Standards Mapping

What this means

This shows how my new network design follows well-known security rules from **NIST CSF** and **CIS Controls**.
Basically, it proves my setup uses the same safety ideas real companies use: limit access, split up networks, and block what's not needed.

🔹 NIST Cybersecurity Framework (CSF)

NIST Rule / ID	What it says	How my design follows it
PR.AC-3 – Least Privilege	Only give systems the access they need.	ACLs only let the web server talk to the database on one port.
PR.AC-5 – Network Segmentation	Split the network into smaller zones.	I made DMZ, Trusted, and Front Desk VLANs to stop attacks from spreading.
PR.PT-4 – Communication Protection	Control traffic between parts of the network.	The router/firewall blocks or allows traffic based on set rules.
DE.CM-7 – Monitor Connections	Watch for anything that breaks the rules.	Denied pings or failed connections show someone tried something blocked.

🔹 CIS Critical Security Controls

CIS Control #	What it means	How it shows up in my setup
4 – Admin Privileges	Keep admin access limited.	Only the jump-host in Trusted VLAN can do admin tasks.
12 – Network Management	Keep your network setup documented and controlled.	ACLs and VLANs are planned and written down clearly.
13 – Network Monitoring	Watch traffic and block bad stuff.	Default-deny ACLs make any strange traffic easy to see.

3 – Data Protection	Keep private data separate from public systems.	Database is in Trusted VLAN, away from Internet and user PCs.

In one line

> This setup follows security best practices: it limits who can talk to what, separates important systems, and blocks anything that doesn’t belong.
