DDoS Attack Investigation Report

Incident Selected: Cloudflare 22.2 Tbps Hyper-Volumetric DDoS (September 2025)

Prepared by: Raseena. R

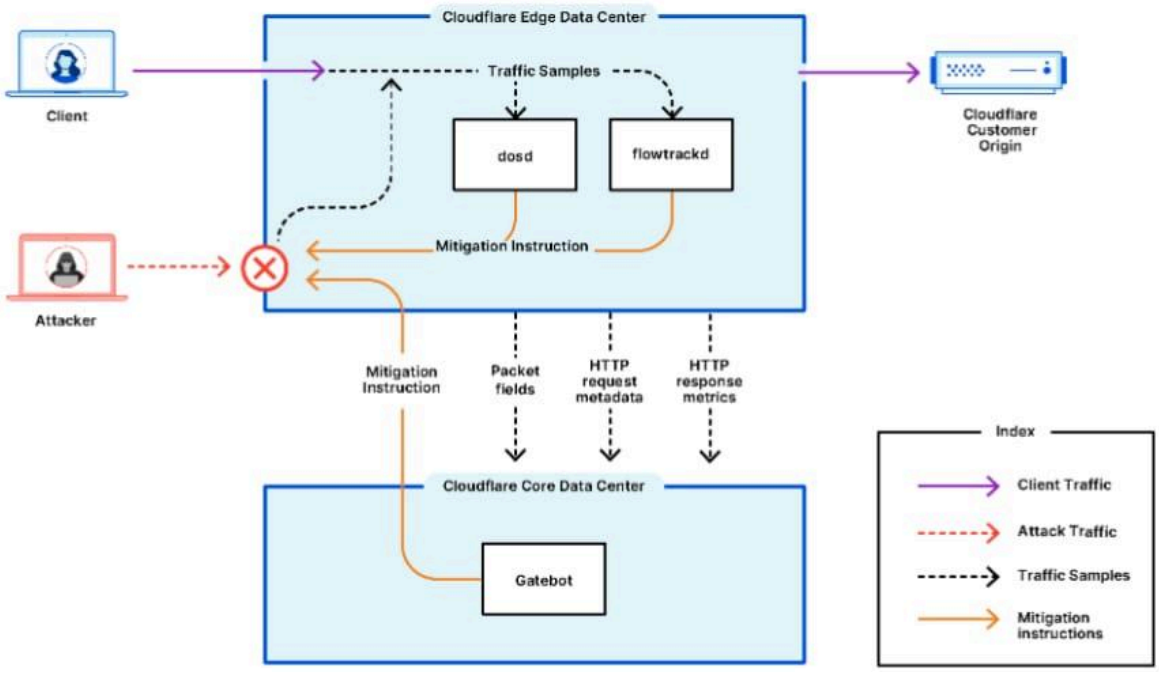
Date: September 28, 2025

1. Target

The attack was observed and absorbed at the Cloudflare global edge network. Cloudflare did not disclose a specific customer target, but the traffic was directed toward services protected by its infrastructure.

2. Technology Used

- The attack peaked at 22.2 terabits per second (Tbps) and ~10.6 billion packets per second (Bpps).
- **Duration:** roughly 40 seconds.
- **Attack type:** hyper-volumetric UDP flood with extremely high bandwidth and packet rates.
- **Likely sources:** large botnets consisting of compromised IoT devices and cloud-based virtual machines.
- **Main effect:** overwhelm network devices by exceeding both bandwidth and packet-processing capacity.



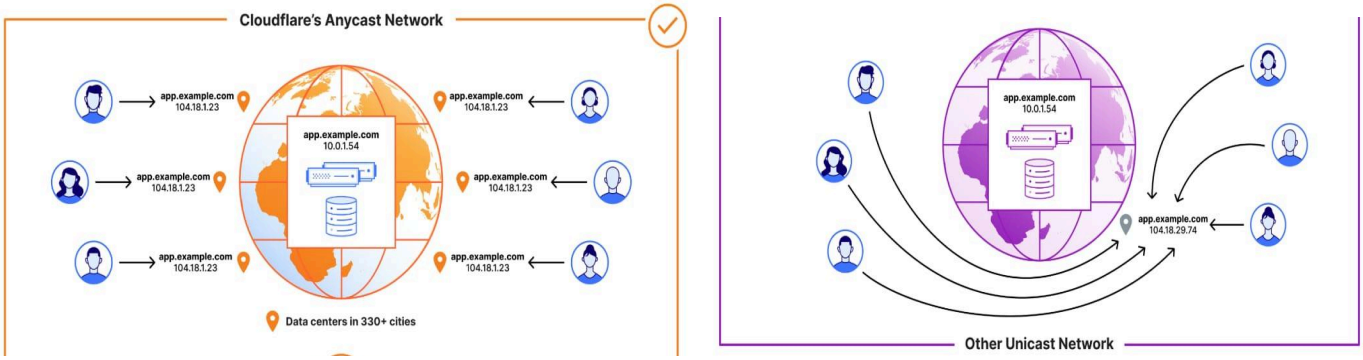
"Cloudflare autonomous edge DDoS mitigation architecture"

3. Attacker's Motive

- Not publicly attributed.
- Possible motives include:
    - Testing a newly built botnet.
    - Demonstrating technical capability for reputation.
    - Distraction for other malicious activity.
    - Potential extortion, though no ransom demand was disclosed.

4. Overall Impact

- Cloudflare successfully mitigated the attack automatically with no reported customer outages.
- However, attacks of this scale highlight systemic risk:
    - Smaller internet service providers or enterprises without access to global scrubbing capacity could suffer service collapse.
    - High packet rates can crash routers and firewalls even if bandwidth seems sufficient.
- The attack sets a new benchmark for the scale of DDoS threats in 2025.

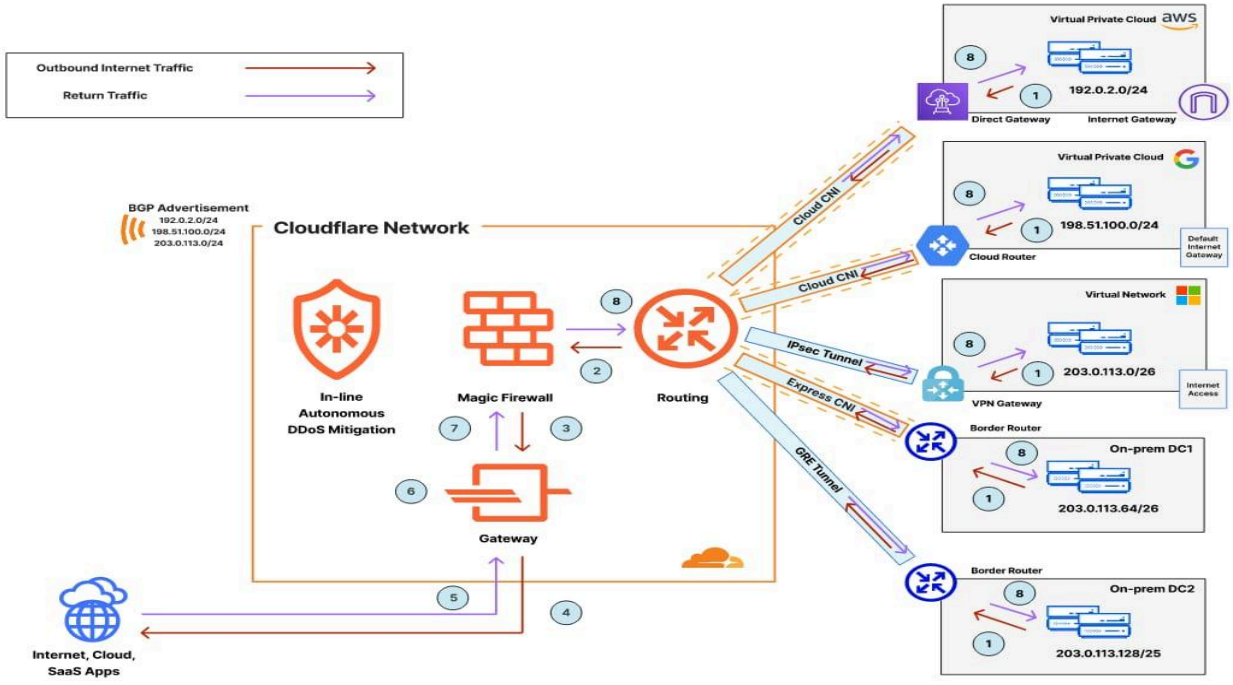


"DDoS flood vs. mitigated traffic flow.

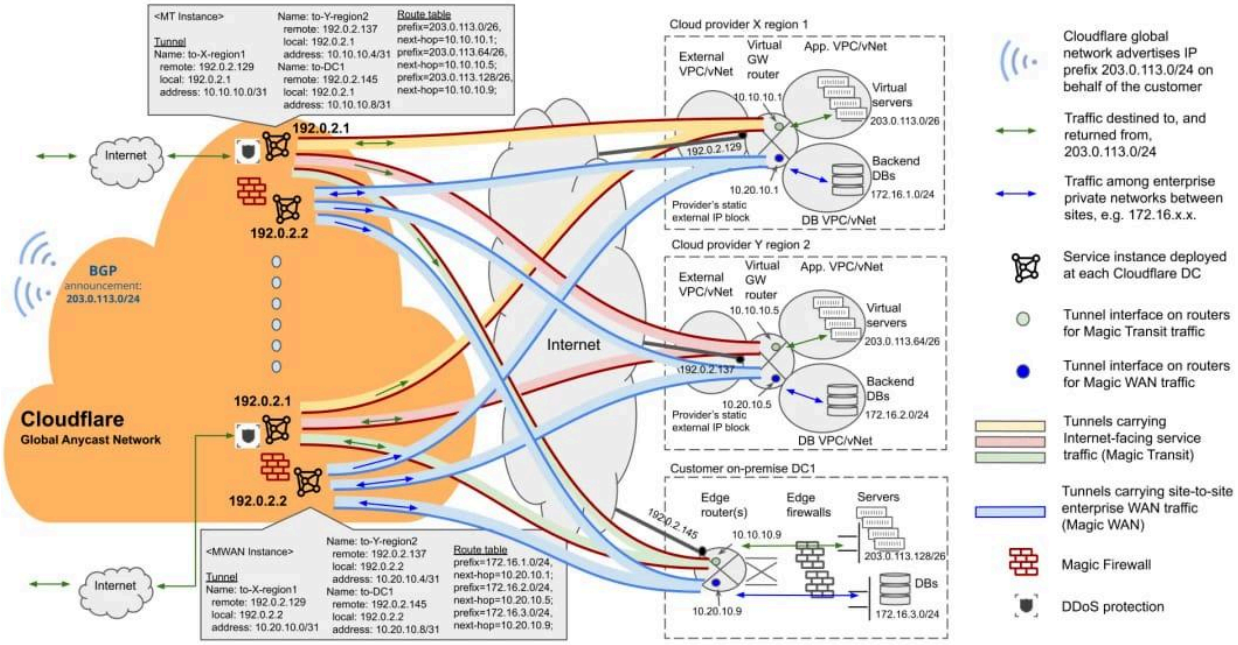
5. Defensive Strategies

Defenses that helped and should be adopted elsewhere:

1. **Distributed scrubbing centers (Anycast + Cloud DDoS protection)** – absorb and filter massive floods before reaching origin servers.
2. **Automated detection & mitigation** – machine learning and anomaly detection systems that respond within seconds.
3. **Packet-processing hardening** – upgrading network devices or offloading to scrubbing to avoid router/firewall overload.
4. **Ingress filtering (BCP38)** – ISPs preventing spoofed traffic at the source.
5. **Upstream cooperation** – working with cloud vendors to shut down compromised virtual machines generating attack traffic.
6. **IoT and device security** – patching, strong authentication, and secure defaults to reduce botnet recruitment.
7. **Application-layer defenses** – rate limiting, challenge–response (e.g., CAPTCHAs) for web services.



"Traffic routing & mitigation via Cloudflare Magic Transit / anycast"



"Reference architecture for protection via Magic Transit"

Conclusion

The **22.2 Tbps hyper-volumetric DDoS attack** against Cloudflare shows that adversaries can generate unprecedented amounts of traffic for short bursts. While Cloudflare absorbed the attack, organizations without such infrastructure are vulnerable. Proactive defenses — combining **cloud-based scrubbing, automated mitigation, ISP cooperation, and device hardening** — are critical to reducing the risk of similar attacks.