



Technical Description

Zayo’s Distributed Denial of Service (DDoS) Protection is a network-based service that proactively monitors customer traffic at the Zayo network edge, detects and mitigates DDoS attack activity upstream of the customer network, and eliminates malicious elements from normal traffic. The service provides an alert system to keep the customer aware of DDoS attacks while Internet traffic flow is unaffected.

Zayo’s DDoS Protection is available to Zayo Internet customers and monitors incoming IP traffic at the host/individual IP address level (/32 level) ensuring only clean traffic is forwarded to the originally intended IP address during an attack. DDoS attack traffic is removed from the traffic flow in a mitigation process that combines BGP Flowspec and the use of Zayo scrubbing devices. Zayo activates DDoS Protection service in a short time – it requires no reconfiguration of customer routing, no additional hardware, and does not use GRE tunnels as it provides network based protection.

CONFIGURATION

The Basic, Standard and Advanced Options provide service on traffic across the Zayo network. The Multi-Carrier Option provides DDoS Protection across non-Zayo carriers (requires Zayo Dedicated Internet Access (DIA) for clean data return).

DDoS Protection Standards	
Number of IP Addresses	Unlimited
Time to Mitigate - Ad-Hoc	15 Mins after a call to our Security Operations Center (SOC) for a manually requested mitigation.
Time to Mitigate - Automatic	Immediate when Auto-Mitigation is enabled. Mitigation relies on BGP to propagate for full effect.
Equipment Vendor	Zayo leverages the Arbor Sightline portfolio deployed globally within its network.
Equipment Ownership	Equipment is owned, operated, updated, configured, and maintained by Zayo.
Hours of Operation	Zayo DDoS Protection Monitoring is always on. Zayo's Security Operations Center (SOC) provides manual mitigation assistance 24x7x365.
Notifications	Zayo provides customers email and SMS alerts when a DDOS attack is detected.
Available Configurations	On Demand, Basic, Standard, Advanced, Multi-Carrier
Protection Portal Access	Zayo’s DDoS Protection Portal is available via the public Internet.
Performance Reporting	Reporting is provided through the Zayo DDoS Protection Portal.



TECHNICAL FEATURES

- **Network-based:** One DDoS Protection Service protects multiple internet services, circuits, and locations anywhere on the Zayo network.
- **Proactive:** Continuously monitoring and identifying DDoS attack activity.
- **Automated:** Automated mitigation helps eliminate response time lags.
- **Distributed:** Zayo distributes mitigation activity across all scrubbing devices, avoiding backhaul, latency, and the potential for a single scrubber to be overwhelmed. Customers are not attached to a single scrubber. Instead Zayo leverages a dirty VRF globally with local Flowspec filtering and scrubbing before returning clean traffic to the Zayo core.
- **Efficient:** Service activation is totally devoid of GRE Tunnels, hardware and configuration requirements. Service is enabled at the IP address level globally.
- **Intelligent:** Access to the Zayo DDoS Portal provides monitoring capabilities, reporting potential and customer involvement in setting thresholds and attack prevention parameters.
- **Surgically applied:** Since scrubbing is done at the individual host level (single /32), our service provides granularity in management and eliminates disruption for non targeted IP addresses. A customer /24 does not need to be inspected when only a single IP is being attacked (unless on Multi-Carrier tier and outside the Zayo network).

HOW IT WORKS

Zayo’s DDoS Protection detects malicious traffic signatures inbound at a per host (/32) level and triggers attack alerts when acceptable traffic levels are exceeded.

- Zayo has developed its own customized mechanisms that can detect some of the newest attack profiles.
- The Service continually updates information related to common DDoS attack patterns.
- The Service uses adjustable algorithms to cull traffic from flows matching known DDoS attack patterns, eliminating false positives.

DDoS Protection Delivery Timeframe (from date of order acceptance)

Site Status	Delivery
All sites with Internet from Zayo	3 calendar days
Ad Hoc Emergency Support (no prior engagement)	45 mins once authorized

GETTING STARTED

Customer Requirements

- A list of IP addresses to be protected
- An order form, including the completed DDoS Mitigation tab on the IP configuration form
- A list of email destinations for Zayo’s alerts and reports

Zayo Requirements

- Provisions the service within 3 days, but can be provisioned in a matter of hours during an ad hoc emergency request (charges apply)
- Sends an Activation Form to the customer confirming the customer’s protected IP addresses
- Provides a login ID and temporary password to access the DDoS Protection Service Portal

