**Secure Cisco DMZ Web Server – Packet Tracer Project**

Prepared for: Matthew  
Date: 27 Aug 2025

# Executive Summary

This project demonstrates a professionally segmented network in Cisco Packet Tracer with a DMZ-hosted web server. A Cisco multilayer switch provides inter‑VLAN routing between an Internal VLAN (10) and a DMZ VLAN (20). Security is enforced by an inbound ACL on the DMZ SVI that permits only HTTP/HTTPS to the web server and denies all other traffic. The report includes architecture, configuration, verification outputs, and evidence screenshots captured during the build.

# 1. Architecture & IP Plan

• VLAN 10 (INTERNAL): 192.168.1.0/24 → SVI 192.168.1.1 → Laptops 192.168.1.2–1.3  
• VLAN 20 (DMZ): 192.168.2.0/24 → SVI 192.168.2.1 → Web Server 192.168.2.2  
• Device cabling: Gi1/0/1 Laptop1, Gi1/0/2 Laptop2, Gi1/0/3 Server0

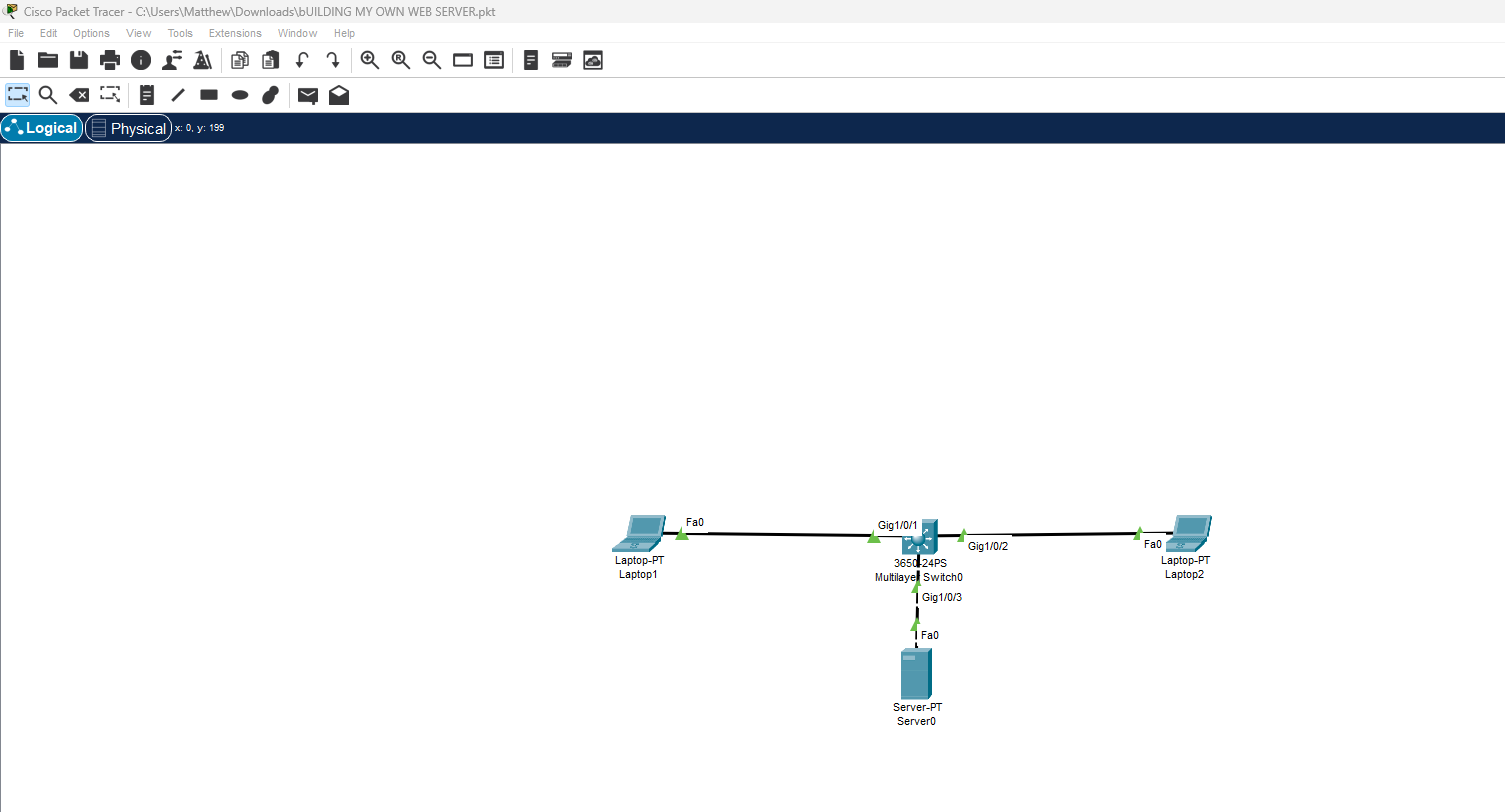


Figure: Packet Tracer topology and addressing.

# 2. Configuration Summary

Key elements on the multilayer switch: VLANs, SVIs, inter‑VLAN routing, and ACL on the DMZ SVI.

!  
! Cisco 3650 Multilayer Switch - Secure DMZ Web Server Lab (Packet Tracer)  
!  
conf t  
!  
hostname MLS-DMZ  
!  
no ip domain-lookup  
!  
vlan 10  
 name INTERNAL  
vlan 20  
 name DMZ  
!  
interface range gigabitEthernet1/0/1 - 2  
 description INTERNAL-ACCESS  
 switchport mode access  
 switchport access vlan 10  
 spanning-tree portfast  
!  
interface gigabitEthernet1/0/3  
 description DMZ-WEBSERVER  
 switchport mode access  
 switchport access vlan 20  
 spanning-tree portfast  
!  
interface Vlan10  
 description GATEWAY-INTERNAL  
 ip address 192.168.1.1 255.255.255.0  
 no shutdown  
!  
interface Vlan20  
 description GATEWAY-DMZ  
 ip address 192.168.2.1 255.255.255.0  
 no shutdown  
!  
ip routing  
!  
! ---- Security ACL: allow only HTTP/HTTPS to the web server 192.168.2.2 ----  
ip access-list extended DMZ-WEB-ONLY  
 remark Permit required web traffic to the DMZ web server  
 permit tcp any host 192.168.2.2 eq 80  
 permit tcp any host 192.168.2.2 eq 443  
 remark Deny all other traffic to the server (log optional)  
 deny ip any host 192.168.2.2  
!  
interface Vlan20  
 ip access-group DMZ-WEB-ONLY in  
!  
end  
write memory  
!  
! ---- Verification (EXEC mode) ----  
! show vlan brief  
! show ip interface brief  
! show ip route  
! show access-lists DMZ-WEB-ONLY  
!

# 3. Verification & Evidence

Below are the critical verification outputs and screenshots.

## 3.1 VLAN Assignment

show vlan brief

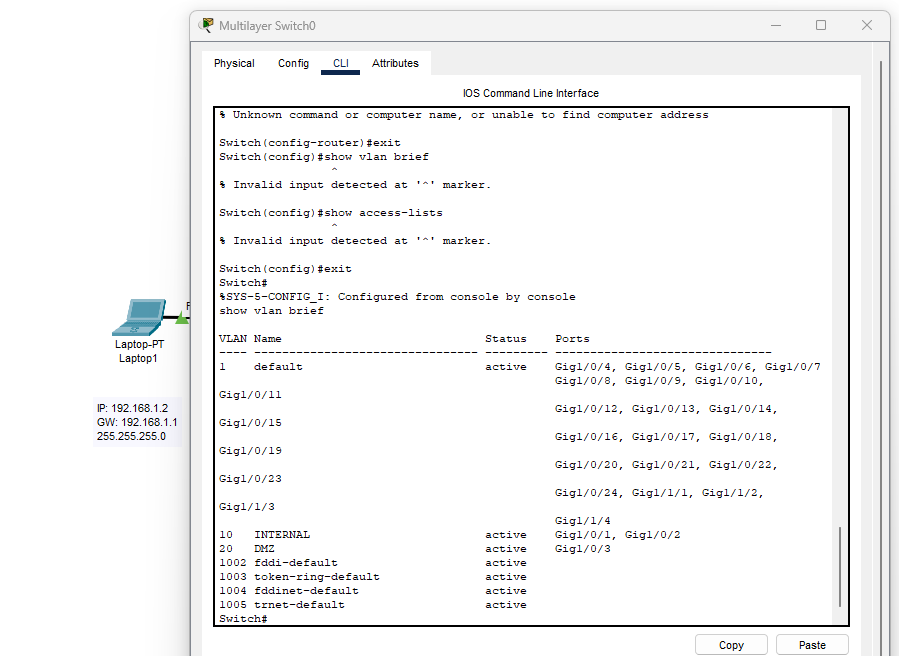


Figure: VLAN 10 for laptops (Gi1/0/1–2), VLAN 20 for server (Gi1/0/3).

## 3.2 SVI Status (Gateways)

show ip interface brief

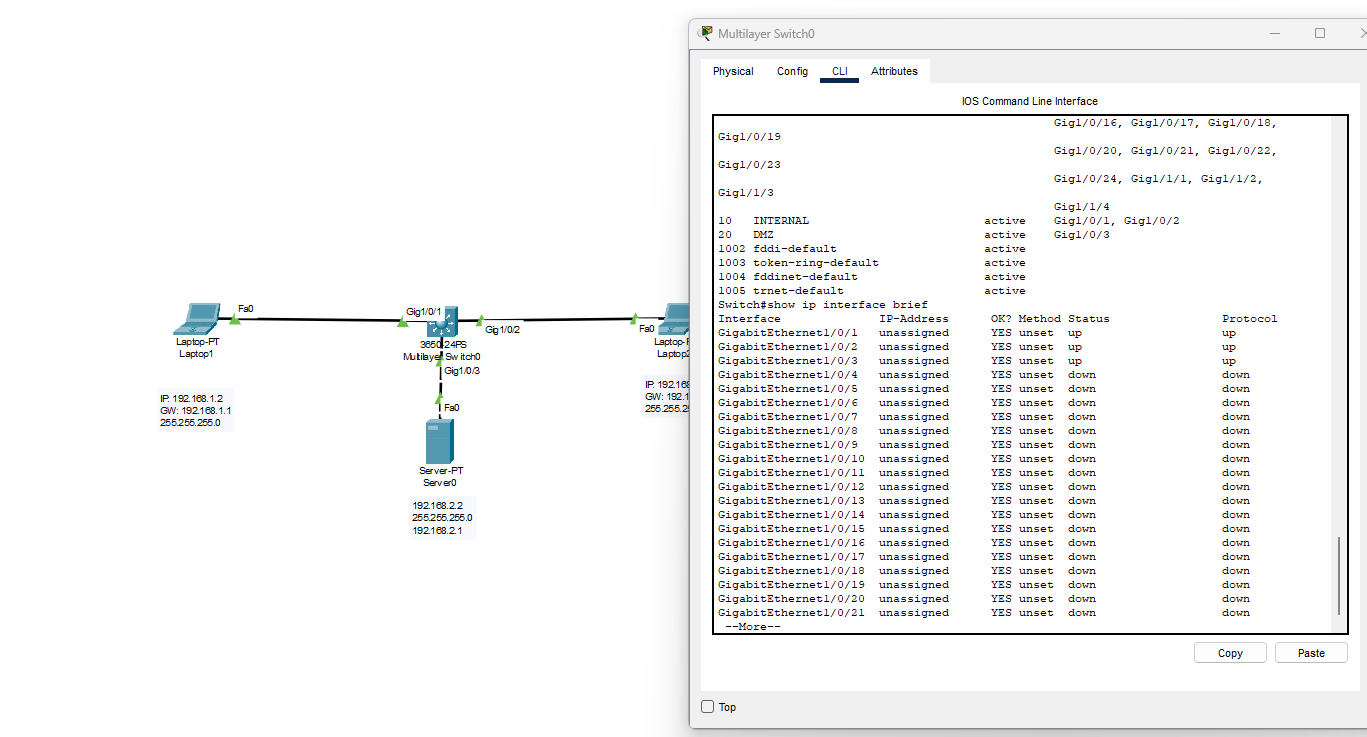


Figure: Interface summary during build. Final state shows Vlan10 192.168.1.1 and Vlan20 192.168.2.1 up/up.

## 3.3 Routing Table

show ip route

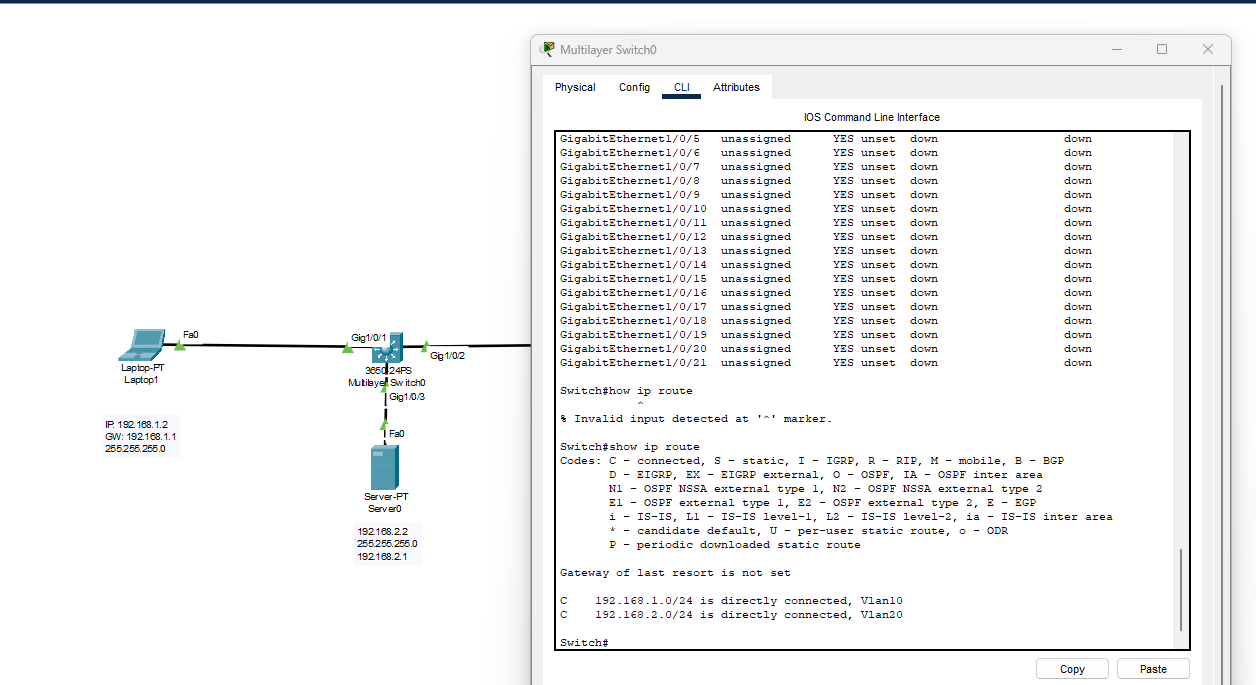


Figure: Connected routes for 192.168.1.0/24 and 192.168.2.0/24 confirm inter‑VLAN routing.

## 3.4 DMZ ACL Hits

show access-lists DMZ-WEB-ONLY

Expected behaviour after applying ACL to Vlan20 inbound:

- ICMP/Telnet/FTP → denied  
- HTTP/HTTPS → permitted

## 3.5 Functional Tests

• From Internal client to Web server via HTTP: PASS (page loads)  
• From Internal client ping to server: FAIL (blocked by ACL)  
• From Internal client non‑web ports to server: FAIL (blocked)

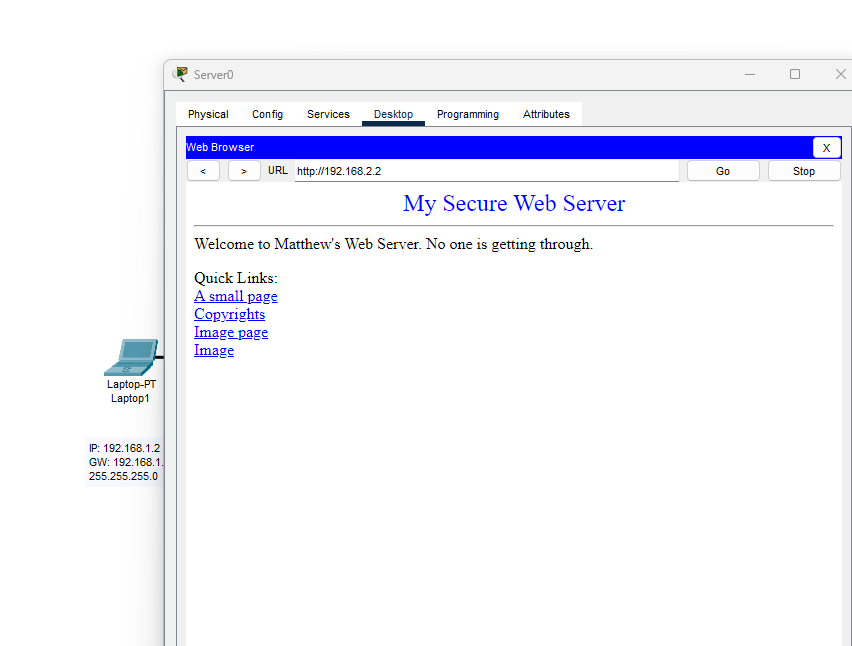


Figure: Web page served by Server0 (192.168.2.2) – functional test success.

## 3.6 Troubleshooting Snapshot (before fix)

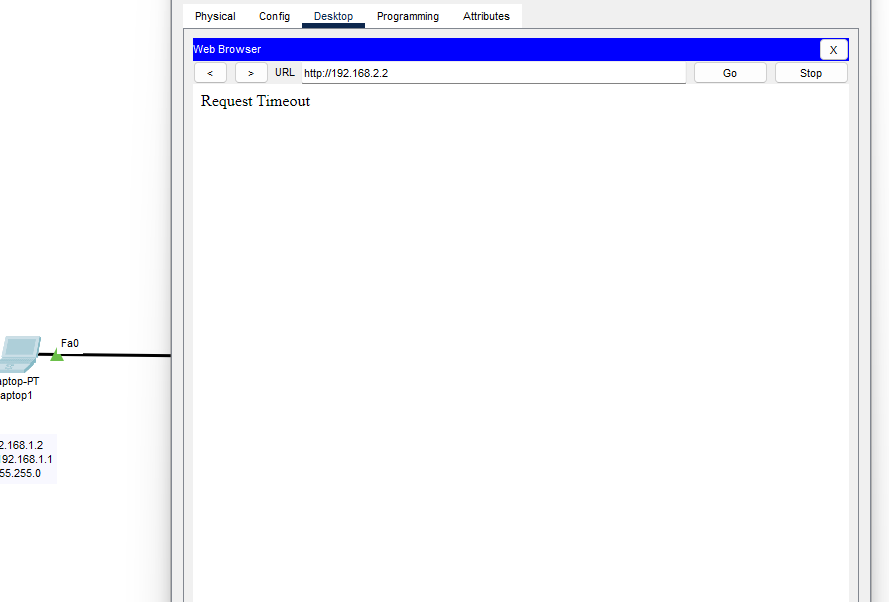


Figure: Initial timeout prior to enabling HTTP and completing routing; retained here as build evidence.

# 4. Security Design Rationale

The web server is isolated in a DMZ and reachable only over the required ports (80/443). Inbound ACL on the DMZ gateway enforces least privilege and mitigates lateral movement. This mirrors enterprise patterns where public‑facing services are separated from internal users.

# 5. Reproducibility Checklist

• Create VLAN 10 (INTERNAL) and VLAN 20 (DMZ); assign ports.

• Configure SVIs: Vlan10 192.168.1.1/24, Vlan20 192.168.2.1/24; enable ip routing.

• Set host IPs: Laptop1 192.168.1.2/24 GW 192.168.1.1; Laptop2 192.168.1.3/24; Server 192.168.2.2/24 GW 192.168.2.1.

• Enable HTTP (and optional HTTPS) on Server0 > Services.

• Verify pings pre‑ACL; then apply ACL DMZ-WEB-ONLY to Vlan20 inbound.

• Re‑verify: web works, pings/non‑web to server are denied.

# Appendix A – Full Switch Configuration

!  
! Cisco 3650 Multilayer Switch - Secure DMZ Web Server Lab (Packet Tracer)  
!  
conf t  
!  
hostname MLS-DMZ  
!  
no ip domain-lookup  
!  
vlan 10  
 name INTERNAL  
vlan 20  
 name DMZ  
!  
interface range gigabitEthernet1/0/1 - 2  
 description INTERNAL-ACCESS  
 switchport mode access  
 switchport access vlan 10  
 spanning-tree portfast  
!  
interface gigabitEthernet1/0/3  
 description DMZ-WEBSERVER  
 switchport mode access  
 switchport access vlan 20  
 spanning-tree portfast  
!  
interface Vlan10  
 description GATEWAY-INTERNAL  
 ip address 192.168.1.1 255.255.255.0  
 no shutdown  
!  
interface Vlan20  
 description GATEWAY-DMZ  
 ip address 192.168.2.1 255.255.255.0  
 no shutdown  
!  
ip routing  
!  
! ---- Security ACL: allow only HTTP/HTTPS to the web server 192.168.2.2 ----  
ip access-list extended DMZ-WEB-ONLY  
 remark Permit required web traffic to the DMZ web server  
 permit tcp any host 192.168.2.2 eq 80  
 permit tcp any host 192.168.2.2 eq 443  
 remark Deny all other traffic to the server (log optional)  
 deny ip any host 192.168.2.2  
!  
interface Vlan20  
 ip access-group DMZ-WEB-ONLY in  
!  
end  
write memory  
!  
! ---- Verification (EXEC mode) ----  
! show vlan brief  
! show ip interface brief  
! show ip route  
! show access-lists DMZ-WEB-ONLY  
!