Palo Alto Firewall Policy Review - CIS Controls Mapping

#	Issue Category	Example Findings	Remediation Action	Related CIS Controls	Review Frequency
1	Over-Permissive Rules	Rules with source:any, dest:any, service:any	Restrict rules; use App-ID	CIS 11.3, 12.3, 9.1	Monthly
2	Shadowed Rules	Rules with zero hits due to prior broader rule	Reorder rules; remove unused	CIS 11.2, 12.1	Quarterly
3	Redundant Rules	Duplicate/overlapping rules	Consolidate or merge	CIS 11.2, 12.5	Quarterly
4	Insecure Ports/Protocols	Telnet, FTP, SMBv1, RDP unnecessarily open	Remove; use SSH/SFTP	CIS 9.2, 12.2	Monthly
5	Risky Applications	Remote admin tools like TeamViewer, TOR	Block/monitor; use App-ID	CIS 11.3, 12.7	Monthly
6	Any-Any Temporary Rules	Temporary 'Allow All' rules left in place	Tag & remove after use	CIS 11.2, 12.5	Monthly
7	Lack of Least Privilege	Broad access across zones	Use User-ID; restrict groups	CIS 14.1, 11.4	Quarterly
8	Unused Rules	Rules with 0 hits	Disable/remove after validation	CIS 11.2, 12.5	Quarterly
9	No Logging Enabled	No 'Log at Session End'	Enable logging; forward to SIEM	CIS 6.2, 12.6	Monthly
10	No Rule Documentation	Missing owner/description	Add purpose & owner	CIS 11.1, 12.5	Quarterly
11	Stale Objects	Unused address/service objects	Remove/cleanup objects	CIS 11.2, 12.4	Semi-annual
12	Open DMZ Segments	DMZ allows any-to-internal	Enforce Zero Trust segmentation	CIS 12.3, 14.1	Semi-annual
13	Unreviewed Policy Changes	No review/approval process	Implement change mgmt workflow	CIS 4.3, 12.5	Ongoing
14	No Automated Audit Reports	Manual review only	Integrate Panorama/Expedition	CIS 11.4, 12.7	Monthly
15	No Config Backup	No scheduled backups	Automate config backups securely	CIS 11.1, 12.7	Weekly