Milestone 1 — Defense-in-Depth Diagram & Access Policy

Student Name: Clayton Holden
Date Submitted: 12/5/2025
Course: CYBR-2102
Instructor: Norma DePriest

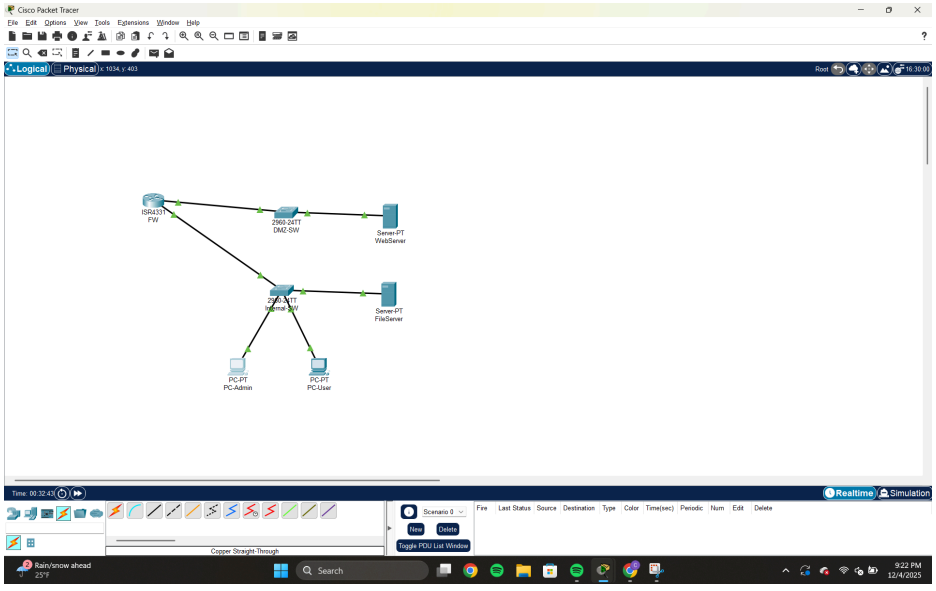
---

1 System Overview

Field	Entry
Project Title	Defense-in-Depth Network Design
Simulation Tool	☑ Packet Tracer ☐ NetLab ☐ Other
Environment Type	☑ On-Prem Lab ☐ Cloud Lab ☐ Hybrid
Network Scope	Number of hosts: **5** Number of zones: **3**

---

2 Network Topology Diagram



Must show:

- External → FW → DMZ → Internal zones
- IP ranges
- Firewall ACL boundaries
- Switches, servers, PCs labeled

3️⃣ Defense Layers and Controls

Defense Layer	Control Implemented	Purpose / Justification	Verification Method
Perimeter	ACL-DMZ on FW (Gig0/0/0)	Only HTTP allowed into DMZ; all other inbound traffic blocked	`show access-lists`
Network	Subnet segmentation: DMZ (192.168.10.0/24), Internal (192.168.20.0/24)	Prevents lateral movement and isolates assets	Ping tests, path tests
Host	Local firewalls enabled on PC-Admin & FileServer	Adds endpoint-level protection against unauthorized access	Firewall screenshot
Application	WebServer exposes only HTTP	Reduces application-layer attack surface	HTTP test from internal hosts
Data	FileServer kept inside Internal LAN only	Protects sensitive data from external or DMZ access	ACL denies DMZ ↔ Internal

---

4️⃣ Access Control Matrix

Role / User Group	Allowed Ports / Services	Denied Ports / Services	Enforcement Mechanism	Result (Test Outcome)
Administrator (192.168.20.11)	SSH (22), RDP (3389)	HTTP, HTTPS, All others	ACL-ADMIN + ACL-INTERNAL	SSH allowed (connection refused); HTTP blocked

IT Support (192.168.20.12)	HTTP (80), HTTPS (443)	SSH, RDP	ACL-IT + ACL-INTERNAL	HTTP allowed; SSH blocked
User (192.168.20.10)	HTTP (80)	All others	ACL-USER + ACL-INTERNAL	HTTP allowed; SSH blocked

---

5 Security Policy Summary

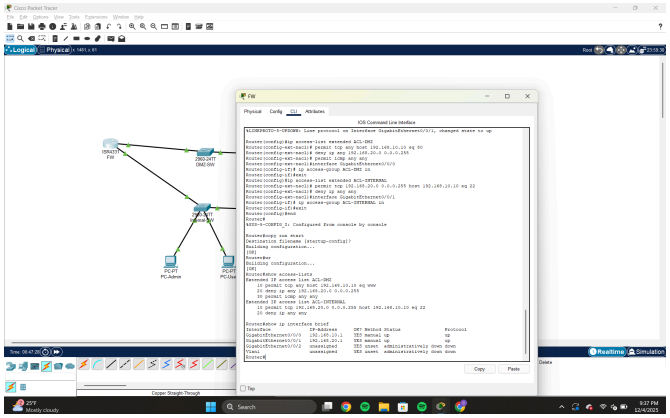
This network uses a defense-in-depth architecture with layered controls at the perimeter, network, host, application, and data levels. ACLs enforce strict zone-to-zone communication rules based on least privilege and role-based access requirements. Host firewalls supplement the perimeter defenses by blocking unnecessary inbound connections. Application-layer restrictions on the WebServer further reduce exposure. Together, these measures align with zero-trust principles by requiring explicit allow rules and denying all other traffic.

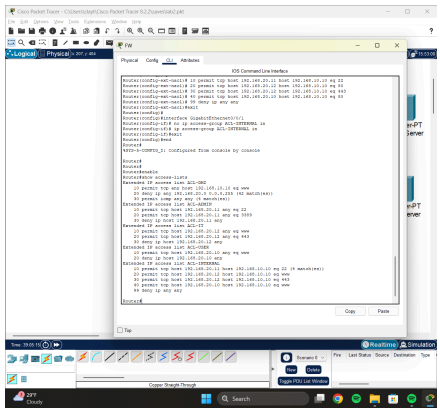
---

6 Verification Evidence

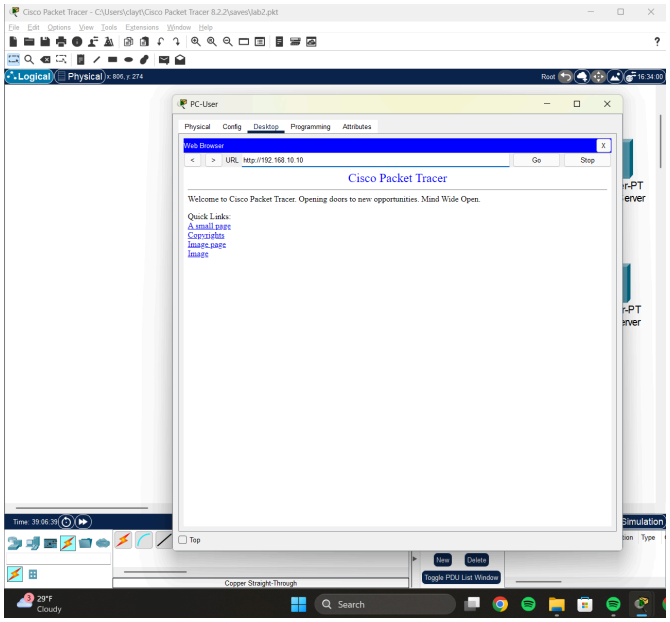
☑ **Network Diagram**

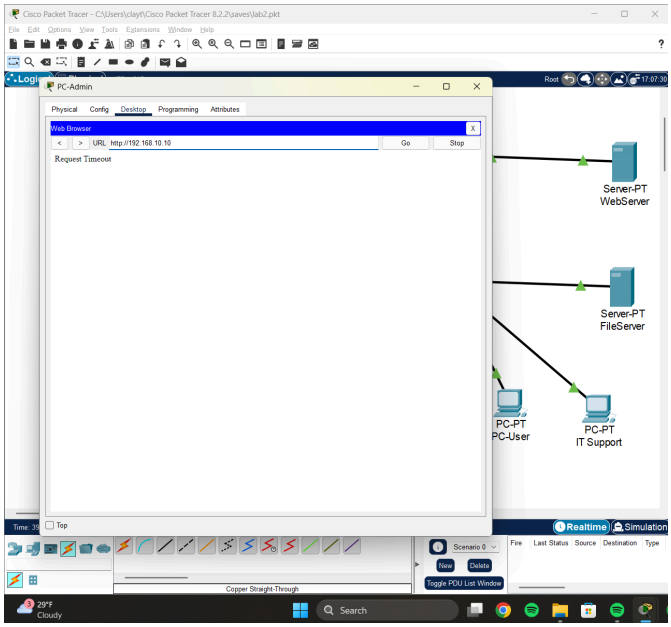
☑ **Firewall Rules (`show access-lists`)**



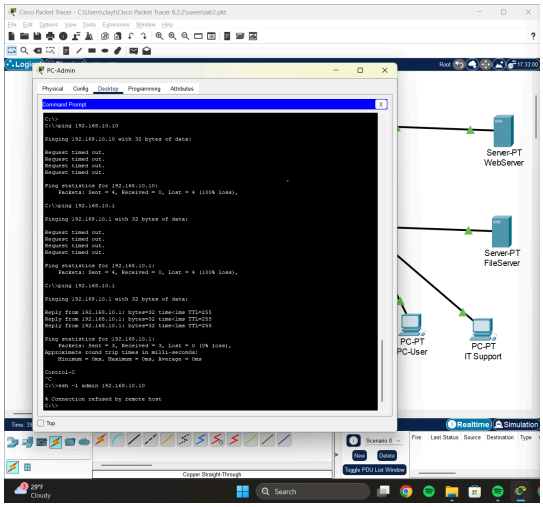


☑ **ACL Output (allowed/blocked tests)**

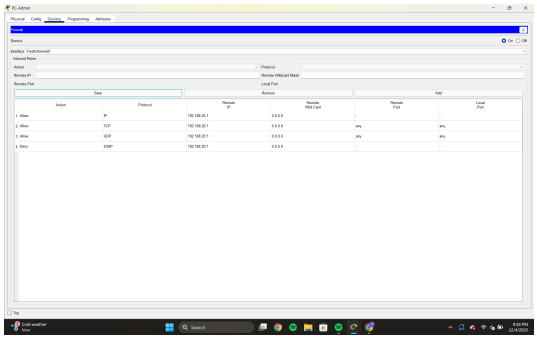




☑ Ping / Traffic Tests



☑ **Host Firewall Screenshot**



7️⃣ Sign-Off

Step	Completed By	Date	Verified By (Instructor Use)
Network Design	Clayton Holden	12/4/2025	
Access Controls Applied	Clayton Holden	12/4/2025	

Evidence Collected	Clayton Holden	12/4/2025	