SYMBEEO

PUBLIC

SOLUTION DESIGN DOCUMENT

Zero-trust access design for a typical buyer, applying SRA-SEC-001 Model A

Design document (HLD + LLD)

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

WRITTEN BY

David Morgan, Principal Security Architect

© 2026 Symbeeo. All rights reserved.

Document control

Document	SDD-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	Applies to	SRA-SEC-001 v1.4, Model A (on-premises microsegmentation, NIST E2B3)
Tested by	STP-SEC-001		
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 representative signs this document before build; the practice lead signs it after."		

Contents

1 · Introduction 3
2 · Prerequisites 4
3 · Solution overview 4
4 · Policy design 5
5 · Enforcement point design 6
6 · Logging 6
7 · Migration 6
8 · Roles and deliverables 6
9 · Security and lifecycle clauses 7

© 2026 Symbeeo. All rights reserved. · Public

CONVENTIONS

The reference architecture applied to one client. Model A is chosen because the typical buyer is data-center-heavy (SRA-SEC-001 §5, D1); Model B would be a separate design. Client values are the typical buyer's [A]; the design items follow the low-level design list an integrator quoted for an ISE deployment: deployment architecture, node roles, authorization methods, identity stores, source sequencing, profiling, supplicants, certificates. A row with more than one tag is counted once: as a published figure if any tag is [S] or [S*], otherwise as an assumption if any tag is [A], otherwise as a design target.

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 · Introduction

1.1 Purpose.

Design for identity-based access across HQ, three branches and two data centers: a policy engine, enforcement on every access port, NGFW pairs at the data centers and branches, posture, certificates, logging. **1.2 Goals.** No network-wide trust; every session tied to an identity and a posture; lateral movement blocked between segments; an audit trail per session. **1.3 Approach.** Monitor mode first (visibility, no enforcement) for four weeks; then low-impact enforcement by site; then closed mode. Cisco IT's order: map identities, register devices and deploy certificates, then enforce [S].

1.4 Change control and reporting.

- **Change orders.** Once this document is signed, any change to the design is a written change order stating what changes, why, and its cost and schedule effect. Both parties sign it before the change is built. The client's change ticket for the work carries the signed change order's number.
- **Weekly status report.** Every week of the build Symbeeo sends the client's security manager a status report giving, per deliverable in §8: % complete, slippage against the plan in §7.
- **Escalation.** Contacts on both sides, by role, are listed in §8.

1.5 Related documents.

SRA-SEC-001 · STP-SEC-001 · SDD-NET-001 (access layer) · vendor datasheets listed in SRA-SEC-001 §1 · lifecycle notices and recommended software releases read Sep 24, 2026, with URLs, in SRA-SEC-001 §9.2 · NIST SP 800-88 Rev. 2 (§9).

© 2026 Symbeeo. All rights reserved. · Public

2 · Prerequisites

Table 2. Prerequisites

#	Prerequisite	Owner	Status
P1	Active Directory groups for user roles; Entra ID tenant details	client	open
P2	Certificate authority with device-certificate template; auto-enrollment for managed devices	client	open
P3	MDM/UEM reachable for posture	client	open
P4	Access switches support 802.1X, MAB, SGT (SDD-NET-001)	Symbeeo	open
P5	Device inventory: managed, BYOD, OT with expected counts	client	open
P6	SIEM/XDR ingestion endpoint and retention (12/24 months)	client	open
P7	Fail-closed decision signed (SRA-SEC-001 R9)	client	open

3 · Solution overview

3.1 Components (the build entry).

Policy engine: Cisco ISE 3.5 Patch 4, two-node deployment on SNS-3895 appliances for 5,000 endpoints, sized from the scalability guide with a 20,000 ceiling (small deployment limit 50,000) [S]. DC enforcement: PA-5570 HA pair per data center on PAN-OS 12.1 [S] (the PA-5450 is not used: end of sale Nov 22, 2026). Branch enforcement: FortiGate 200G HA pair per branch on FortiOS 7.6 [S]. Access enforcement: 802.1X/MAB/SGT on Catalyst 9300X on IOS XE 17.18.4 (SDD-NET-001). Posture: the client's MDM. Logging: the client's SIEM/XDR. Certificates: the client's CA.

3.2 Deployment architecture [A].

ISE: primary admin + monitoring at DC-A, secondary at DC-B, policy service on both; branches authenticate to the nearest; RADIUS with TLS.

3.3 Inventory and lifecycle [A]/[S].

Quantities are the typical buyer's [A]; status read Sep 24, 2026 and restated on the day of the quote (§9).

Table 3. Inventory and lifecycle [A]/[S]

Item	Qty	Where	Planned software	End of sale / end of support, read Sep 24, 2026
Cisco SNS-3895 (ISE)	2	DC-A, DC-B	ISE 3.5 Patch 4	no notice on Cisco's ISE end-of-sale listing [S]; replaces SNS 3795 (end of sale Dec 30, 2025, last support Dec 31, 2030), which is not quoted
Palo Alto PA-5570	4	2 per DC	PAN-OS 12.1 (end of life Aug 28, 2028)	no PA-5500 entry on Palo Alto's end-of-sale page [S]; replaces PA-5450 (end of sale Nov 22, 2026, support to Nov 22, 2031), which is not quoted
Fortinet FortiGate 200G	6	2 per branch	FortiOS 7.6 (support to Jan 25, 2030, secondary source)	no end-of-order date found in public sources; **not verified** in Fortinet's support portal

© 2026 Symbeeo. All rights reserved. · Public

Item	Qty	Where	Planned software	End of sale / end of support, read Sep 24, 2026
Catalyst 9300X access	per SDD-NET-001 §3.2	all sites	IOS XE 17.18.4	no 9300X model on Cisco's 9300 end-of-sale listing [S]

Sources, with URLs: SRA-SEC-001 §9.2.

4 · Policy design

4.1 Identity stores and sequencing.

Internal endpoint store (802.1X certificates, MAB MACs); external AD/Entra; sequence: certificate → AD → deny [S].

4.2 Authorization matrix [A].

Table 4. Authorization matrix [A]

Identity	Posture	Result	SGT	VLAN
domain user, managed device	compliant	full access	10 Employees	20
domain user, managed device	non-compliant	remediation only	99 Quarantine	99
contractor	compliant	app-specific	20 Contractors	20
BYOD (Wi-Fi)	registered	internet + selected apps	30 BYOD	40
OT device (MAB, profiled)	n/a	its own segment only	40 OT	60
unknown	n/a	guest / deny	50 Guest	50 or none

4.3 Microsegmentation.

SGT-based policy matrix enforced at the core and DC NGFW: Employees → apps allowed by port; Contractors → named apps only; OT → OT servers only; Quarantine → remediation servers only.

4.4 Profiling.

DHCP, RADIUS, SNMP probes; custom profiles for the client's OT devices; profiler feed enabled [S].

4.5 Supplicants.

Native supplicant, EAP-TLS with device certificates for managed devices; PEAP disabled after migration [A].

4.6 Certificates.

CA-signed certificates on ISE nodes; device certificates via auto- enrollment; 802.1X trust chain distributed by MDM.

4.7 Fail behavior.

Fail-closed for new sessions; critical-auth VLAN on access ports for OT only, decided in P7.

© 2026 Symbeeo. All rights reserved. · Public

5 · Enforcement point design

5.1 DC NGFW.

PA-5570 pairs: zones per VLAN group; SGT-to-zone mapping; TLS inspection with post-quantum key exchange (ML-KEM, HQC) enabled where the client's endpoints support it [S]. **5.2 Branch NGFW.** FortiGate 200G pairs: internet edge and inter-VLAN enforcement [S]. **5.3 Access.** Per SDD-NET-001 §4.6.

6 · Logging

All authentication and authorization events, NGFW sessions, posture results to SIEM; 12 months hot, 24 months archive; dashboards for failed authentications, quarantine, OT anomalies.

7 · Migration

Table 5. Migration

Step	Action	Rollback
1	ISE deployed; monitor mode on all ports; four weeks of identity and device mapping	none needed
2	Device certificates auto-enrolled; coverage reported weekly until > 98 %	—
3	Low-impact enforcement at HQ, floor by floor	back to monitor mode per port
4	Closed mode at HQ; then branches one per week	back to low-impact per site
5	SGT matrix enforced at core and DC NGFW; STP-SEC-001 use cases run; acceptance	matrix to monitor

8 · Roles and deliverables

Design authority: practice lead and the client's security manager (both sign).

Table 6. Roles and deliverables

Role	Symbeeo	Client
Design authority	practice lead (signs)	security manager (signs)
Build	build engineers	change approver
Acceptance	test lead	named acceptor (security manager)

Escalation contacts (by role; names filled at contract signature).

Table 7. Roles and deliverables

Level	Symbeeo	Client	When
1	build engineer on site	change approver	day-to-day issue in a change window

© 2026 Symbeeo. All rights reserved. · Public

Level	Symbeeo	Client	When
2	practice lead	security manager	slippage against §7, a failed T-case, a disputed change order
3	the Founder	the client's executive sponsor	unresolved at level 2 within 2 business days [A]; any security incident (§9)

Deliverables: this document · STP-SEC-001 with results · as-built (nodes, policies, matrix, certificates) · operations runbook · acceptance certificate · weekly status reports (§1.4) · signed change orders.

Handover pack, delivered at the end of migration step 5 and before signed acceptance: as-built drawings (node placement, enforcement points, logical diagrams) · configurations of every ISE node, NGFW and policy set, with the authorization matrix and SGT matrix versions · credentials transferred to the client and Symbeeo's build and administrator credentials revoked · licenses, with term and renewal date · vendor support contracts, with severity levels (§9) · STP-SEC-001 signed · open items, each with owner and date · media-sanitization certificates for decommissioned equipment (§9).

9 · Security and lifecycle clauses

- **Incident reporting.** A security incident affecting the client's data or systems, discovered by Symbeeo during the engagement, is reported to the client's named security contact within 24 hours of discovery, then escalated per §8.
- **Media sanitization.** Storage media leaving the client's control (decommissioned appliance disks and SSDs, NGFW log drives, returned faulty units) are sanitized to **NIST SP 800-88 Rev. 2** (final, Sep 26, 2025), with a certificate per device giving serial number, method and date [S] `https://csrc.nist.gov/pubs/sp/800/88/r2/final`, read Sep 24, 2026. Sanitization is done before the media leave the client's control; alternatively the media stay with the client under a non-return service. Media holding PHI or other regulated personal data are never taken back unsanitized.
- **No equipment past end of sale.** No item is quoted past its vendor's end-of-sale date. The quote shows the end-of-sale and end-of-support date of every item; §3.3 carries the status read on Sep 24, 2026, restated on the day of the quote. The PA-5450 (end of sale Nov 22, 2026), the SNS 3795 (end of sale Dec 30, 2025) and Secure Network Analytics UCS M6 appliances (end of sale Dec 18, 2026) are excluded on this clause.
- **Support level by severity.** Every quote states the vendor support level bought for each item, as the vendor's response time for severity 1, 2, 3 and 4. The values come from the vendor contract offered at the quote [A]; none is stated here.
- **Handover pack.** Delivered as listed in §8.

© 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.

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