Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
R1(config-if)#ip Add 209.165.100.1 255.255.255.0
R1(config-if)#no Shut
R1(config-if)#
%LINK-8-CHANGED: Interface GigabitEthernet0/0, changed state to up
Exit
R1(config)#ip Route 0.0.0.0 0.0.0.0 209.165.100.2
R1(config)#
```

1. Enable
2. Config T
3. Hostname R1
4. Int G0/1
5. Ip Add 192.168.1.1
255.255.255.0
6. No Shut
7. Int G0/0
8. Ip Add 209.165.100.1
255.255.255.0
9. No Shut
10. Exit
11. Ip Route 0.0.0.0 0.0.0.0
209 165 100 2

ISP



```
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface GigabitEthernet0/1
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/1
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0
Router(config-if)#enable
Router(config-if)#
% Invalid input detected at '^' marker.
Router(config-if)#Config T
%Invalid hex value
Router(config)#hostname ISP
ISP(config)#int G0/1
ISP(config-if)#ip Add 209.165.200.2 255.255.255.0
ISP(config-if)#no Shut
ISP(config-if)#
%LINK-8-CHANGED: Interface GigabitEthernet0/1, changed state to up
Int G0/0
ISP(config-if)#ip Add 209.165.100.2 255.255.255.0
ISP(config-if)#no Shut
ISP(config-if)#
%LINK-8-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
Exit
ISP(config)#
```

1. hostname ISP
2. interface g0/1
3. ip address 209.165.200.2
255.255.255.0
4. no shutdown
5. interface g0/0
6. ip address 209.165.100.2
255.255.255.0
7. no shutdown
8. exit

R3

```
Router(config-if)#  
Router(config-if)#exit  
Router(config)#interface GigabitEthernet0/0  
Router(config-if)#enable  
* Invalid input detected at '^' marker.  
Router(config-if)#Config T  
*Invalid hex value  
Router(config)#Hostname R3  
R3(config)#Int G0/1  
R3(config-if)#Ip Add 192.168.3.1 255.255.255.0  
R3(config-if)#No Shut  
R3(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  
Int G0/0  
R3(config-if)#Ip Add 209.165.200.1 255.255.255.0  
R3(config-if)#No Shut  
R3(config-if)#  
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up  
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up  
Exit  
R3(config)#Ip Route 0.0.0.0 0.0.0.0 209.165.200.2  
R3(config)#Int G0/0  
R3(config-if)#Ip Route 0.0.0.0 0.0.0.0 209.165.200.2  
R3(config)#EXIT  
R3#  
*SYS-5-CONFIG_I: Configured from console by console  
Ip Route 0.0.0.0 0.0.0.0 209.165.200.2
```

1. Enable
2. Config T
3. Hostname R3
4. Int G0/1
5. Ip Add 192.168.3.1
255.255.255.0
6. No Shut
7. Int G0/0
8. Ip Add 209.165.200.1
255.255.255.0
9. No Shut
10. Exit
11. Ip Route 0.0.0.0 0.0.0.0
209 165 200 2

Licencia de seguridad habilitada

Los routers Cisco 1941 requieren habilitar el paquete securityk9 para poder utilizar IPSec, ya que sin esta licencia los comandos de seguridad no estarían disponibles.

Esto se realizó mediante el comando:

license boot module c1900 technology-package securityk9
seguido de un reinicio del sistema (reload).

license boot module c1900 technology-package securityk9

Implementación ACLs

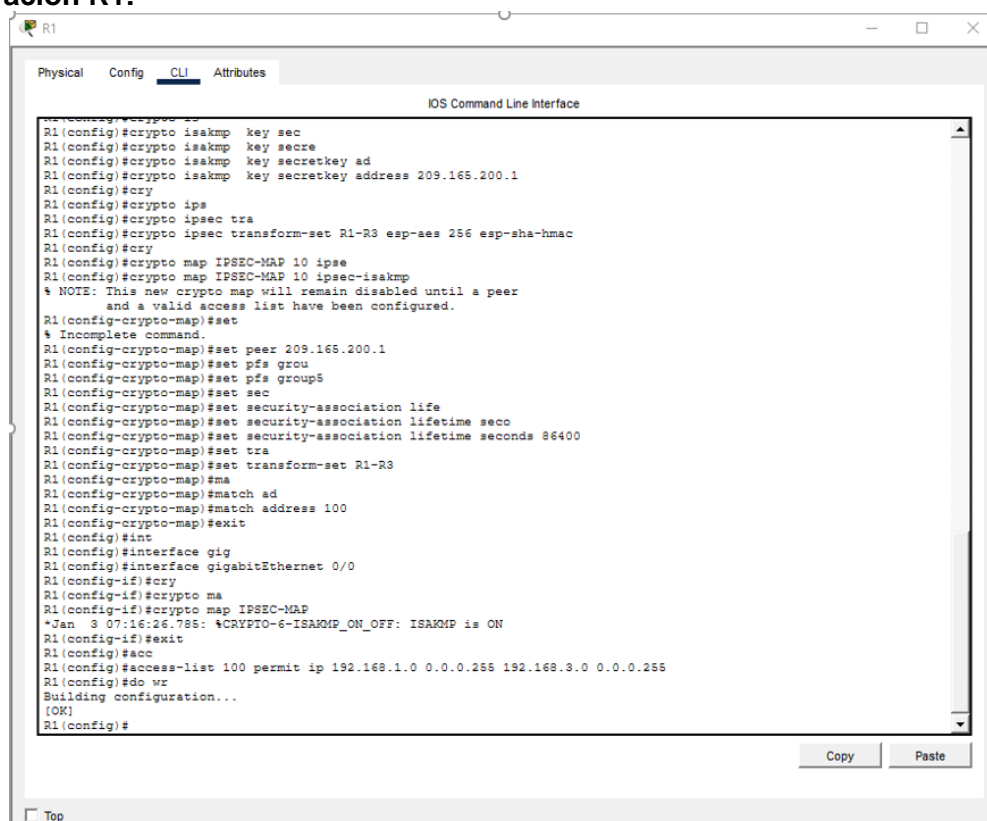
Se configuró una lista de control de acceso (ACL) para identificar el tráfico interesante entre las redes LAN 192.168.1.0/24 y 192.168.3.0/24, el cual será protegido por IPSec.

```
access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
```

```
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)#do wr
R3(config)#access-list 100 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
R3(config)#do wr
```

Fase 1: ISAKMP policy

Configuración R1:



```
R1
Physical Config CLI Attributes
IOS Command Line Interface
R1(config)#crypto isakmp key sec
R1(config)#crypto isakmp key secre
R1(config)#crypto isakmp key secretkey ad
R1(config)#crypto isakmp key secretkey address 209.165.200.1
R1(config)#cry
R1(config)#crypto ipse
R1(config)#crypto ipsec tra
R1(config)#crypto ipsec transform-set R1-R3 esp-aes 256 esp-sha-hmac
R1(config)#cry
R1(config)#crypto map IPSEC-MAP 10 ipse
R1(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.
R1(config-crypto-map)#set
% Incomplete command.
R1(config-crypto-map)#set peer 209.165.200.1
R1(config-crypto-map)#set pfs grou
R1(config-crypto-map)#set pfs group5
R1(config-crypto-map)#set sec
R1(config-crypto-map)#set security-association life
R1(config-crypto-map)#set security-association lifetime seco
R1(config-crypto-map)#set security-association lifetime seconds 86400
R1(config-crypto-map)#set tra
R1(config-crypto-map)#set transform-set R1-R3
R1(config-crypto-map)#ma
R1(config-crypto-map)#match ad
R1(config-crypto-map)#match address 100
R1(config-crypto-map)#exit
R1(config)#int
R1(config)#interface gig
R1(config)#interface gigabitEthernet 0/0
R1(config-if)#cry
R1(config-if)#crypto ma
R1(config-if)#crypto map IPSEC-MAP
*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config-if)#exit
R1(config)#acc
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)#do wr
Building configuration...
[OK]
R1(config)#
```

Configuración R3:

R3

Physical Config **CLI** Attributes

IOS Command Line Interface

```
R3(config)#crypto ipsec
R3(config)#crypto ipsec tra
R3(config)#crypto ipsec transform-set R3-R1 esp-a
R3(config)#crypto ipsec transform-set R3-R1 esp-aes 256 esp
R3(config)#crypto ipsec transform-set R3-R1 esp-aes 256 esp-sha-hmac
R3(config)#cry
R3(config)#crypto map IPSEC-MAP 10 ips
R3(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.
R3(config-crypto-map)#set pe
R3(config-crypto-map)#set peer 209.165.100.1
R3(config-crypto-map)#set pfs gro
R3(config-crypto-map)#set pfs group5
R3(config-crypto-map)#set sec
R3(config-crypto-map)#set security-association lifeti
R3(config-crypto-map)#set security-association lifetime second
R3(config-crypto-map)#set security-association lifetime seconds 86400
R3(config-crypto-map)#set tra
R3(config-crypto-map)#set transform-set R3-R1
R3(config-crypto-map)#mat
R3(config-crypto-map)#match ad
R3(config-crypto-map)#match address 100
R3(config-crypto-map)#exi
R3(config-crypto-map)#exit
R3(config)#inte
R3(config)#interface gi
R3(config)#interface gigabitEthernet 0/0
R3(config-if)#cry
R3(config-if)#crypto map IPSEC-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R3(config-if)#exi
R3(config-if)#exit
R3(config)#ac
R3(config)#access-list 100 pe
R3(config)#access-list 100 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
R3(config)#do wr
Building configuration...
[OK]
R3(config)#
```

Copy Paste

☐ Top

ISAKMP es el protocolo utilizado para establecer y negociar las asociaciones de seguridad (SA) entre los routers, permitiendo autenticar los peers y acordar los parámetros de protección del túnel IPsec.

```
crypto isakmp policy 10
encryption aes 256
authentication pre-share
group 5
crypto isakmp key secretkey address 209.165.200.1
```

IPSEC transform-set

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

Crear el mapa criptográfico

R1	R3
<pre>R1(config-if)#crypto map IPSEC-MAP *Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON R1(config-if)#exit R1(config)#acc 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)#do wr Building configuration... [OK] R1(config)#</pre>	<pre>R3(config-if)#crypto map IPSEC-MAP *Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON R3(config-if)#exi R3(config-if)#exit R3(config)#ac R3(config)#access-list 100 pe R3(config)#access-list 100 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255 R3(config)#do wr Building configuration... [OK] R3(config)#</pre>

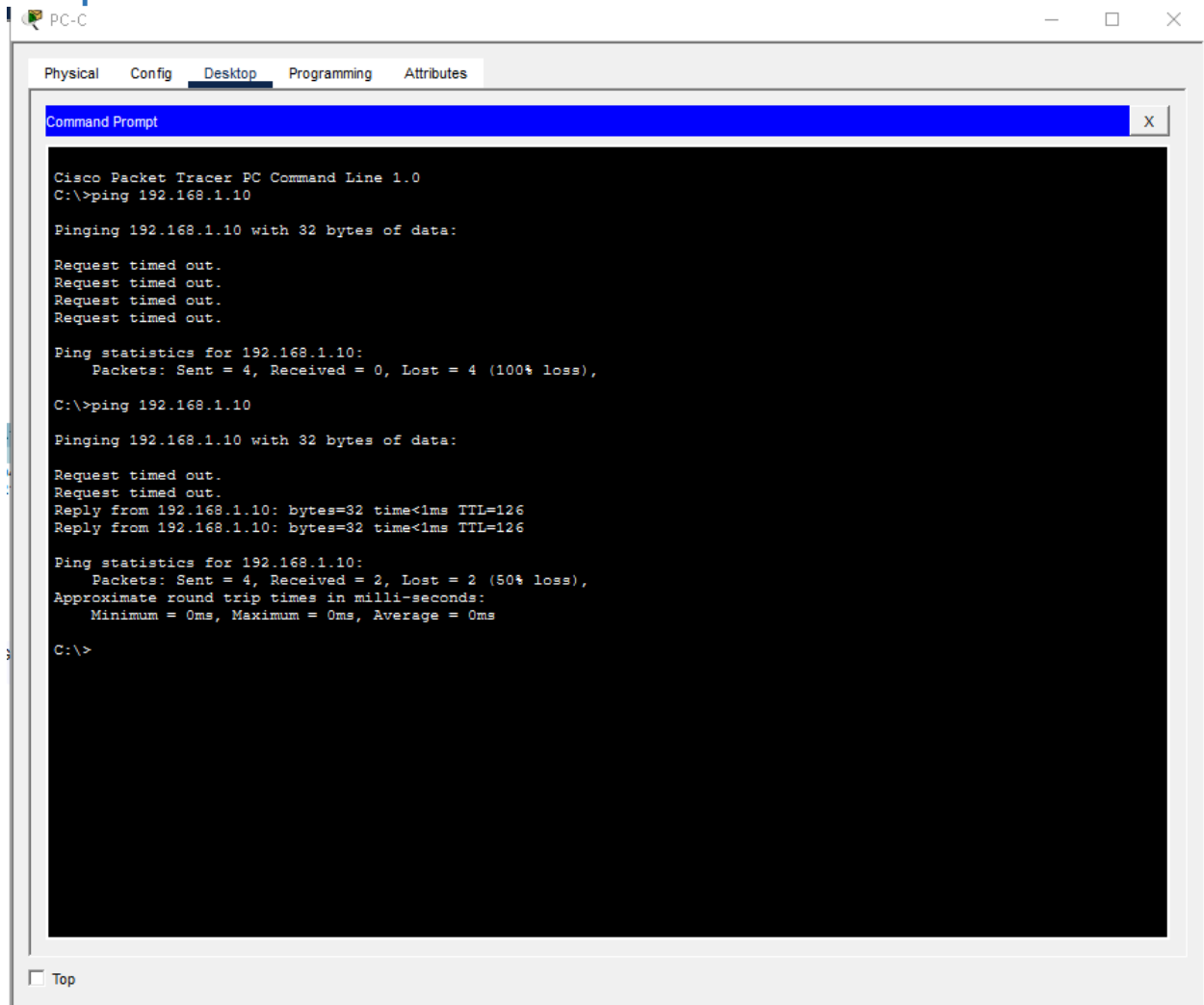
El crypto map vincula el peer remoto, el transform-set y la ACL que define el tráfico protegido, además de parámetros de seguridad como Perfect Forward Secrecy y lifetime.

Aplicar el mapa criptográfico

R1	R3
<pre>R1(config)#interface gigabitEthernet 0/0 R1(config-if)#cry R1(config-if)#crypto ma R1(config-if)#crypto map IPSEC-MAP *Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON</pre>	<pre>R3(config-if)#cry R3(config-if)#crypto map IPSEC-MAP *Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON R3(config-if)#exi</pre>


Finalmente, el mapa criptográfico se aplica a la interfaz de salida hacia la red pública (g0/0), activando el túnel IPsec para el tráfico definido en la ACL.

Comprobación de funcionalidad



Se verificó la conectividad entre las redes LAN mediante pruebas de ping desde la PC de la red 192.168.3.0 hacia la PC de la red 192.168.1.0, observando respuesta exitosa.

Verificación del túnel IPsec

 R1

Physical

Config

CLI

Attributes

IOS Command Line Interface

```
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#sho
R1(config)#show cr
R1(config)#show crypto isakmp sa
^
% Invalid input detected at '^' marker.

R1(config)#configure
R1(config)#configure
^
% Invalid input detected at '^' marker.

R1(config)#terminal
^
% Invalid input detected at '^' marker.

R1(config)#is
R1(config)#cr
R1(config)#show cr
R1(config)#show crypto isakmp
^
% Invalid input detected at '^' marker.

R1(config)#show cr
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
ss
% Incomplete command.

R1#sho
R1#show cr
R1#show crypto isa
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        1026     0 ACTIVE

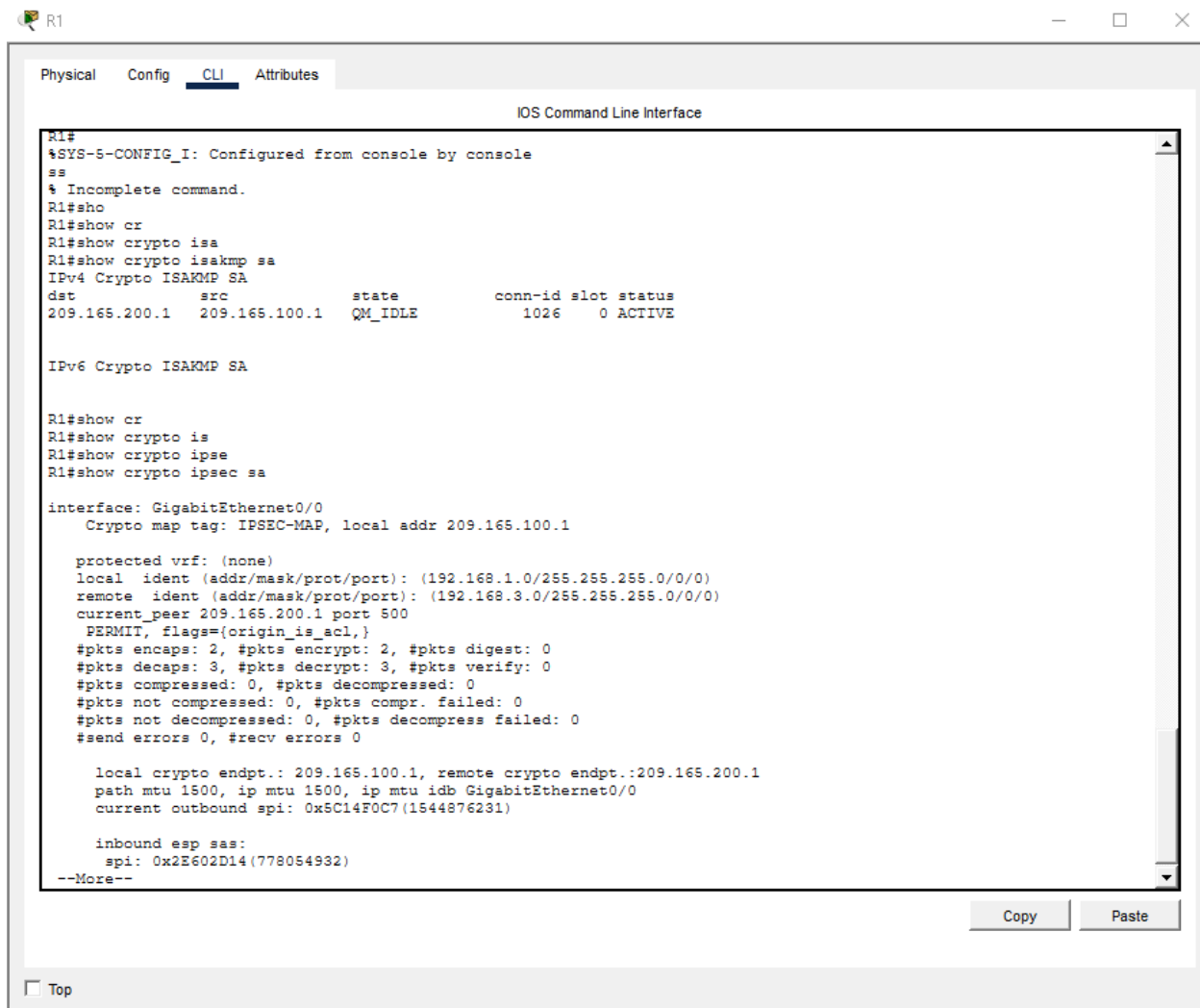
IPv6 Crypto ISAKMP SA

R1#
```

Copy

Paste

☐ Top



```
R1#
%SYS-5-CONFIG_I: Configured from console by console
ss
% Incomplete command.
R1#sho
R1#show cr
R1#show crypto isa
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        1026    0  ACTIVE

IPv6 Crypto ISAKMP SA

R1#show cr
R1#show crypto is
R1#show crypto ipse
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: 2, #pkts encrypt: 2, #pkts digest: 0
#pkts decaps: 3, #pkts decrypt: 3, #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 0, #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: 0x5C14F0C7(1544876231)

inbound esp sas:
spi: 0x2E602D14(778054932)
--More--
```

Se verificó el estado del túnel IPsec mediante el comando `show crypto ipsec sa`, observando el intercambio de paquetes cifrados y descifrados sin errores, confirmando el funcionamiento correcto del túnel VPN.

Lecciones aprendidas

Durante el desarrollo de la práctica se comprendió la importancia de establecer primero la conectividad básica entre dispositivos antes de implementar mecanismos de seguridad como IPsec.

Se aprendió que la configuración de una VPN IPsec requiere la correcta coincidencia de parámetros en ambos extremos, tales como políticas ISAKMP, claves compartidas, transform-sets y ACLs, ya que cualquier discrepancia impide la formación del túnel.

Asimismo, se reforzó el uso de comandos de verificación como `show crypto isakmp sa` y `show crypto ipsec sa`, los cuales permiten comprobar el estado del túnel y el intercambio de paquetes cifrados.

Finalmente, la práctica permitió comprender de manera aplicada cómo las VPN IPsec aseguran la comunicación entre sedes remotas, garantizando confidencialidad, integridad y

autenticación en redes inseguras.

Conclusión

La implementación de IPSec VPN permitió asegurar la comunicación entre dos redes remotas a través de una red pública simulada.

El uso de cifrado AES, autenticación mediante clave compartida y control de tráfico mediante ACL garantizó la confidencialidad e integridad de la información transmitida.

Las pruebas de conectividad y verificación del túnel confirmaron el funcionamiento correcto de la VPN Site-to-Site.