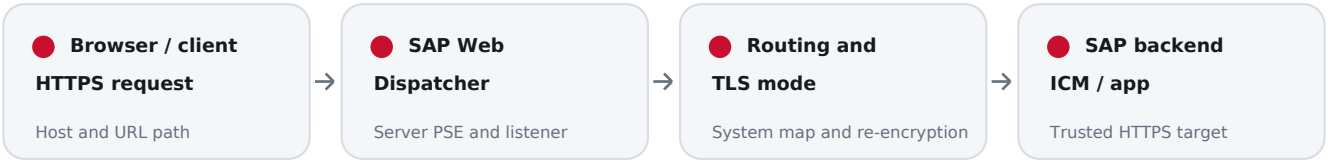
Web Dispatcher HTTPS Architecture

A controlled route from the public TLS endpoint to the intended SAP backend.

Request and trust path



Configuration sequence

1 DISCOVER

Inventory FQDNs, SAP backends, URL paths, ports, PSEs and current certificates.

2 DESIGN

Choose termination, re-encryption or end-to-end routing based on requirements.

3 CONFIGURE

Set listener and system routing; install server certificate and backend trust.

4 VALIDATE

Test TLS, routes and application flows; record traces and rollback steps.

Technical coverage

AREA	CONFIGURATION / CHECK	EVIDENCE / VALIDATION
HTTPS listener	Confirm incoming HTTPS port, external hostname and server PSE selection.	Profile values, browser certificate and reachability
Server identity	Check CSR, private key, SAN, signed certificate, intermediate CA and expiry.	PSE content, certificate chain and hostname match
Backend routing	Map virtual hosts/paths and verify message server or direct backend settings.	System status, route target and request trace
Backend TLS	For re-encryption, configure Web Dispatcher client PSE and trusted backend CA.	Backend handshake and certificate validation
Operations	Protect admin access, monitor errors and track certificate renewal and rollback.	Admin monitor, dev_webdisp trace and change record

Operational note: Distinguish the public server PSE from trust used for outgoing backend HTTPS. Confirm the intended TLS mode before changing profile parameters or replacing a certificate.