



OUR FIBER FUELS GLOBAL INNOVATION



DDoS PROTECTION: PORTAL GUIDE

2021



Visit the Portal

<https://ddos-portal.zayo.com>

Table of Contents

Zayo's DDoS Protection: Portal Guide Overview	Page 3
Zayo Support	Page 4
Solution Summary	Page 4
<ul style="list-style-type: none">• Subscription options• Mitigation types• System operation• Access to Portal: Based on Protection Plan	
Portal Navigation	Page 8
<ul style="list-style-type: none">• Customer Login Process• Status• Alerts• Traffic• Mitigation• Administration	
Portal Use - Advanced Capabilities	Page 15
<ul style="list-style-type: none">• Detection alert• Running a mitigation• Adjust live mitigation• Mitigating to analyze	
Reporting	Page 27
<ul style="list-style-type: none">• Incident report• Summary report	

Zayo's DDoS Protection: Portal Guide Overview

Welcome to Zayo's DDoS Protection Service and congratulations on taking an important step towards a comprehensive cyber security plan. Our goal is to provide the best in DDoS detection and mitigation solutions.

Zayo's DDoS Protection Portal provides:

- Insights with traffic analysis
- Enhanced reporting
- Ability to manage your DDoS Protection Service

This guide covers:

1. Zayo's Security Operations Center Support

2. An overview of Zayo's DDoS Protection Service and Portal Support

- Access to Portal based on Protection Plan
- Subscription options
- Mitigation types
- System operation
- Customer login Process

3. Portal Navigation

- Status
- Alerts
- Traffic
- Mitigation
- Administration
- Quick Tips/Tricks
- Adding & managing users

4. Portal Use - Advanced Capabilities

- Detection alert
- Running a mitigation
- Adjust live mitigation
- Mitigating to analyze

5. Reporting

- Incident report
- Summary report

Zayo Security Operations Center Support

Zayo's Security Operations Center (SOC) team provides 24/7/365 support to DDoS Protection customer inquiries. Contact the SOC for mitigation, configuration and system operation including:

- Activating or deactivating automatic mitigation
- Adding or removing IP addresses
- Changing alert destinations
- Changing report destinations
- Reviewing and adjusting alert thresholds
- Interacting on mitigations
- Discussing operation of Zayo's DDoS Protection

The SOC is part of a global Zayo support capability that includes Zayo's Network Operation Centers (NOCs)

Contact the SOC:

1 866-236-2824, select DDoS Mitigation option

security.support@zayo.com

Contact the NOC:

1 866-236-2824

zayoncc@zayo.com

<https://www.zayo.com/contact/technical-support>

Escalate situations using Zayo Tranzact

(Log in, select My Zayo Team, select Escalation List)

Solution Summary

Below is a summary of Zayo's DDoS Protection Service, including subscription plan options, the types of DDoS attack mitigation options available to you, how our DDoS Protection operates, and finally the depth of Portal access for each subscription plan available.

Subscription options

Zayo offers three subscription plans: Basic, Standard and Advanced. All three offer cloud-based DDoS Protection on a monthly subscription basis with proactive monitoring, incident notification and incident reporting services.

The plans differ in terms of your ability to schedule reporting, how DDoS mitigation is initiated and charged, and your access to the DDoS Portal.

The table below summarizes the DDoS Protection Plans and what they offer.

DDoS Protection Plans	Basic Cover your bases with always-on monitoring	Standard All-around protection with notifications	Advanced Immediate protection for stress-free security
Cloud-Based	✓	✓	✓
Monthly Subscription	✓	✓	✓
Proactive Monitoring	✓	✓	✓
Incident Notification	✓	✓	✓
Incident Reporting	✓	✓	✓
Scheduled Reporting	No	✓	✓
Portal Access	No	✓	✓
Mitigation Type	Authorized, Per-incident	Authorized Mitigation	Authorized, Automatic and Self Mitigation
Scrubbing Cost	Per-incident Fee	Unlimited / Included	Unlimited / Included

Mitigation Types

Below we have outlined how mitigation is initiated and the steps of each mitigation type.

Authorized (Requested) Mitigation:

- Available in the Basic, Standard & Advanced protection plans.
- A traffic anomaly is detected by routers at Zayo’s peering edge.
- A system generated notification is sent via email to designated contact (s) inside the customer’s organization.
- Upon receipt of the alert, the customer contacts the Zayo Security Operations Center to request a mitigation. Mitigation will commence within 15 minutes of the receipt of authorization to mitigate.
- The scrubbing centers filter attack traffic from normal traffic and forward only legitimate traffic to the customer.
- The customer will receive a report of the situation following mitigation of the incident. This report will be sent to the designated contact(s).

Automatic Mitigation:

- Available only in the Advanced protection plan.
- A traffic anomaly is detected by routers at Zayo's peering edge.
- The Zayo's DDoS Protection system is able to identify a DDoS attack with precision and immediately initiate the mitigation process.
- The scrubbing centers filter attack traffic from normal traffic and forward only legitimate traffic to the customer.
- The customer will receive an automatically generated alert upon detection of the anomaly and will receive a report of the situation following mitigation of the incident. This report will be sent to the designated contact (s).

Self Mitigation:

- Available only in the Advanced protection plan. This option provides a customer with the capability to take full control of a mitigation.
- In any situation a customer can activate, manage and terminate mitigation.
- Customers have the ability to adjust, enable or disable individual traffic components of the entire mitigation
- Customers that have sophisticated security staff and want to run mitigations themselves find this capability useful.

Please note that the Basic subscription plan offers only an incident-by-incident mitigation.

System operation

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 identified for protection.

The monitoring process triggers the identification of potential DDoS attacks targeting the IP addresses identified for protection. This triggering mechanism is always on and continually operates in the protection of customer network traffic. The initial indicator of a DDoS attack is the abnormal flow of traffic at the Network Layer (Layer 3). The primary measure of this is the Host Detection Threshold defined in the contractual arrangement for DDoS Protection. As traffic exceeds this barrier at a level two times the defined level, an alert is issued and sent to all addresses specified by the subscriber at the time of system initiation. The alert process is automated. All alerts are system generated.

A sample Alert notification is shown below:

[Sightline] Host Detection alert #112576 incoming to 208.185.166.178 Peakflow SP x

Sightline ncc@zayo.com via email-od.com 4:51 PM (5 minutes ago)
to Account Email Address

DoS host detection alert started at (Date and Time) UTC.

URL: https://ddos-portal.zayo.com/page?id=host_alert&alert_id=112576&customer=sp1dfw2

Host: e.g. 208.185.166.178

Signatures: IP Fragmentation

Impact: 74.7 Gbps/7.4 Mpps

Importance: High

Managed Objects: e.g. MCS_Zayo_Canada_Lab_DDOS_000222_ZYO-Test

Managed Cyber Security--DDoS Protection

Phone Contact: 1 866-236-2824, Option 1 and then Option 2 for DDoS Mitigation

Email Contact: security.support@zayo.com

The process, up to the point an alert is issued, is the same for all of Zayo's DDoS Protection subscription plans. Monitoring, Attack Identification and Alert (Incident Notification) processes are proactively and continually applied to all subscribers of the system.

Upon receipt of an alert, Basic Plan subscribers and Standard Plan subscribers can review the situation described in the alert and determine whether to request a mitigation. We call this "Authorized Mitigation." A mitigation is initiated by contacting the Zayo Security Operations Center. The Zayo support team will initiate the mitigation within fifteen (15) minutes of the customer authorization.

Access to Portal Based on Protection Plan

Subscriptions vary based on billing options, mitigation initiation processes and level of access to Zayo's DDoS Protection portal.

Basic Protection Plan:

- No portal access
- Benefit from proactive monitoring and receive system generated alert notifications when a DDoS attack is detected
- Mitigation will begin upon authorization from the customer, on a per-incident basis.
- To initiate mitigation call the Security Operations Center (SOC). Mitigation will commence within 15 minutes after contacting the SOC
- Charges include a monthly subscription fee plus a per mitigation fee that is based on the amount of clean traffic that is delivered through the mitigation.

Standard Protection Plan:

- Read access to the portal
- Benefit from proactive monitoring and receive system generated alert notifications when a DDoS attack is detected
- Mitigation will begin upon authorization from the customer.
- To initiate mitigation call the Security Operations Center (SOC). Mitigation will commence within 15 minutes after contacting the SOC
- All attacks are mitigated in the single monthly subscription amount. Unlimited mitigations are provided
- View ongoing and historical mitigations

Advanced Protection Plan:

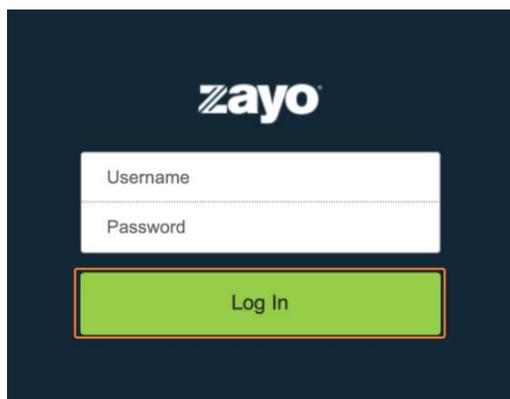
- Most extensive access to the portal
- Benefit from proactive monitoring and receive system generated alert notifications when a DDoS attack is detected
- Access automatic mitigation to eliminate response time, authorized mitigation or perform self mitigation of DDoS attacks on an ad hoc basis
- All attacks are mitigated in the single monthly subscription amount. Unlimited mitigations are provided
- View ongoing and historical mitigations

Portal Navigation

Customer login process

Open the following URL with a web browser <https://ddos-portal.zayo.com/>

Enter your username and **temporary password** and **click 'Log In'**



The image shows a dark blue login portal for Zayo. At the top center is the Zayo logo in white. Below the logo is a white rectangular form containing two input fields: 'Username' and 'Password'. Below the form is a green rectangular button with the text 'Log In' in white. The button has a thin orange border.

You are now at the default landing page



First, let's update your password.

- **Navigate to 'administration'**
- Select **user accounts** and **click username**
- Enter the **old password** and the **new password** twice, then click **'Save'**

The screenshot shows the Zayo Administration page. The 'User Accounts' table is visible, with the 'testadmin' user selected. The 'Account Configuration' form is open, showing fields for Username, Real Name, Email Address, Password Change (Old Password, New Password, Confirm New Password), and User Interface (Timezone, UI Menu). The 'Save' button is highlighted with a red box.

You should see the following banner noting your update

- Optional but recommended: log out and back in to verify new password



Status

The Status tab is an overview snapshot of your service

- View overall network traffic, current ongoing alerts and alerts summary

zDDoS_Test-DDOS_123456_ZYO Security Status | 1 Status Message: EXPAND

zDDoS_Test-DDOS_123456_ZYO Summary

zDDoS_Test-DDOS_123456_ZYO Summary Jan 2021

View more

Alerts

Severity Level	Ongoing	Recent	Last 24 Hours
High	0	4	0
Medium	0	0	0
Low	0	0	0
Total	0	4	0

Ongoing Alerts | Ongoing Mitigations

No results returned for your query

Alerts

The Alerts tab is a log of all alerts with classification and the importance ratings for all alerts and ongoing alerts

All Alerts | All Alerts | Ongoing

4 results (0.44 seconds)

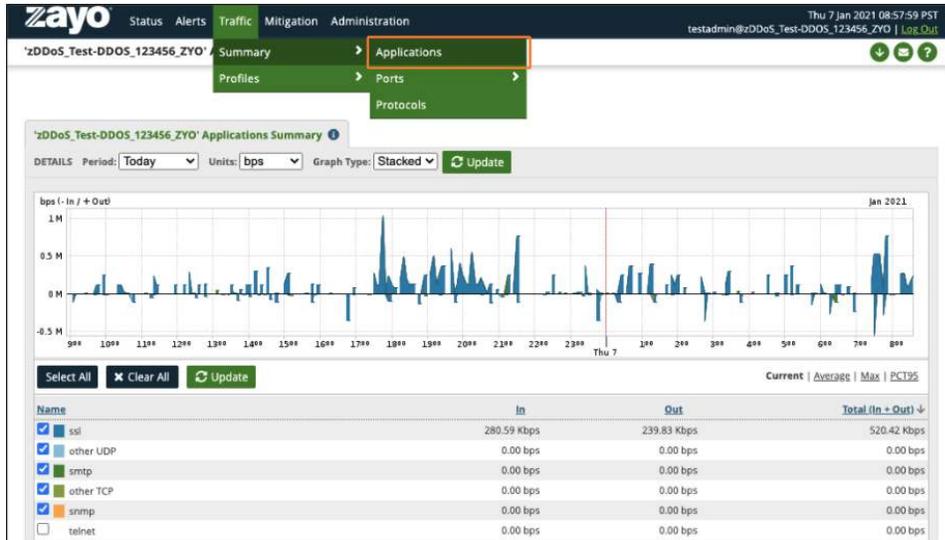
ID	Max Impact	Importance	Alert	Start Time	Classification & Annotations
742709	High Fast Flood 11,988.0% of 50 Mbps 6.0 Gbps, 1.6 Mpps	High Fast Flood	DoS Host Alert Incoming Host Alert to 64.124.0.0 using zDDoS_Test-DDOS_123456_ZYO Misuse Types: Total Traffic, UDP, NTP Amplification	Nov 8 08:43 2020 - 08:50 (0:07)	Possible Attack System began auto-mitigation (by auto-mitigation)
684511	High Fast Flood 2,150.0% of 20 Kpps 483.3 Mbps, 433.6 Kpps	High Fast Flood	DoS Host Alert Incoming Host Alert to 208.185.166.178 using zDDoS_Test-DDOS_123456_ZYO Misuse Types: TCP SYN, Total Traffic	Aug 27 14:30 2020 - 14:43 (0:14)	Possible Attack System began auto-mitigation (by auto-mitigation)
684239	High Fast Flood 2,452.0% of 20 Kpps 551.3 Mbps, 493.8 Kpps	High Fast Flood	DoS Host Alert Incoming Host Alert to 208.185.166.178 using zDDoS_Test-DDOS_123456_ZYO Misuse Types: TCP SYN, Total Traffic	Aug 27 11:42 2020 - 12:50 (1:08)	Possible Attack System began auto-mitigation (by auto-mitigation)
608849	High Fast Flood 2,142.0% of 20 Kpps 479.8 Mbps, 428.4 Kpps	High Fast Flood	DoS Host Alert Incoming Host Alert to 208.185.166.178 using zDDoS_Test-DDOS_123456_ZYO Misuse Types: TCP SYN, Total Traffic	Jul 7 13:44 2020 - 13:57 (0:13)	Possible Attack System began auto-mitigation (by auto-mitigation)

Page generation took 0.96 seconds (Details)

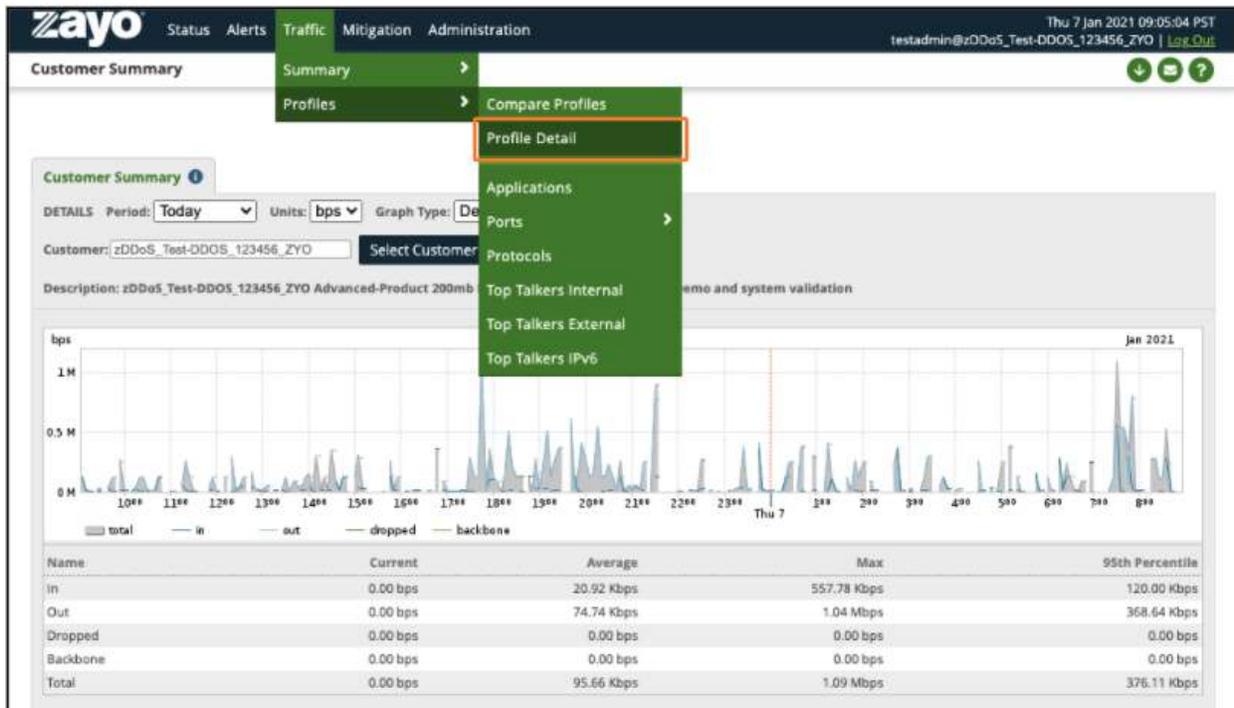
Traffic

The traffic tab displays a summary of network traffic to your protected IP ranges.

- Navigate to **'Traffic' > 'Summary' > 'Applications'** for a view into your traffic per application



Navigate to **'Traffic' > 'Profiles' > 'Profile Detail'** to view traffic per port, by "talkers" and by protocol.



Mitigation

The Mitigation tab is a log of mitigations occurring on your service

- **Ongoing** (current mitigations)
- **Recent** (recent historical mitigations)
- **Threat Management** (ongoing and recent historical mitigations)

The screenshot shows the Zayo Mitigation tab interface. The top navigation bar includes 'Status', 'Alerts', 'Traffic', 'Mitigation', and 'Administration'. The 'Mitigation' tab is active, and the 'Recent' sub-tab is selected. A search bar is visible with the text 'arch' and a 'Wizard' button. Below the search bar, a table lists recent mitigations with columns for Graph, Name, Protection Prefixes, Duration, Start Time, User, Type, and Annotations. A 'Mitigation Search Wizard' dialog box is overlaid on the table, allowing users to filter results by Status (Ongoing or Recent), Search Limit, Items per Page, IP Version (IPv4, IPv6), and Mitigation Type (TMS, Blackhole, Learning). The dialog box has 'Cancel' and 'Search' buttons.

Administration

The administration tab allows you to manage your profile settings and users. Update password, timezone, or email.

The screenshot shows the Zayo Administration tab interface. The top navigation bar includes 'Status', 'Alerts', 'Traffic', 'Mitigation', and 'Administration'. The 'Administration' tab is active, and the 'Edit My Account' sub-tab is selected. The form is divided into three sections: 'Account Configuration', 'Password Change', and 'User Interface'. The 'Account Configuration' section includes fields for Username (testadmin), Real Name (Test Admin Account zDDoS_Test), and Email Address. The 'Password Change' section includes fields for Old Password for testadmin, New Password, and Confirm New Password. The 'User Interface' section includes a dropdown for Timezone (America/Los_Angeles [UTC -08:00 PST]) and a field for UI Menu (Default). The form has 'Cancel' and 'Save' buttons.

User Accounts: Manage other users if you are an admin

Username	Real Name	Capability Level	Email	Device	UI Menu	Status
<input type="checkbox"/> danny.cho	Danny Cho	ZYO user		global	Default	
<input type="checkbox"/> jilleun	Jilleun Eglin	ZYO admin	jilleun.eglin@zayo.com	global	Default	
<input type="checkbox"/> jwhealton	John Whealton	zDDoS_Test-DDoS_123456_ZYO user	john.whealton@zayo.com	global	Default	
<input type="checkbox"/> MattWaldo@allstream.com	Matt Waldo	zDDoS_Test-DDoS_123456_ZYO user	Matt.Waldo@allstream.com	global	Default	
<input type="checkbox"/> pcutinelli	Peter Cutinelli	zDDoS_Test-DDoS_123456_ZYO admin	peter.cutinelli@zayo.com	global	Default	
<input type="checkbox"/> testadmin	Test Admin Account zDDoS_Test	zDDoS_Test-DDoS_123456_ZYO admin		global	Default	
<input type="checkbox"/> testuser	Test User Account zDDoS_Test	zDDoS_Test-DDoS_123456_ZYO user		global	Default	

Login Records: Login history

Username	Last Login Location	Last Login Time	Login Failures
danny.cho	216.239.225.7	2:07 Mar 27 2020	0
jilleun	205.209.41.209	4:28 May 3 2019	0
jwhealton	74.209.254.12	07:26 Aug 13 2019	0
Matt.Waldo@allstream.com	None	19:10 May 27 2020	0
pcutinelli	None	16:00 Dec 31 1969	0
testadmin	73.22.206.58	08:28 Jan 7 2021	0
testuser	74.209.254.12	13:25 Feb 6 2019	0

Creating Additional Users

To add additional users select 'Administration' > 'User Accounts' > Click 'Add Account'

Username	Real Name	Capability Level	Email	Device	UI Menu	Status
<input type="checkbox"/> danny.cho	Danny Cho	ZYO user		global	Default	
<input type="checkbox"/> jilleun	Jilleun Eglin	ZYO admin	jilleun.eglin@zayo.com	global	Default	
<input type="checkbox"/> jwhealton	John Whealton	zDDoS_Test-DDoS_123456_ZYO user	john.whealton@zayo.com	global	Default	
<input type="checkbox"/> MattWaldo@allstream.com	Matt Waldo	zDDoS_Test-DDoS_123456_ZYO user	Matt.Waldo@allstream.com	global	Default	
<input type="checkbox"/> pcutinelli	Peter Cutinelli	zDDoS_Test-DDoS_123456_ZYO admin	peter.cutinelli@zayo.com	global	Default	
<input type="checkbox"/> testadmin	Test Admin Account zDDoS_Test	zDDoS_Test-DDoS_123456_ZYO admin		global	Default	
<input type="checkbox"/> testuser	Test User Account zDDoS_Test	zDDoS_Test-DDoS_123456_ZYO user		global	Default	

Administrator can create additional Admin or User accounts, User is view-only
 Note the account group is pre-selected:

1. Enter **Username**
2. Enter **Real Name**
3. Enter **Email Address**
4. Enter **Password** and **Confirmation password**
5. Choose '**Administrator**' or '**User**' depending on requested access
6. Select '**Timezone**'
7. Click '**Save**'

The screenshot shows the 'Add User Account' form in the Zayo administration interface. The form is titled 'Add User Account' and includes sections for Account Configuration, Password, Storage Appliance, Authorization Settings, and User Interface. The 'Timezone' dropdown menu is highlighted with an orange box and set to 'Default'. The 'Save' button is also highlighted with an orange box.

The new account should now display in the list:

The screenshot shows the 'User Accounts' list in the Zayo administration interface. The list shows a table of user accounts with columns for Username, Real Name, Account Group, Capability Level, Email, Device, UI Menu, and Status. The first row, 'testuser', is highlighted with an orange box.

Username	Real Name	Account Group	Capability Level	Email	Device	UI Menu	Status
testuser	Test User Account zDDoS_Test	zDDoS_Test-DDoS_123456_ZYO	user		global	Default	
testadmin	Test Admin Account zDDoS_Test	zDDoS_Test-DDoS_123456_ZYO	admin		global	Default	
pcutinelli	Peter Cutinelli	zDDoS_Test-DDoS_123456_ZYO	admin	peter.cutinelli@zayo.com	global	Default	
Matt.Waldo@allstream.com	Matt Waldo	zDDoS_Test-DDoS_123456_ZYO	user	Matt.Waldo@allstream.com	global	Default	
lwheatlon	John Wheatlon	zDDoS_Test-DDoS_123456_ZYO	user	john.wheatlon@zayo.com	global	Default	
jilleun	Jilleun Eglin	zDDoS_Test-DDoS_123456_ZYO	admin	jilleun.eglin@zayo.com	global	Default	
danny.cho	Danny Cho	zDDoS_Test-DDoS_123456_ZYO	user		global	Default	

Select the checkbox next to the new user and click 'View As'

- You should now see the default landing page as the new user account

<input type="checkbox"/>	testadmin	Test Admin Account zDDoS_Test	zDDoS_Test-DDoS_123456_ZYO	admin	global	Default
<input checked="" type="checkbox"/>	testuser	Test User Account zDDoS_Test	zDDoS_Test-DDoS_123456_ZYO	user	global	Default
<input type="button" value="Delete"/> <input type="button" value="Disable"/> <input type="button" value="Enable"/> <input type="button" value="View As"/>						

Portal Use - Advanced Capabilities

Detection Alert

If you are using self mitigation, the following steps will walk you through reviewing a detection alert and how to mitigate it.

To review the details of the attack from the detection alert, there are two ways to view details.

- Email alert received: to view more details on the alert **click URL link**

[Sightline] Host Detection alert #112576 incoming to 208.185.166.178 Peakflow SP x
Sightline ncc@zayo.com via email-od.com 4:51 PM (5 minutes ago)
to Account Email Address

DoS host detection alert started at (Date and Time) UTC.

URL: https://ddos-portal.zayo.com/page?id=host_alert&alert_id=112576&customer=sp1dfw2

Host: e.g. 208.185.166.178
Signatures: IP Fragmentation
Impact: 74.7 Gbps/7.4 Mpps
Importance: High
Managed Objects: e.g. MCS_Zayo_Canada_Lab_DDOS_000222_ZYO-Test

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

- Login to the portal and you will see the alert displayed on the dashboard, **click alert link** (in this example the alert link is **742709**)

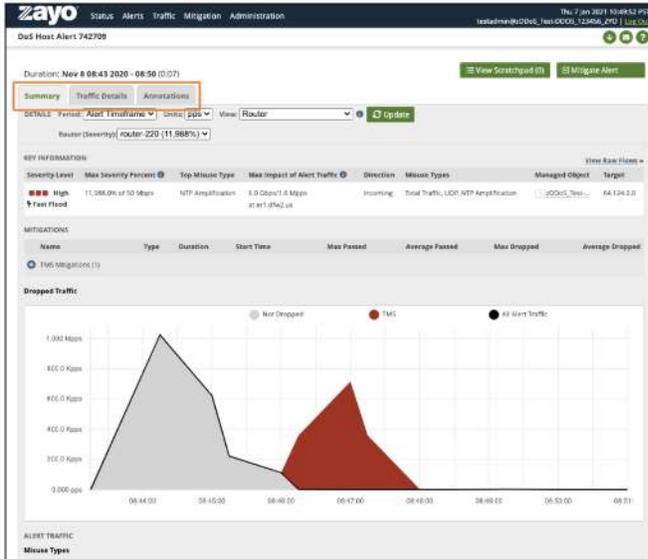
The screenshot shows the Zayo portal dashboard. At the top, there is a navigation bar with 'zayo' logo and menu items: Status, Alerts, Traffic, Mitigation, Administration. The user is logged in as 'testadmin@zDDoS_Test-DDoS_123456_ZYO'. The main content area is titled 'zDDoS_Test-DDoS_123456_ZYO Security Status'. On the left, there is a 'zDDoS_Test-DDoS_123456_ZYO Summary' section with a line graph showing traffic over time. On the right, there is an 'Alerts' table with the following data:

Severity Level	Ongoing	Recent	Last 24 Hours
High	0	0	0
Medium	0	0	0
Low	0	0	0
Total	0	0	0

At the bottom left, there are two buttons: 'Ongoing Alerts' and 'Ongoing Mitigations'.

ID ↓	Max Impact	Importance ⓘ	Alert	Start Time	Classification & Annotations
742709	High	Fast Flood	DoS Host Alert Incoming Host Alert to 64.124.0.0 using zDDoS_Test-DDoS_123456_ZYO Misuse Types: Total Traffic, UDP, NTP Amplification	Nov 8 08:43 2020 - 08:50 (0:07)	Possible Attack System began auto-mitigation (by auto-mitigation)

3. You should now see the alert dashboard, feel free to navigate to different tabs and learn about the alert.



Running a Mitigation

If you have determined the traffic to be an attack, the following procedure walks you through a basic mitigation

Click 'Mitigate Alert' and choose 'Threat Management' from the drop down

The screenshot shows the Zayo alert dashboard for DoS Host Alert 742709. The duration is Nov 8 08:43 2020 - 08:50 (0:07). The dashboard includes a summary tab, traffic details, and annotations. A key information table shows the severity level as High, with a maximum severity percent of 11,988.0% of 50 Mbps. The top misuse type is NTP Amplification, with a maximum impact of 6.0 Gbps/1.6 Mpps. The direction is Incoming, and the misuse types are Total Traffic, UDP, and NTP Amplification. The managed object is zDDoS_Test-... and the target is 64.124.0.0. The 'Mitigate Alert' button is highlighted, and the 'Threat Management' dropdown menu is open, showing options for 'Threat Management' and 'Generate Filter'.

Enter notes in the description (optional) and click 'Protect' on the left.

zayo Status Alerts Traffic Mitigation Administration Thu 7 Jan 2021 10:54:51 PST testadmin@zDDoS_Test-DDoS_123456_ZYO | Log Out

Create TMS Mitigation

Mitigation

- Protect
- TMS Appliances
- Black/White Lists
- IP Based Filter Lists
- Payload
- Countermeasures
- Shaping
- Advanced

Name: DoS Alert 742709

Source Alert ID (Optional): 742709

Description: [Empty]

Internet Protocol Version: IPv4

Mode

Mode: Active Inactive

Inactive mitigations are applied to attack traffic but do not drop any traffic.

Learning Dataset

Learning Dataset: None

CDN Proxy

Enable CDN Proxy Support:

Cancel Save and Start Mitigation Save and View Listing

The affected IP addresses will be listed in the Protection Prefixes section

- Click 'Save and Start Mitigation'

zayo Status Alerts Traffic Mitigation Administration Thu 7 Jan 2021 10:54:51 PST testadmin@zDDoS_Test-DDoS_123456_ZYO | Log Out

Create TMS Mitigation

Mitigation

- Protect
- TMS Appliances
- Black/White Lists
- IP Based Filter Lists
- Payload
- Countermeasures
- Shaping
- Advanced

Managed Object: zDDoS_Test-DDoS_123456_ZYO Select Managed Object

Protection Prefixes: 64.124.0.0/32

Example: 203.0.113.16/30, 198.51.100.0/24

Note: All must fall within managed object CIDRs

Diversion Prefixes: Default Less Specific Custom

Divert the same prefixes to the TMS as the prefixes that the mitigation protects.

Timeout: Example: '600' (Default is no timeout) [Empty] seconds

Flow Specification Filters

Protocol Numbers: Example: 1-6, 17 [Empty]

Source Prefix: Example: 203.0.113.16/30 [Empty]

Match any specified source ports AND any specified destination ports

Match any specified ports

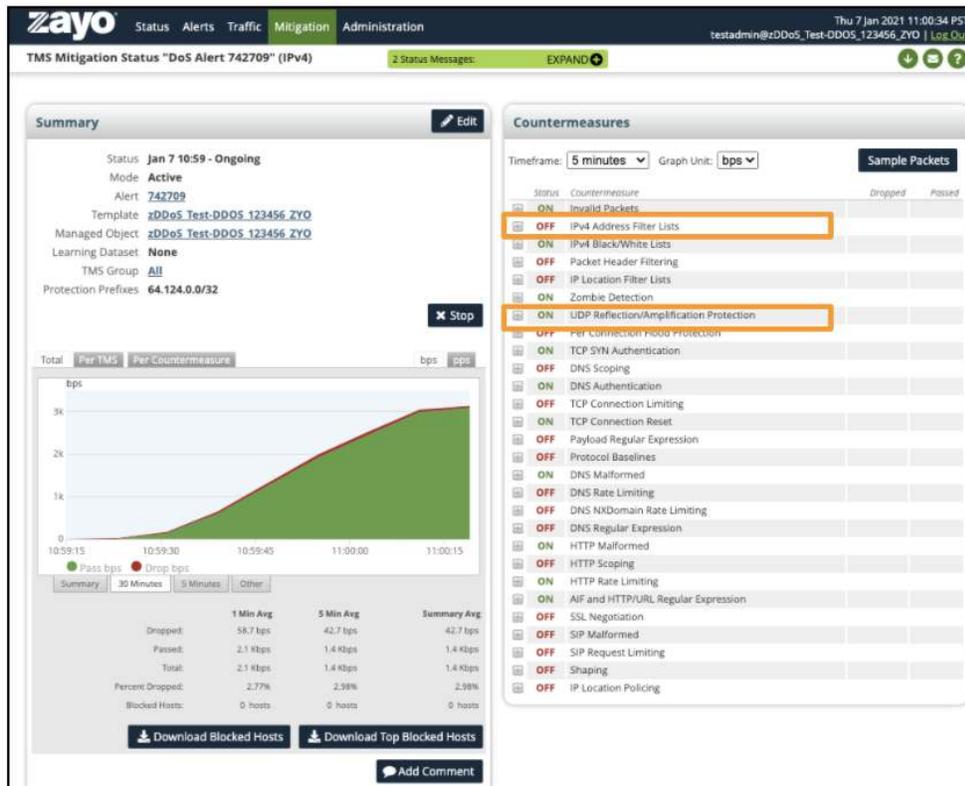
Source Ports: Example: 1-10, 80 [Empty]

Destination Ports: Example: 1-10, 80 [Empty]

Cancel Save and Start Mitigation Save and View Listing

This will drop you into the mitigation summary.

- In this case the TCP SYN flood is registering under Zombie Detection and Invalid Packets.



Adjust Live Mitigation

This next subsection is an example of misclassified traffic and how to adjust a live mitigation to compensate

Situation: Test traffic is not very diverse or high volume and was misclassified by the system as part of the attack.

- To work around this issue, add a white-list entry to pass the test traffic.
- On the right, **click the plus sign** next to IPv4 Black/White Lists
 - Example uses a simple inline filter of "pass src 74.209.211.200"
- **Click Save**

Countermeasures

Timeframe: 1 minute | Graph Unit: bps | Sample Packets

Status	Countermeasure	Dropped	Passed
ON	Invalid Packets	462.8 Mbps	413.2 Kpps
OFF	IPv4 Address Filter Lists		
ON	IPv4 Black/White Lists		

Example:
pass port 80 and src 192.168.6.0/24

Inline Filters:

Open FCAP Wizard

IPv4 Black/White Filter Lists

Select Filter List

Blacklist Fingerprints

Select Fingerprint

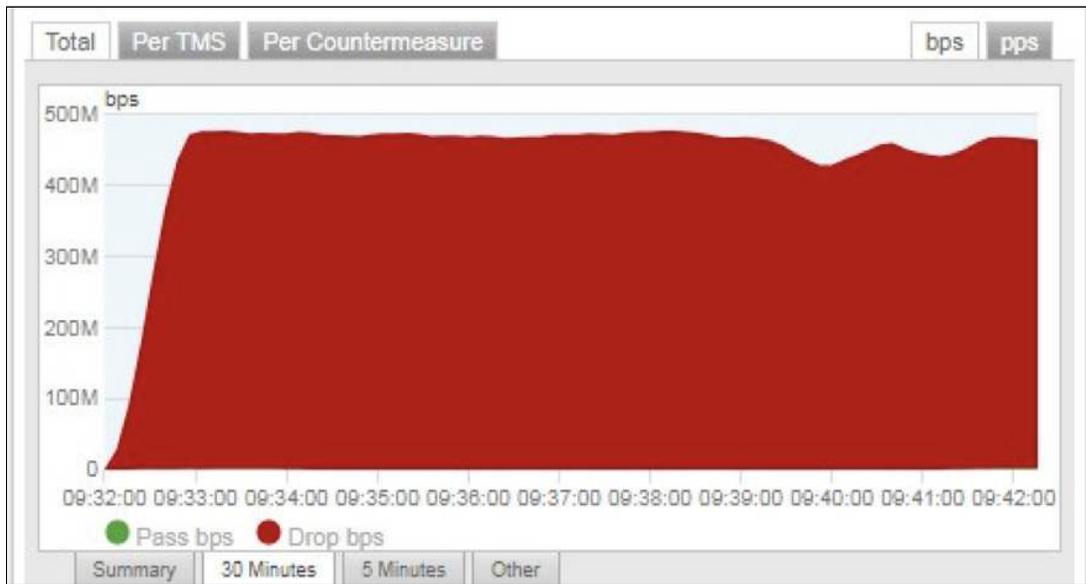
Blacklist Sources

Save

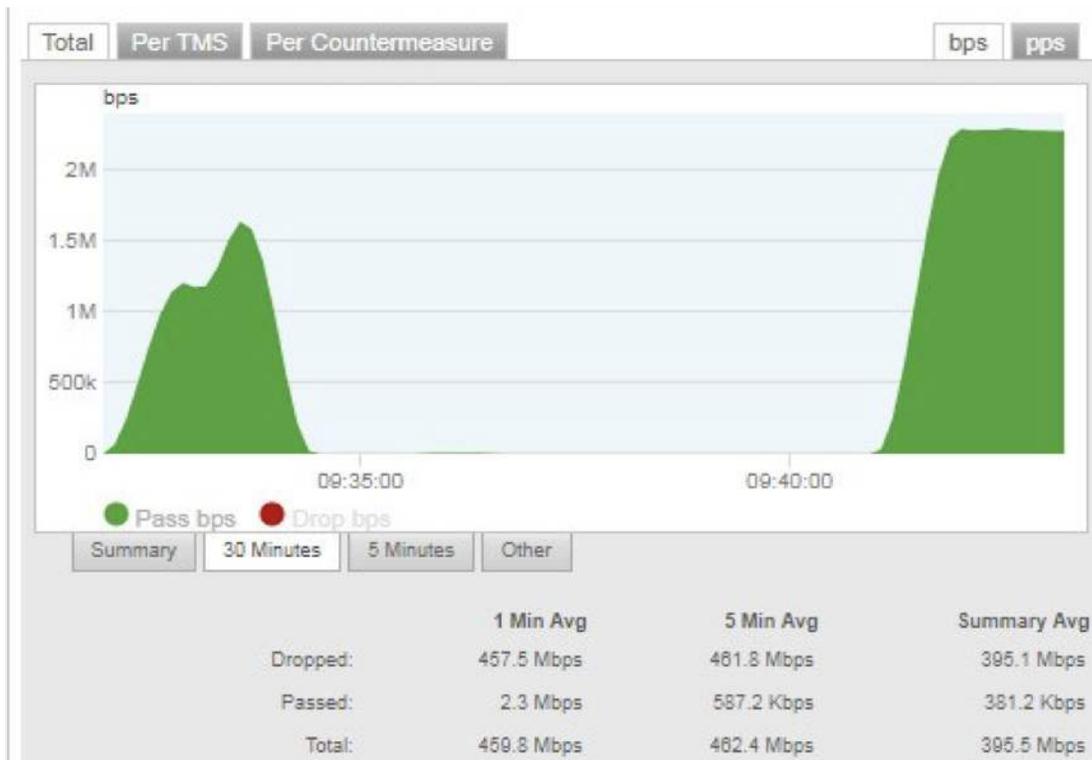
Now All traffic from that source automatically passes

Status	Countermeasure	Dropped	Passed
ON	Invalid Packets	450.7 Mbps	402.4 Kpps
OFF	IPv4 Address Filter Lists		
ON	IPv4 Black/White Lists		790.2 Kbps 1.4 Kpps
OFF	Packet Header Filtering		
OFF	IP Location Filter Lists		
ON	Zombie Detection		
	UDP Reflection/Amplification		

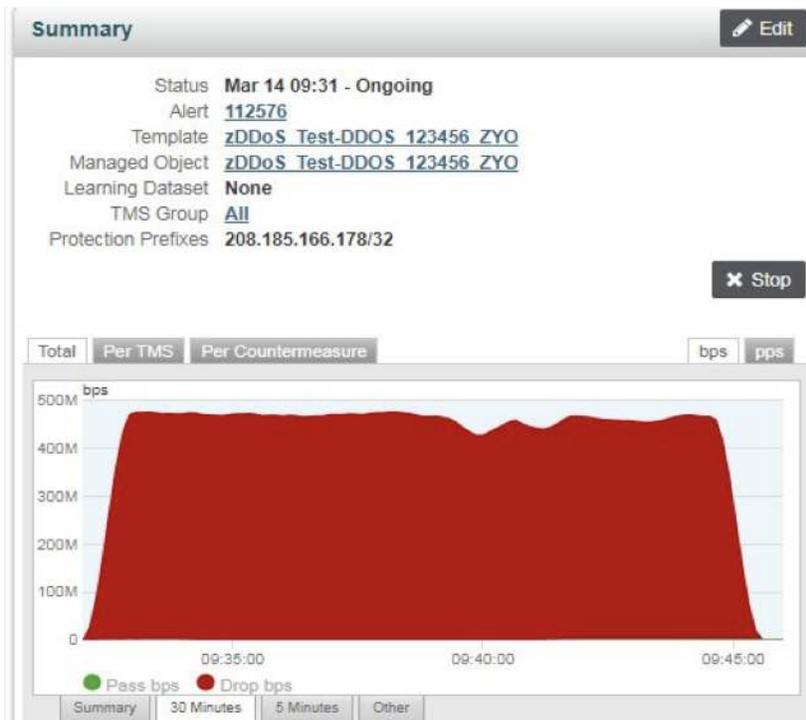
You can select/deselect pass or drop traffic on the graph to see them individually



This is useful in this case as the volume of clean traffic compared to attack are at very different scales (2.3mb pass to 457.5mb drop)

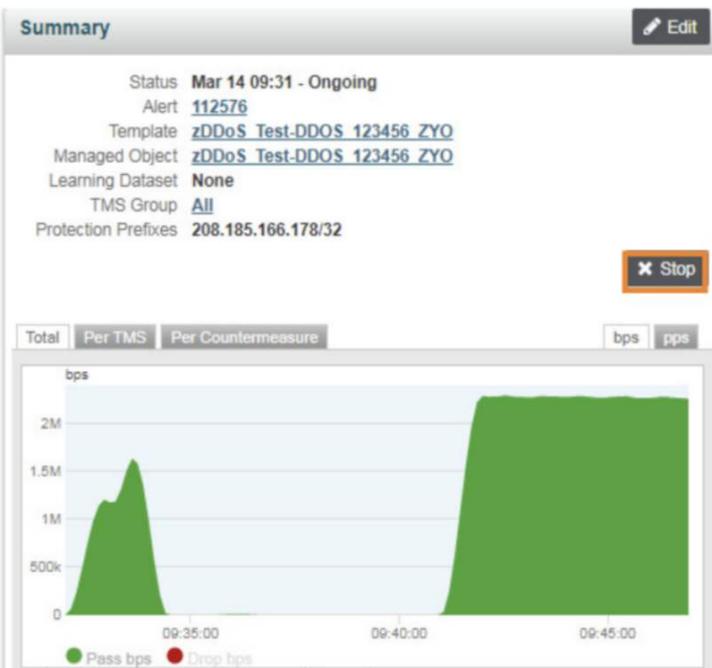


With the attack mitigated, the attackers stop sending the SYN Flood and the traffic levels drop to normal



You can now end the mitigation by clicking '**Stop**' and return traffic to its normal path or leave it running for a few hours in the case of recurring attacks. Subsequent attacks are matched to existing alerts for up to 72 hours so it is not necessary to keep them running.

- Zayo will close mitigations that no longer have active attacks after 24 hours.



After the mitigation or attack ends, Zayo will send another email.

[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 Contact: 1 866-236-2824, Option 1 and then Option 2 for DDoS Mitigation

Email Contact: security.support@zayo.com

Mitigating to Analyze

The following will walk through redirecting an IP that you suspect is receiving malicious traffic

Login to portal > Navigate to 'Mitigation' > 'Threat Management' > Select 'Add Mitigation' > Choose 'IPv4'

The screenshot displays the Zayo TMS Mitigations interface. At the top, there are navigation tabs for Status, Alerts, Traffic, Mitigation (selected), and Administration. The user is logged in as testadmin@zDDoS_Test-DDoS_123456_ZYO on Thu 7 Jan 2021 11:09:39 PST. The main content area shows a search bar with a 'Search' button and a 'Wizard' button. Below the search bar, there is a table of mitigation entries. The first entry is 'Alert 167312 Auto-Mitigation' with a duration of 0:25 (Ended) and a start time of Jul 12 10:49 2019. The table has columns for Graph, Name, Protection Prefixes, Duration, Start Time, User, Type, and Annotations. A green box highlights the 'Add Mitigation' button, which has 'IPv4' and 'IPv6' options.

Graph	Name ↑	Protection Prefixes	Duration	Start Time ⓘ	User	Type	Annotations
	Alert 167312 Auto-Mitigation	208.185.166.178/32	0:25 (Ended)	Jul 12 10:49 2019	auto-mitigation	IPv4 Auto-Mitigation TMS Stopped	Auto-mitigation for alert #167312 Ended. (by auto-annotation)
			0:08			IPv4 Auto-Mitigation	Auto-mitigation for alert

Enter a meaningful name and (optional) description

- Select 'protect' on the left menu.

The screenshot shows the 'Create TMS Mitigation' page in the Zayo interface. The left sidebar has 'Protect' highlighted. The main form area contains the following fields and options:

- Name:** An empty text input field.
- Source Alert ID (Optional):** An empty text input field.
- Description:** A large empty text area.
- Internet Protocol Version:** A dropdown menu set to 'IPv4'.
- Mode:** Radio buttons for 'Active' (selected) and 'Inactive'. A note below states: 'Inactive mitigations are applied to attack traffic but do not drop any traffic.'
- Learning Dataset:** A dropdown menu set to 'None'.
- CDN Proxy:** A checkbox for 'Enable CDN Proxy Support' which is unchecked.

At the bottom of the form are three buttons: 'Cancel', 'Save and Start Mitigation', and 'Save and View Listing'.

Enter the IP address you want to target in protection prefixes

Scroll down and click 'Save' and 'Start mitigation'

- This will open the mitigation summary page.

The screenshot shows the 'Create TMS Mitigation' page, scrolled down to the 'Flow Specification Filters' section. The 'Managed Object' is set to 'zDDoS_Test-DDoS_123456_ZYO'. The 'Protection Prefixes' field is highlighted with an orange box. The 'Flow Specification Filters' section includes the following fields and options:

- Managed Object:** A dropdown menu set to 'zDDoS_Test-DDoS_123456_ZYO'.
- Protection Prefixes:** A large empty text area, highlighted with an orange box. A note below states: 'Note: All must fall within managed object CIDRs'.
- Diversion Prefixes:** Radio buttons for 'Default' (selected), 'Less Specific', and 'Custom'. A note below states: 'Divert the same prefixes to the TMS as the prefixes that the mitigation protects.'
- Timeout:** A text input field with an example of '600' and the label '(Default is no timeout) seconds'.
- Flow Specification Filters:**
 - Protocol Numbers:** A text input field with an example of '1-6, 17'.
 - Source Prefix:** A text input field with an example of '203.0.113.16/30'.
 - Source Ports:** A text input field with an example of '1-10, 80'.
 - Destination Ports:** A text input field with an example of '1-10, 80'.
 - Match any specified source ports AND any specified destination ports:** A radio button that is selected.
 - Match any specified ports:** An unselected radio button.

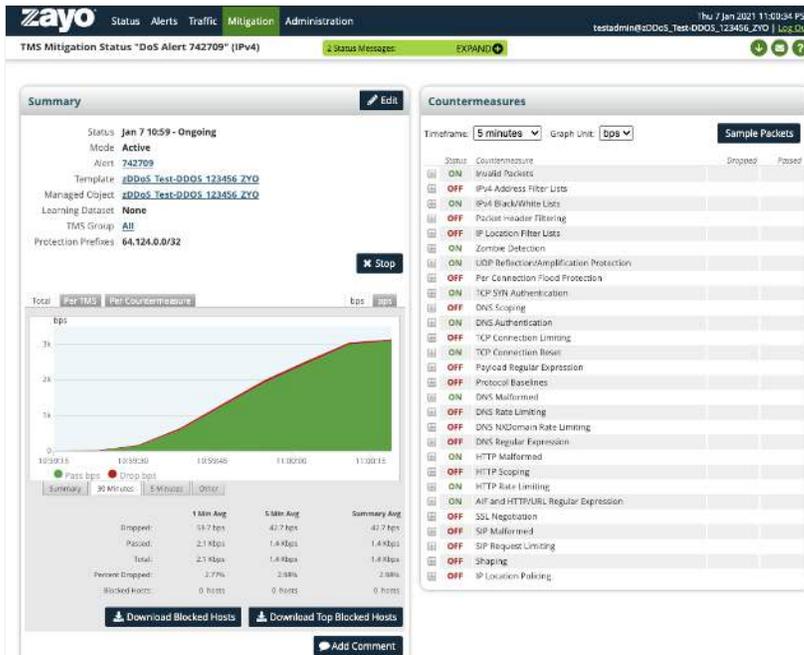
At the bottom of the form are three buttons: 'Cancel', 'Save and Start Mitigation', and 'Save and View Listing'.

Within a few minutes, the graph will populate if there is traffic.

- The 'Countermeasures' section to the right is organized by traffic

Click the plus next to that transaction to see additional details

- In this case the **HTTP Rate limiting** is being triggered



For this example, the test traffic is a very small request at a high rate from a single source IP and is triggering the HTTP Limiter. To optionally remove that limit, you can uncheck '**enable HTTP Object Limiting**' to disable the countermeasure completely or to adjust the HTTP Object Limit via the **slider or the text entry field** and '**save**'

Uncheck '**Enable HTTP Request Limiting**' to disable completely or adjust the values via the **slider or the text box** and select '**Save**'

- In this case the 'HTTP Request limit' is not being triggered but it functions the same way

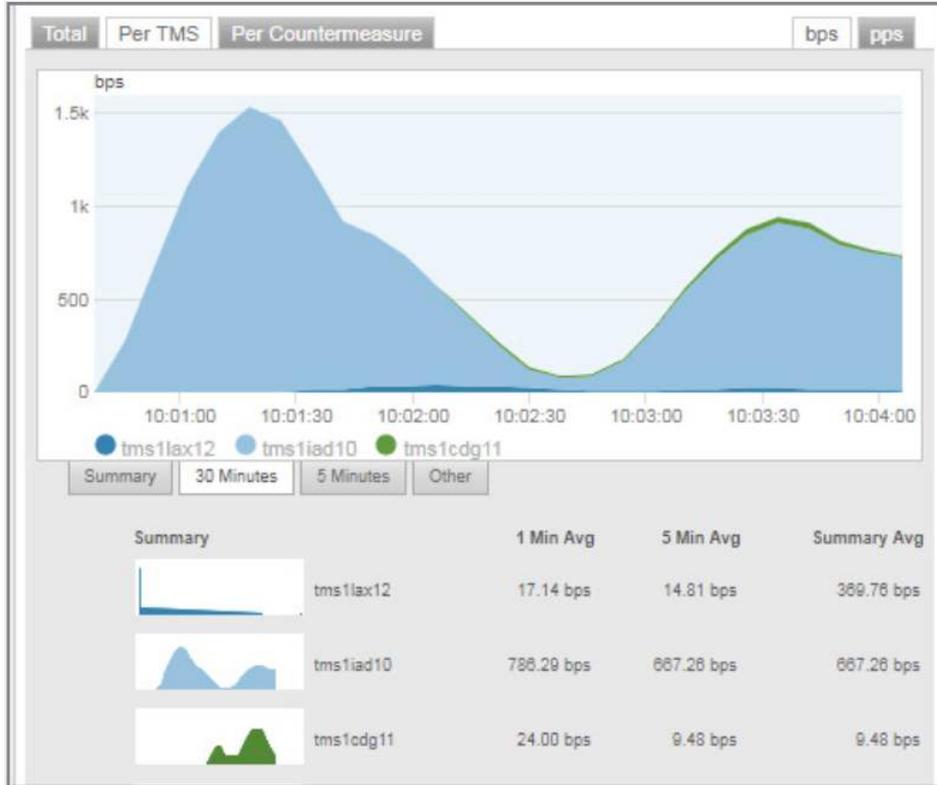
The screenshot shows the configuration page for 'HTTP Rate Limiting'. It is currently set to 'ON'. The page contains two main configuration sections:

- Enable HTTP Object Limiting:** This section has a checked checkbox. Below it, there is a text input field for 'HTTP Object Limit' with a value of '5' and a note: 'Example: '20' (Leave blank to use default '10') requests per second per object'. Below the input is a graph showing 'No Data'.
- Enable HTTP Request Limiting:** This section also has a checked checkbox. Below it, there is a text input field for 'HTTP Request Limit' with a value of '5' and a note: 'Example: '200' (Leave blank to use default '100') requests per second'. Below the input is another graph showing 'No Data'.

At the bottom of the page, there is a green 'Save' button.

To view sample packets you should first verify which TMS are receiving traffic

Select **'Per TMS'** on the graph on the left side of the page and note below the active TMS, in this case **"tms1iad10"** is most active



To view or collect packet information click **'Sample Packets'**



In the new pop-up window, select **"TMS1iad10"** and packets will start displaying

You can save the sample of packet for download by clicking **'Record'**

- Recording will continue for 60 seconds or 5000 packets.
- The sample will automatically download to your browser's default location.
- In most cases, that will be located in your downloads folder.

At this point you can continue to view samples, **Clear** or **Close** the pop-up entirely

The screenshot shows a pop-up window titled "Sample Packets For Mitigation 'Alert 167312 Auto-Mitigation'" with a "Close" button in the top right corner. The window is divided into three main sections:

- Settings:** Contains a "TMS Appliance" dropdown set to "tms1iad10", a "Filter Type" dropdown set to "FCAP Filter", an "FCAP Filter" text input field with an "Apply" button, and a "Filter by" dropdown set to "All Packets".
- Record Sample:** Contains a text box explaining: "Record a sample of packets and download a packet capture file (pcap). This will sample for 60 seconds, or 5000 packets, whichever occurs first." Below this is a green "Record" button.
- Sampled Packets:** Shows "Number of Sampled Packets Shown: 0". Below this is a table with the following headers: "Country", "Src IP", "Port", "Country", "Dst IP", "Port", "Proto", "Len", "Match", and "Countermeasure". The table body is currently empty. At the bottom of this section are buttons for "Continue", "Stop", "Clear", and checkboxes for "dropped" and "passed".
- Packet Contents:** A section at the bottom of the pop-up, currently empty.

Back on the mitigation page. To end the mitigation click '**Stop**'

The screenshot shows the "TMS Mitigation Status" page for "Alert 167312 Auto-Mitigati...". The page has a navigation bar with "Status", "Alerts", "Traffic", "Mitigation" (highlighted), and "Administration".

The main content area is titled "TMS Mitigation Status 'Alert 167312 Auto-Mitigati...'" and contains a "Summary" section with an "Edit" button. The summary details are:

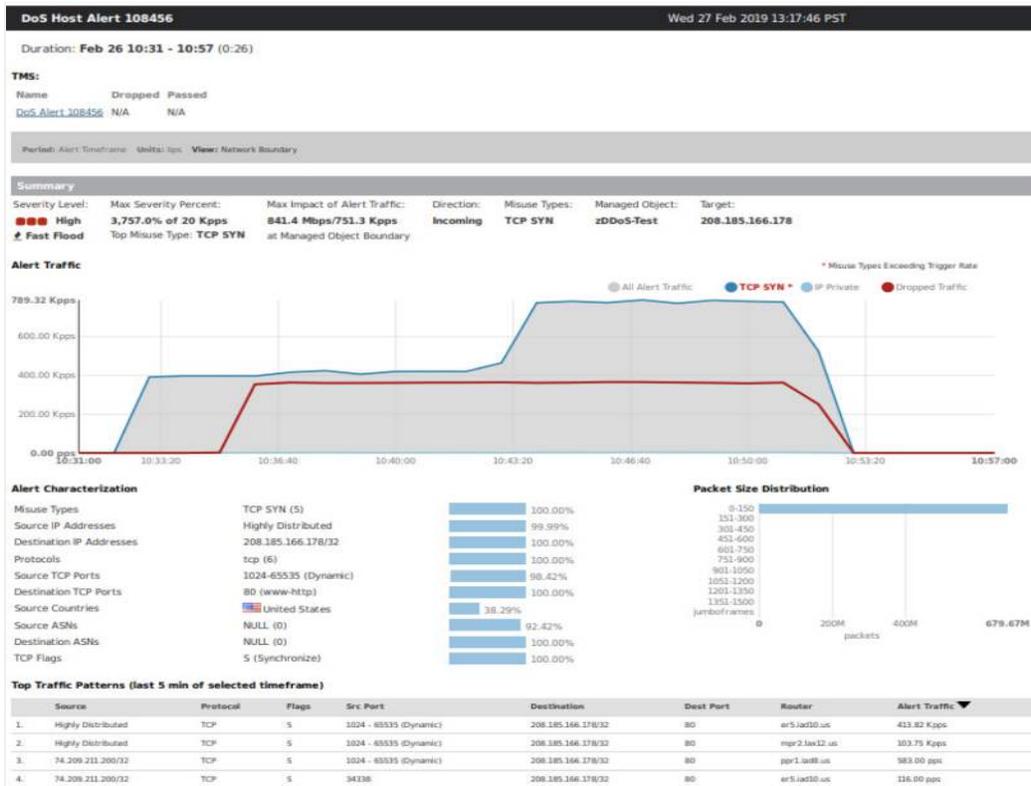
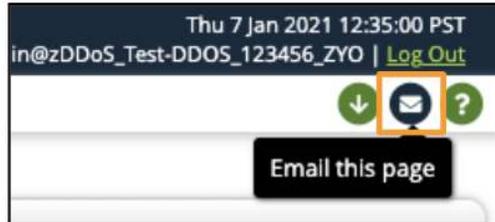
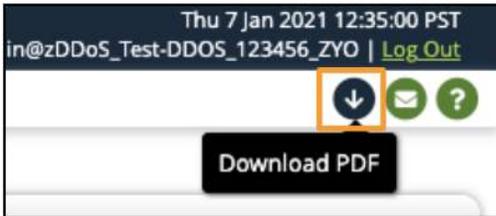
- Status: Jul 12 10:49 2019 - Ongoing
- Mode: Active
- Alert: None
- Template: [zDDoS Test-DDOS 123456 ZYO](#)
- Managed Object: [zDDoS Test-DDOS 123456 ZYO](#)
- Learning Dataset: None
- TMS Group: [All](#)
- Protection Prefixes: 208.185.166.178/32

At the bottom right of the summary section, there is a "Stop" button with a close icon, which is highlighted with an orange box. At the bottom of the page, there are tabs for "Total", "Per TMS", and "Per Countermeasure", and units for "bps" and "pps".

Reporting

Support Incident Reporting:

When viewing an alert under the alerts section, you can **download** or **email** an incident by clicking the icons in the top navigation



Summary Report:

Summary reports are **emailed** on a selected cadence determined during your service delivery.

- Reach out to the Network Control Center (NOC) to make any adjustments

