SYMBEEO

PUBLIC

DESIGN STUDY

Application delivery and WAF for a public-sector portal at 50,000 concurrent users

Complete design on current platforms

CAPABILITY	INDUSTRY	SETTING
Security	Public Sector	National agency
DOCUMENT	VERSION	DATE
SEC-005	1.4	Oct 10, 2026

WRITTEN BY

David Morgan, Principal Security Architect

© 2026 Symbeeo. All rights reserved.

Document control

Document	SEC-005	Version	1.4
Issued	Oct 10, 2026	Status	Issued by Symbeeo
Classification	Public	Supersedes	1.3, Oct 7, 2026
Capability	Security	Industry	Public Sector
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 6
6 · Limits 7
7 · Lessons learned 7
8 · The author 7

© 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 7, 2026	1.3	One public deployment removed from §1c and the related documents; no figure depended on it.
Oct 10, 2026	1.4	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 digital services at a national agency whose citizen portal peaks on deadline days, who has been told by an audit that the WAF is in monitoring mode and TLS terminates in the clear inside the data center, and who needs both fixed without a peak-day outage.

Typical buyer [A]. A national agency's citizen portal: 50,000 concurrent sessions at peak, 2,000 new TLS handshakes per second at peak, 2 Gbps of application traffic at peak, 40 backend application servers in two data centers, a 30-day filing deadline each year that produces the peak.

What is in. Application delivery pair per data center; WAF in blocking mode with a tuned policy; TLS 1.3 from the citizen's browser to the backend; volumetric DDoS absorbed in a cloud scrubbing service before the data center; the method for moving the WAF from monitoring to blocking without false positives on the deadline. **What is out.** Identity for citizens; the application code; the DNS provider; the network between the data centers.

Assumptions. F5 is the application delivery, WAF and DDoS vendor [A]. Two data centers, each able to carry the full peak [A]. The portal is one web application and one JSON API [A]. The application servers support TLS 1.3 [A].

Related documents, read Sep 18, 2026. F5 rSeries appliance product page, `https://www.f5.com/products/big-ip-services/rseries-adc-hardware-appliance` · F5 rSeries platform specifications (r5000/r10000/r12000 platform guide), `https://techdocs.f5.com/en-us/hardware/platform-guide-r5000r10000-series/title--platform-specifications.html` · F5 WAF for BIG-IP, `https://www.f5.com/products/big-ip-services/advanced-waf` · F5 Distributed Cloud DDoS Mitigation, `https://www.f5.com/products/distributed-cloud-services/l3-and-l7-ddos-attack-mitigation` · F5 rSeries datasheet PDF, `https://www.f5.com/pdf/products/f5-application-delivery-controller-system-rseries-data-sheet.pdf` (could not be opened; not used for figures) · F5 case study, a national public-safety science agency on rSeries r4600 with BIG-IP LTM and Advanced WAF (published Aug 13, 2026), read Sep 20, 2026 and Sep 27, 2026, `https://www.f5.com/case-studies/a-public-safety-agency-secures-ai-data-delivery-with-f5`.

© 2026 Symbeeo. All rights reserved. · Public

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
Deployment. A national public-safety science agency put BIG-IP LTM, Advanced WAF, API security and access control on one rSeries r4600 enforcement point in front of its object-storage service, expanding backend clusters without re-pointing a client	F5 · Aug 13, 2026	R7, §3 and §4.1: an rSeries appliance as the single enforcement point for delivery and WAF in a public-sector agency is a published deployment; the page names the r4000-series unit, which this document rejects on tenancy grounds, so the family choice is this document's, not the record's	https://www.f5.com/case-studies/a-public-safety-agency-secures-ai-data-delivery-with-f5

The published public-sector deployment states no concurrency, TPS or attack-size figure, so R1, R5, R6 and R8 remain design assumptions.

2 · Requirements register

Table 3. Requirements register

#	Requirement	Value	Source
R1	Concurrent sessions	50,000	[T]
R2	WAF mode	blocking, on every virtual server	[T]
R3	TLS	1.3 from client to application delivery tier (TLS 1.2 client fallback logged until after the deadline, R14) and from that tier to every backend	[T]
R4	DDoS	volumetric attack absorbed before the application tier	[T]
R5	Peak TLS handshakes	2,000/s	[A]
R6	Peak throughput	2 Gbps application traffic	[A]
R7	Application delivery hardware, per unit	3.3M L7 RPS; 95 Gbps L4, 85 Gbps L7; 80K TPS RSA 2K, 50K TPS ECDHE-ECDSA P-256; 18 tenants	[S] r5000 Series
R8	Hardware headroom at peak	TLS at 4 % of 50K ECC TPS; throughput at 2.4 % of 85 Gbps L7	[A] derived from R5–R7
R9	WAF capabilities	OWASP Top 10 defenses, behavioral L7 DoS detection using machine learning, proactive bot defense, REST/JSON and GraphQL API protection	[S] F5 WAF for BIG-IP

© 2026 Symbeeo. All rights reserved. · Public

#	Requirement	Value	Source
R10	DDoS service	multi-terabit ingest capacity; L3–L7; Always Available or Always On; BGP-based redirection; 99.99 % uptime SLA on the managed option	[S] Distributed Cloud DDoS Mitigation
R11	DDoS mode chosen	Always On for the 30-day deadline period; Always Available the rest of the year	[A]
R12	Availability	active/standby pair per data center; the other data center carries the full peak	[A]
R13	WAF false-positive budget at cut to blocking	fewer than 1 blocked legitimate request per 10,000 on the deadline-week traffic replay	[A]
R14	Backend cipher policy	TLS 1.3 only on the backend pool; TLS 1.2 client fallback logged, disabled after the deadline	[A]

Fourteen rows; three carry a vendor figure, seven are design assumptions, four are design targets.

3 · Architecture overview

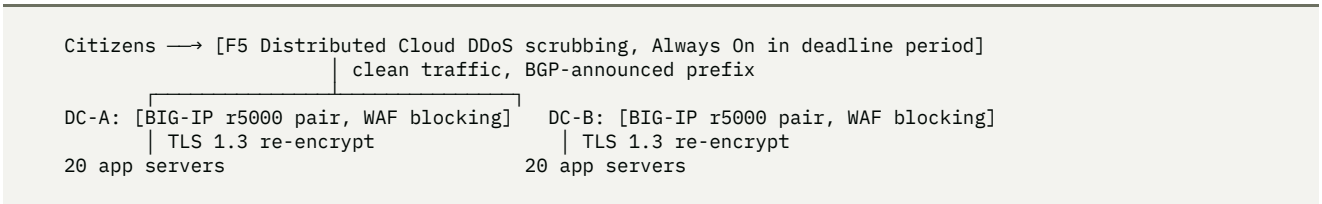


Figure 1. Portal delivery path

Scrubbing in front, one application delivery pair per data center running the WAF in blocking mode, TLS terminated and re-encrypted on the pair so inspection happens without a clear-text hop.

Table 4. Architecture overview

Role	Product (exact model)	Qty	Capacity used	Why this unit
Application delivery and WAF	F5 BIG-IP rSeries, r5000 Series (specific r5000 submodel confirmed at order)	4 (2 pairs)	2,000 of 50,000 ECC TPS; 2 of 85 Gbps L7 [A]/[S]	Smallest rSeries family with 10× headroom on the peak and enough tenants to separate web and API; 18 tenants [S]
WAF	F5 WAF for BIG-IP (Advanced WAF) on the pairs	4 licenses	one policy per virtual server, 2 virtual servers per DC [A]	Behavioral L7 DoS, bot defense, API protection [S]
Volumetric DDoS	F5 Distributed Cloud DDoS Mitigation	1 service, 2 protected prefixes	multi-terabit capacity against an assumed 400 Gbps attack [S]/[A]	Absorbs L3–L4 before the data center link [S]

© 2026 Symbeeo. All rights reserved. · Public

4 · Design by subsystem

4.1 Application delivery pair.

r5000 Series pair per data center, active/standby [A]. One virtual server for the web application, one for the JSON API, each in its own tenant so a WAF policy change on one cannot touch the other [S] tenancy, [A] use. Rejected: r4000 Series — 20K ECC TPS [S] leaves 10× headroom on R5 but the r5000's 18 tenants versus 4 [S] is what separates the API from the web tier; rejected: r10000 Series — 140K ECC TPS [S], unneeded at R5.

4.2 TLS.

Client-side TLS 1.3 with ECDHE P-256 certificates; server-side TLS 1.3 to every backend pool member, certificate pinned per pool [A]. No clear-text segment between the citizen and the application server (R3). The pair's SSL figures [S] are per unit, so a single surviving unit still carries R5 at 4 %.

4.3 WAF policy.

Start from the vendor's OWASP Top 10 template [S], learn for 30 days on mirrored production traffic in transparent mode, tune signatures against the deadline-week replay until R13 is met, then switch to blocking outside the deadline period [A]. API virtual server gets the JSON schema enforced from the agency's OpenAPI definition [A]. Behavioral L7 DoS on, bot defense on with the agency's known automated filers whitelisted by client certificate [A].

4.4 Volumetric DDoS.

The portal prefix is announced through F5 Distributed Cloud in Always On mode for the deadline month and Always Available otherwise (R11); redirection is BGP-based [S]. Application-layer floods that pass the scrubber meet the WAF's behavioral L7 DoS [S].

4.5 Data-center failover.

DNS steering between the two data centers is the agency's existing service; each pair is sized for the full peak (R12) so failover is a DNS change, not a capacity event.

4.6 Change control for the deadline.

Policy freeze from 7 days before the deadline window to 2 days after; only signature updates from the vendor and emergency blocks by the on-call engineer [A].

5 · Failure behavior

Table 5. Failure behavior

Failure	Behavior	Source
Active unit in a pair fails	Standby takes over with connection mirroring; TLS sessions renegotiate where mirroring does not cover them	[A]
Whole data center lost	DNS steers to the other DC; that DC's pair carries the full 50,000 sessions at the headroom in R8	[A]
WAF false positive on a live citizen flow	Request blocked with a support ID; on-call engineer converts to a learning suggestion; policy change inside the freeze only by that path	[A]

© 2026 Symbeeo. All rights reserved. · Public

Failure	Behavior	Source
Volumetric attack above the data-center link	Absorbed by the scrubbing service before the link; in Always Available mode, activation time applies	[S] capacity, [A] activation
Backend server fails TLS 1.3 handshake	Pool member marked down by the monitor; traffic to remaining members	[A]
Scrubbing provider reachability lost	Prefix withdrawn from the scrubber and announced directly; volumetric protection lost until restored	[A]

6 · Limits

- The specific r5000 submodel is not named because the model datasheet could not be opened; family figures are used and the submodel is set at order.
- The 2,000 TPS and 2 Gbps peak figures are assumptions; the agency's last deadline period is measured before the model is fixed.
- WAF blocking mode is only as good as the learning period's traffic; a new portal release during the deadline resets the false-positive budget.
- Always On scrubbing adds latency on the citizen path; the figure is measured in the first year.
- Client TLS 1.2 fallback is logged and disabled after the deadline (R14).

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-005 · Version 1.4 · Oct 10, 2026