



# SEGURIDAD EN RED

Configuración de VPN y ASA.

## DESCRIPCIÓN BREVE

A lo largo de este documento vamos a describir la manera de configurar los diferentes equipos para cumplir con los objetivos de la práctica.

[j.amoros@alumnos.upm.es](mailto:j.amoros@alumnos.upm.es)

Máster en Ingeniería informática

## Tarea 1

- Establezca un túnel con encapsulación GRE sobre IP entre las dos sucursales.

Establezca el encaminamiento necesario para que el tráfico entre sucursales utilice dicho túnel, y compruebe que esto es así realizando un traceroute entre equipos de ambas sucursales y viendo que los routers de Internet no aparecen en el camino.

```
#En el router de la sucursal A:

interface Tunnel1
  Tunnel mode gre ip
  ip address 50.50.50.2 255.255.255.0
  mtu 1476
  tunnel destination 209.165.212.2
exit

ip route 209.165.221.8 255.255.255.248 50.50.50.1

#En el router de la sucursal b

Interface Tunnel1
  Tunnel mode gre ip
  ip address 50.50.50.1 255.255.255.0
  mtu 1476
  tunnel source Serial0/0/0
  tunnel destination 209.165.211.2
exit

ip route 209.165.221.1 255.255.255.248 50.50.50.2
```

Tracert desde un pc de la sucursal b a un pc de la sucursal A. No se muestran routers intermedios.

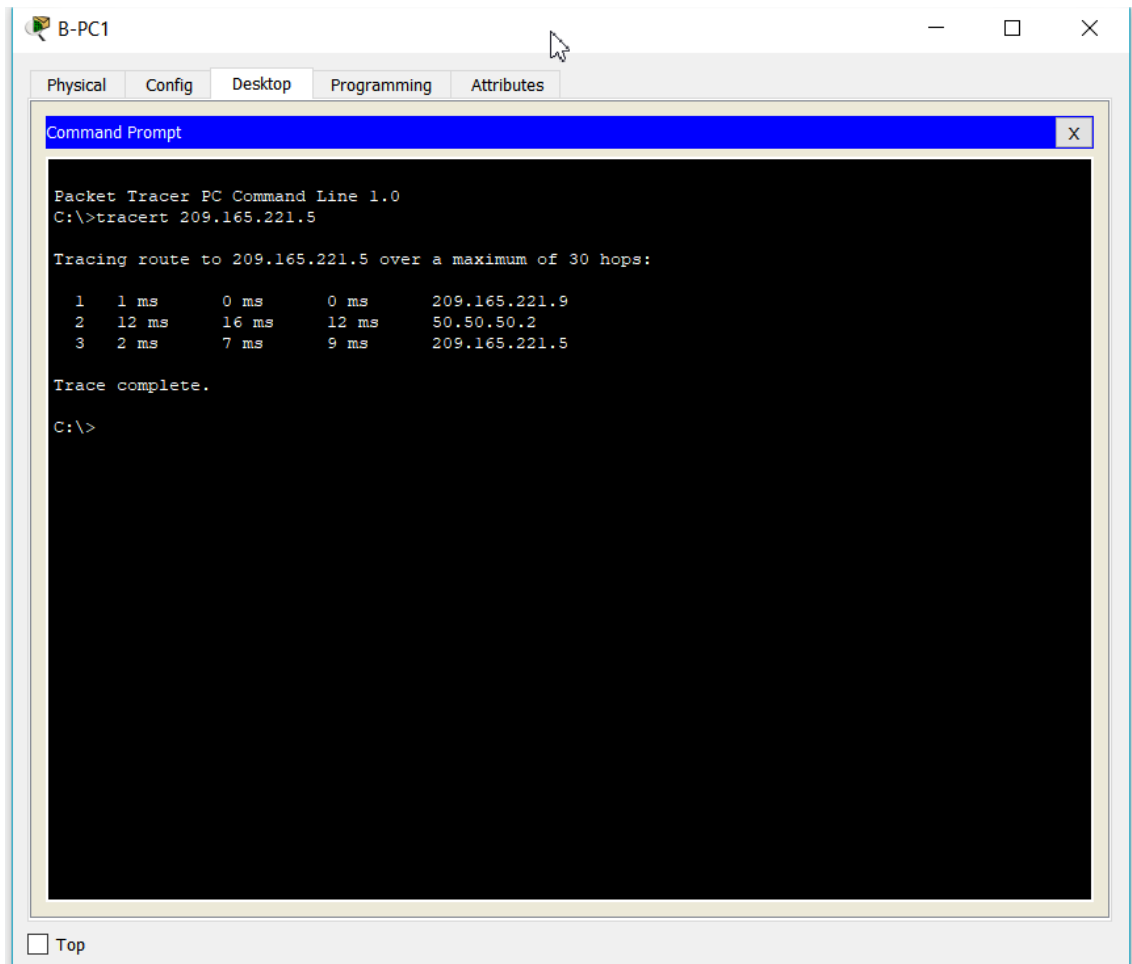


Ilustración 1. Tarea 1 Tracert entre equipos de sucursales.

- En caso de tener direccionamiento privado en las sucursales ¿se podría prescindir de NAT para comunicar equipos diferente subred? Compruebe dicha afirmación creando una subred en la interfaz Gigabit libre de A-R y B-R, comunicándolas por el túnel anterior, sin utilizar NAT .

Tendremos una subred privada en B 192.168.0.0 /24 y otra en A B 192.168.1.0 /24 con lo que los route quedarían de la siguiente manera.

```
#En el router de la sucursal A
interface FastEthernet0/1
    ip address 192.168.1.1 255.255.255.0
exit
```

```
ip route 192.168.0.0 255.255.255.0 50.50.50.1
```

#En el router de la sucursal B

```
interface FastEthernet0/1
```

```
    ip address 192.168.0.1 255.255.255.0
```

```
exit
```

```
ip route 192.168.1.0 255.255.255.0 50.50.50.2
```

#y configuramos 2 pcs asignándole cualquier dirección dentro de la privada.

Así quedaría un ping de la privada de la sucursal B a la privada de la sucursal A.

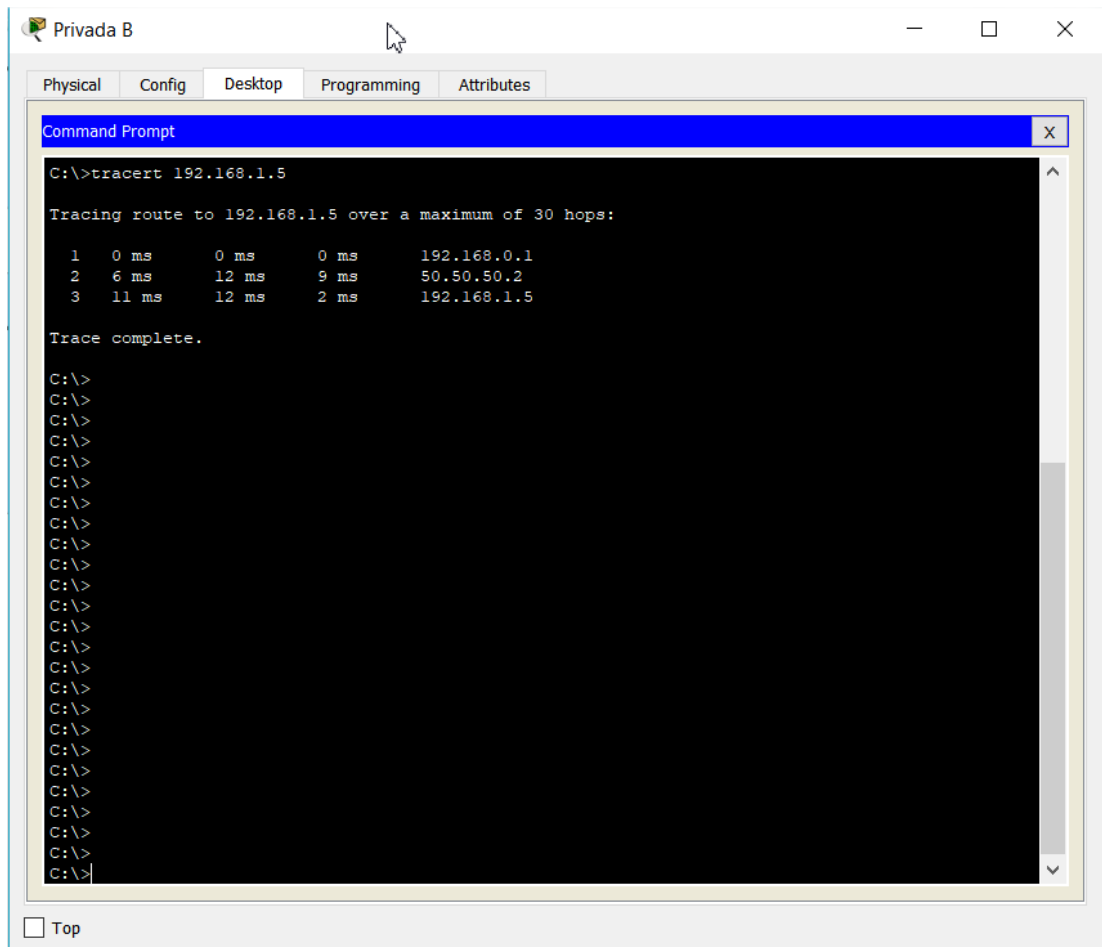


Ilustración 2. Tarea 1 Tracert entre equipos privados de sucursales.

## Tarea 2.

- Configurar una VPN IPsec Site-to-Site para el tráfico entre la subred DMZ de la sede central, y la subred de la sucursal B (redes de direccionamiento público en ambos casos). A continuación, se muestran los parámetros a utilizar en la fase 1 de ISAKMP y en la fase 2 de IPsec:

#El el **router B-R** llevamos a cabo la siguiente configuración

```
crypto isakmp policy 1
    hash sha
    authentication pre-share
    group 2
    lifetime 86400
    encryption aes 256
exit
```

```
crypto isakmp key Vpnpass101 address 209.165.210.2
crypto ipsec transform-set S2-DMZ esp-aes esp-sha-hmac
access-list 101 permit ip 209.165.221.8 0.0.0.7 209.165.0.0 0.0.0.255

crypto map S2-DMZ-MAP 10 ipsec-isakmp
    match address 101
    set pfs group2
    set transform-set S2-DMZ
    set peer 209.165.210.2
Exit

interface s0/0/0
    crypto map S2-DMZ-MAP
exit
```

#El el router C-R llevamos a cabo lo siguiente

```
crypto isakmp policy 1
    hash sha
    authentication pre-share
    group 2
    lifetime 86400
    encryption aes 256
exit

crypto isakmp key Vpnpass101 address 209.165.212.2
crypto ipsec transform-set CENTRAL-S2 esp-aes esp-sha-hmac

access-list 101 permit ip 209.165.0.0 0.0.0.255 209.165.221.8 0.0.0.7

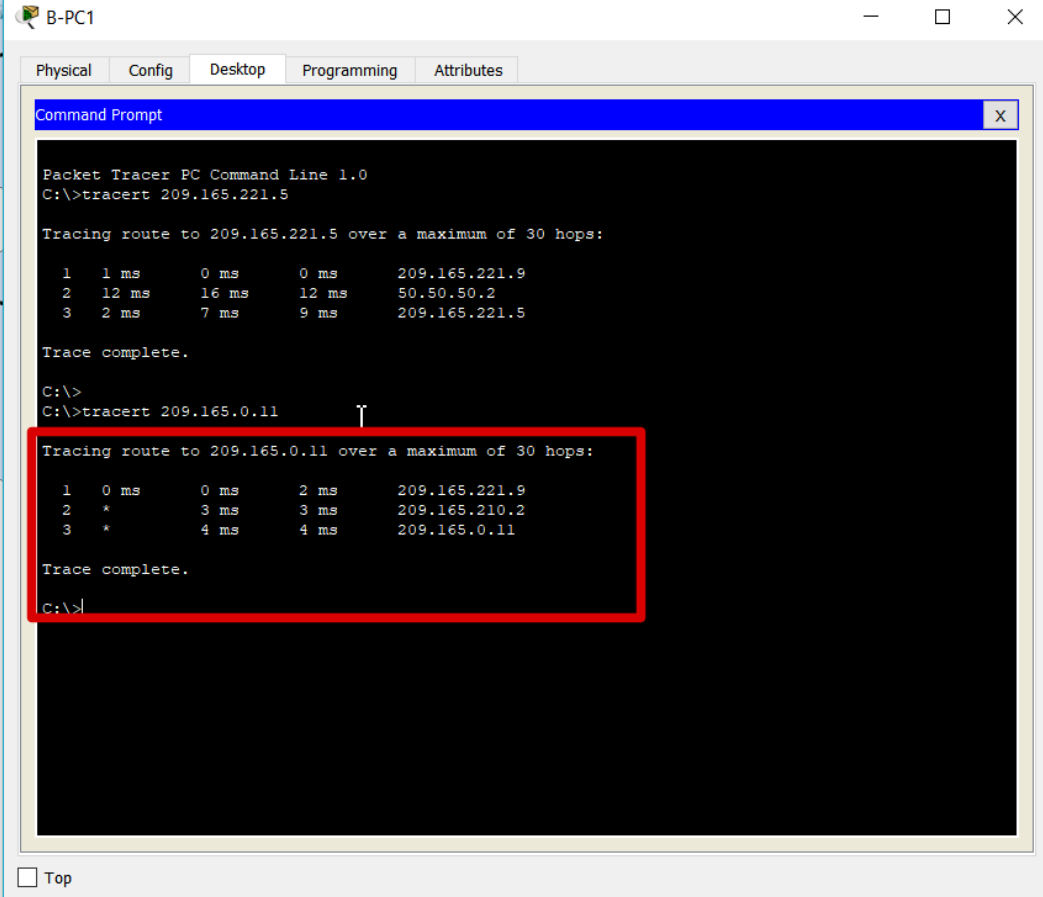
crypto map CENTRAL-ALL-MAP 1 ipsec-isakmp
    match address 101
    set pfs group2
    set transform-set CENTRAL-S2
    set peer 209.165.212.2
Exit

interface s0/0/0
    crypto map CENTRAL-ALL-MAP
exit
```

- Verificar la configuración de VPN comunicando PCs de diferentes sucursales.

Comprobar que los paquetes DMZ y Sucursal B están encriptados, pero no lo están entre DMZ y Sucursal A. Comprobar que en una ruta (traceroute) entre DMZ y Sucursal B no aparecen IPs de los routers de Internet

En la imagen vemos el tracerouter del pc de la sucursal B a un equipo de la DMZ.



```
Packet Tracer PC Command Line 1.0
C:\>tracert 209.165.221.5

Tracing route to 209.165.221.5 over a maximum of 30 hops:

  1  1 ms    0 ms    0 ms    209.165.221.9
  2  12 ms   16 ms   12 ms   50.50.50.2
  3   2 ms    7 ms    9 ms   209.165.221.5

Trace complete.

C:\>
C:\>tracert 209.165.0.11

Tracing route to 209.165.0.11 over a maximum of 30 hops:

  1  0 ms    0 ms    2 ms    209.165.221.9
  2  *       3 ms    3 ms    209.165.210.2
  3  *       4 ms    4 ms    209.165.0.11

Trace complete.

C:\>
```

Ilustración 3. Tarea 2 Tracert entre equipos de la sucursal y la DMZ.

De la misma manera, podemos ver un ping desde un servidor de la dmz a la sucursal.

## Práctica Seguridad en red: VPN y ASA

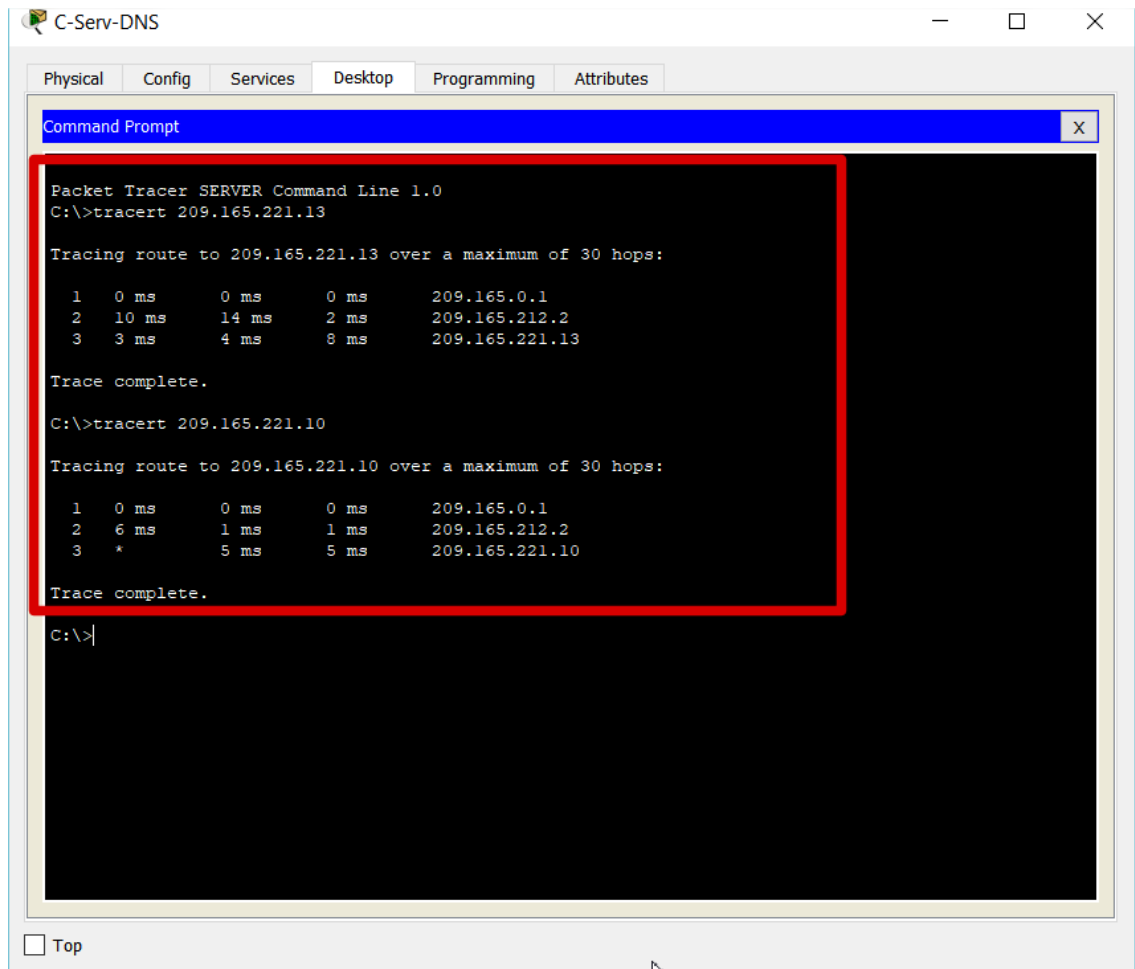
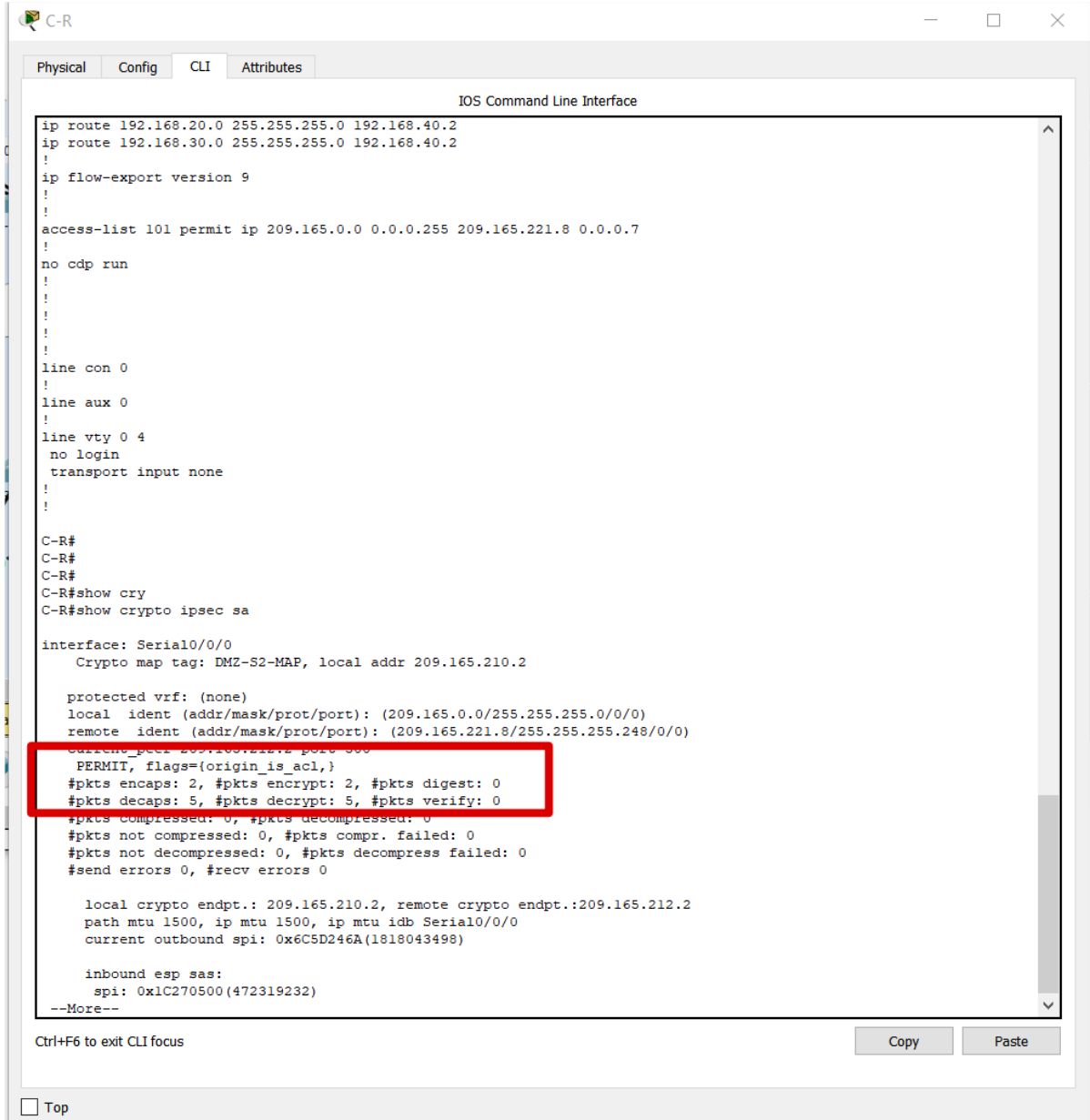


Ilustración 4. Tarea 2 Tracert entre equipos de la sucursal y la DMZ.



En la imagen observamos como pasan los paquetes por el túnel, por lo tanto, lo estamos utilizando correctamente.



```
C-R
Physical Config CLI Attributes
IOS Command Line Interface

ip route 192.168.20.0 255.255.255.0 192.168.40.2
ip route 192.168.30.0 255.255.255.0 192.168.40.2
!
ip flow-export version 9
!
!
access-list 101 permit ip 209.165.0.0 0.0.0.255 209.165.221.8 0.0.0.7
!
no cdp run
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
no login
transport input none
!
!
C-R#
C-R#
C-R#
C-R#show cry
C-R#show crypto ipsec sa

interface: Serial0/0/0
  Crypto map tag: DMZ-S2-MAP, local addr 209.165.210.2

  protected vrf: (none)
  local ident (addr/mask/prot/port): (209.165.0.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (209.165.221.8/255.255.255.248/0/0)
  current peer addr (addr/mask/prot/port): 209.165.221.8/255.255.255.248/0/0
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 2, #pkts encrypt: 2, #pkts digest: 0
  #pkts decaps: 5, #pkts decrypt: 5, #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.: 209.165.210.2, remote crypto endpt.:209.165.212.2
  path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
  current outbound spi: 0x6C5D246A(1818043498)

  inbound esp sas:
    spi: 0x1C270500(472319232)
  --More--

Ctrl+F6 to exit CLI focus
Copy Paste
Top
```

Ilustración 5. Tarea 2 Show crypto ipsec sa

Realizaremos diversas comprobaciones sobre la encriptación de los paquetes.

Aquí podemos observar el paquete antes de salir del router de la sucursal B donde se encuentra sin encriptar.

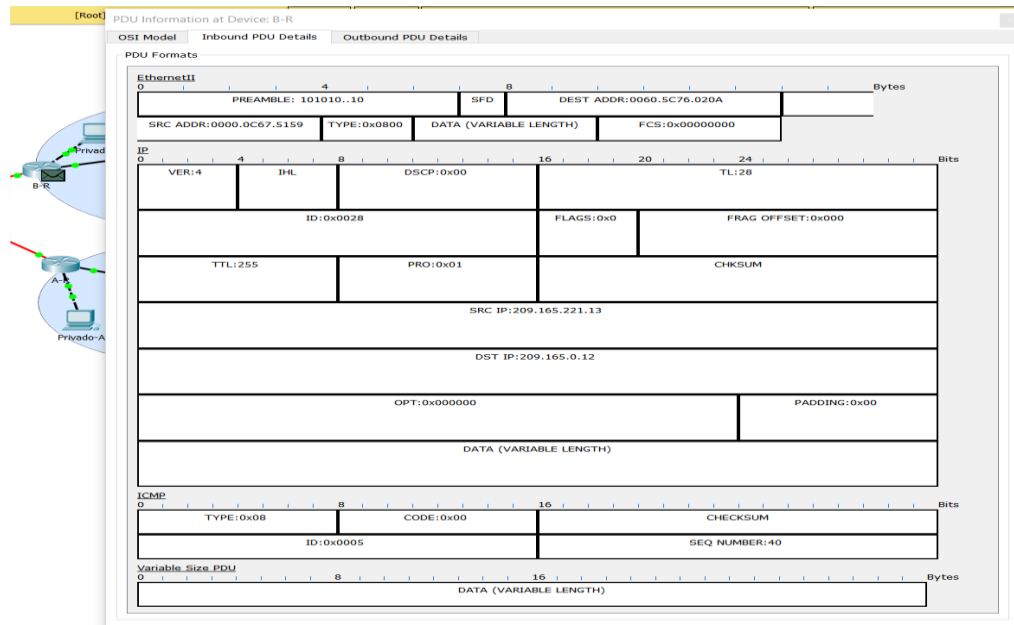


Ilustración 6. Tarea 2 Contenido de un paquete.



Aquí podemos ver el paquete en internet donde ha sido previamente encriptado por el túnel.

## Práctica Seguridad en red: VPN y ASA

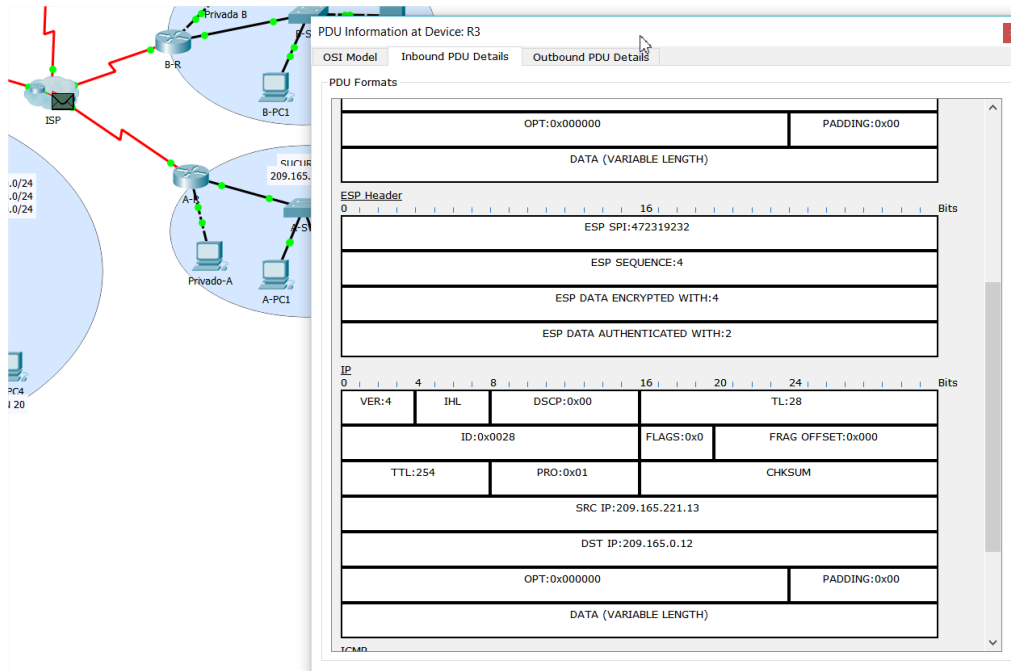


Ilustración 7. Tarea 2 Contenido de un paquete.

Y aquí podemos ver un paquete desde DMZ a la sucursal A en medio de internet donde no está encriptado al no pasar por ningún túnel.

## Práctica Seguridad en red: VPN y ASA

PDU Information at Device: R1

At Device: R1  
Source: C-Serv-RADIUS  
Destination: A-PC1

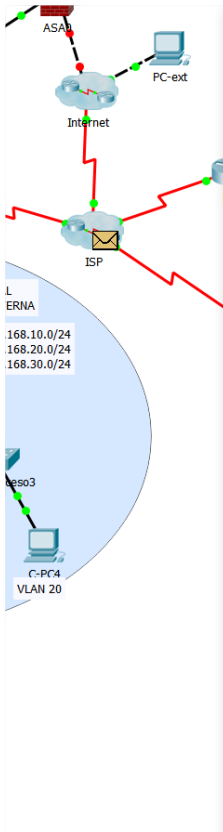
**In Layers**

Layer7
Layer6
Layer5
Layer4
Layer 3: IP Header Src. IP: 209.165.0.12, Dest. IP: 209.165.221.5 ICMP Message Type: 8
Layer 2: HDLC Frame HDLC
Layer 1: Port Serial0/0/0

**Out Layers**

Layer7
Layer6
Layer5
Layer4
Layer 3: IP Header Src. IP: 209.165.0.12, Dest. IP: 209.165.221.5 ICMP Message Type: 8
Layer 2: HDLC Frame HDLC
Layer 1: Port(s): Serial0/1/1

1. Serial0/0/0 receives the frame.



PDU Information at Device: R1

OSI Model Inbound PDU Details Outbound PDU Details

PDU Formats

**HDLC**

0	8	16	Bits
FLG: 0x7E	ADR: 0x8f	CONTROL: 0x0000	
DATA (VARIABLE LENGTH)			
FCS: 0x0000		FLG: 0x7E	

**IP**

0	4	8	16	20	24	Bits
VER: 4	IHL	DSCP: 0x00	TL: 28			
ID: 0x0008			FLAGS: 0x0	FRAG OFFSET: 0x000		
TTL: 254		PRO: 0x01	CHKSUM			
SRC IP: 209.165.0.12						
DST IP: 209.165.221.5						
OPT: 0x000000				PADDING: 0x00		
DATA (VARIABLE LENGTH)						

**ICMP**

0	8	16	Bits
TYPE: 0x08	CODE: 0x00	CHECKSUM	
ID: 0x0002		SEQ NUMBER: 1	

**Variable Size PDU**

0	8	16	Bytes
DATA (VARIABLE LENGTH)			

Ilustración 8. Tarea 2 Contenido de un paquete sin encriptación.

### Tarea 3.

- Configurar una VPN IPsec Site-to-Site para el tráfico entre la subred de la VLAN 30 de la sede central, y la subred de la sucursal A. En este caso, la VLAN 30 tiene direccionamiento privado. Utilizar los mismos parámetros de IPsec que en el apartado anterior.

#### En CR para la configuración del NAT :

```
#Primero configuramos el NAT

ip access-list extended aclNat
    permit ip 192.168.10.0 0.0.0.255 any
    permit ip 192.168.20.0 0.0.0.255 any
    deny ip 192.168.30.0 0.0.0.255 209.165.221.0 0.0.0.7
    permit ip 192.168.30.0 0.0.0.255 any
exit
ip nat pool NAT 209.165.210.2 209.165.210.2 netmask 255.255.255.252
ip nat inside source list aclNat pool NAT overload

interface fastEthernet 0/0
    ip nat inside
exit
interface serial 0/0/0
    ip nat outside
exit
```

#### En A-R para la configuración de la VPN :

```
ip access-list extended 101
permit ip 209.165.221.0 0.0.0.7 192.168.30.0 0.0.0.255
deny ip any any

crypto isakmp policy 1
    hash sha
    authentication pre-share
    group 2
    lifetime 86400
    encryption aes 256
exit

ip access-list 102 permit ip 192.168.30.0 0.0.0.255 209.165.221.0
0.0.0.7
deny ip any any
exit

crypto isakmp key Vpnpass101 address 209.165.210.2
crypto ipsec transform-set A-DMZ esp-aes esp-sha-hmac

crypto map A-DMZ-MAP 10 ipsec-isakmp
    set peer 209.165.210.2
    set pfs group2
```

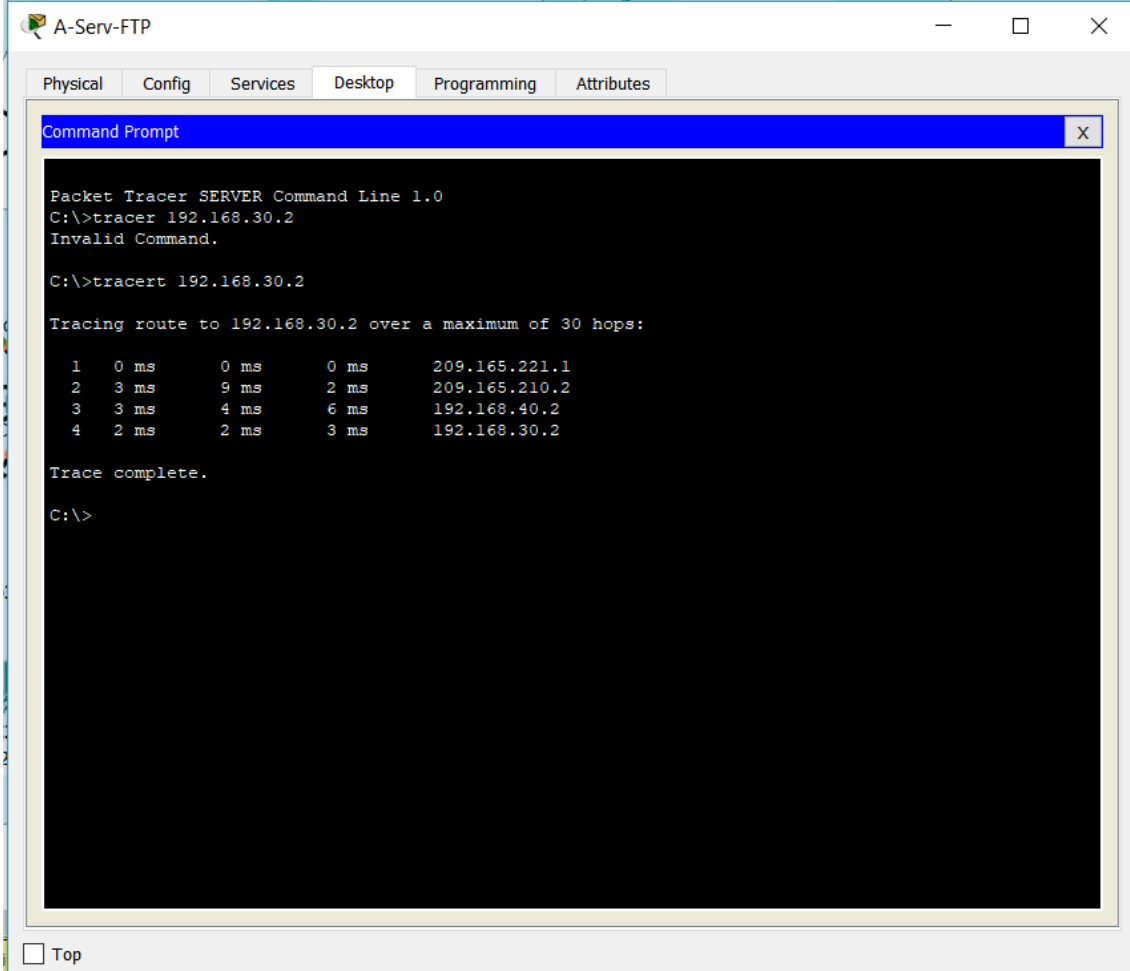
```
set security-association lifetime seconds 900
set transform-set A-DMZ
match address 101
exit

interface Serial0/0/0
crypto map A-DMZ-MAP
```

**En CR para la configuración de la VPN :**

```
ip access-list 102 permit ip 192.168.30.0 0.0.0.255 209.165.221.0
0.0.0.7
deny ip any any
exit
crypto isakmp key Vpnpass101 address 209.165.211.2
crypto ipsec transform-set CENTRAL-A esp-aes esp-sha-hmac
crypto map CENTRAL-ALL-MAP 2 ipsec-isakmp
match address 102
    set pfs group2
    set transform-set CENTRAL-S2
    set peer 209.165.211.2
Exit
```

Tracert desde Servidor FTP en A al servidor de radius en la central. No pasa por ningún servidor del isp.



The screenshot shows a Packet Tracer window titled 'A-Serv-FTP'. Inside, there is a 'Command Prompt' window with the following text:

```
Packet Tracer SERVER Command Line 1.0
C:\>tracer 192.168.30.2
Invalid Command.

C:\>tracert 192.168.30.2

Tracing route to 192.168.30.2 over a maximum of 30 hops:

  1  0 ms    0 ms    0 ms    209.165.221.1
  2  3 ms    9 ms    2 ms    209.165.210.2
  3  3 ms    4 ms    6 ms    192.168.40.2
  4  2 ms    2 ms    3 ms    192.168.30.2

Trace complete.

C:\>
```

At the bottom of the Command Prompt window, there is a 'Top' button.

Ilustración 9. Tarea 3 Tracert desde sucursal a vlan30.

Y en el sentido inverso, aunque ahora usando el servidor syslog.

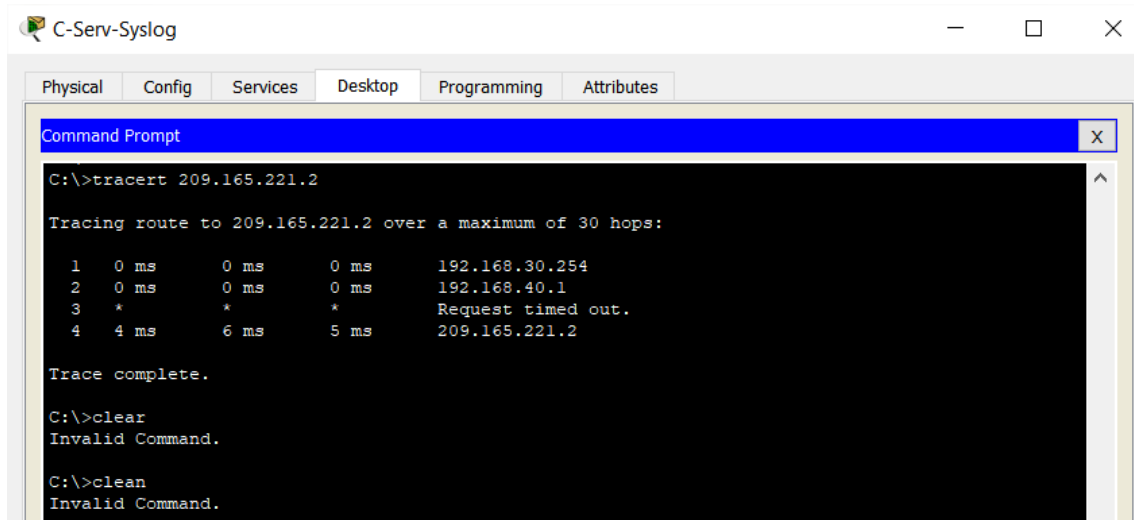


Ilustración 10. Tarea 3 Tracert desde vlan30 a sucursal.



## Tarea 4.

Configure el firewall ASA de una empresa (SOHO, siglas de Small-Office - Home-Office) de forma que:

- Tenga una configuración básica

Configuración básica del ASA. Primeramente, cambiamos el cable que lo conecta con internet ya que el que vienen no funciona correctamente.

Primero configuramos la interfaz de salida a internet con una seguridad de 0 y el ip correspondiente.

```
clock set 17:09:00 10 June 2018
enable password cisco
#La ruta por omisión o Gateway especificado.
route outside 0.0.0.0 0.0.0.0 209.165.232.9
```

- Utilice 3 zonas, inside para PCs, outside hacia Internet y dmz hacia servidores. Cree más equipos si lo desea y asigne los puertos extra. Asigne dos rangos de direcciones privadas internas a su elección.

```
Interface et0/0
Switchport Access vlan2
Exit
Interface vlan2
Nameif outside
Security-level 0
ip address 209.165.232.10 255.255.255.248
exit

interface Vlan3
no forward interface Vlan1
nameif dmz
security-level 50
ip address 192.168.2.1 255.255.255.0
exit
```

- Se comporte como servidor DHCP para los PCs. Use direcciones estáticas en

los servidores.

#Licencia Base 32 equipos.

dhcpd address 192.168.1.10-192.168.1.41 inside

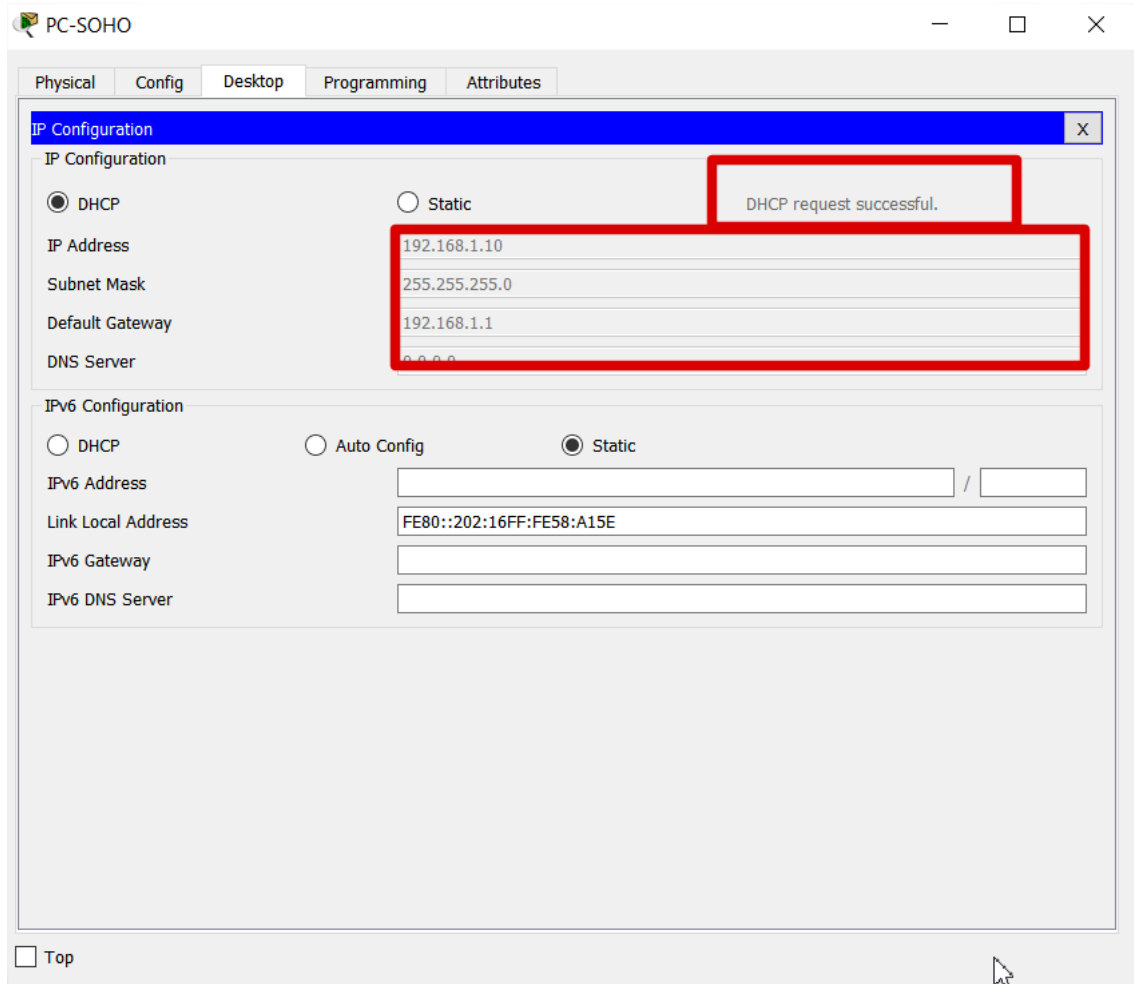


Ilustración 11. Tarea 4 Dhcp devolviendo direcciones.

Después de aplicar el dhcp nos devuelve la primera IP libre del rango configurado cuando el PC-SOHO la requiere.

- Realice NAT con PAT sobre la dirección pública para los PCs internos.

```
object network INSIDE-NET
  subnet 192.168.10.0 255.255.255.248
  nat (inside,outside) dynamic interface
end
```

Si queremos que además nos devuelva los pings de momento utilizamos un ACL a la entrada de outside, en este caso para el pc 1-

```
access-list ACL-IN extended permit ip any host 209.165.232.10
access-list ACL-IN extended permit ip any host 192.168.1.10 access-group ACL-IN in
interface outside
```

En la imagen podemos ver como cambia la cabecera de ip origen cuando se aplica el NAT.

**PDU Information at Device: ASA0**

At Device: ASA0  
Source: PC-SOHO  
Destination: PC-ext

OSI Model	Inbound PDU Details	Outbound PDU Details
<b>In Layers</b>		<b>Out Layers</b>
Layer7		Layer7
Layer6		Layer6
Layer5		Layer5
Layer4		Layer4
Layer 3: IP Header Src. IP: 192.168.1.10, Dest. IP: 209.165.232.18 ICMP Message Type: 8		Layer 3: IP Header Src. IP: 209.165.232.10, Dest. IP: 209.165.232.18 ICMP Message Type: 8
Layer 2: Ethernet II Header 0002.1658.A15E >> 00E0.B0B9.2893		Layer 2: Ethernet II Header 00E0.B0B9.2893 >> 00E0.F714.5301
Layer 1: Port Ethernet0/5		Layer 1: Port(s): Ethernet0/0

1. Ethernet0/5 receives the frame.

Challenge Me      << Previous Layer      Next Layer >>

Ilustración 12. Tarea 4 Traducción NAT.

- Realice NAT estático 1:1 para los servidores con las demás direcciones restantes del rango al que pertenece su dirección externa.

```
access-group OUTSIDE-DMZ in interface dmz
object network DMZ-SERVER
nat (dmz,outside) static 209.165.232.11
```

Aquí podemos ver como cambia la cabecera a la dirección estática introduce una vez es traducida por el asa y proviene del servidor de la DMZ.

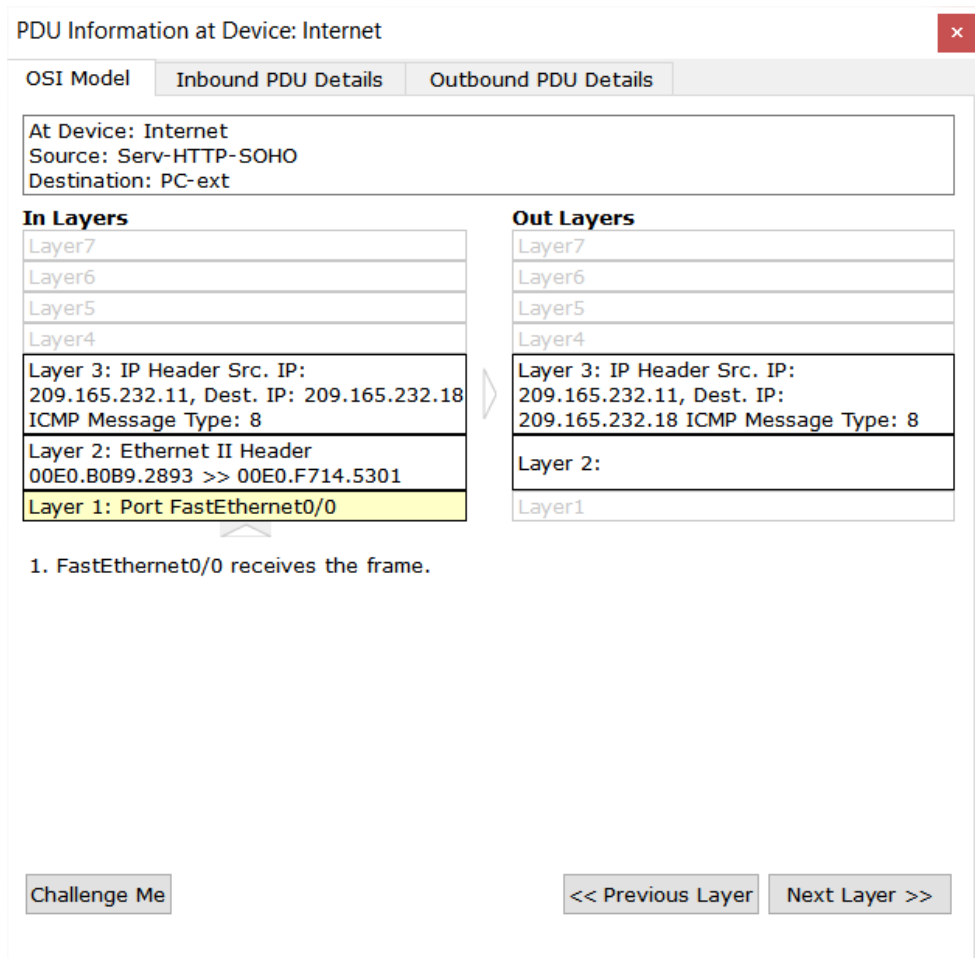


Ilustración 13. Tarea 4 Traducción estática entre servidores.

access-list OUTSIDE-DMZ extended permit ip any host 192.168.2.2

access-list OUTSIDE-DMZ extended permit icmp any any

access-group OUTSIDE-DMZ in interface dmz

- Permita el tráfico al servidor HTTP, y a otros servicios que cree en la DMZ, desde Internet. Permita ICMP de dentro hacia dmz y outside.

```
#Permitimos tráfico solo para peticiones a internet.  
access-list ACL-IN extended permit tcp any host 209.165.232.11  
eq www  
access-group ACL-IN in interface outside
```

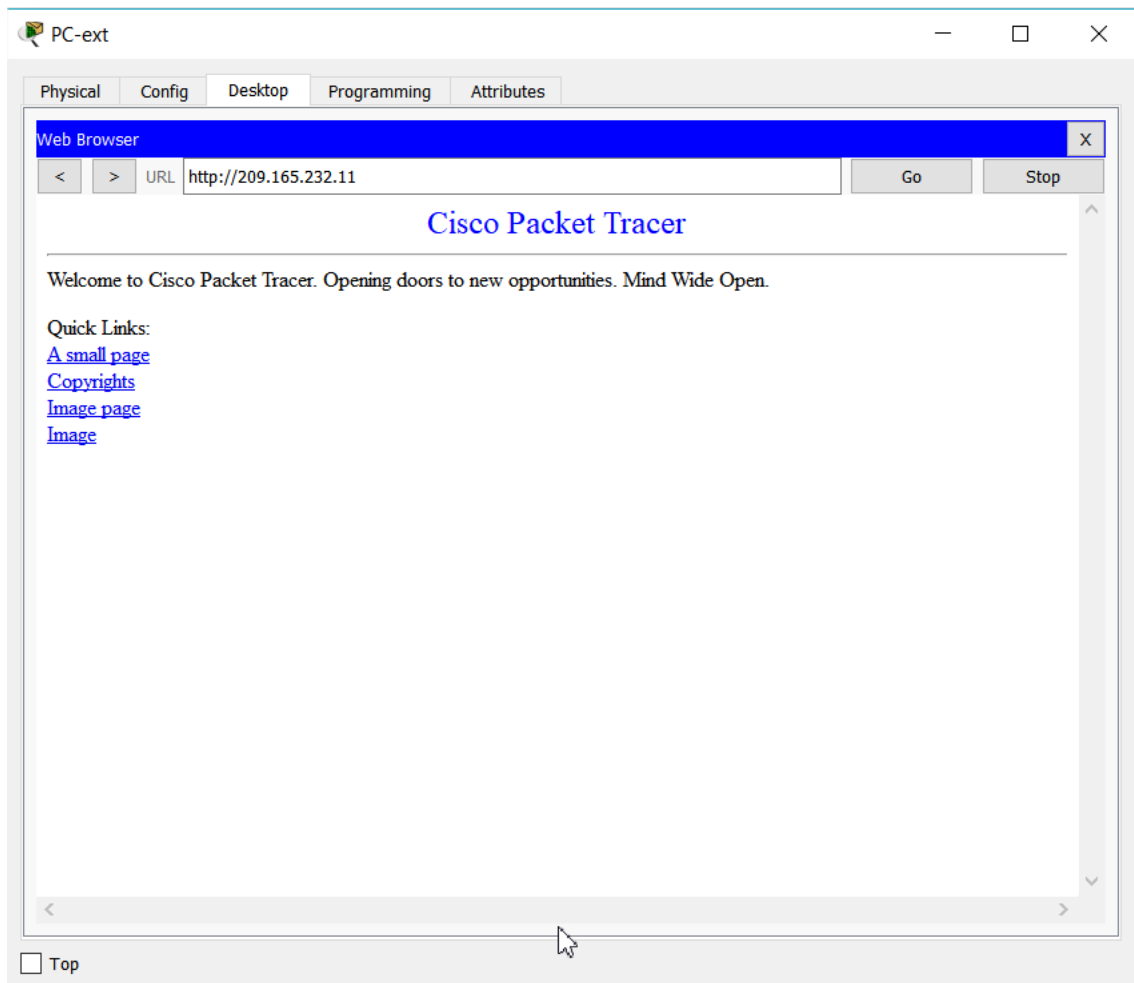


Ilustración 14. Tarea 4 Se permite el tráfico http al servidor en la dmz interna.

En la siguiente imagen vemos que el ping no es devuelto. No es tráfico de internet.

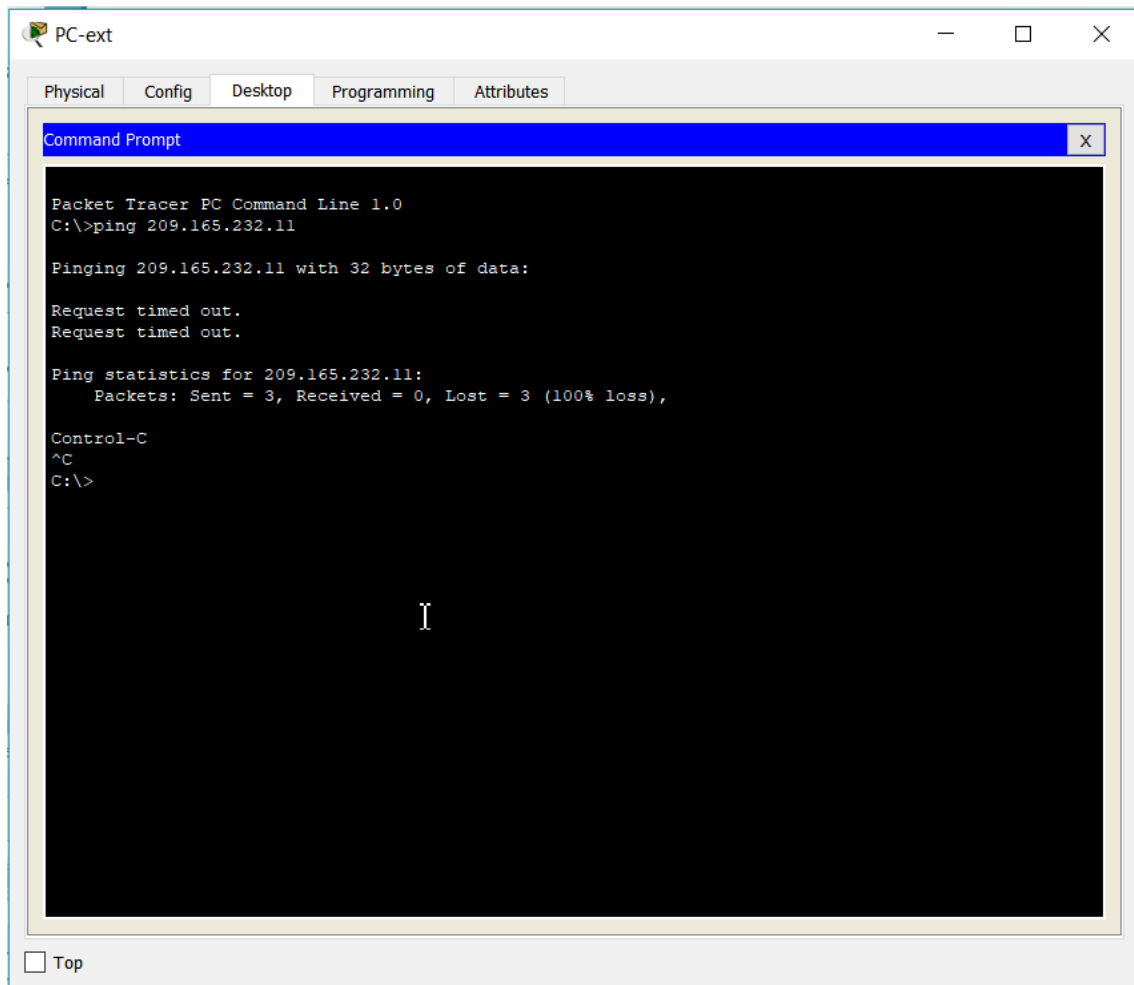


Ilustración 15. Tarea 4 Se deniega el tráfico que no es internet.

# Para el ICMP creamos una política que inspeccione el ICMP.

```
class-map inspection_default
match default-inspection-traffic
exit
policy-map global_policy
class inspection_default
inspect icmp
exit
service-policy global_policy global
```