DMZ

Miércoles 18/2/2026

Laboratorio: Implementación de una DMZ Segura y Funcional

¡Bienvenido a tu desafío de red! En este laboratorio, aplicarás tus conocimientos para construir y asegurar una Zona Desmilitarizada (DMZ). Este es un escenario real donde una organización necesita un servidor web accesible desde Internet, sin comprometer la seguridad de su red interna.

Objetivo de Aprendizaje:

- Configurar direccionamiento IP en una topología compleja.
- Implementar NAT estático para exponer servicios internos de forma segura.
- Diseñar y aplicar Listas de Control de Acceso (ACLs) para controlar el flujo de tráfico y asegurar la red.

Topología del Laboratorio:

Tu entorno de trabajo incluye:

- **Router Central (Router_FW):** Un router Cisco ISR (ej. 2911 o 4331) actuando como el corazón de seguridad.

    - `GigabitEthernet0/0`: Conectado a tu LAN Interna (a través de `SW_Internal`).
    - `GigabitEthernet0/1`: Conectado a la DMZ (a través de `SW_DMZ`).
    - `GigabitEthernet0/2`: Conectado a la Red Externa/Internet (a través de `SW_External`).
- **Switches:** 3x Cisco 2960 (o 2960 IOS15) para cada segmento.
- **Dispositivos Finales:**
    - `PC_Internal`: Representa un usuario en tu red interna.
    - `Server-PT Web_DMZ`: El servidor web que residirá en la DMZ.
    - `PC_External`: Simula un cliente en Internet que intenta acceder a tus servicios.

Instrucciones Detalladas para la Configuración:

Paso 1: Configuración de Direccionamiento IP en Dispositivos Finales

Configura las direcciones IP estáticas en tus dispositivos finales. **¡Presta especial atención a estas IPs, ya que son cruciales para la evaluación automática!**

- **En `PC_Internal` (Desktop -> IP Configuration):**
    - `IP Address`: **192.168.1.10**
    - `Subnet Mask`: **255.255.255.0**
    - `Default Gateway`: **192.168.1.1**
- **En `Server-PT Web_DMZ` (Desktop -> IP Configuration):**
    - `IP Address`: **192.168.2.10**
    - `Subnet Mask`: **255.255.255.0**
    - `Default Gateway`: **192.168.2.1**
- **En `PC_External` (Desktop -> IP Configuration):**
    - `IP Address`: **192.168.3.10**
    - `Subnet Mask`: **255.255.255.0**
    - `Default Gateway`: **192.168.3.1**

Paso 2: Configuración de Interfaces en el Router (Router_FW)

Accede a la CLI del `Router_FW` y configura sus interfaces.

```
Router> enable

Router# configure terminal

Router(config)# hostname Router_FW



Router_FW(config)# interface GigabitEthernet0/0

Router_FW(config-if)# ip address 192.168.1.1 255.255.255.0

Router_FW(config-if)# no shutdown
```

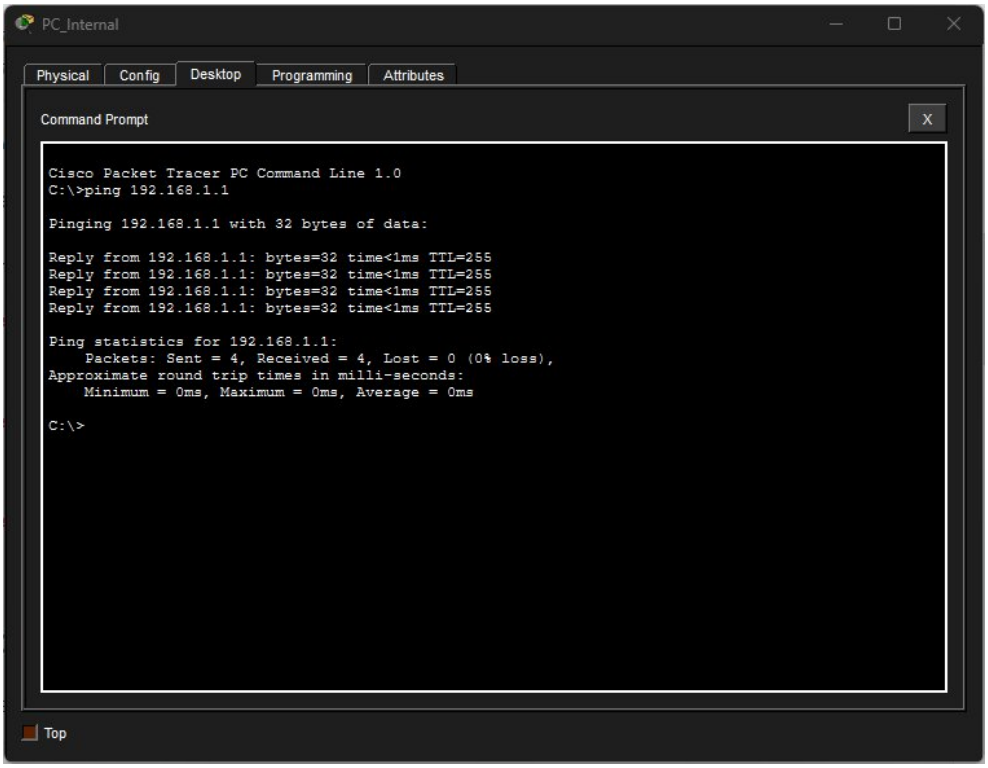
```
Router_FW(config-if)# exit


Router_FW(config)# interface GigabitEthernet0/1
Router_FW(config-if)# ip address 192.168.2.1 255.255.255.0
Router_FW(config-if)# no shutdown
Router_FW(config-if)# exit


Router_FW(config)# interface GigabitEthernet0/2
Router_FW(config-if)# ip address 192.168.3.1 255.255.255.0
Router_FW(config-if)# no shutdown
Router_FW(config-if)# exit


Router_FW(config)# end
Router_FW# write memory
```

Paso 3: Verificación de Conectividad Básica (¡CRÍTICO ANTES DE AVANZAR!)

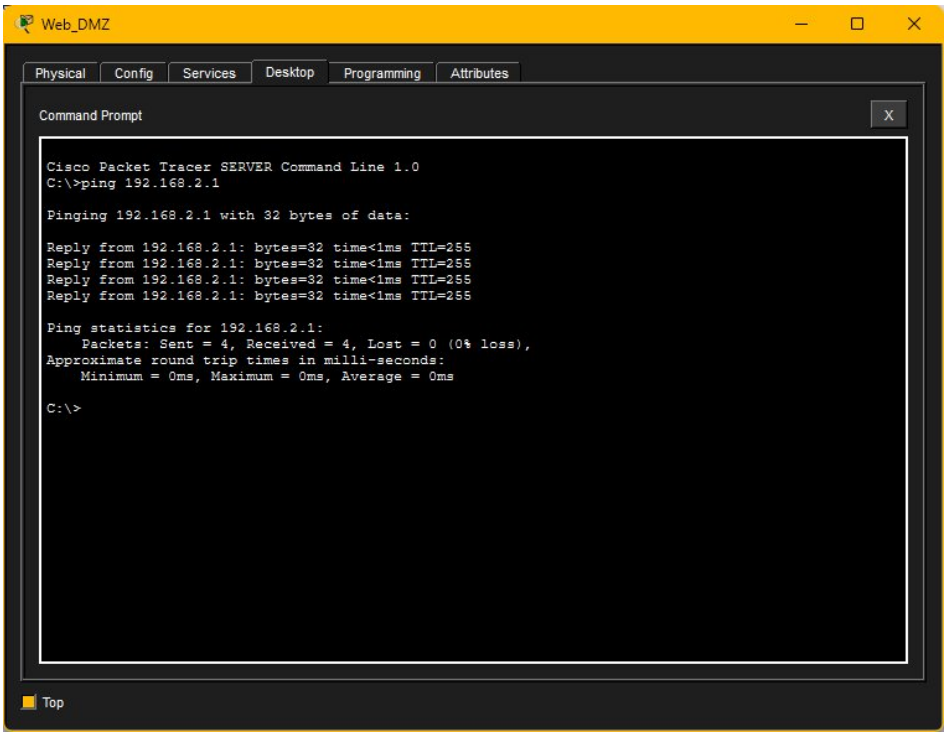
Antes de seguir, asegúrate de que tus dispositivos puedan alcanzar sus respectivos gateways. Si alguno falla, revisa IPs, máscaras, gateways, estado de interfaces (`show ip interface brief` en el router) y el cableado. ¡No continúes hasta que esto funcione!

- **Desde `PC_Internal` (Command Prompt):**
  - `ping 192.168.1.1` (Ping a su Gateway)

- *Resultado esperado: Replies (¡Debe funcionar!).*

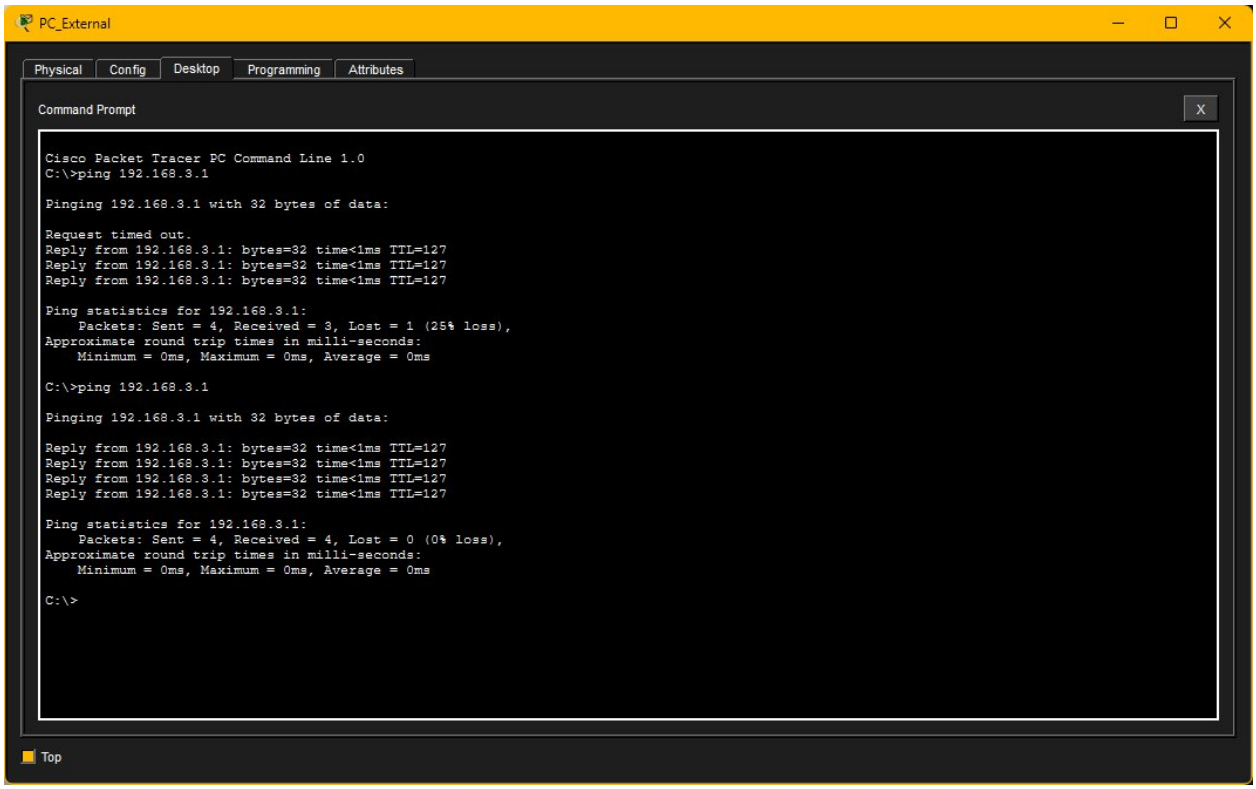


- **Desde `Server-PT Web_DMZ` (Command Prompt):**
  - `ping 192.168.2.1` (Ping a su Gateway)
  - *Resultado esperado: Replies (¡Debe funcionar!).*



- **Desde `PC_External` (Command Prompt):**
  - `ping 192.168.3.1` (Ping a su Gateway)

- *Resultado esperado: Replies (¡Debe funcionar!).*



aquí se puede ver que la primera vez hubo un retraso y falló, pero la conexión estaba bien establecida.

Paso 4: Configuración de NAT Estático en el Router (Router_FW)

Configura el NAT para permitir el acceso al servidor web de la DMZ desde Internet.

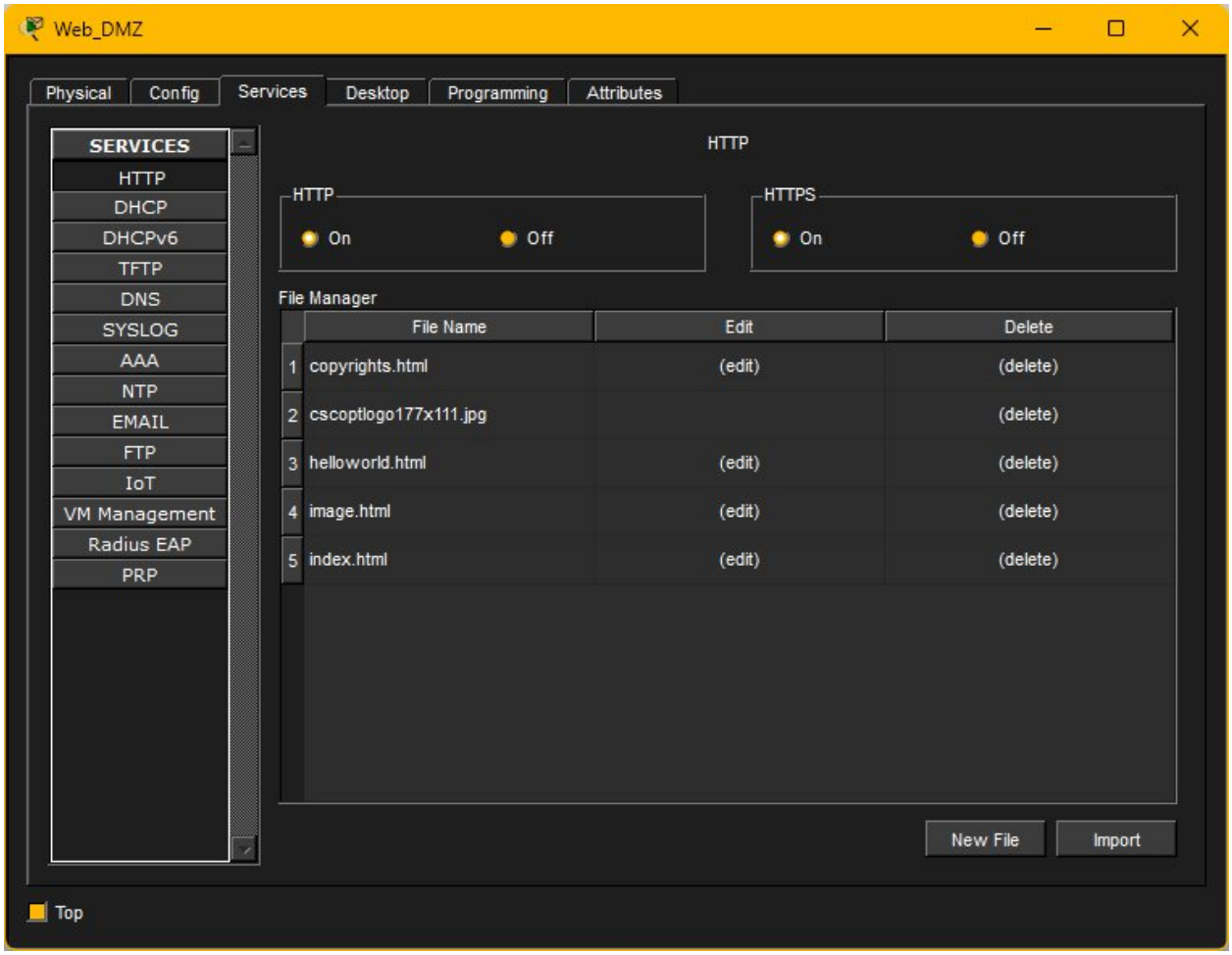
```
Router_FW# configure terminal

Router_FW(config)# interface GigabitEthernet0/1

Router_FW(config-if)# ip nat inside

! La interfaz DMZ es 'inside' para el NAT

Router_FW(config-if)# exit


Router_FW(config)# interface GigabitEthernet0/2

Router_FW(config-if)# ip nat outside

! La interfaz externa es 'outside' para el NAT

Router_FW(config-if)# exit


Router_FW(config)# ip nat inside source static 192.168.2.10 192.168.3.1

Router_FW(config)# end

Router_FW# write memory
```

Nota: Este comando crea un mapeo uno a uno. Desde la perspectiva de la red externa (Internet), el servidor (`192.168.2.10`) será accesible a través de la IP pública **192.168.3.1**.

Paso 5: Activación de Servicios Web en el Servidor DMZ (Server-PT Web_DMZ)

Asegúrate de que el servidor DMZ esté listo para responder a las solicitudes web.

- **En `Server-PT Web_DMZ`:**
  - Ve a la pestaña `Services` -> `HTTP`.
  - Asegúrate de que `HTTP` y `HTTPS` estén en `ON`.
  - (Opcional): Edita el archivo `index.html` para personalizar la página de bienvenida: He puesto un título H1

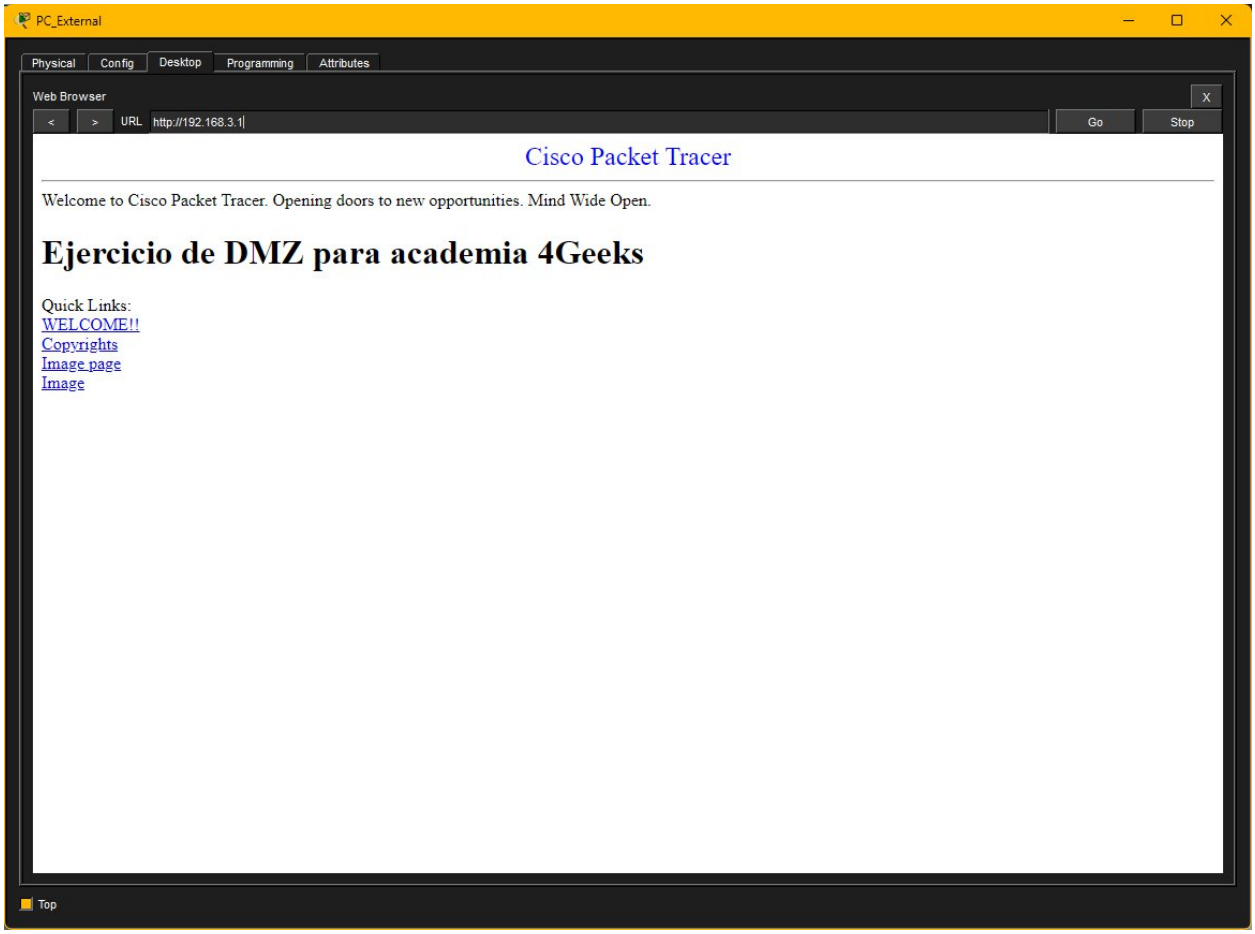


Paso 6: Prueba de Acceso Web Inicial (ANTES de ACLs de Seguridad)

Verifica que el NAT y los servicios web funcionan antes de implementar las ACLs de seguridad.

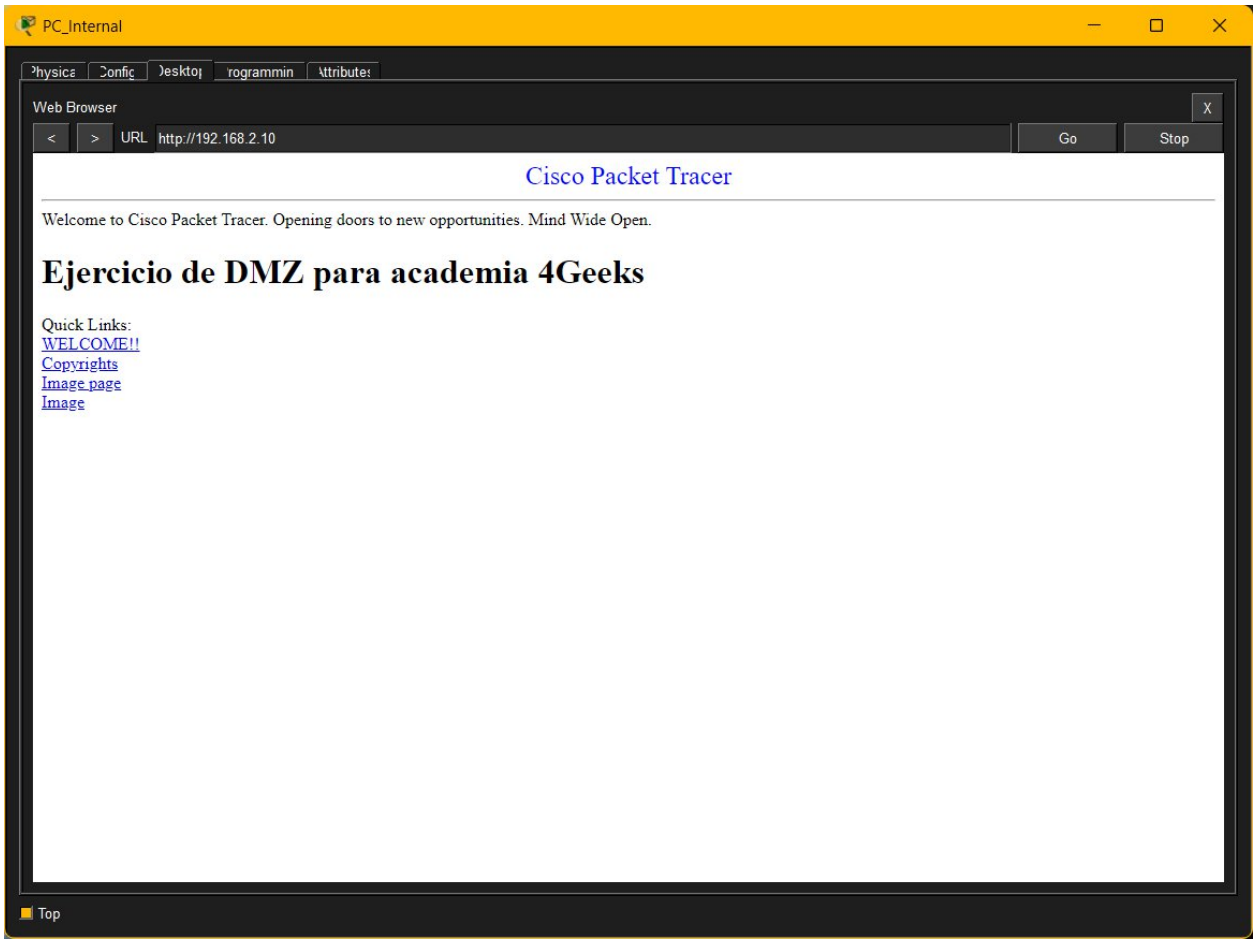
- **Desde `PC_External` (Web Browser):**
  - En la barra de direcciones, escribe `192.168.3.1` y presiona Enter.

- *Resultado esperado: La página web del `Server-PT Web_DMZ` debe cargar.*



- **Desde `PC_Internal` (Web Browser):**
  - En la barra de direcciones, escribe `192.168.2.10` y presiona Enter.
  - *Resultado esperado: La página web del `Server-PT Web_DMZ` debe cargar.*

(en este punto, cargaba la web desde los PC interno y externo)



Paso 7: Configuración de ACLs para Seguridad (¡El Paso Clave de Seguridad Flexible!)

Ahora, implementa las ACLs para controlar el tráfico. **Recuerda que lo importante es el RESULTADO deseado, no el número de ACL o la sintaxis exacta que utilices.**

- **Acceso Web desde Internet a DMZ:**
  - Crea una ACL que permita **solamente** el tráfico HTTP (puerto 80) desde *cualquier origen* (`any`) hacia la IP pública de tu servidor web DMZ (`192.168.3.1`).
  - Esta ACL debe aplicarse a la interfaz `GigabitEthernet0/2` (WAN) en sentido `inbound`.
  - Por defecto, esta ACL implícitamente denegará otros tipos de tráfico desde Internet (incluido ICMP/ping).

```
Router_FW>enable

Router_FW#config terminal

Enter configuration commands, one per line.  End with CNTL/Z.

Router_FW(config)#
```

```
Router_FW(config)# ip access-list extended ACL_EXTERNA

Router_FW(config-ext-nacl)# permit tcp any host 192.168.3.1 eq 80

Router_FW(config-ext-nacl)# exit



Router_FW(config)# interface GigabitEthernet0/2

Router_FW(config-if)# ip access-group ACL_EXTERNA in

Router_FW(config-if)# exit

write memory
```

- **Seguridad DMZ a LAN (¡CRÍTICO!):**
  - Crea una ACL que **DENIEGUE COMPLETAMENTE** cualquier intento de comunicación que se origine desde la red DMZ (`192.168.2.0/24`) y se dirija hacia la red LAN Interna (`192.168.1.0/24`).
  - Esta ACL debe aplicarse a la interfaz `GigabitEthernet0/1` (DMZ) en sentido `inbound`.

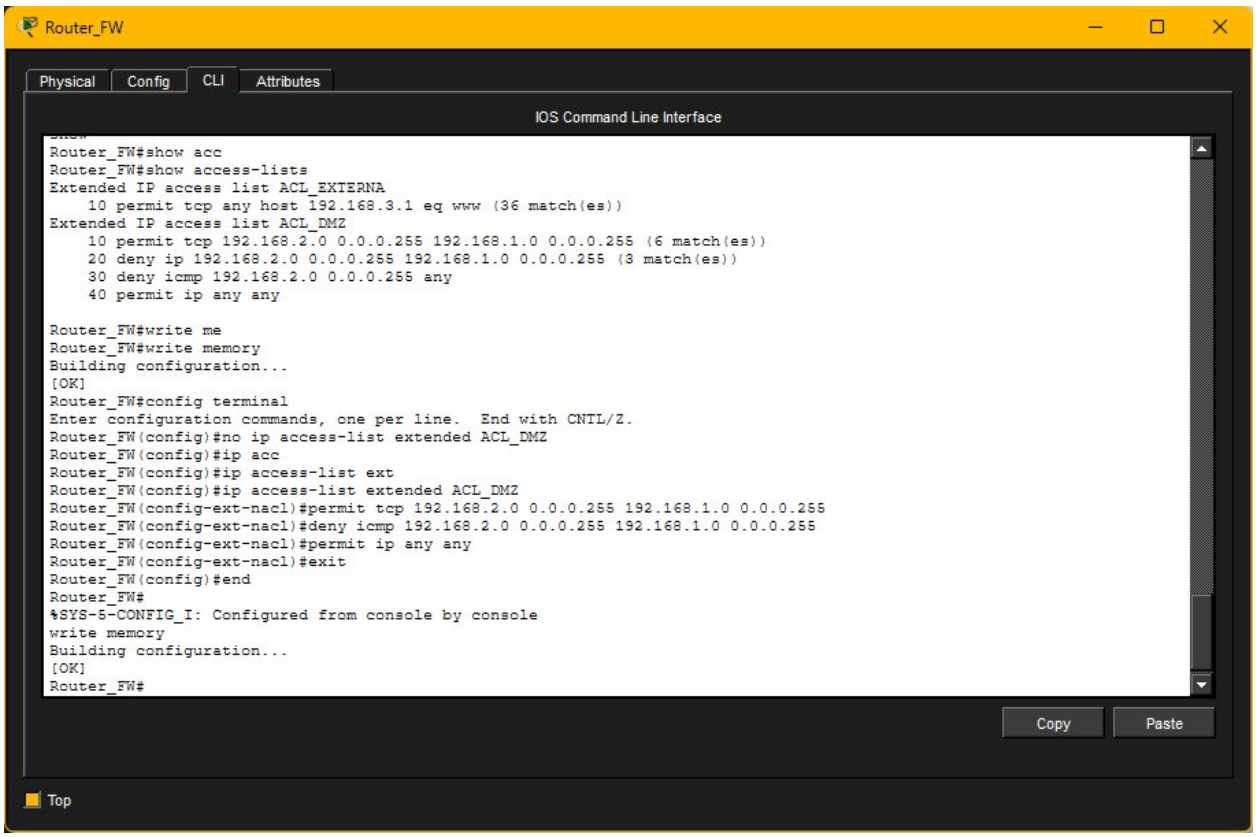
```
Router_FW(config)# ip access-list extended ACL_DMZ

Router_FW(config-ext-nacl)# permit tcp 192.168.2.0 0.0.0.255 192.168.1.0
0.0.0.255 established

Router_FW(config-ext-nacl)# deny ip 192.168.2.0 0.0.0.255 192.168.1.0
0.0.0.255

Router_FW(config-ext-nacl)# permit ip any any

Router_FW(config-ext-nacl)# exit



Router_FW(config)# interface GigabitEthernet0/1

Router_FW(config-if)# ip access-group ACL_DMZ in

Router_FW(config-if)# exit



Router_FW(config)# end

Router_FW# write memory
```

> NOTA: **¿Por qué `permit ip any any` al final en ACL_DMZ?** Para no bloquear el tráfico legítimo del servidor hacia Internet. Solo bloqueamos DMZ → LAN.

He tenido que borrar varias veces la configuración y volver a implementar... Este es el código único final que sería necesario:

```
Router_FW# configure terminal

Router_FW(config)# no ip access-list extended ACL_DMZ
```

```
Router_FW(config)# ip access-list extended ACL_DMZ

Router_FW(config-ext-nacl)# permit tcp 192.168.2.0 0.0.0.255 192.168.1.0
0.0.0.255 established

Router_FW(config-ext-nacl)# deny icmp 192.168.2.0 0.0.0.255 any

Router_FW(config-ext-nacl)# deny ip 192.168.2.0 0.0.0.255 192.168.1.0
0.0.0.255

Router_FW(config-ext-nacl)# permit ip any any

Router_FW(config-ext-nacl)# exit

Router_FW(config)# end

Router_FW# write memory
```

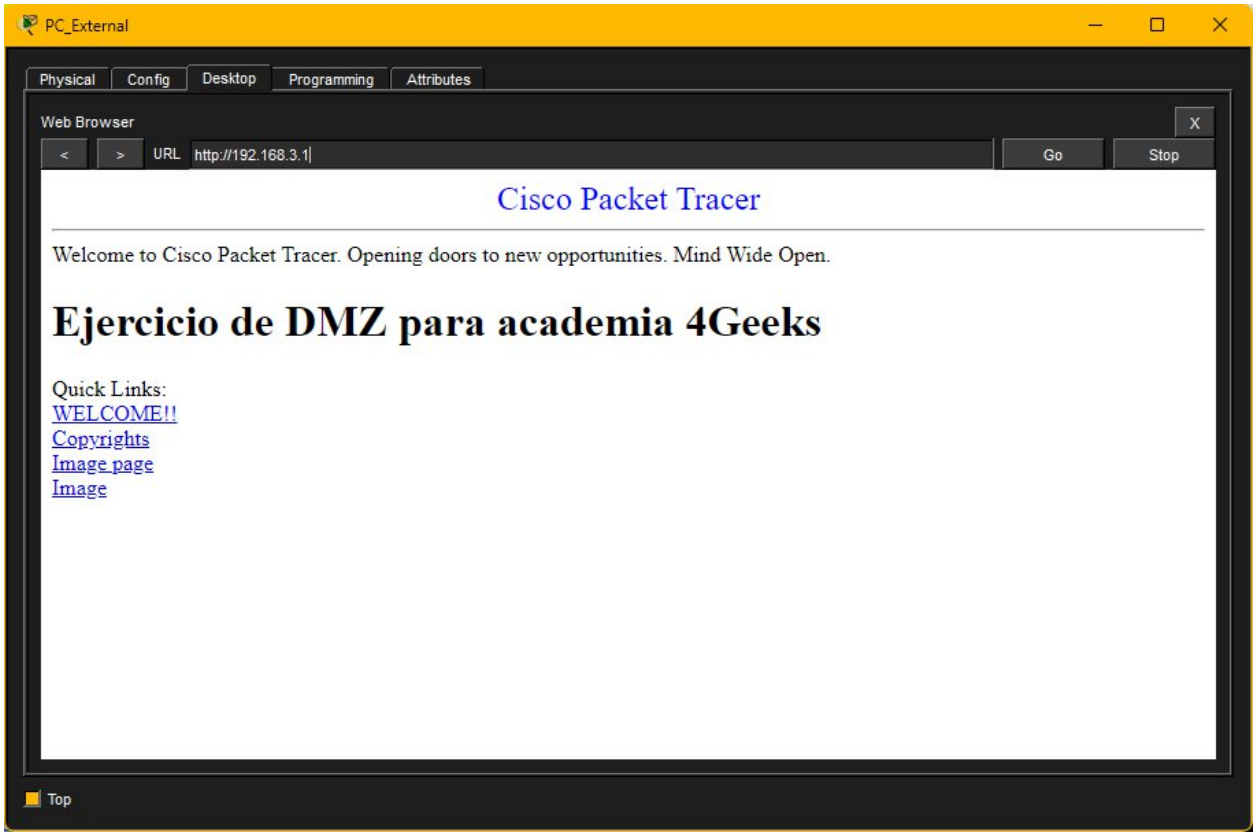


Paso 8: Verificación Final de Seguridad y Funcionalidad

Realiza estas pruebas finales para confirmar que tu DMZ es segura y funcional.

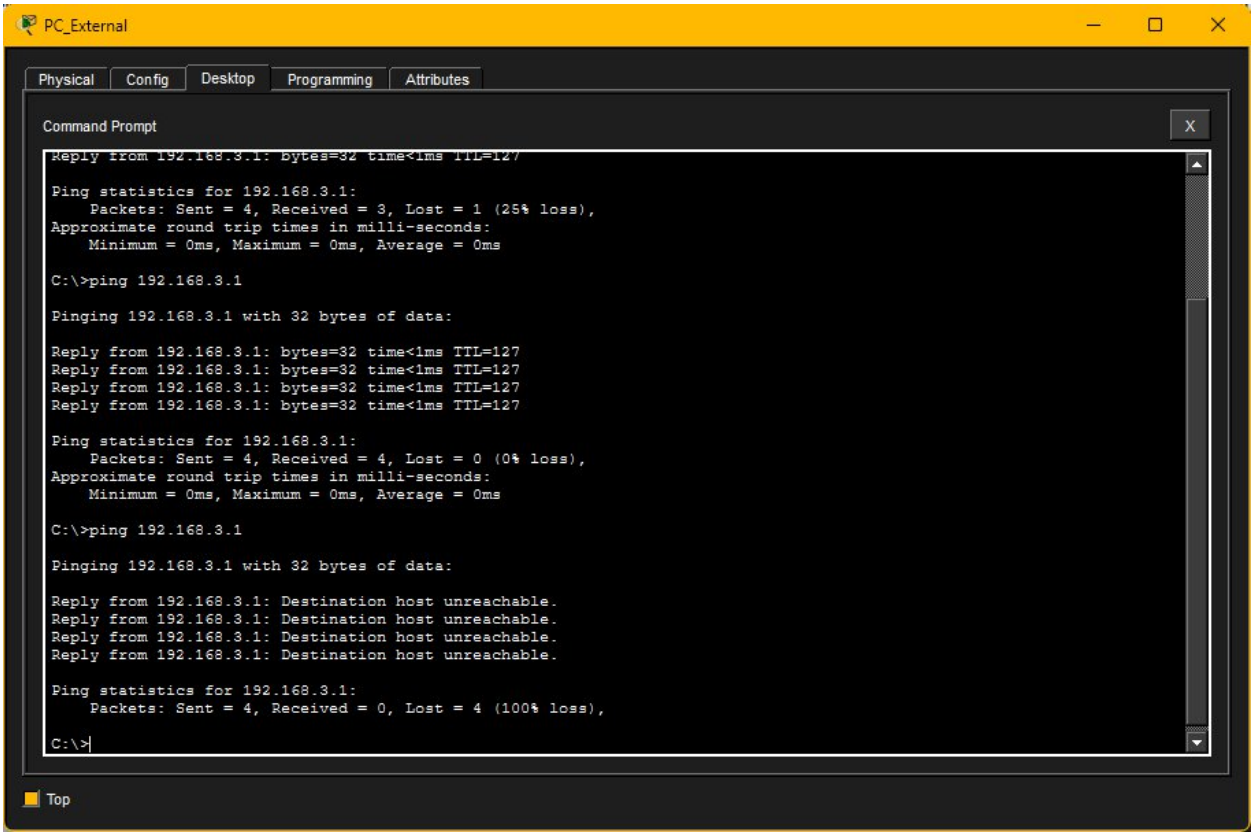
8.1 Desde `PC_External` (Web Browser):

- Accede al servidor web DMZ (`192.168.3.1`). *Resultado esperado: La página web debe* ***cargar****.*



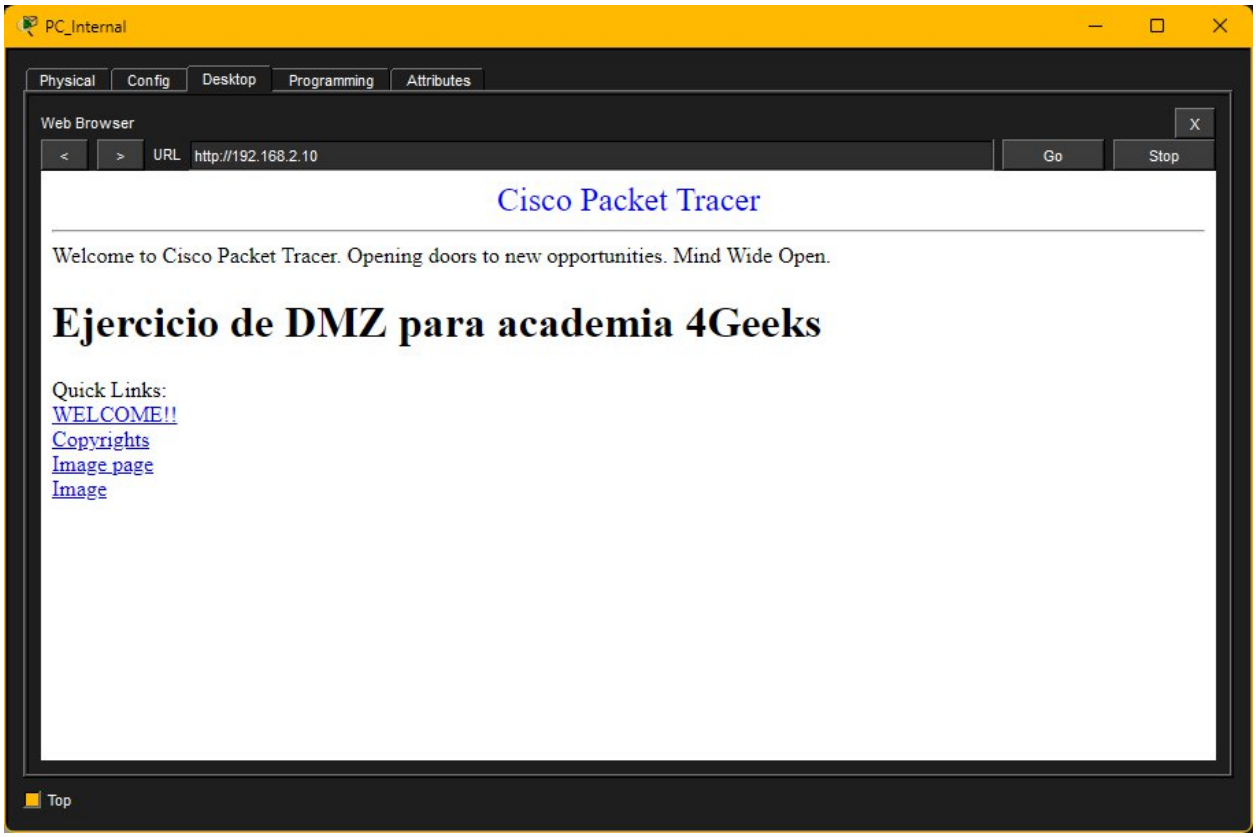
8.2 Desde `PC_External` (Command Prompt):

- `ping 192.168.3.1` (Ping a la interfaz WAN/IP pública del servidor). *Resultado esperado:* ***Request timed out*** *(Debe FALLAR si tu ACL externa bloquea ICMP).*



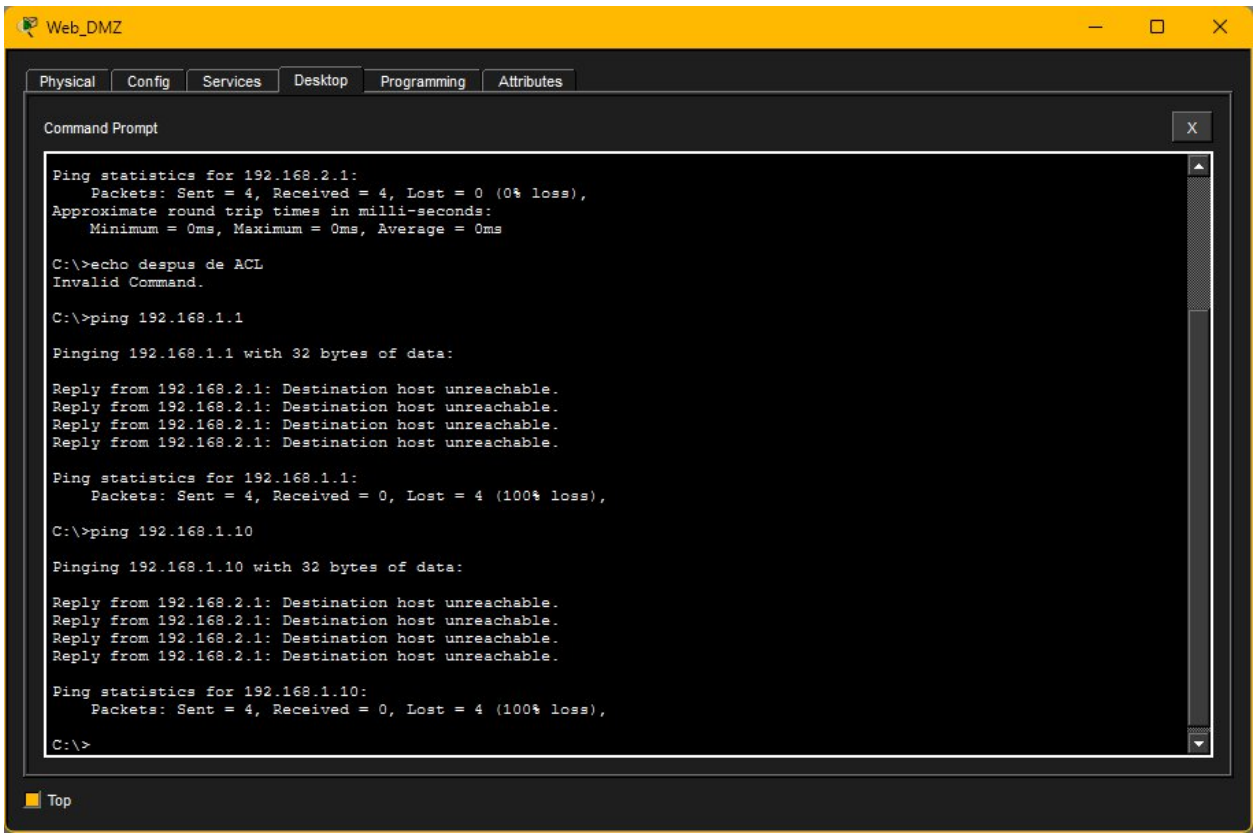
8.3 Desde `PC_Internal` (Web Browser):

- Accede al servidor web DMZ (`192.168.2.10`). *Resultado esperado: La página web debe **cargar**.*



8.4 Desde `Server-PT Web_DMZ` (Command Prompt):

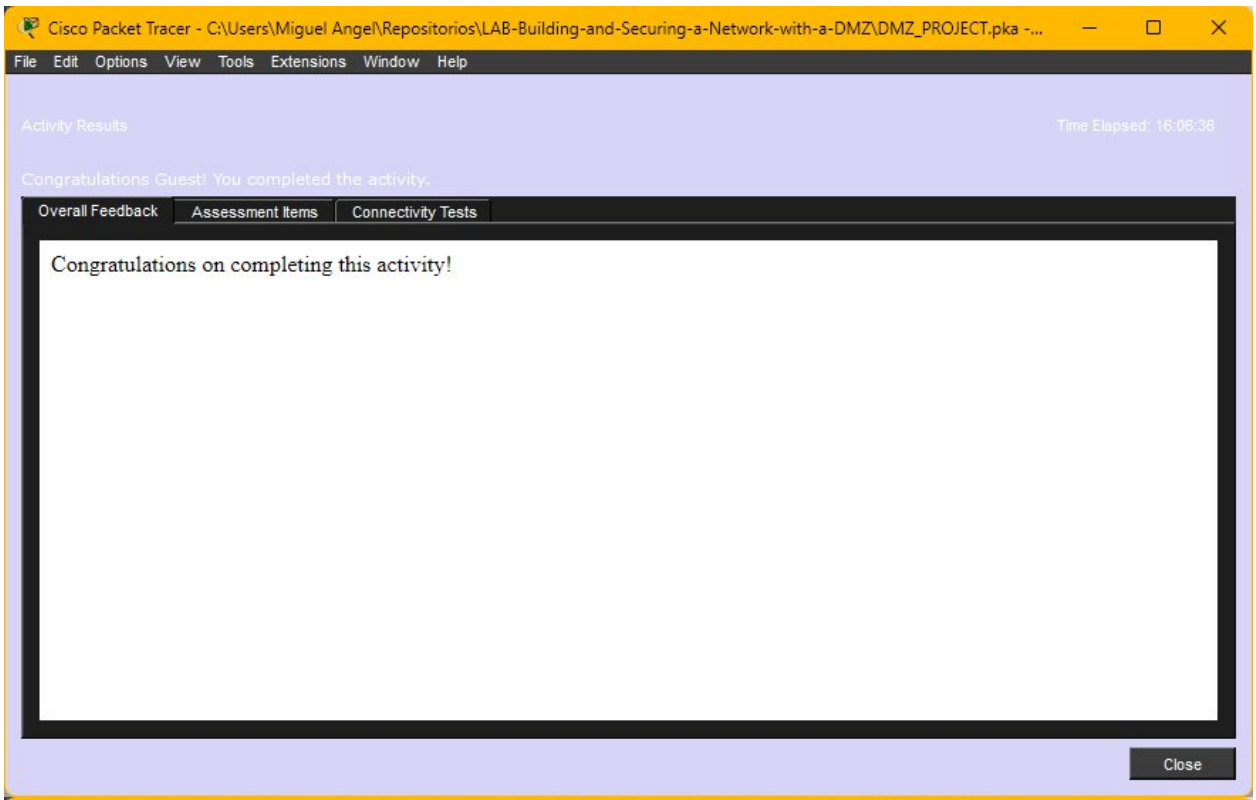
- `ping 192.168.1.10` (Ping a `PC_Internal`). *Resultado esperado:* ***Request timed out*** *(Debe FALLAR - ¡Esto es seguridad crucial!).*

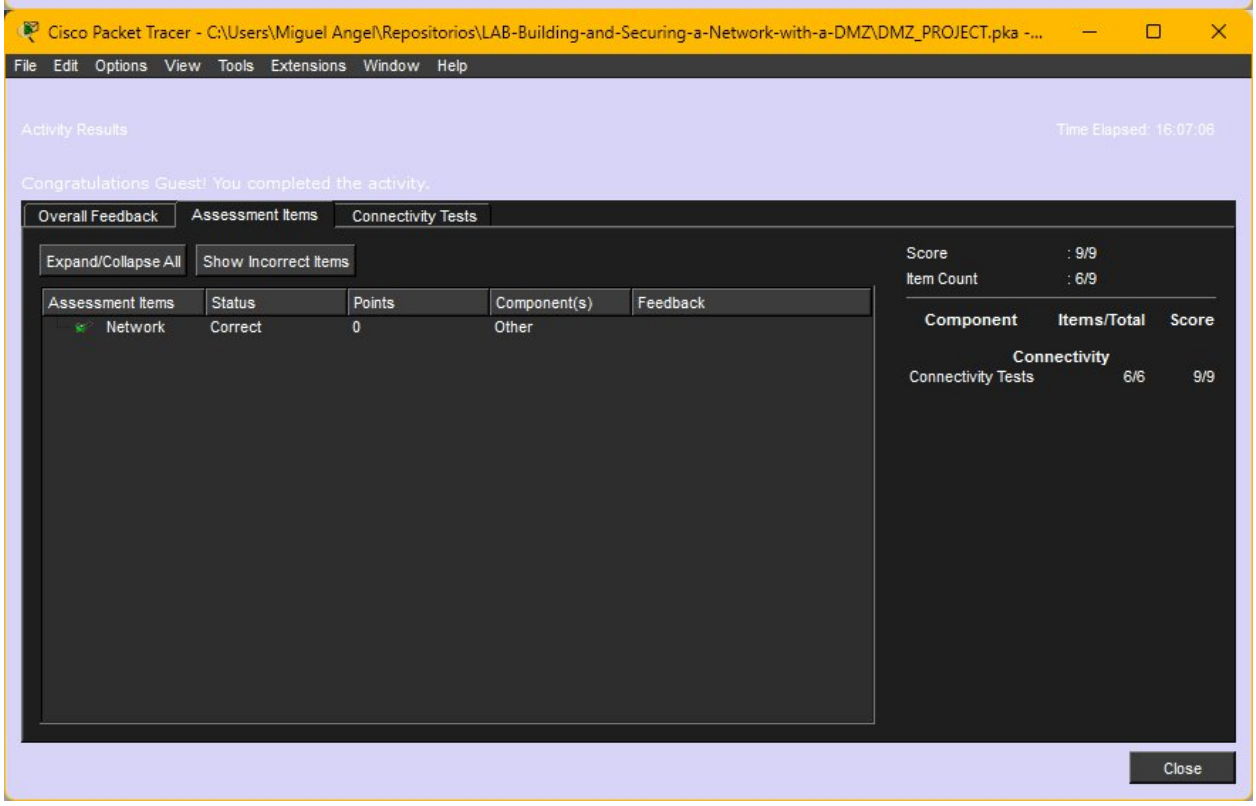


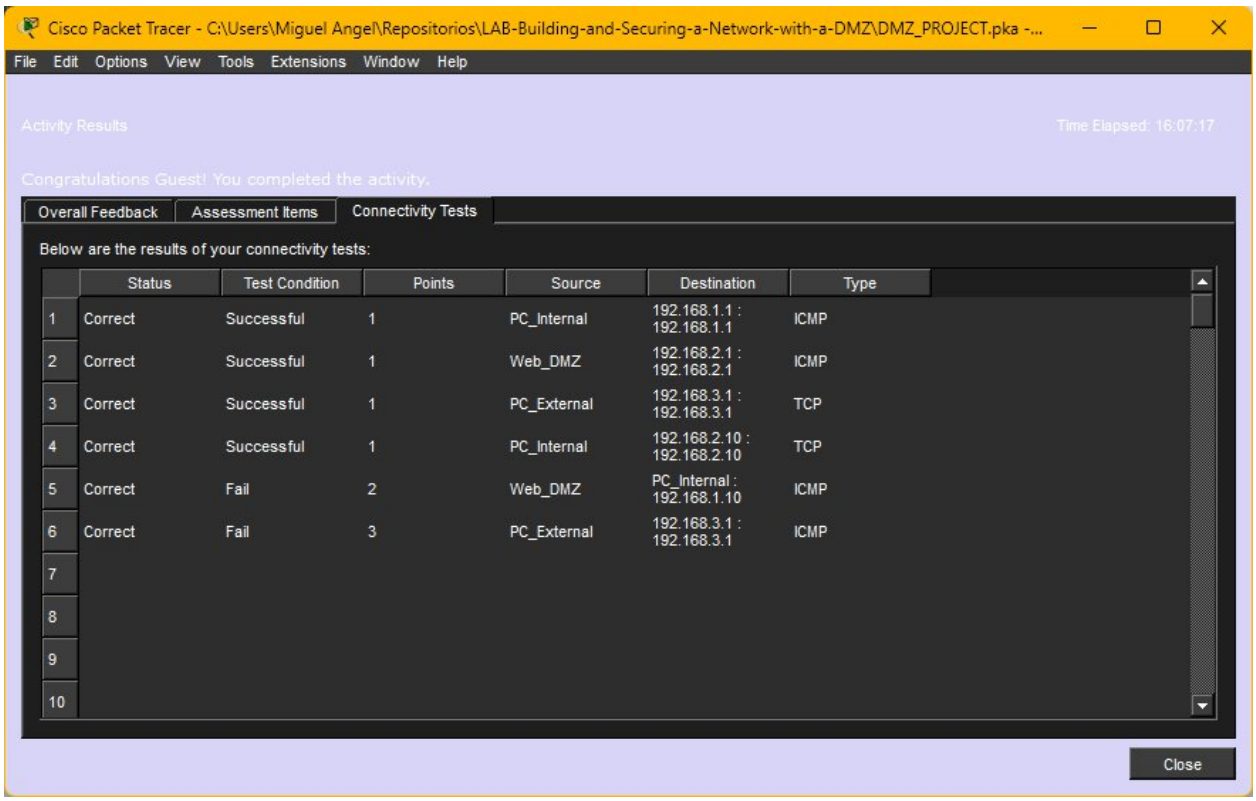
Auto-Evaluación de tu Progreso:

Una vez que hayas completado todos los pasos y las pruebas manuales te den los resultados esperados:

1. Haz clic en el botón `Check Results` en la ventana del laboratorio.
2. El sistema de evaluación te mostrará tu puntuación y si has logrado todos los objetivos de configuración y seguridad.


Cisco Packet Tracer - C:\Users\Miguel Angel\Repositorios\LAB-Building-and-Securing-a-Network-with-a-DMZ\DMZ_PROJECT.pka -...
File Edit Options View Tools Extensions Window Help
Activity Results
Time Elapsed: 16:06:36
Congratulations Guest! You completed the activity.
Overall Feedback
Assessment Items
Connectivity Tests
Congratulations on completing this activity!
Close


Cisco Packet Tracer - C:\Users\Miguel Angel\Repositorios\LAB-Building-and-Securing-a-Network-with-a-DMZ\DMZ_PROJECT.pka -...
File Edit Options View Tools Extensions Window Help
Activity Results
Time Elapsed: 16:07:06
Congratulations Guest! You completed the activity.
Overall Feedback
Assessment Items
Connectivity Tests
Expand/Collapse All
Show Incorrect Items
Assessment Items
Status
Points
Component(s)
Feedback
Network
Correct
0
Other
Score : 9/9
Item Count : 6/9
Component
Items/Total
Score
Connectivity
Connectivity Tests
6/6
9/9
Close



¡Felicidades por llegar a este punto! ¡Ahora, a poner a prueba tus habilidades!