

Informe de configuración de DMZ con Cisco Packet Tracer

Bootcamp de ciberseguridad (4Geeks Academy)

1. Objetivo del laboratorio

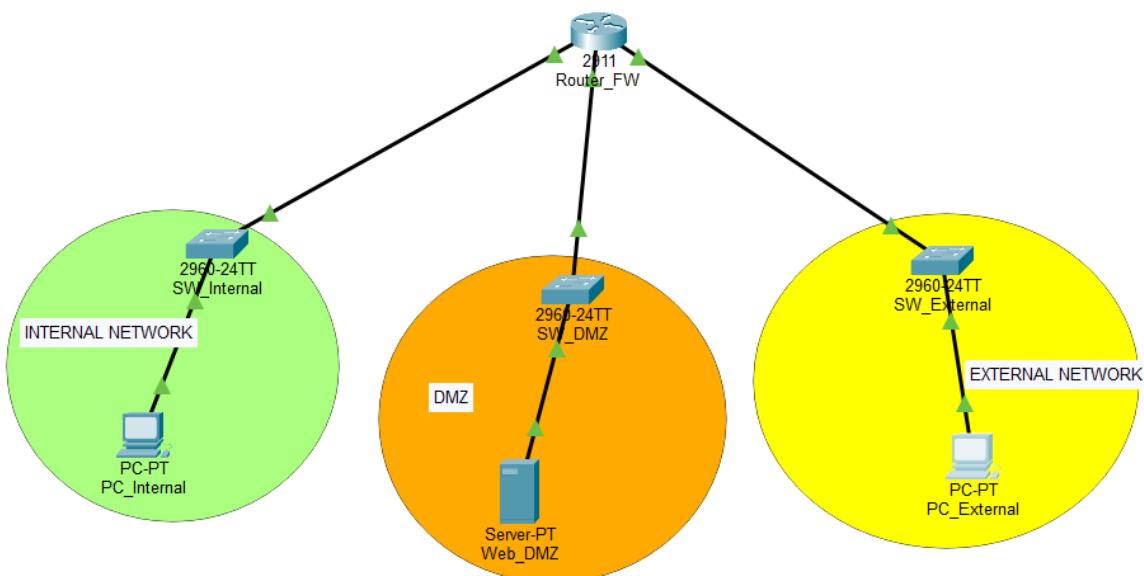
Configurar una DMZ segura y funcional en Cisco Packet Tracer utilizando un router Cisco ISR como firewall central. Se aplicó NAT estático para exponer un servidor web desde la DMZ a Internet, y ACLs extendidas para controlar estrictamente el tráfico: permitir solo HTTP desde red externa a DMZ, y bloquear completamente cualquier comunicación iniciada desde DMZ hacia LAN interna.

2. Topología implementada

Cantidad de redes: 3 subredes (/24 cada una).

Dispositivos usados: 1 Router Cisco 2911 (Router_FW), 3 Switches 2960 (Internal, DMZ, External), 1 PC_Internal, 1 Server-PT Web_DMZ, 1 PC_External.

- LAN Interna (verde, 192.168.1.0/24): Red privada segura (PC_Internal).
- DMZ (naranja, 192.168.2.0/24): Zona expuesta con servidor web público (Server_DMZ).
- Red Externa/Internet (amarillo, 192.168.3.0/24): Simulación de Internet (PC_External).

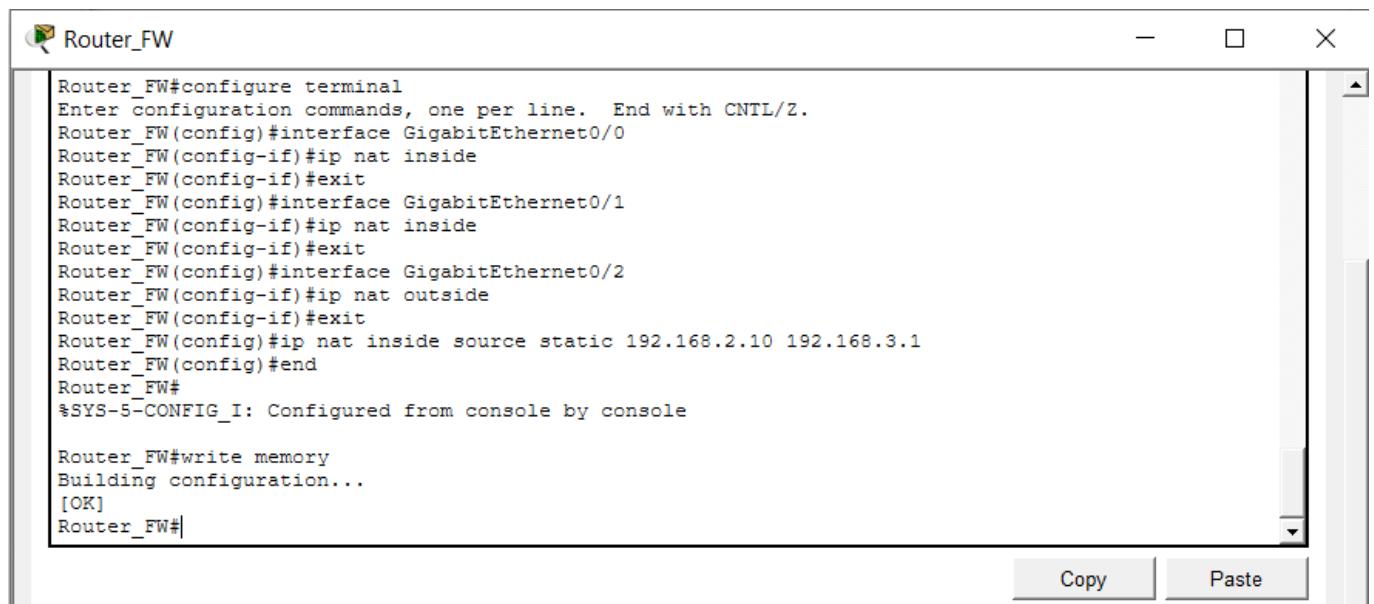


3. Plan de direccionamiento IP

Dispositivo	IP	Máscara	Gateway
PC_Internal	192.168.1.10	255.255.255.0	192.168.1.1
Server_DMZ	192.168.2.10	255.255.255.0	192.168.2.1
PC_External	192.168.3.10	255.255.255.0	192.168.3.1
Router_FW Gi0/0 (LAN)	192.168.1.1	255.255.255.0	--
Router_FW Gi0/1 (DMZ)	192.168.2.1	255.255.255.0	--
Router_FW Gi0/2 (Ext)	192.168.3.1	255.255.255.0	--

4. Configuración aplicada (resumen)

Interfaces:



Router_FW#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router_FW(config)#interface GigabitEthernet0/0
Router_FW(config-if)#ip nat inside
Router_FW(config-if)#exit
Router_FW(config)#interface GigabitEthernet0/1
Router_FW(config-if)#ip nat inside
Router_FW(config-if)#exit
Router_FW(config)#interface GigabitEthernet0/2
Router_FW(config-if)#ip nat outside
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#
%SYS-5-CONFIG_I: Configured from console by console

Router_FW#write memory
Building configuration...
[OK]
Router_FW#

Copy Paste

interface GigabitEthernet0/0
ip address 192.168.1.1 255.255.255.0
ip nat inside

NAT Estático:

interface GigabitEthernet0/1
ip address 192.168.2.1 255.255.255.0
ip nat inside
ip access-group DMZ_INBOUND in

ip nat inside source static 192.168.2.10 192.168.3.1

Mapeo 1:1 del servidor DMZ (privado) a IP pública del router.

interface GigabitEthernet0/2
ip address 192.168.3.1 255.255.255.0
ip nat outside
ip access-group WAN_INBOUND in

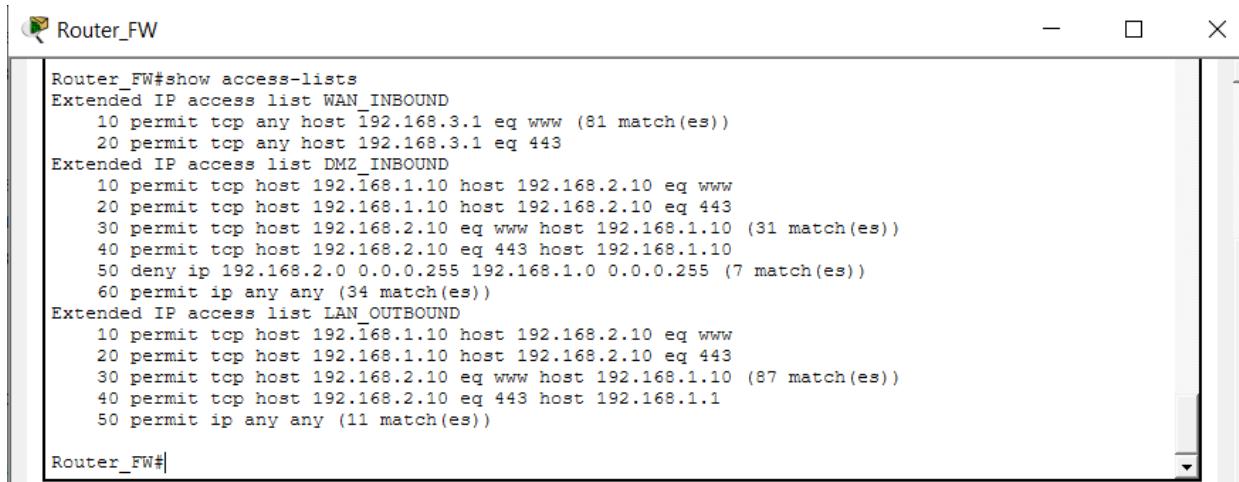
ACLs de Seguridad:

```
ip access-list extended WAN_INBOUND
permit tcp any host 192.168.3.1 eq www
permit tcp any host 192.168.3.1 eq 443
```

(Aplicada inbound Gi0/2: solo HTTP/HTTPS desde Internet a servidor publicado).

```
ip access-list extended DMZ_INBOUND
permit tcp host 192.168.2.10 eq www host 192.168.1.10
permit tcp host 192.168.2.10 eq 443 host 192.168.1.10
deny ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
permit ip any any
```

(Aplicada inbound Gi0/1: permite return TCP web LAN ↔ DMZ, bloquea TODO DMZ → LAN).



```
Router_FW#show access-lists
Extended IP access list WAN_INBOUND
  10 permit tcp any host 192.168.3.1 eq www (81 match(es))
  20 permit tcp any host 192.168.3.1 eq 443
Extended IP access list DMZ_INBOUND
  10 permit tcp host 192.168.2.10 host 192.168.1.10 eq www
  20 permit tcp host 192.168.2.10 host 192.168.1.10 eq 443
  30 permit tcp host 192.168.2.10 eq www host 192.168.1.10 (31 match(es))
  40 permit tcp host 192.168.2.10 eq 443 host 192.168.1.10
  50 deny ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255 (7 match(es))
  60 permit ip any any (34 match(es))
Extended IP access list LAN_OUTBOUND
  10 permit tcp host 192.168.1.10 host 192.168.2.10 eq www
  20 permit tcp host 192.168.1.10 host 192.168.2.10 eq 443
  30 permit tcp host 192.168.2.10 eq www host 192.168.1.10 (87 match(es))
  40 permit tcp host 192.168.2.10 eq 443 host 192.168.1.1
  50 permit ip any any (11 match(es))

Router_FW#
```

5. Verificaciones realizadas

Prueba	Resultado esperado	Resultado real
PC_Internal ping 192.168.1.1	Replies	<input checked="" type="checkbox"/> Replies
Server_DMZ ping 192.168.2.1	Replies	<input checked="" type="checkbox"/> Replies
PC_External ping 192.168.3.1	Replies	<input checked="" type="checkbox"/> Replies
PC_External web → 192.168.3.1	Página web carga	<input checked="" type="checkbox"/> Carga
PC_Internal web → 192.168.2.10	Página web carga	<input checked="" type="checkbox"/> Carga
PC_External ping 192.168.3.1	Timeout (ACL)	<input checked="" type="checkbox"/> Timeout
Server_DMZ ping 192.168.1.10	Timeout (ACL)	<input checked="" type="checkbox"/> Timeout

6. Conclusiones y recomendaciones

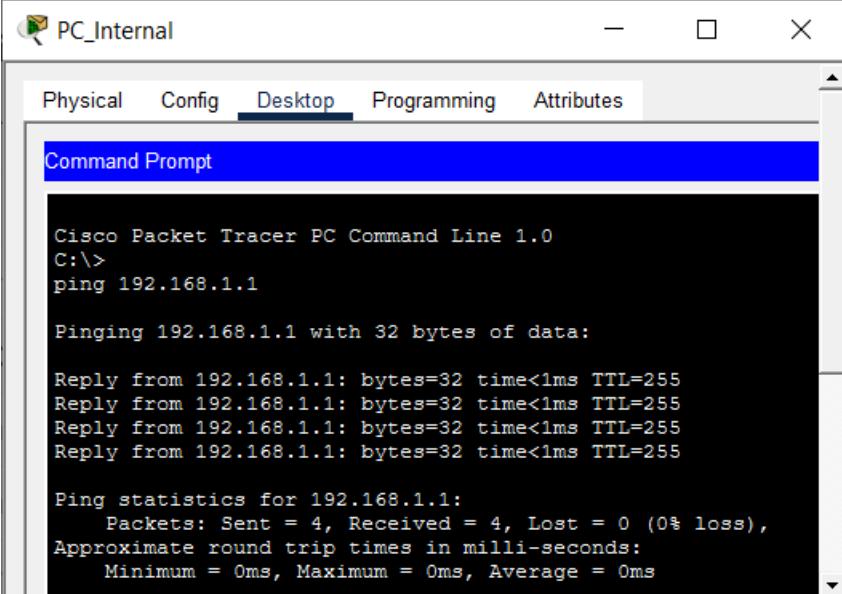
En esta práctica aprendimos que el orden de las ACLs es crítico: el deny DMZ → LAN debe ir antes de permits genéricos para bloquear ICMP. También, en Packet Tracer se necesita permitir explícitamente el tráfico de respuesta TCP desde DMZ a LAN (SYN-ACK), porque no maneja conexiones stateful automáticamente.

Este ejercicio reforzó mi comprensión de DMZ como "zona de sacrificio" en Blue Team: expone servicios públicos sin comprometer LAN interna.

7. Capturas de evidencia

Verificaciones realizadas:

- PC_Internal ping 192.168.1.1 (Replies)



The screenshot shows a Windows-style application window titled "PC_Internal". The window has tabs at the top: Physical, Config, Desktop (which is selected), Programming, and Attributes. Below the tabs is a "Command Prompt" window with a blue header bar. The command line shows the user entering "ping 192.168.1.1". The output of the ping command is displayed below, showing four successful replies from the target IP address. The ping statistics at the end indicate 0% loss and 0ms round trip times.

```
Cisco Packet Tracer PC Command Line 1.0
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

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
```

- Server_DMZ ping 192.168.2.1 (Replies)

Web_DMZ

Physical Config Services Desktop Programming Attributes

Command Prompt

```
Cisco Packet Tracer SERVER Command Line 1.0
C:\>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time<1ms TTL=255
Reply from 192.168.2.1: bytes=32 time=1ms TTL=255
Reply from 192.168.2.1: bytes=32 time<1ms TTL=255
Reply from 192.168.2.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

- **PC_External ping 192.168.3.1 (Replies)**

PC_External

Physical Config Desktop Programming Attributes

Command Prompt

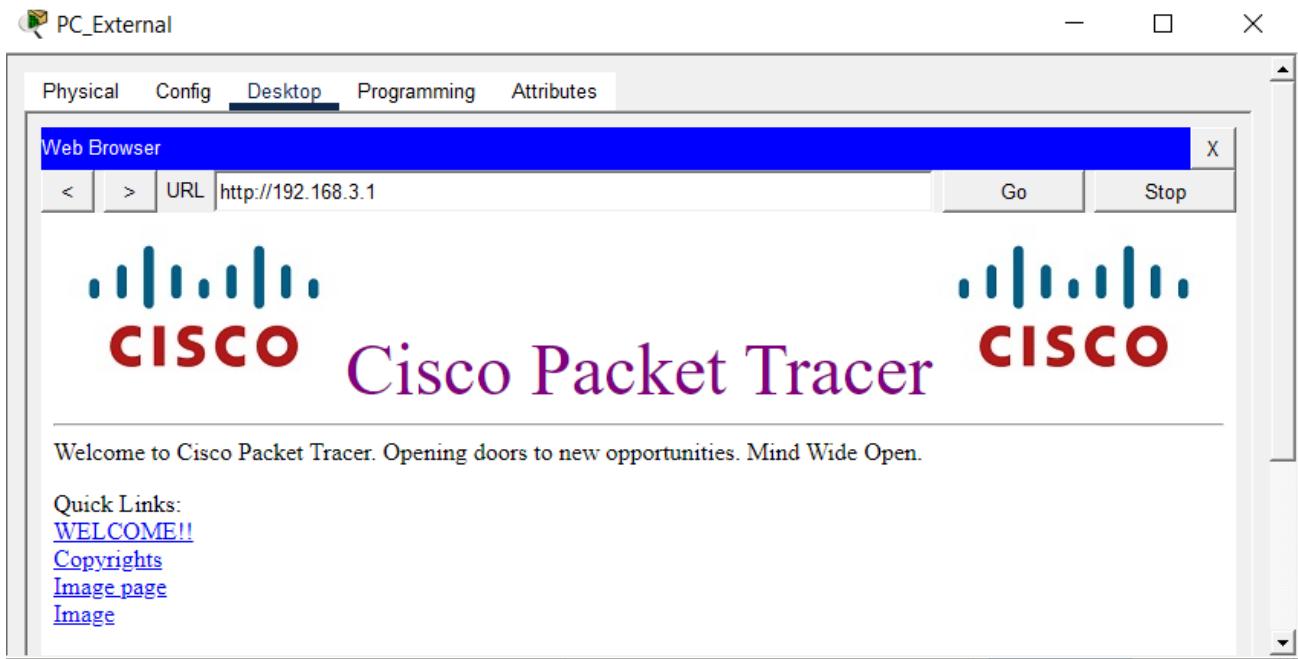
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.3.1

Pinging 192.168.3.1 with 32 bytes of data:

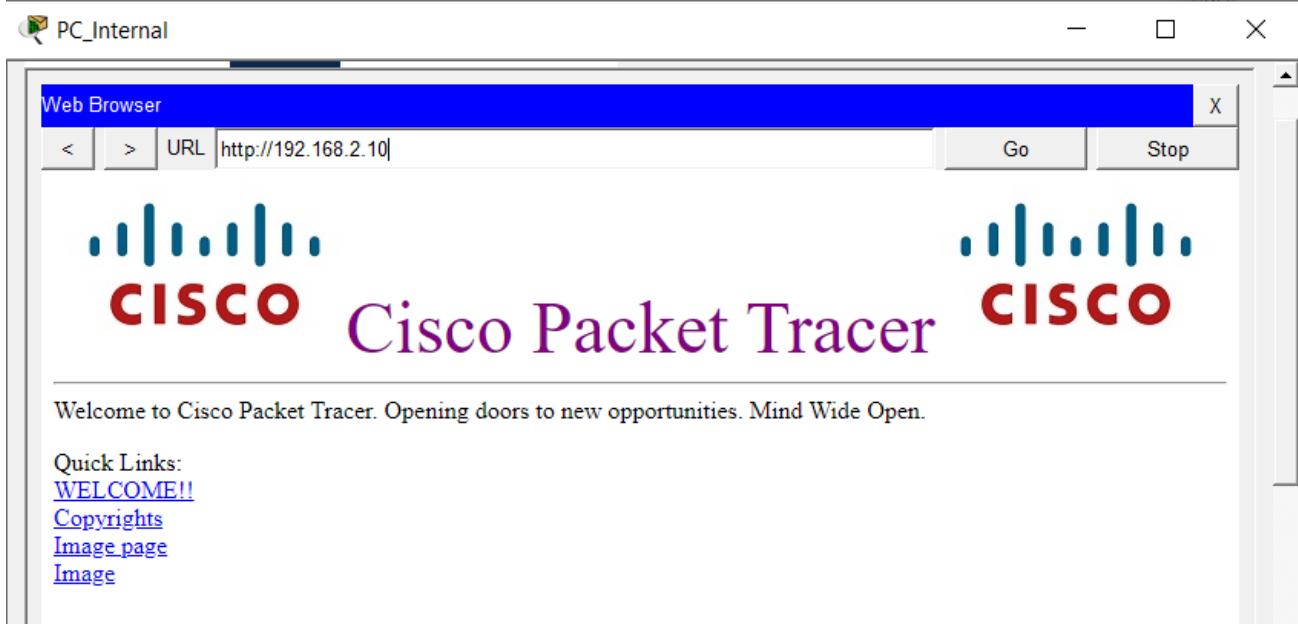
Reply from 192.168.3.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.3.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

- **PC_External web → 192.168.3.1 (Página web carga)**



- PC_Internal web → 192.168.2.10 (Página web carga)



- PC_Exernal ping 192.168.3.1 (Timeout (ACL))

PC_External

```
C:\>ping 192.168.3.1

Pinging 192.168.3.1 with 32 bytes of data:

Reply from 192.168.3.1: Destination host unreachable.

Ping statistics for 192.168.3.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
```

- **Server_DMZ ping 192.168.1.10 (Timeout (ACL))**

Web_DMZ

```
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.

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
```

- **Confirmar que la NAT funcional**

Router_FW

```
Router_FW>enable
Router_FW#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
--- 192.168.3.1        192.168.2.10     ---              ---
Router_FW#
```

- **Resultado de Check Results**

File Edit Options View Tools Extensions Window Help

Activity Results Time Elapsed: 09:21:47

Congratulations Guest! You completed the activity.

Overall Feedback Assessment Items Connectivity Tests

Congratulations on completing this activity!

File Edit Options View Tools Extensions Window Help

Activity Results Time Elapsed: 09:22:21

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 Tests	6/6	9/9

File Edit Options View Tools Extensions Window Help

Activity Results Time Elapsed: 09:23:10

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