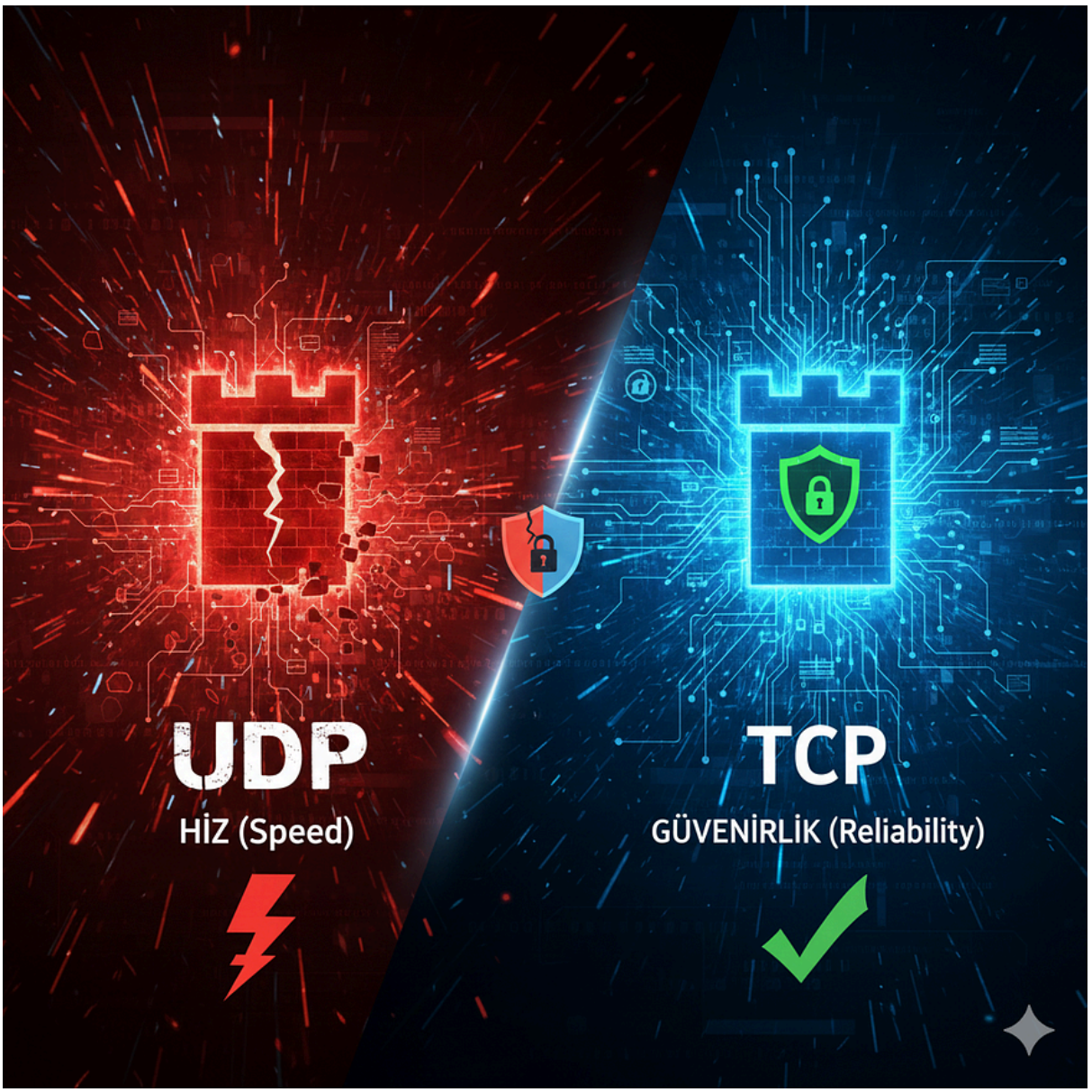
TCP VE UDP: SALDIRGANIN VE SAVUNMACININ GÖZÜNDEN İKİ FARKLI AĞ FELSEFESİ

Bilgisayar ağlarının temelinde yer alan TCP ve UDP, yalnızca veri aktarımı sağlayan teknik protokoller değil; hız, güvenilirlik ve kontrol arasında yapılan bilinçli tercihlerin sonucudur. Bu iki yaklaşım, internetin günlük işleyişinden siber saldırı yöntemlerine kadar geniş bir etki alanına sahiptir. Bu kısa blog yazısında TCP'nin güvenilirlik odaklı yapısı ile UDP'nin hız temelli, bağlantısız felsefesi ele alınacak; DDoS saldırıları ve port tarama teknikleri gibi siber güvenlik senaryoları üzerinden saldırgan ve savunmacı bakış açılarıyla karşılaştırmalı olarak incelenecektir.



Kısaca TCP Nedir?

TCP, ağ üzerinde veri aktarımı kontrollü ve güvenli şekilde gerçekleştiren bir protokoldür. İletişim başlamadan önce karşı tarafla bağlantı kurar ve gönderilen verilerin hedefe ulaşıp ulaşmadığını takip eder. Bu yapı sayesinde veri bütünlüğü korunur

ve aktarım sırasında oluşabilecek hatalar en aza indirilir. İnternette güvenilir veri aktarımının temel taşlarından biridir.

Kısaca UDP Nedir?

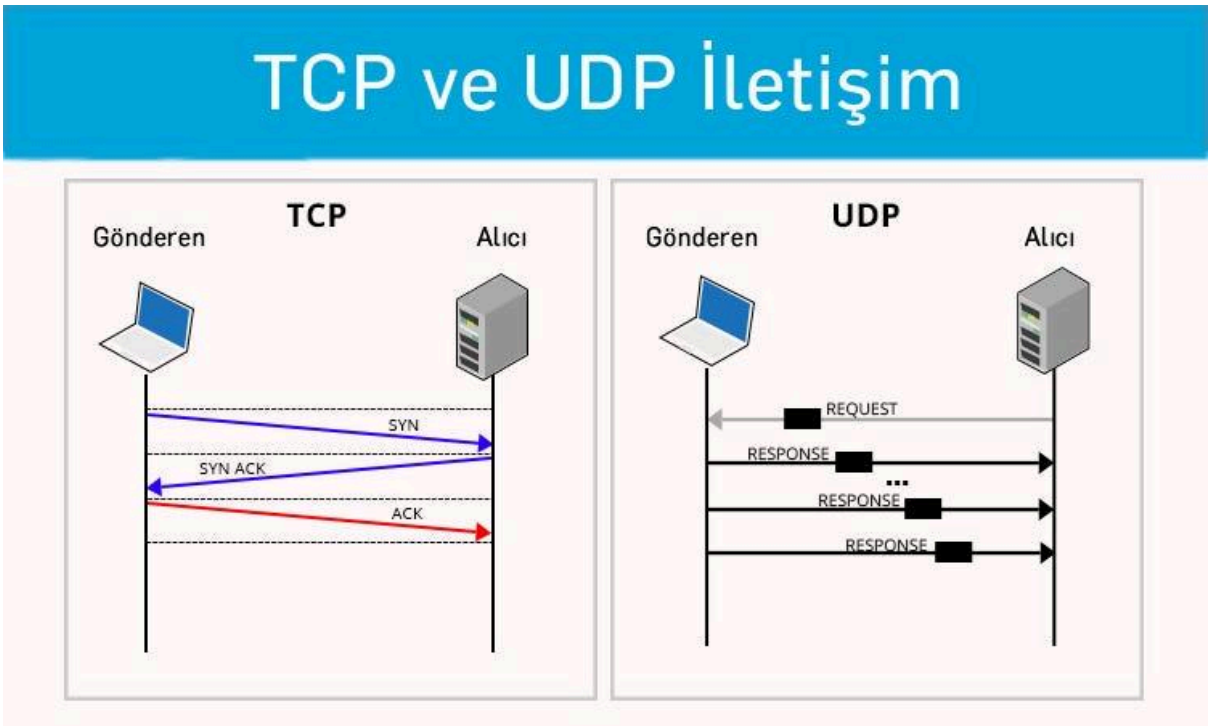
UDP, ağ üzerinde hızlı veri aktarımını sağlamak amacıyla tasarlanmış bir protokoldür. Bağlantı kurma süreci olmadan veri gönderir ve aktarımın durumunu kontrol etmez. Bu sayede düşük gecikme ile çalışır ve anlık veri akışının önemli olduğu sistemlerde yaygın olarak kullanılır. Basit ve hafif yapısı, performans gerektiren uygulamalarda tercih edilmesini sağlar.

GÜVENİLİRLİK VE HIZ: TCP VE UDP'NİN TEMEL YAKLAŞIMI

TCP, veri aktarımı başlamadan önce **Üçlü El Sıkışma (Three-Way Handshake)** süreciyle iki uç arasında güvenilir bir bağlantı kurar. Bu yapı sayesinde gönderilen verilerin sırası korunur, kaybolan paketler tespit edilip yeniden aktarılır. Bu da

TCP’yi dosya transferleri, e-posta ve web trafiği gibi güvenirliğin kritik olduğu senaryolar için ideal hale getirir.

UDP ise **bağlantısız** bir yapıya sahiptir. Veri gönderilmeden önce herhangi bir bağlantı kurulmaz ve paketlerin ulaşıp ulaşmadığı kontrol edilmez. Bu yaklaşım, UDP’yi son derece hızlı kılar. Gerçek zamanlı video yayınları, çevrim içi oyunlar ve sesli iletişim gibi hızın güvenirlikten daha önemli olduğu alanlarda UDP tercih edilir.



BU İKİ FESEFE SALDIRILAR VE PORT TARAMALARI GİBİ SİBER GÜVENLİK SENARYOLARINI NASIL ŞEKİLLENDİRİYOR?

TCP ve UDP'nin temel çalışma felsefeleri, siber güvenlik saldırılarının ve keşif tekniklerinin doğrudan şeklini belirler. TCP'nin bağlantı kurma zorunluluğu, **SYN Flood** gibi DDoS saldırılarının ortaya çıkmasına neden olmuştur. Bu saldırı türünde, saldırgan hedef sunucuya çok sayıda **SYN paketi** gönderir ancak bağlantıyı tamamlamaz. Sunucu, yarım kalan bağlantılar için kaynak ayırmaya devam ettiği için zamanla hizmet veremez hale gelir. Yani TCP'nin güvenilirlik odaklı yapısı, yanlış kullanıldığında bir zafiyete dönüşebilir.

UDP ise bağlantısız yapısı nedeniyle farklı bir saldırı yüzeyi oluşturur. **DNS Amplification** gibi saldırılarda, saldırgan küçük bir UDP isteği göndererek çok daha büyük yanıtların kurbana yönlendirilmesini sağlar. UDP'de bağlantı doğrulaması olmadığı için kaynak adresi kolayca taklit edilebilir (IP spoofing). Bu durum,

UDP tabanlı servisleri yüksek hacimli yansıtma (amplification) saldırıları için cazip hale getirir.

Port taramaları açısından bakıldığında da bu fark net biçimde görülür. **TCP port taramaları** (özellikle SYN Scan), hedef sistemin bağlantı kurma tepkilerine göre açık, kapalı veya filtreli portları tespit etmeye odaklanır. Bu yöntem daha kontrollü ve bilgilendirici olsa da, loglanma ihtimali yüksektir. **UDP port taramaları** ise genellikle daha belirsizdir; çoğu UDP servisi yanıt vermediği için sonuçlar net değildir. Ancak bu sessizlik, UDP taramalarını tespit etmeyi de zorlaştırır.

Sonuç olarak, TCP'nin güvenilirlik ve durum takibi içeren yapısı daha **hedefli ve durum bazlı saldırıları** mümkün kılarken, UDP'nin hız ve doğrulama eksikliği **hacim tabanlı ve yansıtma saldırılarını** öne çıkarır. Bu iki yaklaşım, hem saldırganların yöntemlerini hem de savunma stratejilerinin tasarımını doğrudan etkilemektedir.

UDP vs TCP Comparison

UDP User Datagram Protocol

🚀 SPEED FOCUSED
- Connectionless protocol
- No handshake required
- Fire and forget approach

📦 LIGHTWEIGHT
- 8-byte header only
- Minimal overhead
- Fast transmission

⚡ LOW LATENCY
- 20-50ms typical latency
- Real-time applications
- No acknowledgments

❌ NO GUARANTEES
- 1-10% packet loss
- No error correction
- No delivery confirmation

🎮 BEST FOR:
- Online gaming
- Live streaming, video calls
- DNS queries

VS

TCP Transmission Control Protocol

🛡️ RELIABILITY FOCUSED
- Connection-oriented
- Three-way handshake
- Established connection

📋 COMPREHENSIVE
- 20-60 byte header
- Control information
- Sequence numbers

🐌 HIGHER LATENCY
- 100-200ms typical latency
- Acknowledgment delays
- Error checking overhead

✅ GUARANTEED DELIVERY
- 99.9% success rate
- Error correction
- Packet retransmission

🌐 BEST FOR:
- Web browsing
- File download, email transfer
- Financial transactions

KEY TAKEAWAY

Choose UDP when SPEED matters most (gaming, streaming)
Choose TCP when RELIABILITY is critical (web, email, files)