Securing the Control Plane and Mitigating DDoS at ISP Scale

- Practical lessons from a transit & access provider

Agenda

- Control-plane protection
- Data-plane DDoS mitigation
- Internal vs external scrubbing
- Machine learning approach (coreroute)
- Lessons learned

Context

- Transit & access provider challenges
- Cannot apply textbook uRPF (asymmetry)
- Attacks vary: sub-10G floods to large volumetric
- Goal: layered, automatable protection

Control Plane: Routing Hygiene

- Dynamic prefix + AS-path filters (bgpq4, NTT sources)
- RPKI validation of all BGP announcements
- Downstream filtering + BGP communities (e.g. blackhole)
- No static filters → auto-regeneration

Control Plane: Tooling

- FRR for BGP control plane
- VPP for policy/ACL flexibility
- Open-source stack → agility, no vendor lock
- Update availability outside vendor cycles

Detection Layer

- fastnetmon ingests sFlow/NetFlow
- Triggers detection + playbooks
- Decision: external vs internal scrubbing

External Scrubbing Center

- Used for large volumetric floods (>10/25G)
- Activated via BGP more-specifics
- Clean traffic returned on agreed path
- Offloads backbone capacity

Internal Scrubbing Center (In Dev)

- Built with VPP ACL-Based Forwarding (ABF)
- ABF policies applied on upstream interfaces
- Keeps scrubbed traffic inside backbone
- Avoids loops (never re-enter external ingress)
- Caveat: ABF lacks sanity filtering → careful scoping

ML Classifier (coreroute)

- Developed by Julian Braun / coreroute
- Trained on booter service traffic
- Targets sub-10G attacks → faster + cheaper than external scrubbing
- Reduces dependency on upstream provider

Lessons Learned

- Layers matter: control plane first, then scrubbing
- External vs internal = cost vs precision
- Placement of scrubbers is critical to avoid loops
- Automation > static configs
- Open-source stack accelerates iteration

Closing

- Key takeaway: combine routing hygiene with mitigation
- Operator reality: attackers innovate, so must defenders
- Q&A