OUR FIBER FUELS GLOBAL INNOVATION

DDoS PROTECTION SERVICE

Service Description

Produced by: Zayo Product Management

Version 2.0 (rev. date December 9, 2021)

Table of Contents

NOTICE

DISCLAIMER: THIS DOCUMENT IS INTENDED TO PROVIDE REASONABLY ACCURATE TECHNICAL INFORMATION RELATED TO THE OFFERING SOLELY FOR YOUR (ZAYO CUSTOMER OR POTENTIAL CUSTOMER) BENEFIT AND DOES NOT IN ANY WAY CONSTITUTE AN AGREEMENT BETWEEN YOU AND ZAYO. THIS DOCUMENT IS NOT A WARRANTY, A SERVICE LEVEL AGREEMENT, OR ANY OTHER GUARANTEE OF PERFORMANCE. ANY SUCH WARRANTIES, SERVICE LEVEL AGREEMENTS, OR GUARANTEE OF PERFORMANCE ARE EXCLUSIVELY CONTAINED IN ANY WRITTEN AGREEMENT BETWEEN YOU AND ZAYO. IN THE EVENT OF ANY CONFLICT BETWEEN THIS DOCUMENT AND ANY WRITTEN AGREEMENT BETWEEN YOU AND ZAYO, THE WRITTEN AGREEMENT SHALL CONTROL.

This document provides Zayo's customers or potential customers a description of Zayo's DDoS Protection Service. Sufficient technical detail is included to enable selections of options and customer facing interfaces suitable for their application needs. Please note that this document does not provide ordering information.

Zayo reserves the right to revise or deviate from this document for any reason, including but not limited to, conformity with standards promulgated by various governmental or regulatory agencies; utilization of advances in technology; or to reflect changes in the design of equipment, techniques, or procedures described or referred to herein.

1. Service Description

1.1 General

Distributed Denial of Service (“DDoS”) attacks are costly and disruptive. Zayo’s DDoS Protection service helps enterprises take an important step towards a comprehensive cyber security plan. Our goal is to provide the best in DDoS detection and mitigation solutions. Customers have three standard subscription options for Zayo’s DDoS Protection: Basic, Standard and Advanced. A non-standard, Multi-Carrier option is also available. The differences among these options are presented throughout this document.

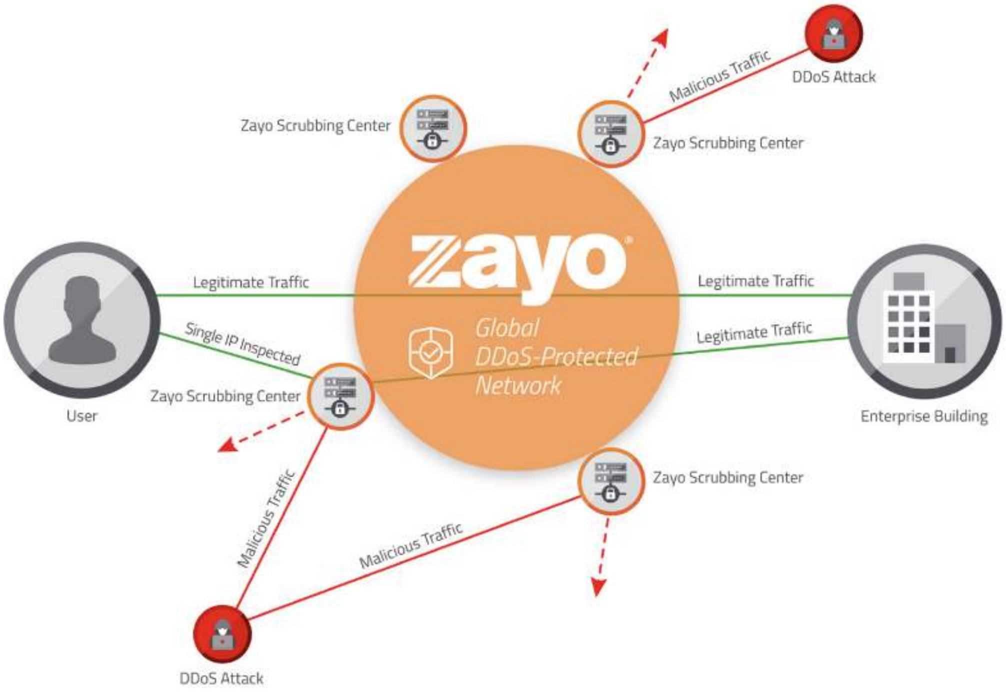


Figure 1: Zayo’s DDoS Protection Service in action.

1.2 Portal Access

Zayo’s DDoS Protection customers who subscribe at the Standard and Advanced levels have access to Zayo’s DDoS Protection Portal. The DDoS Protection Portal provides:

- Insights with traffic analysis,
- Enhanced reporting and
- The ability to manage your DDoS Protection

Basic Subscription users receive the benefit of proactive monitoring and proactive DDoS attack identification. They receive system generated attack alerts and must call in to the Security Operations Center ("SOC") to authorize mitigation of a DDoS attack. Note that this authorized mitigation is offered for an additional charge. Basic Subscription users do not have authorized Portal Access.

Zayo's DDoS Protection Portal access is included in the Standard and Advanced subscriptions.

- Standard Subscription users have read-only access to the Portal;
- Advanced Subscription users have full access to the Portal for use in the self-management of mitigations.

Standard and Advanced Subscriptions offer different methods of authorizing mitigations.

- The Advanced subscriber has the option of Self-Mitigation, Authorized Mitigation or Automatic Mitigation of DDoS attacks. Users of the Advanced option will receive attack alert notifications just like users of other options. Many Advanced Option subscribers choose to test their thresholds before activating the automated mitigation. Alerts are vetted manually for a short period. During that period the customer works with the SOC to optimize threshold levels. Once the customer is comfortable with the threshold levels, Zayo begins automated mitigation. There is no charge for the mitigation.
- The Standard subscriber has authorized mitigation only. Alerts that identify DDoS attacks are sent to the user. The user then calls the SOC to authorize the commencement of a mitigation. The mitigation will commence within fifteen (15) minutes of the authorization call to the SOC. There is no charge for the mitigation.

All Standard and Advanced Subscribers have the ability to view ongoing and historical mitigations within Zayo's DDoS Protection Portal.

1.3 Subscription Options Comparison

Table 1 below presents the high level differences among subscription options:

Service Element	Basic	Standard	Advanced
Pricing Model	Subscription + per scrub	Subscription: MRC* only	Subscription: MRC* only
Monitoring	Proactive/Continual	Proactive/Continual	Proactive/Continual
Attack Identification	Proactive/Continual	Proactive/Continual	Proactive/Continual
Mitigation	Customer calls to request	Customer calls to request	Automated or Self Mitigate

Recovery post mitigation	Immediate	Immediate	Immediate
Incident Notification	Based on alert triggers	Based on alert triggers	Based on alert triggers
Scrubbing Costs	Per incident/mitigation	Unlimited scrubs	Unlimited scrubs
Incident Reporting	Summary of mitigation	Summary of mitigation	Summary of mitigation
Reporting	Not available	Scheduled per subscriber	Scheduled or custom
Portal Access	Not available	Read-only access	Full access

**MRC = monthly recurring charge*

Table 1: Zayo's DDoS Protection service Subscription Options

Multi-Carrier Option: On an individual case basis, Zayo will work with customers to design a multi-carrier DDoS Protection solution.

Zayo's DDoS Multi-Carrier service allows customer connections using networks other than Zayo's AS6461 to be monitored and protected from DDoS attacks. Please note that the Multi-Carrier DDoS Protection option still requires a Zayo IP connection in order to return clean traffic to the customer. Unlike other Zayo's DDoS Protection options, where the customer isn't required to make any network or configuration changes to take advantage of the service, the Multi-Carrier option requires that Zayo interact with customer devices to provide analysis and detection capability on any nodes facing other carriers.

- Customer device(s) must be capable of sending flow data to Zayo's DDoS platform.
- Customer device(s) must allow Read Only SNMP queries from Zayo's DDoS Platform.

In addition, the customer device configuration will require the adjustments listed below, to allow interaction with DDoS specific routing mechanisms. These adjustments allow customer traffic utilizing networks other than Zayo's to be redirected to our scrubbing centers to be analyzed and scrubbed. Zayo will then deliver clean traffic to the customer over their Zayo internet connection(s).

- Customer device(s) should support BGP and more specifically be configured to receive Zayo community tagging of at least a partial BGP table.
- Traffic protected on other carrier networks must be using IPs that the customer is allowed to advertise from other networks. During an attack, targeted subnets will be temporarily moved behind Zayo's defenses.

- Additional configuration details may be unique to the customer. Zayo's Multi-Carrier Product Customer Configuration Guide contains additional information. Please contact your Zayo account manager for a copy of this Guide.

1.4 Mitigation Types

Authorized Mitigation: In the event of an attack, Zayo's DDoS Protection system automatically sends the user a detection alert for review. The user must then call the SOC to authorize (request) the mitigation. This mitigation process is available in the Standard Option and the Basic Option. Zayo will commence mitigation within 15 minutes of the receipt of authorization to mitigate. This option is ideal for enterprises whose businesses need DDoS protection but don't expect to use it often.

Automatic Mitigation: Automatic Mitigation is for the enterprise that needs the peace of mind that comes with automatic protection. The Zayo DDoS Protection System is able to identify DDoS attacks with precision and immediately initiate the mitigation process – without individual authorization from the customer. Automatic Mitigation is available with the Advanced Subscription Option.

Self-Mitigation: Available only in the Advanced Subscription Option, Self-Mitigation provides the user with the capability to take full control of a mitigation and manage the process themselves. The user in any given situation can activate, manage and terminate the mitigation without contacting the Zayo SOC. Subscribers with sophisticated security staff and the desire to run mitigations themselves may find this capability useful.

1.5 Zayo's DDoS Protection Service Activation

Zayo typically activates DDoS Protection Service in 3-5 days after we accept a customer order. To activate, the subscriber must identify:

- The IP addresses and IP address strings to be protected
- The email addresses to which the subscriber wants alerts to be sent
- The email addresses to which the subscriber wants reports sent

In order for Zayo to efficiently and accurately establish the initial IP address configuration, the customer will need to complete the DDoS Mitigation tab of Zayo's IP Configuration Worksheet.

To activate Zayo's DDoS Protection, there is no requirement for the subscriber to change routing tables or router configurations. With the exception of Multi-Carrier DDoS protection, Zayo can configure all the relevant protection and mitigation processes transparently to the customer.

Zayo's DDoS Protection is designed to monitor traffic for each IP address identified by the subscriber as one to be protected. The subscriber can obtain these IP addresses from any source; so long as the subscriber controls the IP address and advertises it over Zayo's network, Zayo can protect it from DDoS attacks. Please note that in order for Zayo to monitor traffic and identify DDoS attack elements, the traffic for the designated IP addresses must flow across the Zayo IP network. Zayo cannot monitor traffic that never touches the Zayo network, unless using the Multi-Carrier service.

The IP address is the key element protected by Zayo's DDoS Protection service. Zayo's DDoS Protection service is a virtual solution that provides an umbrella of protection for all IP addresses the subscriber wishes to protect, no matter where they are located. Again note that Zayo can protect only IP traffic that traverses the Zayo IP network.

A single implementation of Zayo's DDoS Protection Service provides protection to IP addresses associated with any number of customer locations. The price of the service is determined by the amount of bandwidth required for the protected IP addresses. The number of IP locations (for both Dedicated Internet Access ["DIA"] and IP Transit) is not a factor in the price. Zayo places no limit on the number of IP addresses a subscriber can protect, nor is any association made to the underlying circuits ordered from Zayo. A subscriber may add IP addresses by sending an email from an authorized user with the additional IP addresses to the SOC at security.support@zayo.com.

- Please note: The addition of IP addresses may drive an increase in protected IP bandwidth. When increasing IP capacity, the capacity required to protect your IP addresses will also need to increase. Without the commensurate increase in DDoS Protection capacity, your service may not be correctly sized to protect the increased bandwidth. DDoS Protection bandwidth increases may impact the price. Note that Zayo does not charge for attack volume, all bandwidth measurements are in respect to typical clean traffic.

The DDoS Protection service protects all traffic that flows across the customer network. The agreement and the price are based on the customer's estimation of their normal traffic flow. If normal traffic patterns prove to be greater than the contracted bandwidth on a continuing basis, Zayo and the customer will adjust the contracted bandwidth and reset a price commensurate with the adjusted bandwidth.

1.6 System Automation

Zayo's DDoS Protection is an automated system of monitoring, detection and alerting of DDoS attacks. The system provides an automated alert that a DDoS attack is underway. For authorized mitigations, the customer must contact the Zayo support team to initiate a mitigation of the attack. The support team does not monitor the system and does not initiate notification beyond that provided by the automation in the system process. It is incumbent on the subscriber to react to alerts and connect with the support team in the management of mitigations in accordance with the contracted option.

Subscribers may call the support center and request mitigations on traffic that may not be subject to an alert.

- This service is included in the Standard and Advanced Options.
- This service is billable in the Basic Option.

Subscribers are provided a reasonable number of such requests.

2. Important Definitions

Distributed Denial of Service (DDoS) is an attempt to exhaust the resources available to a network, application, or service so that genuine users cannot gain access. Types of DDoS attacks include:

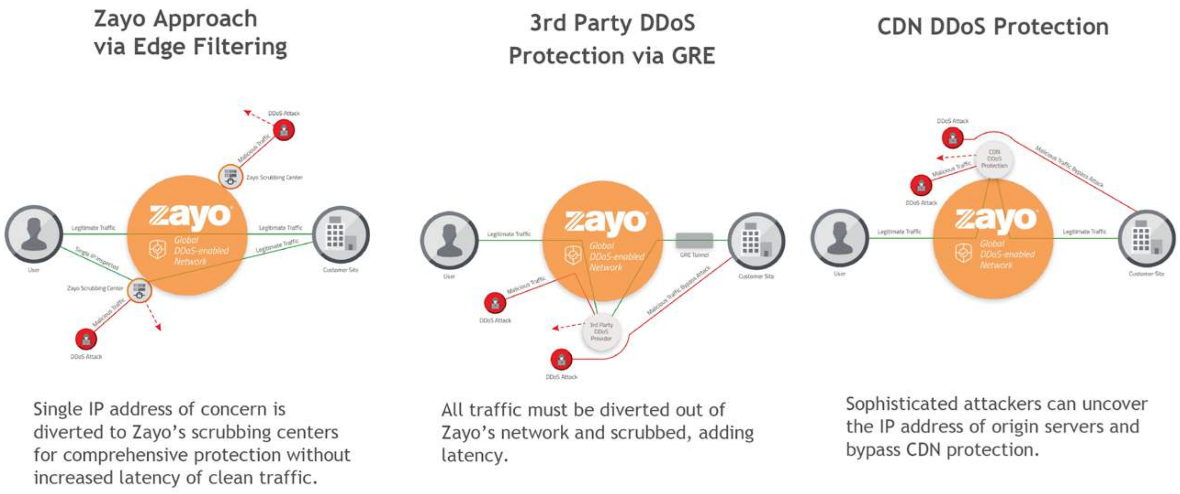
- **Volumetric DDoS Attacks:** Volumetric attacks attempt to consume the bandwidth either within the target network/service, or between the target network/service and the rest of the Internet. These attacks are simply about causing congestion. Examples of Volumetric DDoS attacks include:
    - ICMP Flood
    - IP/ICMP Fragmentation
    - UDP Flood
    - IPSec Flood (IKE/ISAKMP association attempts)
    - HTTP/S Flood

- **TCP State-Exhaustion DDoS Attacks:** TCP State-Exhaustion attacks attempt to consume the connection state tables which are present in many infrastructure components such as load-balancers, firewalls and the application servers themselves. Even high capacity devices capable of maintaining state on millions of connections can be taken down by these attacks. Examples of TCP State-Exhaustion DDoS attacks include:
    - SYN Flood
    - SSL Exhaustion
    - DNS query/NXDOMAIN floods

- **Application Layer DDoS Attacks:** Application Layer attacks target some aspect of an application or service at Layer-7. These are the most disruptive attacks as they can be very effective with as few as one attacking machine generating a low traffic rate (this makes these attacks very difficult to proactively detect and mitigate). Application layer attacks have come to prevalence over the past three or four years and simple application layer flood attacks (HTTP GET flood etc.) have been some of the most common denial of service attacks seen in the wild. Examples of Application Layer DDoS attacks include:

- BGP Hijacking
- Slowloris
- Slow Post
- Slow Read
- Low and Slow Attack
- Large Payload POST requests
- Mimicked User Browsing
- Reflection Amplification DDoS Attacks
- DNS Reflection/Amplification DDoS Attack

Content Delivery Network ("CDN"): A content delivery network, or content distribution network, is a geographically distributed network of proxy servers and their data centers. The goal is to provide high availability and performance by distributing the service spatially relative to end users. Generally, users of CDNs are afforded protection of web services (see web application firewall definition below). DDoS Protection from Zayo extends this web service protection to protection of IP-based applications accessed remotely by employees. CDN networks do not always provide adequate protection of the last mile physical connectivity to a customer location.



Zayo Approach via Edge Filtering

Single IP address of concern is diverted to Zayo's scrubbing centers for comprehensive protection without increased latency of clean traffic.

3rd Party DDoS Protection via GRE

All traffic must be diverted out of Zayo's network and scrubbed, adding latency.

CDN DDoS Protection

Sophisticated attackers can uncover the IP address of origin servers and bypass CDN protection.

Figure 2: Zayo's Inline DDoS Protection provides pure DDoS Attack Protection without the complexities and latency of other methods such as GRE or CDN

A web application firewall ("WAF") is a specific form of application firewall that filters, monitors, and blocks HTTP traffic to and from a web service. Web application firewalls are designed to block HTTP traffic from interfering with the delivery of web applications and services. WAF's are intended to protect against malicious payloads and are not effective against volumetric attacks unless combined with a DDoS protection technology.

Other firewalls are not without DDoS Protection capability. They prevent defined bad traffic from accessing the network. They are limited in their effectiveness and ability to withstand the volume of traffic in a DDoS attack. The DDoS attack environment now requires a specialized DDoS Prevention Service that functions outside the firewall. While firewalls offer some protection against a DDoS attack, a dedicated DDoS Protection Service provides comprehensive coverage at the scale necessary to prevent volumetric attacks from overwhelming upstream connectivity.

BGP Flowspec: Border Gateway Protocol ("BGP") Flowspec is an alternative and a more granular method to Remotely Triggered Black Hole ("RTBH") described in RFC5575 that can be used to mitigate a DDoS attack. Match criteria allow network operators to define a particular flow with source, destination, layer-4 parameters and packet specifics such as length. While BGP Flowspec offers an essential element of DDoS protection against volumetric attacks, it does not offer complete protection. A dedicated DDoS Protection Service provides comprehensive coverage. Zayo utilizes flowspec as part of its defensive strategy to help mitigate volumetric attacks where they enter our network.

Threat Management System (TMS): Zayo's DDoS Protection Service uses DDoS scrubber technology that integrates network-wide intelligence and anomaly detection with carrier-class threat management to help identify and stop volumetric, Transmission Control Protocol ("TCP") state exhaustion and application layer DDoS attacks. Zayo's network appliances provide the vital, traffic-scrubbing component of the Zayo solution.

Inline DDoS Protection: Inline security refers to solutions deployed in the flow of live network traffic and used to identify and prevent cyberattacks and other security incidents for all traffic passing through them. Zayo's solution provides inline DDoS Protection.

3. DDoS Protection Pricing

DDoS Protection prices are based on the aggregated normal levels of clean traffic the customer actually experiences across the network supporting the IP addresses identified by the customer for protection. Typically, actual traffic levels are about half of the committed DIA or IP Transit levels.

"Clean traffic" is the normal (average) level of traffic that crosses the network when there is no DDoS attack activity. If an account has more than one DIA service, the bandwidth is the aggregate of actual traffic across all DIA circuits, services and locations.

One DDoS Protection Service protects IP addresses on all DIA services provided by Zayo. This makes the ordering process easy; with one service order and one price point, customers protect all of their Zayo IP traffic.

4. Features

Please find below a list of the key features of Zayo's DDoS Protection service.

- **Attacks identified/absorbed in Zayo Network**: Zayo is Tier 1 IP provider with over 26Tb+ of peering capacity. The entirety of the Zayo network can be used to filter and absorb attack traffic, shielding the customer whose devices and network cannot absorb significant levels of attack. This is the benefit of an inline DDoS Protection service provided by a Tier 1 provider.

- Zayo's service is **Automated and Proactive:** The Zayo DDoS Protection service is system-driven and automated.
    - **Monitoring** is always on and continually active; all Zayo Peering Edge routers perform monitoring of Zayo's IP traffic.
    - **Identification** of attack traffic is also completed in the Zayo Peering Edge routers, well upstream from the customer firewall and other network devices and applications. Upon recognition of an attack, the Zayo DDoS Protection system sends an alert to the subscriber in the form of an email and/or short message service (SMS). The alert option can interact with Syslog functionality as well.
    - **Mitigation** is incident driven and is activated in response to an attack or upon request by the subscriber. Zayo employs a two-level mitigation capability: BGP Flowspec filtering and DDoS scrubbing. Manual mitigation is initiated by the Zayo Security Operations Center ("SOC") upon request by the subscriber. Automated Mitigation can be enabled for Advanced and Multi Carrier Subscribers upon request, and provides a 'hands off" fully automated DDoS Protection service.
    - **Restore** is an automated process for continued mitigation of traffic for targeted IP addresses to ensure that DDoS attacks are truly finished; traffic is scrubbed for a period to ensure there is no further attack and then redirected to the normal BGP routes.

- **Zayo offers alert choices.** Monitoring and Attack Identification are activated in Zayo Peering Edge Routers automatically. The system will send an Alert Notification to the Zayo DDoS Protection subscriber. Alerts can be sent via:
    - Email - to real and/or alias email addresses
    - SMS - a text message
    - Syslog Interface

- **Zayo's DDoS Protection is a network-based service (Zayo owns the equipment and our Security Operations Center):** This relieves the customer of the expense of people and equipment. Zayo provides the customer scalability and rapid adaptability as the customer's environment evolves. We provide the support structure using Zayo employees in our SOC. Our SOC's security personnel are cybersecurity specialists, experts in the operations of the DDoS Attack environment, skilled in optimizing the Zayo DDoS Protection Service to the customer's IP environment and willing and able to discuss a variety of cybersecurity issues with the customer at any time. Since Zayo owns the infrastructure, the DDoS mitigation is in-line and within our core network. Your traffic does not have to be diverted to another network for mitigation first.

- We employ a **unique scrubbing technique:** Zayo scrubbers are located at the most highly trafficked peering points on the Zayo network. DDoS attacks are often geographically dispersed, where malicious traffic is sent from multiple geographies to the targeted host. In the Zayo scheme, malicious traffic is routed to the scrubber nearest the point where the attack enters the Zayo network. For example, attack traffic from the Pacific will enter the Zayo network on the West Coast and flow through the Los Angeles scrubber. Traffic in the same attack that originates in France will enter the Zayo network in Europe and be scrubbed in Paris. Zayo scrubs regionally without backhaul, and delivers clean traffic to the customer.

This process reduces latency as most traffic will flow through these locations and scrubbing will not affect traffic flow. Further, this technique distributes scrubbing, using all Zayo scrubbers in each DDoS attack, eliminating the reliance on a single scrubber dedicated to a specific account in a specific geographic location. Zayo's scrubbing technique eliminates the bottlenecks and limitations created by a configuration that assigns a single scrubber to a customer.

- **Ease of Activation:** As an inline DDoS Protection Service, Zayo can activate DDoS Protection in about three (3) days, and more quickly in an emergency. The process excludes use of GRE configuration and (except for the Multi Carrier Option) does not require configuration activity on the part of the subscriber. Subscribers need only provide a list of IP addresses to be protected and destination email addresses for alerts and the weekly and monthly reports.

- **Access to the Zayo DDoS Protection Portal** is included in Standard, Advanced and Multi Carrier Option subscriptions. In addition to the monitoring, attack identification, alerting and mitigation provided by Zayo, the subscriber has a window into all activities associated with Alerts, Mitigations and traffic flows that are monitored by Zayo. This is real time data from which the subscriber can glean critical information about malicious activities on its network and can work with the Zayo Security Operations Center to understand traffic thresholds, establish counter measures, and optimize the Zayo DDoS Protection service for maximum benefit to the subscriber.

- **Scrub at IP Address level:** Zayo's DDoS Protection protects defined IP addresses. It is a virtual service that is not associated with a circuit, a location or a specific service. Only the traffic for the targeted IP address enters the scrubbing process. This maintains the integrity of the remaining traffic and ensures continued uptime and availability of business critical network connections. An attack against a single IP (/32) can be mitigated at a single IP level without touching the flow of other hosts on the same /24 subnet (with the exception of Multi-Carrier customers using other networks as primary transport).

- **One DDoS Protection service for many Internet services:** Zayo's DDoS Protection is a virtual overlay service able to protect multiple Dedicated Internet Access ("DIA") or IP Transit services obtained from Zayo. The DDoS Protection Service is agnostic relative to circuit, location or service. One DDoS Protection Service (a single service order and a single price point) provides DDoS Protection to Internet services that include multiple locations, multiple circuits, and multiple Internet Services.

- **Multi Factor Authentication to Zayo's DDoS Protection Portal:** Zayo can offer Multi Factor Authentication to the Zayo DDoS Protection Service Portal. The capability is a non billable functionality that enhances the security of Zayo's DDoS Protection Service capability. Accessibility to Subscriber Zayo DDoS Protection Service Portal requires greater authentication than is provided by a .username and password.

5. Use Cases

Zayo's DDoS Protection is ideal for any user of Zayo's DIA or IP Transit wishing to protect their IP traffic from DDoS attack, but without the cost of investing in a full protection system, the security personnel required to operate the system around the clock, and the data intelligence integrated within the system.

Zayo's DDoS Protection is especially useful for businesses whose brands are vulnerable to attacks, and who have distributed their IP services to Zayo and other internet providers. Examples include:

- **High-Visibility Brands** - the more recognizable the name, the more vulnerable the business is to attacks.
- **High-Impact Enterprises** - we place healthcare and financial institutions in this category - when lives or livelihoods are on the line, protection and security of the network are paramount.
- **Cloud Users** - any enterprise with data stored, processed or accessed from the cloud is vulnerable to an attack of the network accessing that data.
- **Companies with Firewalls only** - Firewalls are not enough; they won't mitigate large DDoS attacks. Firewalls often fail with very low throughput as they are designed to track state.
- **Users of Content Delivery Networks (CDNs):** CDNs protect web services. DDoS Protection from Zayo extends this web service protection to protection of IP-based applications accessed remotely by employees.

All Internet Traffic is Covered

Another way to view Zayo's DDoS Protection is to test its applicability to different activities and services accessed via the Internet. Zayo's DDoS Protection safeguards all of the following traffic:

- E-Commerce: clients that connect to your servers;
- Business-to-Business ("B2B"): business partners that connect to your servers;
- Internet: your employees and contractors that connect to the internet; and
- Virtual Private Networks ("VPN"): employees working remotely that connect to your enterprise.
- Much more!

Most DDoS attacks are on services without protection. Zayo *can* mitigate a DDoS attack without an existing subscription, but one-off mitigation costs are expensive and inconvenient. During a just-in-time mitigation, service is down until restored. Additionally, this reactive solution takes time; Zayo and the customer have not established an understanding of the usual traffic flows.

With a subscription in place, all protected traffic is proactively monitored. The DDoS Protection system identifies the attack and activates an alert well upstream of the subscriber network. Healthy traffic is unaffected by the attack. Zayo's subscription options offer a massive inline network of protection for a reasonable cost.

Zayo looks forward to designing a DDoS Protection solution that is ideal for each customer's business security.

6. Technical Description

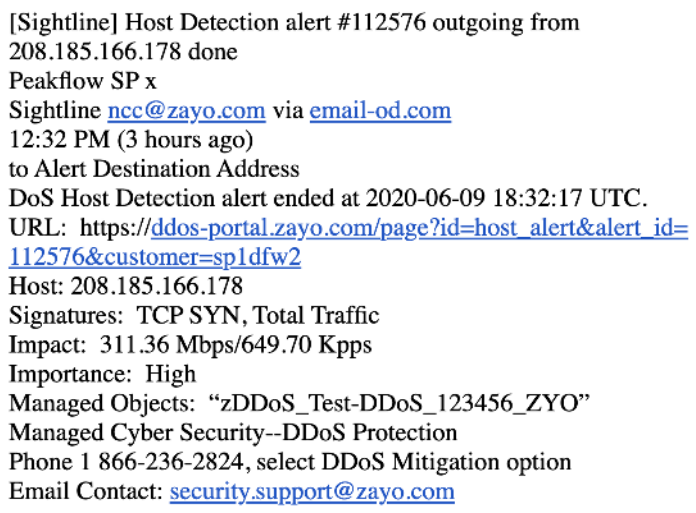
6.1 Zayo’s DDoS Protection System Operation - Sample Alert

Zayo’s DDoS Protection provides automated and proactive monitoring of customer traffic as it enters the Zayo network. This process is always active and continually tracks the flow of traffic to the IP addresses the customer identified for protection.

The monitoring process identifies potential DDoS attacks targeting the IP addresses identified for protection. This identification mechanism is always on and continually operates to protect customer traffic.

Zayo and the customer first define the Host Detection Threshold - the ‘normal’ flow of the customer’s IP traffic. When the customer’s traffic flow deviates from the Detection Threshold defined at twice the defined level, an alert is issued and sent to all email addresses specified by the customer at the time of system initiation. This alert process is automated; all alerts are system generated.

Figure 2 below presents an example alert. Please note that Zayo provides the same information in email and SMS text alerts:



```
[Sightline] Host Detection alert #112576 outgoing from
208.185.166.178 done
Peakflow SP x
Sightline ncc@zayo.com via email-od.com
12:32 PM (3 hours ago)
to Alert Destination Address
DoS Host Detection alert ended at 2020-06-09 18:32:17 UTC.
URL:  https://ddos-portal.zayo.com/page?id=host_alert&alert_id=
112576&customer=sp1dfw2
Host: 208.185.166.178
Signatures:  TCP SYN, Total Traffic
Impact:  311.36 Mbps/649.70 Kpps
Importance:  High
Managed Objects:  “zDDoS_Test-DDoS_123456_ZYO”
Managed Cyber Security--DDoS Protection
Phone 1 866-236-2824, select DDoS Mitigation option
Email Contact: security.support@zayo.com
```

Figure 2: A example system-generated alert of a DDoS attack in progress

The process, up to the point an alert is issued, is the same for all Zayo’s DDoS Protection subscriptions. Zayo proactively and continually applies monitoring, attack identification and alerts (incident notifications) to all subscribers of Zayo’s DDoS Protection service.

6.2 Zayo's DDoS Protection System Operation - Mitigation Types

Upon receipt of an alert, Basic and Standard Option subscribers can review the situation described in the alert and determine whether to request a mitigation. A subscriber needs to authorize the mitigation by contacting the Zayo SOC and requesting a mitigation. The Zayo support team will then initiate the mitigation within fifteen (15) minutes of the authorization.

For Advanced Option subscribers, Zayo sets the default mitigation to "Authorize." This means that Advanced Option subscribers need to contact the Zayo SOC to change this default setting. Advanced mitigation options include:

- **Fully automated mitigation**. Zayo's DDoS Protection system will automatically mitigate a DDoS attack. Mitigations will commence immediately upon recognition of a DDoS attack and will be system generated. The subscriber will still receive an alert. After receipt of the alert, the subscriber may contact the SOC to request that the mitigation be terminated.
- **Self-mitigation.** The subscriber may take full charge of the mitigation. Follow the steps in the DDoS Protection Portal Guide under the heading, "Running a Mitigation." This is something the subscriber can do on an ad hoc basis. The action will override the otherwise automated mitigation process.
- **Authorized mitigation (default setting).** The default mitigation setting for Advanced Option subscribers is Authorized mitigation. With Authorized mitigation, the subscriber must call into the Zayo SOC to authorize (request) mitigation. Zayo has set Authorized mitigation as the default option because many Advanced Option subscribers prefer to first review alerts and determine whether mitigation is desired. The mitigation will commence within fifteen (15) minutes of the time the subscriber authorizes (requests) the mitigation.

Advanced Option subscribers can contact the SOC to request a change to any of the mitigation options available. The support team will activate the change upon request.

6.3 Zayo's DDoS Protection System Operation - Data Center Customers

Customers located within data centers might take advantage of "blendwidth" - where the data center operator incorporates multiple carriers in the delivery of traffic to the data center, often using a shared IP subnet (smaller than /24). The benefit of this is that the data center operator delivers customer traffic across any of the carrier circuits. Traffic usually takes the most available circuit.

In this environment the Zayo DDoS Protection will not be complete:

- Zayo will see and be able to monitor only the traffic that transits the Zayo circuits. Traffic crossing circuits of other carriers will not be monitored.
- Additionally, since customer traffic is directed to the most available carrier circuit, the traffic that flows across the Zayo circuit will be variable and will not represent an accurate baseline flow of traffic. Zayo's DDoS Protection service detects DDoS attacks by monitoring against an accurate baseline.

Generally, customers in such a "blendwidth" environment cannot take advantage of the full protection offered by any provider's DDoS protection service. Zayo may be able to design a customized Multi-Carrier DDoS Protection service for data center customers (see Section 1.3 above). Ask your account manager and sales engineer if such a design is possible and would benefit you.

7. Zayo Support for DDoS Protection

Zayo's Security Operations Center ("SOC") manages Zayo's DDoS Protection service. Zayo trains an extensive security team to respond to subscriber inquiries related to the DDoS Protection platform. The team is available twenty-four (24) hours per day, 365 days per year. Any subscriber may contact the SOC team for any questions concerning mitigations, configuration and system operation.

Customers may contact the SOC to:

- Activate or deactivate Automated Mitigation
- Add IP addresses or delete IP addresses
- Change alert destinations
- Change report destinations
- Review and adjust alert thresholds
- Interact on mitigations
- Discuss any aspect of the operation of Zayo's DDoS Protection service

Contact the Cyber Security DDoS Protection team within the SOC:

- Phone Contact: 1 866-236-2824, Option 1 and then Option 2 for DDoS Mitigation
- Email Contact: security.support@zayo.com

The SOC is part of a global Zayo support capability that includes Network Operations Centers (collectively referred to as the Zayo NOC) in:

- Tulsa, Oklahoma, US
- Montreal, Quebec, Canada
- Westminster, Colorado, US

For network-related issues, please contact the NOC by:

- Calling 1 866-236-2824
- Emailing zayoncc@zayo.com
- Clicking https://www.zayo.com/contact/technical-support

To escalate any issue, you can find Zayo’s escalation contacts here:
https://tranzact.zayo.com/#!/escalation-lists

8. Glossary

Term	Definition
Autonomous Systems ("AS")	A group of connected Internet Protocol routing prefixes governed by one or more network operators. Each AS presents a clearly defined routing policy to the internet and is assigned an Autonomous System Number (ASN) to enable the free-flow exchange of information via BGP.
Availability (IP)	IP "Availability" means the percentage of time that a Customer location can access the Zayo network. The Availability measurement period begins when a Zayo trouble ticket is opened and is calculated on a calendar month basis.
Bit	A binary unit of information. It is represented by one of two possible conditions, such as the value 0 or 1, on or off, high potential or low potential, conducting or not conducting, magnetized or demagnetized. A bit is the smallest unit of information, by definition.
Border Gateway Protocol ("BGP")	The standard routing mechanism for the internet, it is designed to exchange and forward packets among all Autonomous Systems (AS) and identifies the most optimal route from source to destination.
BGP Hijacking Attack	BGP hijacking is an application-layer DDoS attack. It is also referred to as prefix hijacking, route hijacking and IP hijacking. BGP hijacking is the attempted takeover of groups of IP addresses by corrupting Internet routing tables maintained using the Border Gateway Protocol (BGP).
DNS Query NXDOMAIN Flood Attack	In a Domain Name Server (DNS) non-existent domain (NXDOMAIN) flood attack, the attacker floods the DNS with requests for invalid or nonexistent records. These state exhaustion DDoS attacks are handled by a DNS Proxy server, which will use nearly all of its resources querying the DNS Authoritative server with these records.
DNS Reflection/Amplification DDoS Attack	This type of attack takes advantage of vulnerabilities in domain name servers (DNS) to amplify small queries creating larger payloads. These payloads consume all the bandwidth typically used by legitimate traffic, blocking that traffic while bringing down the attacked servers.
GRE Tunnel	Generic Routing Encapsulation is a protocol for encapsulating data packets that use one routing protocol inside the packets of another protocol. GRE Tunnels forwards traffic to the origin network after the traffic has been scrubbed from a DDoS Attack which increases latency

HTTP/S Flood	HTTP/S floods are DDoS attacks designed to overwhelm a web server's resources by continuously requesting standard URLs from the server. When the server reaches its limit of concurrent connections, it cannot respond to legitimate requests. An HTTP/S flood may consist of either GET (images and scripts), POST (files and forms) or combined GET and POST requests.
ICMP Flood Volumetric Attack	An Internet Control Message Protocol (ICMP) flood DDoS attack, also known as a Ping flood attack, is a common Denial-of-Service (DoS) attack in which an attacker attempts to overwhelm a targeted device with ICMP echo-requests (pings).
IP/ICMP Fragmentation Volumetric Attack	An Internet Protocol (IP)/Internet Control Message Protocol (ICMP) fragmentation DDoS attack is a common form of volumetric denial of service (DoS) attack. In such an attack, datagram fragmentation mechanisms are used to overwhelm the network. IP fragmentation occurs when IP datagrams are broken apart into small packets, then transmitted across a network, and finally reassembled into the original datagram as part of normal communications.
IPSec Flood/IKE/ISAKMP Volumetric Attack	An Internet Protocol Security (IPSec) Internet Key Exchange (IKE) flood is a layer 5 DDoS attack that tries to consume VPN server resources in order to flood the VPN. This DDoS attack normally sends rapid IPSec IKE requests to a VPN server within the network, making the VPN server respond back with IKE traffic. The resource consumption takes place on the victim VPN server. Also known as an Internet Security Association and Key Management Protocol (ISAKMP) flood.
Large Payload POST Requests Attack	Large Payload Post DDoS attacks occur when web services use a DOM parser to create an in-memory representation of the SOAP message. During this process, the SOAP message size can double, or in some cases, grow as much as 30 times larger. The resulting large documents result in memory exhaustion.
Latency	The measurement of time that it takes for some data to get to its destination across the network. Typically measured as a round trip delay - the time taken for information to get to its destination and back again. Latency is usually measured in milliseconds (ms).
Low and Slow Attack	Low and Slow is a DDoS attack that takes place over the course of hours, making legitimate requests of the network, but then delaying the response. The sheer volume of requests and slow responses limit availability for legitimate connections.
Mimicked User Browsing Attack	Mimicked User Browsing DDoS attacks use bots to imitate a legitimate user's browsing patterns. These bots generate spikes in traffic posing as high visitor traffic, clogging the IP network connection and preventing legitimate traffic from getting through.
Network Interface	A software or hardware interface between two pieces of equipment or protocol layers in a computer network.

Network Operations Center ("NOC")	Network Operations Center ("NOC") collectively refers to Zayo's locations and teams responsible for maintaining, controlling, and responding to network events.
Protection	A mechanism to automatically recover from failures within complex systems including equipment failure, fiber cuts, and systemic or logical errors.
Protocol	The rules for the transmission of data which must be followed if communication is to be effected; the complete interaction of all possible series of messages across an interface.
Provisioning	The act of acquiring a service from the submission of the requirement through the activation of service. Provisioning includes all associated transmission, wiring, and equipment.
Reflection Amplification Attack	In a reflection amplification attack, the attacker magnifies or amplifies the amount of malicious traffic they generate, overwhelming the target and occluding the circuit so good traffic is blocked, all while obscuring the sources of the attack.
Security Operations Center ("SOC")	Security Operations Center ("SOC") is a place and team that responds to security related network issues and events (ex. DDoS).
Slowloris Attack	Slowloris is a type of application layer DDoS attack which uses partial HTTP requests to take down a web server using minimal bandwidth. Slowloris tries to keep many connections to the target web server open and hold them open as long as possible, overwhelming and slowing down the target. Slowloris has minimal impact on services and ports unrelated to the attack.
Slow Post Attack	Slow Post DDoS attacks transmit HTTP requests that target web servers, sending data extremely slowly, but not slowly enough for the server to time out. The bandwidth required to launch a slow post attack is minimal, so the attack can be launched from a single computer. Because the server keeps the connection open in anticipation of additional data, genuine users are prevented from accessing the server.
Slow Read Attack	In a slow-read DDoS attack, the attacker sends an HTTP request to a server, but then reads the response from the server at a very slow speed. Reading the response slowly accomplishes two things: the server cannot time out from an idle state, and legitimate traffic is blocked from the server.
SSL TCP State Exhaustion Attack	A secure sockets layer (SSL) DDoS attack targets the SSL handshake protocol either by sending worthless data to the SSL server which will result in connection issues for legitimate users or by abusing the SSL handshake protocol itself.
SYN Flood TCP State Exhaustion Attack	Transmission Control Protocol (TCP) synchronized (SYN) flood is a type of DDoS attack that exploits part of the normal TCP three-way handshake to consume resources on the targeted server and render it unresponsive. With SYN flood DDoS, the attacker sends TCP connection requests faster than the targeted machine can process them, causing network saturation.

UDP Flood Volumetric Attack	A User Datagram Protocol flood attack is a type of Denial of Service (DoS) attack in which the attacker overwhelms random ports on the targeted host with IP packets containing UDP datagrams. The receiving host checks for applications associated with these datagrams and—finding none—sends back a "Destination Unreachable" packet. As more and more UDP packets are received and answered, the system becomes overwhelmed and unresponsive to other clients.

Note: Attack definitions were drawn from various sources.