PRÁCTICA DISEÑO Y SEGURIDAD EN REDES

Securización de dispositivos, AAA y Firewall

DESCRIPCIÓN BREVE

Securización, AA y firewall.

j.amoros@alumnos.upm.es
Máster en Ingeniería informática

Tarea 1. Configuración básica

Por cada switch su ip y su Gateway correspondiente en la tabla de enrutamiento.

```
interface vlan0030

ip address 192.168.30.11 255.255.255.0

Ip default gateway
```

Para el router CR

```
access-list 1 permit 192.168.10.0 0.0.0.255
ip access-list 1
ip access-list standard 1
20 permit 192.168.20.0 0.0.0.255
exit
ip nat pool NatPoolCR 209.165.210.2 209.165.210.2  netmask 255.255.255.254
ip nat inside source list 1 pool NatPoolCR

interface serial0/0/0
ip nat outside
exit

interface FastEthernet0/0
ip nat inside
exit
```

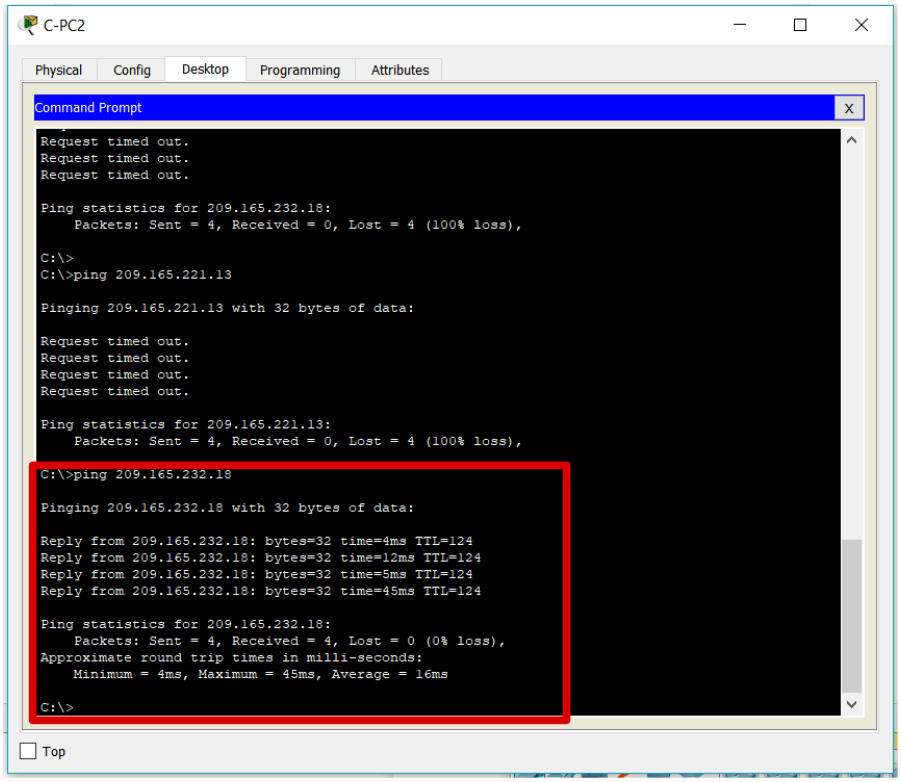

Ilustración 1. Ping hacia internet ordenador PC Ext.

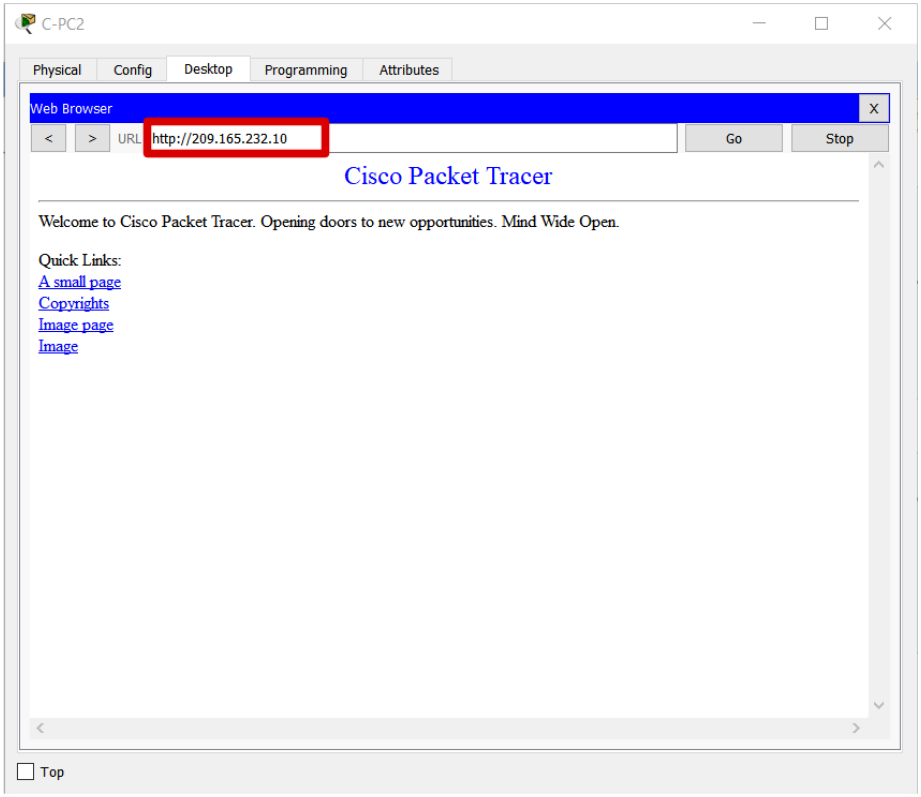

Ilustración 2. Acceso al servidor HTTP externo.

Tarea 2 . Configurar Syslog y NTP.

Configuramos el servidor NTP previamente de la siguiente manera.

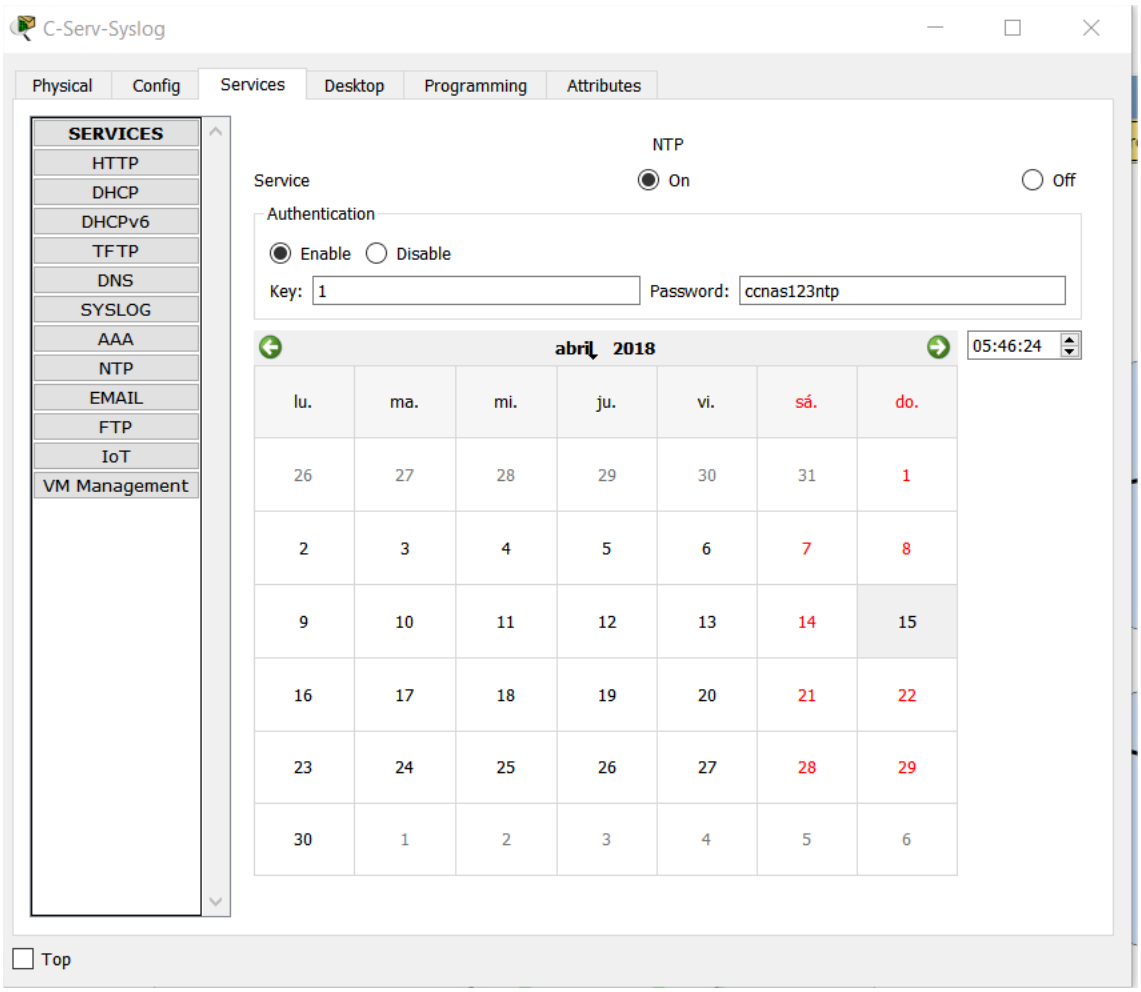

Ilustración 3. Configuración de la clave en el servidor NTP.

Para la configuración de NTP realizamos en los routers CR y CR2 lo siguiente.

```
show clock
*6:23:37.28 UTC Mon Mar 1 1993

npt server 209.165.0.13 key 1

C-R(config)#exit

show ntp status
Clock is synchronized, stratum 2, reference is 209.165.0.13
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**19
reference time is DE4CE96A.00000048 (11:07:22.072 UTC Sat Apr 7 2018)
clock offset is 0.00 msec, root delay is 0.00 msec
root dispersion is 0.02 msec, peer dispersion is 0.02 msec.
```

```
conf t
ntp authenticate
ntp authentication-key 1 md5 ccnas123ntp
ntp trusted-key 1
```

Para la configuración de SysLog, comprobamos que el servicio esta activado en el servidor y realizamos en los routers CR y CR2 lo siguiente.

```
loggin host 209.165.0.13
loggin trap debugging

loggin on

service timestamps log datetime msec

service timestamps debug datetime msec

exit
```

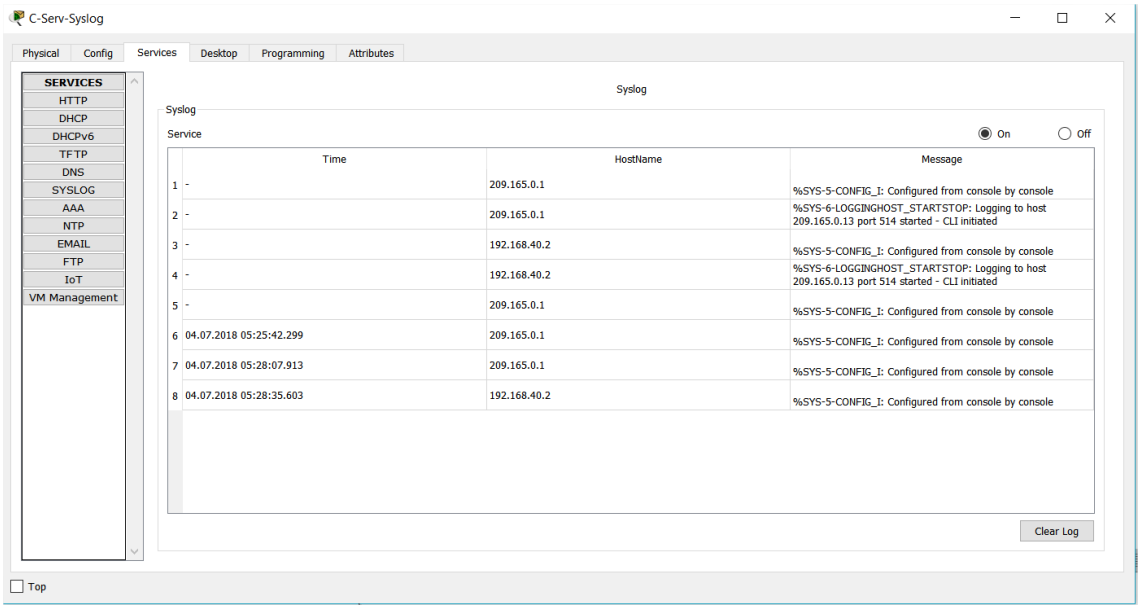

Ilustración 4. Comprobamos que se emiten mensajes de log en el servidor.

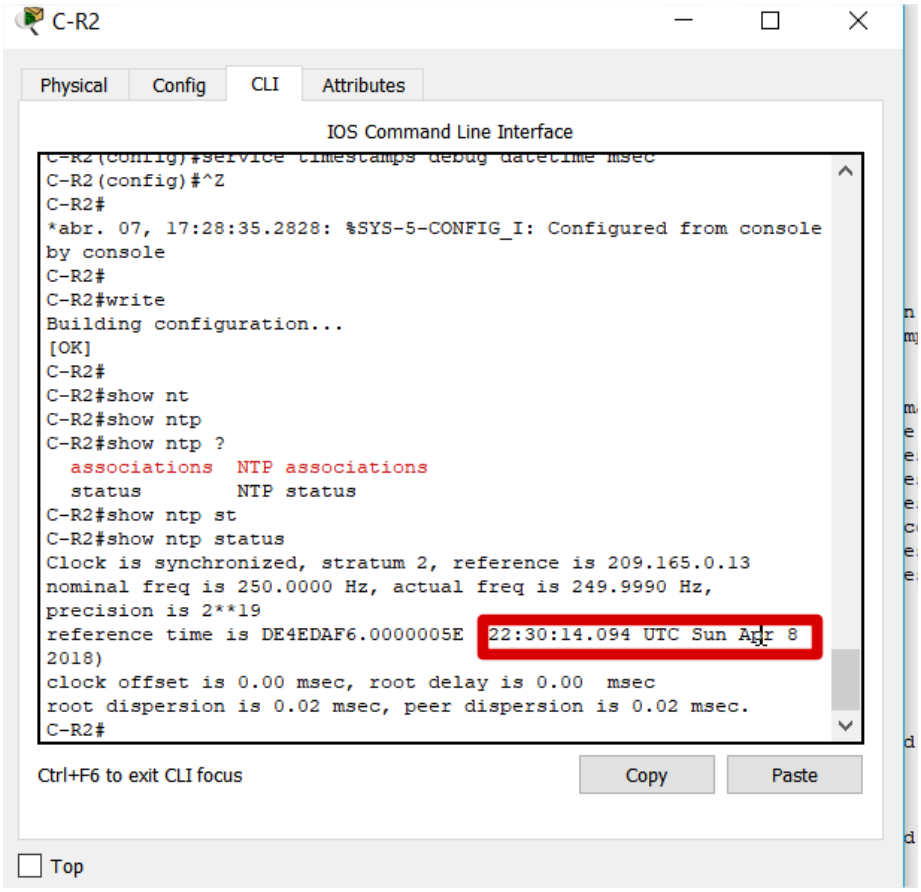

Ilustración 5. Comprobamos que el NTP está correctamente configurado.

Tarea 3. Reforzar la seguridad de los routers y switches

Para los routers CR y CR2 hemos realizado la siguiente configuración.

Para la generación de usuarios y la securización de las líneas se realiza lo siguiente en routers y switches.

```
enable
conf t
username admin secret ccnas123adm
enable secret ccnas123en
conf t
line con 0
password ccnas123con
exit
line vty 0 4
password ccna123con
exit
```

Para la configuración del usuario especial supervisor que solo puede ejecutar comando básicos y reload, se ha generado un nivel 2 específico para ese usuario.

```
privilege exec level 2 reload
enable secret level 2 ccnas123sup
username supervisor privilege 2 secret ccnas123sup
```

Para la configuración del protocolo SSH, desactivando además el protocolo Telnet que viene habilitado por defecto y que se considera inseguro.

```
hostname CR
ip domain-name unDominio.com
crypto key generate rsa
1024
ip ssh version 2
line vty 0 4
login local
transport input ssh
```

```
end
conf t
ip ssh authentication-retries 3
ip ssh timeout 120
login on-succes log
login on-failure log
```

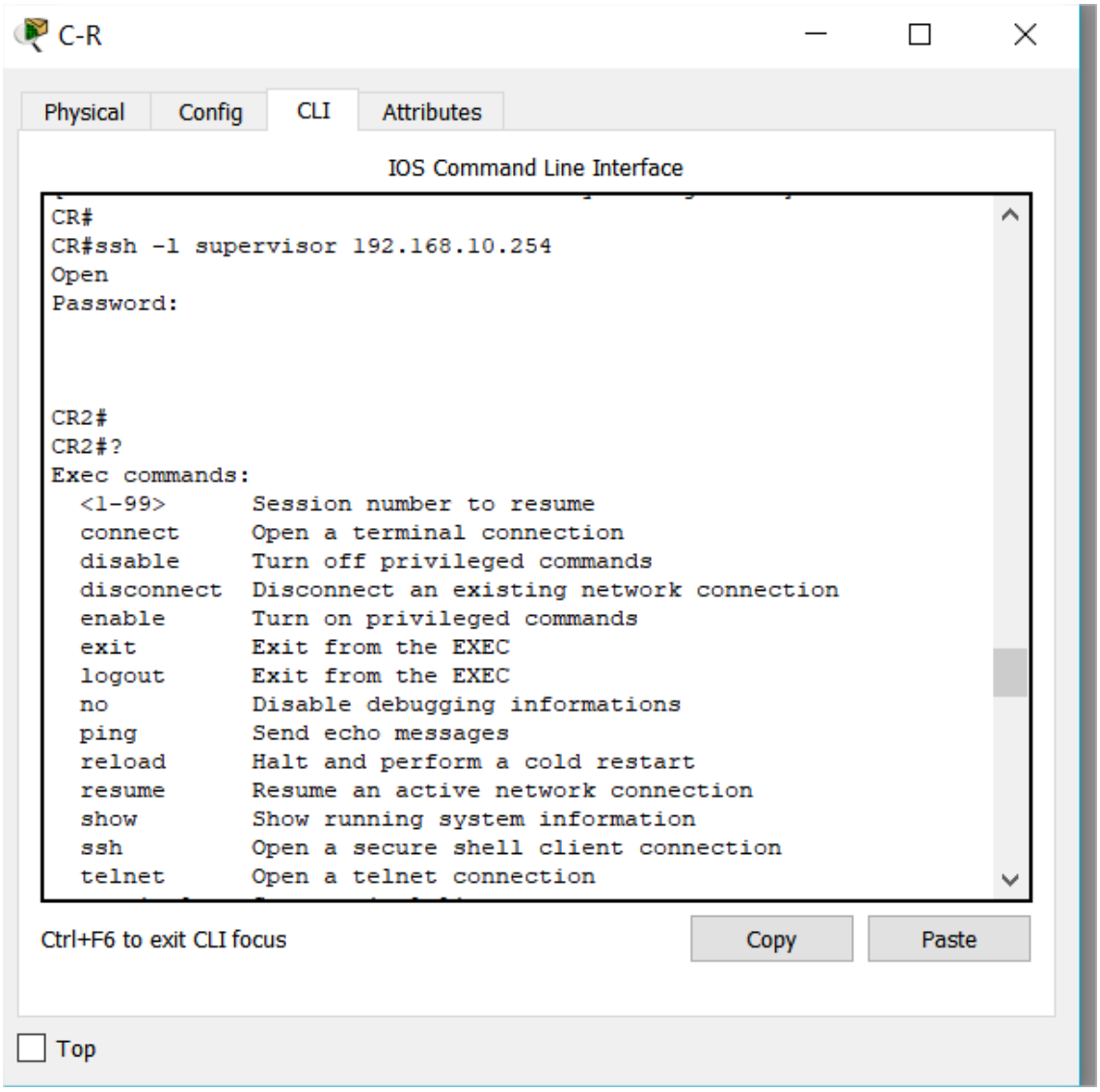

Ilustración 6. SSH de CR a CR2 como supervisor, imposibilidad de ejecutar comando como show running config.

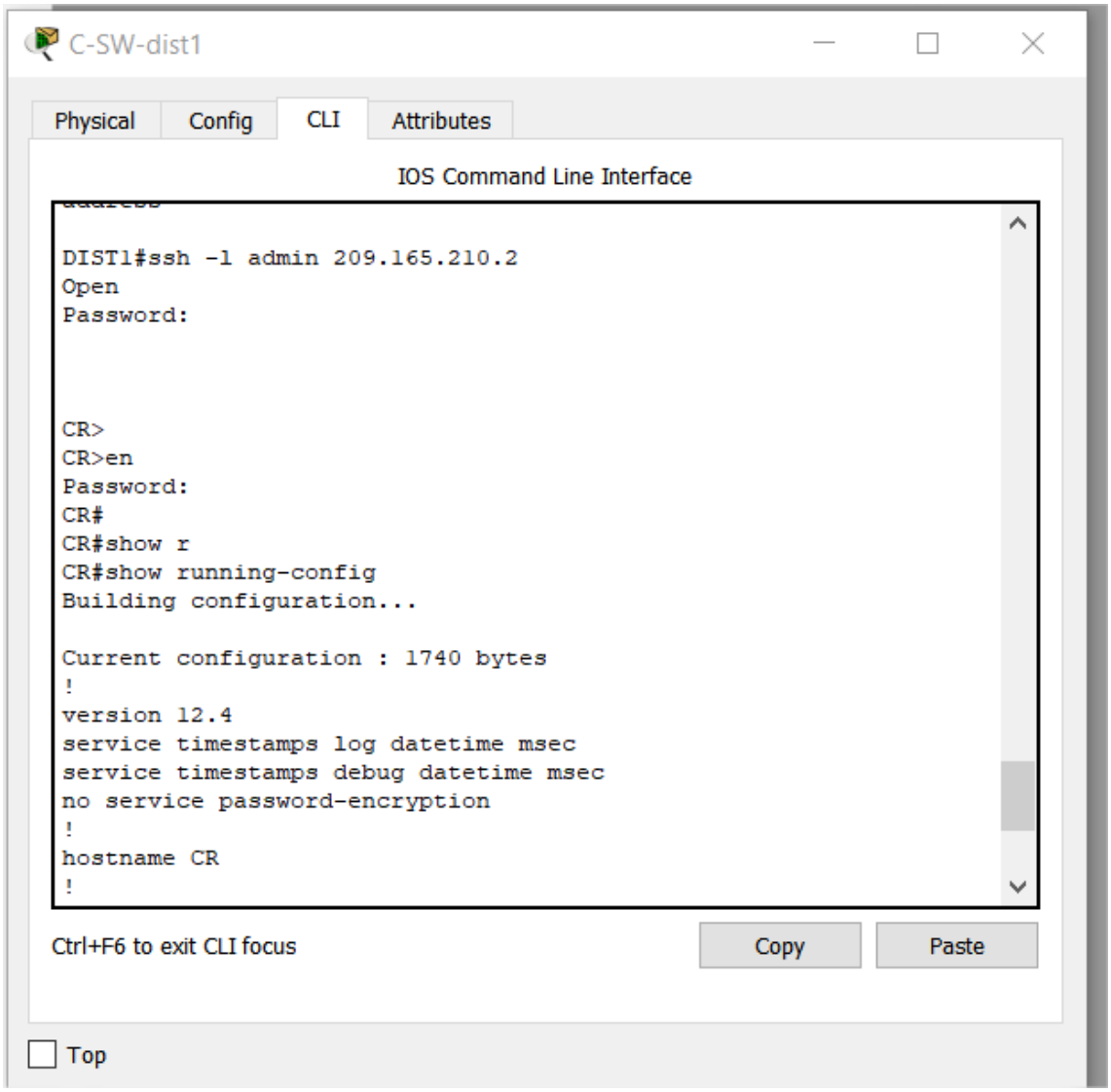

Ilustración 7. SSH desde un switch a router CR como adming, deja hacer running config al contar con todos los privilegios.

Tarea 4. AAA con autenticación frente a RADIUS.

Para la configuración de AAA con un servidor RADIUS se ha realizado la siguiente configuración el servidor RADIUS. En ella se puede apreciar que se ha creado el usuario contra el que se autentica, remoteAdmin. Y además se dan de alta los dispositivos autorizados a utilizar dicho servidor RADIUS con una contraseña RadiusPa55w0rd.

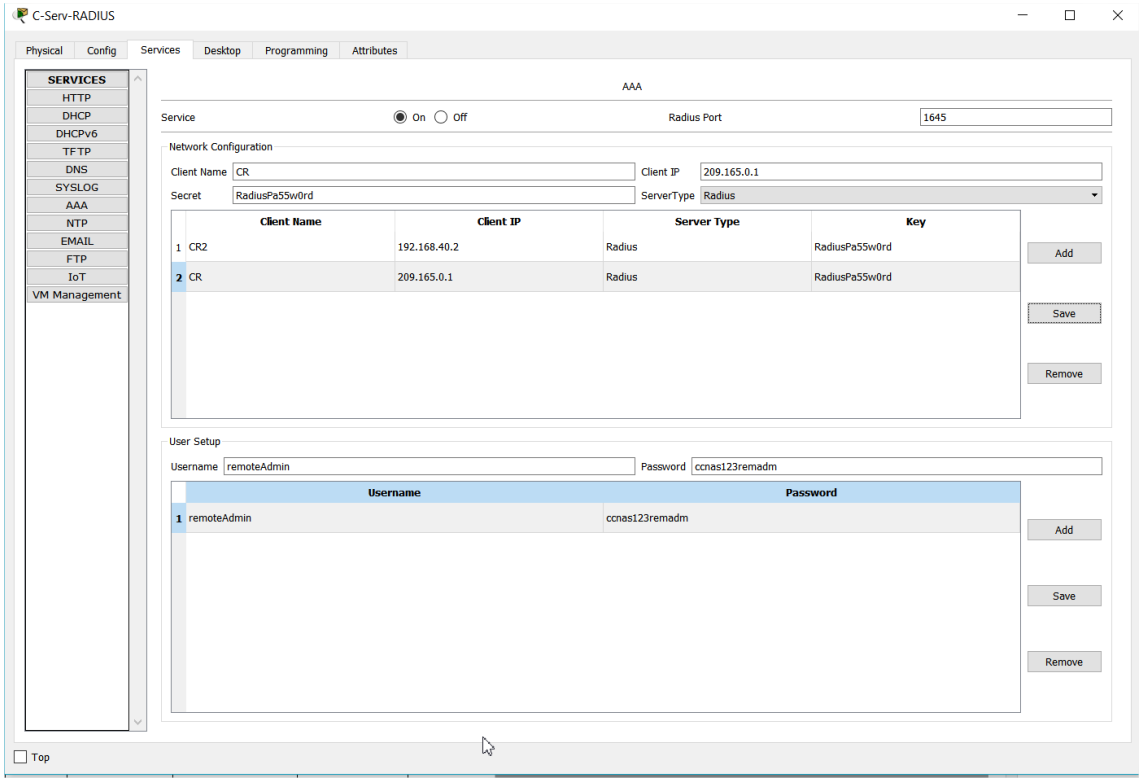

Ilustración 8. Configuración del servidor radius

En cada router se lleva a cabo la siguiente configuración.

```
Aaa new-model

radius-server host 209.165.0.12 key RadiusPa55w0rd

aaa authentication login default group radius local
```

Nos aseguramos de que las dos contraseñas introducidas coinciden tanto en el cliente como en el servidor.

Adicionalmente se establece como segundo método de autenticación alternativo el local.

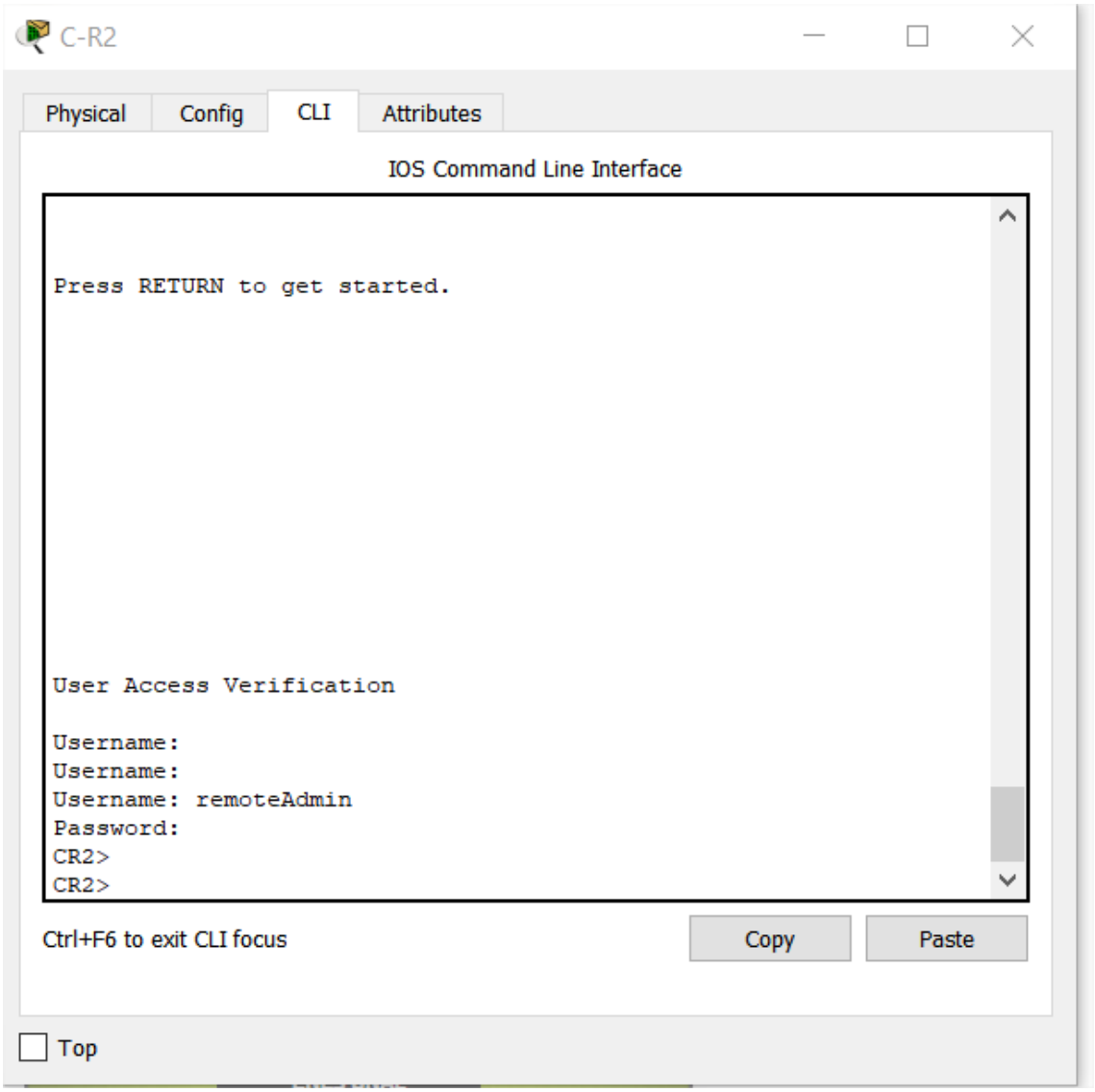

Ilustración 9. Ejemplo de autenticación contra el servidor RADIUS.

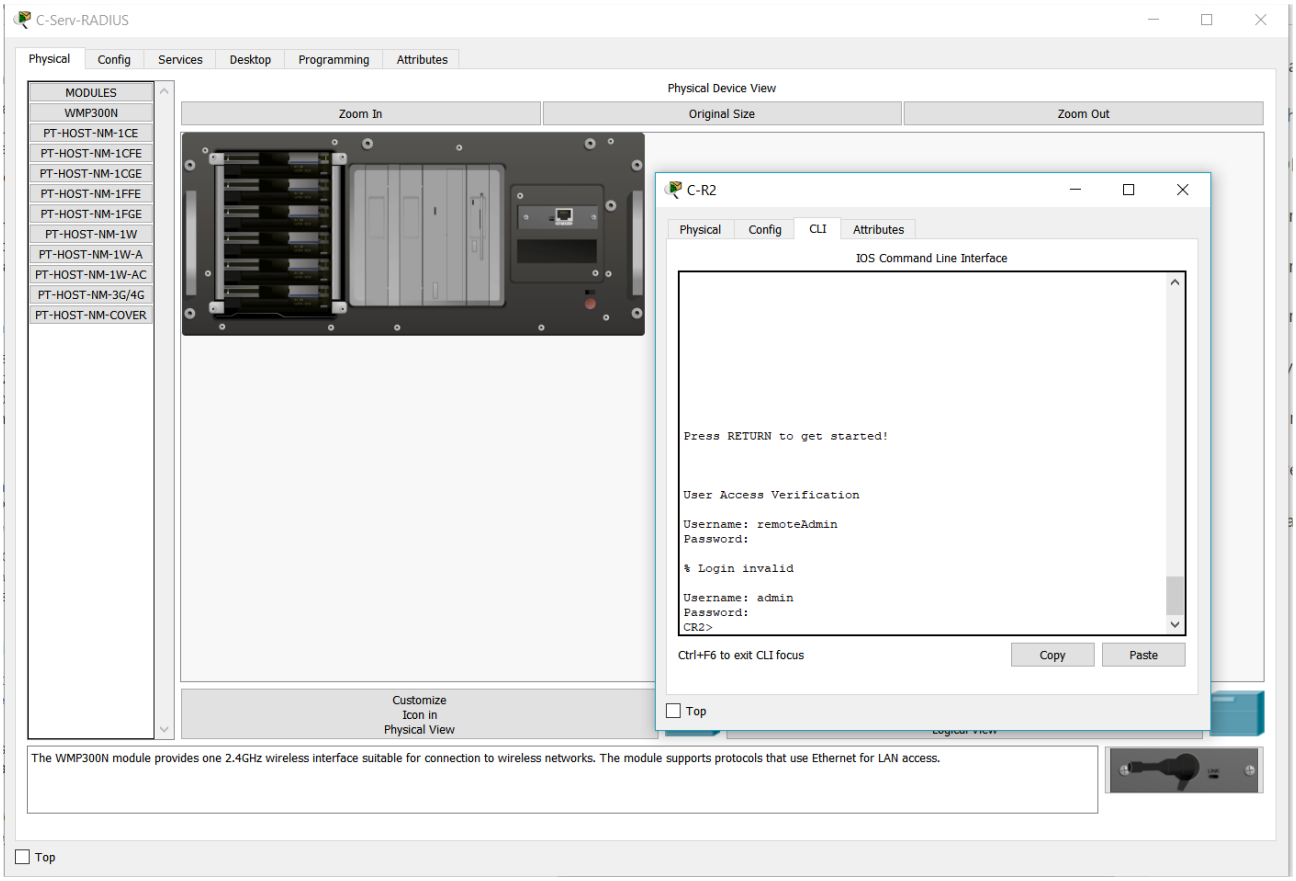

Ilustración 10. Comprobando con el servidor RADIUS apagado que hace login localmente con el usuario admin.

Tarea 5. Configurar un firewall de filtrado de paquetes en la sucursal B.

Para la configuración hemos aplicado dos ACL, una de entrada y otra salida en la interfaz interna del router de la sucursal B FastEthernet 0/0. Para la ACL de salida hemos denegado las conexiones a internet al servidor de dicha sucursal, denegando aquellas salidas que utilicen los puertos 80 o 443 utilizados para conexiones a internet.

En la ACL de salida permitimos los paquetes de toda la red interna de la empresa, así como el DMZ, y adicionalmente permitimos conexiones de vuelta que se hayan establecido. Es decir, cuando un dispositivo se conecta a internet, permite su vuelta con el comando established. Esta mira en la trama el bit de la ACK para dejar pasar o no una trama.

```
En
Conf t
Ip Access-list extended ACL_IN
deny tcp host 209.165.221.10 any eq 80
deny tcp host 209.165.221.10 any eq 443
permit ip any any
exit

Ip Access-list extended ACL_OUT
permit ip 209.165.221.0 0.0.0.7 any
permit ip 209.165.221.8 0.0.0.7 any
permit ip 209.165.0.0 0.0.0.255 any
permit tcp any any established
exit

interface fa0/0
ip access-group ACL_IN in
ip access-group ACL_OUT out
```

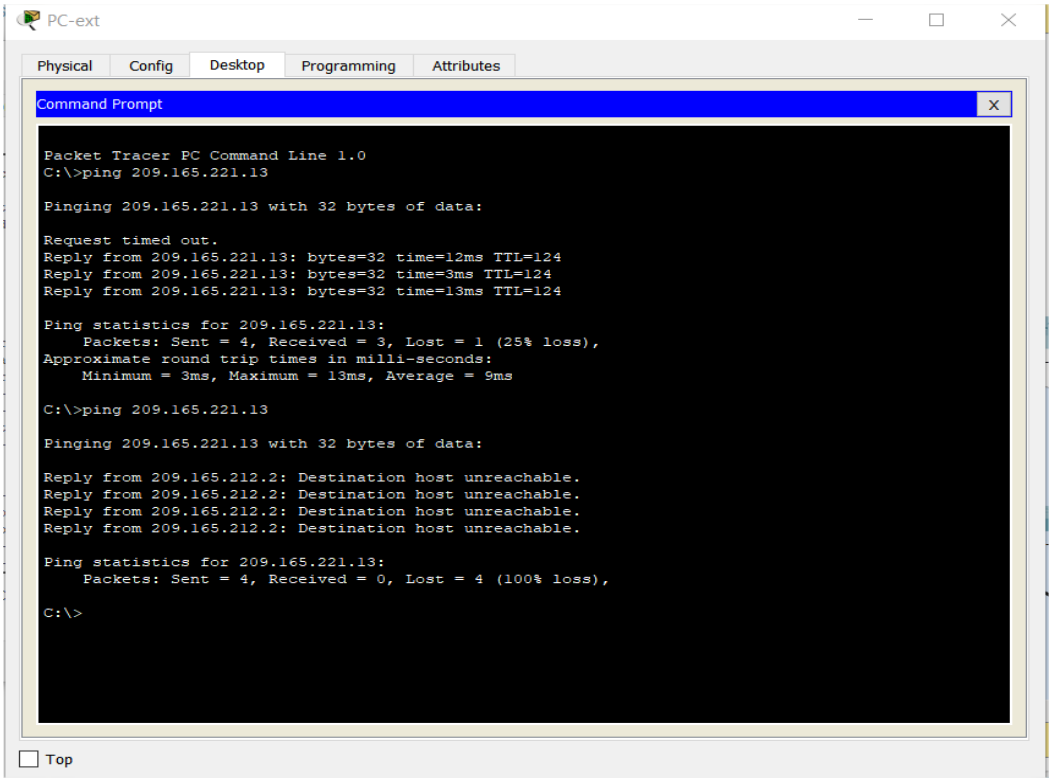

Ilustración 11. Desde el PC externo ya no se permite acceso a la sucursal B.

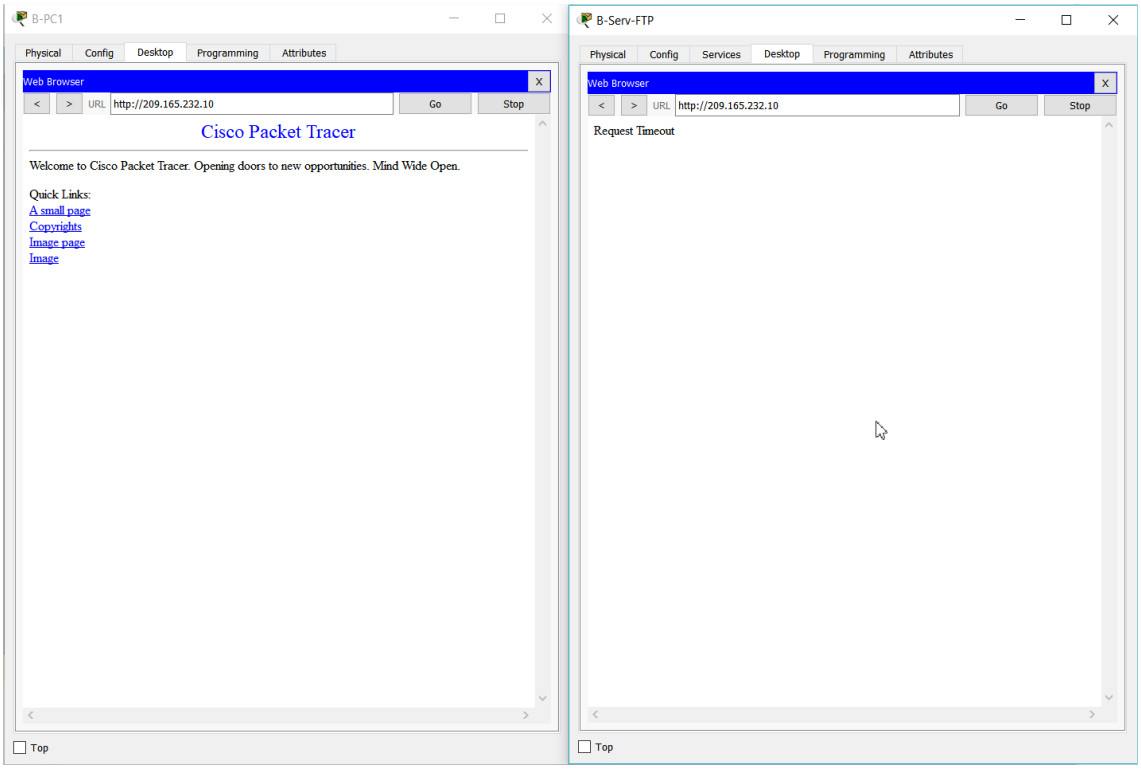

Ilustración 12. Desde la sucursal B, un pc accede a internet pero el servidor no puede.

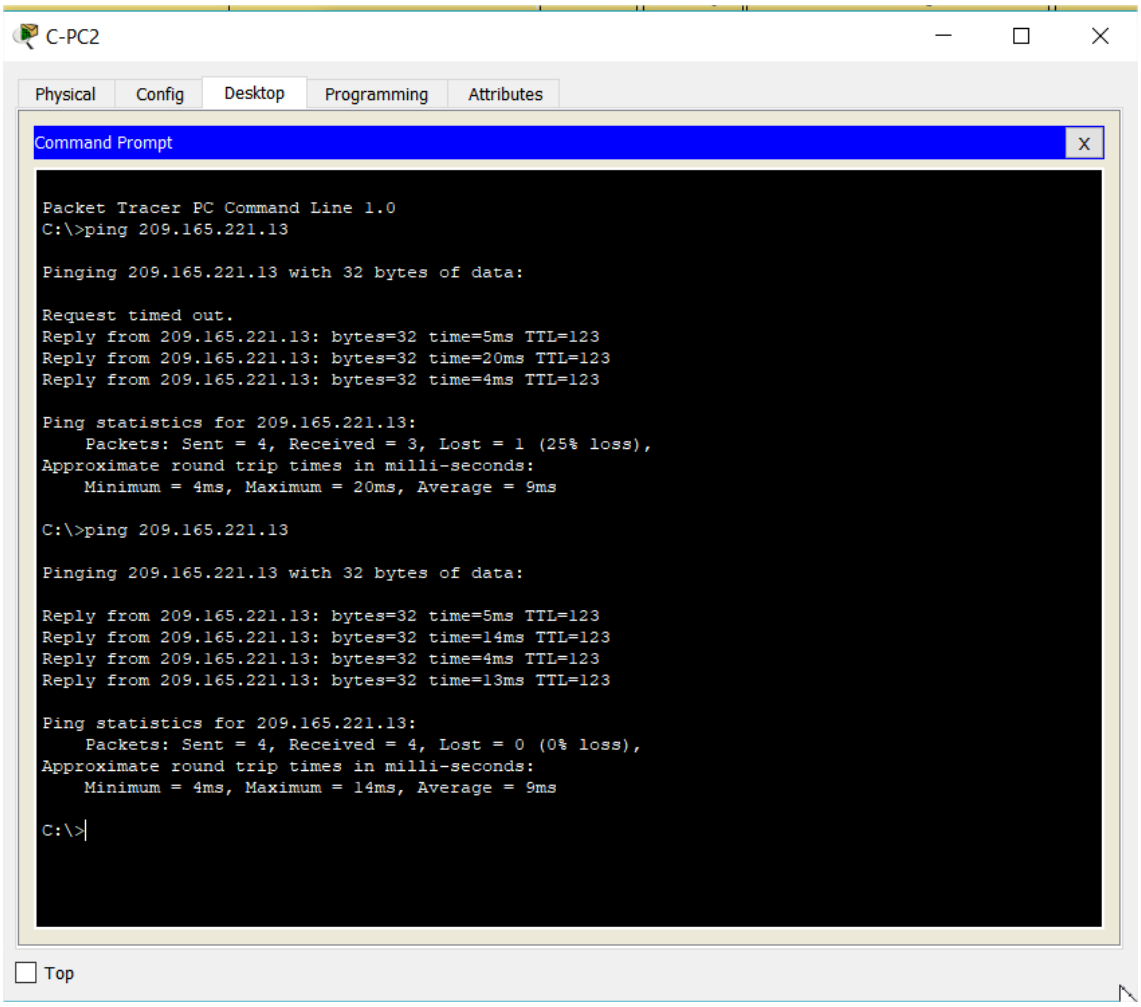

Ilustración 13. Se permite el acceso desde la central a un ordenador de la sucursal B.

Tarea 6. Configurar un firewall ZPF en la sede central.

Para la tarea 6 nos hemos quedado sin tiempo para conseguir que funcione.

Hemos habilitado el acceso a internet desde la dmz a internet para las actualizaciones.

```
zone security DMZ
zone security INTERNET
zone security INTERNA

class-map type inspect match-any UPDATES
match protocol dns
match protocol http
exit

policy-map type inspect DMZ-TO-INTERNET
class type inspect UPDATES
inspect
exit
exit

%Creamos la ACL que permite conexiones a ciertos equipos desde fuera
ip acces-list extended RAD_SYS_HTTP_DNS
permit ip any host 209.165.0.10
permit ip any host 209.165.0.11
permit ip 209.165.221.8 0.0.0.7 host 209.165.0.13
permit ip 209.165.221.0 0.0.0.7 host 209.165.0.13
permit ip 209.165.221.0 0.0.0.7 host 209.165.0.12
permit ip 209.165.221.8 0.0.0.7 host 209.165.0.12
exit
```

```
%Creamos la clase y la política que ira desde internet hasta la DMZ
class-map type inspect match-any INTERNET-DMZ
match access-group name RAD_SYS_HTTP_DNS
exit
policy-map type inspect match-any DMZ-TO-INTERNET
class type inspect  INTERNET-DMZ
inspect
exit



ip Access-list extended INTERNA-DMZ
permit 192.168.40.0 0.0.0.255 host 209.165.0.12
permit 192.168.40.0 0.0.0.255 host 209.165.0.13
exit
class-map type inspect match-any INTERNA-DMZ-CLASS
match access-group name INTERNA-DMZ
exit
policy-map type inspect match-any INTERNA-DMZ-POLICY
class type inspect  INTERNA-DMZ-CLASS
inspect
exit



zone-pair security DMZ-INTERNET source DMZ destination INTERNET
service-policy type inspect DMZ-TO-INTERNET
exit
zone-pair security INTERNET-DMZ source INTERNET destination DMZ
service-policy type inspect DMZ-TO-INTERNET
exit
zone-pair security INTERNA-DMZ source INTERNA destination DMZ
service-policy type inspect INTERNA-DMZ-POLICY
```

```
exit




Interface fa0/0
zone-member security INTERNA
exit
interface fa0/1
zone-member security DMZ
exit
interface serial0/0/0
zone-me
zone-member secu
zone-member security INTERNET
```

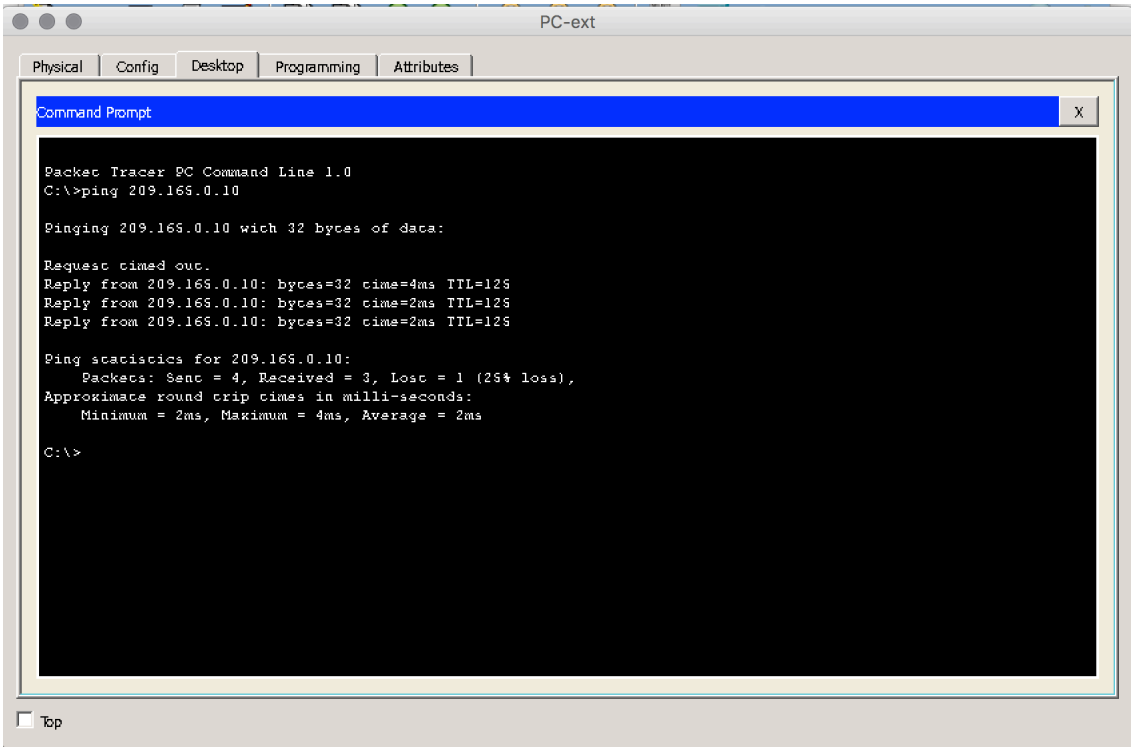

Ilustración 14. Se permite el ping externo desde pcExt al servidor DNS o http.