SYMBEEO

PUBLIC

DESIGN STUDY

Firewall consolidation: nine vendors to one platform across 18 sites

Complete design on current platforms

CAPABILITY	INDUSTRY	SETTING
Security	Financial Services	Regional bank
DOCUMENT	**VERSION**	**DATE**
SEC-003	1.3	Oct 10, 2026

WRITTEN BY

David Morgan, Principal Security Architect

© 2026 Symbeeo. All rights reserved.

Document control

Document	SEC-003	Version	1.3
Issued	Oct 10, 2026	Status	Issued by Symbeeo
Classification	Public	Supersedes	1.2, Sep 27, 2026
Capability	Security	Industry	Financial Services
Author	David Morgan	Role	Principal Security Architect
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. Design study: every figure is vendor-published, a design target or a marked assumption.		
Sign-off	"An engagement under this design is signed by the practice lead before any build proceeds."		

Contents

1 · Scope 3
1c · Public implementations this design follows 4
2 · Requirements register 4
3 · Architecture overview 5
4 · Design by subsystem 6
5 · Failure behavior 7
6 · Limits 7
7 · Lessons learned 8
8 · The author 8

© 2026 Symbeeo. All rights reserved. · Public

CONVENTIONS

Source tags. [S] figure read from the vendor's own current page on Sep 18, 2026 · [S*] figure from the vendor's page summary where the page itself could not be opened · [A] design assumption for the typical buyer, to be confirmed by the signing engineer · [T] design target taken from the design's stated outcome or derived from it. Every figure carries one tag. No figure comes from any prior engagement, file or asset. 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 18, 2026	`1.0`	First issue.
Sep 20, 2026	`1.1`	Public implementations added; figures reconciled with published sources.
Sep 27, 2026	`1.2`	Figures and platform details rechecked against published sources.
Oct 10, 2026	`1.3`	Approval line now reads: approved by the Founder, issued by Symbeeo. David Morgan remains the author.

1 · Scope

Who it is for. The CISO of a regional bank that has inherited nine firewall estates through mergers and branch refreshes, each with its own console, rule base and support contract, and who must show the regulator one policy, one owner per rule, and one change process.

Typical buyer [A]. A regional bank with 18 branches and two data centers. Two data-center perimeters at 10 Gbps internet each, 18 branch edges at 200 Mbps–1 Gbps, roughly 9,000 rules across the nine estates before the audit, 2,400 staff, and a core-banking application in each data center. Nine vendors today; the record does not name them and this document does not either.

What is in. One gateway platform for data centers and branches; one management plane; the rule audit and migration method; rule ownership; the cut-over sequence across 18 sites and two data centers; the acceptance test. **What is out.** SD-WAN transport; endpoint security; cloud-hosted workloads; the SIEM.

Assumptions. Check Point is the sole firewall vendor after the program [A]. Each data center has an internet edge and an internal segmentation gateway; branches have one edge each [A]. The audit produces the rule-cut count; this document does not predict it [T].

Related documents, read Sep 18, 2026. Check Point Quantum Force 9300 datasheet, `https://www.checkpoint.com/downloads/products/quantum-force-9300-datasheet.pdf` · Check Point Quantum Spark 2500 series datasheet, `https://www.checkpoint.com/downloads/products/quantum-spark-2500-datasheet.pdf` · Check Point Quantum Smart-1 700-S and 700-M overview, `https://sc1.checkpoint.com/documents/Appliances/GSG_Smart1_700SM/EN/Content/Topics-GSG-700-SM/Overview-700-SM.htm` · Check Point Force 9300 product page, `https://www.checkpoint.com/quantum/force/9300/` (page could not be opened; figures taken from the datasheet PDF above) · Check Point Quantum Force 9400 datasheet (dated Jul 12, 2026), read Sep 27, 2026, `https://www.checkpoint.com/downloads/products/quantum-force-9400-datasheet.pdf` · Check Point Quantum Force 9700 datasheet (dated Jul 8, 2026), read Sep 27, 2026, `https://www.checkpoint.com/downloads/products/quantum-force-9700-datasheet.pdf` · Check Point Quantum Smart-1 Cloud Administration Guide, Management and Smart-1 Cloud Overview, read Sep 27, 2026 (the Aug 4, 2024 PDF edition no longer resolves), `https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/Check-Point-SmartCloud-Admin-Guide/Topics-Smart-1-Cloud/Overview.htm` · Check Point Smart-1 Cloud datasheet ("Manage up to 400 gateways"), read Sep 27, 2026, `https://www.checkpoint.com/downloads/products/smart-1-cloud-security-management-datasheet.pdf` · Check Point CheckMates

© 2026 Symbeeo. All rights reserved. · Public

community forum (practitioner advice, not a vendor specification), sizing a gateway against published throughput — plan the upgrade at 50 %, expect about half the advertised figure in service (read Sep 20, 2026) — https://community.checkpoint.com/t5/Firewall-and-Security-Management/How-to-size-a-firewall-according-to-the-different-throughputs/td-p/147519.

1c · Public implementations this design follows

Deployment rows are real public deployments, each dated. Where no public deployment matches, the row is Vendor documentation: the vendor's document that this design, Symbeeo's own, is built on.

Table 2. Public implementations this design follows

Implementation	Who published it · date	What it settles for this design	URL
Vendor documentation. Smart-1 Cloud Administration Guide: one management plane for Quantum Spark (1500–3000 series), Quantum Security Gateways and Maestro, up to 400 gateways per management	Check Point · admin guide Aug 4, 2024 (now served as HTML); datasheet read Sep 27, 2026	R10 and §4.3: branch Spark gateways and data-center gateways under one policy and one log store is the vendor's documented model; the on-premises Smart-1 700-M limit of 50 gateways (R11) is the figure this document is sized to	https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/Check-Point-SmartCloud-Admin-Guide/Topics-Smart-1-Cloud/Overview.htm · https://www.checkpoint.com/downloads/products/smart-1-cloud-security-management-datasheet.pdf

2 · Requirements register

Table 3. Requirements register

#	Requirement	Value	Source
R1	Sites	18 branches, 2 data centers	[T]
R2	Firewall estates before	9; after: 1 policy plane	[T]
R3	Rules with a named owner after migration	100 %	[T]
R4	Rule reduction	the count the audit produces; not predicted here	[T]
R5	Data-center gateway throughput	129 Gbps firewall, 73.7 Gbps IPS, 57.6 Gbps NGFW, 20 Gbps threat prevention (enterprise test conditions)	[S] Force 9700
R6	Data-center gateway form and ports	1 RU, 4 × RJ45 and 4 × 1/10GbE SFP+ on board, two expansion slots, each 8 × 1/10G or 4 × 10/25G or 2 × 40/100G	[S] Force 9700
R7	Data-center gateway clustering	Active/Active L2, Active/Passive L2 and L3, ClusterXL or VRRP; Maestro 2–3 appliances	[S] Force 9700

© 2026 Symbeeo. All rights reserved. · Public

#	Requirement	Value	Source
R8	Branch gateway throughput, large branch	5,500 Mbps threat prevention, 11,000 Mbps firewall, 16 × 1GbE + 4 × 10GbE SFP+	[S] Spark 2590
R9	Branch gateway throughput, standard branch	1,850 Mbps threat prevention, 3,750 Mbps firewall, 8 × 1GbE + 2 × 10GbE SFP+	[S] Spark 2560
R10	Branch gateways centrally managed	Spark 2500 managed by Smart-1 and management server	[S] Spark 2500
R11	Management capacity	up to 50 gateways, 25,000 logs/s sustained	[S] Smart-1 700-M
R12	Gateways under management day one	26 (8 data-center cluster members + 18 branch), each cluster member counted as one gateway; 26 ÷ 50 = 52 % of the 700-M limit	[S]/[A]
R13	Peak log rate	8,000 logs/s across the estate	[A]
R14	Change window per branch	4 hours, outside trading hours	[A]
R15	Data-center cut-over	one DC at a time, the other DC carrying the application	[A]

Fifteen rows; eight carry a vendor figure, three are design assumptions, four are design targets.

3 · Architecture overview

```
Internet ──[Force 9700 HA pair]── DC-A ──[Force 9700 HA pair, internal]── core banking
                                  ‖ (DC interconnect, out of scope)
Internet ──[Force 9700 HA pair]── DC-B ──[Force 9700 HA pair, internal]── core banking

Branch × 18 ──[Spark 2560 / 2590]── WAN ── DC-A / DC-B

Smart-1 700-M pair (primary DC-A, standby DC-B): one policy, one log store, one console
```

Figure 1. Consolidated firewall estate

Four Force 9700 pairs in the data centers (eight appliances), one Spark 2500 per branch (18), one Smart-1 700-M pair managing all 26 gateways. Nine estates become one policy package with per-site layers.

Table 4. Architecture overview

Role	Product (exact model)	Qty	Capacity used	Why this unit
DC internet edge	Check Point Quantum Force 9700	4 (2 pairs)	10 Gbps peak on the active unit against 20 Gbps threat prevention, 50 %; the same 50 % on the standby after a failover, see §4.1 [A]/[S]	Smallest Force model that carries the edge within the 50 % rule; 1 RU; 2 × 40/100G expansion for growth [S]

© 2026 Symbeeo. All rights reserved. · Public

Role	Product (exact model)	Qty	Capacity used	Why this unit
DC internal segmentation	Check Point Quantum Force 9700	4 (2 pairs)	20 Gbps peak on the active unit against 57.6 Gbps NGFW, 35 % [A]/[S]	Same platform, same management, one spare stock [A]
Large branch edge (4 branches)	Check Point Quantum Spark 2590	4	1 Gbps of 5,500 Mbps threat prevention [A]/[S]	1 U, 16 × 1GbE + 4 × 10GbE SFP+ [S]
Standard branch edge (14 branches)	Check Point Quantum Spark 2560	14	200–500 Mbps of 1,850 Mbps threat prevention [A]/[S]	8 × 1GbE + 2 × 10GbE SFP+, desktop [S]
Management and logging	Check Point Quantum Smart-1 700-M	2	26 of 50 gateways; 8,000 of 25,000 logs/s [A]/[S]	Sized with headroom for the audit period when both estates log in parallel [A]

4 · Design by subsystem

4.1 Data-center gateways.

Force 9700 pairs in ClusterXL High Availability, Active/Passive L3 (one active member, one standby) [S], at the internet edge and again inside for segmentation. Threat prevention on at the edge; IPS and application control inside.

Sizing ceiling. Published appliance figures are measured under the vendor's own test conditions and are not a design budget; practitioner advice on Check Point's CheckMates community forum (not a vendor specification) is to plan the upgrade at **50 %** and to expect roughly half the advertised throughput in service [A]. **The rule applied here: peak design load on the unit carrying it sits at or below 50 % of that unit's published figure for the feature set turned on, in normal operation and after one unit of a pair is lost.** In an active/standby pair the active unit carries the whole peak, and after a failure the standby carries the same peak, so the rule is met on one unit's figure. Edge, threat prevention on: 10 Gbps peak ÷ 0.50 = 20 Gbps of published threat prevention needed per unit [A]/[S]. Force 9300: 10.5 Gbps [S], 10 ÷ 10.5 = 95 % — fails. Force 9400: 14 Gbps [S], 10 ÷ 14 = 71 % — fails. Force 9700: 20 Gbps [S], 10 ÷ 20 = 50 % — meets the rule, before and after a failover, with no margin left: any growth above the 10 Gbps peak is the point to revisit the model [A]. The 9700 datasheet also mentions 25 Gbps of threat prevention in its prose; the design uses the 20 Gbps in its performance table. Internal, IPS and application control on (the NGFW figure): 20 Gbps peak ÷ 57.6 Gbps [S] = 35 %; the 9300's 28.2 Gbps would put it at 71 %. **The design is therefore two Force 9700 appliances per role per data center, active/standby, with a full appliance remaining when one is lost.** Rejected: load sharing on 9300s — each member at 5 ÷ 10.5 = 48 % in normal operation, but the survivor carries 10 Gbps at 95 % after a failure, which breaks the rule when it matters. Rejected: Maestro hyperscale day one — one 9700 per role carries the load with the ceiling applied; Maestro remains the growth path [S].

4.2 Branch gateways.

Spark 2560 for standard branches, Spark 2590 where the branch has a local server room or more than 150 staff [A]. Both managed from the Smart-1 [S]. Rejected: a Force appliance per branch — the branch throughput is under 1 Gbps and the Spark line is managed in the same console [S].

4.3 Management plane.

Smart-1 700-M primary in DC-A, secondary in DC-B [A]. One policy package; a shared global layer (bank-wide deny list, management access, logging) and one ordered layer per site. Every rule carries an owner field, a ticket reference and a

© 2026 Symbeeo. All rights reserved. · Public

review date; a rule without an owner does not pass the install check [A].

4.4 Rule audit and migration.

Export the nine rule bases; normalize to one schema (source, destination, service, action, hit count, last hit, comment); classify each rule as unused (no hit in 90 days), shadowed, duplicate, over-broad, or live [A]. Unused and shadowed rules are dropped; duplicates merged; over-broad rules narrowed to the observed traffic; live rules carried across with an owner assigned by the application inventory. The number cut is the audit output (R4). Rejected: vendor-neutral conversion tooling as the whole method — tooling converts syntax, not ownership.

4.5 Cut-over sequence.

Branches first, two per week, 9 weeks [A]; the new gateway is installed in parallel and traffic moved by default-gateway change inside the 4-hour window (R14), old device left in place one week. Then DC-B internal, DC-B edge, then DC-A, one gateway pair per weekend with the other DC carrying the application (R15). Both estates log to the Smart-1 during the parallel period, hence the log headroom in R11–R13.

4.6 Decommission.

Nine support contracts ended, nine consoles retired, configurations archived read-only for the audit record [A].

5 · Failure behavior

Table 5. Failure behavior

Failure	Behavior	Source
Active Force 9700 in a pair fails	ClusterXL fails over to the standby member, which carries the same peak at the same 50 % or less (§4.1); sessions held	[S] clustering, [A] session sync on
Branch gateway fails	Branch loses WAN access; hot spare shipped; branch staff fall back to another branch's systems	[A]
Smart-1 primary down	Gateways keep enforcing the installed policy; secondary takes management; logs queue on gateways until reconnected	[A]
Policy install error	Install verification fails, previous policy stays; no gateway is left without a policy	[A]
Migrated rule blocks a live flow	Old gateway still in place for one week; rule added with owner; nothing rolled back wholesale	[A]

6 · Limits

- The rule-cut figure is unknown until the audit runs; the document does not estimate it.
- Threat-prevention figures are vendor enterprise-mix figures [S]; the bank's traffic mix is measured before the model is fixed.
- Session synchronization across the DC-A/DC-B pair is not designed here; each DC is its own cluster.
- Branch resilience is a single gateway; a second unit per branch is a cost decision the design leaves to the client.
- Smart-1 700-M is sized for 50 gateways; with the 8 data-center cluster members counted, a branch count above 42 (50 − 8) moves the design to the next Smart-1 model.

© 2026 Symbeeo. All rights reserved. · Public

- The internet edge sits exactly at the 50 % ceiling on the Force 9700 (§4.1); a larger internet circuit moves the edge to the next Force model or to Maestro.

7 · Lessons learned

None yet — this is a design study; populated after the first build against it.

8 · The author

WRITTEN BY

David Morgan

Principal Security Architect

CCISO, CISSP, CISSP-ISSEP, CISM, CISA, CRISC, PMP, CCSP, Adopting Zero Trust (Forrester)

Signed off by Edwin Ozer, Founder.

© 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.

SEC-003 · Version 1.3 · Oct 10, 2026