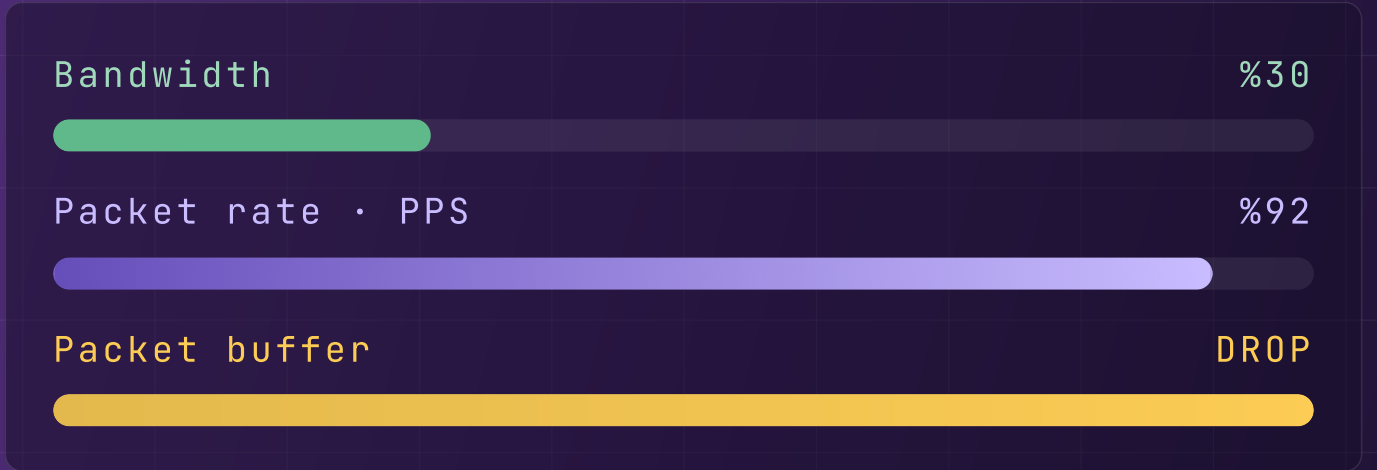


Görünen kapasite

Bandwidth %30. Firewall'da  
neden packet drop oluyor?



Bu haftanın kontrolü

# Firewall Capacity

Don't Deploy on Friday. Verify on Friday.

Tek kapasite yok

Firewall kapasitesi yalnızca Mbps veya Gbps değildir.

Aynı anda farklı sınırlar çalışır:

Packet rate

PPS



Connection rate

CPS



Concurrent sessions



TLS / IPS inspection



Packet buffer



Birinin dolması, trafik için yeterlidir.

Aynı trafik, farklı yük

Az sayıda büyük packet ile çok sayıda küçük packet aynı bandwidth'i üretebilir.

AZ · BÜYÜK PACKET



1 Gbps · 3 packet

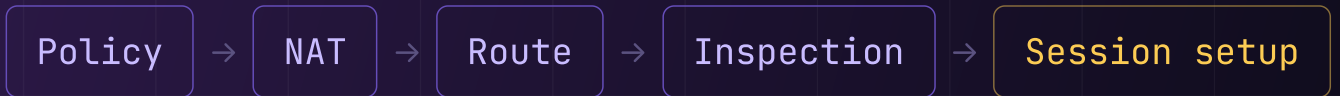
ÇOK · KÜÇÜK PACKET



1 Gbps · 24 packet

Fakat küçük packet'larda firewall'ın saniyede işlemesi gereken packet sayısı yükselir.

Yeni connection'lar ayrıca:



adımlarından geçer.

Yanlış refleks

“Bandwidth boşsa firewall rahat çalışıyordur.”

Bu varsayım packet-rate veya session-rate darboğazını gizler.

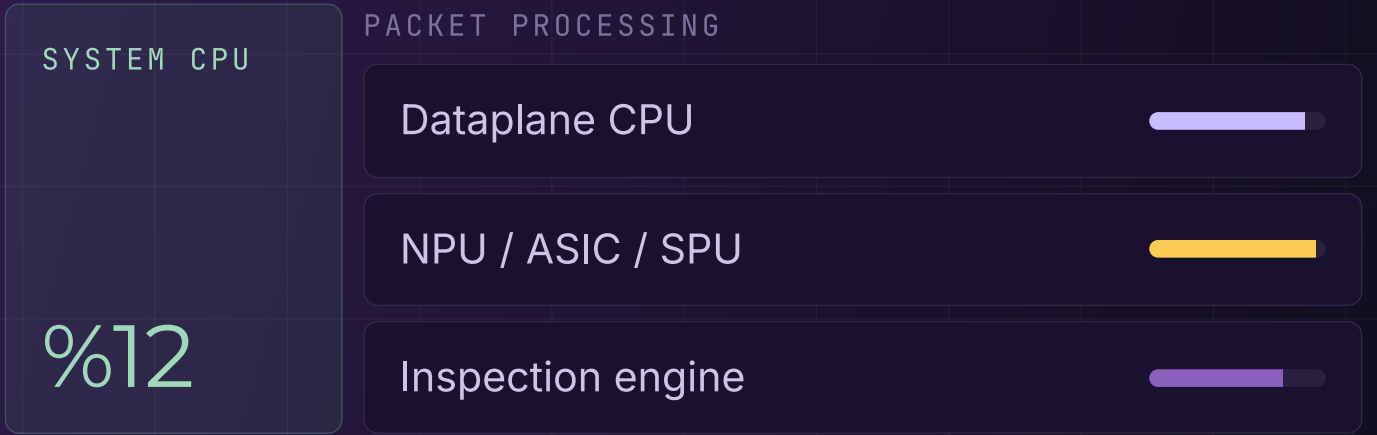
Drop görülünce limitleri kontrolsüz artırmak da packet buffer ve session table üzerindeki baskıyı büyütebilir.

---

Önce hangi kapasitenin dolduğunu bulun.

CPU tek değildir

Firewall'ın system veya management CPU'su ile trafiği işleyen kaynaklar aynı olmayabilir.



Packet processing bu katmanlara dağılabilir.

Genel CPU'nun düşük görünmesi, packet-processing yolunun **rahat olduğu anlamına gelmez.**

Bazı platformlarda özel işlemciler için utilization yerine offload, buffer ve drop metrikleri izlenir.

## Friday check

Aynı zaman aralığında üç kontrol yapın:

### 1 Traffic shape

Bandwidth ile PPS peak'lerini karşılaştırın.

### 2 Session pressure

CPS, active session ve session-table kullanımına bakın.

### 3 Processing path

System/dataplane CPU, offload, inspection, packet buffer ve drop reason'ları birlikte inceleyin.



5 dakikalık ortalama yerine **kısa peak'leri** görün.

Sinyalleri birlikte okuyun

Bandwidth düşük + PPS yüksek + buffer drop

→ Packet-rate baskısını araştırın.

Bandwidth düşük + CPS yüksek + session setup drop

→ Connection churn, scan veya retry trafiğini araştırın.

System CPU düşük + dataplane/buffer baskısı yüksek

→ Yanlış işlem katmanına bakıyorsunuz.

Kaynaklar normal + belirli policy'de drop

→ Kapasite yerine rule veya threshold davranışını inceleyin.

Bulguyu aksiyona çevirin

Soruna göre:

- 01 Yoğun source ve destination'ı bulun
- 02 Gereksiz connection churn'ü azaltın
- 03 DoS/rate limit'i baseline'a göre ayarlayın
- 04 Offload dışı ve inspection gören trafiği ayırın
- 05 Kapasiteyi Gbps ile değil, darboğaz metriğiyle boyutlandırın

↓ Sonrasında drop rate ve connection setup p99 düşmeli.

Reliability ilkesi

Bandwidth, trafik hacmini gösterir.

Firewall yükünü ise her  
packet ve session için **yapılan  
gerçek iş** belirler.

Firewall kapasitesini hâlâ yalnızca Gbps ve  
genel CPU ile mi izliyorsunuz?

**Don't Deploy on Friday. Verify on Friday.**

Every Friday. One Production Check.