Firewall Security Assessment

Prepared for **Acme Group (Sample)**

Device: demo-fw-edge-01 (paloalto, 11.1.0)

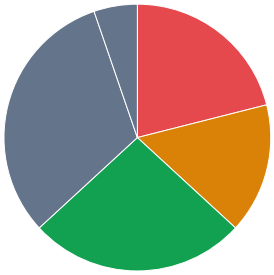
Assessment date: 22 September 2026

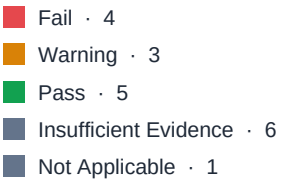
Contents

Executive Summary

This assessment evaluated **19 technical controls** against the exported configuration of **demo-fw-edge-01**. 4 control(s) failed, 3 carry warnings, and 6 could not be assessed from the offline export. The overall risk position is **High** (39/100 — lower is better).

Risk: High





Control status distribution

Key findings requiring attention:

• **No overly broad allow rules** (critical) — Broad allow rules: TEMP - broad outbound pending review.

• **Administrative password complexity** (high) — Password complexity is disabled.

• **Administrative lockout** (high) — Weak lockout on: Authentication profile lockout configured. (Authentication profile lockout configured: attempts=None, lockout=Nonem)

• **External threat intelligence blocking (EDL / IP Reputation)** (high) — No External Dynamic Lists (EDLs) are configured. Palo Alto threat intelligence feeds (panw-known-ip-list, panw-highrisk-ip-list, panw-bulletproof-ip-list) should be referenced in a deny policy.

• **Application-aware rule enforcement** (high) — Port-based rules: Allow approved SaaS, TEMP - broad outbound pending review.

Firewall Best Practice Assessment

Control	Status	Severity	Evidence & recommended action
BP-001 No overly broad allow rules	FAIL	critical	Broad allow rules: TEMP - broad outbound pending review. **Recommended action:** Replace broad rules with least-privilege rules scoped to named zones and addresses.
BP-002 Application-aware rule enforcement	WARNING	high	Port-based rules: Allow approved SaaS, TEMP - broad outbound pending review. **Recommended action:** Migrate port-based rules to application-aware definitions.
BP-003 Threat prevention profiles on allow rules	WARNING	high	Rules without profiles: TEMP - broad outbound pending review, Allow guest wifi internet. **Recommended action:** Attach a standard security profile group to every allow rule.
BP-004 Traffic logging at session end	PASS	medium	All 23 enabled allow rule(s) log at session end.
BP-005 Rule documentation	PASS	medium	All 23 enabled allow rule(s) are documented.
BP-006 No unused objects	WARNING	low	Unused objects: TCP-22. **Recommended action:** Remove unreferenced objects during scheduled housekeeping.

Control	Status	Severity	Evidence & recommended action
BP-007 No duplicate objects	PASS	low	No duplicate object values.
BP-008 Disabled rule housekeeping	PASS	info	No disabled rules retained.

Security Hardening Assessment

Control	Status	Severity	Evidence & recommended action
HD-001 Administrative password complexity	FAIL	high	Password complexity is disabled. **Recommended action:** Enable complexity with 12+ minimum length, 4 character classes, and history.
HD-002 Administrative lockout	FAIL	high	Weak lockout on: Authentication profile lockout configured. (Authentication profile lockout configured: attempts=None, lockout=Nonem) **Recommended action:** Set failed-attempts to 5 or fewer and lockout time to 15+ minutes.
HD-003 Management interface exposure	PASS	critical	Management access restricted to specific sources.
HD-004 Insecure management services disabled	INSUFFICIENT EVIDENCE	high	The required evidence was not present in the collected export.
HD-005 Time synchronisation configured	INSUFFICIENT EVIDENCE	medium	The required evidence was not present in the collected export.
HD-006 SNMP hardening	INSUFFICIENT EVIDENCE	high	The required evidence was not present in the collected export.
HD-007 Remote log forwarding	INSUFFICIENT EVIDENCE	medium	The required evidence was not present in the collected export.
HD-008 Administrative session timeout	INSUFFICIENT EVIDENCE	medium	The required evidence was not present in the collected export.
HD-009 Pre-login banner	INSUFFICIENT EVIDENCE	low	The required evidence was not present in the collected export.
TI-001 External threat intelligence blocking (EDL / IP Reputation)	FAIL	high	No External Dynamic Lists (EDLs) are configured. Palo Alto threat intelligence feeds (panw-known-ip-list, panw-highrisk-ip-list, panw-bulletproof-ip-list) should be referenced in a deny policy. **Recommended action:** PAN-OS: reference Palo Alto Threat Intelligence EDLs (panw-known-ip-list, panw-highrisk-ip-list, panw-bulletproof-ip-list) in a deny policy. FortiGate: enable FortiGuard IP Reputation in IPS profile and enable Botnet C&C; detection. Also consider KEV-derived IP block lists as supplementary feeds.

Certificate Assessment

Control	Status	Severity	Evidence & recommended action
CR-001 Certificate validity	NOT APPLICABLE	medium	No certificates present in the configuration.

Hardening Baseline Assessment

Assessed against the **SentryIQ Hardening Baseline v1.0**, built from vendor hardening guidance and NCSC network security principles.

Profile	Score	Met	Warning	Failed	Insufficient
Essential	**25%**	1	0	3	2
Hardened	**36%**	2	1	4	6

CVE Exposure Assessment

No advisory data was supplied, so vulnerability exposure was not assessed. Use 'Fetch Palo Alto feed' on the CVE page (or supply a local advisory JSON file) to enable this section.

Compliance scope: all supported frameworks — Cyber Essentials, PCI DSS v4.0, ISO/IEC 27001:2022, NCSC CAF.

Cyber Essentials Technical Control Assessment

Indicative readiness view derived from configuration evidence. This is not certification evidence, an IASME Cyber Essentials assessment, a PCI DSS QSA opinion, or evidence of ISO/IEC 27001 ISMS conformity. Controls marked 'manual' require organisational evidence outside the configuration export. NCSC CAF references are to contributing outcomes of the Cyber Assessment Framework (Crown copyright, Open Government Licence); this view supports but does not constitute a CAF self-assessment or audit.

Framework control	Status	Evidence
CE-FW-1 Default passwords changed / strong authentication	Gap	Password complexity is disabled.
CE-FW-2 Administrative interface not internet-accessible	Aligned	Management access restricted to specific sources.
CE-FW-3 Inbound connections blocked by default	Gap	Broad allow rules: TEMP - broad outbound pending review.
CE-FW-4 Rules documented with business justification	Aligned	All 23 enabled allow rule(s) are documented.
CE-MP-1 Malware protection applied to traffic	Attention	Rules without profiles: TEMP - broad outbound pending review, Allow guest wifi internet.
CE-MP-2 Malware protection — network-level blocking	Gap	No External Dynamic Lists (EDLs) are configured. Palo Alto threat intelligence feeds (panw-known-ip-list, panw-highrisk-ip-list, panw-bulletproof-ip-list) should be referenced in a deny policy.
CE-SC-1 Unnecessary rules and objects removed	Attention	Unused objects: TCP-22.
CE-SC-1 Unnecessary rules and objects removed	Aligned	No disabled rules retained.
CE-SC-2 Insecure services disabled	Manual	The required evidence was not present in the collected export.
CE-SC-3 Default credentials and services changed	Manual	The required evidence was not present in the collected export.

Framework control	Status	Evidence
CE-SU-1 Critical/high security updates applied within 14 days	Manual	No advisory data was loaded; provide a local or fetched advisory feed to assess patch exposure.
CE-UAC-1 Brute-force protection	Gap	Weak lockout on: Authentication profile lockout configured. (Authentication profile lockout configured: attempts=None, lockout=Nonem)

PCI DSS v4.0 Technical Control Assessment

Indicative readiness view derived from configuration evidence. This is not certification evidence, an IASME Cyber Essentials assessment, a PCI DSS QSA opinion, or evidence of ISO/IEC 27001 ISMS conformity. Controls marked 'manual' require organisational evidence outside the configuration export. NCSC CAF references are to contributing outcomes of the Cyber Assessment Framework (Crown copyright, Open Government Licence); this view supports but does not constitute a CAF self-assessment or audit.

Framework control	Status	Evidence
1.2.5 Ports/protocols/services approved and documented	Aligned	All 23 enabled allow rule(s) are documented.
1.2.6 Security features for insecure services	Attention	Port-based rules: Allow approved SaaS, TEMP - broad outbound pending review.
1.2.6/1.3 NSC rules restrict traffic	Gap	Broad allow rules: TEMP - broad outbound pending review.
10.2 Audit logs capture network decisions	Aligned	All 23 enabled allow rule(s) log at session end.
10.3.3 Audit logs backed up to central location	Manual	The required evidence was not present in the collected export.
10.6 Time-synchronisation mechanisms	Manual	The required evidence was not present in the collected export.
2.2 Secure configuration standards	Attention	Unused objects: TCP-22.
2.2 Secure configuration standards	Aligned	No duplicate object values.
2.2 Secure configuration standards	Manual	The required evidence was not present in the collected export.
2.2.7 Non-console administrative access encrypted	Manual	The required evidence was not present in the collected export.
6.3.1 Security vulnerabilities and threats addressed	Gap	No External Dynamic Lists (EDLs) are configured. Palo Alto threat intelligence feeds (panw-known-ip-list, panw-highrisk-ip-list, panw-bulletproof-ip-list) should be referenced in a deny policy.
6.3.3 Critical vulnerabilities patched within one month	Manual	No advisory data was loaded; provide a local or fetched advisory feed to assess patch exposure.
8.2.8 Idle session timeout (15 minutes)	Manual	The required evidence was not present in the collected export.
8.3.4 Account lockout	Gap	Weak lockout on: Authentication profile lockout configured. (Authentication profile lockout configured: attempts=None, lockout=Nonem)

Framework control	Status	Evidence
8.3.6 Password minimum length and complexity	Gap	Password complexity is disabled.

ISO/IEC 27001:2022 Technical Control Assessment

Indicative readiness view derived from configuration evidence. This is not certification evidence, an IASME Cyber Essentials assessment, a PCI DSS QSA opinion, or evidence of ISO/IEC 27001 ISMS conformity. Controls marked 'manual' require organisational evidence outside the configuration export. NCSC CAF references are to contributing outcomes of the Cyber Assessment Framework (Crown copyright, Open Government Licence); this view supports but does not constitute a CAF self-assessment or audit.

Framework control	Status	Evidence
A.5.15 Access control	Aligned	Management access restricted to specific sources.
A.5.15 Access control	Manual	The required evidence was not present in the collected export.
A.5.17 Authentication information	Gap	Password complexity is disabled.
A.8.15 Logging	Aligned	All 23 enabled allow rule(s) log at session end.
A.8.15 Logging	Manual	The required evidence was not present in the collected export.
A.8.17 Clock synchronisation	Manual	The required evidence was not present in the collected export.
A.8.20 Networks security	Gap	Broad allow rules: TEMP - broad outbound pending review.
A.8.20 Networks security	Attention	Port-based rules: Allow approved SaaS, TEMP - broad outbound pending review.
A.8.20 Networks security	Manual	The required evidence was not present in the collected export.
A.8.21 Security of network services	Aligned	All 23 enabled allow rule(s) are documented.
A.8.22 Segregation of networks	Gap	Rulebase analysis of 24 rule(s): 2 shadowed (dead), 3 redundant, 2 consolidation group(s) covering 5 rule(s).
A.8.5 Secure authentication	Gap	Weak lockout on: Authentication profile lockout configured. (Authentication profile lockout configured: attempts=None, lockout=Nonem)
A.8.5 Secure authentication	Manual	The required evidence was not present in the collected export.
A.8.7 Protection against malware	Gap	No External Dynamic Lists (EDLs) are configured. Palo Alto threat intelligence feeds (panw-known-ip-list, panw-highrisk-ip-list, panw-bulletproof-ip-list) should be referenced in a deny policy.
A.8.8 Management of technical vulnerabilities	Manual	No advisory data was loaded; provide a local or fetched advisory feed to assess patch exposure.
A.8.9 Configuration management	Attention	Unused objects: TCP-22.
A.8.9 Configuration management	Aligned	No duplicate object values.

Framework control	Status	Evidence
A.8.9 Configuration management	Aligned	No disabled rules retained.
A.8.9 Configuration management	Manual	The required evidence was not present in the collected export.

NCSC CAF Technical Control Assessment

Indicative readiness view derived from configuration evidence. This is not certification evidence, an IASME Cyber Essentials assessment, a PCI DSS QSA opinion, or evidence of ISO/IEC 27001 ISMS conformity. Controls marked 'manual' require organisational evidence outside the configuration export. NCSC CAF references are to contributing outcomes of the Cyber Assessment Framework (Crown copyright, Open Government Licence); this view supports but does not constitute a CAF self-assessment or audit.

Framework control	Status	Evidence
B2.a Identity verification and authentication	Gap	Password complexity is disabled.
B2.a Identity verification and authentication	Gap	Weak lockout on: Authentication profile lockout configured. (Authentication profile lockout configured: attempts=None, lockout=Nonem)
B2.a Identity verification and authentication	Manual	The required evidence was not present in the collected export.
B2.c Privileged user management	Aligned	Management access restricted to specific sources.
B2.c Privileged user management	Manual	The required evidence was not present in the collected export.
B4.a Secure by design	Gap	Broad allow rules: TEMP - broad outbound pending review.
B4.a Secure by design	Attention	Unused objects: TCP-22.
B4.a Secure by design	Aligned	No disabled rules retained.
B4.a Secure by design	Gap	Rulebase analysis of 24 rule(s): 2 shadowed (dead), 3 redundant, 2 consolidation group(s) covering 5 rule(s).
B4.b Secure configuration	Gap	Broad allow rules: TEMP - broad outbound pending review.
B4.b Secure configuration	Attention	Port-based rules: Allow approved SaaS, TEMP - broad outbound pending review.
B4.b Secure configuration	Aligned	All 23 enabled allow rule(s) are documented.
B4.b Secure configuration	Attention	Unused objects: TCP-22.
B4.b Secure configuration	Aligned	No duplicate object values.
B4.b Secure configuration	Aligned	No disabled rules retained.
B4.b Secure configuration	Manual	The required evidence was not present in the collected export.
B4.c Secure management	Manual	The required evidence was not present in the collected export.

Framework control	Status	Evidence
B4.d Vulnerability management	Gap	No External Dynamic Lists (EDLs) are configured. Palo Alto threat intelligence feeds (panw-known-ip-list, panw-highrisk-ip-list, panw-bulletproof-ip-list) should be referenced in a deny policy.
C1.a Monitoring coverage	Attention	Rules without profiles: TEMP - broad outbound pending review, Allow guest wifi internet.
C1.a Monitoring coverage	Aligned	All 23 enabled allow rule(s) log at session end.
C1.b Securing logs	Manual	The required evidence was not present in the collected export.
C1.b Securing logs	Manual	The required evidence was not present in the collected export.
C1.c Generating alerts	Aligned	All 23 enabled allow rule(s) log at session end.
C1.c Generating alerts	Manual	The required evidence was not present in the collected export.
C2.a Threat intelligence	Gap	No External Dynamic Lists (EDLs) are configured. Palo Alto threat intelligence feeds (panw-known-ip-list, panw-highrisk-ip-list, panw-bulletproof-ip-list) should be referenced in a deny policy.

Contributing outcomes evidenced from configuration

Outcome	Class	Status	Basis
B2.a Identity verification and authentication	evidence	gap	Password policy, administrative lockout and idle session timeout are read directly from device configuration.
B2.c Privileged user management	evidence	aligned	Management-plane exposure and pre-logon banner configuration evidence how privileged access to the device is constrained.
B3.a Understanding data / protection in transit	contributes	no configuration evidence	Certificate validity evidences transport protection on the device; wider data-flow protection requires organisational evidence.
B4.a Secure by design	evidence	gap	Rulebase analysis (overly broad rules, shadowed/redundant rules, unused objects) evidences whether the perimeter is designed on least-privilege, minimised lines — distinct from B4.b point checks.
B4.b Secure configuration	evidence	gap	Per-control configuration checks across rulebase hygiene, SNMP hardening and service configuration.
B4.c Secure management	evidence	manual	Insecure management services (telnet/HTTP) and encrypted administrative access are read from configuration.
B4.d Vulnerability management	contributes	gap	Threat-prevention configuration plus CVE/advisory exposure of the running version against vendor advisory data. The organisational patch process itself is not evidenced.
C1.a Monitoring coverage	evidence	attention	Security profile attachment and session logging on rules evidence whether traffic decisions are observable.
C1.b Securing logs	evidence	manual	Remote log forwarding and time synchronisation evidence log integrity and off-device retention.
C1.c Generating alerts	contributes	aligned	Session logging and syslog forwarding show alert-capable telemetry is produced and exported; alert triage rules and SOC handling are organisational.

Outcome	Class	Status	Basis
C2.a Threat intelligence	contributes	gap	External dynamic lists, IP reputation and botnet protection configuration evidence threat-intelligence ingestion at the perimeter. Feed sourcing and analysis process are organisational.
C2.b Proactive security event discovery	contributes	no configuration evidence	Threat log analysis evidences whether detected events are acted upon — threats allowed through after detection, and sensors left in monitor mode. Only populated when threat logs are supplied alongside the configuration; hunting and triage process are organisational.

Outcomes not evidenced from configuration

Area	Why it is out of scope for this assessment
Objective A (Managing security risk)	Governance, risk management, asset management and supply chain are organisational outcomes; firewall configuration cannot evidence them.
Objective B — outcomes beyond those listed	Data security, staff awareness and physical/personnel controls require organisational evidence outside a configuration export.
Objective C — C1.d, C1.e	Incident identification and analysis are process outcomes requiring organisational evidence. C2.b is evidenced only when threat-log data is supplied alongside the configuration.
Objective D (Minimising the impact of incidents)	Response, recovery and lessons-learned are entirely organisational; no configuration evidence applies.

Recommended Remediation

1. No overly broad allow rules (critical, FAIL)
Replace broad rules with least-privilege rules scoped to named zones and addresses.

2. Administrative password complexity (high, FAIL)
Enable complexity with 12+ minimum length, 4 character classes, and history.

3. Administrative lockout (high, FAIL)
Set failed-attempts to 5 or fewer and lockout time to 15+ minutes.

4. External threat intelligence blocking (EDL / IP Reputation) (high, FAIL)
PAN-OS: reference Palo Alto Threat Intelligence EDLs (panw-known-ip-list, panw-highrisk-ip-list, panw-bulletproof-ip-list) in a deny policy. FortiGate: enable FortiGuard IP Reputation in IPS profile and enable Botnet C&C; detection. Also consider KEV-derived IP block lists as supplementary feeds.

5. Application-aware rule enforcement (high, WARNING)
Migrate port-based rules to application-aware definitions.

6. Threat prevention profiles on allow rules (high, WARNING)
Attach a standard security profile group to every allow rule.

7. No unused objects (low, WARNING)
Remove unreferenced objects during scheduled housekeeping.

CAB Summary

Proposed changes: 7 remediation item(s) across 2 area(s). Each item includes evidence and remediation suitable for change justification. Insufficient-evidence controls (6) require additional exports before assessment.

Rulebase Optimisation

Analysed 24 rule(s): **2 shadowed** (dead — can never take effect), 3 redundant, 2 partially overlapped, 2 consolidation group(s).

Rule	Finding	Covered by / merges with	Detail
Allow Windows Update	PARTIAL (review)	Allow ops-team to app tier, Allow dev-team to app tier, Allow qa-team to app tier, Allow finance-team to app tier, Allow corp users to dc-web-01, Allow corp users to dc-web-02, Allow corp users to dc-web-03	Partially overlapped by earlier rule(s) Allow ops-team to app tier, Allow dev-team to app tier, Allow qa-team to app tier, Allow finance-team to app tier, Allow corp users to dc-web-01, Allow corp users to dc-web-02, Allow corp users to dc-web-03; review whether the intended traffic is fully served.
Allow approved SaaS	PARTIAL	Allow ops-team to app tier, Allow dev-team to app tier, Allow qa-team to app tier, Allow finance-team to app tier, Allow corp users to dc-web-01, Allow corp users to dc-web-02, Allow corp users to dc-web-03, Allow syslog to SIEM, Allow NTP sync	Partially overlapped by earlier rule(s) Allow ops-team to app tier, Allow dev-team to app tier, Allow qa-team to app tier, Allow finance-team to app tier, Allow corp users to dc-web-01, Allow corp users to dc-web-02, Allow corp users to dc-web-03, Allow syslog to SIEM, Allow NTP sync; review whether the intended traffic is fully served.
Allow guest wifi internet	REDUNDANT (review)	TEMP - broad outbound pending review	Fully covered by earlier rule(s) with the same action ('allow'); this rule is unnecessary. Why (TEMP - broad outbound pending review): source any covers guest-wifi (192.168.50.0/24); destination identical (any); application any covers web-browsing/ssl; service any covers application-default.
Allow corp to app tier duplicate	REDUNDANT (review)	TEMP - broad outbound pending review	Fully covered by earlier rule(s) with the same action ('allow'); this rule is unnecessary. Why (TEMP - broad outbound pending review): source any covers corp-users (10.10.0.0/16); destination any covers dc-app-01 (10.30.2.10/32); application any covers ssl; service any covers application-default.
Allow backup traffic	REDUNDANT	TEMP - broad outbound pending review	Fully covered by earlier rule(s) with the same action ('allow'); this rule is unnecessary. Why (TEMP - broad outbound pending review): source any covers backup-targets (10.99.5.0/24); destination any covers dc-db-cluster (10.30.3.0/24); application any covers ms-sql-db; service any covers TCP-1433.
Deny all and log	SHADOWED	TEMP - broad outbound pending review	Match space fully covered by earlier rule(s) TEMP - broad outbound pending review with a different action; this rule can never take effect. Why (TEMP - broad outbound pending review): source identical (any); destination identical (any); application any covers any; service any covers any.
Allow RDP to app tier	SHADOWED	Deny all and log	Match space fully covered by earlier rule(s) Deny all and log with a different action; this rule can never take effect. Why (Deny all and log): source any covers mgmt-jumphosts (10.99.1.0/24); destination any covers dc-app-01 (10.30.2.10/32); application any covers ms-rdp; service any covers TCP-3389.
Allow ops-team to app tier	MERGEABLE (review)	Allow dev-team to app tier, Allow qa-team to app tier, Allow finance-team to app tier	4 rules are identical except for source; they can be consolidated into one rule with source = [dev-team, finance-team, ops-team, qa-team]. Shared identity: destination [dc-app-01]; application [ssl]; service [application-default]; action allow.

Rule	Finding	Covered by / merges with	Detail
Allow corp users to dc-web-01	MERGEABLE (review)	Allow corp users to dc-web-02, Allow corp users to dc-web-03	3 rules are identical except for destination; they can be consolidated into one rule with destination = [dc-web-01, dc-web-02, dc-web-03]. Shared identity: source [corp-users]; application [ssl, web-browsing]; service [application-default]; action allow.

Note: 'TEMP - broad outbound pending review' matches any/any/any/any/any and trivially overlaps all 18 preceding rule(s) — expected for a catch-all/default-deny rule, so it was not listed as an individual PARTIAL finding.

Note: Some rules use PAN-OS container applications (e.g. web-browsing, ssl). Application hierarchy is not fully modelled, so findings marked 'review' should be verified against App-ID dependencies.

Assessment Scope — Checks Performed

Every control evaluated in this assessment, its category, and what was checked. Controls returning INSUFFICIENT EVIDENCE indicate the exported configuration did not carry the required evidence; they are never silently marked as passed.

Control	Category	What is checked	Why it matters
BP-001 No overly broad allow rules	best practice	Enabled allow rules must not permit any-source to any-destination traffic.	Any/any rules defeat segmentation and allow lateral movement.
BP-002 Application-aware rule enforcement	best practice	Allow rules should use application identification rather than raw ports.	Port-based rules permit any protocol on the port, including tunnelled threats.
BP-003 Threat prevention profiles on allow rules	best practice	Every enabled allow rule should carry security/threat prevention profiles.	Unprofiled allow rules pass traffic with no inspection.
BP-004 Traffic logging at session end	best practice	Allow rules should log at session end for audit and incident response.	Without session logging, investigations and audits lack traffic evidence.
BP-005 Rule documentation	best practice	Every rule should carry a description with business justification.	Undocumented rules cannot be reviewed, owned, or safely retired.
BP-006 No unused objects	best practice	Address and service objects should be referenced or removed.	Unused objects accumulate risk of accidental reuse and obscure review.
BP-007 No duplicate objects	best practice	Object values should not be duplicated under different names.	Duplicates cause drift: one copy gets updated, the other stays stale.
BP-008 Disabled rule housekeeping	best practice	Disabled rules should be retired once their retention window passes.	Retained disabled rules bloat review scope and risk accidental re-enablement.
HD-001 Administrative password complexity	hardening	Password complexity must be enforced for administrative accounts.	Weak administrative passwords are the primary brute-force target on edge devices.
HD-002 Administrative lockout	hardening	Authentication profiles must lock accounts after repeated failures.	Without lockout, administrative interfaces can be brute-forced indefinitely.
HD-003 Management interface exposure	hardening	The management plane must not be reachable from broad or untrusted networks.	Exposed management interfaces are the leading exploitation path on edge devices.

Control	Category	What is checked	Why it matters
CR-001 Certificate validity	certificates	Certificates in the configuration must be valid and not near expiry.	Expired certificates break VPN/decryption services and erode user trust in warnings.
HD-004 Insecure management services disabled	hardening	Cleartext management services (Telnet, HTTP) must be disabled on all interfaces.	Cleartext management sessions expose credentials to interception on any network path.
HD-005 Time synchronisation configured	hardening	The device must synchronise its clock with at least one NTP source.	Without accurate time, logs cannot be correlated across devices and lose evidential value in investigations.
HD-006 SNMP hardening	hardening	SNMP v1/v2c community strings must not be in use, especially defaults.	Community strings transit in cleartext and act as shared passwords; defaults like 'public' allow device reconnaissance by anyone on the path.
HD-007 Remote log forwarding	hardening	Device logs must be forwarded to remote, centralised storage.	Logs kept only on the device are lost on failure and can be erased by an attacker with device access.
HD-008 Administrative session timeout	hardening	Idle administrative sessions must time out within 15 minutes.	Unattended authenticated sessions allow opportunistic takeover of the management plane.
HD-009 Pre-login banner	hardening	A pre-login banner should state that access is restricted and monitored.	Absence of a warning banner can weaken the legal position when pursuing unauthorised access.
TI-001 External threat intelligence blocking (EDL / IP Reputation)	hardening	Firewall policy should reference current threat intelligence feeds to block known malicious sources and destinations without manual intervention.	Without automated threat intelligence, known command-and-control infrastructure, malicious hosting, and active exploit sources can freely traverse the firewall.

Technical Appendix

Collector: paloalto · Model schema: v1.1 · Controls evaluated: 19 · Source: demo_estate.xml · Generated: 2026-09-22 10:19 UTC