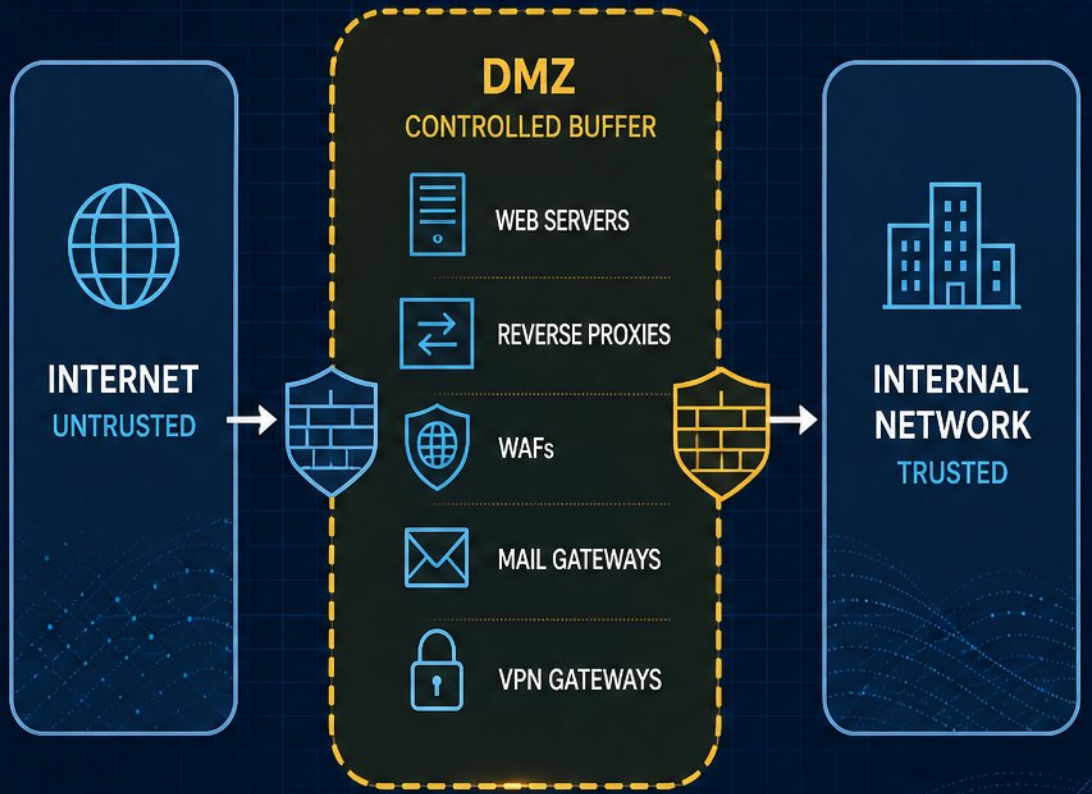
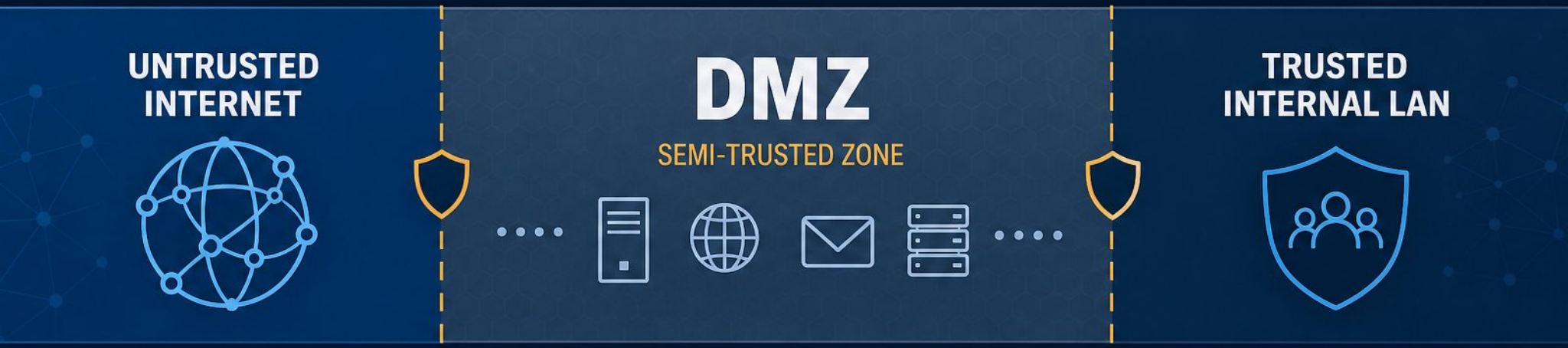
Demilitarized Zone Computer Networking: Concepts, Purpose, and Examples

- **Course roadmap:** define the DMZ, explain its purpose, show designs
- **Core idea:** a controlled buffer between untrusted internet and trusted internal network
- **Real-world anchors:** web servers, reverse proxies, WAFs, mail gateways, VPN gateways
- **Terminology:** screened subnet, perimeter network, bastion host, default deny
- **Focus:** concepts, topology examples, and defensible design trade-offs



What a DMZ Is and What It Is Not



IS

- A physical or logical subnet separating internal LAN from untrusted networks

IS

- Hosts services that must be reachable from the outside

IS NOT

- A design pattern and zone — not one machine or one firewall rule

IS NOT

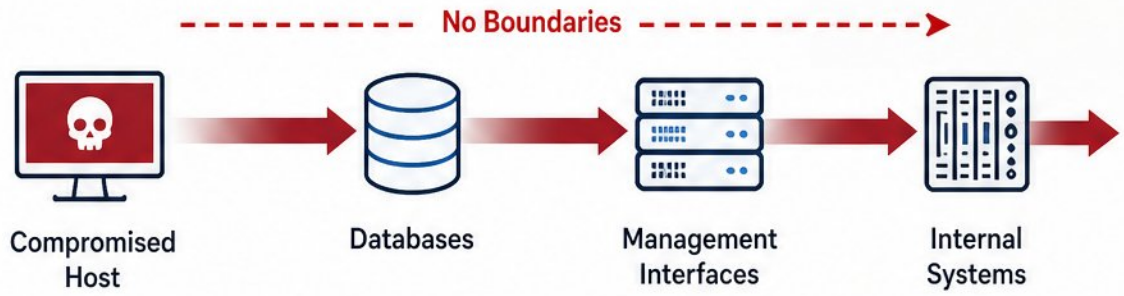
- Does not replace patching, hardening, or identity-based controls

IS

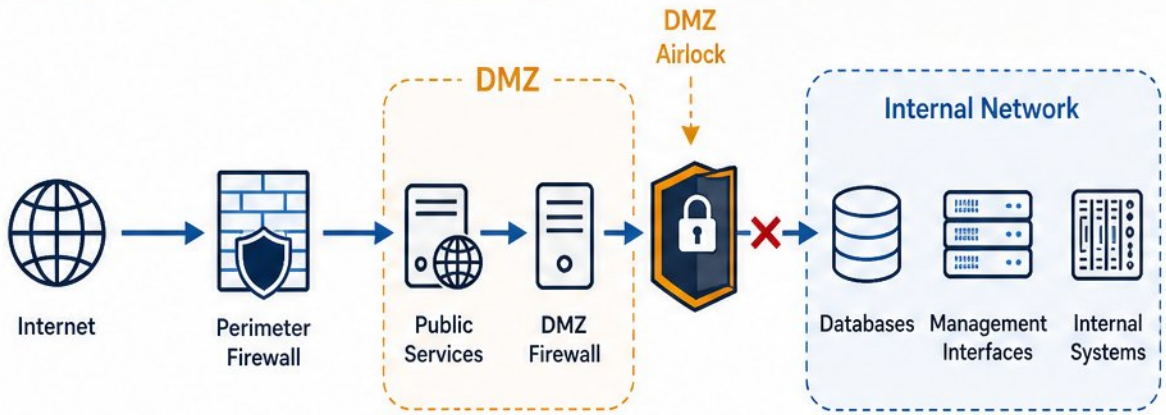
- Semi-trusted: between untrusted internet and highly trusted internal systems

Why Segmentation and a DMZ Exist

1) Flat Network: No Segmentation



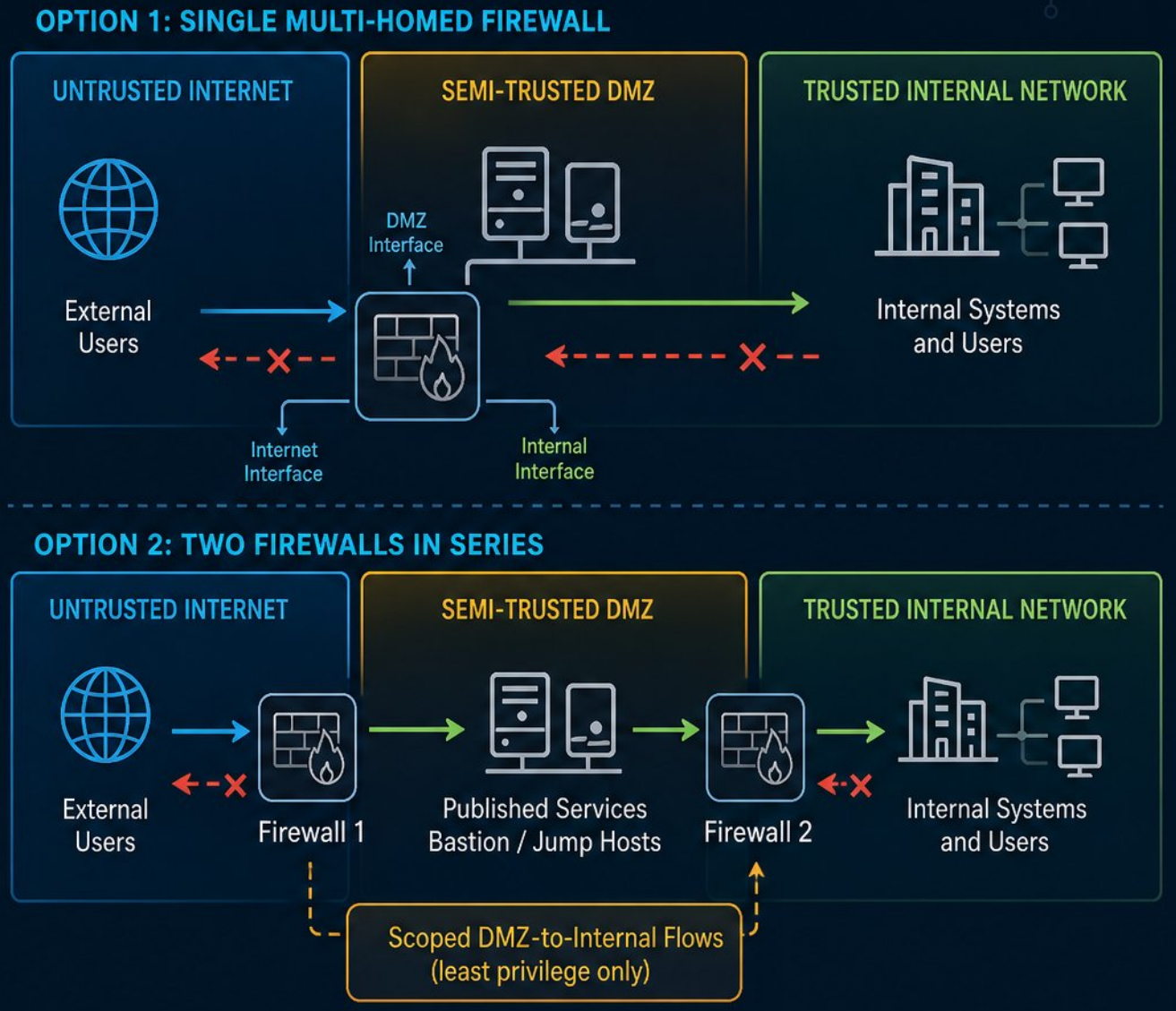
2) Segmented Network: With DMZ



- Flat networks let one compromised host reach databases and management interfaces
- DMZ limits blast radius: public service breach should not expose internal systems
- Defense in depth: firewalls, IDS/IPS, WAFs, patching, least privilege, monitoring
- Default deny: block all, permit only justified flows; denials reveal attacks
- Caveat: DMZ cannot secure unpatched or misconfigured services

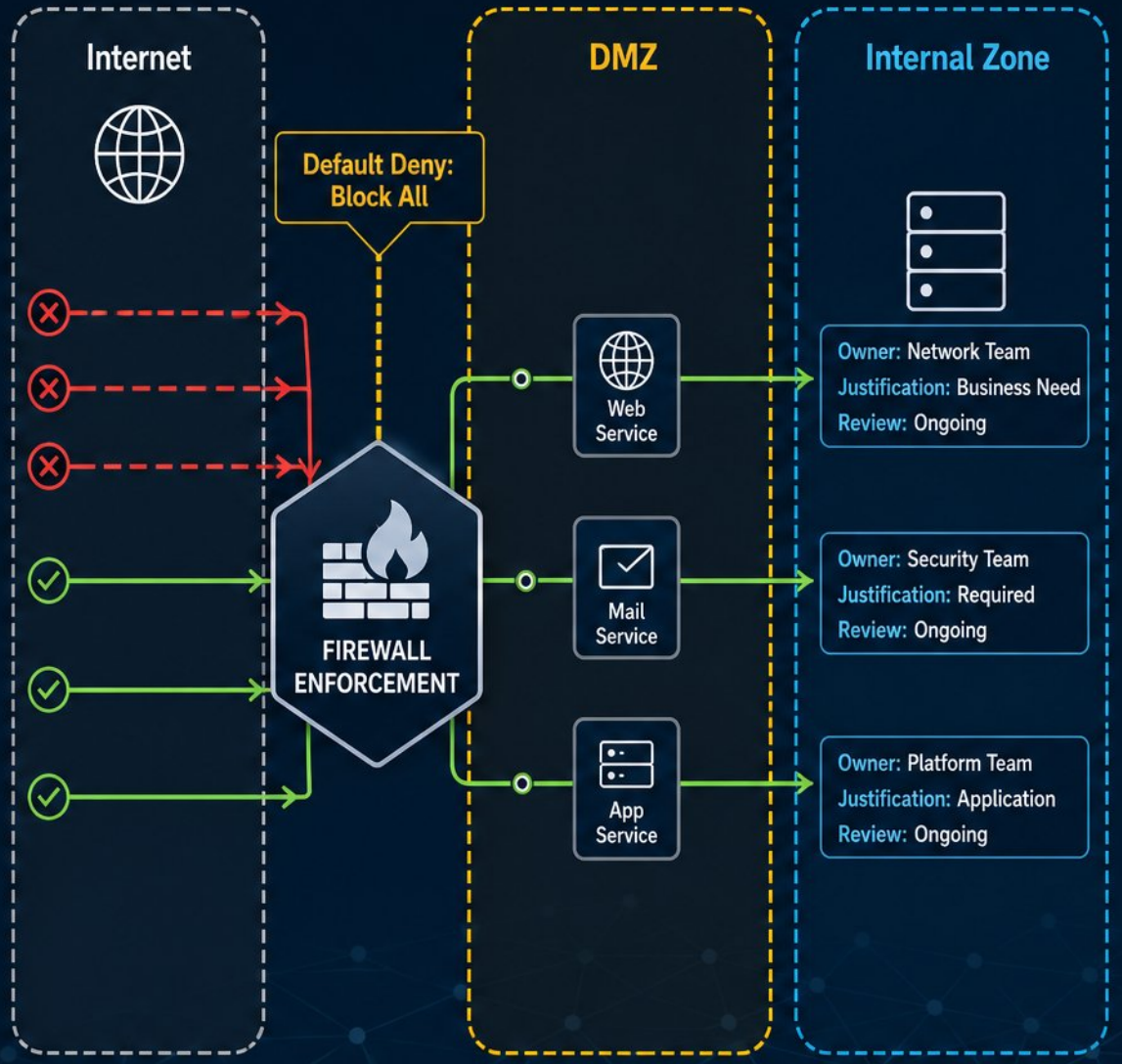
Zones, Firewalls, and Traffic Flow

- Three zones: untrusted internet, semi-trusted DMZ, trusted internal network
- Enforcement at every boundary, not just at the internet edge
- Single multi-homed firewall vs. two firewalls in series
- Inbound to published services; controlled DMZ outbound; scoped DMZ-to-internal flows
- Bastion and jump hosts: hardened admin access, off application traffic paths
- Key question: should the DMZ initiate connections inward? Usually no.



Design Principles and Rules of Engagement

- Default deny: block all, then permit only justified flows
- Least privilege: specific hosts and ports, never whole subnets
- Separation of duties: unique credentials and management paths
- Log DMZ traffic as untrusted: denials, WAF events, unusual egress
- Change control: review, test, document, expire, re-certify rules



What Typically Lives in a DMZ — and What Should Not

TYPICAL DMZ RESIDENTS

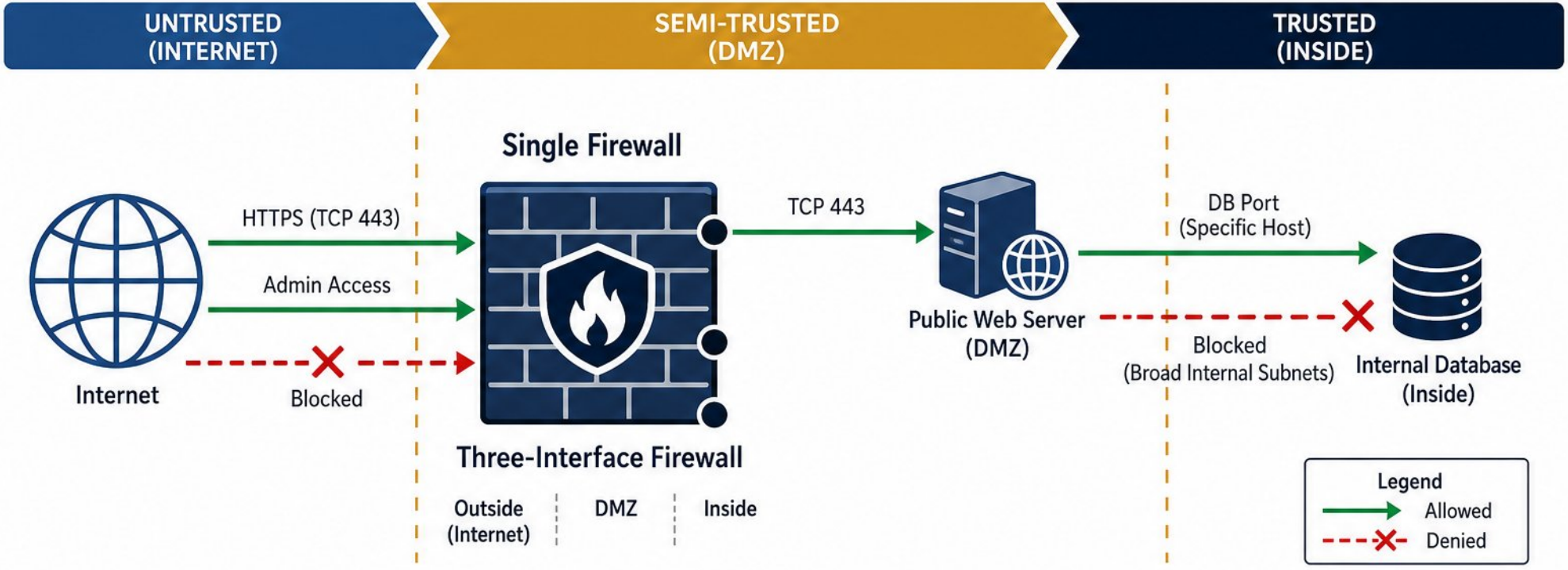
- Web Servers
- Reverse Proxies
- Load Balancers
- Mail Relays
- External DNS
- WAFs
- VPN Gateways / VPN Concentrators

MUST NOT RESIDE IN THE DMZ

- Sensitive Databases
- Domain Controllers
- Internal File Shares
- Backup Controllers

- Standard residents: web servers, reverse proxies, load balancers, API gateways, mail relays, external DNS, WAFs
- Remote-access gateways and VPN concentrators: common DMZ residents, though ZTNA shifts some designs
- Each belongs because it legitimately accepts connections from the internet
- Never place here: sensitive databases, domain controllers, internal file shares, backup controllers
- Anti-pattern: placing systems in the DMZ for convenience, not genuine public reachability

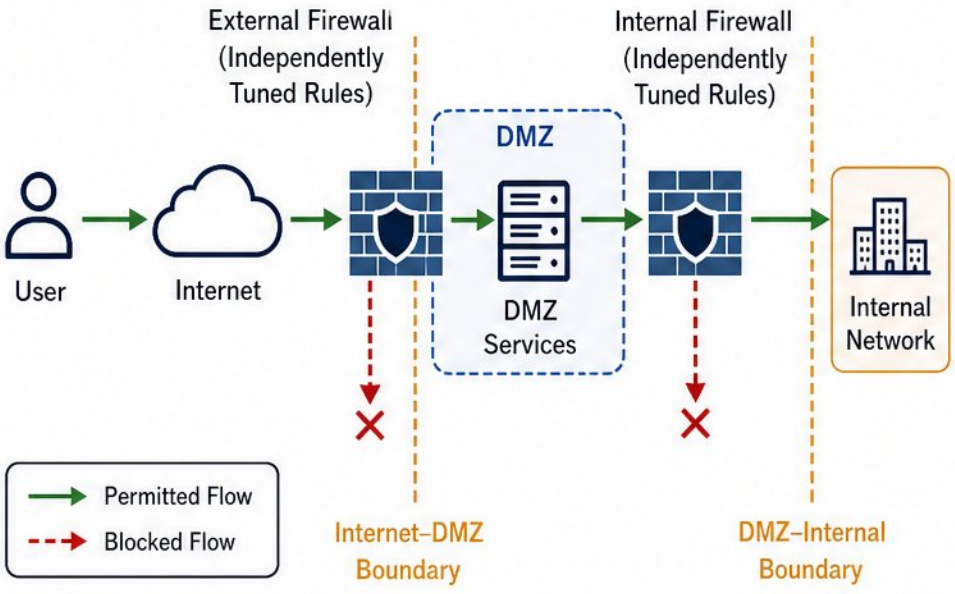
Example 1: Basic Screened Subnet with a Single Firewall



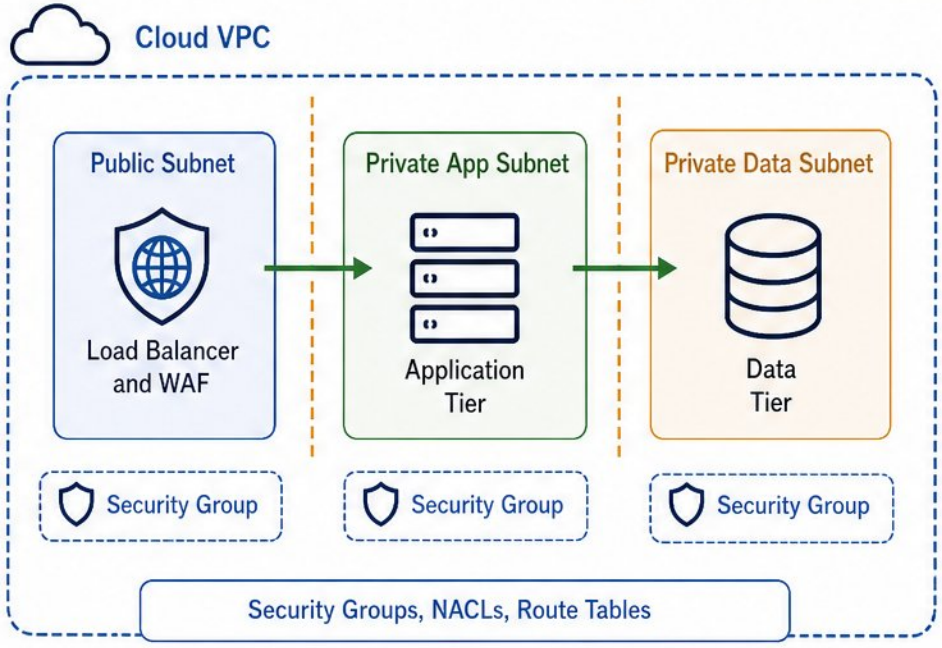
- Three-interface firewall: outside (internet), DMZ, and inside interfaces
- Public web server placed in DMZ, serves TCP 443 from internet
- Internal database behind inside interface, reached only by web server
- **Allowed:** internet → DMZ:443; DMZ → specific DB host:DB port; admin → DMZ
- **Denied:** internet → internal, DMZ → broad internal subnets, unneeded inside → DMZ
- Single firewall is a single point of failure; harden and monitor heavily

Example 2: Dual-Firewall DMZ and Cloud DMZ

On-Premises: Dual-Firewall DMZ Architecture



Cloud Equivalent: DMZ Design

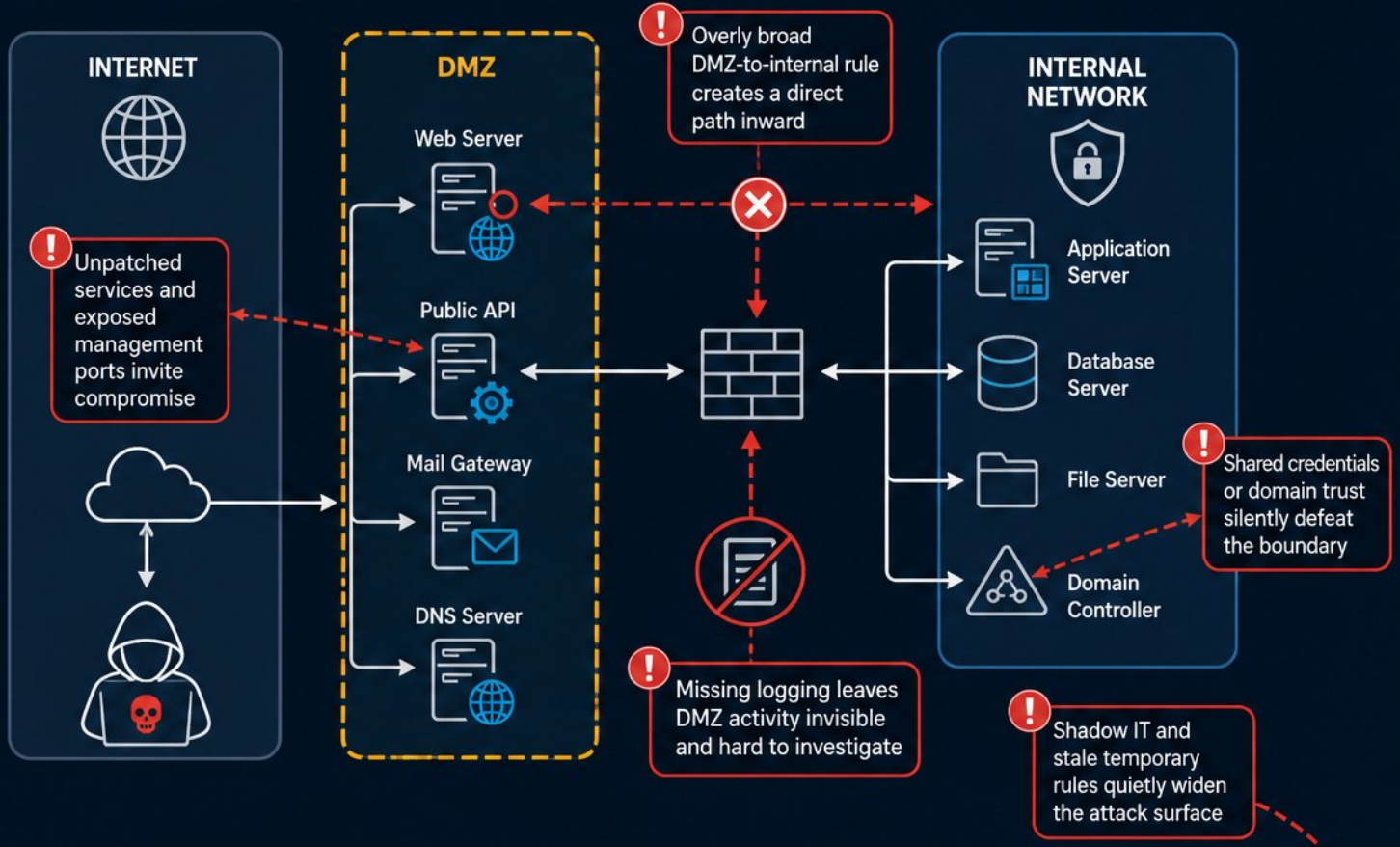


- Dual-firewall: external firewall guards internet–DMZ; internal firewall guards DMZ–internal.
- Each firewall keeps its own independently tuned rule set.
- Gain stronger compartmentalization and possible vendor diversity.
- Cost: higher expense, more devices, greater operational complexity.
- Cloud equivalent: public subnet (load balancer, WAF), private app subnet, private data subnet.
- Flow: user → internet → cloud WAF/load balancer → DMZ app tier → restricted internal data tier.
- Maps to AWS VPCs, subnets, route tables, security groups, and NACLs.

Legend

- Permitted Flow (Allowed)
- Blocked Flow (Denied)
- Firewall Enforcement (Policy Boundary)

Common Misconfigurations and How They Fail



- Overly broad DMZ-to-internal rules create a direct path inward
- Shared credentials or domain trust silently defeat the boundary
- Unpatched services and exposed management ports invite compromise
- Missing logging leaves DMZ activity invisible and hard to investigate
- Shadow IT and stale temporary rules quietly widen the attack surface

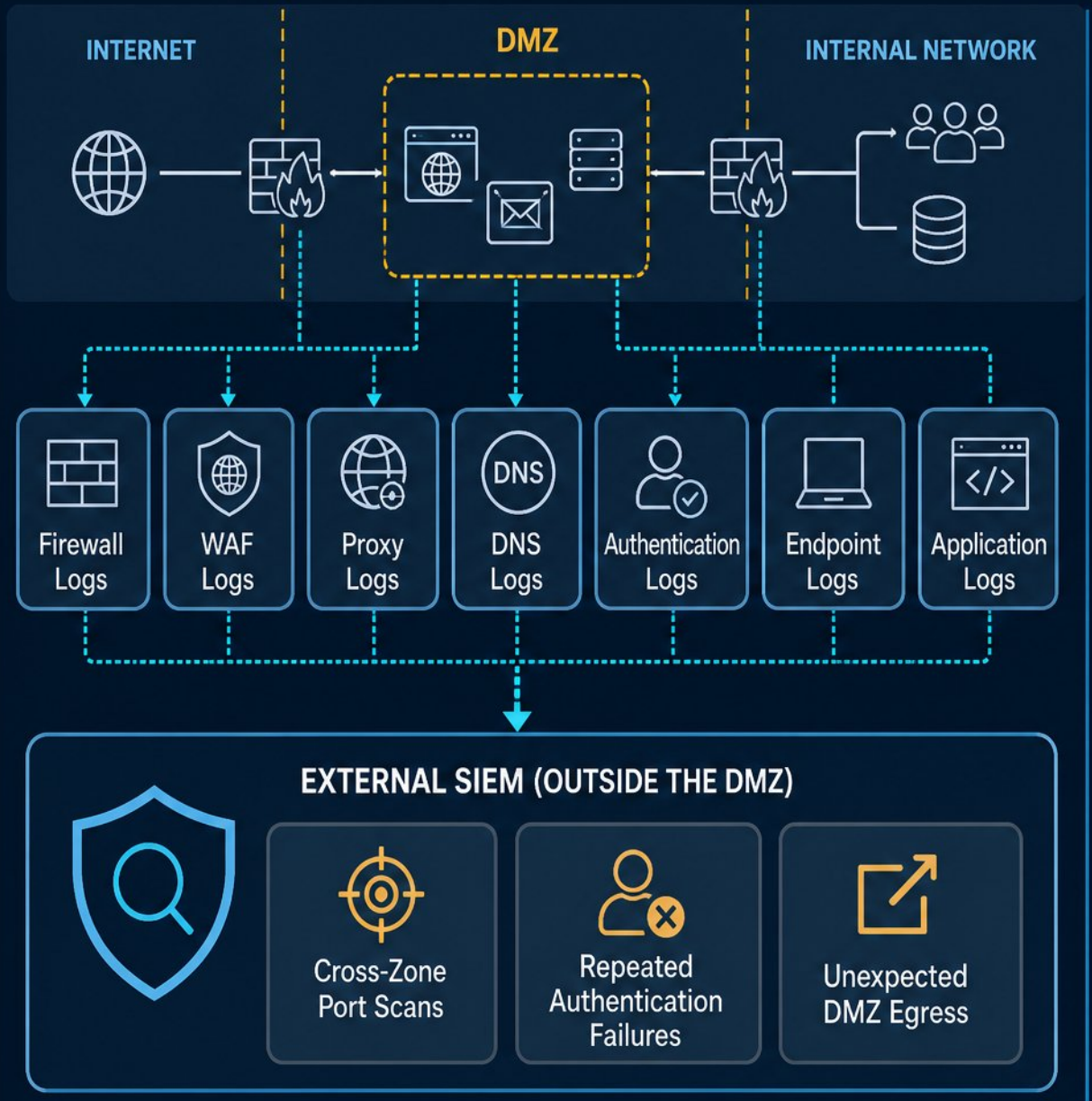
HOST-PLACEMENT LEDGER

BELONG IN THE DMZ	MUST NEVER BE IN THE DMZ
Web Servers	Database Servers
Public APIs	File Servers
Mail Gateways	Domain Controllers
DNS Servers	Internal Management Systems

FIREWALL / RULE BASE (EXAMPLE)

SOURCE	DESTINATION	SERVICE	PURPOSE	
Internet	DMZ Web Server	Web	Allow	✓
Internet	DMZ Mail Gateway	Mail	Allow	✓
DMZ Any	Internal Any	Any	Temporary Access	!
DMZ Admin Host	Internal Servers	Management	Admin Access	✓

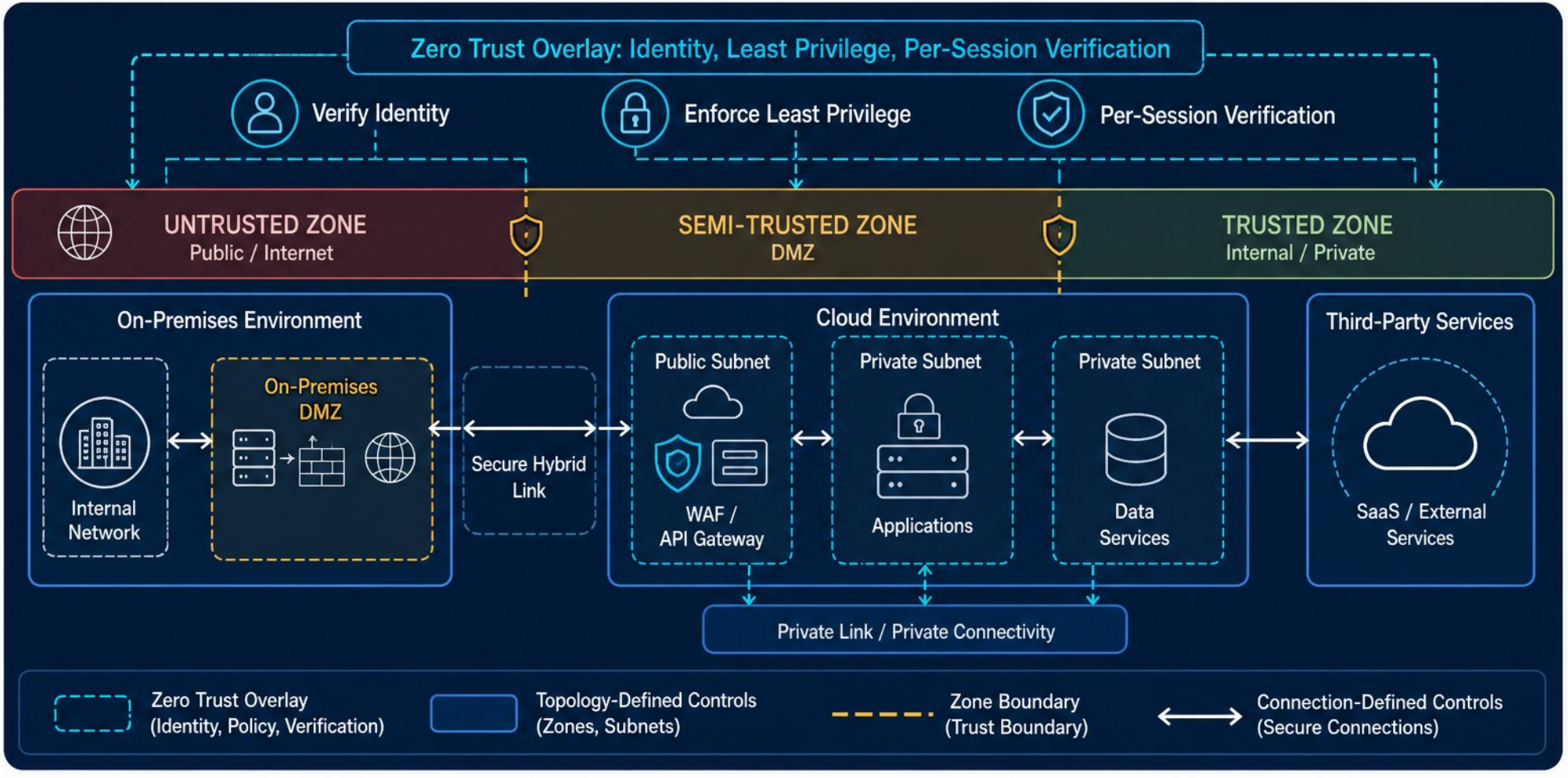
Monitoring, Detection, and Incident Response in the DMZ



- Centralize logs in an external SIEM: firewall, WAF, DNS, authentication
- Baseline normal inter-zone traffic; alert on deviations and unexpected egress
- Place IDS/IPS at both boundaries: internet–DMZ and DMZ–internal
- Watch for port scans, repeated auth failures, and forbidden destinations
- Assume compromise: design and rehearse containment and rollback

DMZ in Cloud, Hybrid, and Zero Trust Contexts

- Zero trust reframes the DMZ: identity, least privilege, per-session verification
- Stack topology-defined controls (zones, subnets) with connection-defined controls
- Cloud equivalents: VPCs, public/private subnets, WAFs, API gateways, private link
- Hybrid designs link on-premises DMZs to cloud and third-party services
- Zone-based thinking still matters in 2026 as enforcement shifts to policy engines



Operational Practices: Hardening, Patching, and Rule Hygiene

1. Hardened DMZ Host

2. Patch Cadence

Public-facing and crypto services → **Faster cycles**

Standard services → Standard cycles

3. Firewall Rule Card

Owner | Business Justification | Review Date | Expiration | Re-certification

- Harden DMZ hosts: minimal packages, only required services, no dev tools or default accounts
- Patch public-facing and crypto services faster than standard cycles—they are first targets
- **Rule hygiene:** owner, business justification, review date, expiration, and re-certification
- Configuration drift: temporary test rules can persist for years without regular firewall audits
- Validate with controlled scans, authorized pen tests, and internal pivot tests

Host-Placement Ledger: What Belongs in the DMZ vs. What Must Never Be There

Belongs in the DMZ

Web servers

Mail gateways

Public DNS

Must Never Be in the DMZ

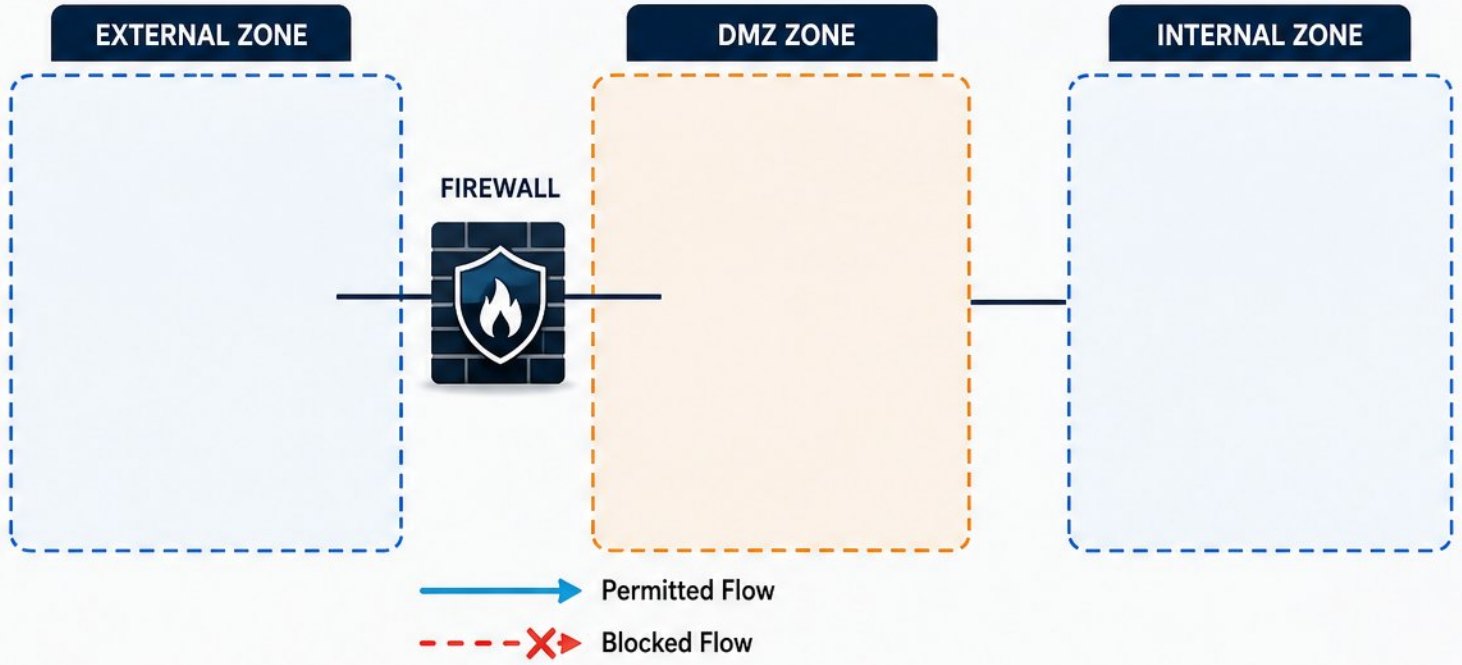
Databases

Internal applications

Directory services

Hands-On Lab: Designing and Verifying a Small DMZ

- **Goal:** design a small DMZ with firewall, web server, and internal database
- **Tasks:** define zones, write allow/deny rules, map traffic matrix
- **Verify:** test external, DMZ, and internal connectivity paths
- **Tools:** Packet Tracer, GNS3, Linux netfilter, or cloud simulators
- **Watch for:** missing implicit deny, overly broad rules, untested denied paths



TRAFFIC MATRIX (MAP ALLOW/DENY)

Source \ Destination	External Zone	DMZ Zone	Internal Zone
External Zone			
DMZ Zone			
Internal Zone			

RULES (WRITE ALLOW / DENY RULES)

ALLOWED RULES	DENIED RULES

TEST VIEWPOINTS & RESULTS

External Viewpoint	
DMZ Viewpoint	
Internal Viewpoint	

1 Define Zones → 2 Write Rules → 3 Place Services → 4 Test Connectivity

Key Takeaways and Review Questions

UNTRUSTED ZONE	SEMI-TRUSTED ZONE (DMZ)	TRUSTED ZONE
Internet	Controlled Access	Internal Network

- DMZ is a design pattern, not a product: controlled separation, not absolute security
- Core principles: default deny, least privilege, explicit flows, monitoring, change control
- Never in the DMZ: sensitive databases, directory services, backup controllers
- Review: Why is the DMZ semi-trusted? How does zero trust change it?
- Next steps: audit a network, draft a flow matrix, fix placements

CORE PRINCIPLES

DEFAULT DENY
Block by default. Allow only what is required.

LEAST PRIVILEGE
Give users and systems only the access they need.

MONITOR AND CHANGE-CONTROL
Continuously monitor and control changes with discipline.

NEVER IN THE DMZ

- Sensitive Databases
- Directory Services
- Backup Controllers

REVIEW QUESTIONS

- Why is the DMZ semi-trusted?
- How does dual-firewall separation support the DMZ design?
- How does zero trust change the DMZ model and access approach?

NEXT STEPS

audit a network, draft a flow matrix, fix placements

PersonWise.

PersonWise • AI digital-human course platform

Scan the code or click anywhere to watch this course live, with voice Q&A

personwise.ai/t/3bf03fef/public