SYMBEEO

PUBLIC

COMPARISON

Firewalls: Nine Vendors to One

Published comparison

CAPABILITY	DOCUMENT	VERSION	DATE
Security	CMP-SEC-001	1.1	Nov 7, 2026

WRITTEN BY

David Morgan, Principal Security Architect

© 2026 Symbeeo. All rights reserved.

What this document is. Five firewall platforms held to one written requirement: nine firewall estates across a bank's 18 branches and two data centers, brought under one platform, one policy and one change process. Three platforms meet it, each with a named condition. Two stay open on clauses their own documents do not settle.

Document control

Document	CMP-SEC-001	Version	1.1
Issued	Nov 7, 2026	Status	Issued by Symbeeo
Classification	Public	Supersedes	1.0, Oct 24, 2026
Capability	Security	Author	David Morgan
Role	Principal Security Architect		
Credentials	CCISO, CISSP, CISSP-ISSEP, CISM, CISA, CRISC, PMP, CCSP		
Approval	Version 1.0 issued by Symbeeo, Oct 24, 2026. Version 1.1 issued by Symbeeo, Nov 7, 2026. Every mark carries its source; prices are not published.		

Contents

1 · The requirement 3
2 · The options 4
3 · Conformance, clause by clause 4
4 · The hardware criteria 6
5 · Price and due diligence 6
6 · The verdict 7
7 · Sources 7
8 · The assessor 9

© 2026 Symbeeo. All rights reserved. · Public

CONVENTIONS

Marks. MET the vendor's own current document shows the clause is met · **MET WITH A CONDITION** met only if the named condition is on the order or confirmed at the quote · **OPEN** the documents read do not settle it; the reason is given · **NOT MET** the vendor's own figure falls short.

Source tags. [S] read with curl from the vendor's own current page or document between October 22 and 24, 2026 · [S*] from a summary of the vendor's page where the page itself could not be opened; provisional, never settles a mark · [A] an inference, stated as one · [T] a figure set by the requirement. No price, discount or price figure appears in this document.

Table 1. Revision history

Date	Version	Change
Oct 24, 2026	1.0	First issue.
Nov 7, 2026	1.1	Wording on HPE Juniper Networking: sizing and migration tool not confirmed from the public documents we could open. No mark changed.

1 · The requirement

The requirement comes from Symbeeo's design study Firewall consolidation: nine vendors to one platform across 18 sites. It was fixed before any option was assessed and names no product. Each clause names the option expected to split on it.

Table 2. The requirement

Clause	The buyer's words	Expected to split
R-1	Each data-center gateway, on its own after its partner fails, carries its peak at no more than half of its vendor's published figure for the features turned on: 10 Gbps with full threat prevention at the internet edge, 20 Gbps with intrusion prevention and application control inside. [T]	Platforms whose largest 1RU or 2RU unit publishes less than 20 Gbps of threat prevention
R-2	Each branch gateway carries the branch peak, up to 1 Gbps at a large branch and 500 Mbps at a standard one, at no more than half its published threat-prevention figure, with 10 GbE fibre ports at the large branches. [T]	Few; every platform has a branch line
R-3	One management system on the bank's premises holds one policy for all 26 gateways and their logs, takes 8,000 logs per second, and keeps a standby in the second data center. [T]	Platforms whose log rate is not published, or that need a second product for logs
R-4	The nine existing rule bases are converted with migration tooling that the new platform's vendor supports, from the other major firewall vendors' configurations. [T]	Platforms whose vendor has withdrawn its migration tool
R-5	Every change is approved by a second administrator before it reaches any gateway, and the approval is recorded for the regulator. [T]	Platforms with no built-in approval step

Why half the published figure. Published throughput is measured under each vendor's own test mix, and each vendor names its figure differently: Threat Prevention (Check Point, Palo Alto Networks), Threat Protection (Fortinet), FW + AVC + IPS (Cisco), Advanced Threat Protection (HPE Juniper Networking). Planning at half the figure keeps one appliance able to carry the whole peak after its partner fails. The bank's own traffic mix is measured before a model is fixed.

The criteria used. Conformance to the requirement comes first. Beside it, the hardware set: rack fit, power draw, lead time and availability (section 4). Five-year cost is a supporting column, never a criterion.

© 2026 Symbeeo. All rights reserved. · Public

2 · The options

Assessed, all on Symbeeo's line card:

Table 3. The options

Option	Platform as assessed	Why it is in
A	Check Point: Quantum Force 9700, Quantum Spark 2560 and 2590, Smart-1 700-M	The platform the design study is drawn on
B	Palo Alto Networks: PA-3440 and PA-5420, PA-1410 and PA-440, Panorama	Major enterprise firewall line
C	Fortinet: FortiGate 900G and 3200F, FortiGate 120G and 70G, FortiManager with FortiAnalyzer	Major enterprise firewall line
D	Cisco: Secure Firewall 3120 and 3140, Secure Firewall 1220CX and 1210CE, Firewall Management Center 2800	Major enterprise firewall line
E	HPE Juniper Networking: SRX4700 and SRX4300, SRX1600, Junos Space Security Director	Major enterprise firewall line

Each option uses the smallest model in its vendor's current line that meets the sizing clauses, read from the vendor's own figures.

Set aside before assessment, with the reason:

Table 4. The options

Vendor	Reason
F5, Akamai	Application delivery and edge services; no branch firewall line for 18 branches [A]
HPE Aruba Networking	Its branch security sits in SD-WAN, which the requirement leaves out [A]
AWS, Google Cloud, Equinix	Cloud or colocation; the gateways sit on the bank's own sites
Not on the line card (for example Sophos, SonicWall, WatchGuard, Forcepoint)	Not assessed; Symbeeo assesses what it can supply and support

3 · Conformance, clause by clause

Each cell gives the mark, the fact and its source key. Keys resolve in section 7.

© 2026 Symbeeo. All rights reserved. · Public

Table 5. Conformance, clause by clause

Clause	A · Check Point	B · Palo Alto Networks	C · Fortinet	D · Cisco	E · HPE Juniper Networking
R-1 data center	**MET.** Force 9700: 20 Gbps threat prevention, 57.6 Gbps NGFW [S, K1]. Edge 10 of 20 = 50 %, at the ceiling; inside 20 of 57.6 = 35 %	**MET.** Edge PA-3440: 20 Gbps threat prevention [S, P1], 50 %, at the ceiling. Inside PA-5420: 50 Gbps threat prevention [S, P1], 40 %	**MET.** Edge FortiGate 900G: 30 Gbps threat protection [S, F1], 33 %. Inside FortiGate 3200F: 47 Gbps NGFW [S, F2], 43 %	**MET WITH A CONDITION.** Edge 3120: 21 Gbps FW + AVC + IPS, 48 %; inside 3140: 45 Gbps, 44 % [S, C1]. Cisco's figure covers intrusion prevention and application control; malware and URL inspection are not in it, so the edge is sized on it [A]	**OPEN.** SRX4300: 11 Gbps Advanced Threat Protection [S, J1], 91 % at the edge, not met. SRX4700 publishes no threat-protection figure [S, J2]. Inside, SRX4700 NGFW 60 Gbps [S, J2], 33 %, met
R-2 branches	**MET.** Spark 2590: 5,500 Mbps threat prevention, 10GbE SFP+ ports; Spark 2560: 1,850 Mbps [S, K2]	**MET.** PA-1410: 4.5 Gbps threat prevention, 10G SFP+ ports; PA-440: 1.2 Gbps [S, P1]	**MET WITH A CONDITION.** FortiGate 120G: 2.8 Gbps; 70G: 1.3 Gbps threat protection [S, F2]. The matrix lists 10 GE SFP+ ports for this group but its per-model columns are not legible; confirm on the 120G datasheet	**MET.** 1220CX: 9 Gbps FW + AVC + IPS, 2 × 10G SFP+; 1210CE: 6 Gbps [S, C2]	**MET.** SRX1600: 2 Gbps Advanced Threat Protection, 4 SFP+ ports [S, J3]; 50 % at a large branch, at the ceiling
R-3 one management system	**MET.** Smart-1 700-M: up to 50 gateways, 25,000 logs per second [S, K3]. Active and standby management servers [S, K4]	**MET.** A high-availability Panorama pair manages up to 5,000 firewalls [S, P2]. M-300 in Panorama mode: 16,500 logs per second [S, P5]	**MET WITH A CONDITION.** FortiManager 410G: 150 devices, high availability [S, F3]; the log rate needs FortiAnalyzer 1000G on the order: 20,000 logs per second, high availability [S, F4]	**MET.** Management Center 2800: 300 devices, 15,000 events per second, active/standby [S, C3]	**OPEN.** Junos Space keeps a standby site with near-real-time replication [S, J5]. Its device count and log rate were not found in the documents read
R-4 migration tooling	**MET WITH A CONDITION.** SmartMove converts Cisco ASA, Juniper, Fortinet and Palo Alto Networks configurations [S, K6]. Maintained "on a best effort basis" [S, K6]; confirm support terms at the quote	**OPEN, at risk.** "Starting from January 2025, Palo Alto Networks will no longer support the Expedition tool" [S, P4]. No supported successor found in the documents read	**MET.** FortiConverter converts Check Point, Cisco, Juniper, Palo Alto Networks, SonicWall and Sophos configurations [S, F5]	**MET WITH A CONDITION.** The Migration Tool converts ASA, Check Point, Palo Alto Networks, Fortinet and Microsoft Azure configurations [S, C4]. Juniper is not listed; it matters only if one of the nine estates is Juniper	**OPEN.** Juniper's route found is a migration service, not a tool; its page did not open [S*]

© 2026 Symbeeo. All rights reserved. · Public

Clause	A · Check Point	B · Palo Alto Networks	C · Fortinet	D · Cisco	E · HPE Juniper Networking
R-5 second-person approval	**MET.** "Approval Cycle for Sessions": administrators submit changes for approval before publishing [S, K5]	**OPEN.** Panorama offers administrator-specific commits [S, P3]; the PAN-OS 12.1 commit and push page describes no approval step [S, P6]	**MET.** "Workflow mode enforces an approval process model" [S, F3]	**MET WITH A CONDITION.** Change management with separate approver roles is documented for the cloud-delivered management center [S, C5]; the same workflow on the on-premises 2800 is inferred [A]	**MET.** Change Control Workflow: requester, approver and a ticket number field [S, J4]
Stage 2 standing	**Conforms, with a condition:** SmartMove support terms	**Not passed to stage 3:** R-4, R-5 open	**Conforms, with a condition:** FortiAnalyzer on the order; SFP+ on the 120G	**Conforms, with a condition:** sizing basis, Juniper sources, on-premises approval	**Not passed to stage 3:** R-1, R-3, R-4 open

4 · The hardware criteria

Table 6. The hardware criteria

Criterion	A · Check Point	B · Palo Alto Networks	C · Fortinet	D · Cisco	E · HPE Juniper Networking
Rack fit, data center	Force 9700: 1RU [S, K1]	PA-3440: 1U [S, P1]. PA-5420: height not legible in the summary sheet; OPEN	900G: 1RU [S, F1]. 3200F: 2RU [S, F2]	3120 and 3140: 1RU [S, C1]	SRX4700: 1U [S, J2]
Power draw, data-center edge unit	224.5 W average, 374.3 W maximum [S, K1]	450 W AC supply rating; draw not published in the sheet read [S, P1]	170 W average, 313 W maximum [S, F1]	400 W AC supply rating; draw not published in the sheet read [S, C1]	SRX4700 not confirmed from the public documents we could open. SRX4300: 393 W maximum [S, J1]
Lead time	OPEN: taken from distributor data at stage 4	OPEN	OPEN	OPEN	OPEN
Availability	OPEN: checked at stage 4	OPEN	OPEN	OPEN	OPEN

5 · Price and due diligence

Stage 3, price. Price is weighed only among the three options that passed stage 2: Check Point, Fortinet and Cisco. No price figure is published here. They are not ranked: the buyer's own quote, for the same 26 gateways, the management and log systems and the migration tooling named above, decides between them. Palo Alto Networks and HPE Juniper Networking are not evaluated on price; cost never rescues an option that has not met the requirement.

Stage 4, due diligence. Lead time and allocation for the chosen models are checked with authorized distribution before the order. Nothing in this document states a delivery date.

© 2026 Symbeeo. All rights reserved. · Public

6 · The verdict

Check Point, Fortinet and Cisco meet the requirement once named conditions are settled at the quote: Check Point, SmartMove's support terms; Fortinet, FortiAnalyzer on the order for the log rate and the SFP+ ports on the 120G; Cisco, a threat figure without malware and URL inspection, a migration tool that reads no Juniper estate, and the approval workflow on the on-premises management center. The buyer's quote decides between them.

What splits the field is not throughput. Four of the five publish an edge unit big enough, and all five have one for the inside. The split is in what consolidation needs around the gateways: a supported migration tool and a built-in approval step. Palo Alto Networks stopped supporting its migration tool in January 2025, and its PAN-OS 12.1 commit page describes no approval step. HPE Juniper Networking publishes no threat-protection figure for the SRX4700, and its migration route is a service.

Still open, to settle before an order: the bank's own traffic mix against each vendor's test mix; Juniper's management capacity and log rate; any successor to Palo Alto Networks' Expedition; lead time and allocation at stage 4.

7 · Sources

Read with curl under a user agent that names Symbeeo and a contact address, one request at a time, no sign-in, between October 22 and 24, 2026, with retries after pauses. The date in brackets is the document's own.

- **K1** Check Point Quantum Force 9700 datasheet (July 8, 2026). https://www.checkpoint.com/downloads/products/quantum-force-9700-datasheet.pdf
- **K2** Check Point Quantum Spark 2500 datasheet (July 22, 2026). https://www.checkpoint.com/downloads/products/quantum-spark-2500-datasheet.pdf
- **K3** Check Point Smart-1 700-S and 700-M overview (April 16, 2026). https://sc1.checkpoint.com/documents/Appliances/GSG_Smart1_700SM/EN/Content/Topics-GSG-700-SM/Overview-700-SM.htm
- **K4** Check Point R82 Security Management, Management High Availability (October 12, 2026). https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_SecurityManagement_AdminGuide/Content/Topics-SECMG/Management-High-Availability.htm
- **K5** Check Point R82 Security Management, Session Flow for Administrators (October 12, 2026). https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_SecurityManagement_AdminGuide/Content/Topics-SECMG/Session-flow-for-Administrators.htm
- **K6** Check Point SmartMove, Check Point's own repository. https://raw.githubusercontent.com/CheckPointSW/SmartMove/master/README.md
- **P1** Palo Alto Networks Next-Generation Firewall Specifications and Features Summary (2026, PAN-OS 12.1). https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/product-summary-specsheet
- **P2** Palo Alto Networks Panorama product page. https://www.paloaltonetworks.com/network-security/panorama
- **P3** Palo Alto Networks Panorama datasheet (2025). https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/panorama-centralized-management-datasheet
- **P4** Palo Alto Networks Expedition documentation, end-of-life notice. https://pan.dev/expedition/docs/
- **P5** Palo Alto Networks PAN-OS 12.1 help, Panorama > Setup > Interfaces, logging rates. https://docs.paloaltonetworks.com/ngfw/help/12-1/panorama-web-interface/panorama-setup-interfaces

© 2026 Symbeeo. All rights reserved. · Public

- **P6** Palo Alto Networks PAN-OS 12.1 help, Panorama Commit Operations (updated July 9, 2026). https://docs.paloaltonetworks.com/ngfw/help/12-1/panorama-web-interface/panorama-commit-operations
- **F1** Fortinet FortiGate 900G Series datasheet (September 29, 2026). https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-900g-series.pdf
- **F2** Fortinet Product Matrix (October 2026). https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/Fortinet_Product_Matrix.pdf
- **F3** Fortinet FortiManager datasheet (April 21, 2026). https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf
- **F4** Fortinet FortiAnalyzer datasheet (July 15, 2026). https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortianalyzer.pdf
- **F5** Fortinet FortiConverter Tool 7.0.3, supported versions and conversions. https://docs.fortinet.com/document/forticonverter/7.0.3/online-help/220359
- **C1** Cisco Secure Firewall 3100 Series data sheet (updated October 6, 2026). https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.html
- **C2** Cisco Secure Firewall 1200 Series data sheet (updated July 9, 2025). https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-1200-series-ds.html
- **C3** Cisco Secure Firewall Management Center x800 Series data sheet (2026). https://www.cisco.com/c/en/us/products/collateral/security/firesight-management-center/x800-series-ds.pdf
- **C4** Cisco Secure Firewall Migration Tool 10.0.3 release notes (May 13, 2026). https://www.cisco.com/c/en/us/td/docs/security/firepower/migration-tool/b_cisco-secure-firewall-migration-tool-release-notes-10-0-3.html
- **C5** Cisco Security Cloud Control, Change Management, cloud-delivered management center (April 28, 2026; section headings read, body loads by script). https://securitydocs.cisco.com/docs/scc-fw/ftd/manage/74221.dita
- **J1** Juniper SRX4300 hardware specifications. https://apps.juniper.net/hct/product/SRX4300/hwspecs
- **J2** Juniper SRX4700 hardware specifications. https://apps.juniper.net/hct/product/SRX4700/hwspecs
- **J3** Juniper SRX1600 hardware specifications. https://apps.juniper.net/hct/product/SRX1600/hwspecs
- **J4** Junos Space Security Director 26.1, Change Control Workflow. https://www.juniper.net/documentation/us/en/software/nm-apps26.1/junos-space-security-director/topics/task/junos-space-security-director-ccw-example.html
- **J5** Junos Space 26.1, Disaster Recovery Overview. https://www.juniper.net/documentation/us/en/software/junos-space26.1/junos-space-high-availability/topics/concept/disaster-recovery-overview.html

Tried, with retries after pauses. Juniper's product pages and datasheets now redirect to hpe.com, which timed out on every try; the SRX4700 sizing and the SRX migration service are not confirmed from the public documents we could open; Palo Alto Networks' community notice on Expedition refused the request (403), so the same notice was read on pan.dev; Fortinet's FortiConverter datasheet address returned 404; Check Point's SmartMove support article loads by script.

© 2026 Symbeeo. All rights reserved. · Public

8 · The assessor

WRITTEN BY

David Morgan

Principal Security Architect

CCISO, CISSP, CISSP-ISSEP, CISM, CISA, CRISC, PMP, CCSP

Issued by Symbeeo.

© 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.

CMP-SEC-001 · Version 1.1 · Nov 7, 2026