SYMBEEO

PUBLIC

TEST PLAN AND ACCEPTANCE RECORD

Test plan for SDD-SEC-001 against the requirements, failure conditions and use cases of SRA-SEC-001

Test document — plan complete; results are recorded at acceptance

CAPABILITY	DOCUMENT	VERSION	DATE
Security	STP-SEC-001	1.5	Oct 10, 2026

WRITTEN BY

David Morgan, Principal Security Architect

© 2026 Symbeeo. All rights reserved.

Document control

Document	STP-SEC-001	Version	1.5
Issued	Oct 10, 2026	Status	Issued by Symbeeo
Classification	Public	Supersedes	1.4, Oct 7, 2026
Capability	Security	Author	David Morgan
Role	Principal Security Architect		
Tests	SRA-SEC-001 R2–R12 (R1 is an input; R12's use cases are T5–T9) and F1–F5, F7 (F6 applies to Model B only) NIST SP 1800-35 functional demonstrations SDD-SEC-001 migration step 3 (T19) and step 5 (T6, T8, T9)		
Credentials	CCISO, CISSP, CISSP-ISSEP, CISM, CISA, CRISC, PMP, CCSP, Adopting Zero Trust (Forrester)		
Approval	Approved by Edwin Ozer, Founder, Oct 10, 2026. Issued by Symbeeo, Oct 10, 2026.		
Sign-off	"The customer's named acceptor signs the results; the practice lead countersigns. Acceptance = every T-case marked pass or waived with a reason."		

Contents

1 · Scope, environment, entry and exit 3

2 · Test cases 3

3 · Validated components and versions 6

4 · Acceptance record 7

© 2026 Symbeeo. All rights reserved. · Public

> CONVENTIONS
>
> Structure follows NIST SP 1800-35 §6, functional demonstrations: a methodology, then use cases run against the build. Use case A (discovery and identification) and the lateral-movement case are mandatory; the others are run where the client's scope includes them. Results are recorded at acceptance.

Table 1. Revision history

Date	Version	Change
Sep 15, 2026	1.0	First issue.
Sep 21, 2026	1.1	Corrections to wording, figure numbering and citations.
Sep 27, 2026	1.2	Revised to current platform versions and the current document format.
Sep 29, 2026	1.3	Reissued with the practice set; no change.
Oct 7, 2026	1.4	Reissued with the practice set; no change.
Oct 10, 2026	1.5	Approval line now reads: approved by the Founder, issued by Symbeeo. David Morgan remains the author.

1 · Scope, environment, entry and exit

Scope. Policy engine, enforcement points, identity, posture, certificates, logging, in Model A. **Environment.** HQ first in monitor mode, then enforcement; branches after. **Entry.** SDD-SEC-001 signed; P1–P7 closed; SDD-NET-001 access layer in service. **Exit.** All mandatory use cases pass; every failure condition tested; evidence archived.

2 · Test cases

Table 2. Test cases

ID	Tests	Method	Pass criterion	Evidence it produces	Result	Evidence captured	Date · initials
T1	R2 identity sources	authenticate a domain user and a certificate-only device	sequence certificate → AD works; unknown denied	log extract: ISE live-authentication entries for the user, the device and the denied unknown; eapol_test output	☐ pass ☐ fail		
T2	R5 policy-engine sizing	load 5,000 endpoints in monitor mode	no dropped authentications; latency within guide	load-generator report (requests, failures, latency); screenshot of the ISE deployment health view	☐ pass ☐ fail		
T3	R8 certificates	auto-enroll a managed device; check chain on the client	device certificate issued; EAP-TLS succeeds	screenshot of the device certificate and its chain; log extract of the EAP-TLS authentication	☐ pass ☐ fail		

© 2026 Symbeeo. All rights reserved. · Public

ID	Tests	Method	Pass criterion	Evidence it produces	Result	Evidence captured	Date · initials
T4	R3 MFA	attempt admin access to an enforcement point without MFA	denied	log extract: denied admin login on the PA-5570, the FortiGate and ISE; screenshot of the MFA prompt on a permitted login	☐ pass ☐ fail		
T5	R4 device classes · R12 use case A · discovery and identification	plug in each device class; read profiler results	managed, BYOD and OT correctly classified	screenshot of the ISE endpoint view per device class; log extract of the profiler result	☐ pass ☐ fail		
T6	R4 posture rule per class · R12 use case · policy enforcement	matrix rows 1–6 of SDD-SEC-001 §4.2	each identity lands in its SGT and VLAN	log extract: authorization result, SGT and VLAN per matrix row; switch session output per port	☐ pass ☐ fail		
T7	R12 use case · posture	put a managed device out of compliance	moved to quarantine; remediation reachable; restored on compliance	log extract of the posture change and reauthorization, timestamped; MDM screenshot of the compliance state	☐ pass ☐ fail		
T8	R12 use case · least privilege	contractor attempts a non-listed application	blocked at core or DC NGFW; logged	NGFW traffic-log extract showing the deny with user and SGT	☐ pass ☐ fail		
T9	R12 use case · lateral movement	from an OT segment, attempt to reach the user segment and a DC server	blocked by SGT matrix and NGFW; alert in SIEM	NGFW and switch deny-log extracts; screenshot of the SIEM alert	☐ pass ☐ fail		
T10	R11 revocation	disable a user in AD	access lost ≤ 5 min	timing record: AD disable time against session-end time from the ISE log	☐ pass ☐ fail		
T11	R6 DC NGFW	throughput and TLS inspection test on the PA-5570 with post-quantum key exchange where supported	inspection active; throughput as designed [A]; ML-KEM hybrid group negotiated	traffic-generator report (throughput with threat prevention on); packet-capture extract of the TLS handshake showing the key-exchange group; NGFW decryption-log extract	☐ pass ☐ fail		
T12	R7 branch NGFW	threat-protection test at a branch	signatures fire; throughput as designed [A]	FortiGate IPS-log extract of the test signatures; traffic-generator report	☐ pass ☐ fail		

© 2026 Symbeeo. All rights reserved. · Public

ID	Tests	Method	Pass criterion	Evidence it produces	Result	Evidence captured	Date · initials
T13	R10 logging (proof that security logs reach the client's collector)	raise a test event on every source (ISE, PA-5570, FortiGate, access switch, MDM); verify each reaches the SIEM; check retention setting	100 % of event types visible at the client's collector within 60 s [A], with source name and timestamp; 12/24 months configured	screenshot of the SIEM search showing one event per source; screenshot of the retention setting	☐ pass ☐ fail		
T14	F1 policy-engine node down (failover test)	power off one ISE node (SNS-3895)	no user impact	failover timing from a client re-authentication log; ISE deployment-status log extract	☐ pass ☐ fail		
T15	F2, R9 policy-engine cluster down (failover test)	isolate both nodes	new sessions refused (R9); existing continue; restored within the restore time signed with P7 [A]	log extract: refused new sessions and surviving sessions, timestamped; restore timing record	☐ pass ☐ fail		
T16	F3 identity store unreachable	block AD	new auth fails; cached sessions continue; alert raised	log extract of the failed authentications; screenshot of the alert	☐ pass ☐ fail		
T17	F4, F5 NGFW member down (failover test)	power off one member of each pair	no session loss	failover timing from the traffic generator's loss count per pair; HA log extract from the survivor	☐ pass ☐ fail		
T18	F7 CA unreachable	block the CA	existing certificates valid; enrollment fails gracefully	log extract of the failed enrollment; EAP-TLS success log for an existing certificate	☐ pass ☐ fail		
T19	migration step 3	low-impact enforcement on one floor	no user complaints in one week; rollback tested	change log with timestamps for enforcement and rollback; the week's service-desk ticket count	☐ pass ☐ fail		
T20	Encryption in transit (SDD §3.2)	attempt Telnet, HTTP and SNMPv1/v2c to ISE, the PA-5570 and the FortiGate; read RADIUS/TLS status between access switches and ISE; capture the syslog stream to the SIEM	no clear-text management protocol answers; RADIUS carried over TLS; syslog to the SIEM over TLS [A]	log extract per device; packet-capture extract of the RADIUS and syslog streams showing TLS	☐ pass ☐ fail		

© 2026 Symbeeo. All rights reserved. · Public

ID	Tests	Method	Pass criterion	Evidence it produces	Result	Evidence captured	Date · initials
T21	Encryption at rest (SDD §8, §9)	take an ISE backup and try to restore it without its encryption key; export one configuration from each NGFW; inspect the evidence archive	restore without the key fails; no clear-text secret in any exported configuration (PAN-OS master key changed from default, FortiGate private-data encryption on) [A]; archive stored encrypted in the client's repository	log extract of the refused restore; redacted configuration extract of the secret lines per NGFW; screenshot of the archive's encryption setting	☐ pass ☐ fail		

3 · Validated components and versions

Planned software was read on Sep 24, 2026 and is read again on the day of staging. Software at test, serial and test result stay empty until the test runs: together they are the per-device quality record.

3.1 Devices and software

Table 3. Devices and software

Device	Model	Planned software, read Sep 24, 2026	Software at test	Serial	Test result	Validated in
	ISE nodes and roles: SNS-3895, primary admin + monitoring at DC-A, secondary at DC-B, policy service on both	ISE 3.5 Patch 4 [S]				T1–T7, T10, T13–T16, T20, T21
	PA-5570 (the PA-5450 is not used: end of sale Nov 22, 2026)	PAN-OS 12.1, maintenance release per Palo Alto's preferred-release guidance at staging [S]/[A]				T4, T8, T9, T11, T13, T17, T20, T21
	FortiGate 200G	FortiOS 7.6, build per Fortinet's recommended release at staging [A]				T4, T12, T13, T17, T20, T21
	Access switch software: Catalyst 9300X	IOS XE 17.18.4 [S]				T6, T8, T9, T13, T19, T20
	Certificate template and CA	client's CA, version recorded at staging [A]				T3, T18
	Matrix version: authorization matrix and SGT matrix	version number recorded at staging [A]				T6, T8, T9
	Client MDM/UEM and SIEM	the client's, versions recorded at staging [A]				T7, T13

Sources for the planned software: Cisco ISE 3.5 release notes (Patch 4, Sep 14, 2026), Palo Alto end-of-life summary (PAN-OS 12.1 to Aug 28, 2028), Cisco recommended IOS XE releases (page updated Sep 4, 2026); FortiOS from a secondary source because Fortinet's own page needs a login. URLs in SRA-SEC-001 §9.2.

© 2026 Symbeeo. All rights reserved. · Public

3.2 Test tools

Table 4. Test tools

Tool	Version	Used in
eapol_test (built from wpa_supplicant)	2.12, released Aug 7, 2026 [S] `https://w1.fi/releases/`, read Sep 24, 2026	T1, T3, T18
OpenSSL s_client, TLS client with ML-KEM	3.5.8 LTS, released Aug 25, 2026 (secondary source `https://endoflife.date/openssl`, read Sep 24, 2026)	T11, T20
Wireshark	4.6.16, released May 19, 2026 (secondary source `https://endoflife.date/wireshark`, read Sep 24, 2026)	T11, T20
iperf3	3.21, released Apr 9, 2026 [S] `https://github.com/esnet/iperf/releases`, read Sep 24, 2026	T12 (branch baseline)
Application-mix traffic generator	make, model and software version recorded when the kit is fixed [A]	T11, T12, T17
RADIUS load generator	product and version recorded when the kit is fixed [A]	T2
Test endpoints: managed laptop, BYOD phone, OT device	model and OS version recorded when the kit is fixed [A]	T3, T5–T7

A case run with a tool whose version is not recorded here is not evidence and is run again [A].

4 · Acceptance record

Table 5. Acceptance record

	Name	Role	Signature	Date
Client acceptor (security manager)				
Symbeeo test lead				
Symbeeo practice lead				

Waivers and open defects are recorded at acceptance.

Acceptance terms:

- **Acceptance is positive and signed.** It exists only when the client's named acceptor signs the table above. Silence, use of the system in production, or the passing of a deadline is never acceptance.
- **Review window.** The client has **10 business days** from delivery of the results to review them [A].
- **Fix window.** For any failed case, Symbeeo has **10 business days** to fix it, then the case is run again and the client has **one re-review** [A].
- **Warranty.** The warranty starts on the date of signed acceptance.

The 10-and-10 are defaults drawn from the 5–30 day range found in public contracts, marked [A]; the Founder can set others per engagement.

© 2026 Symbeeo. All rights reserved. · Public

SYMBEEO

Each vendor's tool shows you their option. We show you all of them against one requirement.

Compared. Then Delivered.

hello@symbeeo.com · symbeeo.com

© 2026 Symbeeo. All rights reserved.

Product and company names and logos are their owners' trademarks, shown only to identify the lines Symbeeo sources. Naming a vendor or showing its logo does not mean the vendor sponsors or approves Symbeeo's comparisons or any recommendation Symbeeo makes.

Figures are as published by their sources on the dates given in this document; figures marked [A] are assumptions.

STP-SEC-001 · Version 1.5 · Oct 10, 2026