# DMZ Firewall ACL Configuration and Access Control Report

## Project Overview

This project involved designing and configuring a Demilitarized Zone (DMZ) architecture in Cisco Packet Tracer, and implementing a Firewall Access Control List (ACL) to properly regulate traffic between the LAN and the DMZ.

The goal was simple:

- Allow secure HTTPS traffic from the LAN to the DMZ web server
- Block insecure HTTP traffic
- Allow basic diagnostic traffic (ICMP)
- Ensure the DMZ server is reachable only through approved services
- Deny all other traffic by default

This project aligns with real-world firewall best practices used in defensive security.

## Network Topology Description

The topology consists of three security zones:

1. WAN (Internet Side)
2. DMZ (Public Server Zone)
3. LAN (Internal Private Network)

Two routers serve as firewalls separating these zones:

Firewall-1 (WAN to DMZ)

- Controls access between external networks and the public server
- Protects the DMZ from unsecured WAN access

Firewall-2 (DMZ  LAN)

- Controls access from internal devices to the DMZ
- Prevents direct LAN exposure to possible web threats

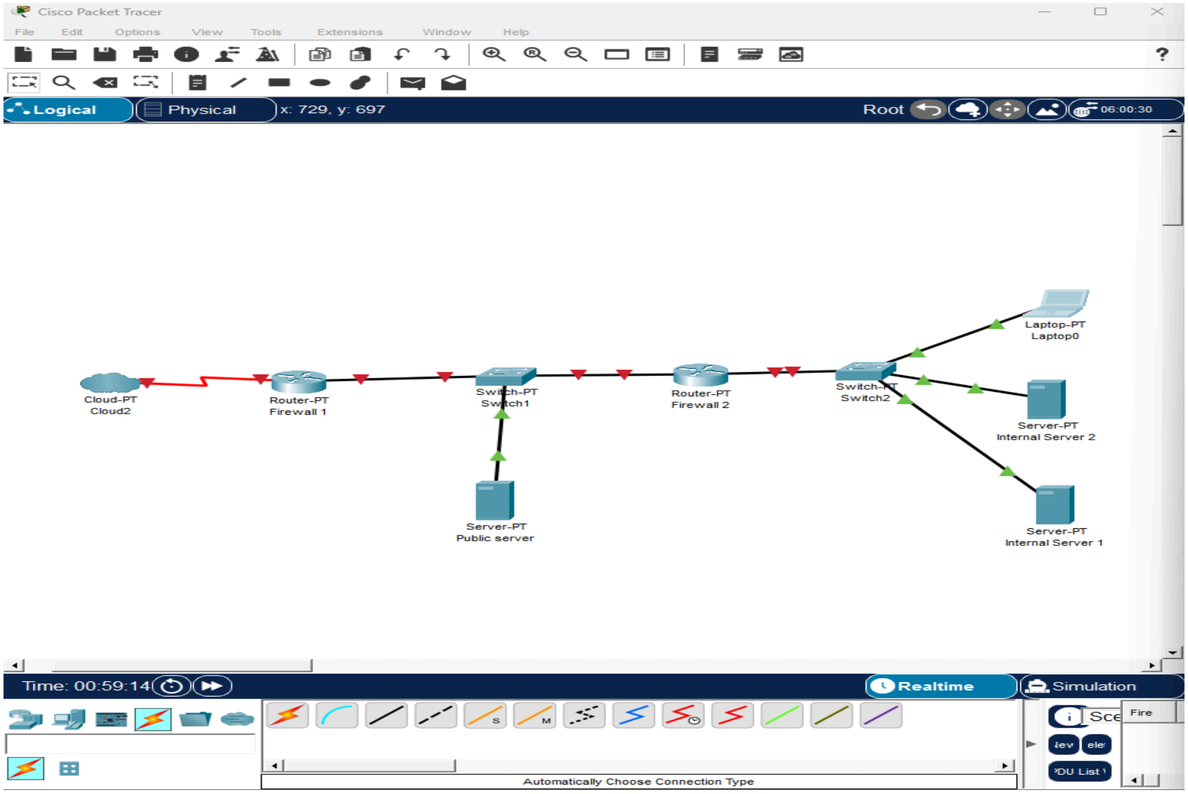
Public server is placed in the DMZ, providing a secure buffer between internal LAN and external networks.

**Network Configuration and Tools Used**

This network was implemented using the following devices:

- PT Cloud (Which acts as the WAN/Internet, and is connected to the Firewall-1)
- PT Router (used as Firewall-1, connected to the cloud/WAN and DMZ)
- PT Switch(labelled switch-1, which is also the DMZ switch connected to the public server)
- PT Server(public server inside the DMZ)
- PT Router(used as Firewall-2, connected between DMZ and LAN)
- Switch 2960 (labelled switch-1, which is also the LAN switch connected to internal devices)
- Laptop PC + Two Server PTs (internal LAN devices connected to the LAN switch)

Each device was connected using copper straight-through cables, and IP addresses were manually assigned to match the DMZ and LAN subnets.



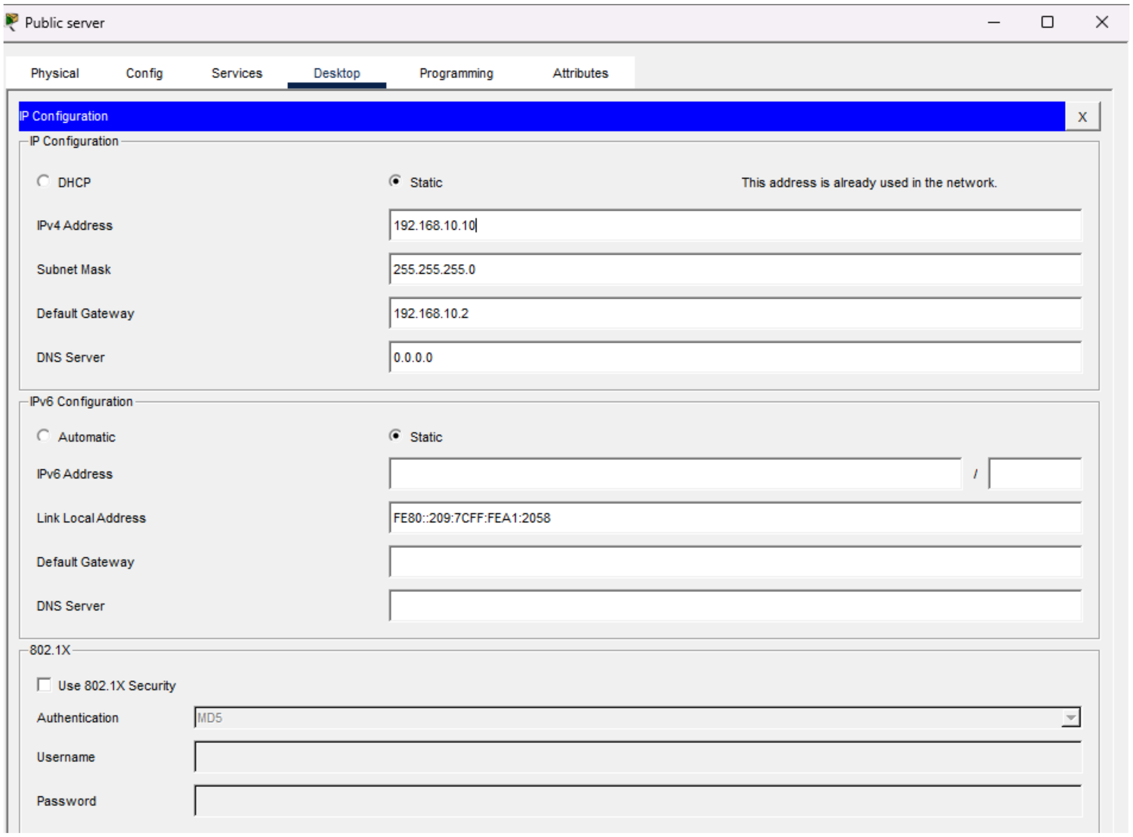
**IP Addressing**

Each device was assigned a static IP address according to the DMZ and LAN subnet plan.

| **Zone** | **Device** | **Interface** | **IP Address** | **Purpose** |
|---|---|---|---|---|
| WAN | Cloud | NIC | NIC | WAN/Internet |
| WAN | Firewall-1 | Fa1/0 | 203.1.133.1 | WAN |
| DMZ | Firewall-1 | Fa0/0 | 192.168.10.2 | Gateway to Public Server |
| DMZ | Public Server | NIC | 192.168.10.10 | HTTPS Server |
| DMZ to LAN Link | Firewall-2 | Fa0/0 | 192.168.10.1 | DMZ Gateway |
| LAN | Firewall-2 | Fa1/0 | 192.168.30.1 | Internal Gateway |
| LAN | Laptop | NIC | 192.168.30.10 | Client Machine |
| LAN | Internal server-1 | NIC | 192.168.30.30 | Client Machine |
| LAN | Internal server-2 | NIC | 192.168.30.20 | Client Machine |

- Subnet Mask (all interfaces): 255.255.255.0
- Public Server Gateway: 192.168.10.2
- LAN Device Gateway: 192.168.30.1

The screenshots below show the manual configuration of the firewall interfaces, the public server, and the LAN devices.



IP Configuration

IP Configuration

○ DHCP ● Static This address is already used in the network.

IPv4 Address: 192.168.10.10

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.10.2

DNS Server: 0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::209:7CFF:FEA1:2058

Default Gateway:

DNS Server:

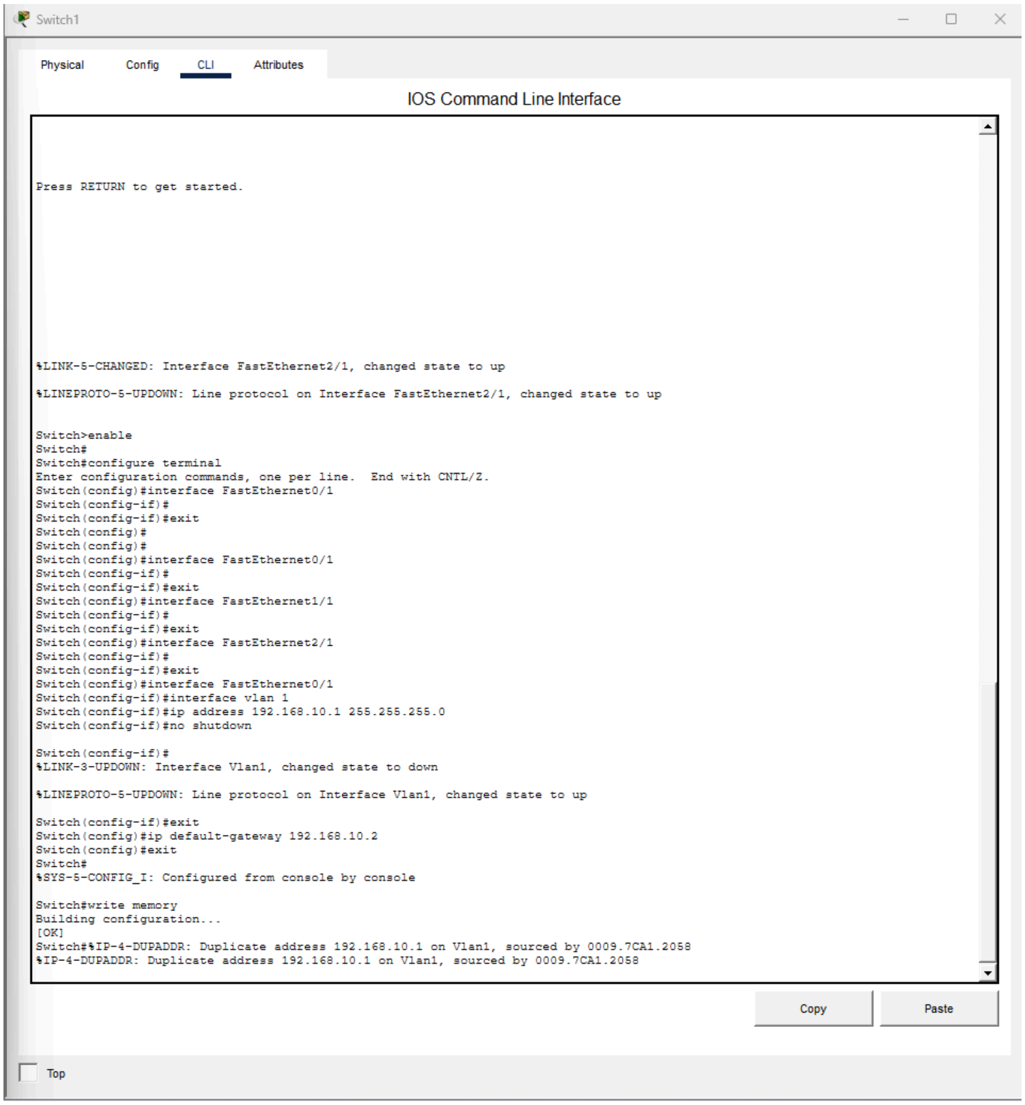
802.1X

□ Use 802.1X Security

Authentication: MD5

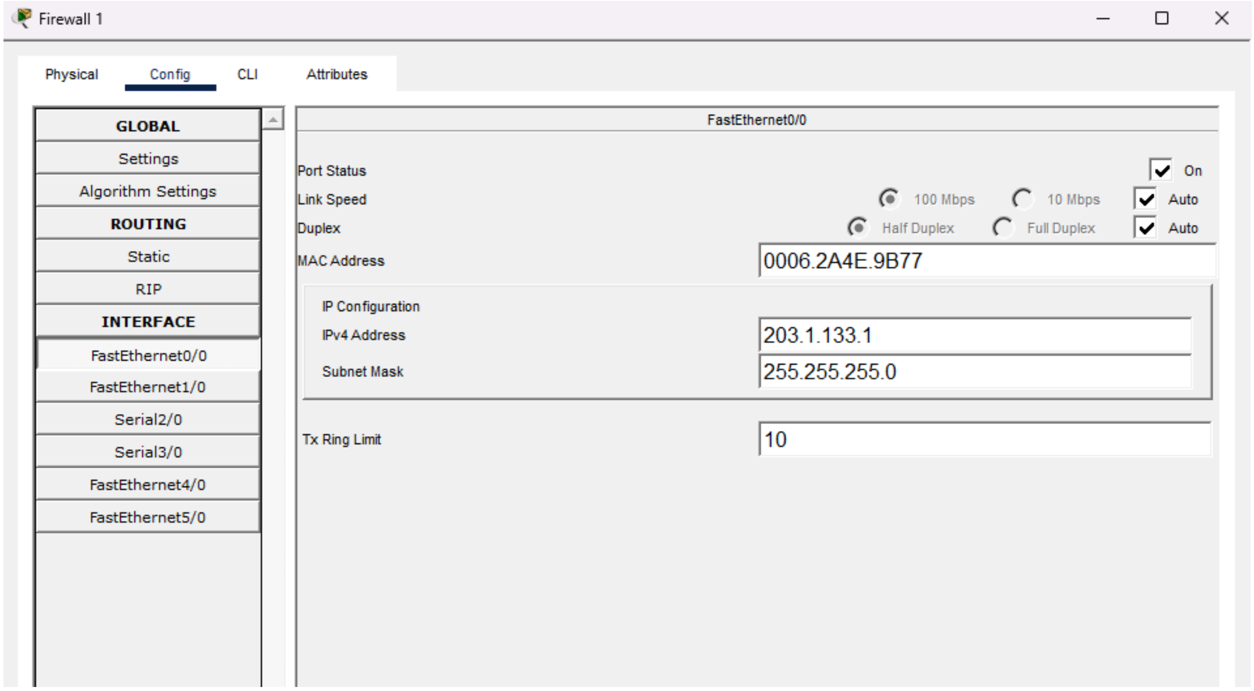
Username:

Password:



IOS Command Line Interface

```
Press RETURN to get started.







%LINK-5-CHANGED: Interface FastEthernet2/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet2/1, changed state to up


Switch>enable
Switch#
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface FastEthernet0/1
Switch(config-if)#
Switch(config-if)#exit
Switch(config)#
Switch(config)#
Switch(config)#interface FastEthernet0/1
Switch(config-if)#
Switch(config-if)#exit
Switch(config)#interface FastEthernet1/1
Switch(config-if)#
Switch(config-if)#exit
Switch(config)#interface FastEthernet2/1
Switch(config-if)#
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/1
Switch(config-if)#interface vlan 1
Switch(config-if)#ip address 192.168.10.1 255.255.255.0
Switch(config-if)#no shutdown

Switch(config-if)#
%LINK-3-UPDOWN: Interface Vlan1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

Switch(config-if)#exit
Switch(config)#ip default-gateway 192.168.10.2
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#write memory
Building configuration...
[OK]
Switch#%IP-4-DUPADDR: Duplicate address 192.168.10.1 on Vlan1, sourced by 0009.7CA1.2058
%IP-4-DUPADDR: Duplicate address 192.168.10.1 on Vlan1, sourced by 0009.7CA1.2058
```



FastEthernet0/0

Port Status ☑ On

Link Speed ● 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ● Half Duplex ○ Full Duplex ☑ Auto

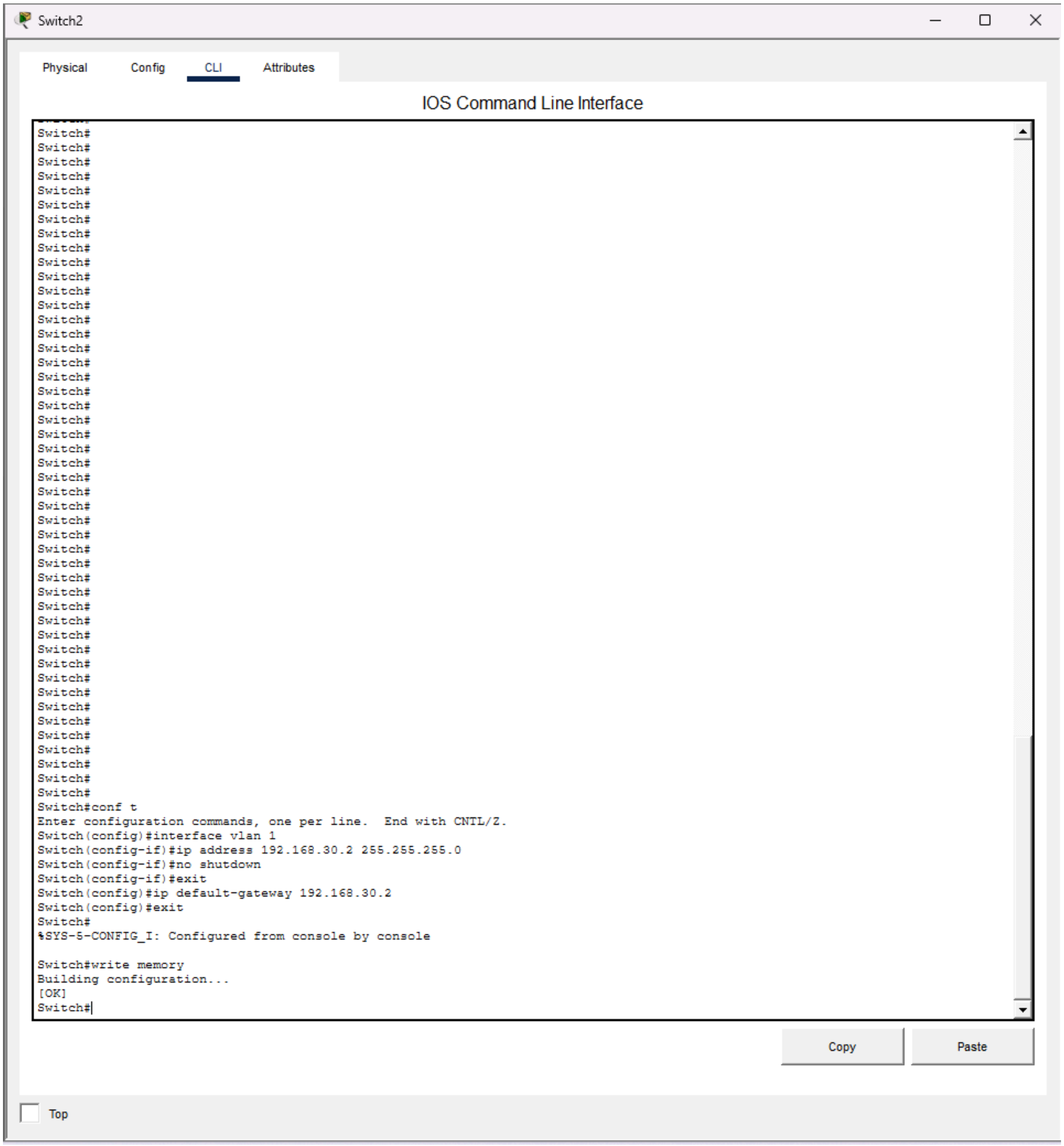
MAC Address 0006.2A4E.9B77

IP Configuration

IPv4 Address 203.1.133.1

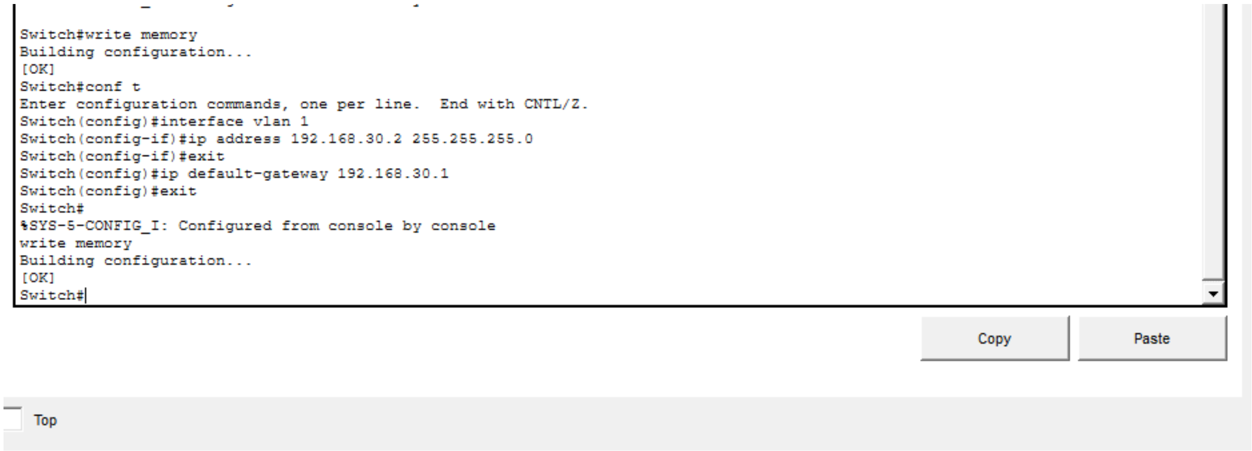
Subnet Mask 255.255.255.0

Tx Ring Limit 10

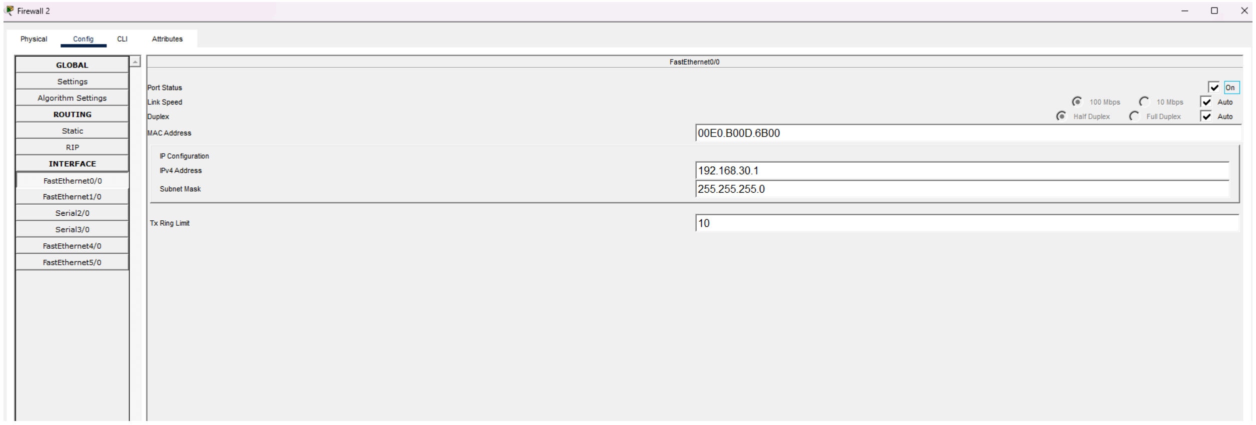


IOS Command Line Interface

```
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface vlan 1
Switch(config-if)#ip address 192.168.30.2 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#ip default-gateway 192.168.30.2
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#write memory
Building configuration...
[OK]
Switch#
```

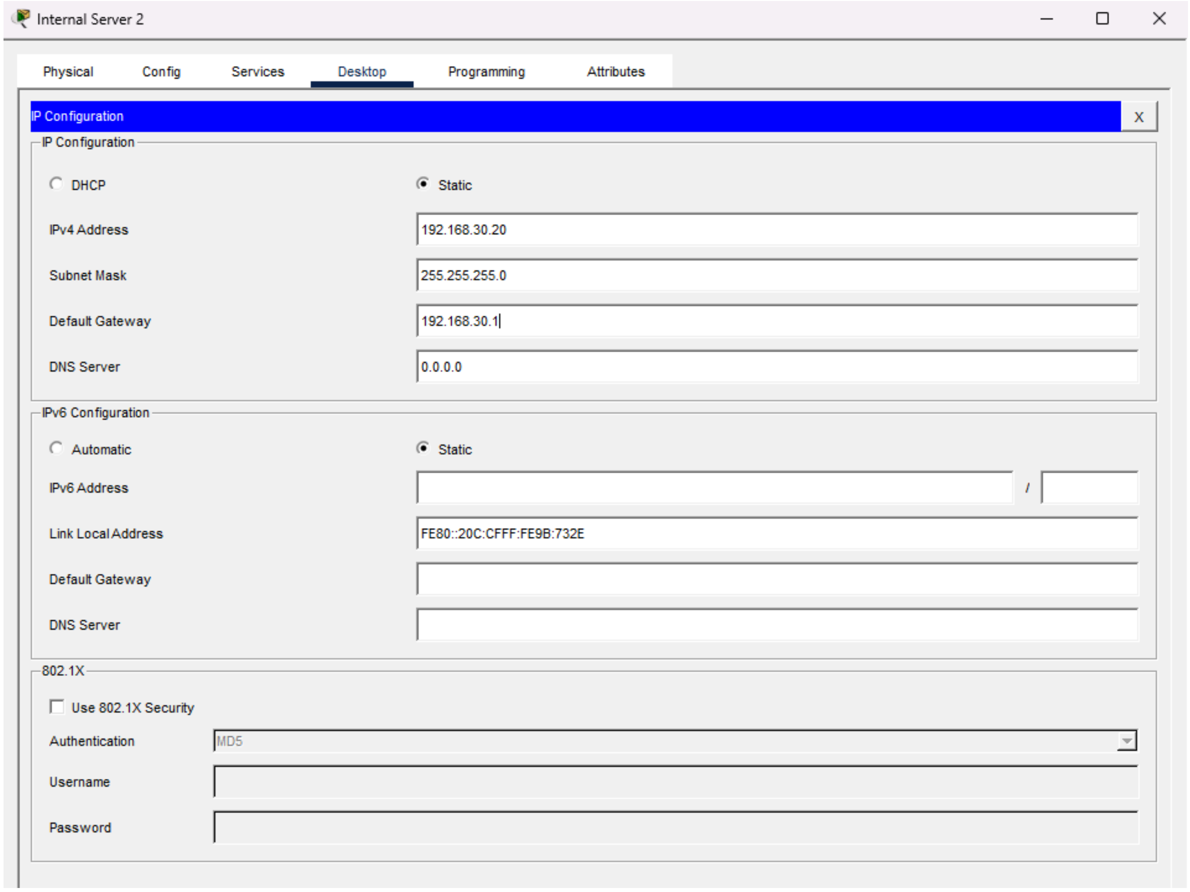


```
Switch#write memory
Building configuration...
[OK]
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface vlan 1
Switch(config-if)#ip address 192.168.30.2 255.255.255.0
Switch(config-if)#exit
Switch(config)#ip default-gateway 192.168.30.1
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console
write memory
Building configuration...
[OK]
Switch#
```



FastEthernet0/0

| | |
|---|---|
| Port Status | ☑ On |
| Link Speed | ● 100 Mbps ○ 10 Mbps ☑ Auto |
| Duplex | ● Half Duplex ○ Full Duplex ☑ Auto |
| MAC Address | 00E0.B00D.6B00 |
| IP Configuration | |
| IPv4 Address | 192.168.30.1 |
| Subnet Mask | 255.255.255.0 |
| Tx Ring Limit | 10 |



IP Configuration

| | |
|---|---|
| ○ DHCP | ● Static |
| IPv4 Address | 192.168.30.20 |
| Subnet Mask | 255.255.255.0 |
| Default Gateway | 192.168.30.1 |
| DNS Server | 0.0.0.0 |

IPv6 Configuration

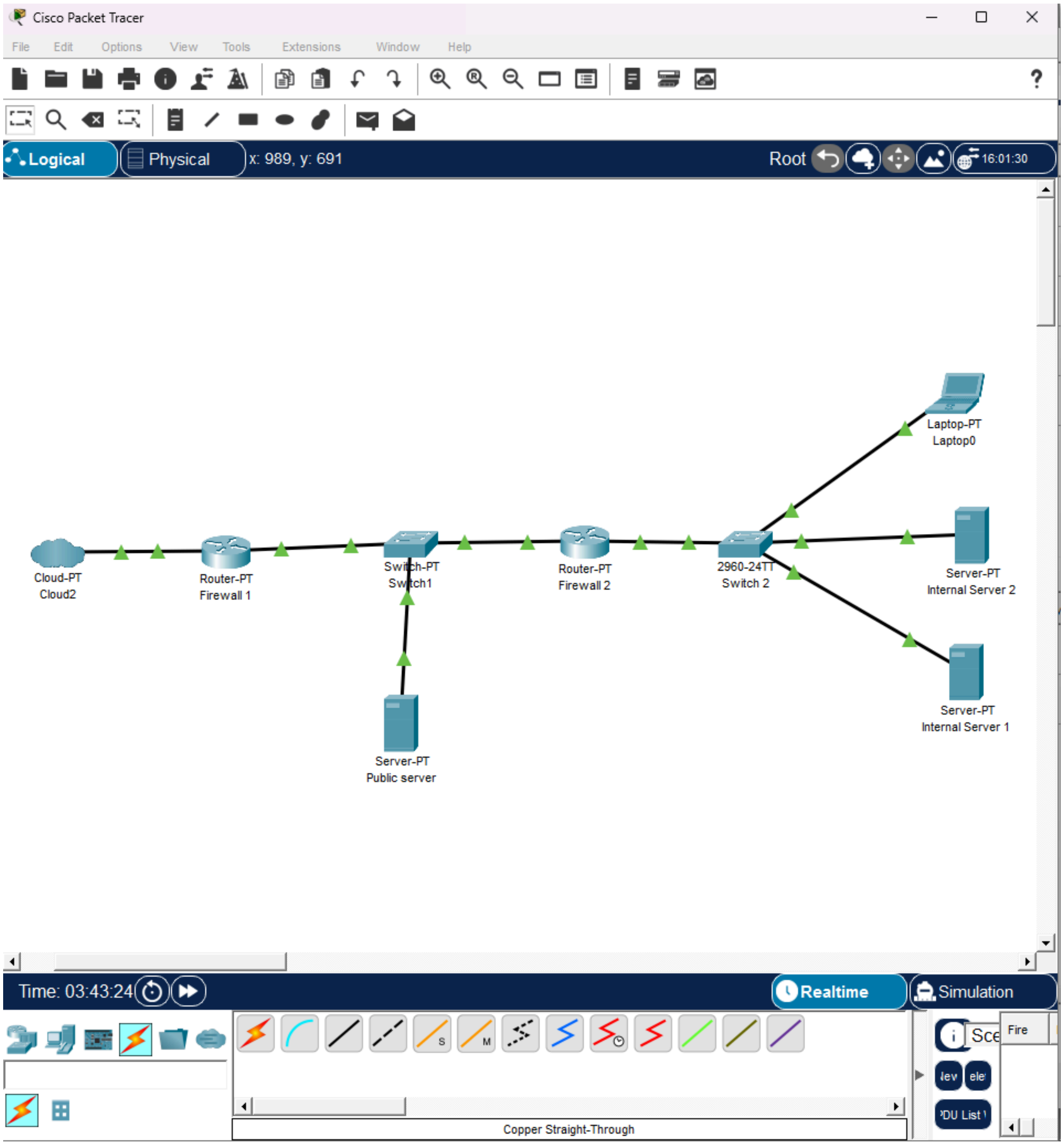
| | |
|---|---|
| ○ Automatic | ● Static |
| IPv6 Address | / |
| Link Local Address | FE80::20C:CFFF:FE9B:732E |
| Default Gateway | |
| DNS Server | |

802.1X

□ Use 802.1X Security

| | |
|---|---|
| Authentication | MD5 |
| Username | |
| Password | |

As shown in the initial image above, the connection indicators were red due to missing IP configurations. After assigning the correct IP addresses and gateways, all links turned green, confirming successful connectivity across the network.



**Firewall ACL Configuration**

The goal of the ACL was to control traffic from the LAN to the DMZ server. The policy was designed to:

- Allow HTTPS traffic (TCP Port 443) from the LAN to the DMZ server
- Allow ICMP traffic for monitoring and troubleshooting
- Block HTTP traffic (TCP Port 80) to prevent unencrypted web access
- Block all other unauthorized traffic by default

This ensures that only secure, encrypted communication is permitted to the public server, while unsafe or unwanted traffic is denied.

**ACL Applied on Firewall-2 (LAN to the DMZ Direction)**

```
#enable
#configure terminal
#ip access-list extended lan2dmz
#permit icmp 192.168.30.0 0.0.0.255 192.168.19.0 0.0.0.255
#permit tcp 192.168.30.0 0.0.0.255 192.168.19.0 0.0.0.255 eq 443
#deny tcp 192.168.30.0 0.0.0.255 192.168.19.0 0.0.0.255 eq 80
#deny ip any any
#exit

#interface FastEthernet1/0
#ip access-group lan2dmz out
#end
#write memory
```

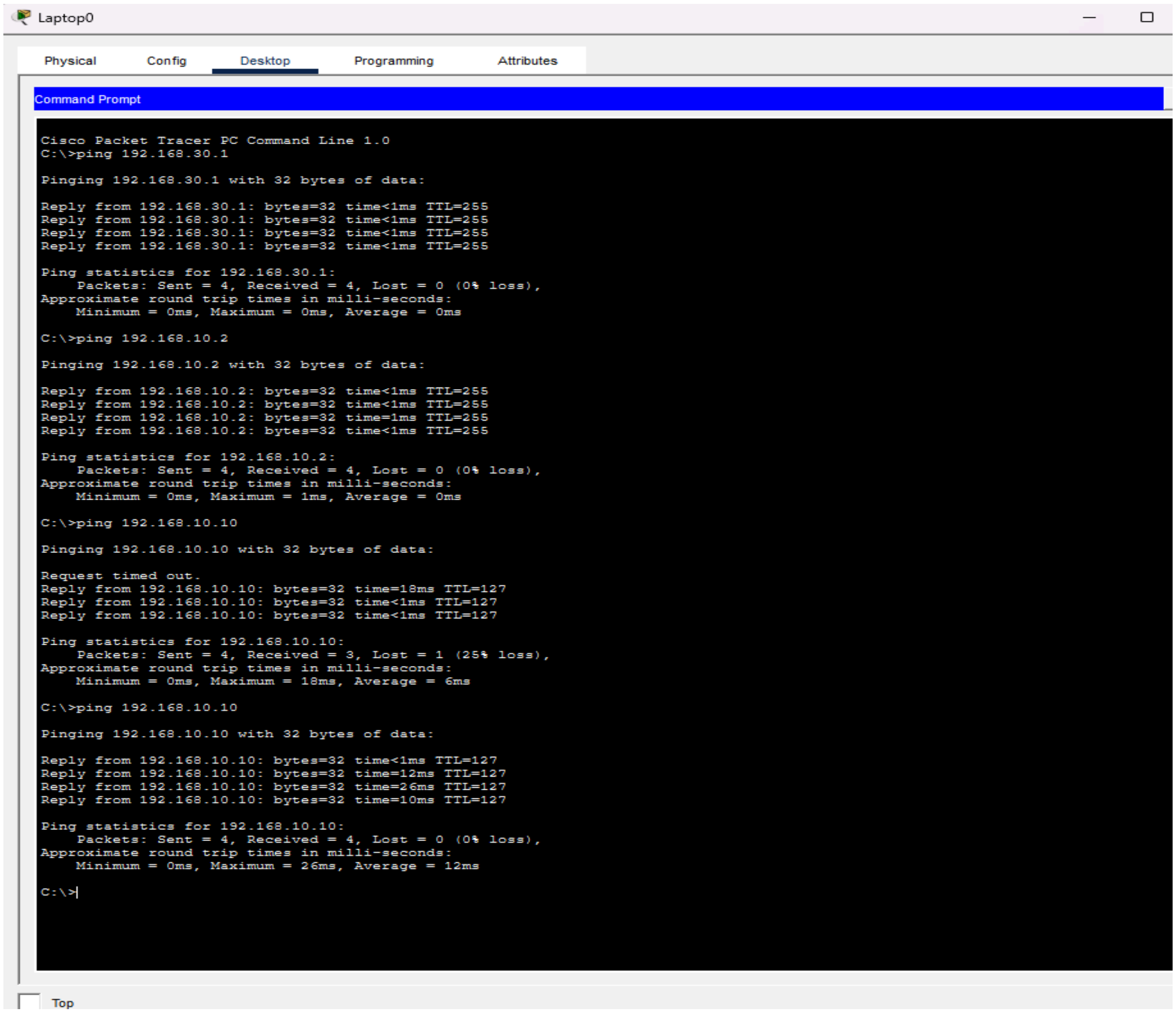
**Test and Validation**

To verify network connectivity, I used the LAN laptop to perform ICMP ping tests to the firewall gateways (Firewall-1 and Firewall-2) and the public server in the DMZ.

The results below confirm successful communication across all configured devices.

## Connectivity Test

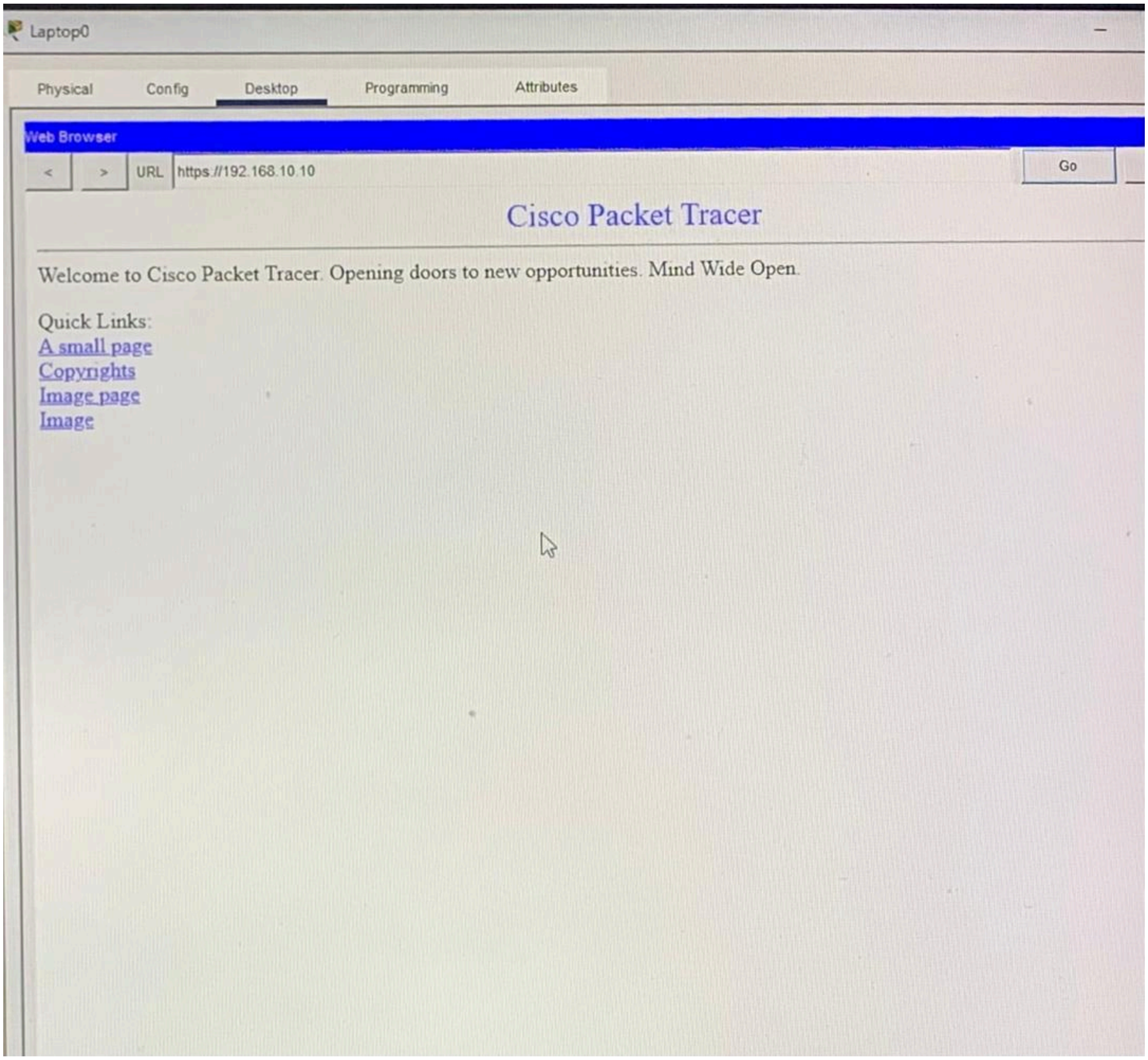
| Test | Source | Results |
|---|---|---|
| Ping Firewall-1 | LAN Laptop (192.168.30.10) | Responds |
| Ping Firewall-2 | LAN Laptop (192.168.30.10) | Responds |
| Ping Public Server | LAN Laptop (192.168.30.10) | Responds |



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.30.1

Pinging 192.168.30.1 with 32 bytes of data:

Reply from 192.168.30.1: bytes=32 time<1ms TTL=255
Reply from 192.168.30.1: bytes=32 time<1ms TTL=255
Reply from 192.168.30.1: bytes=32 time<1ms TTL=255
Reply from 192.168.30.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.30.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

Reply from 192.168.10.2: bytes=32 time<1ms TTL=255
Reply from 192.168.10.2: bytes=32 time<1ms TTL=255
Reply from 192.168.10.2: bytes=32 time=1ms TTL=255
Reply from 192.168.10.2: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.10.10

Pinging 192.168.10.10 with 32 bytes of data:

Request timed out.
Reply from 192.168.10.10: bytes=32 time=18ms TTL=127
Reply from 192.168.10.10: bytes=32 time<1ms TTL=127
Reply from 192.168.10.10: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.10.10:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 18ms, Average = 6ms

C:\>ping 192.168.10.10

Pinging 192.168.10.10 with 32 bytes of data:

Reply from 192.168.10.10: bytes=32 time<1ms TTL=127
Reply from 192.168.10.10: bytes=32 time=12ms TTL=127
Reply from 192.168.10.10: bytes=32 time=26ms TTL=127
Reply from 192.168.10.10: bytes=32 time=10ms TTL=127

Ping statistics for 192.168.10.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 26ms, Average = 12ms

C:\>
```

### Application Layer Test (Web browser on LAN Laptop to Public Server)

| Protocol | URL | Results |
|---|---|---|
| HTTP (Unsecure) | http://192.168.10.10 | Blocked |
| HTTPS (Secure) | https://192.168.10.10) | Successful (Page Loaded) |



https://192.168.10.10

Cisco Packet Tracer

Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

Quick Links:
A small page
Copyrights
Image page
Image

This project successfully demonstrates how to secure network communication using a DMZ and firewall access control lists. By placing a public web server behind Firewall-1 and restricting access through Firewall-2, internal resources remain protected while still allowing controlled, secure service access.

The ACL rule correctly enforced:

- Secure traffic allowed (HTTPS/443)
- Unsecured traffic blocked (HTTP/80)

This design mirrors real-world enterprise security models, where only encrypted services are available publicly, reducing cyberattack risks such as sniffing, man-in-the-middle attacks, and unauthorized access.