Carrier-Grade Routing Solution Brief: Deploying Border Router DDoS Mitigation: BGP Flowspec and RTBH Configuration Standards

TARGET NETWORK POSITIONING

The Border Router DDoS Mitigation platform is engineered for deployment at the peering edge and core aggregation tiers of carrier-grade and large enterprise networks. It provides a purpose-built control-plane and data-plane foundation for orchestrating BGP Flowspec and Remotely Triggered Black Hole (RTBH) filtering, enabling network operators to surgically suppress volumetric and application-layer attacks without disrupting legitimate transit or peering traffic.

This solution brief details the architectural advantages, redundancy mechanisms, and operational standards that position the border routing platform as the first line of defense against distributed denial-of-service (DDoS) campaigns. It is intended for network architects, security operations engineers, and procurement teams evaluating carrier-class edge routing infrastructure.



HARDWARE-LEVEL FAILOVER REDUNDANCY

The platform is designed around a fully redundant hardware topology to ensure uninterrupted mitigation services even under component failure. Key redundancy features include:

- Dual hot-swappable power supplies with independent AC/DC feeds and load-sharing capability.
- Redundant control-plane and forwarding-plane processors with sub-second stateful failover.
- Hot-swappable fan trays with N+1 rotor redundancy and real-time tachometer telemetry.
- Redundant management interfaces (out-of-band and in-band) for always-on orchestration access.

- BGP graceful restart and non-stop forwarding (NSF) to preserve peering sessions during control-plane restarts.
- Link-level protection through BFD (Bidirectional Forwarding Detection) at sub-50ms intervals for rapid topology convergence.

These hardware-level safeguards ensure that the DDoS mitigation control plane remains available and the forwarding plane continues line-rate filtering even during maintenance or unexpected hardware events.

PROTOCOL SUPPORT MATRIX

The platform delivers comprehensive protocol support for both flow-specification-based mitigation and destination-based blackholing:

- BGP Flowspec (RFC 5575 / RFC 8955) with IPv4 and IPv6 address families.
- BGP Flowspec redirect to VRF, redirect to IP, and traffic-rate limiting actions.
- Remotely Triggered Black Hole (RTBH) using BGP community-based next-hop manipulation (RFC 3882 / RFC 7999).
- BGP ADD-PATH, BGP Large Communities (RFC 8092), and BGP Extended Communities for granular policy enforcement.
- Route Reflector and Route Server capabilities with cluster-based redundancy.
- BGPsec (RFC 8205) path validation for mitigation signal authenticity.

- BMP (BGP Monitoring Protocol, RFC 7854) for real-time telemetry export to external DDoS mitigation controllers.

- sFlow, NetFlow v9/IPFIX, and streaming telemetry for flow-level visibility.

CORE PARAMETERS

The following core parameters define the operational envelope for DDoS mitigation deployment:

- Maximum BGP Flowspec rules: 128,000 (IPv4) / 64,000 (IPv6) per forwarding engine.

- RTBH trigger-to-filter convergence: < 500 ms.

- Flowspec rule installation rate: > 10,000 rules per second.

- Line-rate filtering throughput: 400 Gbps per slot / 3.2 Tbps per chassis.

- BGP peering sessions: up to 4,096 per control-plane instance.

- Mitigation action latency: < 10 microseconds for hardware-accelerated drop and rate-limit actions.

- Control-plane memory: 64 GB ECC for BGP RIB and Flowspec NLRI storage.

Parameter	**Specification**
Form Factor	Modular Chassis / 2RU to 14RU depending on configuration

Switching Capacity	Up to 3.2 Tbps per chassis / 400 Gbps per line card slot
Power Supply	Dual Hot-Swappable Redundant AC/DC (-48V DC, 200-240V AC)
BGP Flowspec Support	RFC 5575 / RFC 8955 (IPv4/IPv6), redirect, rate-limit, drop actions
RTBH Support	RFC 3882 / RFC 7999 with BGP community-based next-hop manipulation
Convergence Time	< 500 ms RTBH trigger-to-filter / < 50 ms BFD failover
Flowspec Rule Capacity	128,000 IPv4 / 64,000 IPv6 per forwarding engine
Mitigation Throughput	Line-rate 400 Gbps per slot with hardware-accelerated filtering
MTBF	> 350,000 hours (Telcordia SR-332)
Redundancy	Dual PSU, N+1 fan trays, redundant supervisor, NSF/GR
Telemetry	BMP, sFlow, NetFlow v9/IPFIX, streaming telemetry
Operating Temperature	0°C to 40°C continuous / -5°C to 55°C short-term

LIFECYCLE ASSURANCE (MTBF)

The platform is designed for carrier-grade availability with the following lifecycle assurance metrics:

- Mean Time Between Failures (MTBF): > 350,000 hours (40 years) calculated per Telcordia SR-332.
- Mean Time To Repair (MTTR): < 2 hours with hot-swappable modular components.
- Annualized Failure Rate (AFR): < 0.25% at 40°C ambient.
- Component derating: All power and thermal components derated by 20% for extended operational life.
- Field-replaceable units: Power supplies, fan trays, line cards, and supervisor modules.
- Warranty: Limited lifetime hardware warranty with advance replacement options.

TARGET BACKBONE TOPOLOGIES

The border router DDoS mitigation solution is optimized for the following

deployment topologies:

- Peering Edge Mitigation: Deployed at external BGP peering points to filter inbound attack traffic before it enters the core.
- Distributed Scrubbing Architecture: RTBH and Flowspec signals orchestrated across multiple border routers to divert traffic to centralized scrubbing centers.
- Anycast Blackholing: RTBH destinations advertised via anycast to distribute drop actions across the backbone.
- Multi-Tier Mitigation: Flowspec at the edge for surgical filtering, RTBH at the core for volumetric emergencies.
- Hybrid Cloud Mitigation: BGP Flowspec redirect to cloud-based scrubbing via GRE or VXLAN tunnels.
- Autonomous System Border Router (ASBR) Integration: Flowspec and RTBH policy propagation across inter-AS boundaries with consistent community mapping.

