|  |  |
| --- | --- |
| Resultado de imagen de politecnica upm  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  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.

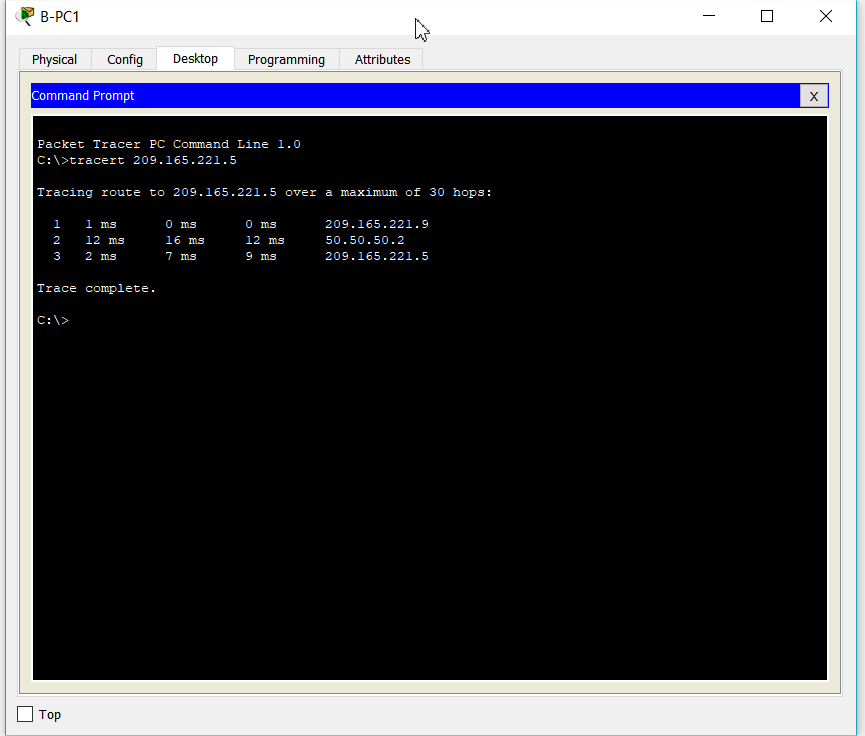


Ilustración 1. Tarea 1 Tracert entre equipos de sucursales.

* 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.

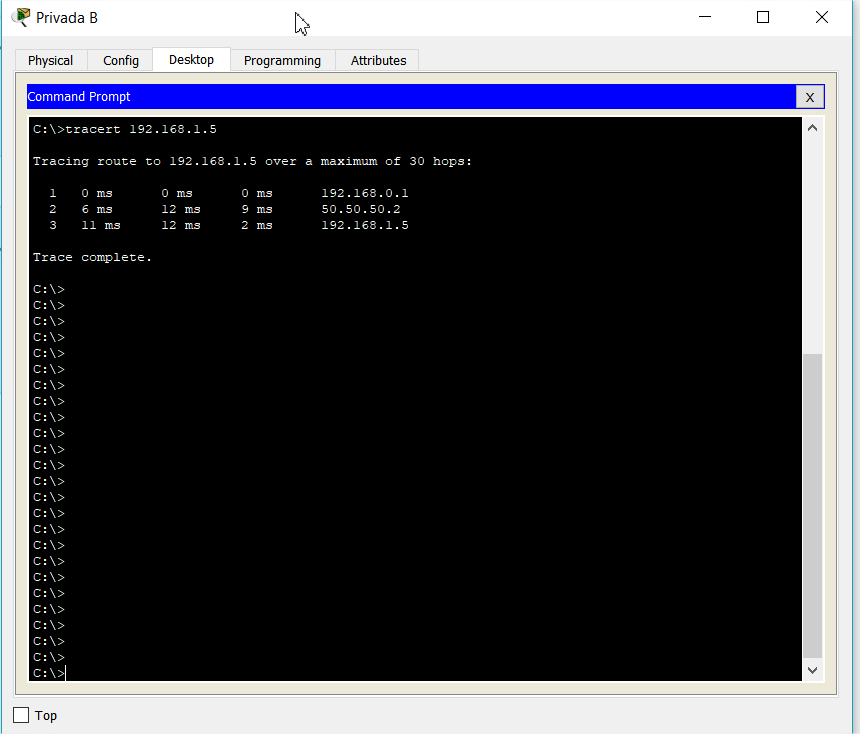


Ilustración 2. Tarea 1 Tracert entre equipos privados de sucursales.

# 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.

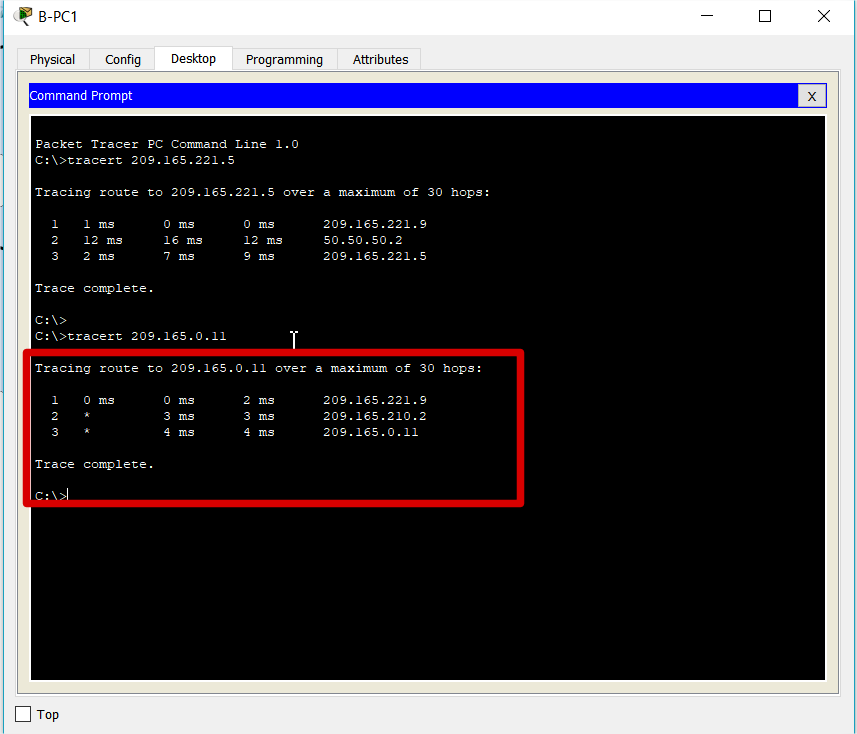


Ilustración 3. Tarea 2 Tracert entre equipos de la sucursal y la DMZ.

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

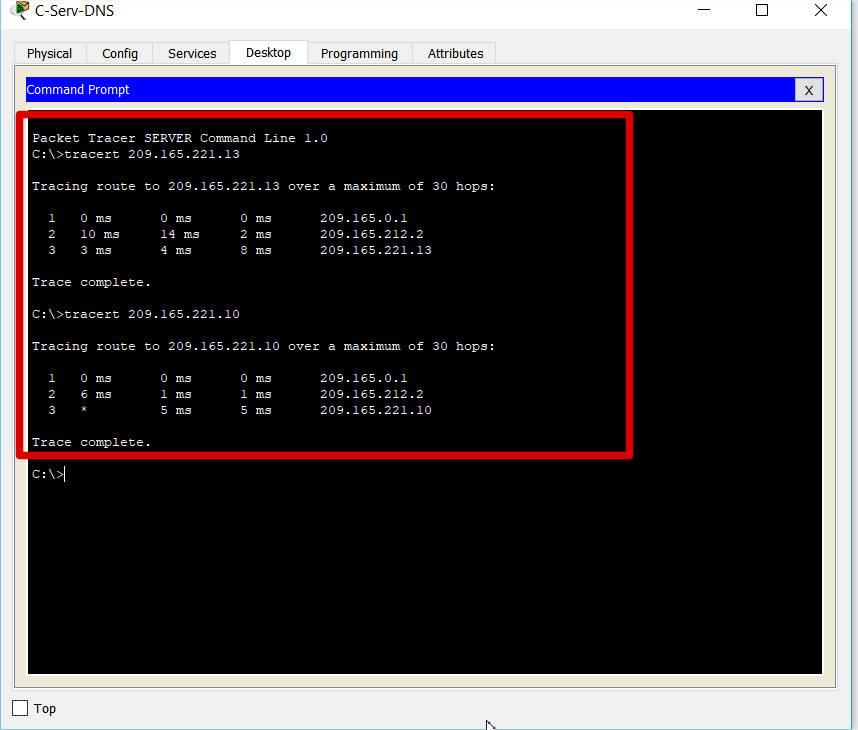


Ilustración 4. Tarea 2 Tracert entre equipos de la sucursal y la DMZ.

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

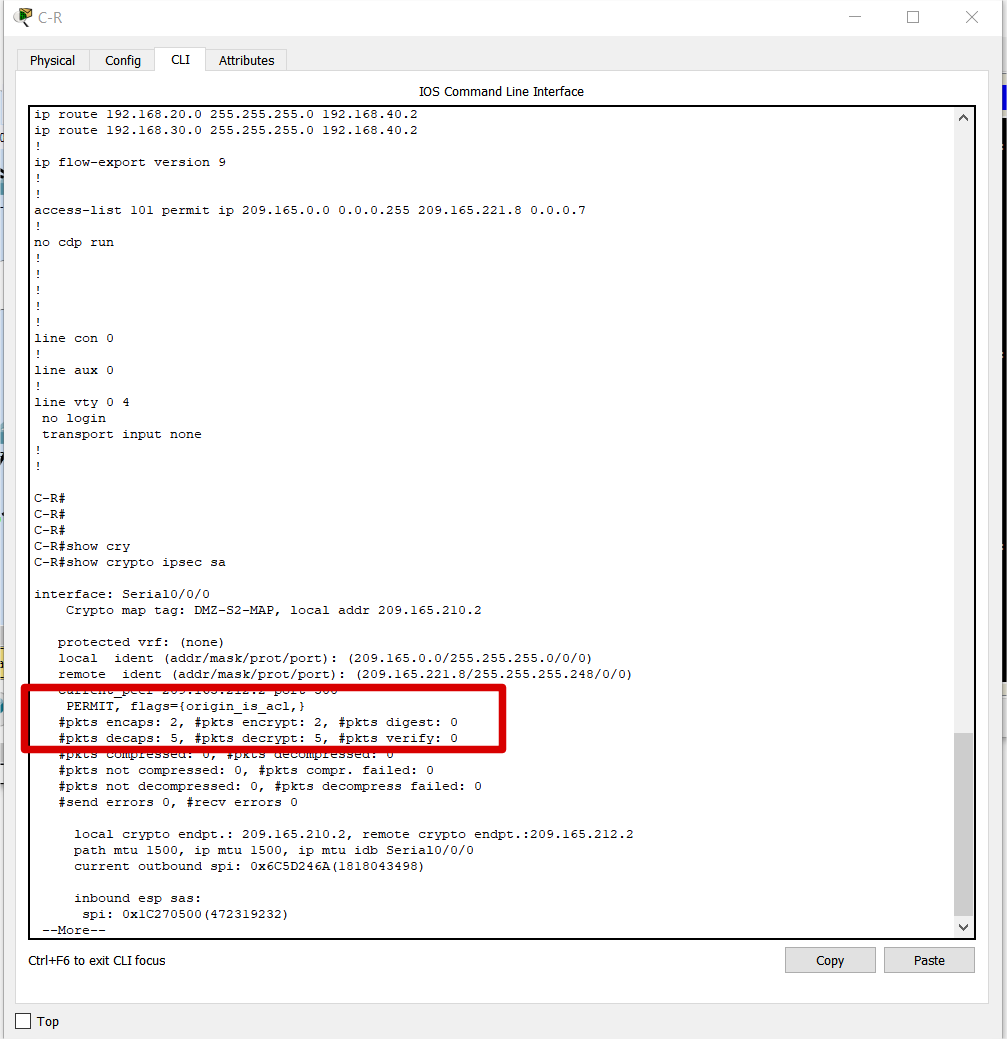


Ilustración 5. Tarea 2 Show crypto ipsec sa

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.

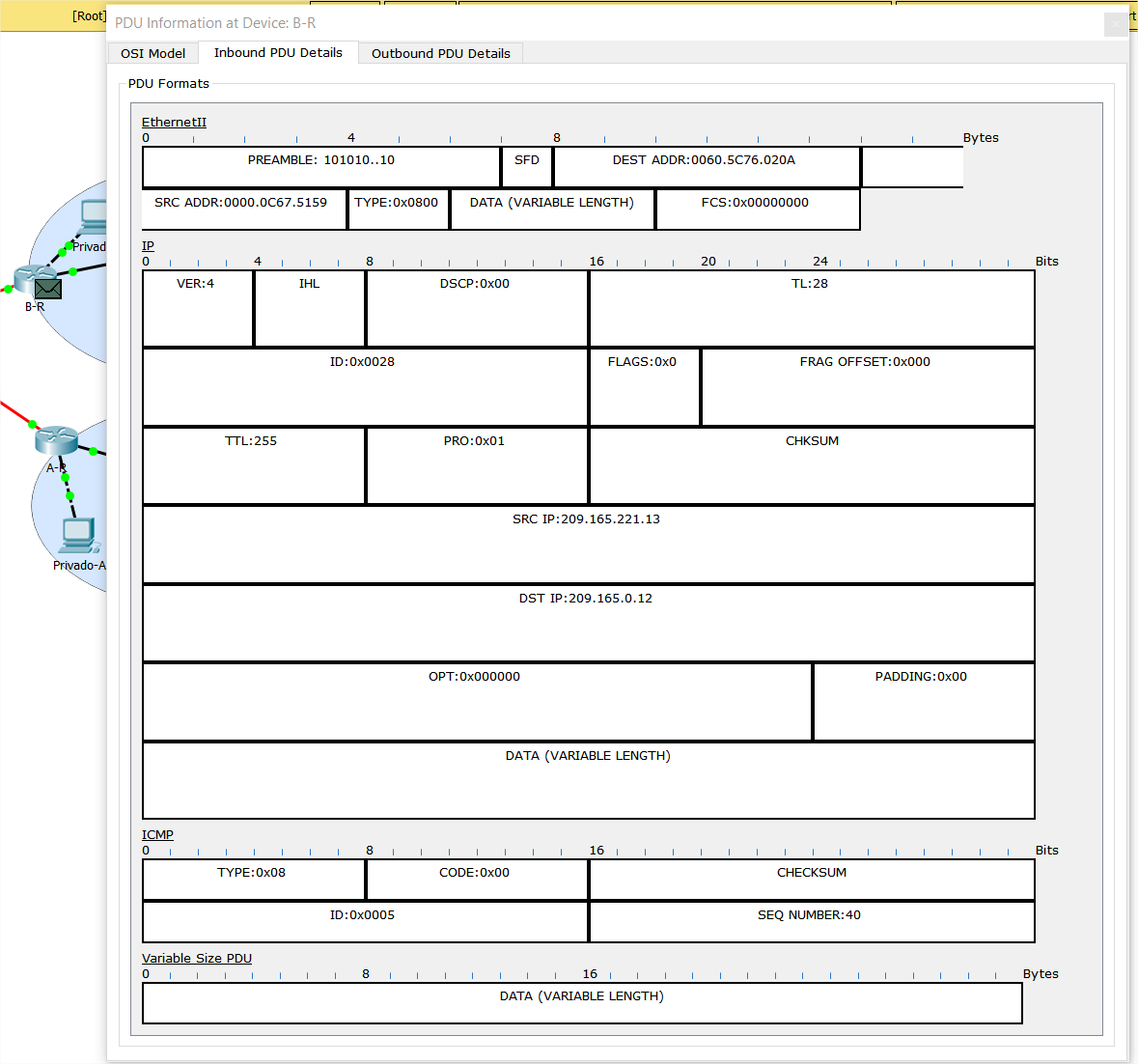


Ilustración 6. Tarea 2 Contenido de un paquete.

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

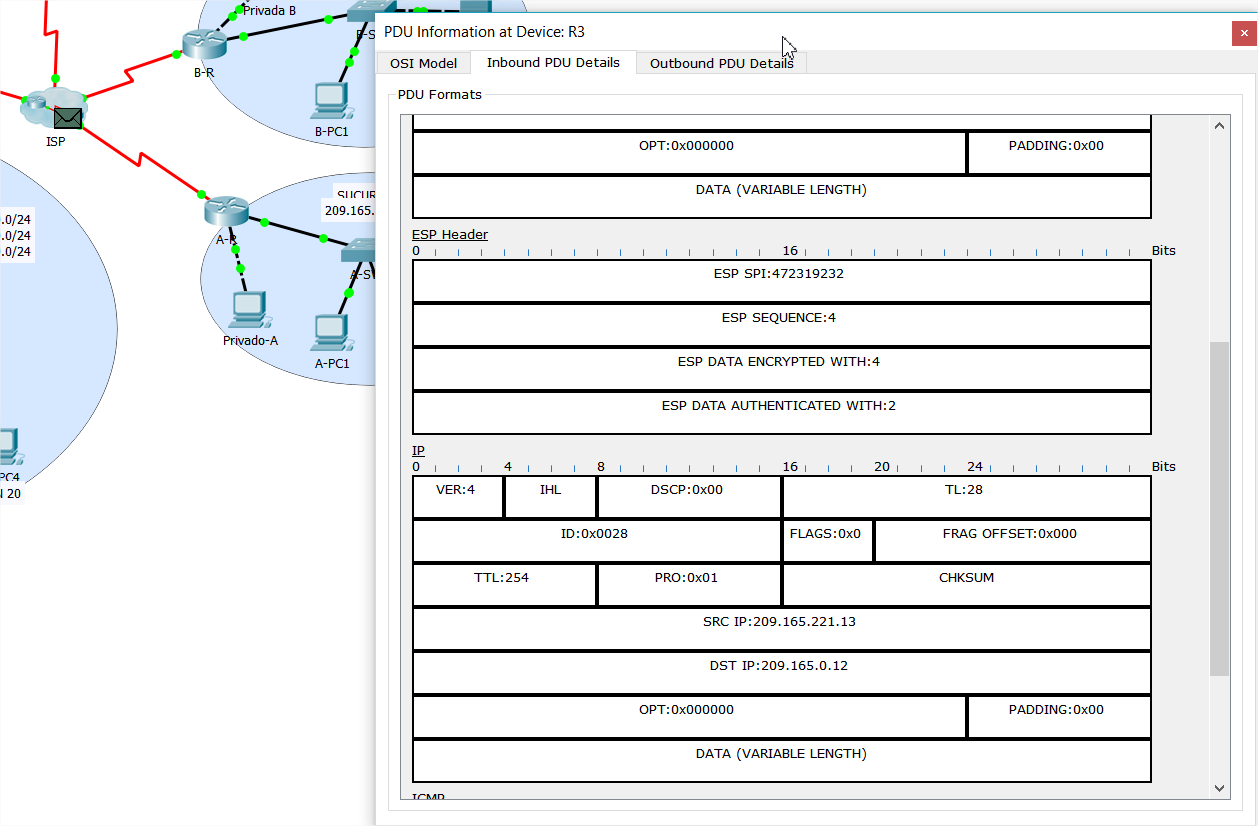
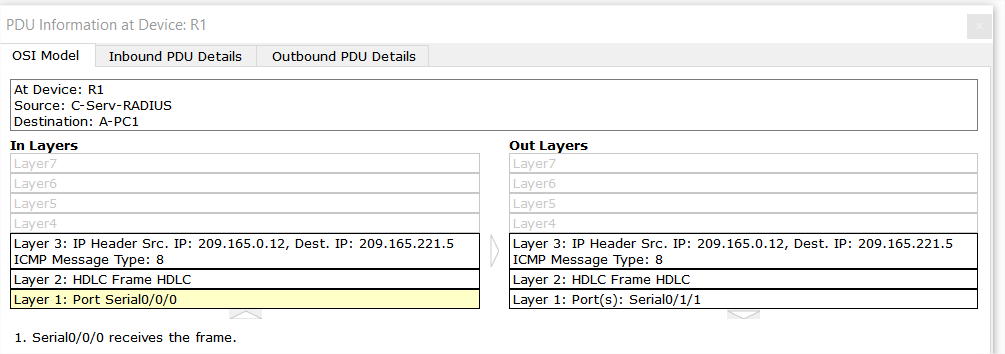


Ilustración 7. Tarea 2 Contenido de un paquete.

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.



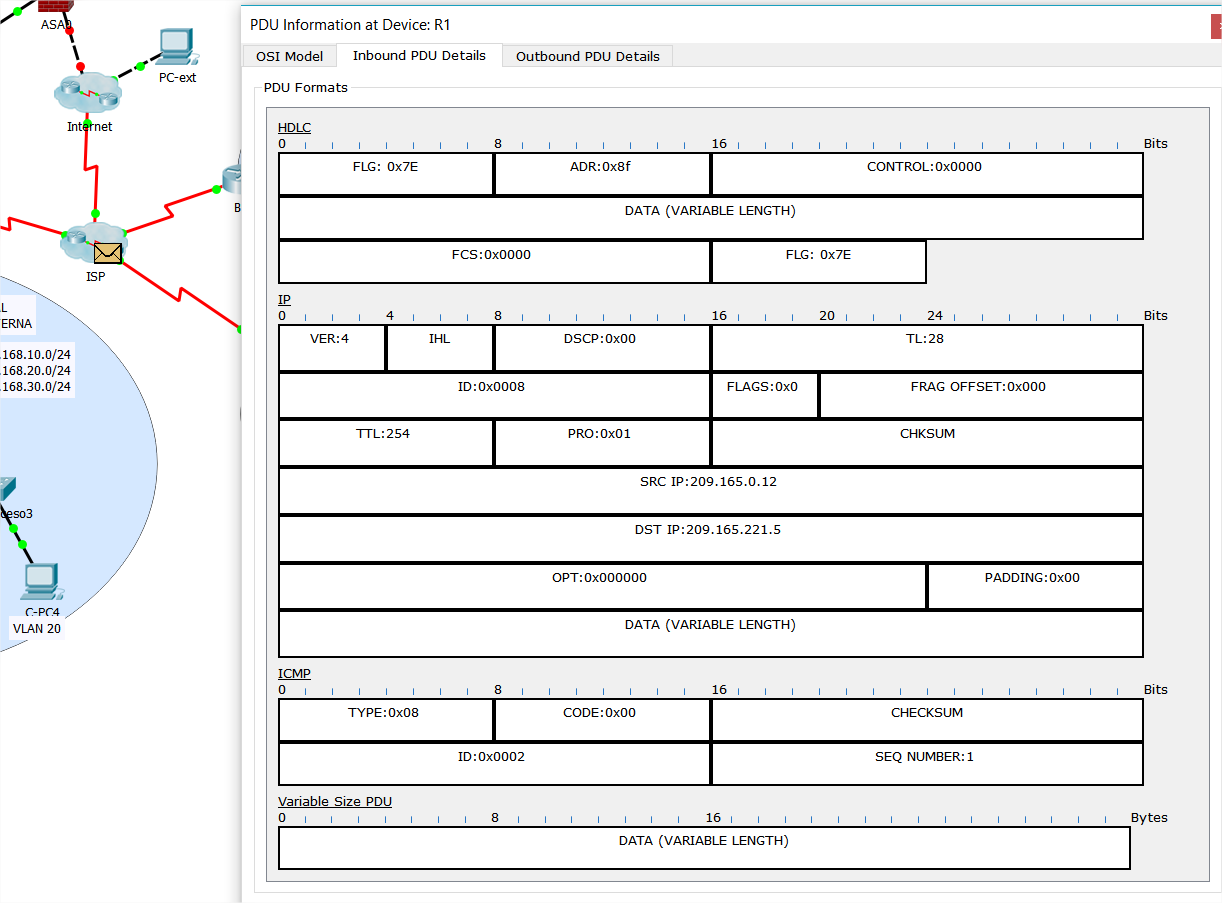


Ilustración 8. Tarea 2 Contenido de un paquete sin encriptación.

# 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.

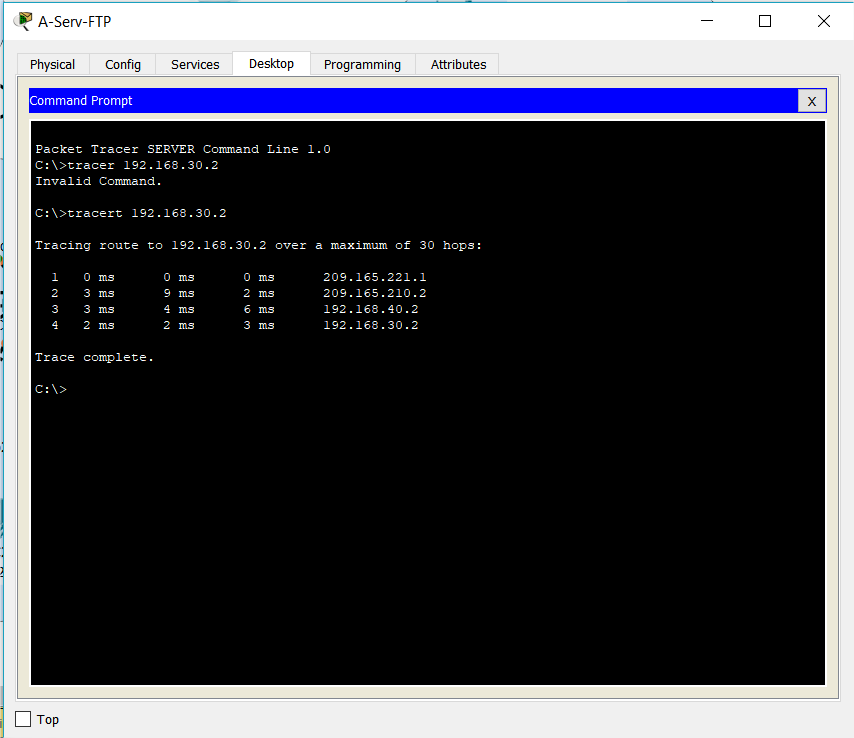


Ilustración 9. Tarea 3 Tracert desde sucursal a vlan30.

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

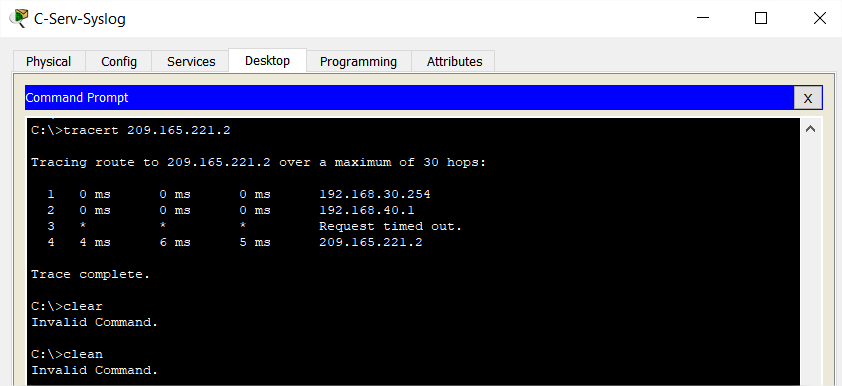


Ilustración 10. Tarea 3 Tracert desde vlan30 a sucursal.

# 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

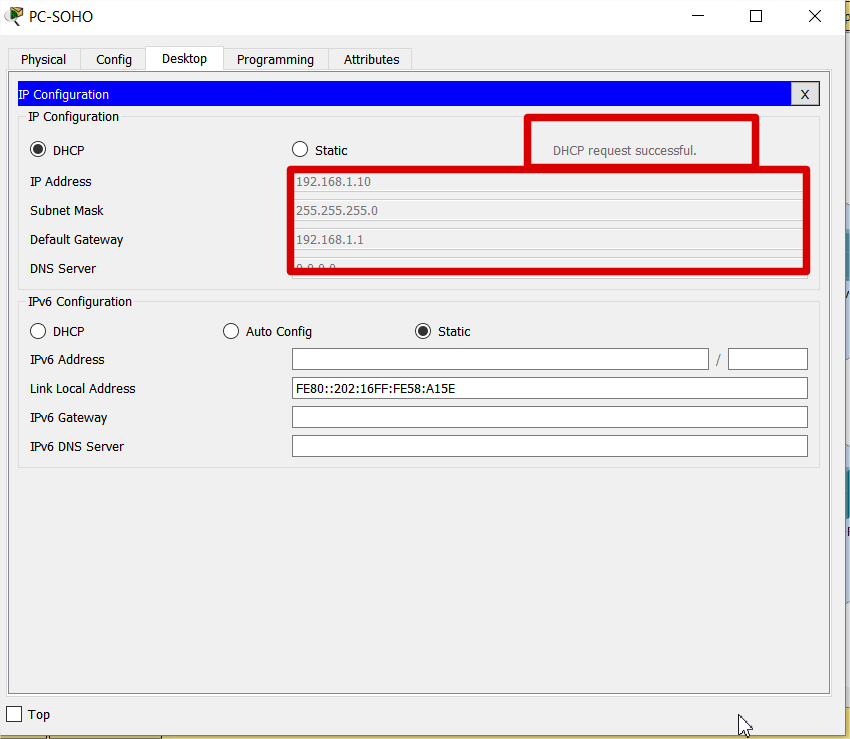


Ilustración 11. Tarea 4 Dhcp devolviendo direcciones.

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.

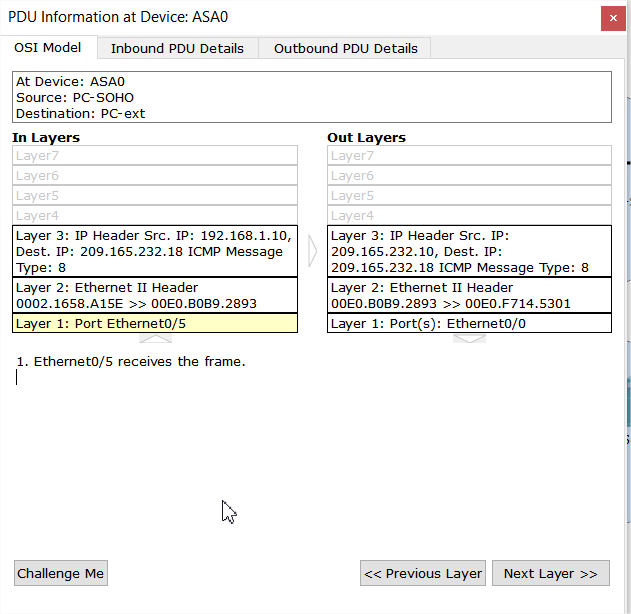


Ilustración 12. Tarea 4 Traducción NAT.

* 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.

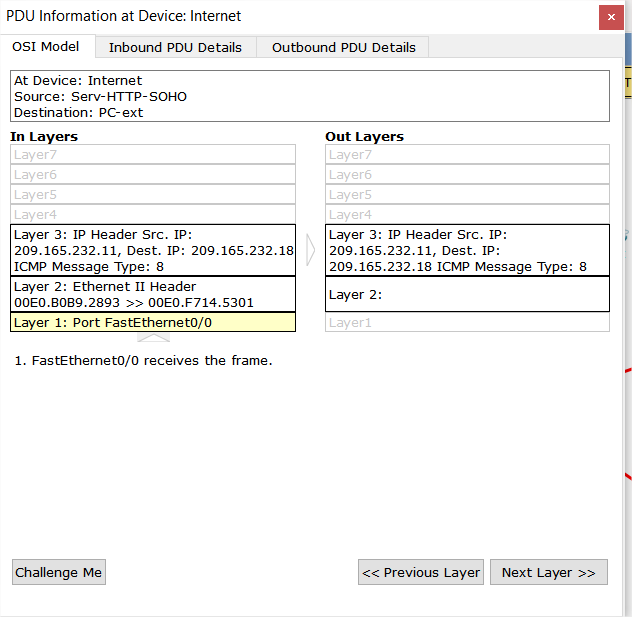


Ilustración 13. Tarea 4 Traducción estática entre servidores.

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.

#Pertimos 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

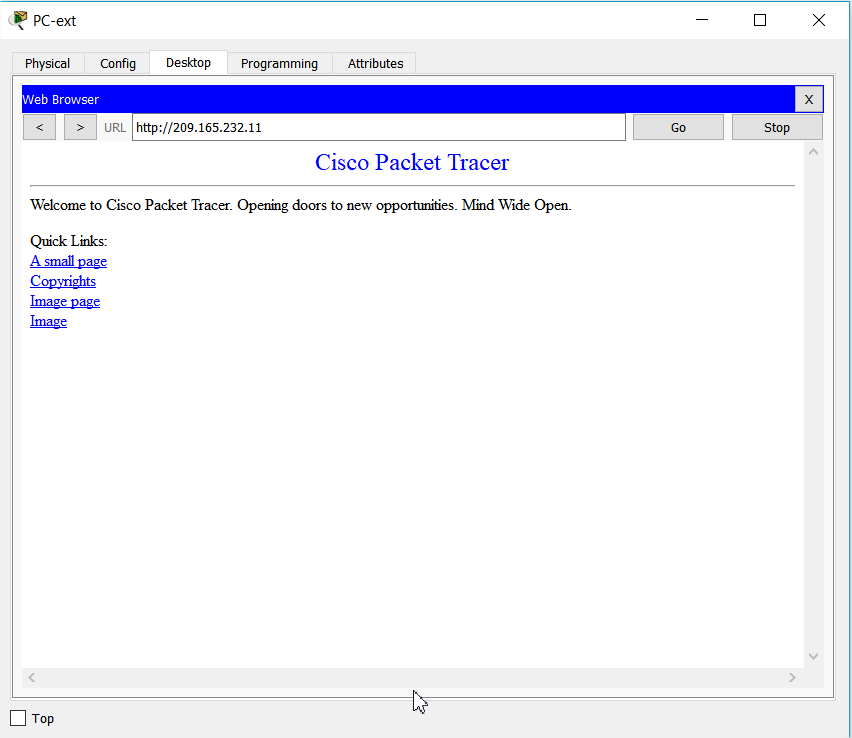


Ilustración 14. Tarea 4 Se permite el trafico http al servidor en la dmz interna.

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

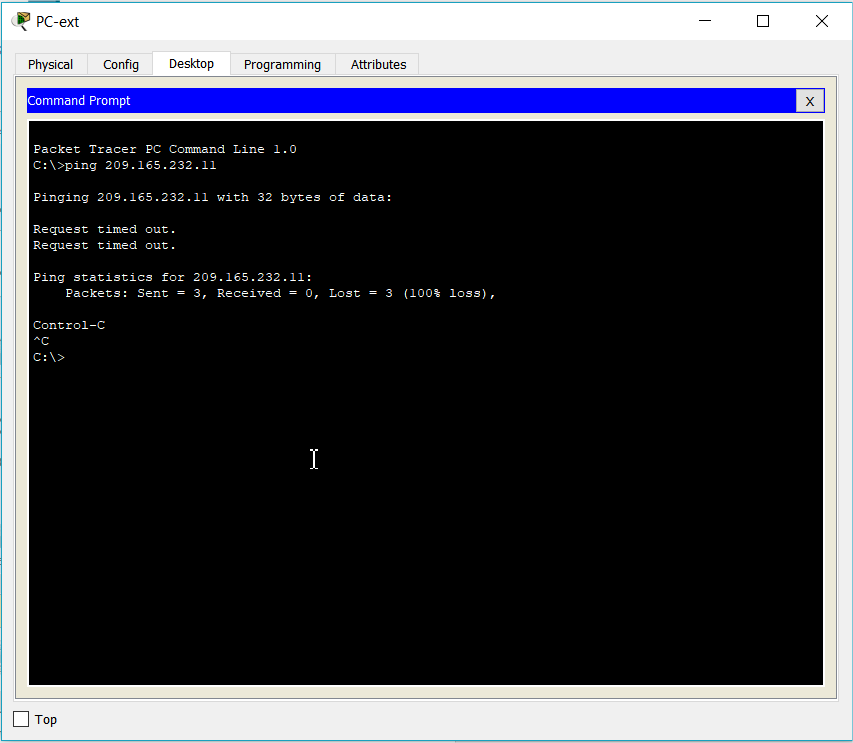


Ilustración 15. Tarea 4 Se deniega el tráfico que no es internet.

# 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