Detection Strategy for Weaken Encryption: Disable Crypto Hardware on Network Devices, Detection Strategy DET0494

Archived: 2026-04-05 12:40:08 UTC

AN1360

Defenders may observe attempts to disable dedicated crypto hardware on network devices, often visible through anomalous CLI commands, unexpected firmware or configuration updates, and degraded encryption performance. Suspicious indicators include commands that alter hardware acceleration settings (e.g., disabling AES-NI or crypto engines), modification of system image files, or logs showing fallback from hardware to software encryption. Network traffic analysis may also reveal a sudden downgrade in throughput or cipher negotiation behavior consistent with the absence of hardware acceleration.

Log Sources

Data Component	Name	Channel
Command Execution (DC0064)	networkdevice:cli	Execution of commands disabling crypto hardware acceleration (e.g., 'no crypto engine enable')
File Modification (DC0061)	networkdevice:config	Configuration changes referencing cryptographic hardware modules or disabling hardware acceleration
Network Traffic Content (DC0085)	NSM:Flow	Degraded encryption throughput or switch to weaker cipher suites compared to historical baselines

Mutable Elements

Field	Description
AuthorizedAdminAccounts	Defines trusted administrator accounts allowed to modify encryption hardware settings; deviations trigger alerts.
BaselineThroughput	Expected performance metrics with hardware acceleration enabled; drops may indicate tampering.
ApprovedFirmwareVersions	Whitelist of vendor-signed firmware versions; unexpected updates could signal malicious modification.
TimeWindow	Period of correlation between configuration change and observed traffic downgrade; tunable to reduce false positives.

Source: https://attack.mitre.org/detectionstrategies/DET0494#AN1360