Source	Destination	Action	Business Justification	Risk if Misconfigured
Internet	Web Server (DMZ, 192.168.10.10)	**ALLOW** TCP 80, 443	Public website must be reachable.	Allowing more than 80/443 widens attack surface; blocking breaks availability.
Internet	Database (Trusted, 192.168.20.10)	**DENY** all	DB is a crown-jewel; never exposed to Internet.	Direct exposure → data breach / RCE on DB.
Web Server (DMZ, 192.168.10.10)	Database (Trusted, 192.168.20.10)	**ALLOW** TCP 3306 (single host→host)	Backend app needs DB on one port from one source (least privilege).	Over-allowing (any→DB, many ports) enables lateral movement & exfiltration.
Front Desk VLAN (192.168.30.0/24)	Database (Trusted, 192.168.20.0/24)	**DENY** all	Users don't require DB access.	If allowed, phished PCs can reach sensitive data.
Trusted VLAN (192.168.20.0/24)	Web Server (DMZ)	**ALLOW** HTTP/HTTPS + narrow admin (as justified)	Ops/QA, updates via jump host.	If fully blocked, maintenance breaks; if too open, unnecessary DMZ exposure.
Any other host	Database (Trusted, 192.168.20.10)	**DENY** all	Enforce least privilege to crown jewels.	Misallowing gives attackers a pivot into DB.
Any	Any (inter-VLAN not explicitly listed)	**DENY** (default)	Default-deny at boundaries controls blast radius.	Without default-deny, flat-network risks (worms/ransomware spread).