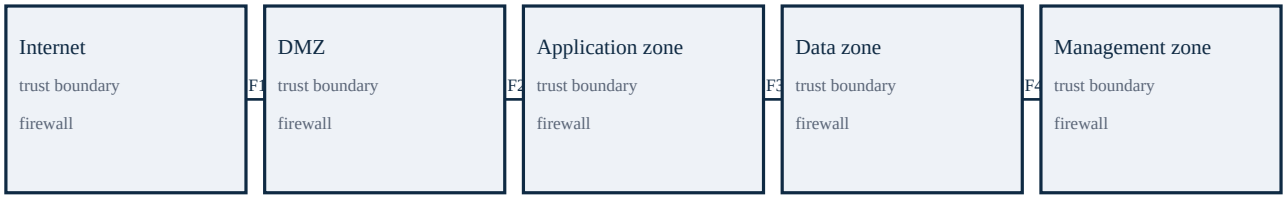
Network Architecture & Data Flow Diagram — Payments Switch

Architecture diagram · data flow diagram · synthetic assessor-grade test document

Diagram ID	SOU-DGM-0211
System	Payments Switch
Owner	Priya Sharma (Chief Information Security Officer)
Version	2.1
Last reviewed	25 Sep 2026
Status	Current — reflects production topology

1. Diagram



Arrows are data flows (see section 3); every boundary crossing is a firewall or identity control point.

2. Zones and trust boundaries

Zone	Contents and boundary control
Internet	Untrusted; DDoS protection, WAF
DMZ	Reverse proxies, API gateway, DNS
Application zone	Payments Switch application tier
Data zone	Databases, key management, backups
Management zone	Jump hosts, PAM, monitoring, out-of-band

3. Data flows

Flow	Source -> destination	Data	Protocol / encryption	Controls at the boundary
F1	Internet -> DMZ	Customer HTTPS traffic	TLS 1.3	Next-generation firewall, WAF, DDoS mitigation, intrusion prevention
F2	DMZ -> Application zone	API calls via gateway	mTLS	Firewall default-deny, network segmentation, API authentication
F3	Application zone -> Data zone	Database queries	TLS 1.2+	Firewall rule per service/port, database authentication, encryption at rest
F4	Management zone -> All zones	Administrative access	SSH / RDP via jump host	Remote access with MFA, PAM session recording, VPN

Flow	Source -> destination	Data	Protocol / encryption	Controls at the boundary
F5	Partner gateway -> Payments zone	SWIFT / payments messages	IPsec VPN + mTLS	Dedicated network segment, allow-listed peers, boundary protection
F6	All zones -> SIEM	Firewall, DNS, network device and host logs	TLS syslog	Central logging, network traffic monitoring
F7	Corporate wireless -> Corporate	Staff Wi-Fi	WPA3-Enterprise	Wireless isolated from production; certificate authentication

4. Security controls shown

Control area	Implementation
Boundary protection	Firewalls between every zone, default-deny, rule review every six months
Network segmentation	Production, management and corporate networks segregated; payments zone isolated
Remote access	VPN with MFA terminating in the management zone; no direct administrative access from the internet
Network devices	Routers, gateways and firewalls hardened, configuration backed up, changes under change control
Monitoring	Network traffic and DNS logged to the SIEM; intrusion detection on ingress and egress

5. Control framework mapping

Framework	Indicative mapped controls
ASD ISM	Guidelines: Access, System hardening, Monitoring
Essential Eight	ML2 target
ISO/IEC 27001:2022	A.5.15, A.5.18, A.8.2, A.8.16, A.5.23
SOC 2 (TSC)	CC6.1, CC6.2, CC6.3, CC7.2
APRA CPS 234	Information security capability, Control testing, Incident notification

Maintained under change control; reviewed after every material network or identity change and at least annually. Source: enterprise architecture repository (system context and network topology views).