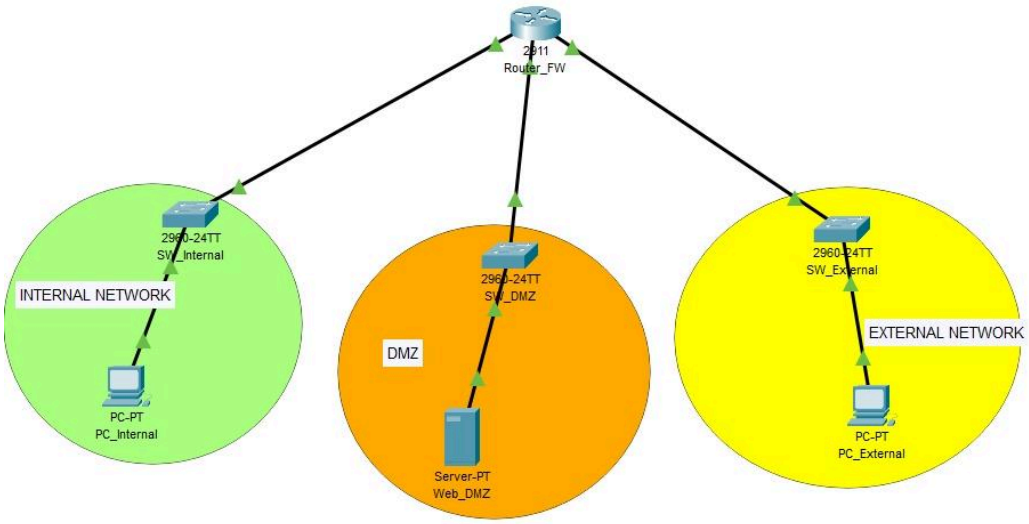
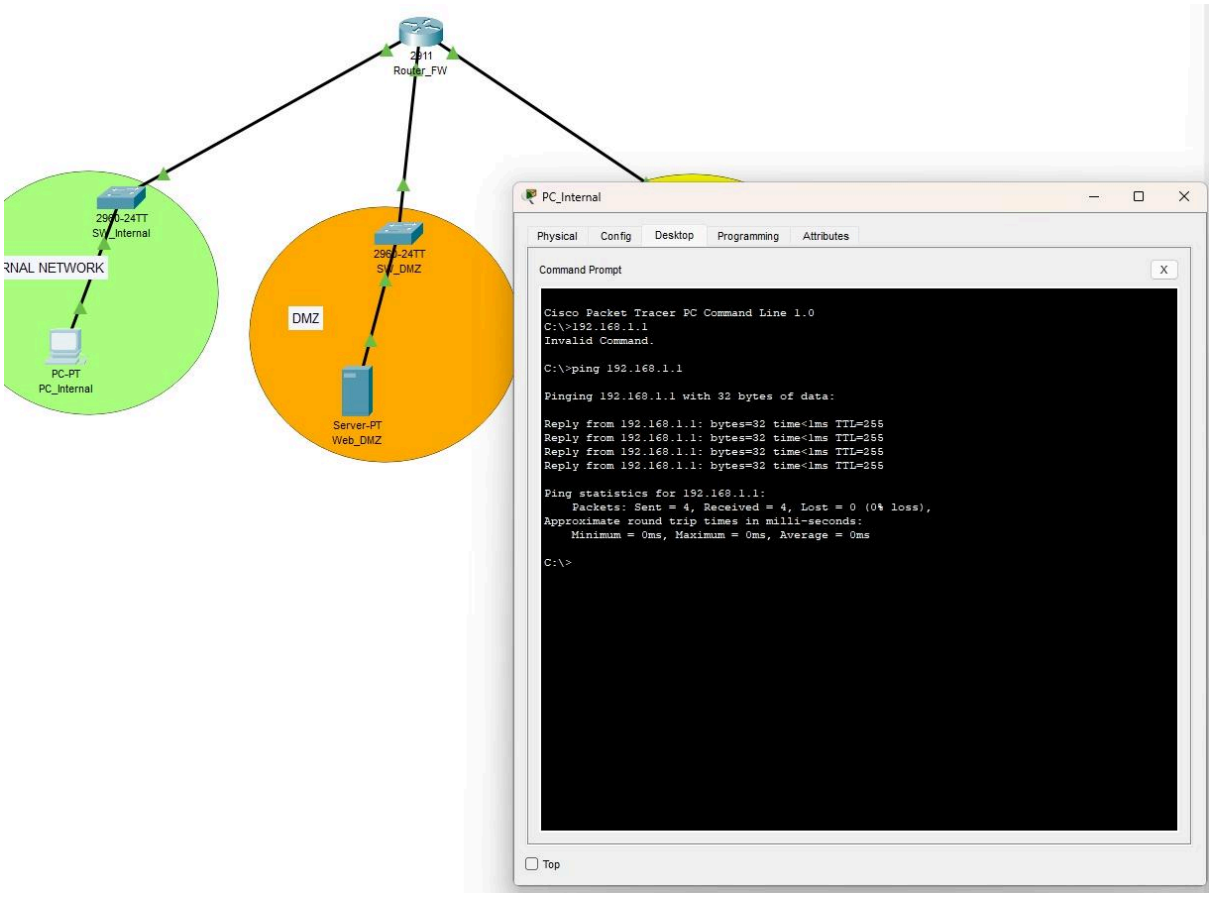
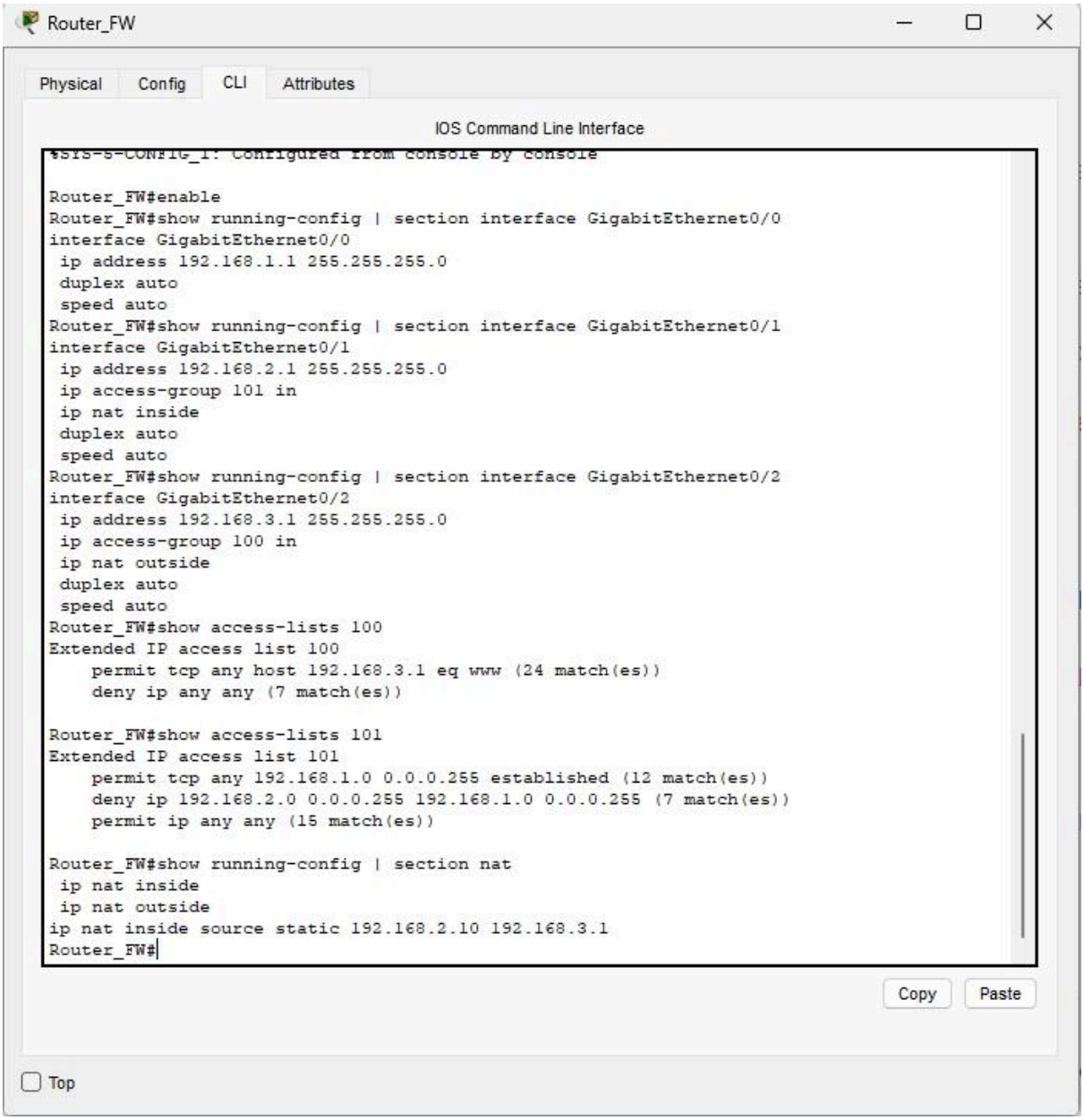
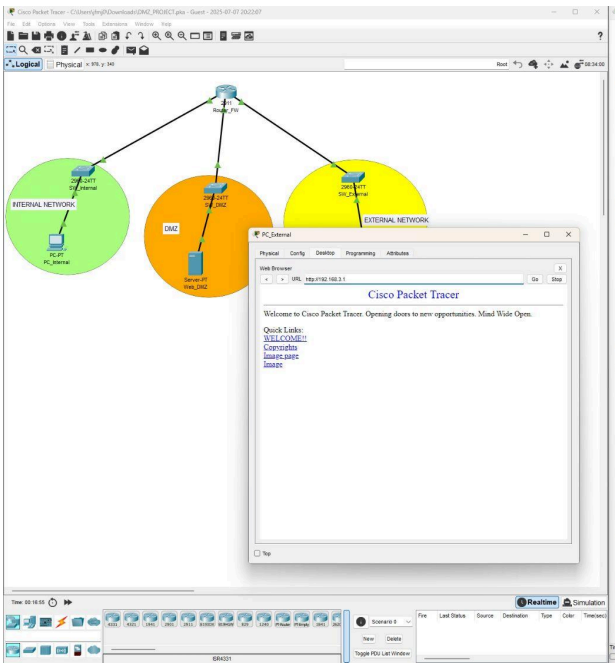

2811
Router_FW
2960-24TT
SW_Internal
INTERNAL NETWORK
PC-PT
PC_Internal
2960-24TT
SW_DMZ
DMZ
Server-PT
Web_DMZ
2960-24TT
SW_External
EXTERNAL NETWORK
PC-PT
PC_External


2811
Router_FW
2960-24TT
SW_Internal
RNAL NETWORK
PC-PT
PC_Internal
2960-24TT
SW_DMZ
DMZ
Server-PT
Web_DMZ
PC_Internal
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>192.168.1.1
Invalid Command.
C:\>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Ping statistics for 192.168.1.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
Top


Router_FW
Physical
Config
CLI
Attributes
IOS Command Line Interface
%SYS-5-CONFIG_I: Configured from console by console
Router_FW#enable
Router_FW#show running-config | section interface GigabitEthernet0/0
interface GigabitEthernet0/0
ip address 192.168.1.1 255.255.255.0
duplex auto
speed auto
Router_FW#show running-config | section interface GigabitEthernet0/1
interface GigabitEthernet0/1
ip address 192.168.2.1 255.255.255.0
ip access-group 101 in
ip nat inside
duplex auto
speed auto
Router_FW#show running-config | section interface GigabitEthernet0/2
interface GigabitEthernet0/2
ip address 192.168.3.1 255.255.255.0
ip access-group 100 in
ip nat outside
duplex auto
speed auto
Router_FW#show access-lists 100
Extended IP access list 100
permit tcp any host 192.168.3.1 eq www (24 match(es))
deny ip any any (7 match(es))
Router_FW#show access-lists 101
Extended IP access list 101
permit tcp any 192.168.1.0 0.0.0.255 established (12 match(es))
deny ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255 (7 match(es))
permit ip any any (15 match(es))
Router_FW#show running-config | section nat
ip nat inside
ip nat outside
ip nat inside source static 192.168.2.10 192.168.3.1
Router_FW#
Copy
Paste
Top



- 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.

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.*

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).
- **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`.

Paso 8: Verificación Final de Seguridad y Funcionalidad

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

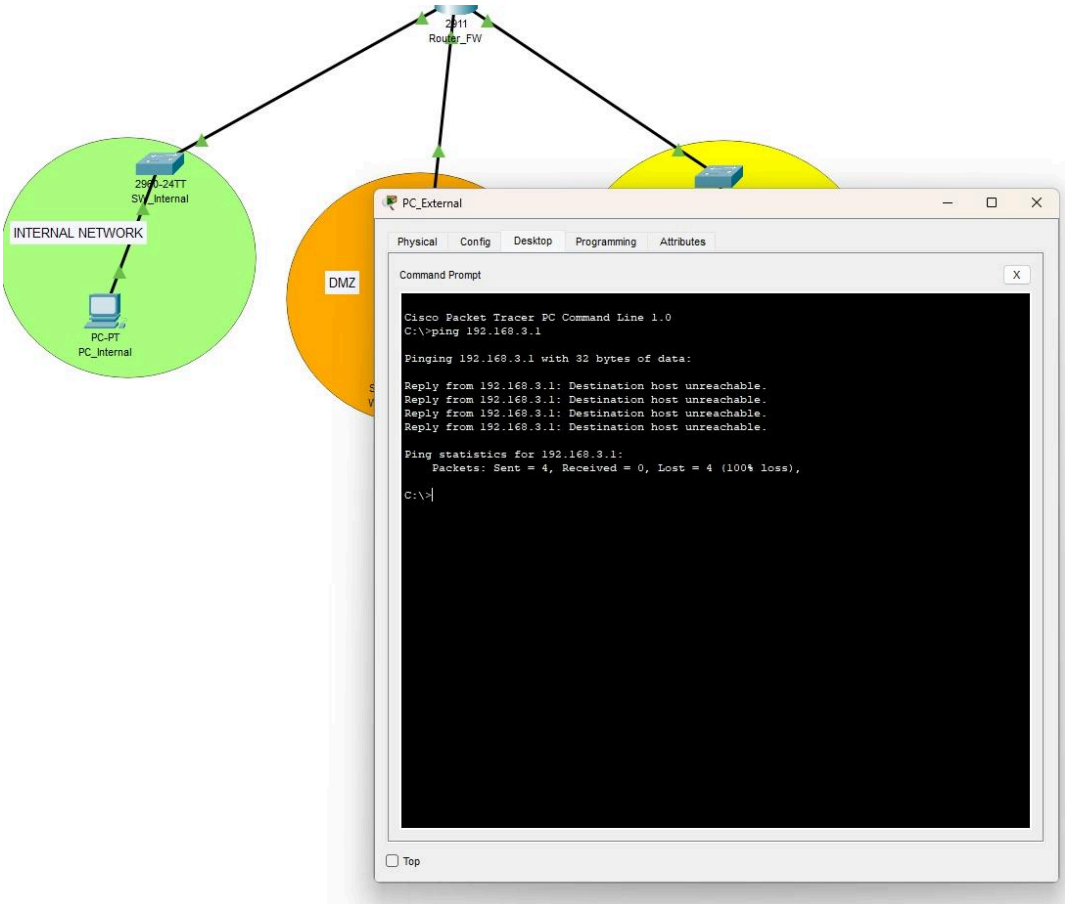
- **Desde `PC_External` (Web Browser):**
  - Accede al servidor web DMZ (`192.168.3.1`). *Resultado esperado: La página web debe **cargar**.*
- **Desde `PC_External` (Command Prompt):**
  - `ping 192.168.3.1` (Ping a la interfaz WAN/IP pública del servidor). *Resultado esperado: **Request timed out** (Debe FALLAR si tu ACL externa bloquea ICMP).*
- **Desde `PC_Internal` (Web Browser):**
  - Accede al servidor web DMZ (`192.168.2.10`). *Resultado esperado: La página web debe **cargar**.*
- **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!).*

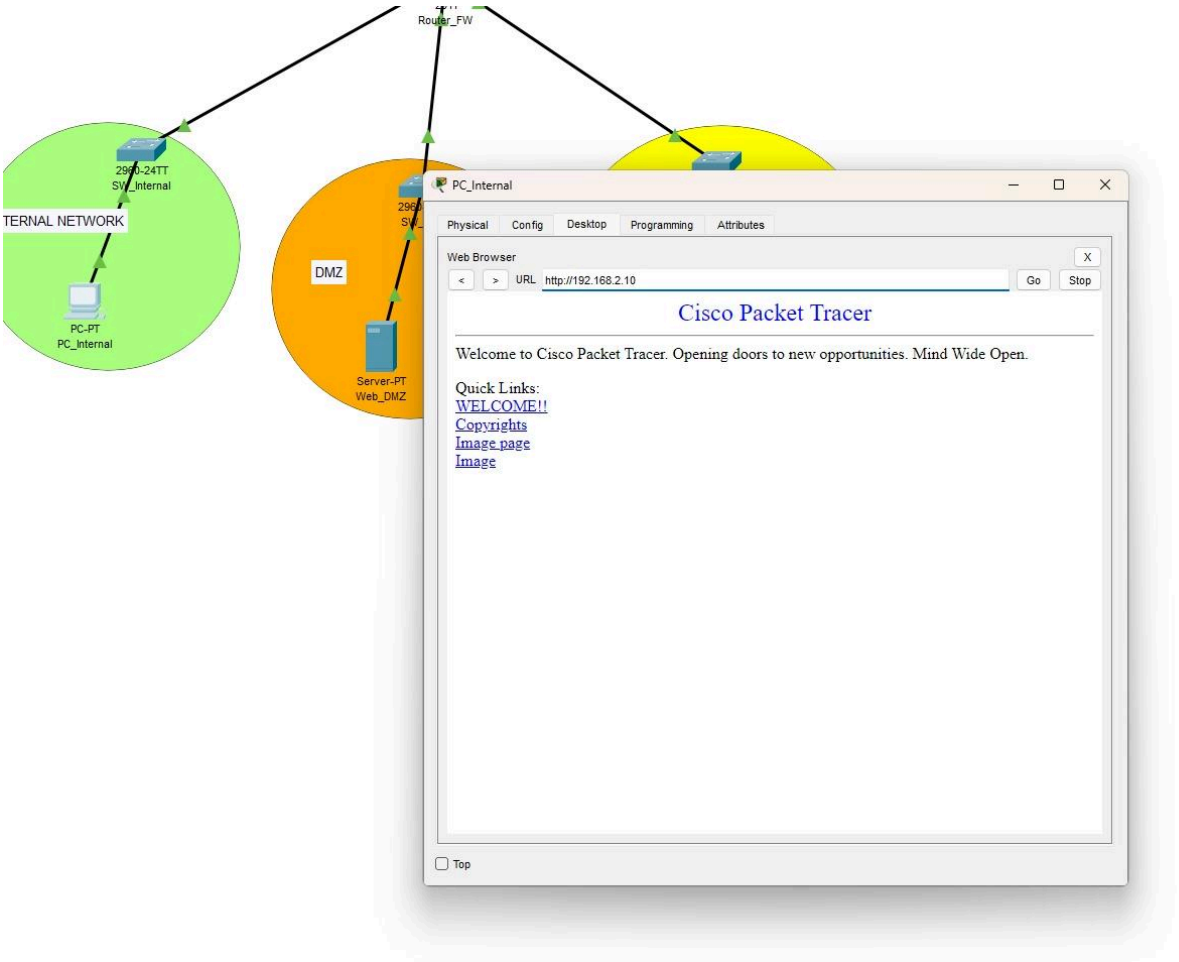
Auto-Evaluación de tu Progreso:

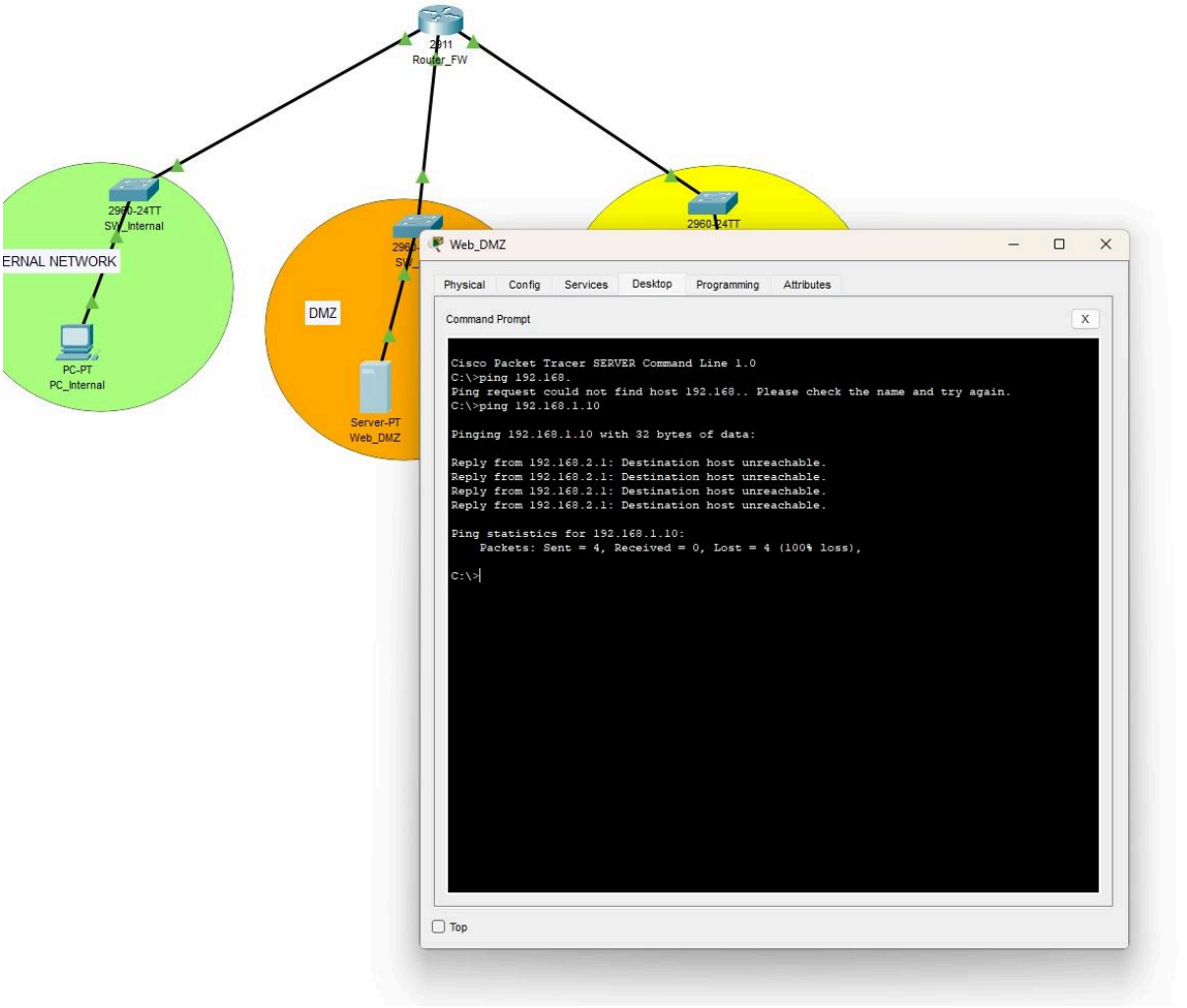
Una vez que hayas completado todos los pasos y las pruebas manuales te den los resultados esperados:

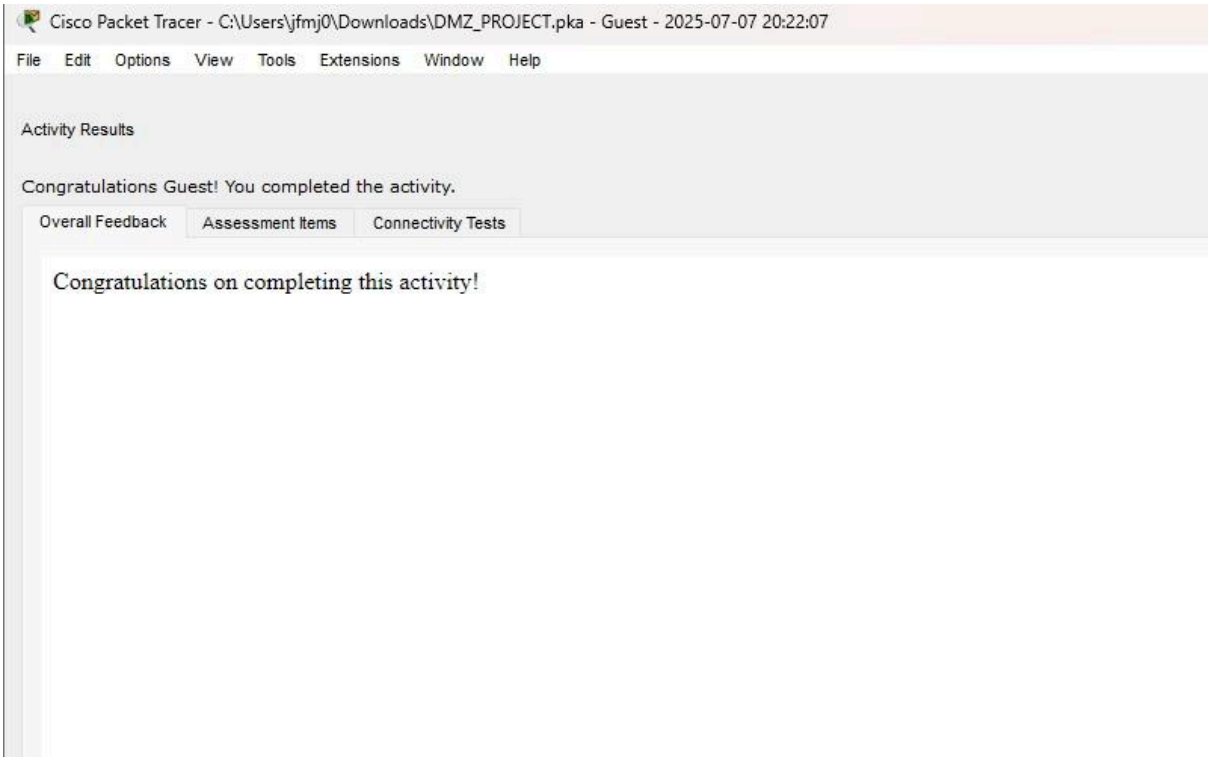
1. Haz clic en el botón `Check Results` en la ventana del laboratorio.
2. El sistema de evaluación te mostrará tu puntuación y si has logrado todos los objetivos de configuración y seguridad.

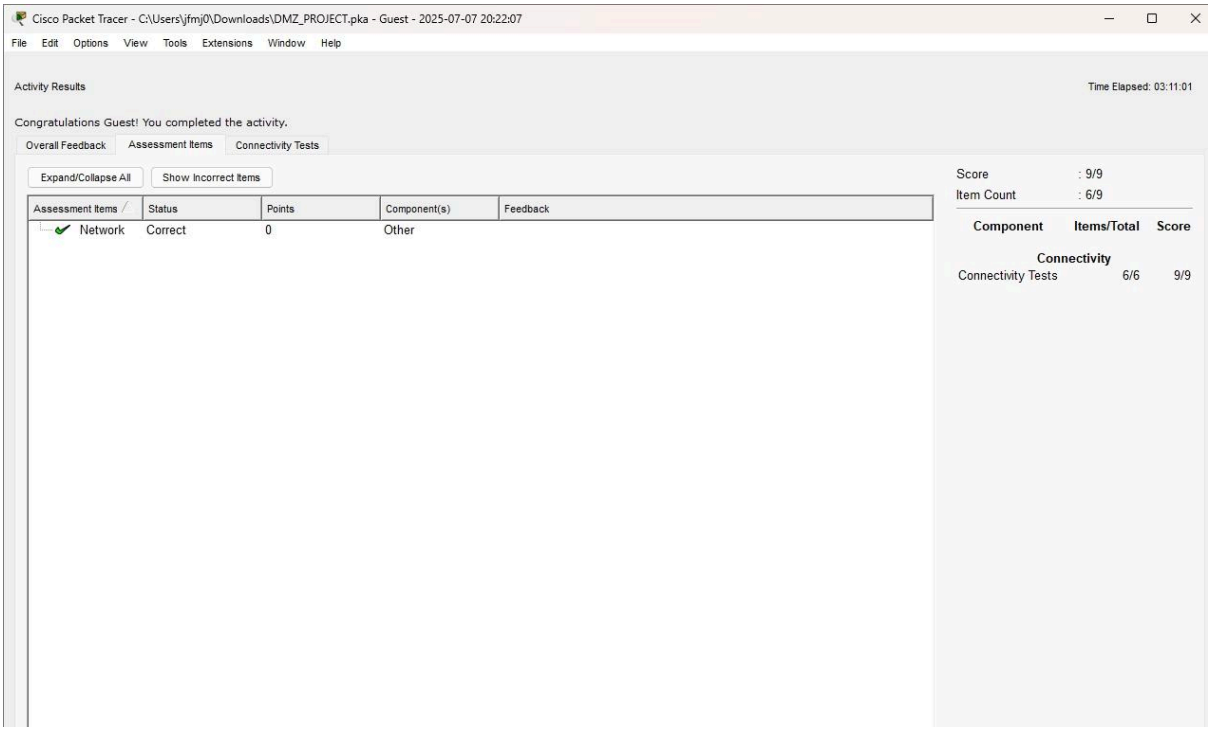
¡Felicidades por llegar a este punto! ¡Ahora, a poner a prueba tus habilidades!

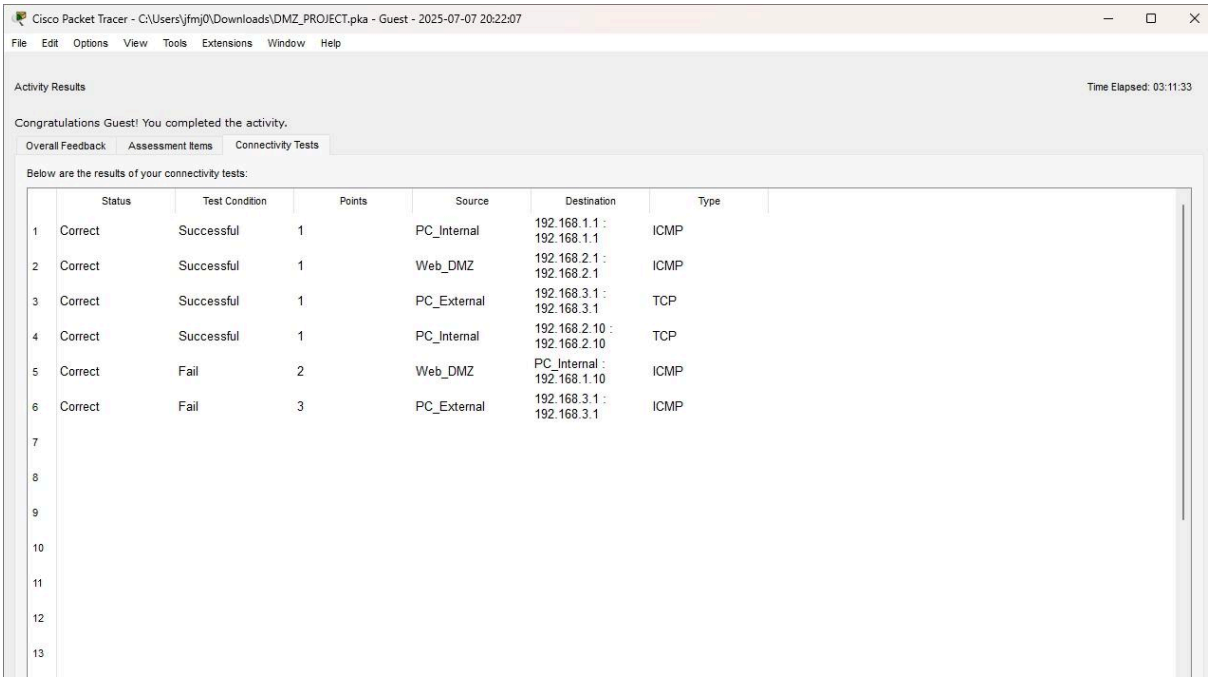



Router_FW
2960-24TT
SW_Internal
TERNAL NETWORK
PC-PT
PC_Internal
DMZ
Server-PT
Web_DMZ
PC_Internal
Physical
Config
Desktop
Programming
Attributes
Web Browser
X
URL
http://192.168.2.10
Go
Stop
Cisco Packet Tracer
Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.
Quick Links:
WELCOME!!
Copyrights
Image page
Image
Top


2911
Router_FW
2960-24TT
SW_Internal
ERNAL NETWORK
PC-PT
PC_Internal
DMZ
Server-PT
Web_DMZ
2960-24TT
Web_DMZ
Physical
Config
Services
Desktop
Programming
Attributes
Command Prompt
X
Cisco Packet Tracer SERVER Command Line 1.0
C:\>ping 192.168.
Ping request could not find host 192.168.. Please check the name and try again.
C:\>ping 192.168.1.10
Pinging 192.168.1.10 with 32 bytes of data:
Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.
Ping statistics for 192.168.1.10:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
Top


Cisco Packet Tracer - C:\Users\jfmj0\Downloads\DMZ_PROJECT.pka - Guest - 2025-07-07 20:22:07
File
Edit
Options
View
Tools
Extensions
Window
Help
Activity Results
Congratulations Guest! You completed the activity.
Overall Feedback
Assessment Items
Connectivity Tests
Congratulations on completing this activity!


Cisco Packet Tracer - C:\Users\jfmj0\Downloads\DMZ_PROJECT.pka - Guest - 2025-07-07 20:22:07
File Edit Options View Tools Extensions Window Help
Activity Results
Time Elapsed: 03:11:01
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


Cisco Packet Tracer - C:\Users\jfmj0\Downloads\DMZ_PROJECT.pka - Guest - 2025-07-07 20:22:07
File Edit Options View Tools Extensions Window Help
Activity Results
Time Elapsed: 03:11:33
Congratulations Guest! You completed the activity.
Overall Feedback
Assessment Items
Connectivity Tests
Below are the results of your connectivity tests:
Status
Test Condition
Points
Source
Destination
Type
1 Correct Successful 1 PC_Internal 192.168.1.1 : 192.168.1.1 ICMP
2 Correct Successful 1 Web_DMZ 192.168.2.1 : 192.168.2.1 ICMP
3 Correct Successful 1 PC_External 192.168.3.1 : 192.168.3.1 TCP
4 Correct Successful 1 PC_Internal 192.168.2.10 : 192.168.2.10 TCP
5 Correct Fail 2 Web_DMZ PC_Internal : 192.168.1.10 ICMP
6 Correct Fail 3 PC_External 192.168.3.1 : 192.168.3.1 ICMP
7
8
9
10
11
12
13