Southern Mutual Bank

51 824 753 556

Firewall Rule Review — Core Banking (Temenos T24) — Q2 2026

Register · synthetic assessor-grade test document

Generated 09 November 2026 · CyberSentien test harness · personalised to Southern Mutual Bank

Register ID	SOU-REG-0111
Version	1.1
Owner	Priya Sharma (Chief Information Security Officer)
Classification	Internal Use Only
Status	Maintained — current
Last reviewed	20 Oct 2026
Review cycle	Quarterly

1. Purpose

This register records the firewall rule review — core banking (temenos t24) — q2 2026 maintained by Southern Mutual Bank. It is reviewed on a defined cycle; overdue or expired entries are escalated to the accountable owner and the Executive Risk Committee. It is compiled from the firewall configuration export: each rule's settings, source and destination network segmentation zones and service were reviewed for boundary protection and least privilege.

2. Register entries

Rule	Source zone -> destination zone	Service / port	Business owner	Review decision	Change ref
FW-1000	DMZ -> Application zone	TCP/443 HTTPS	Mei-Lin Tan	Retain — firewall rule justified	CHG-208200
FW-1003	DMZ -> Application zone	TCP/443 HTTPS	Priya Sharma	Retain — firewall rule justified	CHG-208201
FW-1006	Partner gateway -> SWIFT zone	ANY (legacy)	James O'Connor	Retain — firewall rule justified	CHG-208202
FW-1009	Management -> Any	TCP/22 SSH	David Okafor	REMOVE — overly permissive, no business owner	CHG-208203
FW-1012	Partner gateway -> SWIFT zone	TCP/22 SSH	Tom Bauer	Retain — firewall rule justified	CHG-208204
FW-1015	DMZ -> Application zone	TCP/22 SSH	Aisha Khan	Retain — firewall rule justified	CHG-208205

Rule	Source zone -> destination zone	Service / port	Business owner	Review decision	Change ref
FW-1018	Corporate -> Payments zone	TCP/8443 API gateway	Laura Mendez	Retain — firewall rule justified	CHG-208206
FW-1021	Internet -> DMZ	TCP/443 HTTPS	Daniel Wright	Tighten — restrict source to network segmentation zone	CHG-208207
FW-1024	Partner gateway -> SWIFT zone	TCP/443 HTTPS	Nadia Petrova	Retain — firewall rule justified	CHG-208208
FW-1027	Partner gateway -> SWIFT zone	ANY (legacy)	Greg Thompson	Retain — firewall rule justified	CHG-208209
FW-1030	Remote access VPN -> Corporate	TCP/8443 API gateway	Mei-Lin Tan	Retain — firewall rule justified	CHG-208210
FW-1033	Corporate -> Payments zone	TCP/1433 database	Priya Sharma	Retain — firewall rule justified	CHG-208211
FW-1036	Corporate -> Payments zone	UDP/53 DNS	James O'Connor	REMOVE — overly permissive, no business owner	CHG-208212
FW-1039	Corporate -> Payments zone	ANY (legacy)	David Okafor	Retain — firewall rule justified	CHG-208213
FW-1042	DMZ -> Application zone	TCP/443 HTTPS	Tom Bauer	Retain — firewall rule justified	CHG-208214
FW-1045	Corporate -> Payments zone	ANY (legacy)	Aisha Khan	Retain — firewall rule justified	CHG-208215
FW-1048	Internet -> DMZ	TCP/22 SSH	Laura Mendez	Retain — firewall rule justified	CHG-208216
FW-1051	Management -> Any	ANY (legacy)	Daniel Wright	Retain — firewall rule justified	CHG-208217

3. 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