

HTTP/2–3 & TLS Sürüm/Cipher Tuning Checklist Şablonu — Yazılım / Sunucu ve Güvenlik (v1.0)

Asset Amaç: Bu asset; taşıma katmanı (*transport layer*) modernizasyonunu (HTTP/2, HTTP/3 QUIC ve TLS politikaları) güvenlik standartları ve performans optimizasyonu ile eş zamanlı olarak planlamak için hazırlanmıştır. Zayıf ve güvensiz protokol/cipher algoritmalarının kademeli ve ölçümlü bir şekilde kapatılmasını, CDN/ALB uç nokta (*edge*) optimizasyonu ile TLS el sıkışma (*handshake*) maliyetlerinin düşürülmesini hedefler. Core Web Vitals (CWV) ve TTFB (Time to First Byte) üzerindeki etkileri izlenmeden canlı ortama sert ve riski yüksek değişiklikler yapılmasını engeller.

Kim Kullanır?: DevOps / Backend Mühendisleri, Teknik SEO Uzmanları (Otel ve B2B Performans / Güvenlik Sahipleri).

Nasıl Kullanılır?

1. Mevcut HTTP/TLS altyapı envanterinizi çıkarın ve hedeflenen kurumsal TLS/Cipher politikasını dökümanente edin.
2. HTTP/2 varsayılan ve HTTP/3 (QUIC) pilot geçiş planını oluşturarak TTFB, CWV ve Handshake ölçüm KPI'larını izleme paneline bağlayın.
3. Eski TLS sürümleri ile güvensiz cipher'ların kapatılmasını kademeli olarak uygulayın; olası müşteri/eski tarayıcı etkileri için geri alma (*rollback*) prosedürünü hazır tutun.

CHECKLIST & SPRINT PLAN — HTTP/2–3 & TLS Sürüm/Cipher Tuning

1) Ölçüm & Önceliklendirme Kontrol Listesi (Checklist)

- **[] Mevcut HTTP Sürümü (1.1/2/3) Envanterlendi:** Origin, Load Balancer ve CDN katmanlarında desteklenen HTTP protokol sürümleri tespit edildi.
- **[] TLS Min Sürüm Hedefi (1.2/1.3) Yazıldı:** TLS 1.0 ve 1.1 protokollerinin tamamen kapatılması, minimum TLS 1.2 ve öncelikli TLS 1.3 hedefi netleştirildi.
- **[] Zayıf Protokol / Cipher Kapanış Planı Var (Kademeli):** CBC modlu şifreler, RSA key exchange ve zayıf algoritmaların kademeli devre dışı bırakılma takvimi hazırlandı.
- **[] Session Reuse / Resumption Hedefi Belirlendi:** TLS Session Tickets ve Session ID caching aktif edilerek tekrarlayan bağlantılarda handshake maliyeti düşürüldü.
- **[] CDN / ALB Terminasyon Ayarları Envanterlendi:** Edge (CDN) üzerindeki TLS terminasyonu ile Origin arasındaki TLS politikaları ayrıştırıldı ve optimize edildi.
- **[] Keep-Alive / Connection Reuse Kontrol Edildi:** TCP/QUIC keep-alive süreleri ve HTTP/2 multiplexing bağlantı limitleri gözden geçirildi.
- **[] CWV / TTFB Ölçüm Dashboard'u Hazır:** Değişiklik öncesi ve sonrası TTFB, LCP, INP ve Handshake sürelerini anlık izleyecek dashboard kuruldu.
- **[] Pilot Rollout Planı (Trafik Segmenti) Hazır:** Değişikliklerin ilk aşamada mobil trafik veya belirli bir coğrafi segment üzerinde denenmesi kurgulandı.
- **[] Rollback Prosedürü Yazıldı:** Herhangi bir regresyon veya eski cihaz uyumsuzluğu durumunda 5 dakika içinde eski TLS/cipher konfigürasyonuna dönüş adımları dökümanente edildi.

- **[] Değişiklik Sonrası Tarayıcı Uyumluluğu Test Edilecek:** Legacy mobil tarayıcılar, otel Smart TV sistemleri ve B2B API istemcilerinin uyumluluk testleri planlandı.

2) Problem → Kök Neden → Çözüm Tablosu

Problem	Kök Neden	Çözüm (Tuning Yaklaşımı)
Güvenlik Uyarısı / Legacy Risk	Eski TLS (1.0/1.1) ve güvensiz cipher'ların açık olması	TLS Policy güncelle $\mathbf{+}$ Zayıf cipher'ları kademeli kapat
TTFB (Time to First Byte) Yüksek	Yüksek el sıkışma (<i>handshake</i>) ve TCP bağlantı kurma maliyeti	TLS Session Reuse $\mathbf{+}$ Keep-Alive $\mathbf{+}$ Edge Termination
Mobilde Yavaş Bağlantı / Paket Kaybı	Yüksek latency'li mobil ağlar ve TCP head-of-line blocking	HTTP/3 (QUIC) Pilotu $\mathbf{+}$ UDP tabanlı taşıma ölçümü
Performans / Erişim Regresyonu	Ölçümsüz ve kontrolsüz sert altyapı değişiklikleri	KPI Dashboard $\mathbf{+}$ Pilot Rollout $\mathbf{+}$ Rollback Tatbikatı

3) 14 Günlük Uygulama Sprint Planı (Gün 1–14)

[Gün 1–4: Envanter & Policy] → [Gün 5–8: HTTP/3 & Staging Deneme] → [Gün 9–11: Prod Pilot & Rollback] → [Gün 12–14: Genişletme & Rapor]

- **Gün 1:** Mevcut HTTP/TLS envanterinin çıkarılması ve aktif kullanılan TLS/cipher parametrelerinin analizi.
- **Gün 2:** Hedef kurumsal TLS politikasının dökümante edilmesi (Min TLS 1.2, ECDHE+AESGCM/CHACHA20 öncelikli cipher seti).
- **Gün 3:** HTTP/2 varsayılan doğrulamasının yapılması ve performans baseline (TTFB/CWV) ölçümlerinin kaydedilmesi.
- **Gün 4:** CDN ve Application Load Balancer (ALB) üzerinde Keep-Alive ve TLS Session Resumption ayarlarının optimize edilmesi.
- **Gün 5:** Mobil trafik ve belirli kullanıcı grupları için HTTP/3 (QUIC) pilot planının hazırlanması.
- **Gün 6:** Zayıf protokollerin (TLS 1.0/1.1) ve eski cipher'ların kademeli kapatılma takviminin oluşturulması.

- **Gün 7:** Hazırlanan konfigürasyonların Staging veya düşük trafikli bir test ortamında uygulanması.
- **Gün 8:** Real User Monitoring (RUM) ile TTFB/CWV ölçüm dashboard'unun ve anomali alarmlarının kurulması.
- **Gün 9:** Prod ortamında pilot rollout (Trafığın %5-%10'luk kısmına yeni TLS/HTTP3 politikasının uygulanması).
- **Gün 10:** Canlı izleme, tarayıcı/cihaz uyumluluk kontrolleri ve regresyon analizi.
- **Gün 11:** Olası bir acil durumda geri dönüş hızını doğrulamak için Rollback prosedürü tatbikatı.
- **Gün 12:** Kademeli genişletme (Trafik oranının %50 → %100 seviyesine çıkarılması).
- **Gün 13:** Yeni konfigürasyonun dökümanite edilmesi ve IaC repositories üzerinde versiyonlanması.
- **Gün 14:** Yönetimsel sonuç raporunun sunulması ve yıllık (365 gün) TLS/Cipher gözden geçirme takviminin kilitlenmesi.

4) Öncesi / Sonrası KPI Tablosu

KPI Metriği	Önce (Mevcut Durum)	Sonra (Sprint Sonrası)	Hedef Yönü
TTFB (Time to First Byte)	~ 280 ms	< 120 ms	Hedef ↓ (Düşüş)
TLS Handshake Süresi	~ 110 ms (Full Handshake)	< 35 ms (Resumption / TLS 1.3)	Hedef ↓ (Düşüş)
Core Web Vitals (LCP / INP)	LCP: 3.2 s / INP: 240 ms	LCP: < 1.8 s / INP: < 100 ms	Hedef ↑ (İyileşme)
HTTP/2 & HTTP/3 Kullanım Oranı (%)	~60% HTTP/1.1 ~40% HTTP/2	~0% HTTP/1.1 ~75% HTTP/2 ~25% HTTP/3	Hedef ↑ (Yükselme)

Deliverables (Teslim Edilecek Çıktılar)

- **Güvenlik & Performans Odaklı TLS Policy Dokümanı (v1.0):** Minimum TLS sürümü, kabul edilen cipher suite'ler ve öncelik sıralaması rehberi.

- **HTTP/2 Default & HTTP/3 (QUIC) Pilot Geçiş Planı:** Origin ve CDN katmanlarında QUIC/HTTP3 aktifleştirme adımları.
- **CDN / ALB Edge Tuning & Session Optimization Notları:** TLS session resumption, ticket keys ve keep-alive konfigürasyon kılavuzu.
- **TTFB / CWV Ölçüm Raporu & Acil Durum Rollback Prosedürü:** Performans değişim analizi ve 5 dakikada eski ayarlara dönüş kılavuzu.



[Checklist Card]

DevOps mühendisleri, backend mimarları ve teknik SEO uzmanları için tasarlanmış, 1200x1200px (1:1) kare formatında yüksek çözünürlüklü bir HTTP/TLS Tuning Checklist Kartı. Koyu karbon gri ve parlak yeşil/siyan tonlarındaki teknolojik zemin üzerinde; HTTP/3 QUIC hızlandırıcı simgeleri, TLS 1.3 kilit ikonu, TTFB/CWV performans grafikleri ve 14 günlük tuning sprint takvimi yer alıyor. Kartın üzerinde; "Modern TLS 1.3 & Safe Cipher Suite Policy", "HTTP/3 (QUIC) & Session Resumption Tuning", "CDN/ALB Edge Handshake Optimization" ve "CWV & TTFB Performance Impact Dashboards" teslimat kalemi başlıkları, yanlarında parlak yeşil onay işaretleriyle scannable ve kurumsal bir checklist-card formatında sergileniyor.