SYMBEEO

PUBLIC

DESIGN STUDY

Arena payments on event days: PCI DSS 4.0.1 segmentation at point of sale, guest apart from operations

Complete design on current platforms

CAPABILITY	INDUSTRY	SETTING
Security	Sports & Entertainment	Arena operator
DOCUMENT	**VERSION**	**DATE**
SEC-007	1.1	Oct 10, 2026

WRITTEN BY

David Morgan, Principal Security Architect

© 2026 Symbeeo. All rights reserved.

Document control

Document	SEC-007	Version	1.1
Issued	Oct 10, 2026	Status	Issued by Symbeeo
Classification	Public	Supersedes	1.0, Sep 27, 2026
Capability	Security	Industry	Sports & Entertainment
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 6
4 · Design by subsystem 7
5 · Failure behavior 8
6 · Limits 8
7 · Lessons learned 8
8 · The author 9

© 2026 Symbeeo. All rights reserved. · Public

CONVENTIONS

Source tags. [S] figure or clause read from the vendor's or standards body's own current page or document on Sep 25, 2026 · [S*] figure from a page summary or a faithful copy where the owner's own page could not be opened · [A] assumption about 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 27, 2026	1.0	First issue.
Oct 10, 2026	1.1	Approval line now reads: approved by the Founder, issued by Symbeeo. David Morgan remains the author.

1 · Scope

Who it is for. The head of technology at an arena operator who takes card payments at several hundred points on 170 nights a year, shares the building's network with a concessionaire, a ticketing provider and 18,000 fans on guest Wi-Fi, and has to show the acquirer and the assessor where the cardholder data environment ends — and keep it that way on a night when someone wants a firewall change 40 minutes before doors.

Typical buyer [A]. An arena operator with an 18,500-seat multi-purpose arena: one resident team, concerts and family shows, about 170 event days a year. Two merchants take cards in the building: the arena itself (merchandise, box office, premium bars) and a third-party concessionaire (food and drink) with its own merchant ID. 240 fixed payment lanes, 360 handheld terminals, 12 box-office terminals, 64 ticket scanners at the gates, one guest Wi-Fi network. Internet is 2 × 10 Gbps from two providers. The arena's existing access switching and Wi-Fi stay.

What is in. The PCI DSS scope decision and the segmentation that holds it; network security controls (NSCs) between the payment zone, the operations zones and guest Wi-Fi; network access control on every wired and wireless port that can reach a payment device; logging for the retention PCI DSS asks for; the event-day change freeze and the test that follows any change to a segmentation control. **What is out.** The payment terminals and the P2PE solution itself (the acquirer's and the solution provider's); the ticketing platform (a SaaS provider); the e-commerce ticket channel; access switching and Wi-Fi hardware (retained); the building's physical security.

Assumptions. Every payment terminal in the building — both merchants' — is on one PCI-listed point-to-point encryption (P2PE) solution, so account data leaves each terminal already encrypted [A]. The acquirer accepts SAQ P2PE for both merchants [A]. Fortinet is the security vendor; FortiOS 7.6 is the baseline, as in SRA-SEC-001 [A]. The concessionaire agrees in writing to the responsibility split in §4.6 [A].

Related documents, read Sep 25, 2026.

- SRA-SEC-001, SDD-SEC-001, STP-SEC-001 — this capability's reference architecture, design and test plan (FortiGate 200G figures as read Sep 24, 2026 in SRA-SEC-001 R7)
- PCI DSS v4.0.1, Requirements and Testing Procedures (June 2024), PCI SSC's text; the Council's document library could not be opened and the text was read from a faithful copy — `https://www.middlebury.edu/sites/default/files/2025-01/PCI-DSS-v4_0_1.pdf`
- PCI SSC, Point-to-Point Encryption (P2PE) — `https://www.pcisecuritystandards.org/standards/point-to-point-encryption-p2pe/`

© 2026 Symbeeo. All rights reserved. · Public

- Fortinet FortiGate 900G Series data sheet (FG-900G-DAT-R22-20260605) — https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-900g-series.pdf
- Fortinet FortiNAC data sheet (FNC-DAT-R30-20260918) — https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortinac.pdf
- Fortinet FortiAnalyzer data sheet (FAZ-DAT-R88-20260715) — https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortianalyzer.pdf
- FortiOS 7.6 Administration Guide, HA active-passive cluster setup — https://docs.fortinet.com/document/fortigate/7.6.6/administration-guide/900885/ha-active-passive-cluster-setup

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. Information Supplement: PCI DSS Scoping and Segmentation Guidance for Modern Network Architectures, covering micro-segmentation, zero trust and verification of scope and segmentation controls; supplemental, it replaces no standard	PCI SSC · Sep 9, 2024	§3 and §4.1: the payment zone is drawn from the data flows and the systems connected to them, not from the VLAN plan; the segmentation test in R7 is the Council's verification method, not this document's	https://blog.pcisecuritystandards.org/new-information-supplement-pci-dss-scoping-and-segmentation-guidance-for-modern-network-architectures
Vendor documentation. Merchants using PCI-listed P2PE solutions "have fewer applicable PCI Data Security Standard (PCI DSS) requirements"	PCI SSC · standards page, May 3, 2024, updated Jul 23, 2025	R3 and §4.1: encrypting in the terminal is the scope lever; segmentation is designed to full PCI DSS anyway (§4.1)	https://www.pcisecuritystandards.org/standards/point-to-point-encryption-p2pe/
Deployment. A 68,000-seat NFL stadium operator on FortiGate NGFWs, FortiAP, FortiSwitch, FortiExtender, FortiAnalyzer and FortiMonitor, carrying ticketing, concessions, merchandise sales and fan connectivity on game days, 15 years with one vendor	Fortinet blog · Mar 21, 2025	§3: the venue pattern — ticketing, concessions and fan traffic on one Fortinet estate — is published at stadium scale; the post gives no device counts or segmentation detail, so it settles the pattern, not the sizing	https://www.fortinet.com/blog/customer-stories/pittsburgh-steelers-leverage-fortinet-security-fabric-for-industry-leading-defense

2 · Requirements register

Table 3. Requirements register

#	Requirement	Value	Source
R1	Venue	18,500 seats · about 170 event days a year · two merchants	[A]

© 2026 Symbeeo. All rights reserved. · Public

#	Requirement	Value	Source
R2	Payment terminals (POI)	612: 240 fixed lanes, 360 handhelds, 12 box office	[A]
R3	Account data on the venue network	encrypted in the terminal by one PCI-listed P2PE solution; no merchant system sees clear account data	[A] solution; [S] P2PE page, fewer applicable requirements
R4	Inbound traffic to the payment zone	only traffic that is necessary; all other traffic specifically denied	[S] PCI DSS 1.3.1
R5	Wireless into the payment zone	NSCs between every wireless network and the payment zone; denied by default; only traffic with an authorized business purpose	[S] PCI DSS 1.3.3
R6	NSC configuration review	at least once every six months	[S] PCI DSS 1.2.7
R7	Segmentation penetration test	at least once every 12 months and after any change to segmentation controls or methods	[S] PCI DSS 11.4.5
R8	Retest timing	any change to a payment-zone NSC is retested (R7) before the next event day	[T]
R9	Wireless access point detection	at least once every three months [S] PCI DSS 11.2.1; and on every event day, doors to egress	[T] event day
R10	Terminal inspection	frequency and type set by a targeted risk analysis [S] PCI DSS 9.5.1.2.1; every handheld inspected at issue and at return on every event day	[T]
R11	Audit log retention	at least 12 months, the most recent three months immediately available	[S] PCI DSS 10.5.1
R12	Scope confirmation	at least once every 12 months and on significant change; each season's new concession layout treated as significant	[S] PCI DSS 12.5.2; [A] layout
R13	Venue firewall	FortiGate 900G: 30 Gbps threat protection, 31 Gbps NGFW, 42 Gbps IPS, 164 Gbps firewall, 28 million sessions, 1 RU, 4 × 25G SFP28, 4 × 10GE SFP+, 17 × GE RJ45	[S] FortiGate 900G data sheet
R14	Payment-zone firewall	FortiGate 200G: 6 Gbps threat protection, 7 Gbps NGFW, 9 Gbps IPS, 8 × 10GE SFP+, 8 × 5GE RJ45	[S] via SRA-SEC-001 R7
R15	Load ceiling	peak design load at or below 50 % of the published figure for the features turned on	[A] design rule
R16	Network access control	FortiNAC-CA-500F, up to 15,000 managed endpoints; 3,200 non-guest endpoints in the arena	[S] FortiNAC data sheet; [A] count

© 2026 Symbeeo. All rights reserved. · Public

#	Requirement	Value	Source
R17	Logging	FortiAnalyzer 1000G: 660 GB/day, 20,000 logs/s analytics sustained, 32 TB, 60 days of analytics at the full sustained rate	[S] FortiAnalyzer data sheet
R18	Event-day change freeze	24 h before doors to 2 h after the building clears; no payment-zone NSC change inside it	[T]

Eighteen rows; thirteen carry a standards body's or vendor's figure, three are design assumptions, two are design targets.

3 · Architecture overview

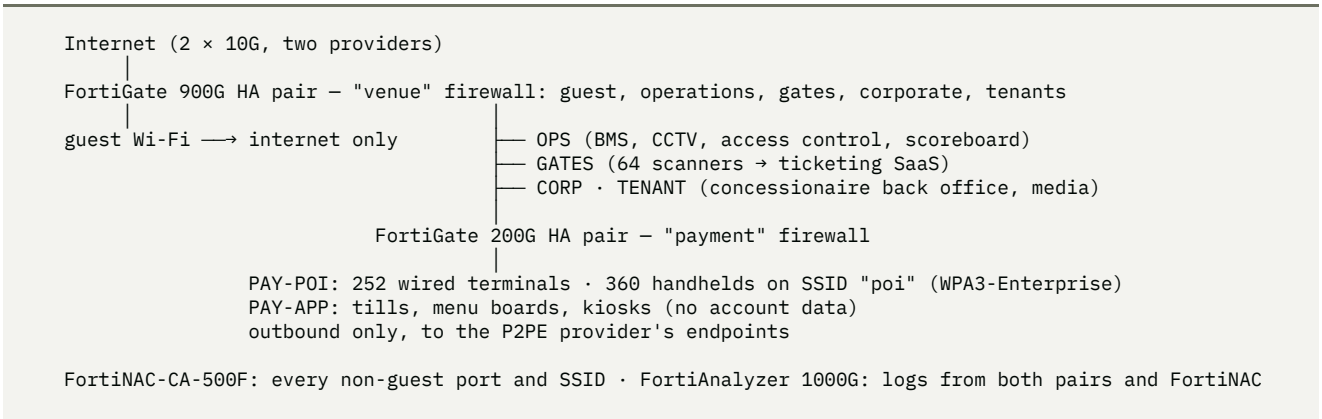


Figure 1. Venue and payment segmentation

Two firewall pairs, not one. The venue pair carries everything that changes often — guest capacity, a promoter's production network, a new sponsor kiosk. The payment pair carries only the payment zone and its rule base changes only in change weeks. Every wireless network reaches the payment zone through the payment pair (R5), including the handheld SSID, which lands in the payment zone rather than beside it.

Table 4. Architecture overview

Role	Product (exact model)	Qty	Capacity used	Why this unit
Venue firewall	Fortinet FortiGate 900G	2 (HA pair)	9 Gbps event-day peak of 30 Gbps threat protection, 30 % [A]/[S]	Inside the 50 % ceiling (R15) at the event-day peak; 25G ports to the core [S]
Payment firewall	Fortinet FortiGate 200G	2 (HA pair)	under 200 Mbps of 6 Gbps threat protection, under 4 % [A]/[S]	Sized for port count and change isolation, not throughput; 8 × 10GE SFP+ [S]
Network access control	Fortinet FortiNAC-CA-500F	2 [A]	3,200 of 15,000 endpoints, 21 % [A]/[S]	Standalone control and application server; 4 × GbE RJ45; 1 RU [S]
Logging	Fortinet FortiAnalyzer 1000G	1	6,000 logs/s event-day peak of 20,000, 30 % [A]/[S]	660 GB/day, 32 TB [S]; retention checked against R11 in §4.5

© 2026 Symbeeo. All rights reserved. · Public

4 · Design by subsystem

4.1 Scope.

The P2PE solution reduces the requirements that apply (R3) [S]; the design does not lean on that reduction. The payment zone is segmented to the full PCI DSS standard — NSCs, the six- monthly review, the segmentation test — so that if the acquirer withdraws SAQ P2PE eligibility, or a terminal type outside the solution arrives with a new bar operator, the building is not in scope overnight [A]. The zone holds the terminals (PAY-POI) and the tills and menu boards that drive them (PAY-APP); the tills never receive account data but can affect a transaction, so they sit behind the same pair [A]. The scope statement is confirmed each close season and whenever the concession layout changes (R12). Rejected: a flat payment VLAN on the venue firewall — every venue change would become a change to a segmentation control, and R7 would trigger a retest most weeks.

4.2 Payment firewall.

FortiGate 200G pair in FGCP active-passive: one primary processes traffic, the secondary synchronizes configuration and sessions [S] FortiOS 7.6 guide. Inbound to PAY-POI: nothing (R4). Outbound: HTTPS to the P2PE provider's published endpoints by address object; DNS and NTP to two internal servers; nothing else [A]. PAY-APP to PAY-POI: the semi-integrated terminal protocol on one port per till pair [A]. Rejected: a VDOM on the 900G — cheaper, but a firmware upgrade or HA event on the venue pair then touches the payment zone.

4.3 Venue firewall and guest Wi-Fi.

FortiGate 900G pair, active-passive [S]. Guest Wi-Fi lands in its own zone with a route to the internet and nowhere else; it has no path to the payment pair (R5) [A]. The ticket scanners (GATES) reach the ticketing SaaS only; OPS reaches its vendors' remote-support brokers only. Sizing: 8 Gbps guest peak plus 1 Gbps other traffic [A] against 30 Gbps threat protection [S] is 30 %, under the 50 % ceiling (R15). Rejected: one 900G — the ceiling holds on one unit, but the arena has no maintenance window during a 170-night season in which to replace it.

4.4 Network access control.

FortiNAC on every non-guest wired port and SSID [A]. Terminals are admitted by MAC and certificate where the model supports it, else by MAC and profile, and only on ports provisioned for them; a terminal moved to a bar that has no terminal port is refused, not re-homed [A]. Handhelds use a WPA3-Enterprise SSID that maps to PAY-POI [A]. Rogue access points: the retained WLAN's scanning radios report every event day (R9); the concessionaire's and promoters' hotspots are recorded as authorized or not before doors [A].

4.5 Logging.

Both pairs, FortiNAC and the WLAN controller log to FortiAnalyzer [A]. R11 needs 90 days immediately available; the data sheet gives 60 days of analytics at the full sustained rate of 20,000 logs/s [S]. The arena's rate is under a third of that on event days and far lower between them [A], so 90 days is expected to fit, and is measured at first build; 12-month history is archived off-box [A].

4.6 Two merchants, one building.

Both merchants' terminals sit in PAY-POI on the same P2PE solution [A], so the venue network carries only encrypted account data for either. The operator's position is that this does not make it a service provider to the concessionaire; the QSA confirms it before first issue [A]. The written split (§1): the arena owns the network, the NSCs, NAC and logs; the concessionaire owns its terminals' inspection (R10) and its own SAQ [A].

© 2026 Symbeeo. All rights reserved. · Public

4.7 Event-day change freeze.

From 24 h before doors to 2 h after the building clears (R18) no change is made to the payment pair, FortiNAC terminal policy or the PAY SSID [T]. Venue-pair changes inside the freeze need the event technology lead and the security lead, named on the event sheet [A]. Payment-zone changes are batched into change weeks set against the event calendar, and each is followed by the segmentation test before the next event day (R7, R8) [T]. The six-monthly NSC review (R6) falls in the close season and at the season's midpoint break [A]. An emergency payment-zone change inside the freeze is allowed only to restore trading; it is retested the next working day and recorded as a significant change for R12 [A].

5 · Failure behavior

Table 5. Failure behavior

Failure	Behavior	Source
Primary of either firewall pair fails	secondary takes the primary role with synchronized sessions; terminals re-establish to the P2PE provider	[S] FGCP active-passive; [A] terminal retry
Both internet links lost	terminals fall back to the solution's offline or store-and-forward mode where the acquirer allows it; guest Wi-Fi off	[A]
FortiNAC unreachable	ports already admitted stay up; a newly plugged terminal waits; no port opens by default	[A]
Ticketing SaaS unreachable	scanners use their offline list; gate staff admit by printed exception	[A]
Handheld fails inspection at issue	withdrawn, bagged and reported to the acquirer; a spare issued	[A]

6 · Limits

- The design depends on one P2PE solution for every terminal; a second, non-listed payment method in the building changes the scope decision and this document.
- The service-provider question in §4.6 is the operator's position, not a ruling; the QSA decides it.
- FortiAnalyzer retention (R11) is expected, not shown: the published 60 days is at full rate and the arena's rate is an assumption until measured.
- The retained access switches and WLAN must support the NAC methods in §4.4; they are not surveyed here.
- A promoter arriving the day before doors with a network request is refused by design (R18).

7 · Lessons learned

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

© 2026 Symbeeo. All rights reserved. · Public

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-007 · Version 1.1 · Oct 10, 2026