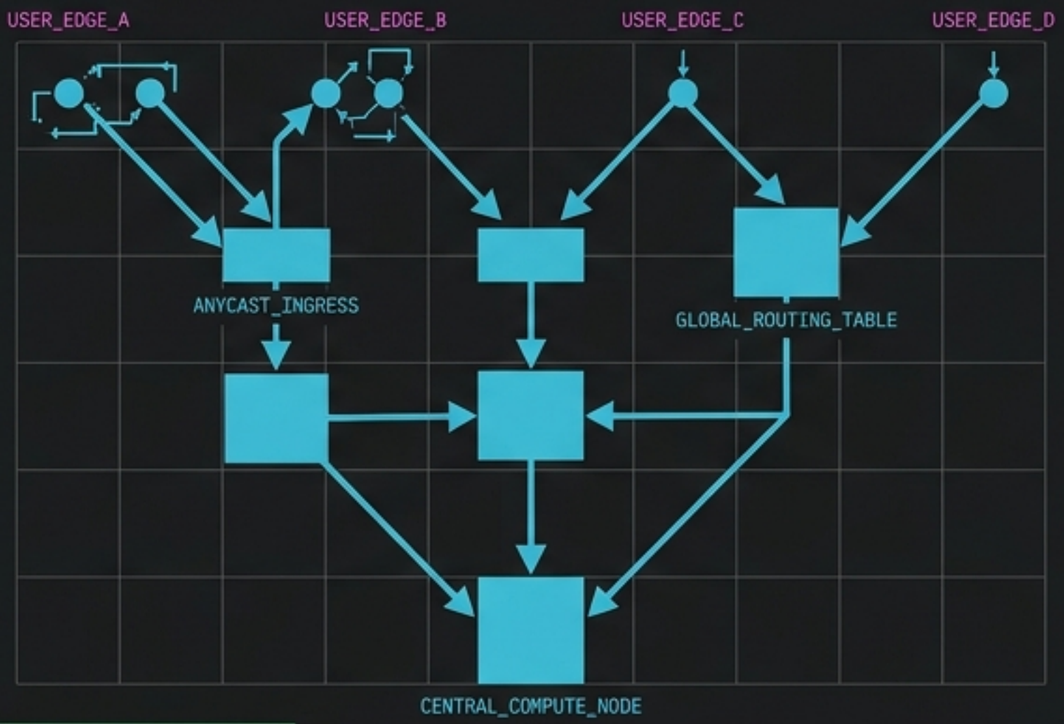
# Web Architecture — S02E03

## WAF Internals, L3/L4/L7 DDoS Mitigation, Bot Fingerprinting & Edge Rate Limiting




Target Audience: Platform, Backend & Security Engineering

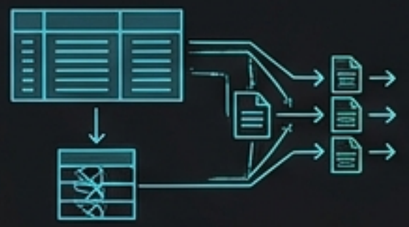
mode: strict_technical_deep_dive

Gemini Notebook

# THE EDGE DEFENSE EXECUTION PIPELINE

## NETWORK EDGE (L3/L4)

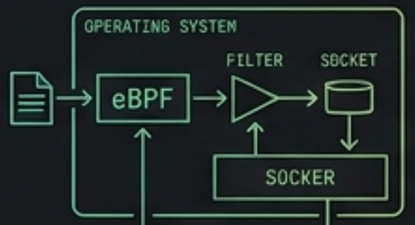
BGP FLOWSPEC & ANYCAST ROUTING (STATELESS)

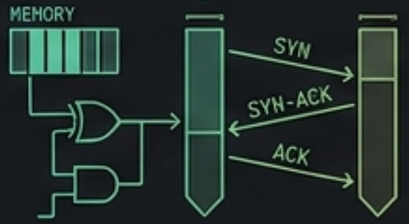




## OS KERNEL (L4)

EBPF / XDP & TCP STACK (PRE-SOCKET)

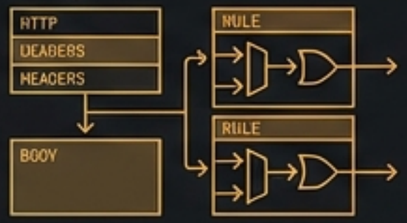



## USER SPACE PROXY (L7)

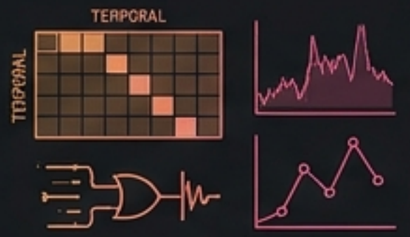
TLS TERMINATION, HTTP PARSING & WAF RULES (STATEFUL)




## BEHAVIORAL ENGINE (L7)

BOT FINGERPRINTING & RATE LIMITING (TEMPORAL)

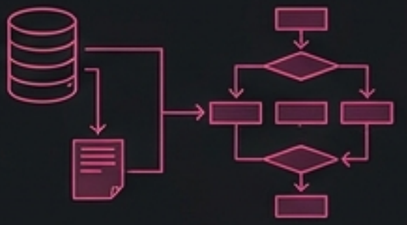






## ORIGIN SERVER

AUTHENTICATED LOGIC





Defense-in-depth is an execution pipeline. You cannot inspect an HTTP payload until TLS is terminated; you cannot terminate TLS if your TCP sockets are exhausted by a SYN flood. Survival requires sequential filtering.

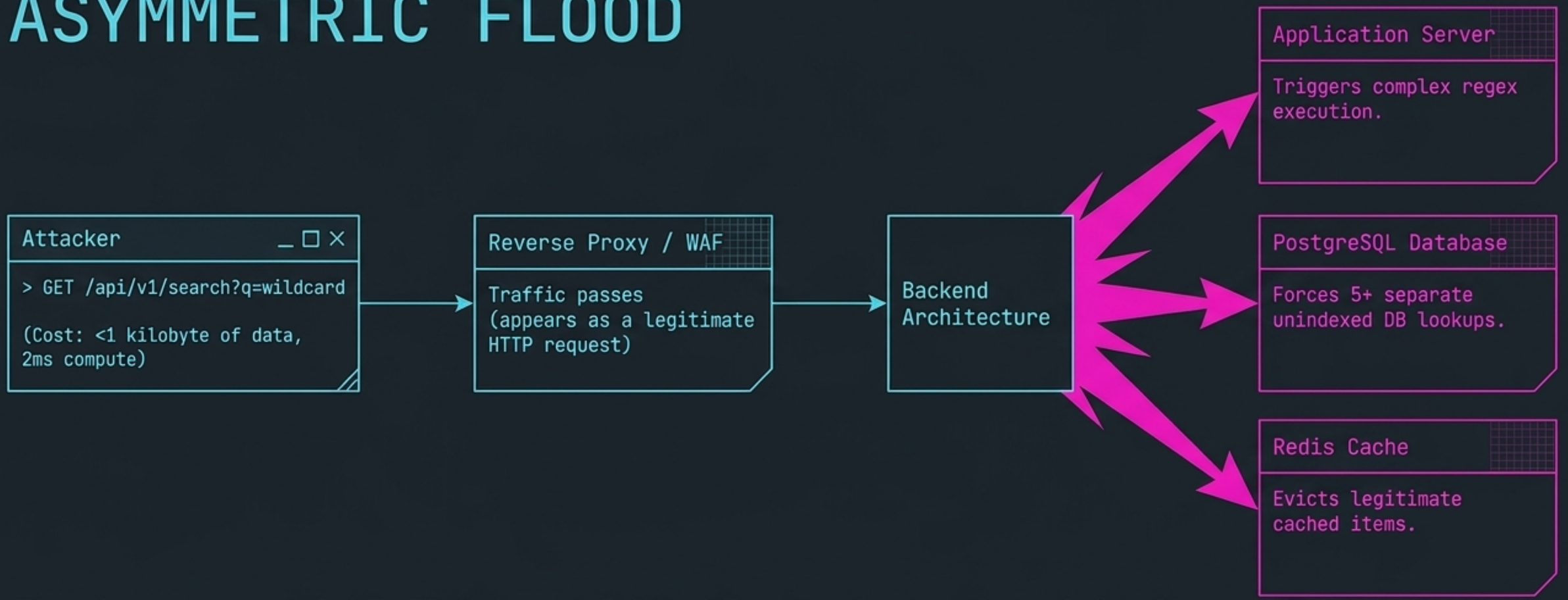
Gemini Notebook

# THE ASYMMETRY OF DENIAL OF SERVICE

| | L3/L4 (Volumetric / State) | L7 (Application Logic) |
|---|---|---|
| Vector | ICMP ping floods, UDP reflection (DNS/NTP), TCP SYN floods. | HTTP GET/POST floods targeting APIs and dynamic pages. |
| Bottleneck | Exhausts network bandwidth and kernel socket memory. | Exhausts server CPU, database connections, and memory. |
| Attacker Cost | Requires high bandwidth (Gbps/Tbps) and large spoofed botnets. | Requires low bandwidth, operating asymmetrically (a few RPS can crash a DB). |
| Mitigation Locus | Network Edge (hardware/routers). | Reverse-Proxy/WAF (software/logic). |

Gemini Notebook

# ANATOMY OF AN L7 ASYMMETRIC FLOOD

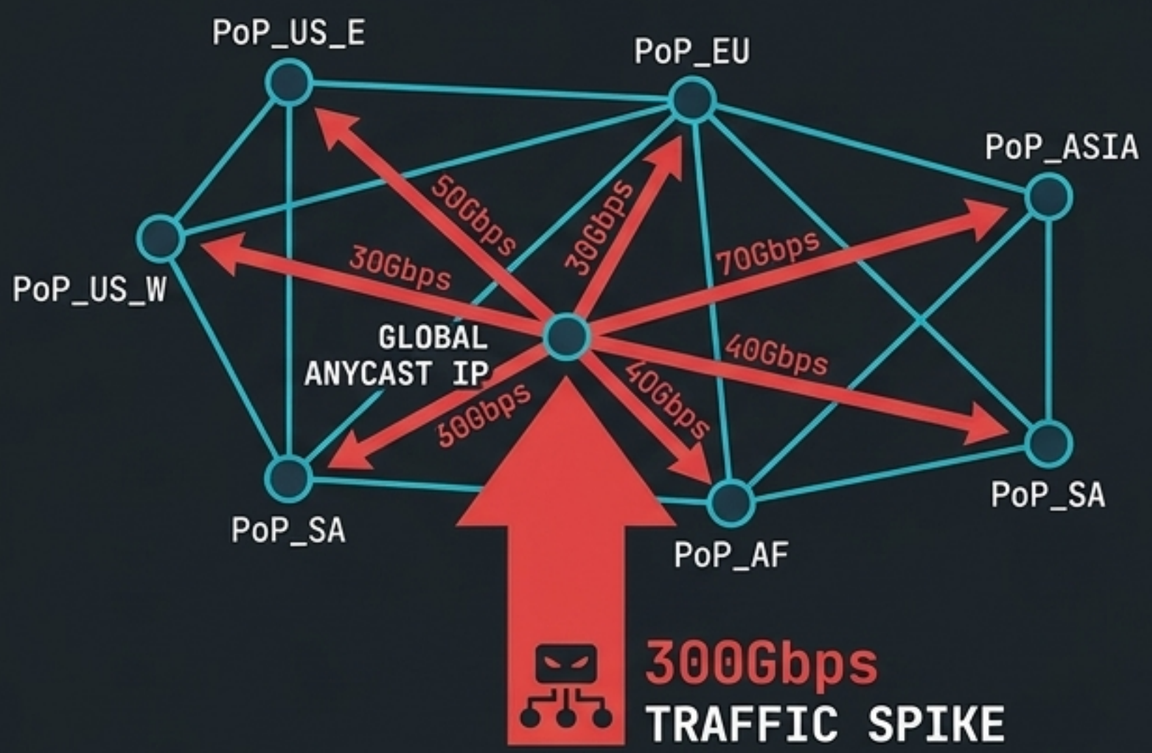



The Asymmetry of L7 Floods: Unlike L3 attacks measured in Gbps, L7 attacks require only low-bandwidth Requests Per Second (RPS) to exhaust expensive backend database queries and compute cycles.

Gemini Notebook

# ABSORBING VOLUMETRIC FLOODS: BGP & ANYCAST

## ANYCAST DIFFUSION




Anycast routing announces the same IP globally, naturally scattering localized botnet attacks geographically to prevent single data center collapse.

## BGP FLOWSPEC (BLACKHOLE ROUTING)

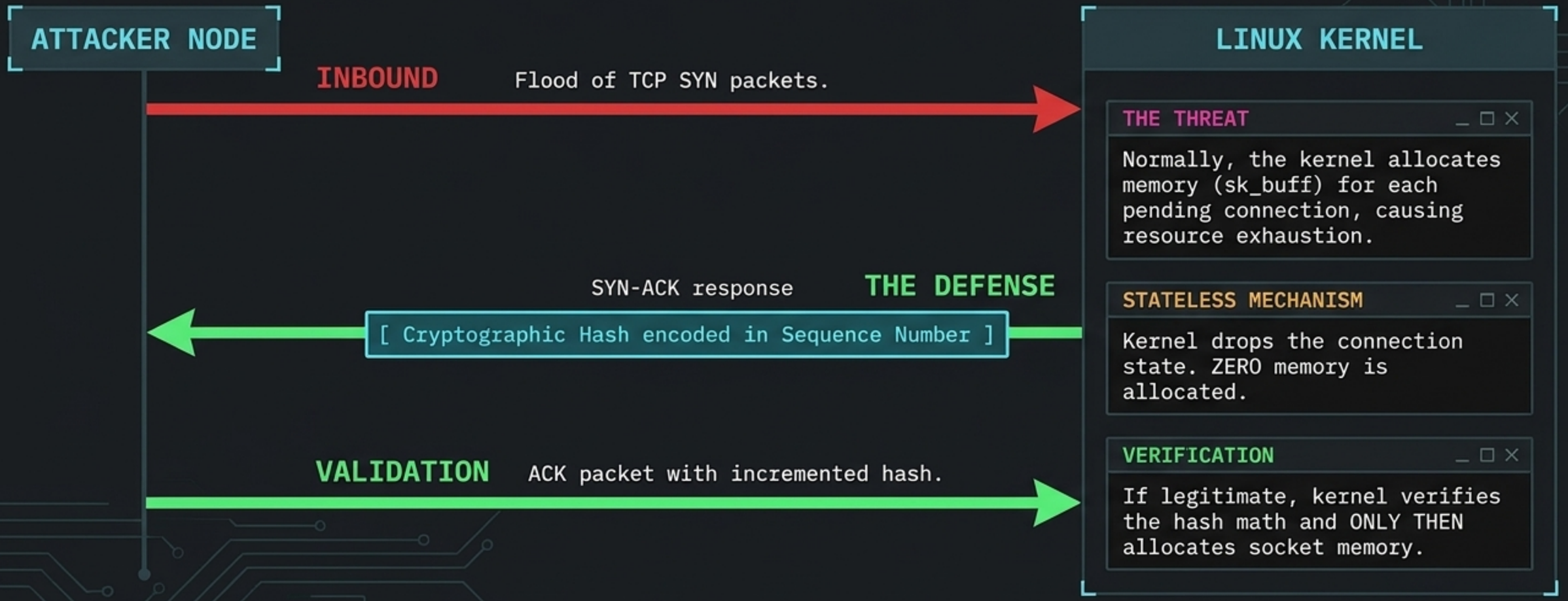
BGP_Flowspec_Rules.conf

```
> match
    destination-port 123
    protocol udp
  then
    discard
```

Massive amplification attacks (e.g., NTP UDP floods) are dropped at the edge routers via BGP routing rules before touching application servers.

Gemini Notebook

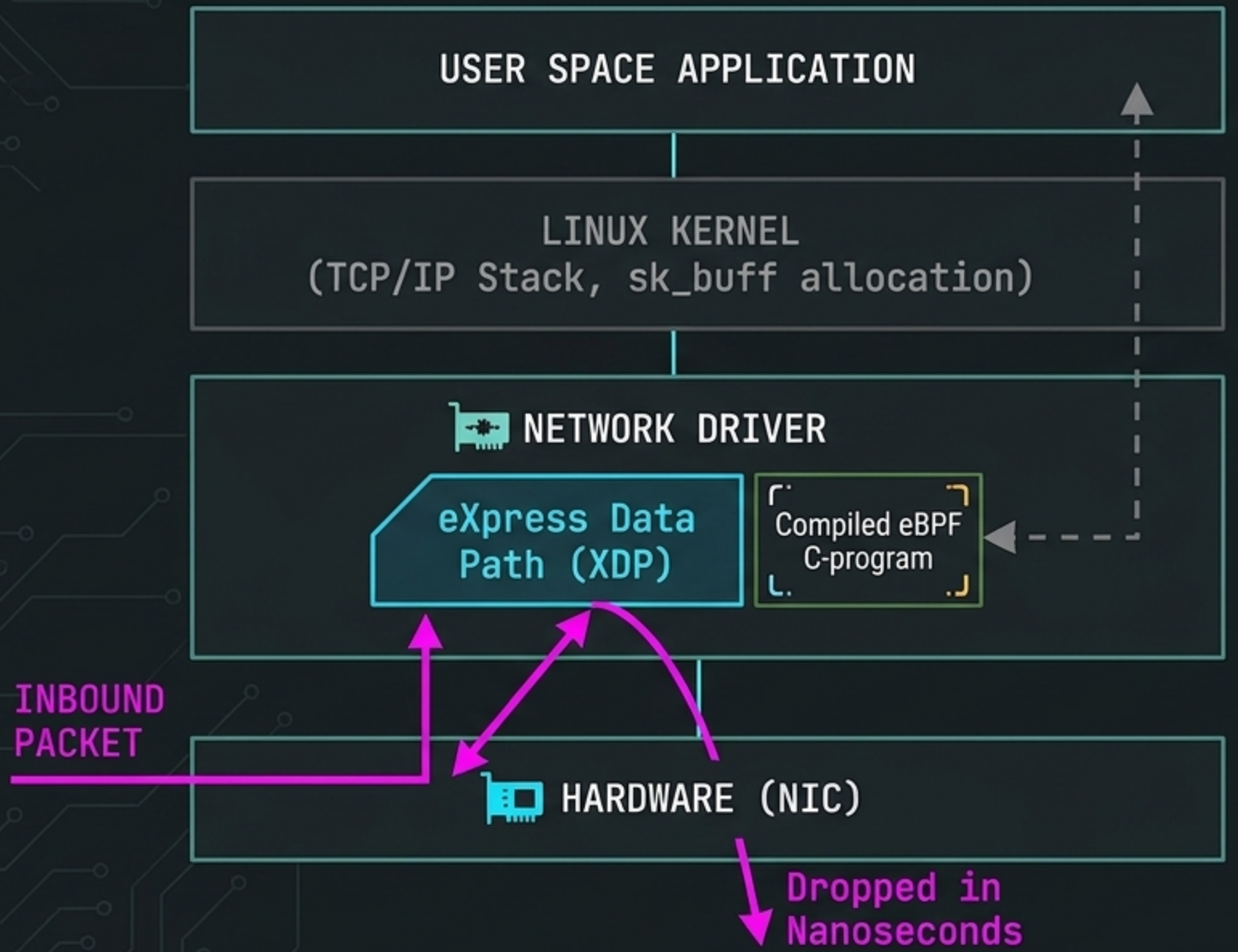
# STATELESS SOCKET DEFENSE: TCP SYN COOKIES




Stateless socket defense proves client legitimacy mathematically before committing server RAM.

Gemini Notebook

# KERNEL-BYPASS PACKET DROPPING (eBPF/XDP)




Traditional slow OS networking path completely bypassed.

**KEY INSIGHT:**

eBPF/XDP allows executing custom, compiled packet-filtering logic with minimal CPU overhead, destroying L3/L4 junk traffic directy directly in the network driver before the OS even knows it exists.

Gemini Notebook

# THE LAYER-7 WAF EXECUTION ARCHITECTURE

USER SPACE PROXY

## TLS TERMINATION

Decrypts HTTPS traffic. WAFs cannot inspect encrypted L4 streams.

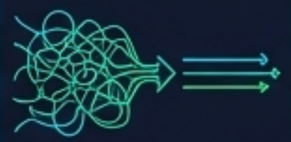
## HTTP REQUEST PARSING

Breaks plaintext into Headezs, Cookiss, URI, and Body.




## ANTI-EVASION NORMALIZATION

Standardizes the obfuscated payload.



## RULE ENGINE EVALUATION

Matches parameters against security policies.



## ACTION ROUTING

Branches out to Count, Challenge, or Block.

### COUNT
Log and Allow

### CHALLENGE
CAPTCHA / JS Challenge

### BLOCK
Drop Connection / 403 Forbidden

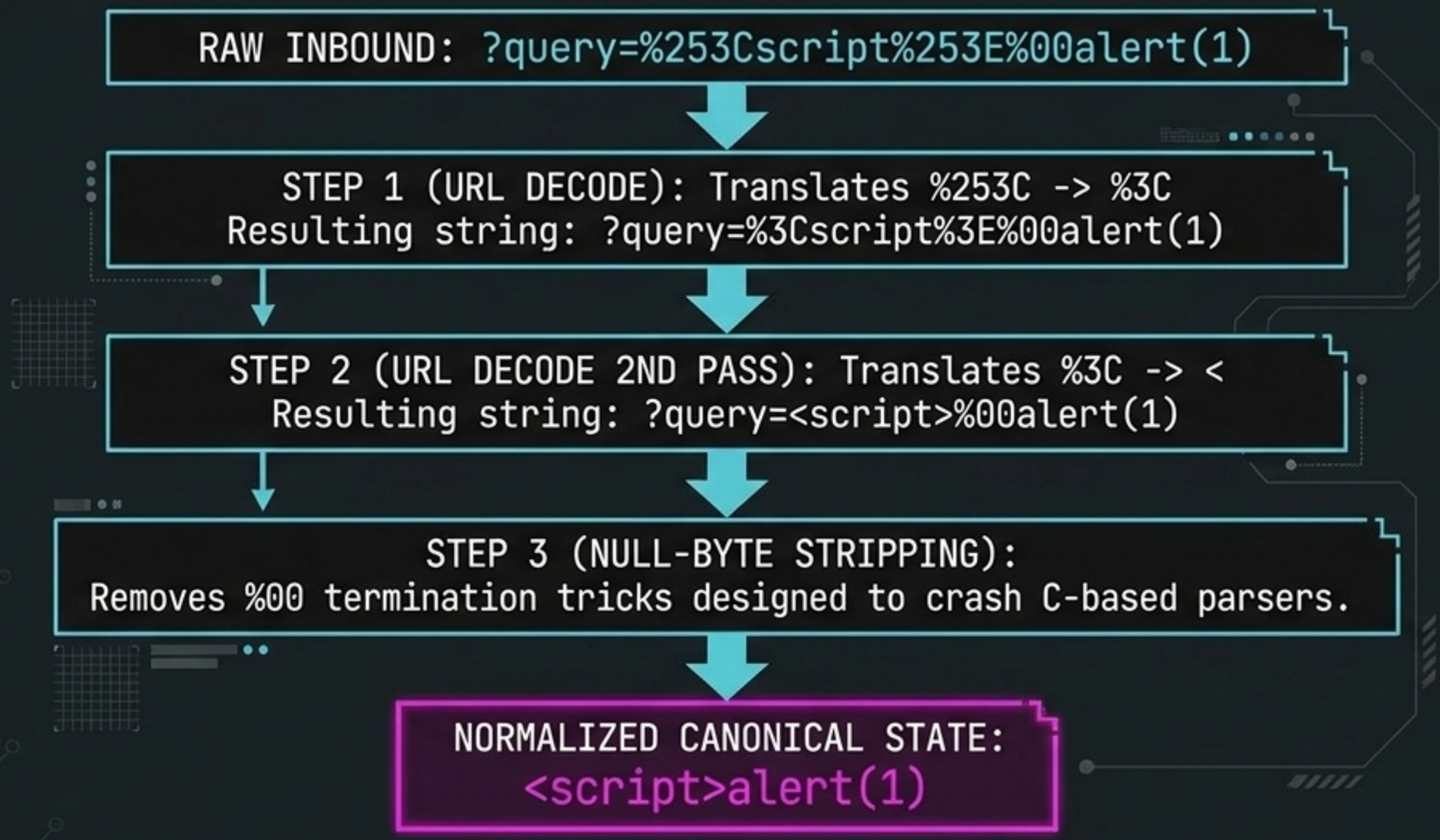
## TERMINAL OUTPUT

A Web Application Firewall (WAF) operates as a reverse-proxy. It terminates the client connection, inspects the payload, and establishes a secondary, clean connection to the origin server.

>_

Gemini Notebook

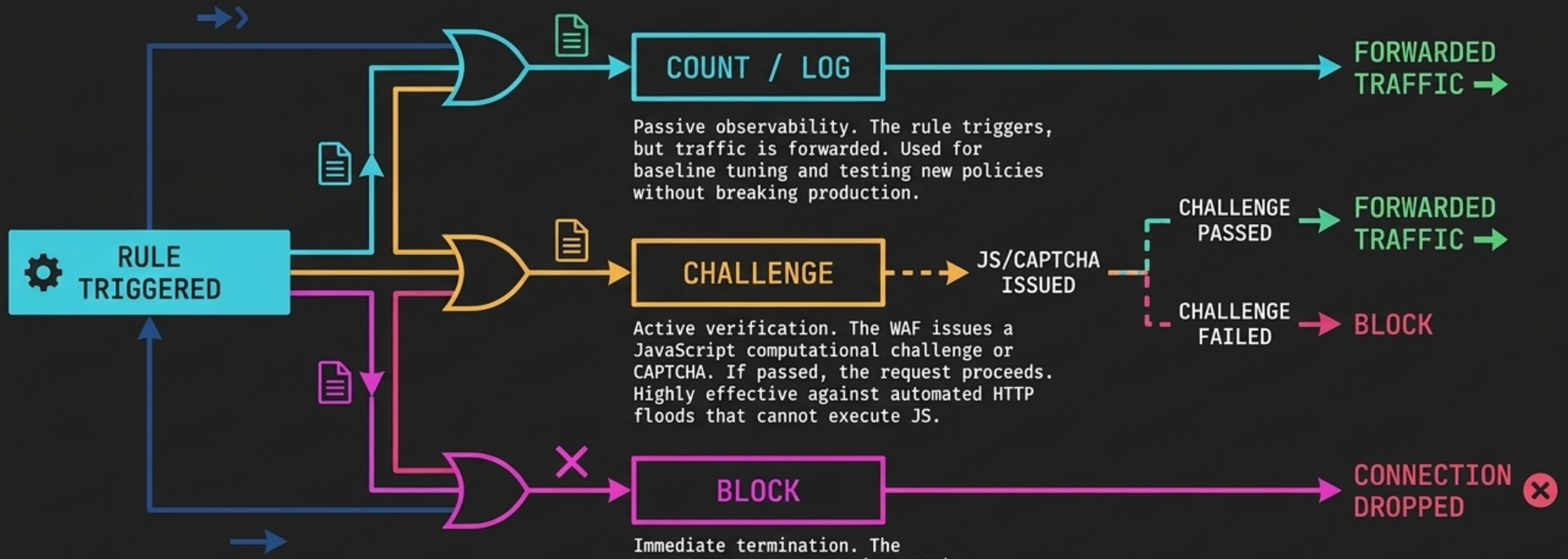
# ANTI-EVASION & NORMALIZATION




CONCLUSION: Normalization is mandatory. Without recursive decoding and canonicalization, signature-based WAF engines are easily bypassed by trivial character encoding mutations.

Gemini Notebook

# RULE ENGINE ACTIONS & STATE

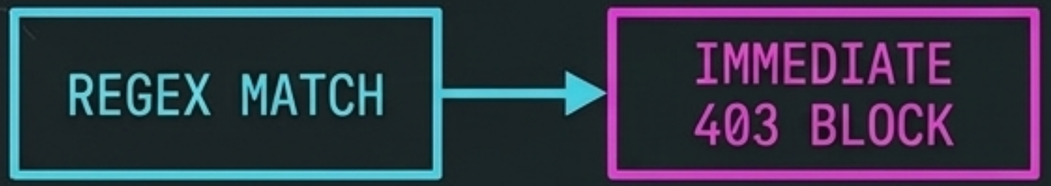



WAFs are not binary. Modern edge defense relies on dynamic challenges to filter out basic scripts while preserving the user experience for actual humans.

Gemini Notebook

# SINGLE-RULE BLOCKLISTS VS. ANOMALY SCORING

## SINGLE-RULE BLOCKLIST (LEGACY)




Concept: Negative security model (bouncing known bad traffic).

Flaw: Highly brittle. A single false positive immediately breaks the application for a legitimate user.

## CUMULATIVE ANOMALY SCORING (MODERN CRS)

- Missing Accept Header (+2)
- Generic SQLi keyword matched (+5)
- User-Agent looks synthetic (+2)

---

Total Anomaly Score: 9

Threshold logic:
If Score > 10, then Block.

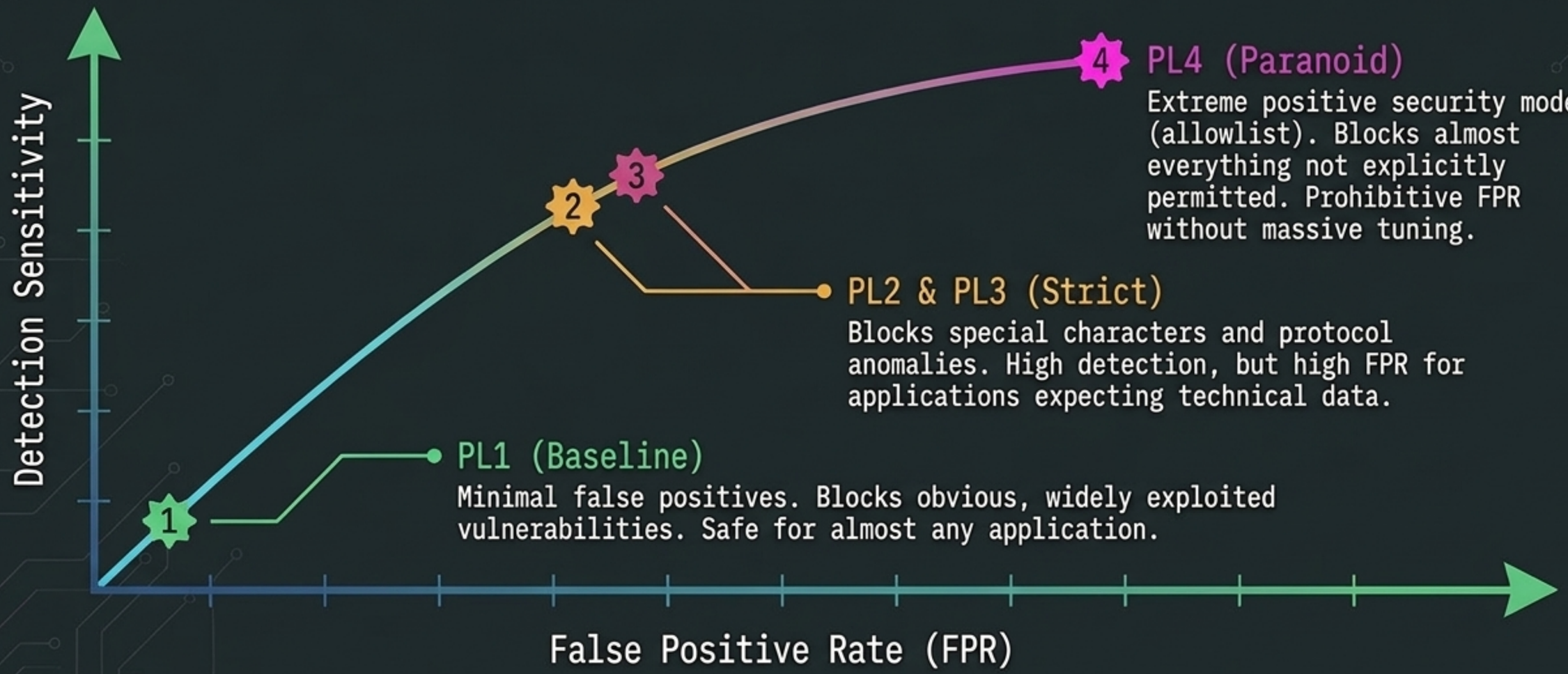
(Score is 9, request passes)

OWASP CRS drastically reduces False Positives by requiring a confluence of suspicious indicators before terminating a session.

Gemini Notebook

# OWASP Paranoia Levels (PL1–PL4)

The fundamental security engineering tradeoff:
Balancing threat sensitivity against operational usability.




**PL4 (Paranoid)**
Extreme positive security model (allowlist). Blocks almost everything not explicitly permitted. Prohibitive FPR without massive tuning.

**PL2 & PL3 (Strict)**
Blocks special characters and protocol anomalies. High detection, but high FPR for applications expecting technical data.

**PL1 (Baseline)**
Minimal false positives. Blocks obvious, widely exploited vulnerabilities. Safe for almost any application.

Gemini Notebook

# THE API & TECHNICAL PAYLOAD CHALLENGE

## DEVELOPER API SUBMISSION

```
{
  "comment": "Update the config map: `<script>init();</script>`",
  "command": "SELECT * FROM users WHERE status = 'active';"
}
```

A completely legitimate API request containing nested Markdown and raw code snippets.

## WAF RULE EVALUATION

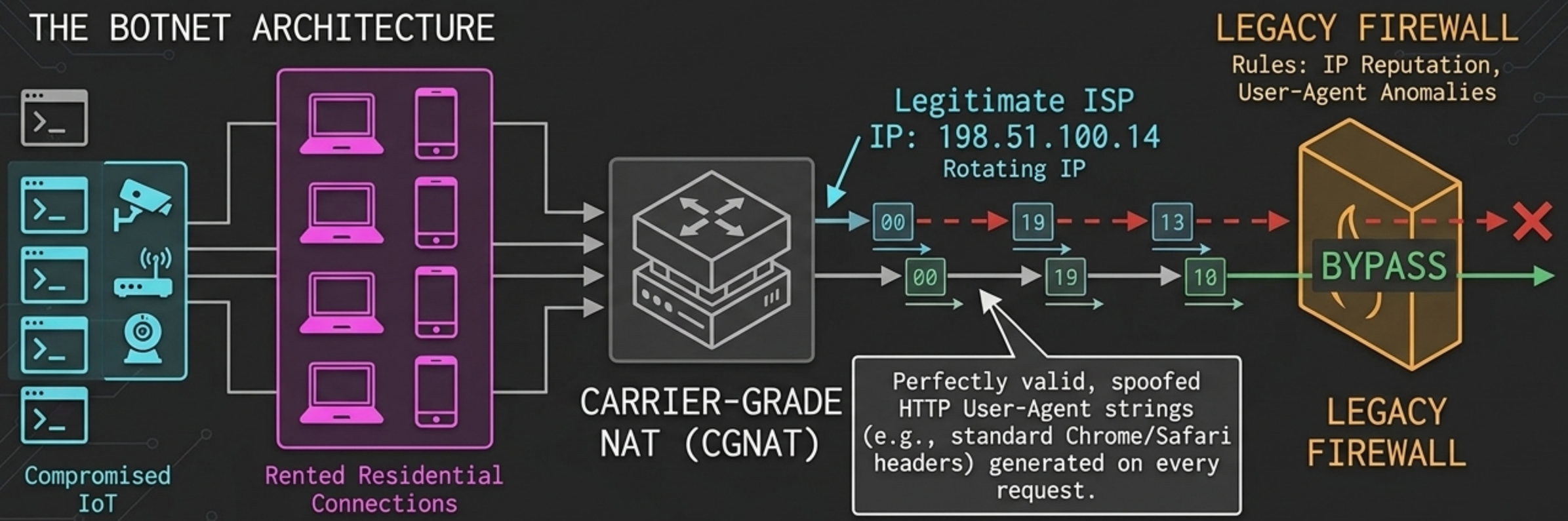
```
[CRITICAL] False Positive Triggered!
- XSS rule matched on '<script>'
- SQLi rule matched on 'SELECT * FROM'

Result: Traffic Blocked.
```

The Solution: Modern architectures heavily utilizing JSON, GraphQL, and Markdown must systematically deploy targeted rule exclusions (tuning) on specific URIs to prevent blocking legitimate application logic.

Gemini Notebook

# THE FAILURE OF IP AND USER-AGENT

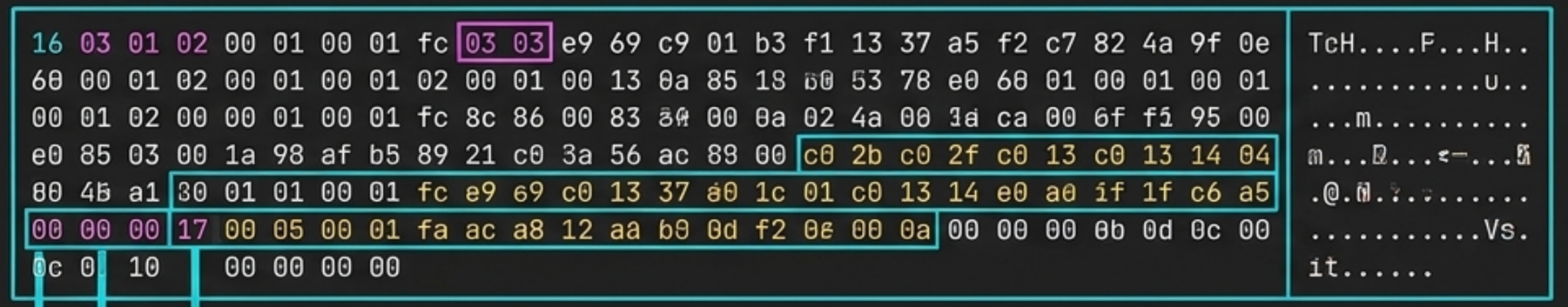



Traditional signals are dead. You cannot block based on IP reputation or User-Agent anomalies because the proxy traffic mathematically mirrors legitimate human populations. Defense requires cryptographically fingerprinting the underlying client software.

Gemini Notebook

# TLS FINGERPRINTING (JA3 / JA4)

TLS ClientHello Packet




03 03 → TLS 1.2 → TLS Version

c0 2b c0 2f c0 2c c0 30 cc a9 cc a8 c0 13 c0 14... → Accepted Cipher Suites

00 00 00 17 00 15 00 0d 00 12 00 10 00 0b 00 0a... → TLS Extensions

00 00 00 00 00 00 00 00 00 00 0d 00 10 00 00 00 3b... → MD5 / SHA256 Hash Function → JA3/JA4 Fingerprint: 771,4865-4866-4867,0-23-65281...

Explanation:

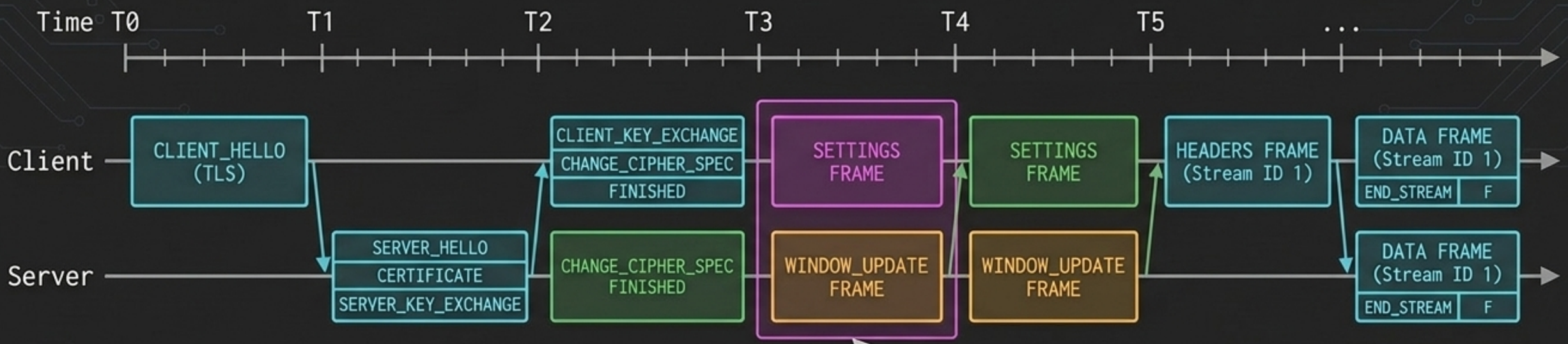
- Different networking libraries (Python requests, Golang, Chrome) construct ClientHello packets differently.

- JA3/JA4 hashes these static structural choices to fingerprint the underlying client engine.

The Result: If the HTTP header says ‘Mozilla/5.0 (Windows)’ but the JA4 TLS hash strictly matches the Python urllib library, we have definitively identified a spoofing bot.

Gemini Notebook

# HTTP/2 FRAME FINGERPRINTING




HTTP/2 establishes connection parameters unique to the specific client implementation (e.g., Headless Chrome vs standard browser).

$$\text{Client_Identity} = \text{Hash}\ (\ \text{JA4_TLS_Signature} + \text{HTTP2_Settings_Signature}\ )$$

By measuring the immutable, low-level binary configuration of the connection stack, the edge defense establishes a highly deterministic fngerprint for headless browsers and scripts, completely ignoring easily forged application-layer headers.

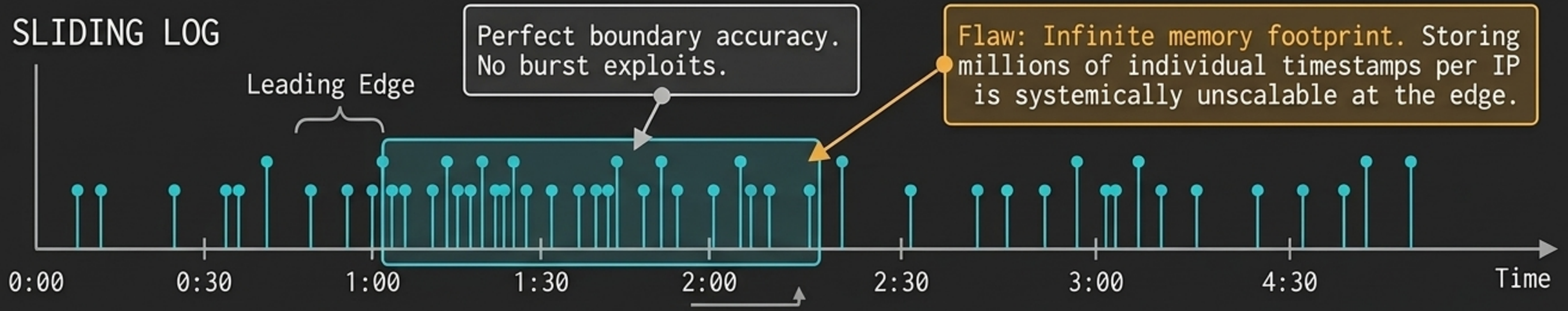
Gemini Notebook

# FIXED WINDOW VS. SLIDING LOG ALGORITHMS

## FIXED WINDOW




## SLIDING LOG



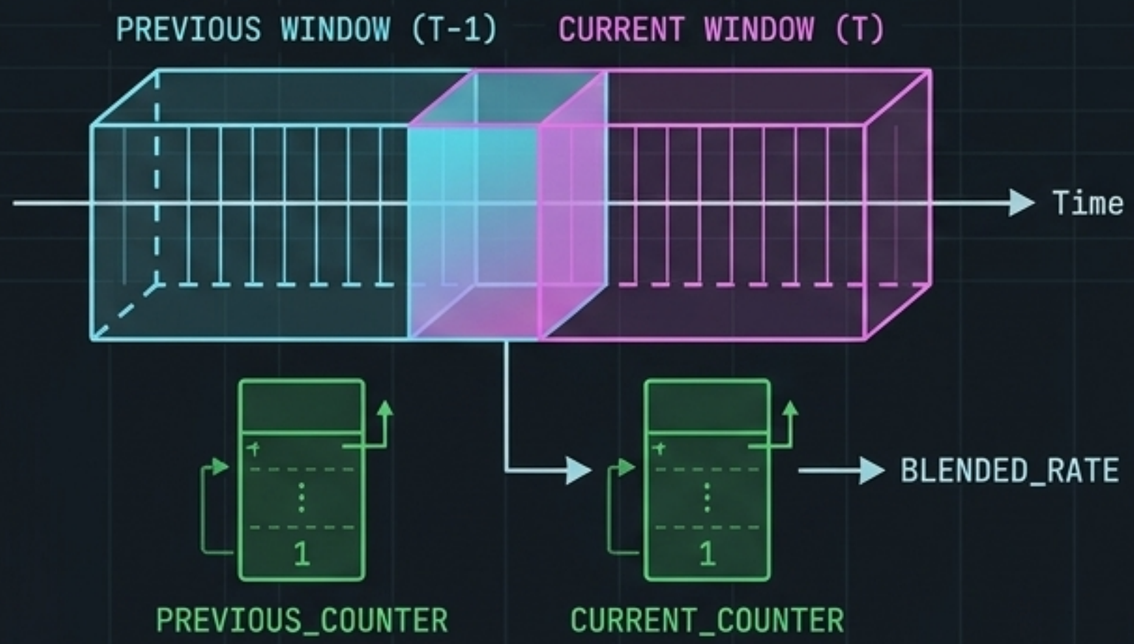

The classic rate limiting tradeoff: Memory efficiency vs. Boundary accuracy.

Gemini Notebook

# PRODUCTION-GRADE ALGORITHMS: SLIDING WINDOW COUNTER & TOKEN BUCKET

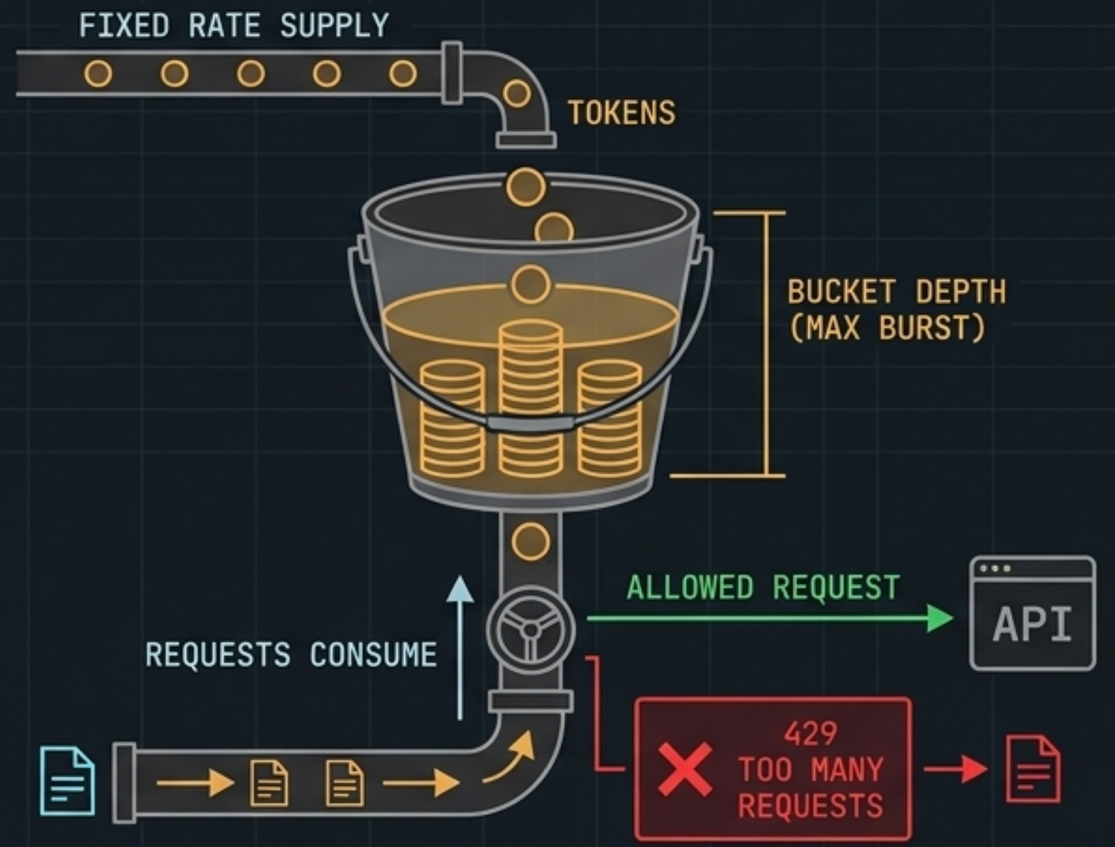
## SLIDING WINDOW COUNTER

REQUESTS = (PREVIOUS_COUNT * OVERLAP_PERCENTAGE) + CURRENT_COUNT




VERDICT: Highly memory efficient (requires only two counters per key) while seamlessly smoothing out traffic bursts. Excellent for general DDoS protection.

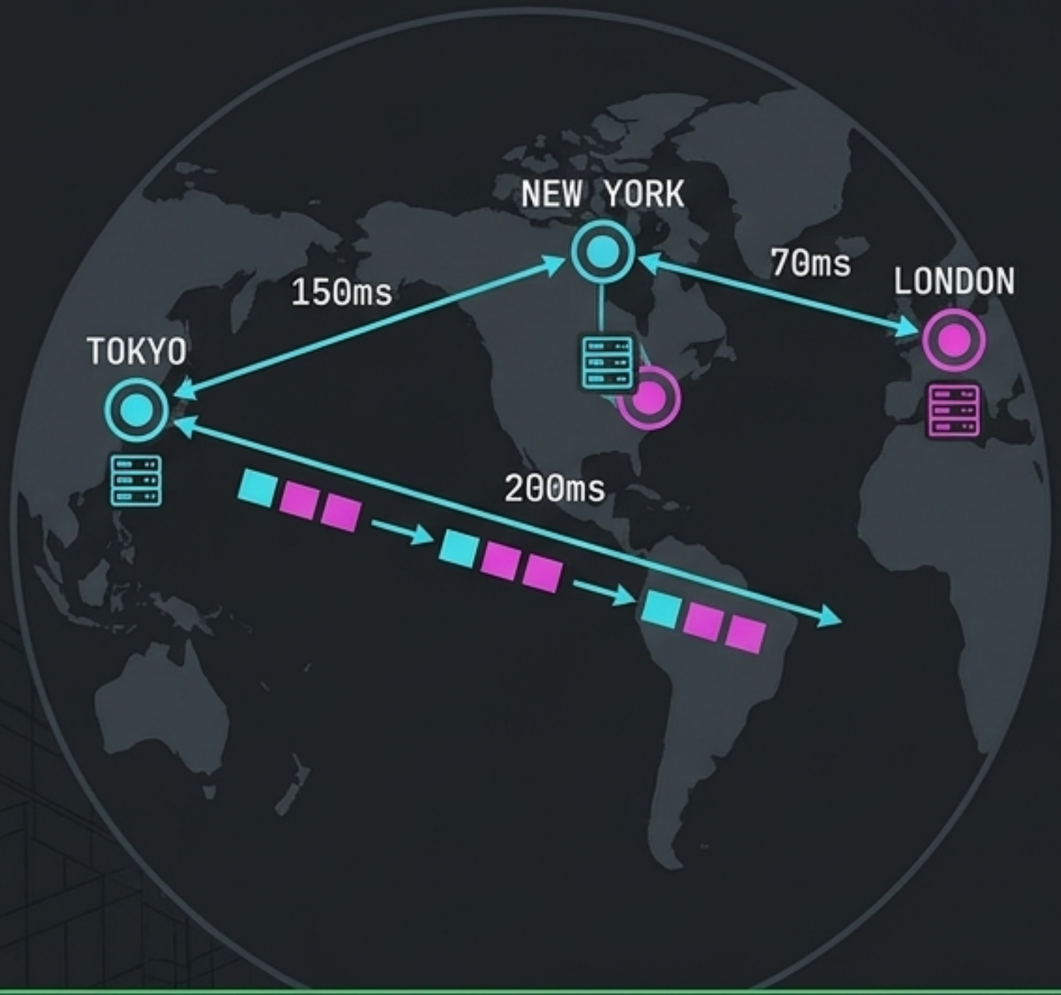
## TOKEN BUCKET

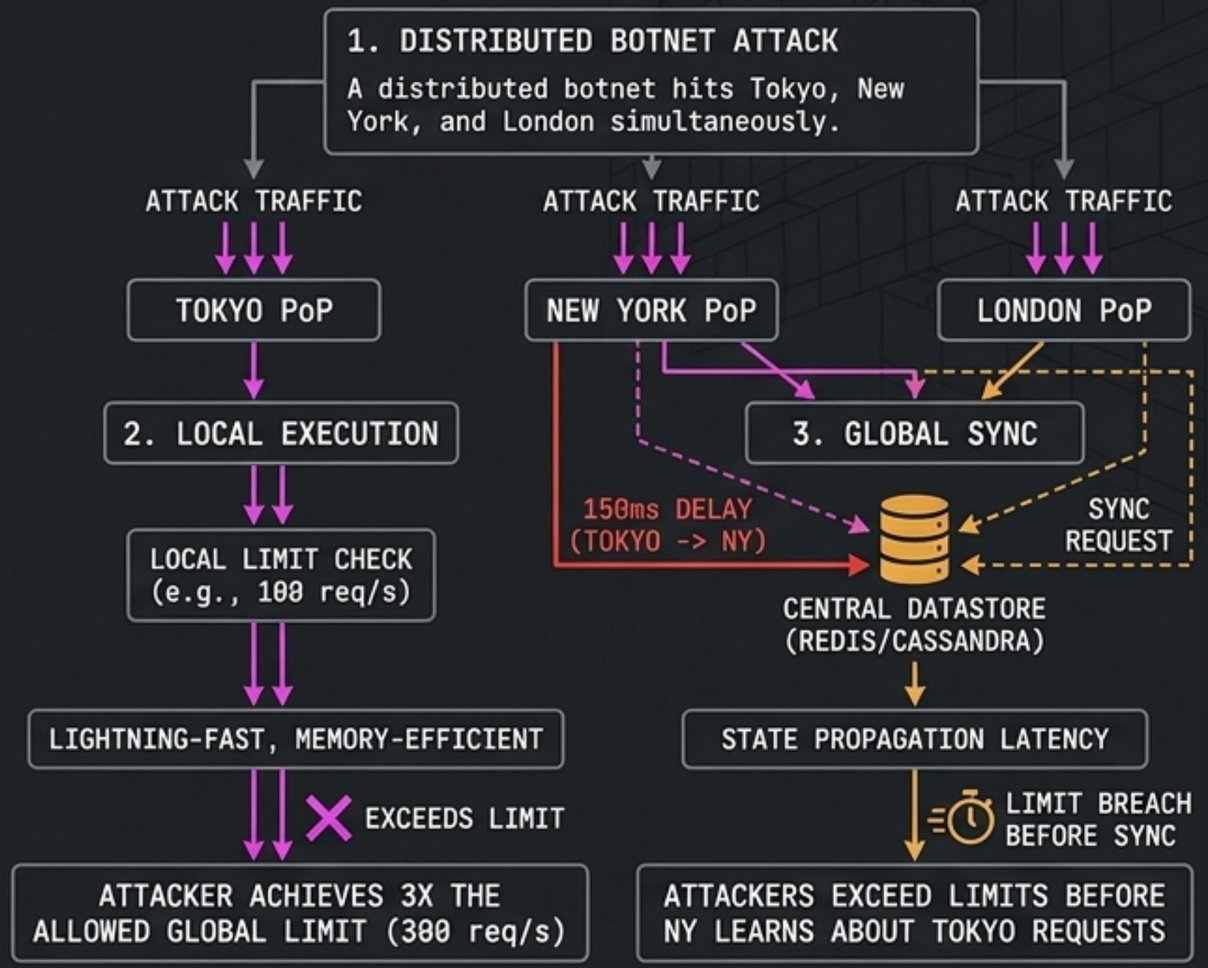



VERDICT: Allows governed, immediate bursts of traffic (up to the bucket's depth) while enforcing a strict long-term average rate. Ideal for API burst tolerance.

Gemini Notebook

# THE GLOBAL STATE SYNC PROBLEM




THE EDGE TRADEOFF: Choose between eventual consistency (leaky global limits) or strict, localized edge limits based on the application's tolerance for abuse.

Gemini Notebook

# COMPOSITE KEYS & CGNAT COLLATERAL DAMAGE

## THE ANTI-PATTERN

```
rate_limit_key = hash(client_ip)
```

Danger: Due to Carrier-Grade NAT (CGNAT) and corporate VPNs, a single IP address might represent 5,000 legitimate users. Blocking the IP blocks the entire organization.

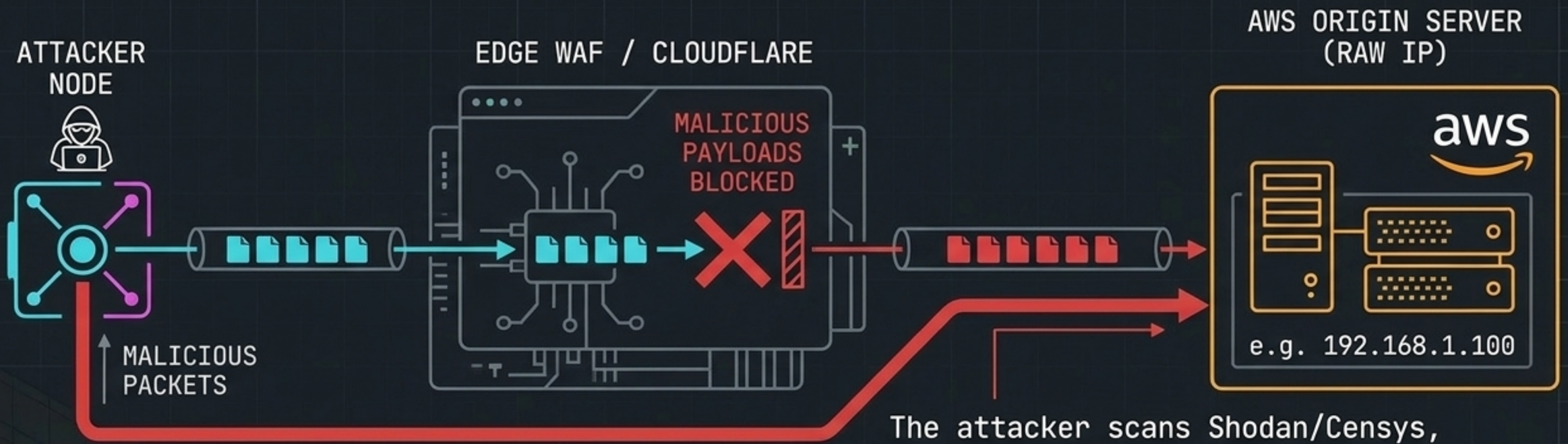
## THE SOLUTION - COMPOSITE KEYS

```
rate_limit_key = hash(client_ip
                 + http_session_cookie
                 + api_key)
```

Safe rate limiting requires extracting Layer 7 state and blending it with network state. This isolates abusive sessions without causing collateral damage to innocent neighbors sharing the NAT.

Gemini Notebook

# DIRECT-TO-ORIGIN IP BYPASSES

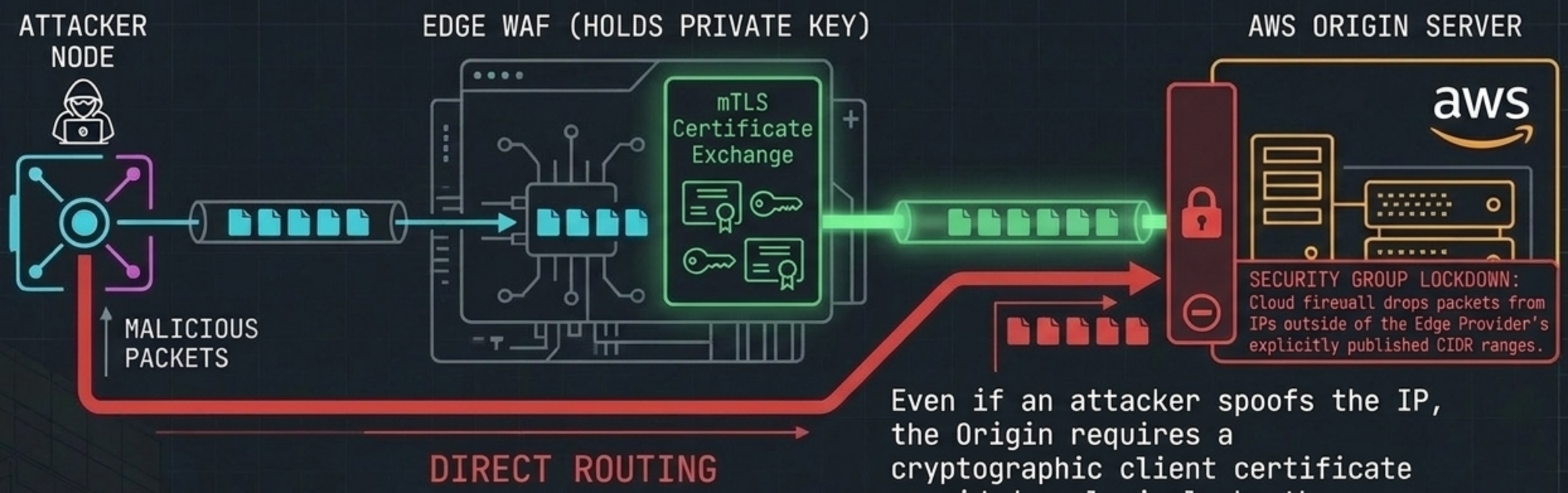



The attacker scans Shodan/Censys, discovers the raw, underlying IP address of the Origin Server, and routers, and routes HTTP traffic directly to it.

**CORE PRINCIPLE:** A WAF is a reverse-proxy. If the origin server accepts HTTP traffic directly from the open internet, the edge defense is functionally irrelevant.

Gemini Notebook

# HARDENING THE ORIGIN (mTLS & AUTHENTICATED PULLS)

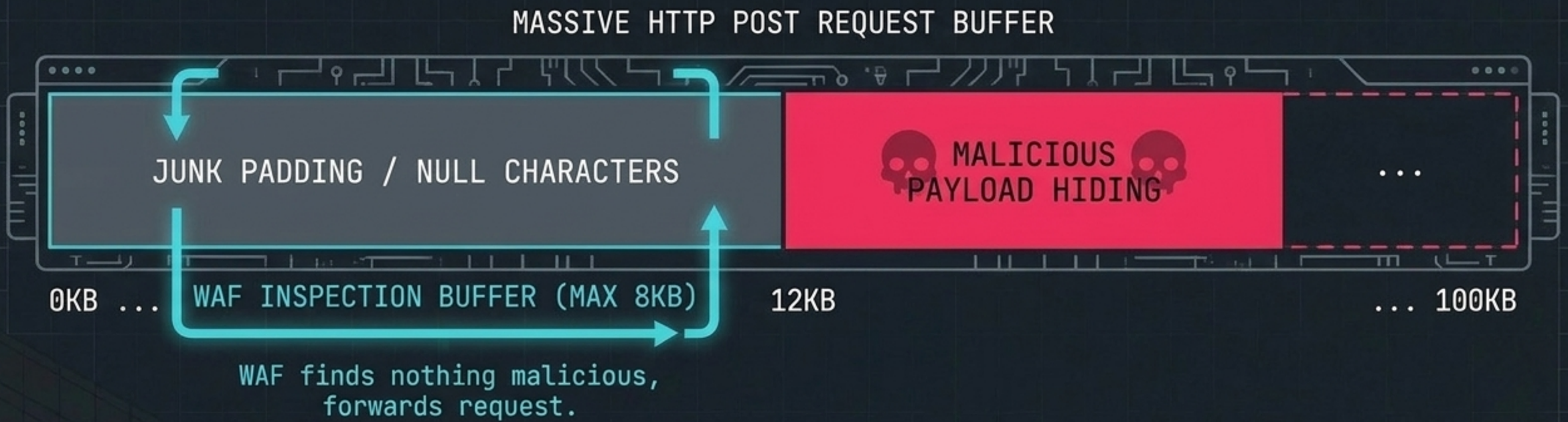



Even if an attacker spoofs the IP, the Origin requires a cryptographic client certificate provided exclusively by the Edge WAF.

Authenticated Origin Pulls cryptographically guarantee that all traffic passed through the WAF inspection pipeline.

Gemini Notebook

# PAYLOAD TRUNCATION & PARSER DIFFERENTIALS



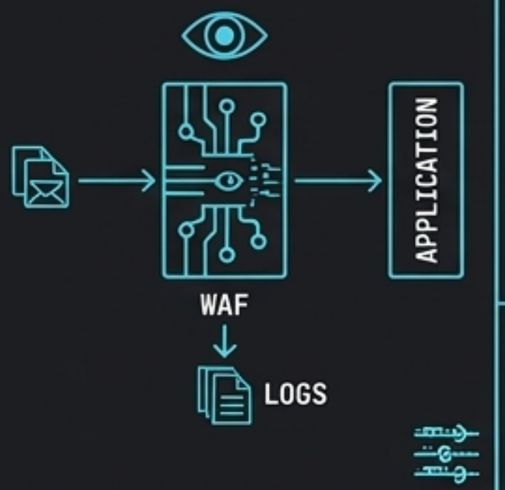

THE EXPLOIT: Attackers pad requests with junk space to push the payload past the WAF's physical RAM inspection limits, executing safely on the backend.

THE FIX: Enforce strict Content-Length limits matching WAF inspection capabilities. Reject any request that exceeds the proxy's visibility.

Gemini Notebook

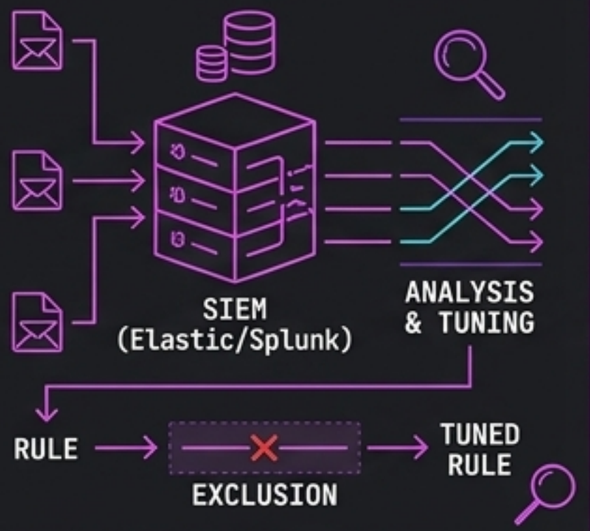
# SAFE ROLLOUT: THE COUNT-TO-BLOCK PLAYBOOK

## PHASE 1: LOG MODE



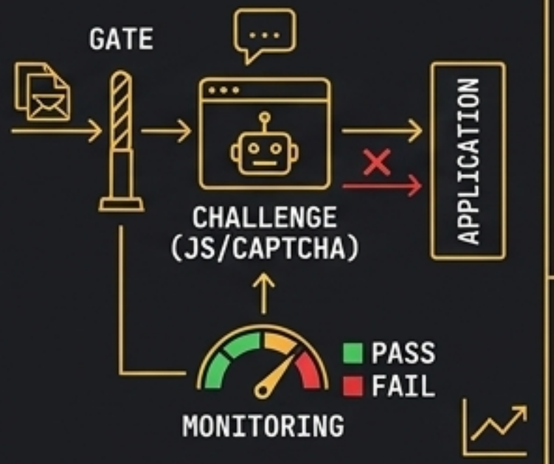

Deploy all WAF rules in passive Count/Log mode. No traffic is blocked.

## PHASE 2: OBSERVABILITY & TUNING



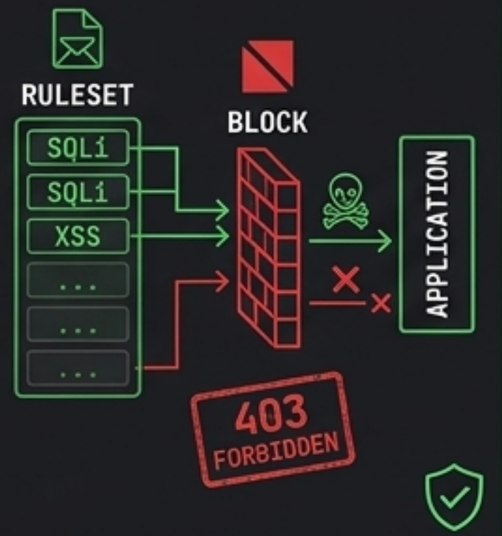

Ingest logs into a SIEM (Elastic/Splunk). Identify False Positives on legitimate application logic. Write targeted exclusions.

## PHASE 3: CHALLENGE MODE




Transition tuned rules to issue JS/CAPTCHA challenges. Monitor completion rates.

## PHASE 4: BLOCK MODE

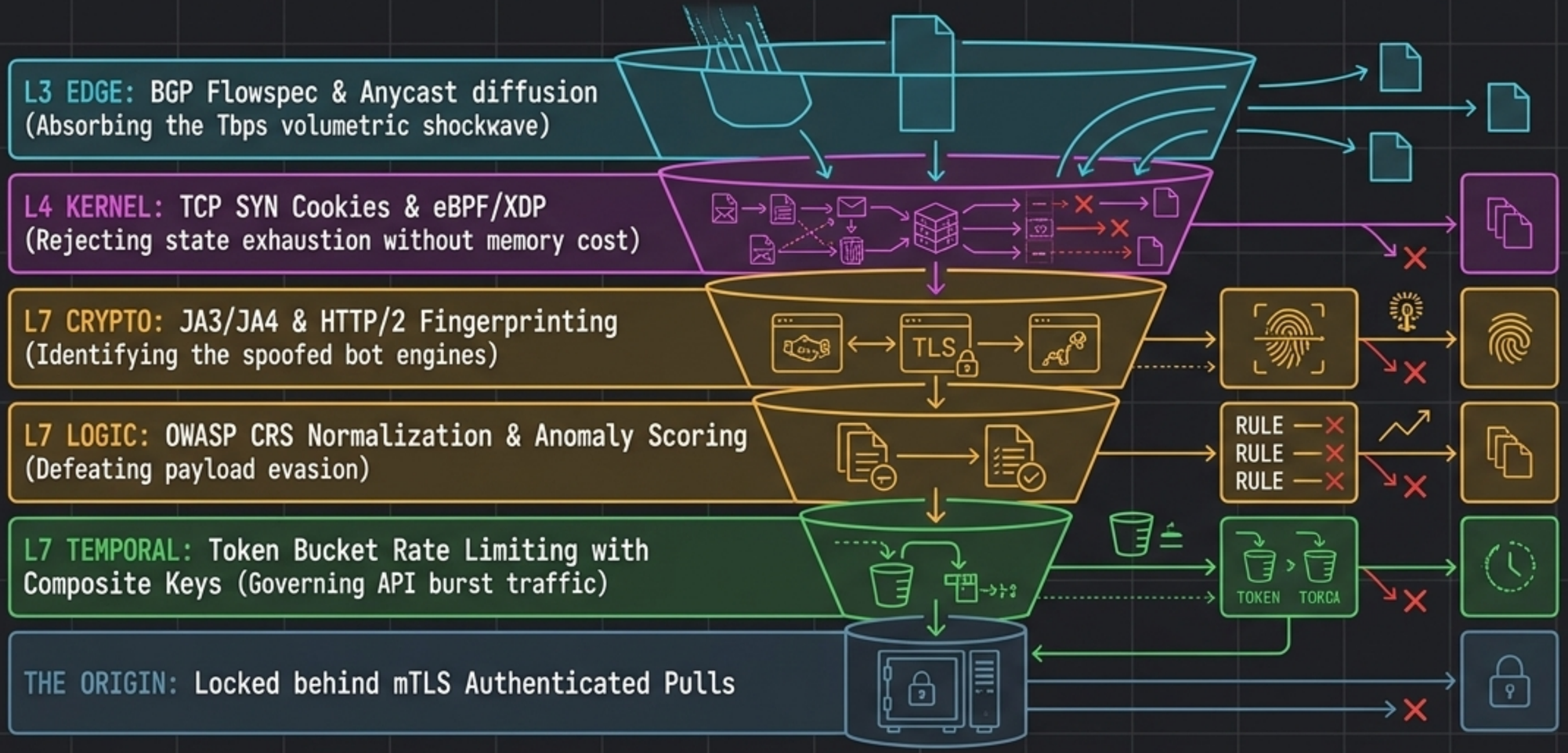



Transition high-confidence rules (e.g., SQLi, XSS) to hard 403 blocks.

**WAFs break applications if deployed blindly.** Rigorous observability and a strict, progressive state transition lifecycle are mandatory for production stability.

Gemini Notebook

# SYNTHESIS: THE HARDENED WEB ARCHITECTURE




True web architecture is a composite of specialized layers. No single firewall stops every threat; robust security is achieved exclusively through the sequential, mathematical exhaustion of the attacker's asymmetric advantages.

Gemini Notebook