

PKIFACTOR BY ZETACERT · DEPLOYMENT GUIDE

Deploying & managing certificates on F5 BIG-IP

2026-08-30 · PKIFactor v1.5.144 · captured on BIG-IP VE 17.5.1.8

A screen-by-screen walkthrough of the PKIFactor interface — from connecting a BIG-IP with a least-privilege account to hitless rotation, all-CA governance and a live cryptographic posture (CBOM) of the estate.

PKIFactor manages certificates on **F5® BIG-IP® Local Traffic Manager™ (LTM)** and complements the **F5® Application Delivery and Security Platform (ADSP)**: F5 ADSP delivers and secures the applications; **PKIFactor** governs the certificate lifecycle behind them. Captured live on a lab BIG-IP (v17.5.1.8), no environment variables — every setting is in the UI.

WHAT YOU'LL SEE

1. **Connect the F5** — least-privilege endpoint, partition probe, key custody
2. **Discover the estate** — live TLS inventory, full coverage
3. **Bindings & lifecycle** — link, renew, provision, hitless rotate, veto
4. **Crypto visibility** — posture & CBOM across the fleet

1 CONNECT THE F5 BIG-IP

Declare the appliance with a least-privilege iControl® account and prove the connection before a single byte is written.

1 Endpoints overview

Menu **Endpoints****Add an F5**

The estate landing page: appliances PKIFactor pushes and renews certificates on. Here, one **F5-1** BIG-IP with **8 bindings**, **0 drift** and **0 failures**. Open the endpoint to drive it.

Dashboard > Endpoints
EN
admin Admin

Endpoints

The appliances (F5 BIG-IP) on which PKIFactor pushes and renews certificates. Automatic renewal and deployment at D-X, with safeguards and per-binding veto.

+ Add an F5

1 Endpoints

0 Unreachable

8 Bindings

0 Planned (7d)

0 Drift

0 Failures

0 Paused

Deployment defaults
j-30

NAME	VERSION	CONTACT	BINDINGS	ACTIONS
F5-1 F5 BIG-IP	17.5.1.8	r�seau contact@zetacert.com	8	Open →

F1 Endpoints — one F5-1 BIG-IP under management: 8 bindings, 0 drift, 0 failures. "Open" drives the endpoint.

2 Add the endpoint — connection & partition probe

Fill the **iControl REST connection** with a least-privilege **service account** (`svc-pkifactor-f5`) — never the Administrator role. Two least-privilege options: **Install crypto via SOAP** (runs the whole deployment under a resource-admin account) and **Resolve the served cert's SPKI** (key-stable anti-drift signal). Then **Test & detect partitions** probes the box.

Endpoints > Add an F5

Add an F5 BIG-IP

Least-privilege iControl account; never Administrator in production.

Name *
F5-1

Description
BIG-IP VE — lab HA pair (unit 1)

Connector type
F5 BIG-IP

iControl REST connection

Management host *
f5-1.lab.zetacert.com

Service account *
svc-pkifactor-f5

Password *

☒ Verify the management TLS certificate

☒ Test & detect partitions

☐ Resolve the served cert's SPKI (SOAP) — key-stable anti-drift signal

☒ Install crypto via SOAP (least-privilege, no Administrator)

Import cert and key with the inline SOAP import instead of the Administrator-only file transfer (on by default). With it off, a private key is never uploaded through the file-transfer path (clear-text residue on the appliance): push_both bindings are refused, cert-only installs still work.

☒ Follow the ACTIVE unit of the HA pair

If the configured host is the standby member of a device-group, writes are sent to the active member automatically (management address read from the pair, same credentials). A failover then needs no reconfiguration. If the active peer cannot be reached, the write is refused — never done on the standby.

F2 Add an F5 — iControl REST connection with a least-privilege service account; "Test & detect partitions" probes the box before anything is written. "Follow the ACTIVE unit of the HA pair" keeps every write on the active member.

F5-1

F5 BIG-IP v17.5.1.8 contact@zetacert.com

Default D-X

30



Discover estate



Edit



Test connection

✓ OK -- BIG-IP 17.5.1.8 [zeta-dg: In Sync, standby] -- NOTE: this unit is STANDBY; writes will follow the ACTIVE member f5-2.lab.zetacert.com (10.20.10.61) with the same credentials -- NOTE: ce compte ne peut pas lire les déclarations AS3 ; les profils pilotés par AS3 ne seront pas reconnus comme tels -- NOTE (least-privilege): account has ALL-PARTITIONS access but this target only writes to 'automation' -- for strict least-privilege use a partition-scoped custom role (note: the built-in resource-administrator is all-partitions by design) or rely on the managed-partition allowlist - csr-on-device REST available

F3 Connection test — BIG-IP 17.5.1.8, HA pair detected (zeta-dg: In Sync). The configured unit is the standby member of the lab pair: PKIFactor says so and routes every write to the ACTIVE member (f5-2) with the same credentials, never to the standby. The least-privilege scope is checked too: the account only writes to the managed partition (automation).

3 Add the endpoint — key custody & create

Choose **on-device key custody**. With an external **network HSM** (partition **HSM-ZETACERT**, PKCS#11) the private key is minted and held on the appliance and **never exported** — bindings then use **csr_on_device**. Set the owner team (daily digest + veto), the default **D-X** and the default **automation level** (**Full auto** — install & activate, or **Install** — deposited, you activate), then **Create endpoint**.

Safe by default: whatever the level, PKIFactor never writes to a standby unit, never overwrites an out-of-band change (it holds), and installs the private key only through the least-privilege SOAP path.

On-device key custody

nethSM — external network HSM (PK

nethSM partition *

HSM-ZETACERT

Where the appliance mints the key for a `csr_on_device` deployment. Anything but 'normal' keeps the private key inside the HSM, never exportable: this endpoint then refuses any key push, and its bindings must use `csr_on_device` custody. The HSM brand is none of the CLM's business: the appliance's own external-HSM configuration (PKCS#11 library) answers. Requires the FIPS / External-HSM module to be licensed AND active on the BIG-IP.

Owner team

Receives the daily digest of scheduled deployments (advance notice + veto).

Contact name

Network team

Email

network@zetacert.com

Default D-X for this F5 (days before expiry)

30

Each binding on this F5 inherits this D-X (still overridable per binding).

Automation

Full auto — issue, renew, install & activate

Inherited by each new binding on this F5 (still overridable per binding).

✓ Create endpoint

Cancel

F4 Key custody — external network HSM (partition HSM-ZETACERT): the key is born on the appliance, never exported. Owner team, default D-X and default automation level (Full auto — install & activate), then Create endpoint.

2 DISCOVER THE ESTATE

Inventory what the F5 actually serves — read-only, nothing is modified.

4 Discover estate

Endpoint **F5-1**



Discover estate

A live inventory of the TLS objects served by the BIG-IP appliance, along the chain **virtual server** → **client-SSL profile** → **served certificate**. Every object here is already **Managed** — full coverage of the fleet.

F5-1

F5 BIG-IP v17.5.1.8 contact@zetacert.com

Default D-X

30



Discover estate



Edit



Test connection

F5

From the endpoint header, "Discover estate" reads the live TLS objects served by the BIG-IP appliance.

Endpoints > F5-1 > Discovery

EN

admin

Admin

Estate discovery

Live inventory of the TLS objects served by this F5 (virtual server → client-SSL profile → certificate). The entry point for onboarding and reconciliation.

Refresh

By CA

Attach all

Filter: VS, profile, CN...

7 / 7 TLS object(s) discovered

VIRTUAL SERVER	CLIENT-SSL PROFILE	SERVED CERTIFICATE	EXPIRY	STATUS	ACTION
/automation/vs_bastion_https	/automation/cssl_bastion	bastion.zetacert.lan 3b0000008aee20dc...	Aug 21 14:17:44 2027 GMT	Managed	
/automation/vs_ejbca_https	/automation/cssl_ejbca	ejbca.zetacert.lan 3b000000997ef7206...	Aug 28 10:05:06 2027 GMT	Managed	
/automation/vs_ldaps	/automation/cssl_ldap	ldap.zetacert.lan 3b00000002a362e18...	Aug 6 21:41:05 2027 GMT	Managed	
/automation/vs_pve_https	/automation/cssl_pve	pve.zetacert.lan 3b0000002020c9ef...	Aug 6 21:40:53 2027 GMT	Managed	
/automation/vs_sso_https	/automation/cssl_sso	sso.zetacert.lan 3b00000000d0451c...	Aug 22 02:19:49 2027 GMT	Managed	
/automation/vs_vault_https	/automation/cssl_vault	vault.zetacert.lan 3b0000000757f67db...	Aug 16 00:59:20 2027 GMT	Managed	
/automation/vs_web_https	/automation/cssl_web	pki.zetacert.lan 3b00000008f5048fb...	Aug 22 02:22:25 2027 GMT	Managed	

F6

Estate discovery — 7 TLS objects (virtual server → client-SSL profile → served certificate), every one Managed.

3 BINDINGS & LIFECYCLE

Link a certificate to a profile, then run the whole lifecycle — renew, provision on-device, hitless rotation — each write gated by the safe-deployment policy.

5 Bindings overview

The 8 deployed certificates. Each row shows its **automation level** (**Full auto** / **Install**), **key custody** (**key on device** / **key pushed**), **state** (**verified** / **idle** / **deployed-unverified**) and next deploy date. The last row is a **server-ssl** binding — outbound mTLS — alongside the client-ssl ones.

Bindings — deployed certificates + Add a binding

VS / profile... Served CN... All modes All states Clear 8 / 8

VIRTUAL SERVER / PROFILE	SERVED CERTIFICATE	MODE	STATE	DEPLOY	VETO
/automation/vs_ejbca_https /automation/cssl_ejbca	ejbca.zetacert.ian RSA-2048 TLS 1.0	Full auto key on device	verified	2027-07-29 auto - D-30	Pause
/automation/vs_pve_https /automation/cssl_pve	pve.zetacert.ian RSA-2048 TLS 1.0	Install key on device	idle	manual	Pause
/automation/vs_bastion_https /automation/cssl_bastion	bastion.zetacert.ian RSA-2048 TLS 1.0	Full auto key on device	verified	2027-07-22 auto - D-30	Pause
/automation/vs_sso_https /automation/cssl_sso	sso.zetacert.ian RSA-2048 TLS 1.0	Full auto key pushed	verified	manual	Pause
/automation/vs_vault_https /automation/cssl_vault	vault.zetacert.ian RSA-4096 TLS 1.0	Provide key pushed	idle	manual	Pause
/automation/vs_web_https /automation/cssl_web	pki.zetacert.ian RSA-2048 TLS 1.0	Full auto key pushed	verified	manual	Pause
— /automation/ssl_srv_partner	—	Install key on device	deployed (unverified)	manual	Pause
/automation/vs_idaps /automation/cssl_idap	ldap.zetacert.ian RSA-2048 TLS 1.0	Install key on device	idle	manual	Pause

F7 Bindings — 8 deployed certificates with automation level (Full auto, Install, Provide), key custody (key on device / key pushed), state and next-deploy date; ssl_srv_partner is a server-ssl outbound-mTLS binding.

/automation/vs_ejbca_https /automation/cssl_ejbca	ejbca.zetacert.ian RSA-2048 TLS 1.0	Full auto key on device	verified	2027-07-29 auto - D-30	Pause
--	--	----------------------------	----------	---------------------------	--------------------

F8 One binding at a glance: virtual server and profile, served cert (RSA-2048, TLS 1.0 flagged), automation level, key custody, verified state and D-30 schedule.

6 Link a certificate — the three axes

Endpoint → Add a binding

TLS ROLE

profile_type

client-ssl — server cert to inbound clients

server-ssl — client cert for outbound mTLS

forward-proxy-ca — TLS inspection CA

KEY CUSTODY

custody_mode

csr_on_device — key born on the box, never leaves

push_both — key pushed by PKIFactor

AUTOMATION

automation

Full auto — renewed at D-X, installed and activated, hands-off

Install — deposited (or provisioned on demand), you activate

ACME (advanced) — the appliance renews itself, PKIFactor supervises

API values: delivery_mode × auto_renew

On F5-1 — renewal and deployment will follow the guardrail policy.

F9 Link a certificate — the three axes: SSL profile type, key custody and automation level (Full auto — install & activate, or Install — you activate). Auto-renewal follows the level; only the D-X threshold is set here.

Per-binding controls: **auto-renew at D-X**, a one-click **Renew + deploy now**, the schedule, and **notice recipients** — pinned peers (mTLS partners, trust stores) warned ahead of a renewal via the D-X advance notice. They can veto by pausing the binding, and **never receive the private key**.

F10 Binding detail — Full auto level: hands-off renewal at D-30, one-click “Renew + deploy now”, schedule and notice recipients (peers warned ahead; never given the private key).

8 Provision the key on the appliance

Binding



Provision on appliance

For a `csr_on_device` binding, **Provision on appliance** generates the key **on the box / HSM**, the appliance produces the CSR, and PKIFactor gets it signed by the profile's CA. **The private key never traverses the wire.**

Endpoints > F5-1 > Binding #3

EN admin Admin

[/automation/vs_pve_https](#) [Edit binding](#) [Provision on appliance](#) [Renew + deploy now](#) [Pause...](#) [Delete binding](#)

[key on device](#) [Install](#)

Profile: /automation/cssl_pve Profile type: client-ssl - inbound Renewal: manual Deployed serial: -

Verify: unknown 2020-08-30 13:36 UTC

Identity

Certificate: pve.zetacert.1an #38 (ISSUED) Key algorithm: RSA-2048 (inherited from the certificate) Device key reuse: no — a new key at each renewal

Automation

Current level: Install — put in place, manual activate

Level: Install — put in place, manual activate [Save](#) Full auto = hands-off, install = deposited, you activate. The mechanism follows the key custody.

Schedule

D-X (days before expiry): 30 [Save](#)

Install with the key on the appliance: provisioning is MANUAL — no planned date. Trigger it with "Provision on device" when you decide; the threshold only drives the alerts.

Notice recipients

Peers (mTLS partners, pinned truststores) warned of an upcoming renewal via the D-X advance notice. If one objects, pause the binding (veto). They never receive the private key.

No subscribers.

Add a subscriber

Name: Contact (email/URL): Channel: Email [+ Add](#)

F11 `csr_on_device` binding at Install level — "Provision on appliance" mints the key on the box/HSM and gets its CSR signed by the profile's CA; the key never leaves the appliance.

9 Deploy & hitless rotation

Whatever the automation level, the operator keeps the hand: **Deploy now** installs and repoints the profile; **Hitless rotate** swaps the active cert-key-chain **atomically** — **no dropped connections**. The automation level is editable inline on the binding page.

Endpoints > F5-1 > Binding #11

admin Admin

/automation/vs_sso_https

verified Full auto key pushed

Edit binding Deploy now Renew + deploy now **Hitless rotate** Pause... Delete binding

Profile: /automation/cssl_sso Profile type: client-ssl · inbound Renewal: manual Deployed serial: 3b000000d8d451c...

Verify up to date: 2026-08-30 13:36 UTC

Identity

Certificate: sso.zetacert.lan #158 (ISSUED) Key algorithm: (inherited from the certificate) Device key reuse: no — a new key at each renewal

Automation

Current level: Full auto — install & activate

Level: Full auto — install & activate Save Full auto = hands-off, install = deposited, you activate. The mechanism follows the key custody.

Schedule

D-X (days before expiry): 30 Save

Automatic renewal is OFF on this binding (older configuration): save the automation level above to re-enable renewal at D-X.

Notice recipients

Peers (MTLS partners, pinned truststores) warned of an upcoming renewal via the D-X advance notice. If one objects, pause the binding (veto). They never receive the private key.

No subscribers.

Add a subscriber

Name: Contact (email/URL): Channel: Email + Add

F12 push_both binding at Full auto level — “Deploy now”, “Renew + deploy now” and “Hitless rotate” (atomic cert-key-chain swap, no dropped connections).

10 Pause & resume — the human veto

Your F5 team keeps control: **Pause** suspends automatic writes on a binding; **Resume** hands control back. Combined with the daily digest, this is the veto window before any change ships.

Endpoints > F5-1 > Binding #3

admin Admin

/automation/vs_pve_https

idle Install key on device

Edit binding Provision on appliance Renew + deploy now **Pause...** Delete binding

Profile: /automation/cssl_pve Profile type: client-ssl · inbound Renewal: manual

Verify unknown: 2026-08-30 13:36 UTC

Reason for pausing (why stop auto renew/deploy?):

test

Pausing stops automatic renewal and deployment for this binding only. Resume when the situation is cleared.

Confirm pause

F13 Human veto — “Pause...” opens an inline form: a reason is mandatory and kept in the record; nothing changes until “Confirm pause”.

Bindings — deployed certificates

+ Add a binding

VS / profile... Served CN... All modes All states Clear 8 / 8

VIRTUAL SERVER / PROFILE	SERVED CERTIFICATE	MODE	STATE	DEPLOY	VETO
/automation/vs_ejbca_https /automation/cssl_ejbca	ejbca.zetacert.lan RSA-2048 TLS 1.0	Full auto key on device	verified	2027-07-29 auto · D-30	Pause
/automation/vs_pve_https /automation/cssl_pve	pve.zetacert.lan RSA-2048 TLS 1.0	Install key on device	idle paused Paused: test	manual	Resume
/automation/vs_bastion_https /automation/cssl_bastion	bastion.zetacert.lan RSA-2048 TLS 1.0	Full auto key on device	verified	2027-07-22 auto · D-30	Pause

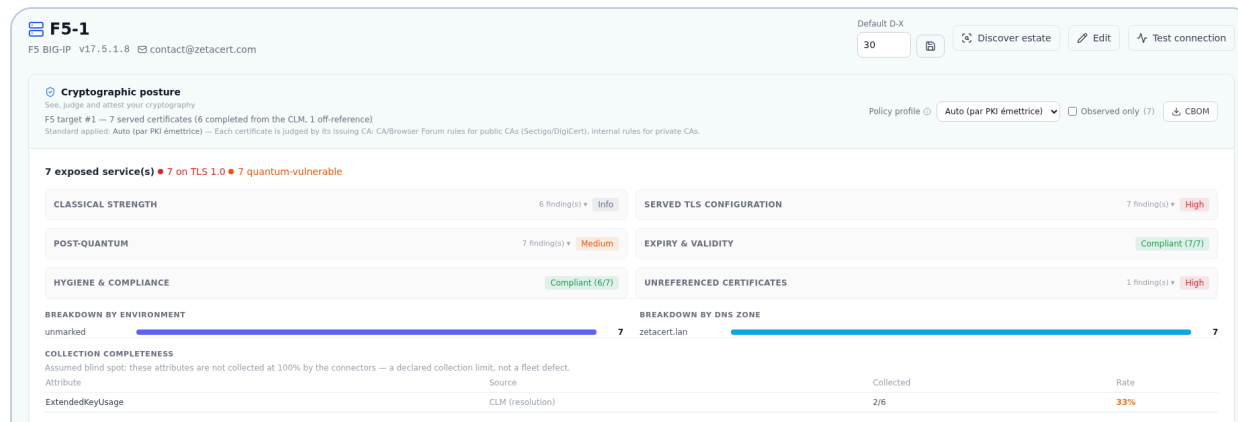
F14 A paused binding (reason recorded: “test”): automatic renewal and deployment are suspended for this binding only; “Resume” hands control back.

4 CRYPTO VISIBILITY & POSTURE

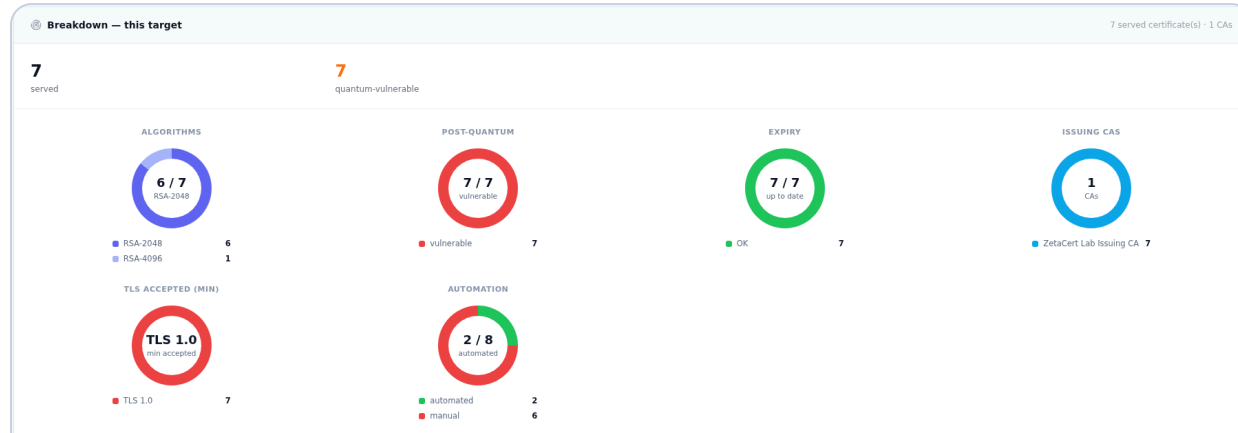
Beyond lifecycle: a live cryptographic posture (CBOM) of everything the BIG-IP appliance serves — classical strength, post-quantum exposure and TLS hardening.

11 Cryptographic posture & CBOM

A per-endpoint **CBOM** grades every served certificate across classical strength, post-quantum exposure, served TLS configuration, expiry, hygiene and unreferenced certs. Nothing is hidden: **7 services on TLS 1.0, 7 quantum-vulnerable**, each with an actionable, one-move remediation.



F15 Cryptographic posture — a per-endpoint CBOM: 7 served certificates graded across classical strength, post-quantum, TLS configuration, expiry, hygiene and unreferenced certs.



F16 Breakdown — algorithms (6× RSA-2048, 1× RSA-4096), post-quantum (7/7 vulnerable), expiry (7/7 up to date), issuing CAs (1), minimum TLS accepted (TLS 1.0) and automation coverage (2/8).

Post-quantum, stated plainly. F5 ADSP already supports post-quantum cryptography at the *transport* layer (hybrid TLS). PKIFactor governs the *certificate lifecycle* and maintains the CBOM so the classical-to-PQC migration can be staged in advance — ready to issue and manage PQC certificates the day the ecosystem supports them.

Served TLS configuration — 7 finding(s)

- High** ● OBSERVED **Profile « cssl_bastion »: 1 service(s) on TLS 1.0: obsolete version (RFC 8996)**
RFC 8996 — Deprecating TLS 1.0 and TLS 1.1 · bastion.zetacert.lan
→ Raise the minimum TLS version of profile « cssl_bastion » to 1.2 (ideally 1.3): fixes the 1 service(s) in one move
- High** ● OBSERVED **Profile « cssl_ejbca »: 1 service(s) on TLS 1.0: obsolete version (RFC 8996)**
RFC 8996 — Deprecating TLS 1.0 and TLS 1.1 · ejbca.zetacert.lan
→ Raise the minimum TLS version of profile « cssl_ejbca » to 1.2 (ideally 1.3): fixes the 1 service(s) in one move
- High** ● OBSERVED **Profile « cssl_ldap »: 1 service(s) on TLS 1.0: obsolete version (RFC 8996)**
RFC 8996 — Deprecating TLS 1.0 and TLS 1.1 · ldap.zetacert.lan
→ Raise the minimum TLS version of profile « cssl_ldap » to 1.2 (ideally 1.3): fixes the 1 service(s) in one move
- High** ● OBSERVED **Profile « cssl_pve »: 1 service(s) on TLS 1.0: obsolete version (RFC 8996)**
RFC 8996 — Deprecating TLS 1.0 and TLS 1.1 · pve.zetacert.lan
→ Raise the minimum TLS version of profile « cssl_pve » to 1.2 (ideally 1.3): fixes the 1 service(s) in one move
- High** ● OBSERVED **Profile « cssl_sso »: 1 service(s) on TLS 1.0: obsolete version (RFC 8996)**
RFC 8996 — Deprecating TLS 1.0 and TLS 1.1 · sso.zetacert.lan
→ Raise the minimum TLS version of profile « cssl_sso » to 1.2 (ideally 1.3): fixes the 1 service(s) in one move
- High** ● OBSERVED **Profile « cssl_vault »: 1 service(s) on TLS 1.0: obsolete version (RFC 8996)**
RFC 8996 — Deprecating TLS 1.0 and TLS 1.1 · vault.zetacert.lan
→ Raise the minimum TLS version of profile « cssl_vault » to 1.2 (ideally 1.3): fixes the 1 service(s) in one move
- High** ● OBSERVED **Profile « cssl_web »: 1 service(s) on TLS 1.0: obsolete version (RFC 8996)**
RFC 8996 — Deprecating TLS 1.0 and TLS 1.1 · pki.zetacert.lan
→ Raise the minimum TLS version of profile « cssl_web » to 1.2 (ideally 1.3): fixes the 1 service(s) in one move

F17 Served TLS findings — each profile still accepting TLS 1.0 is flagged High (RFC 8996) with a one-move remediation: raise the profile's minimum TLS version. Observed live on the box.

F5, BIG-IP, Local Traffic Manager, and iControl are trademarks, service marks, or trade names of F5, Inc., in the U.S. and other countries. PKIFactor is a product of ZetaCert.

Screens captured live on a lab BIG-IP (F5-1, v17.5.1.8); certificate names and hosts are lab values.