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

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.

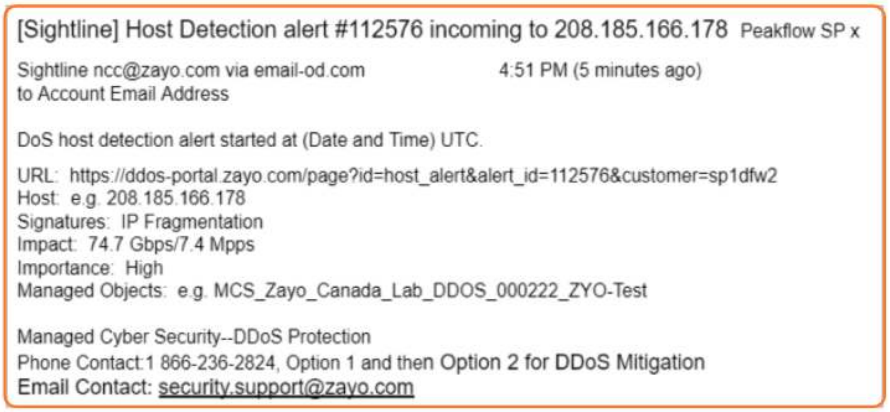
Please note that the Basic subscription plan offers only an incident-by-incident mitigation.

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:

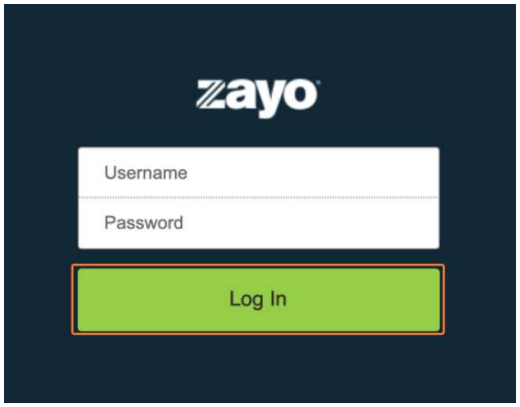
- Most extensive access to the portal
- Benefit from proactive monitoring and receive system generated alert notifications when a DDoS attack is detected
- Access automatic mitigation to eliminate response time, authorized mitigation or perform self mitigation of DDoS attacks on an ad hoc basis
- All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

Portal Navigation

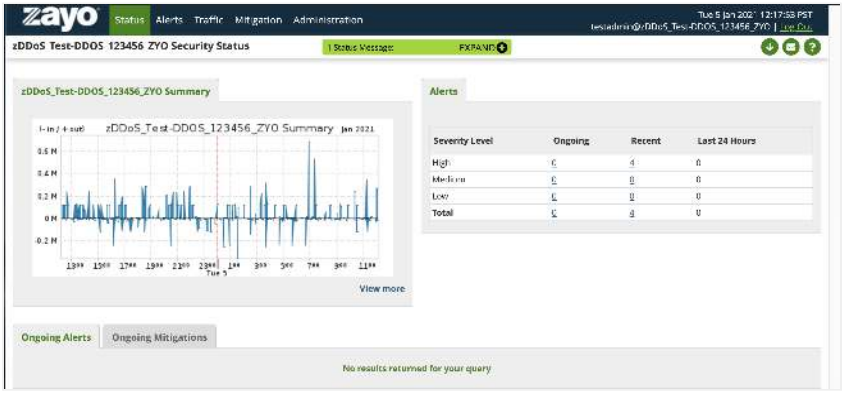
Customer login process

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

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

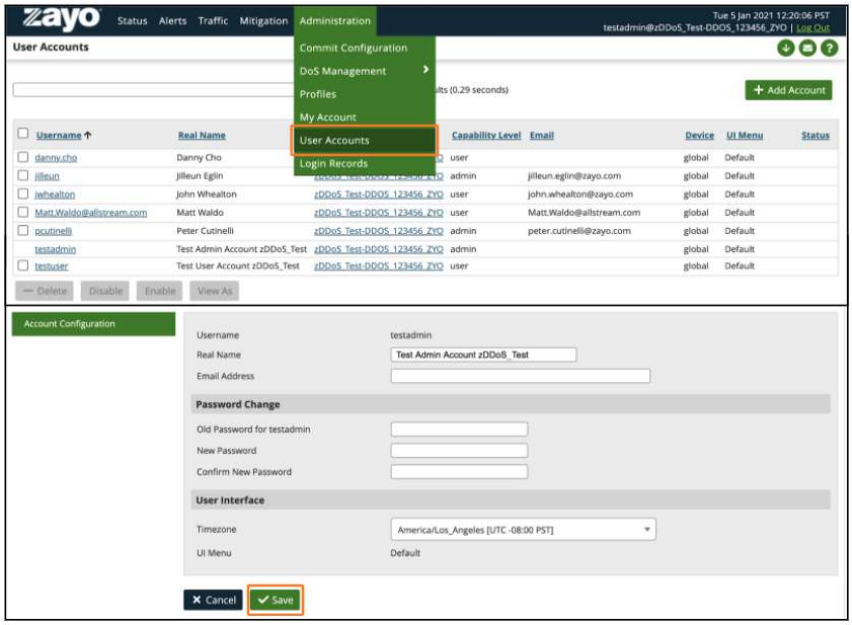


You are now at the default landing page



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'**



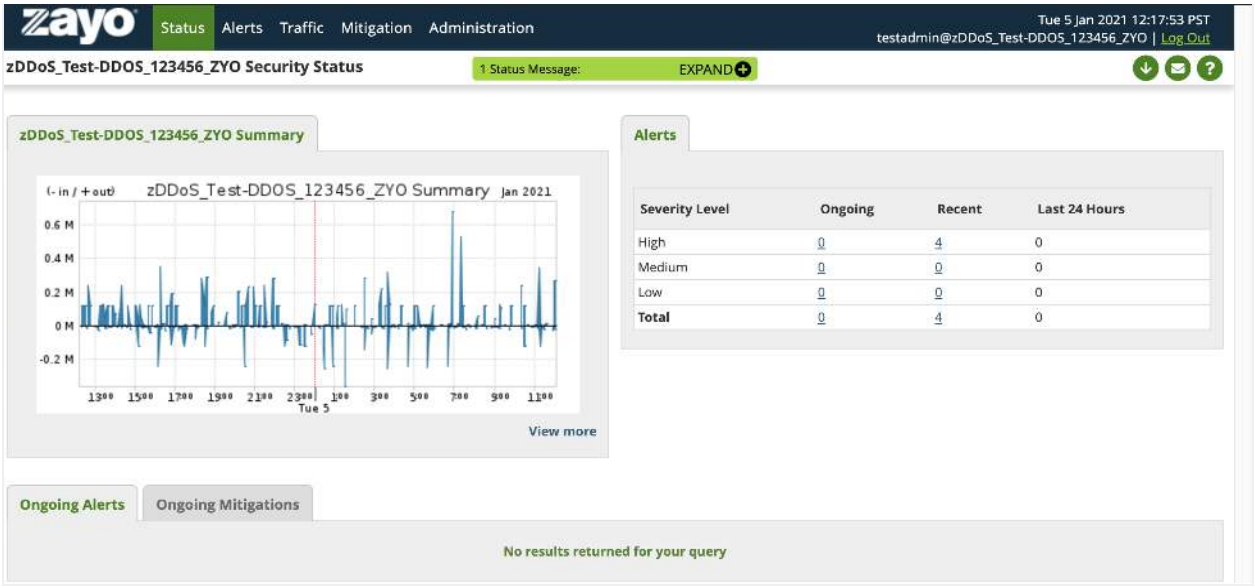
You should see the following banner noting your update

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

Status

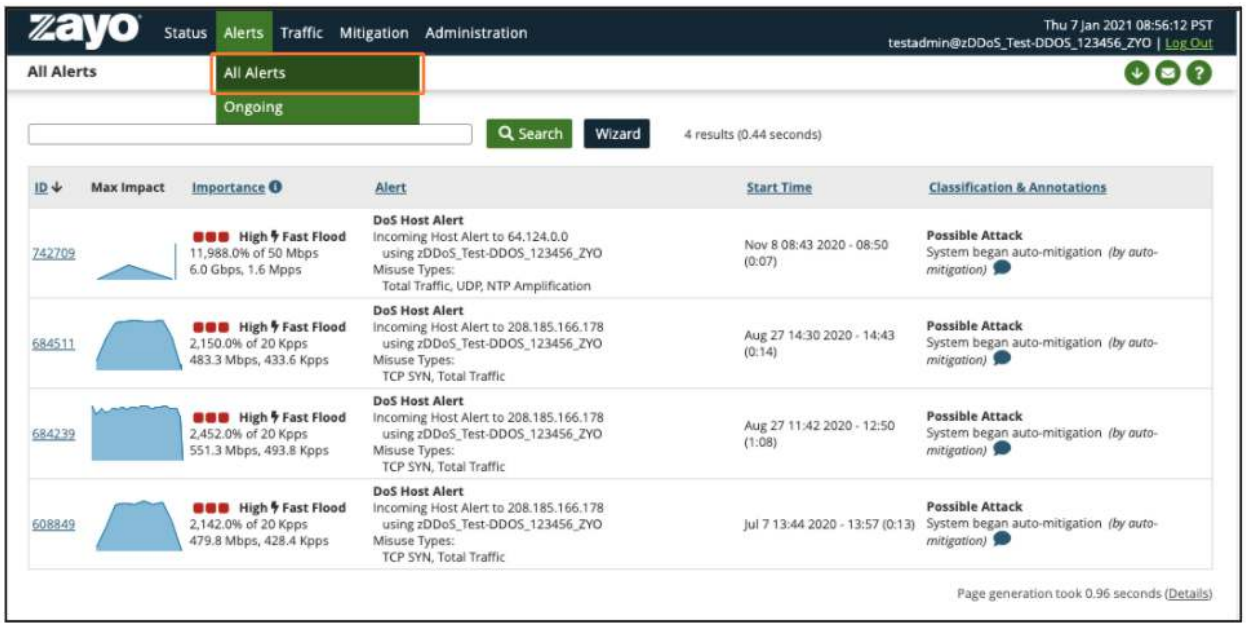
The Status tab is an overview snapshot of your service

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



Alerts

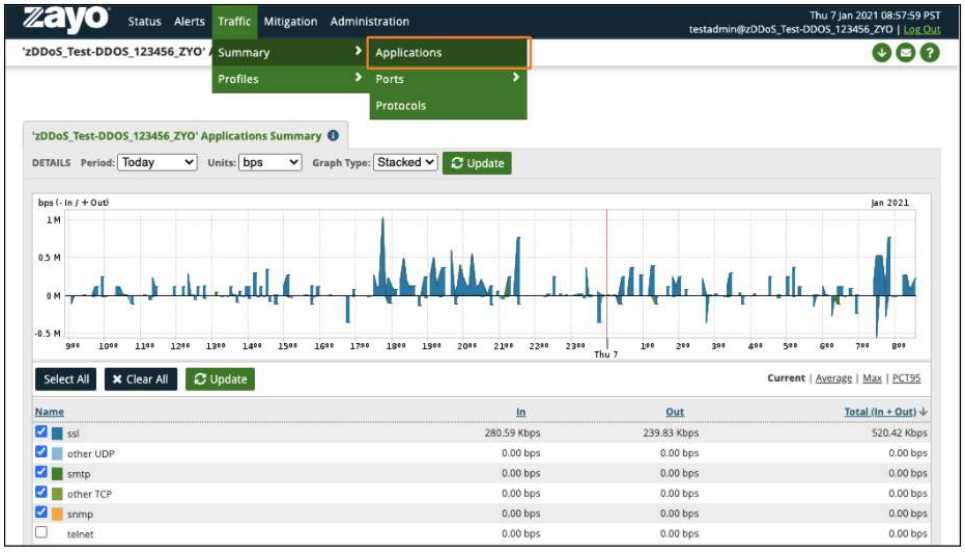
The Alerts tab is a log of all alerts with classification and the importance ratings for all alerts and ongoing alerts



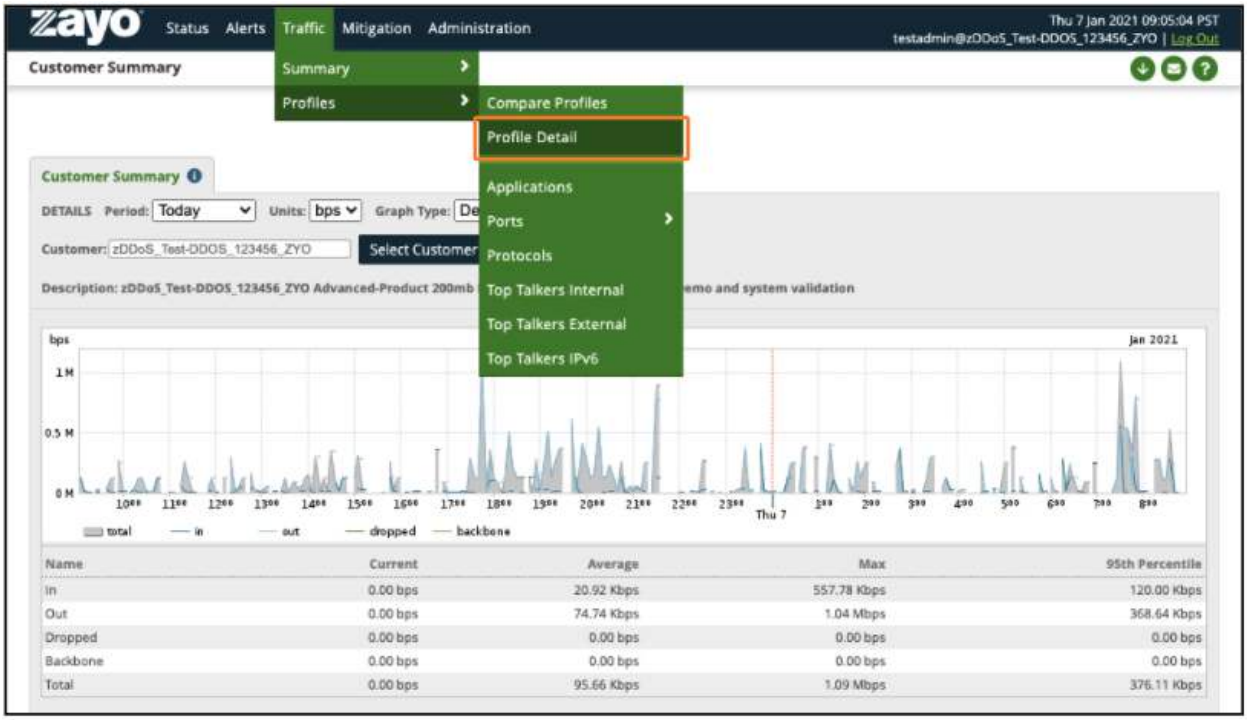
Traffic

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



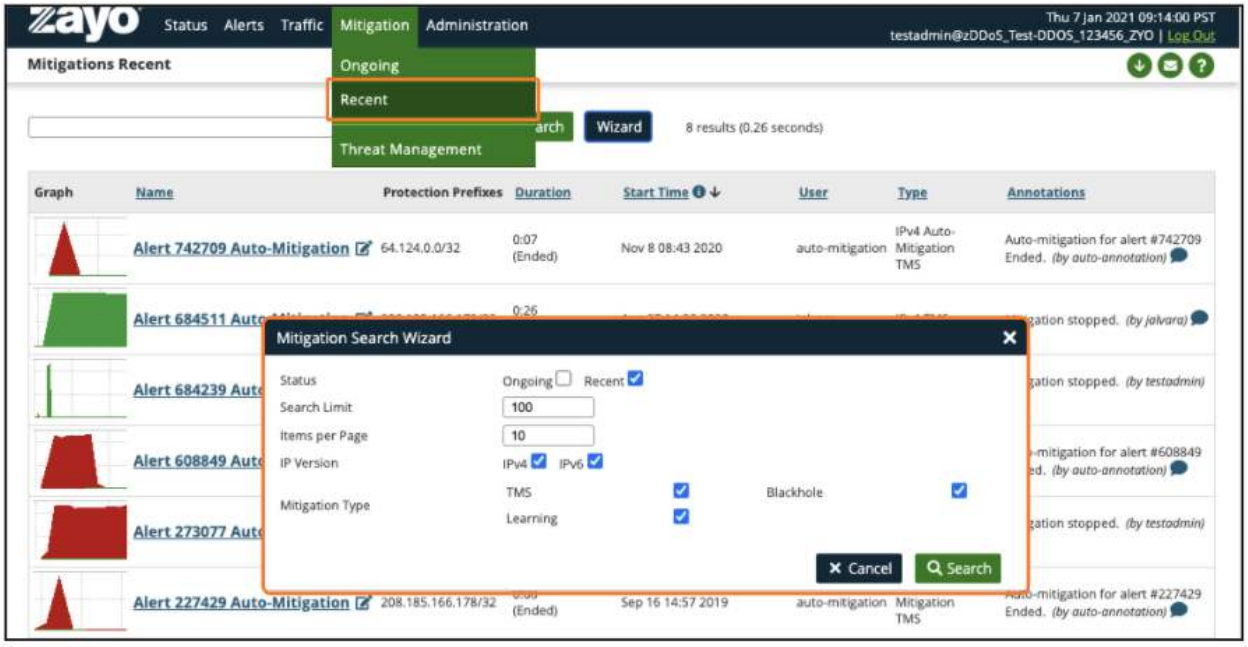
Navigate to **'Traffic'** > **'Profiles'** > '**Profile Detail**' to view traffic per port, by "talkers" and by protocol.



Mitigation

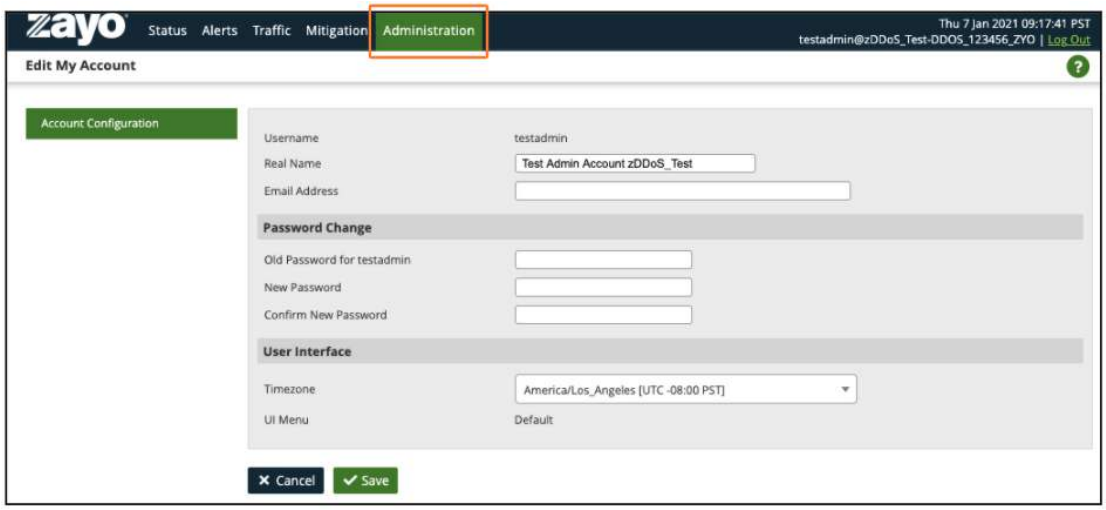
The Mitigation tab is a log of mitigations occurring on your service

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

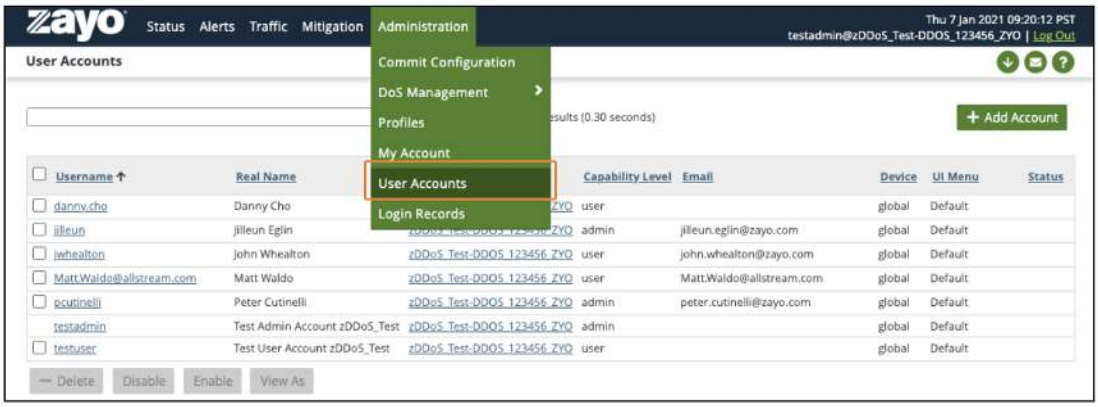


Administration

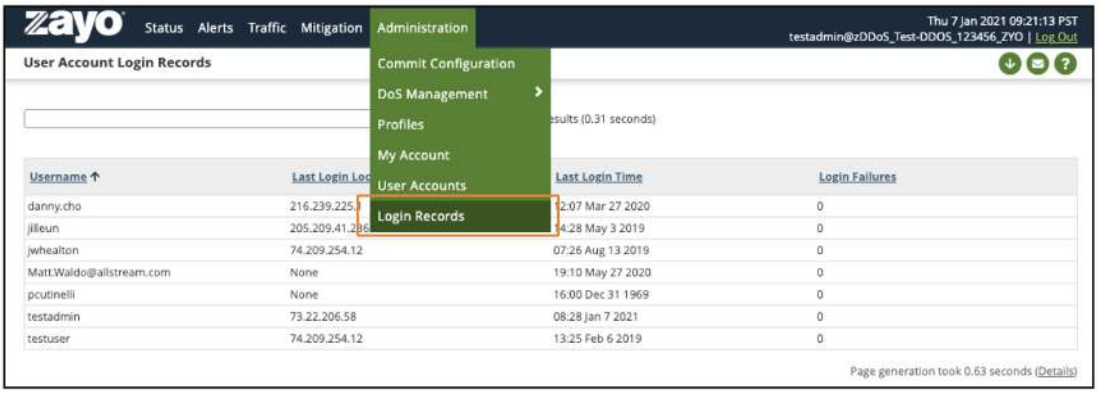
The administration tab allows you to manage your profile settings and users. Update password, timezone, or email.



User Accounts: Manage other users if you are an admin

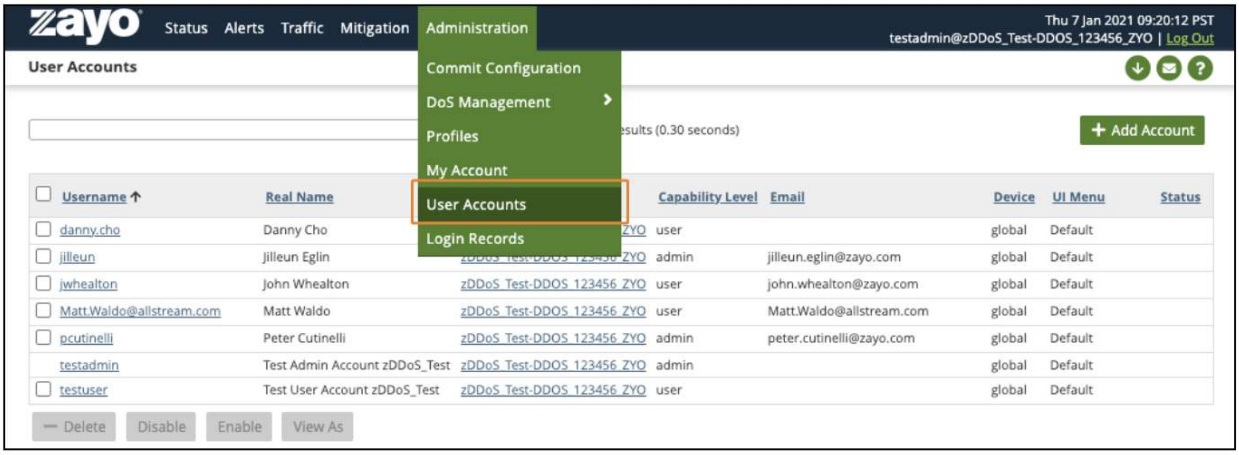


Login Records: Login history



Creating Additional Users

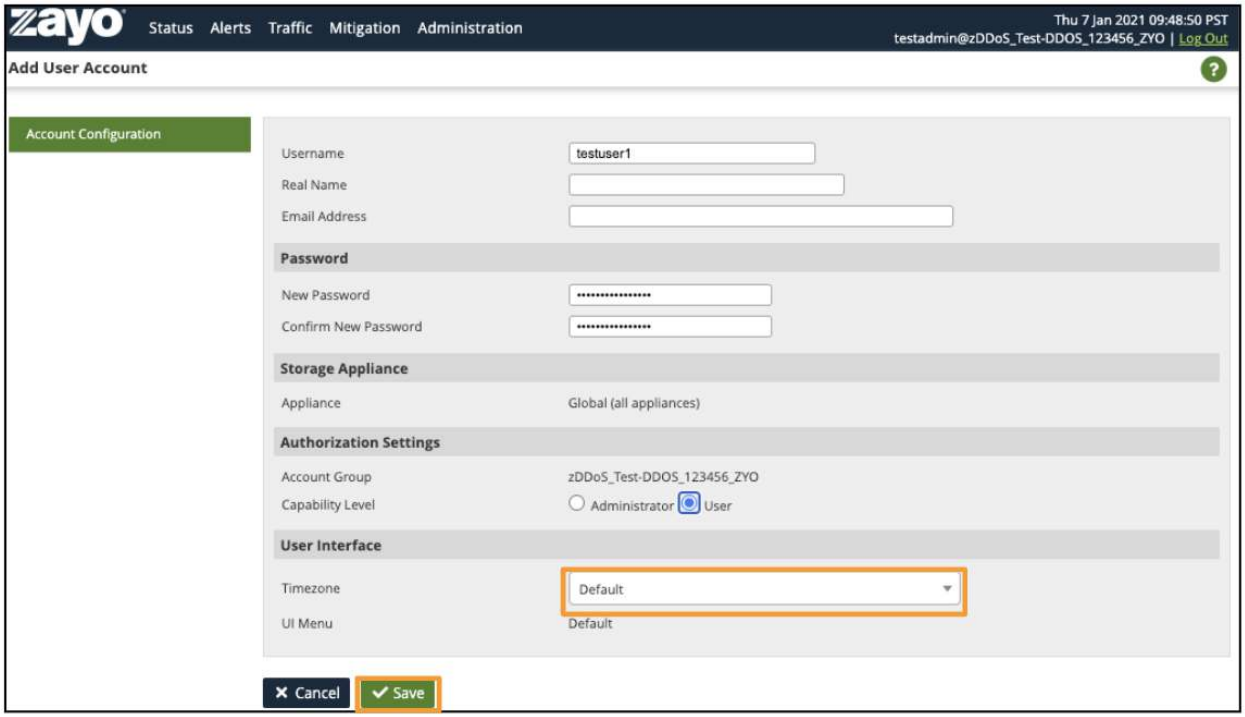
To add additional users select **'Administration'** > **'User Accounts'** > Click **'Add Account'**



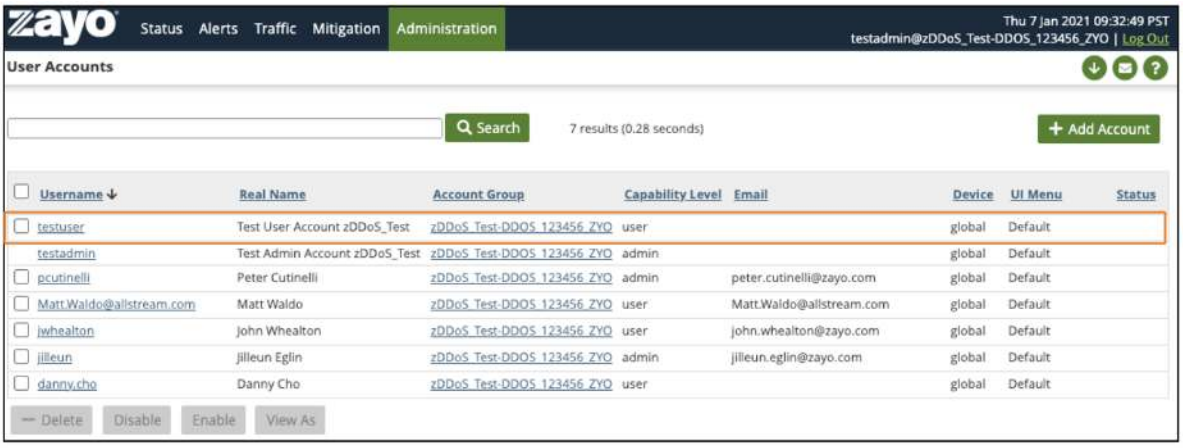
Administrator can create additional Admin or User accounts, User is view-only

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 new account should now display in the list:



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

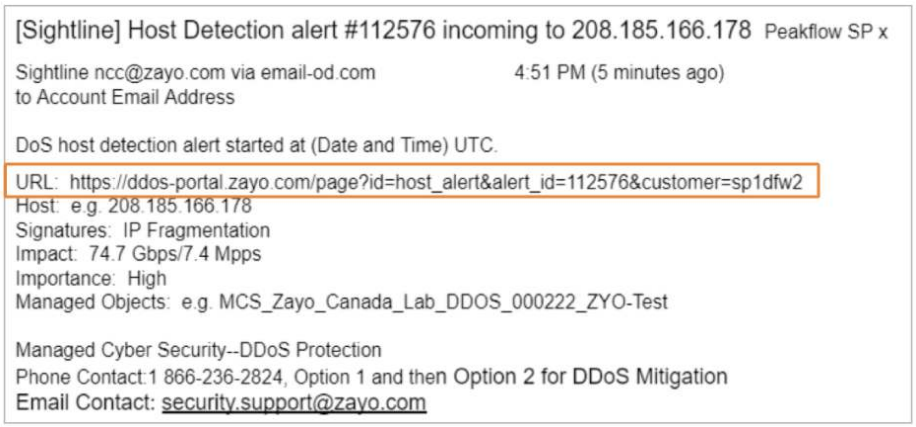
Portal Use - Advanced Capabilities

Detection Alert

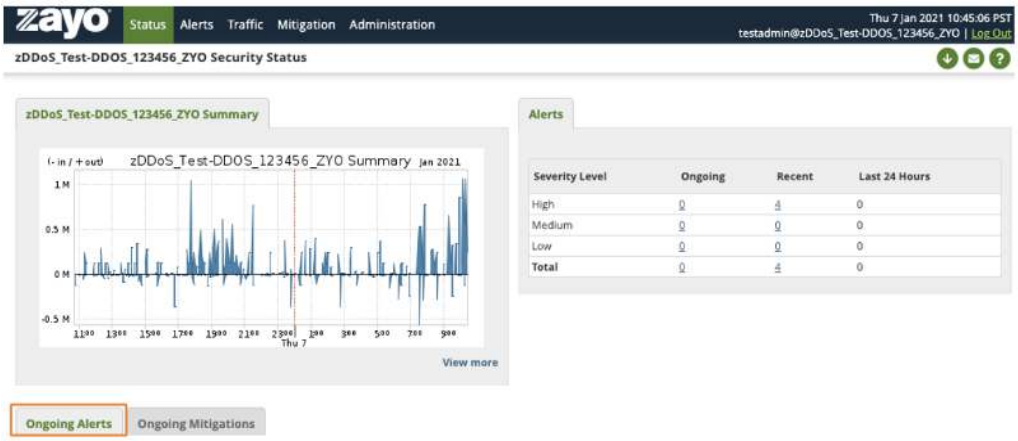
If you are using self mitigation, the following steps will walk you through reviewing a detection alert and how to mitigate it.

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

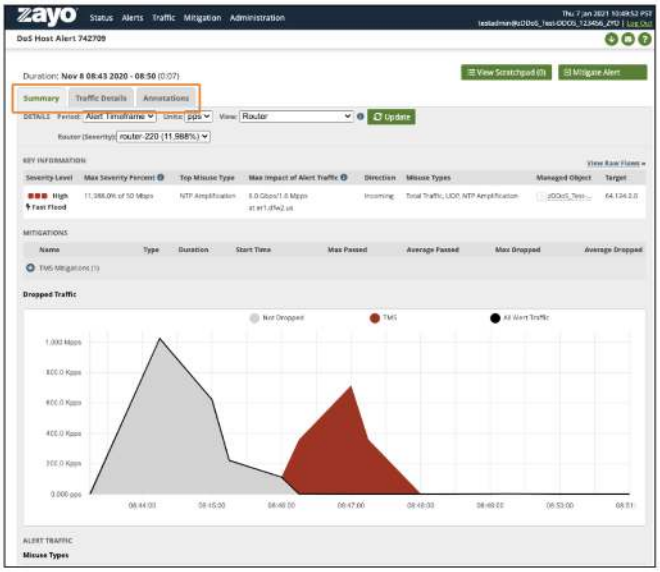
1. Email alert received: to view more details on the alert **click URL link**



2. 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**)



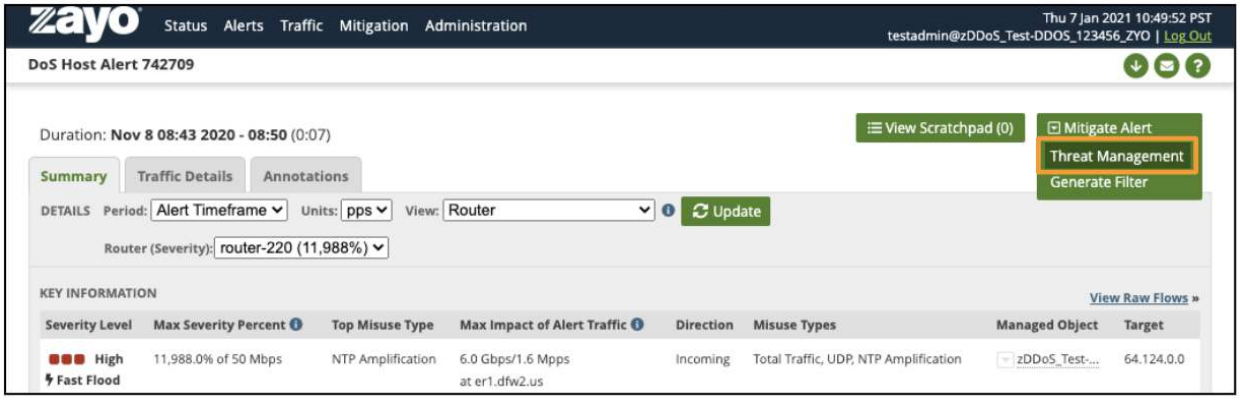
3. You should now see the alert dashboard, feel free to navigate to different tabs and learn about the alert.



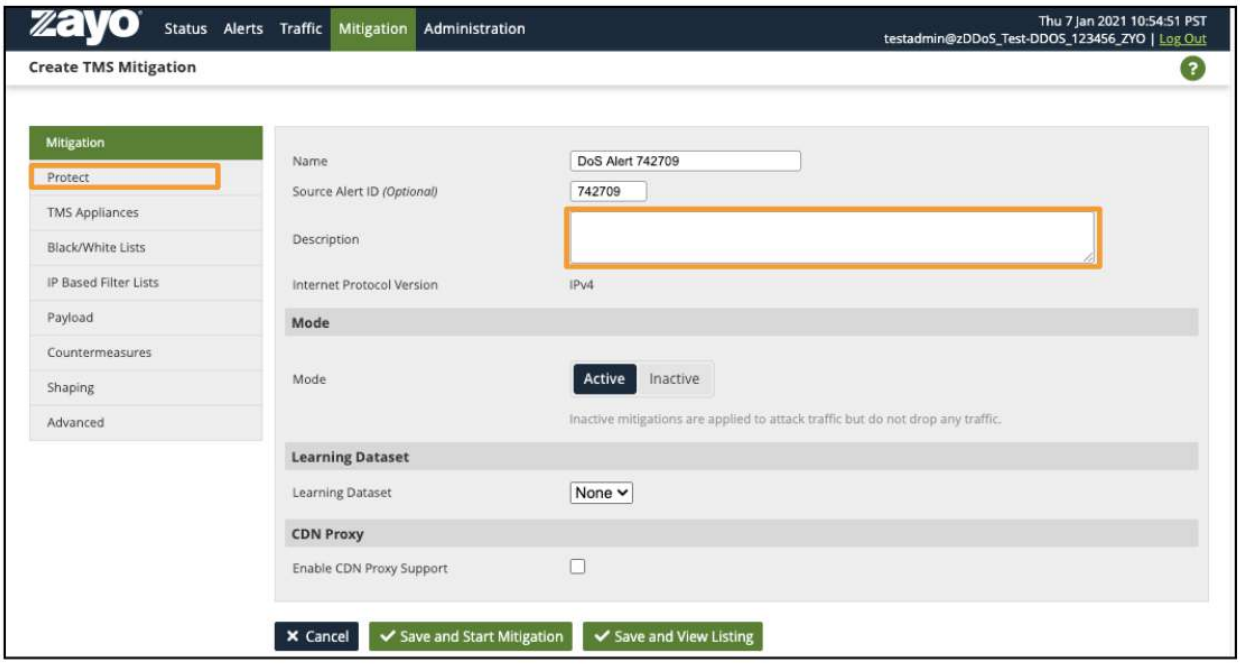
Running a Mitigation

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

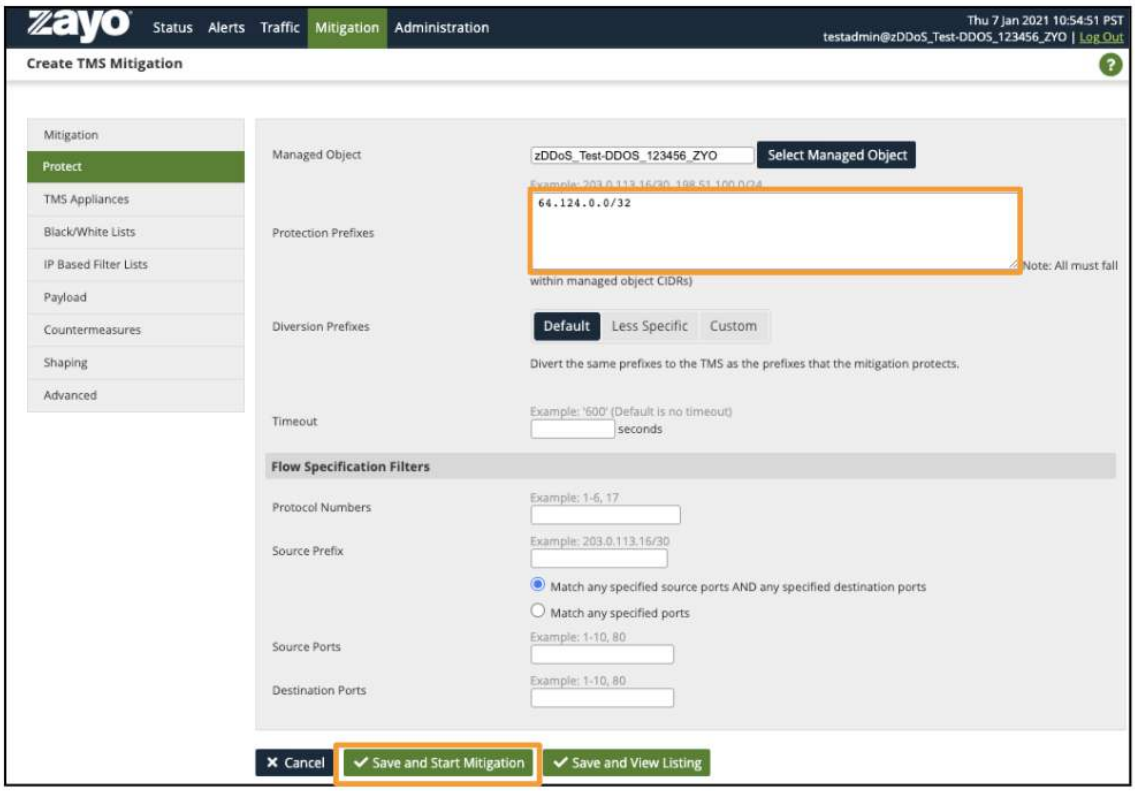


Enter notes in the description (optional) and click '**Protect**' on the left.



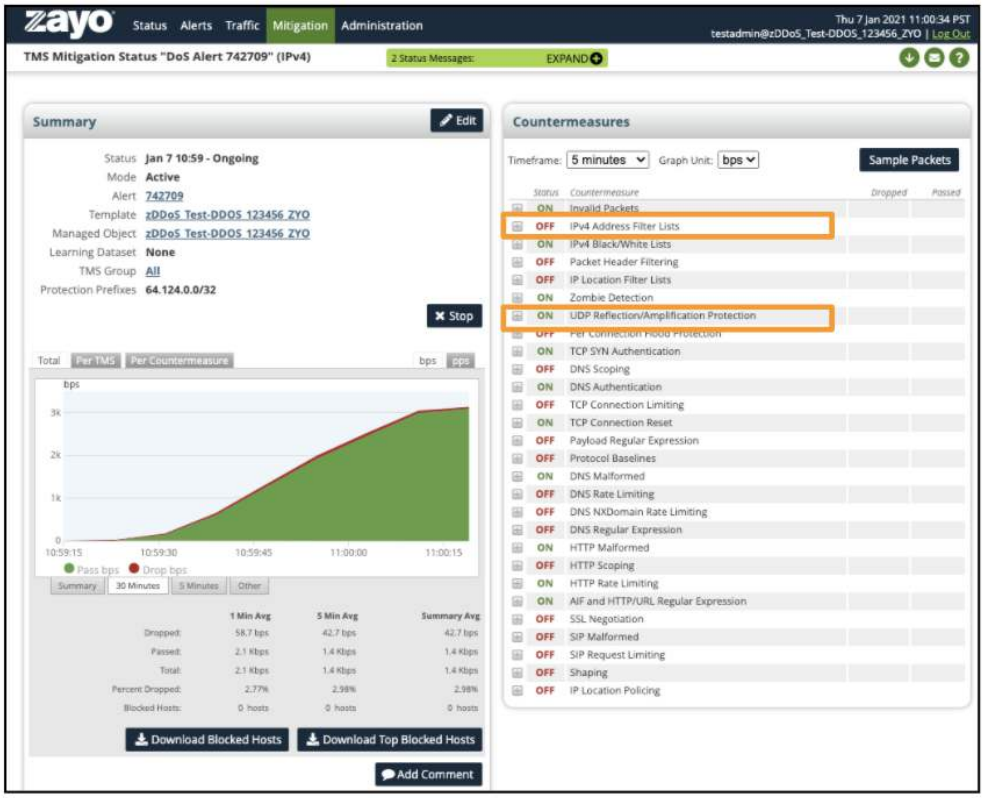
The affected IP addresses will be listed in the Protection Prefixes section

- Click '**Save and Start Mitigation**'



This will drop you into the mitigation summary.

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



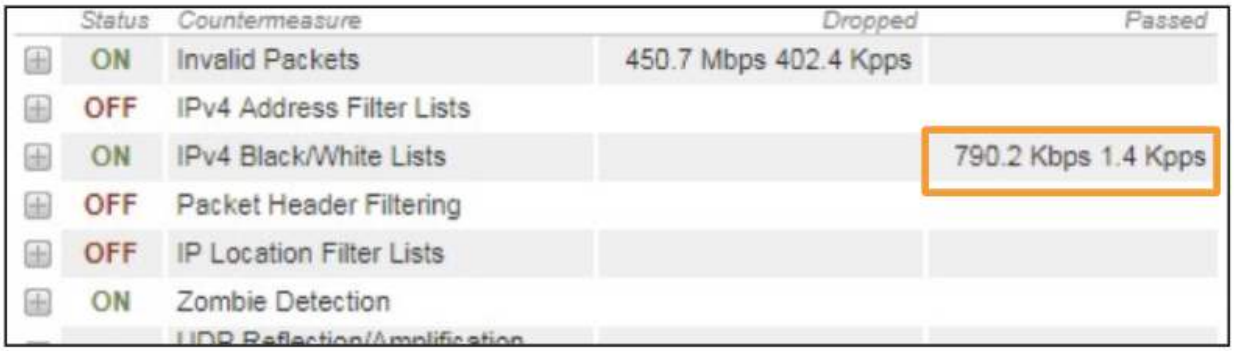
Adjust Live Mitigation

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

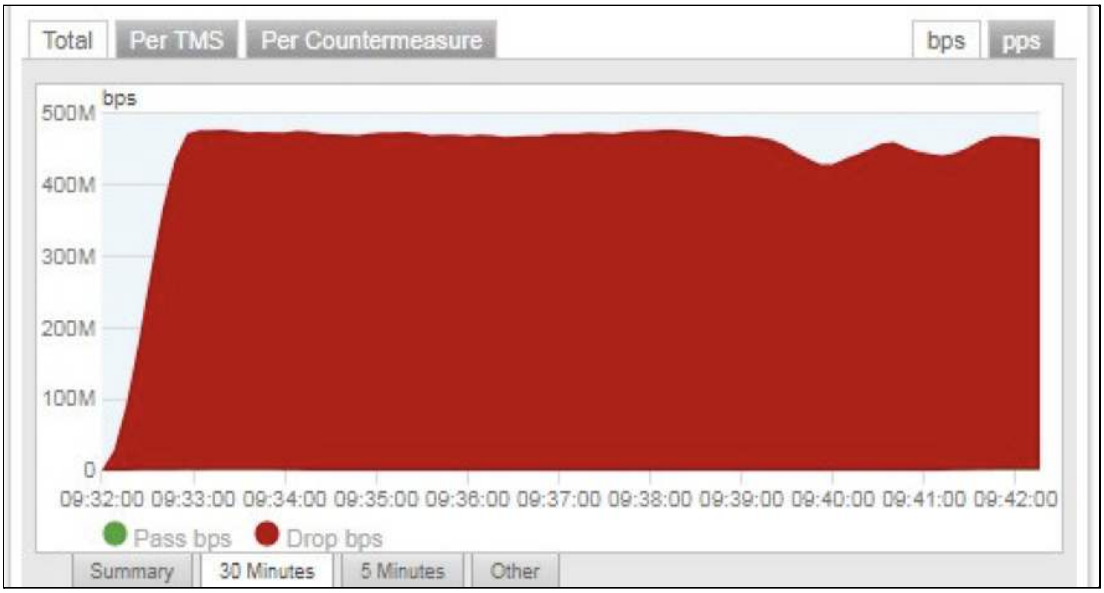
Situation: Test traffic is not very diverse or high volume and was misclassified by the system as part of the attack.

- 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**

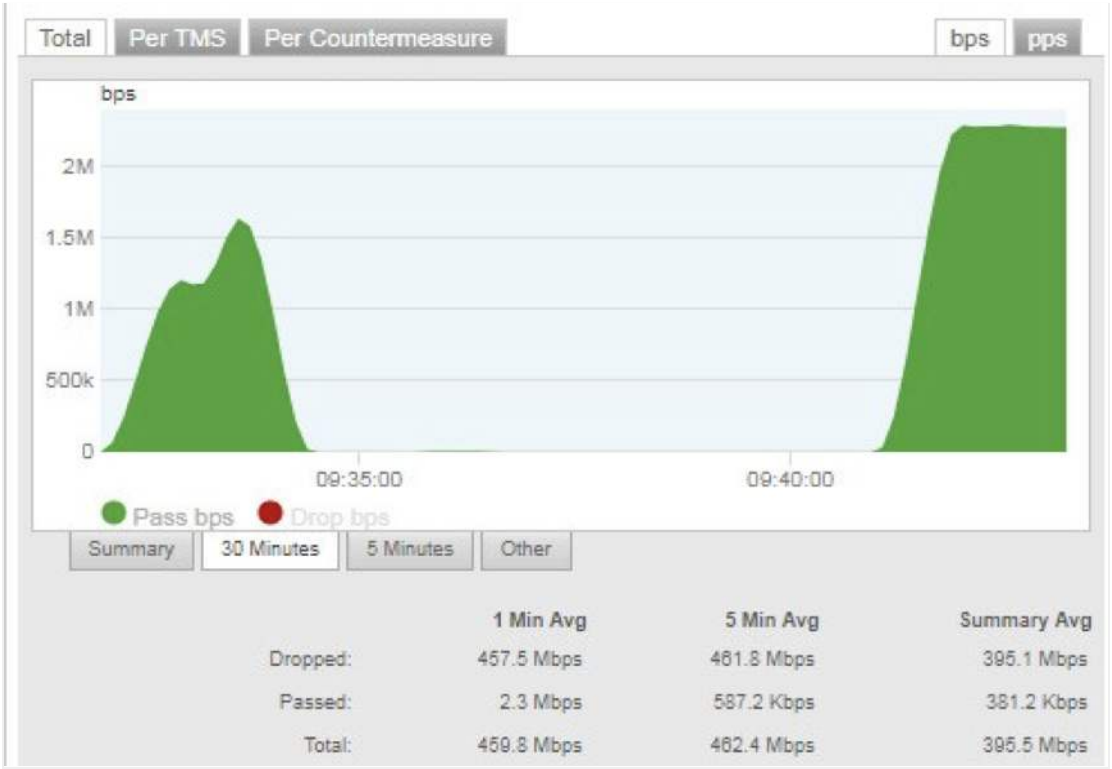
Now All traffic from that source automatically passes



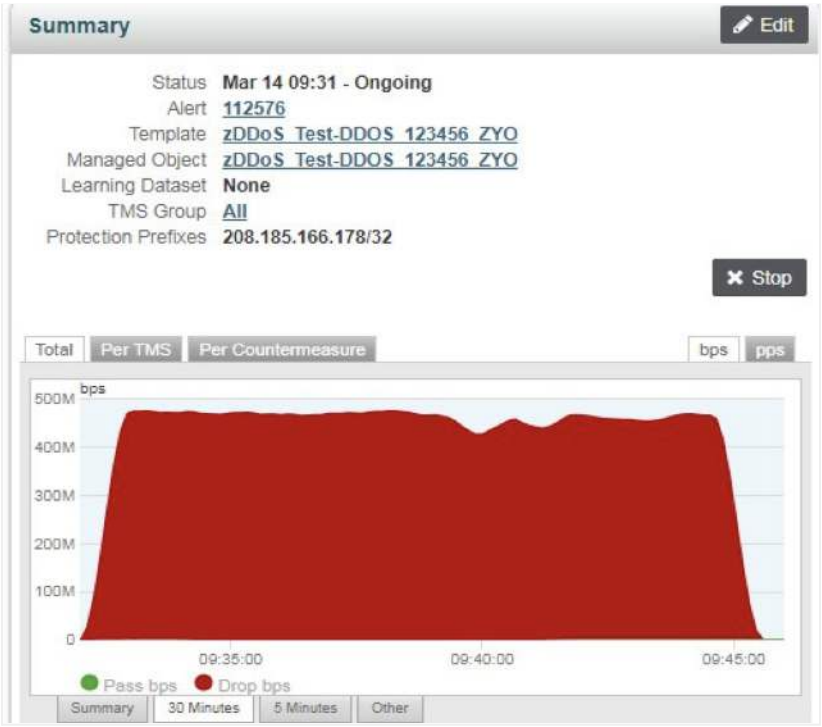
You can select/deselect pass or drop traffic on the graph to see them individually



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.

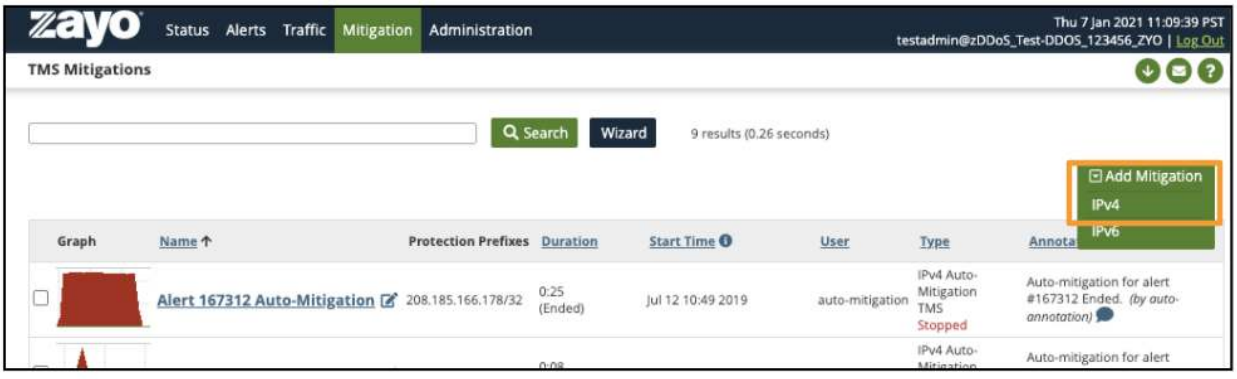
URL: https://ddos-portal.zayo.com/page?id=host_alert&alert_id=112576&customer=sp1dfw2
Host: 208.185.166.178
Signatures: TCP SYN, Total Traffic
Impact: 311.36 Mbps/649.70 Kpps
Importance: High
Managed Objects: "zDDoS_Test-DDoS_123456_ZYO"

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

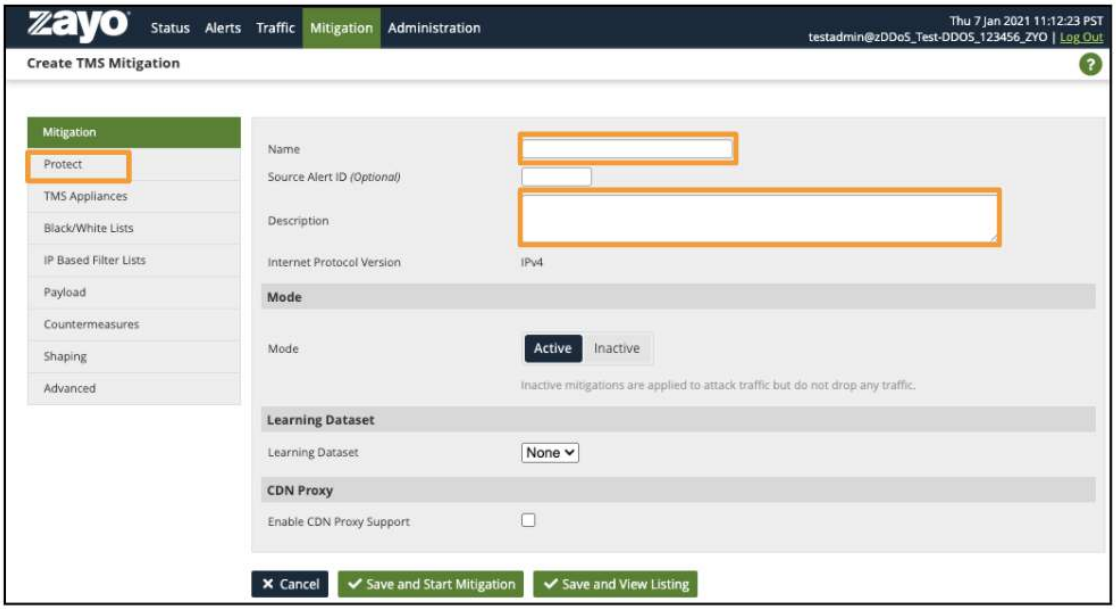
The following will walk thought redirecting an IP that you suspect is receiving malicious traffic

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



Enter a meaningful name and (optional) **description**

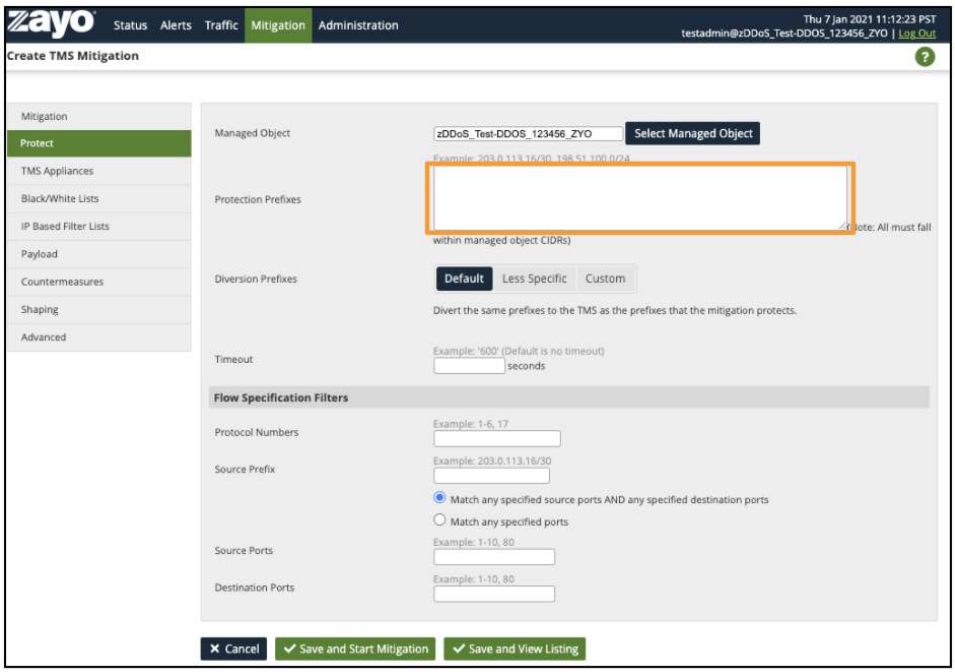
- Select '**protect**' on the left menu.



Enter the IP address you want top target in protection prefixes

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

- This will open the mitigation summary page.

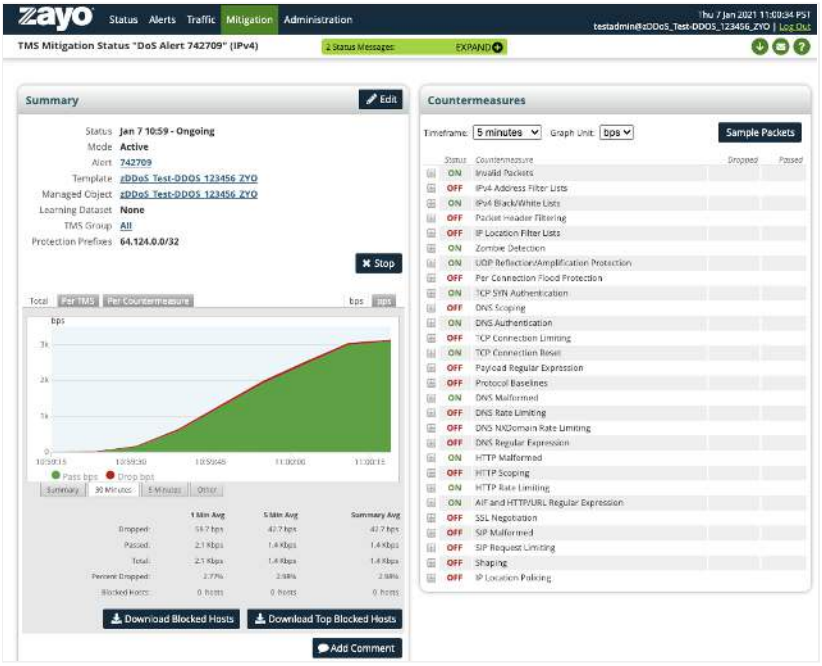


Within a few minutes, the graph will populate if there is traffic.

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

Click the plus next to that transaction to see additional details

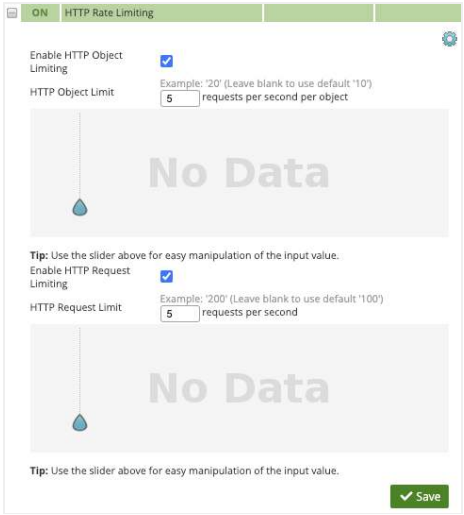
- In this case the **HTTP Rate limiting** is being triggered



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'**

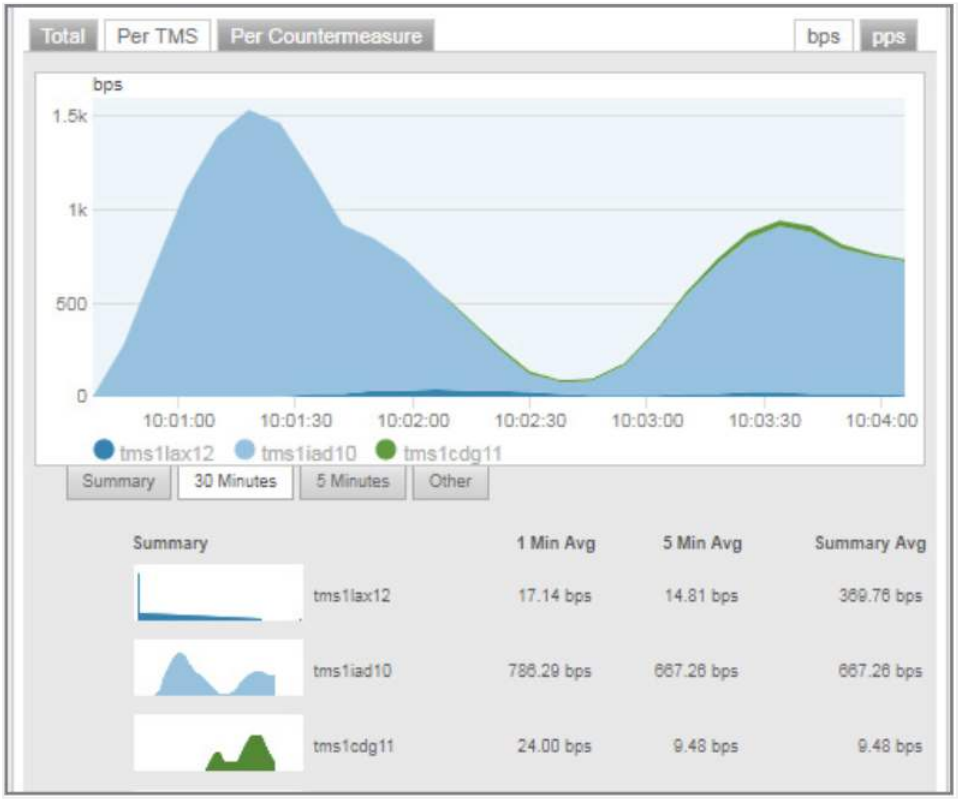
Uncheck '**Enable HTTP Request Limiting**' to disable completely or adjust the values via the **slider or the text box** and select **'Save'**

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

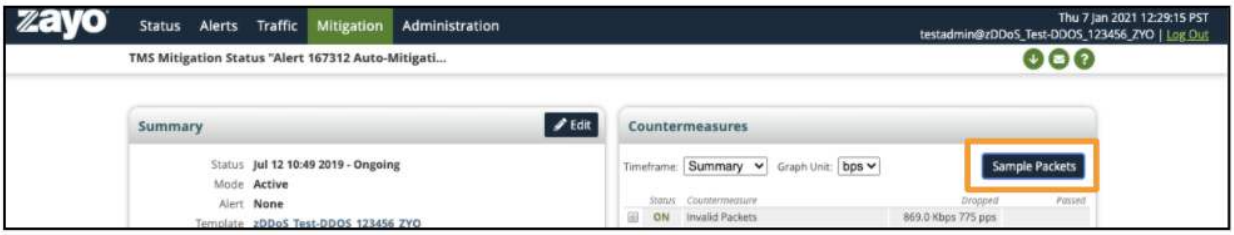


To view sample packets you should first verify which TMS are receiving traffic

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'**

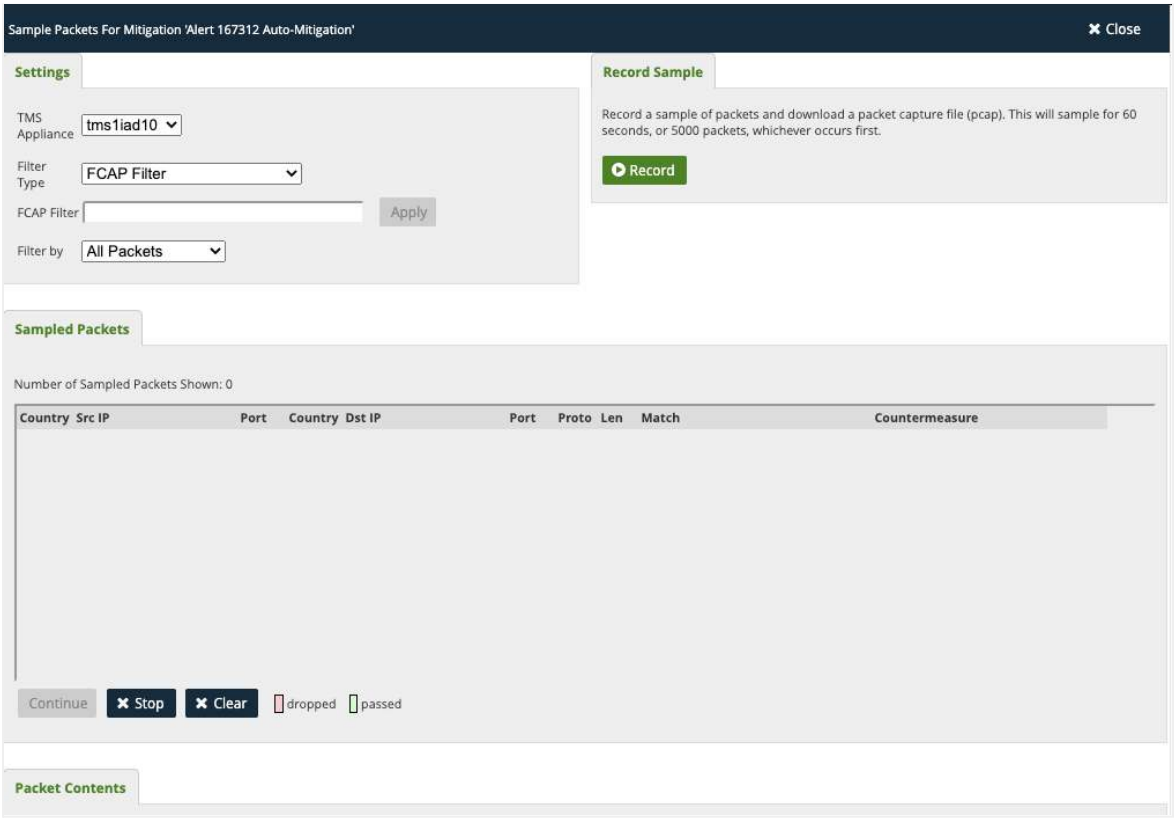


In the new pop-up window, select **"TMS1iad10"** and packets will start displaying

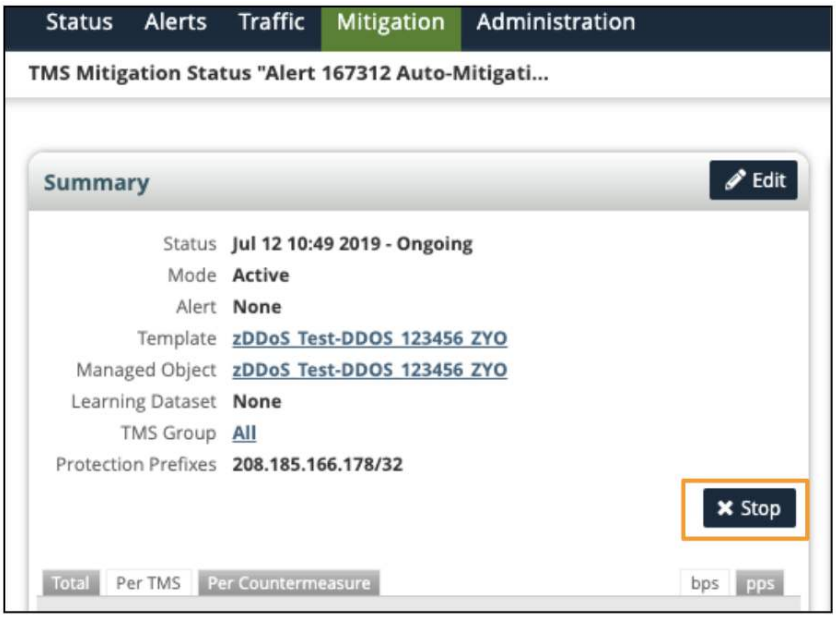
You can save the sample of packet for download by clicking **'Record'**

- 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



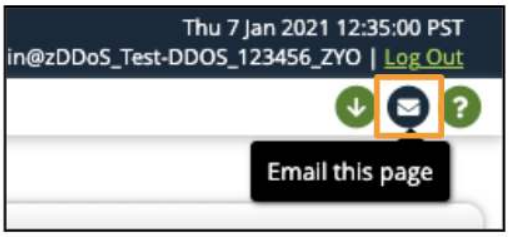
Back on the mitigation page. To end the mitigation click **'Stop'**

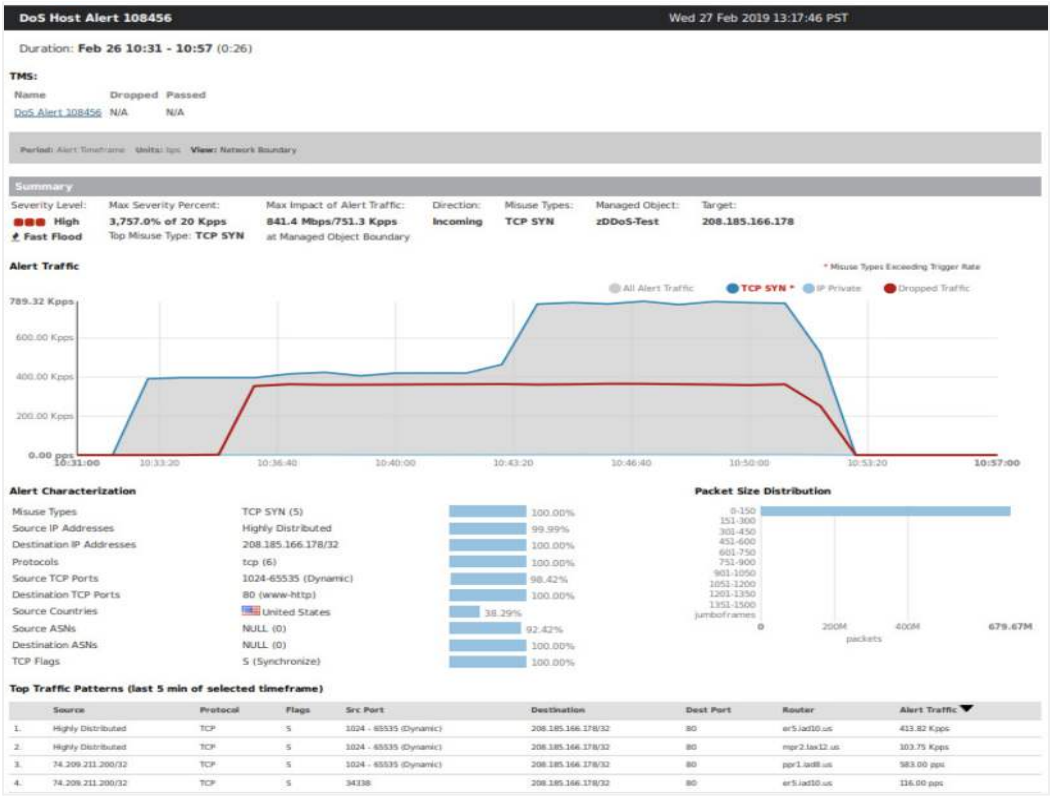


Reporting

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