GUIDE

DDoS Mitigation Summary Report User Guide

Spectrum ENTERPRISE™

Table of contents

Spectrum Enterprise DDoS Protection service

Spectrum Enterprise monitors internet traffic for DDoS events by polling data samples at regular intervals and measuring the data volume against predefined thresholds based on a client's normal traffic patterns. These thresholds are defined during the service activation process.

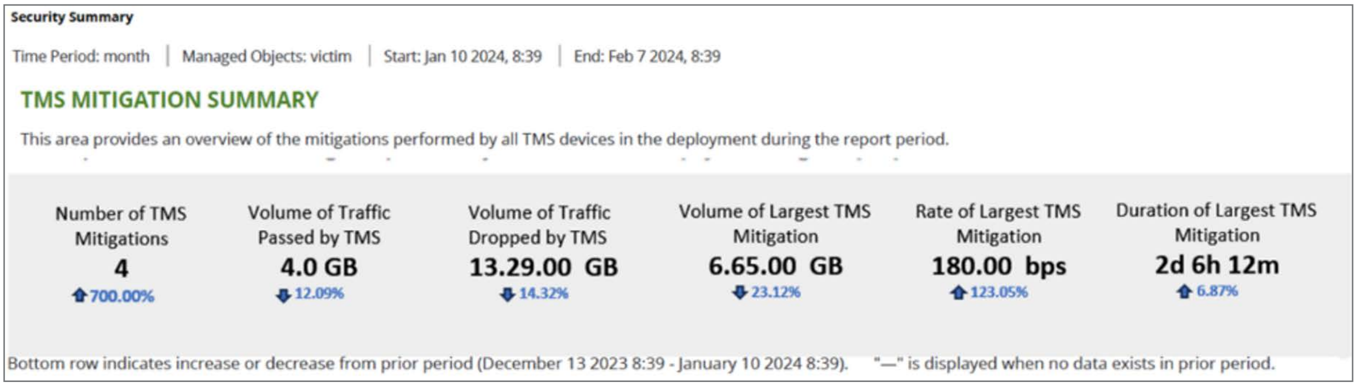
When a client's traffic patterns exceed the predefined threshold, the Spectrum Enterprise DDoS Protection platform will trigger an alert of a potential DDoS event and categorize the event as high, medium, or low based on the severity of the event. DDoS mitigation is performed on high alerts and initiated based on the clients' subscription type.

- **Proactive subscription** – When a high alert is detected, Spectrum Enterprise will automatically begin DDoS Protection. Clients will receive a notification that the DDoS Protection has begun and a second notification when the DDoS Protection has ended.
- **Reactive subscription** – When a high alert is detected, Spectrum Enterprise will notify the client of a potential DDoS event. Clients will need to contact Spectrum Enterprise to begin DDoS Protection. Clients will receive a second notification when the DDoS Protection has ended.

NOTE: Clients without any DDoS events detected or mitigated during the 28-day period will have no data in the summary dashboards and / or graphs.

Threat Mitigation System (TMS) summary dashboard

The TMS summary dashboard provides statistics on the DDoS Protection performed by the Spectrum Enterprise DDoS Protection platform within the last 28 days and a measurement against the previous 28 days.



Security Summary

Time Period: month | Managed Objects: victim | Start: Jan 10 2024, 8:39 | End: Feb 7 2024, 8:39

TMS MITIGATION SUMMARY

This area provides an overview of the mitigations performed by all TMS devices in the deployment during the report period.

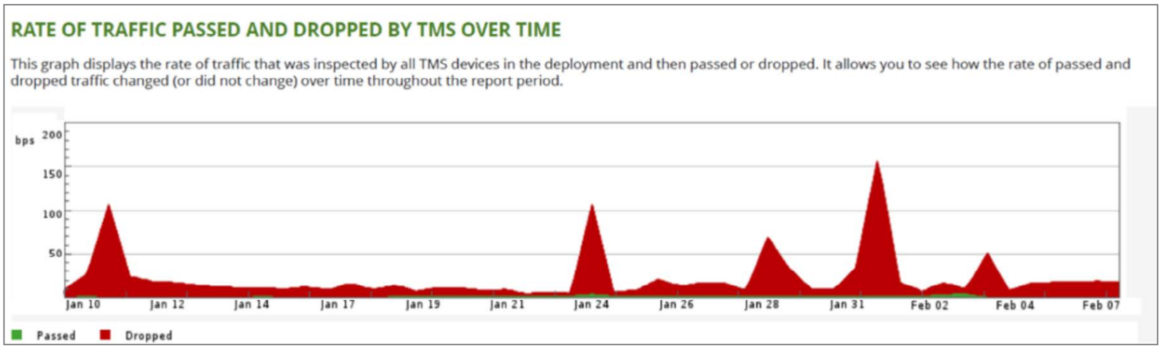
Number of TMS Mitigations	Volume of Traffic Passed by TMS	Volume of Traffic Dropped by TMS	Volume of Largest TMS Mitigation	Rate of Largest TMS Mitigation	Duration of Largest TMS Mitigation
4	4.0 GB	13.29.00 GB	6.65.00 GB	180.00 bps	2d 6h 12m
⬆700.00%	⬇12.09%	⬇14.32%	⬇23.12%	⬆123.05%	⬆6.87%

Bottom row indicates increase or decrease from prior period (December 13 2023 8:39 - January 10 2024 8:39). "—" is displayed when no data exists in prior period.

- **Number of TMS** – Count of DDoS events that required mitigation.
- **Volume of traffic passed by TMS** – Amount of traffic analyzed for DDoS events. This will be equal to or less than the bandwidth of the circuit being monitored for DDoS activity.
- **Volume of traffic dropped by TMS** – Amount of DDoS traffic that was identified and scrubbed by Spectrum Enterprise DDoS Protection.
- **Volume of largest TMS mitigation** – Size of the largest DDoS Protection event.
- **Rate of largest TMS mitigation** – Speed of the largest DDoS Protection event.
- **Duration of longest TMS mitigation** – Mitigation time of longest DDoS Protection event.

Rate of traffic passed and dropped by TMS over time

The rate of traffic / passed over time graph shows the traffic passed (green) and dropped (red) over the previous 28 days. Spikes in traffic (red) indicate when a DDoS event occurred.



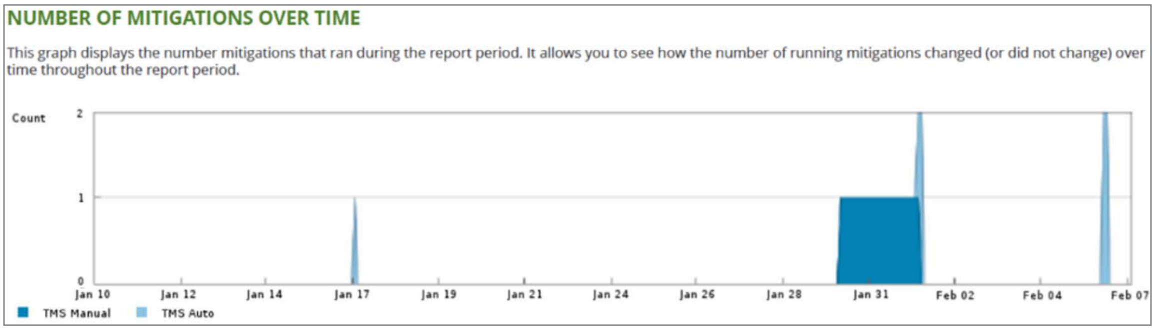
RATE OF TRAFFIC PASSED AND DROPPED BY TMS OVER TIME

This graph displays the rate of traffic that was inspected by all TMS devices in the deployment and then passed or dropped. It allows you to see how the rate of passed and dropped traffic changed (or did not change) over time throughout the report period.

The largest spike in this graph will correlate to the volume of traffic dropped by TMS in the TMS summary dashboard.

Number of mitigations over time

The mitigations over time graph indicates the type (manual or auto) of mitigation that occurred over the previous 28 days.



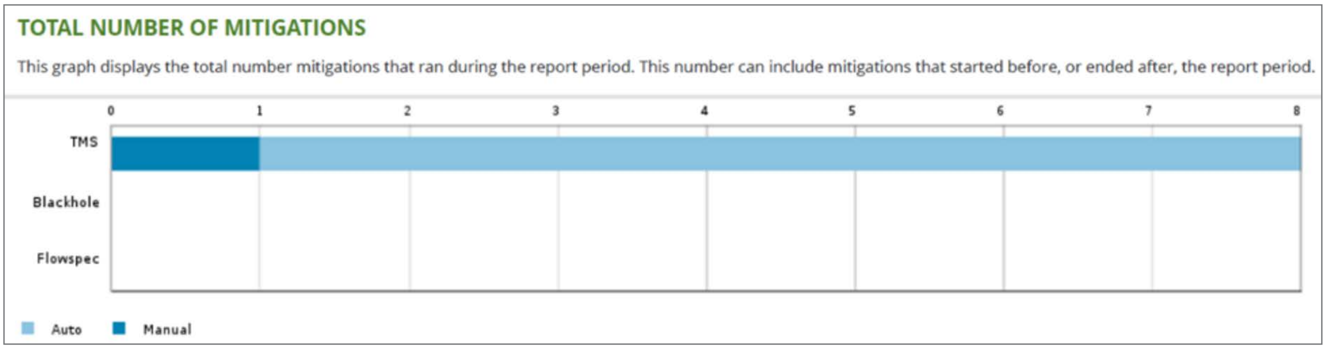
NUMBER OF MITIGATIONS OVER TIME

This graph displays the number mitigations that ran during the report period. It allows you to see how the number of running mitigations changed (or did not change) over time throughout the report period.

- Clients with proactive DDoS subscription will only have manual mitigation data if the client requested DDoS Protection.
- Clients with reactive DDoS will not have any auto mitigation data.

Total number of mitigations

The mitigations over time graph will display the total number of auto and manual mitigations over the previous 28 days. This should correlate to the number of mitigations displayed in the TMS mitigation summary dashboard.



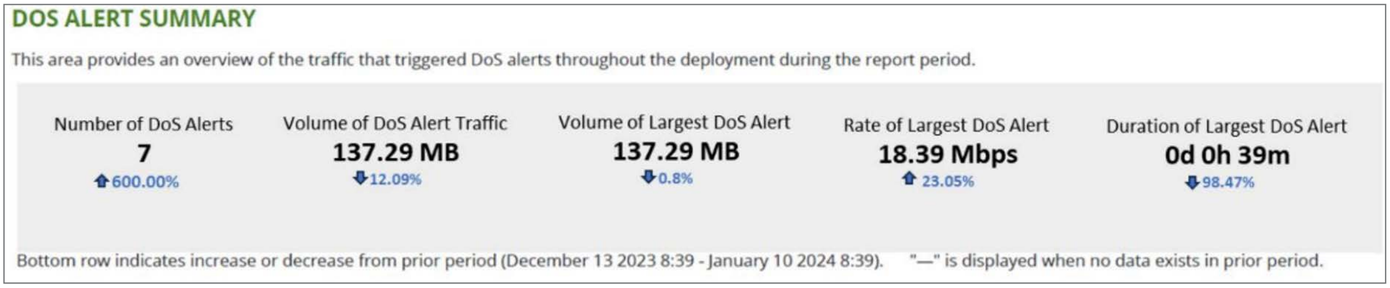
TOTAL NUMBER OF MITIGATIONS

This graph displays the total number mitigations that ran during the report period. This number can include mitigations that started before, or ended after, the report period.

- Blackhole is a countermechanism used to mitigate a DDoS attack where all traffic (malicious and legitimate) is dropped without informing the source that the data did not reach the intended recipient. Since suspicious traffic is only blackholed at the Spectrum Enterprise core / edge and never routed across a client's FIA circuit, this measurement will never display any data.
- Clients with proactive DDoS Protection subscription will only have manual mitigation data if the client requested DDoS Protection.
- Clients with reactive DDoS Protection will not have any auto mitigation data.
- Flowspec is a sample of the client's data that is collected and polled at regular intervals to monitor for potential DDoS activity. If DDoS activity is suspected through the flowspec monitoring, the flowspec data sample will be mitigated with all of the traffic on the clients monitored circuit.

DDoS alert summary

The DDoS alert summary dashboard provides statistics on DDoS alerts that were triggered by events within the monitored traffic within the last 28 days, as well as a measurement against the previous 28 days.



DOS ALERT SUMMARY

This area provides an overview of the traffic that triggered DoS alerts throughout the deployment during the report period.

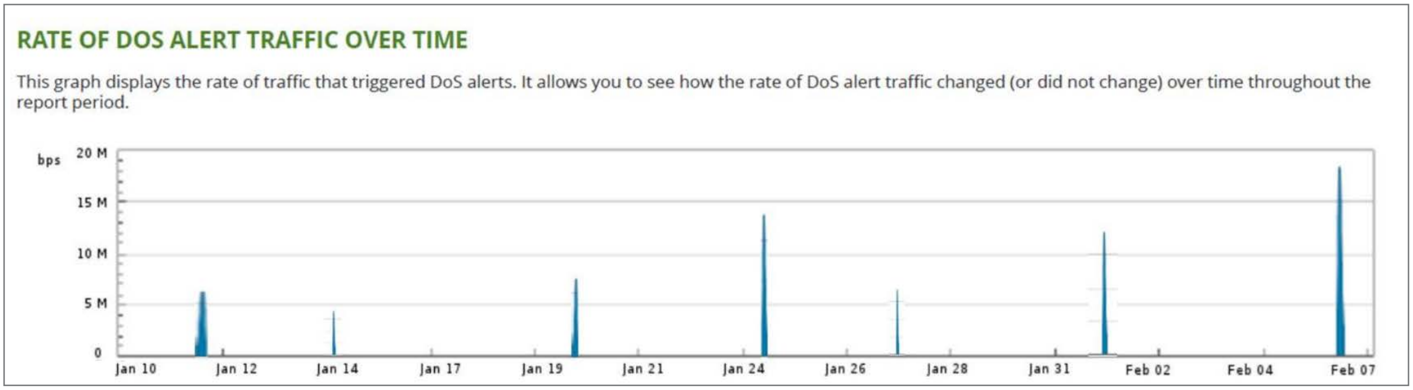
Number of DoS Alerts	Volume of DoS Alert Traffic	Volume of Largest DoS Alert	Rate of Largest DoS Alert	Duration of Largest DoS Alert
7	137.29 MB	137.29 MB	18.39 Mbps	0d 0h 39m
⬆600.00%	⬇12.09%	⬇0.8%	⬆23.05%	⬇98.47%

Bottom row indicates increase or decrease from prior period (December 13 2023 8:39 - January 10 2024 8:39). "—" is displayed when no data exists in prior period.

- **Number of DDoS alerts** – Count of all DDoS event that triggered DDoS alerts.
- **Volume of DDoS alert traffic** – Amount of DDoS alerts over the past 28 days.
- **Volume of largest DDoS alert**– Size of the largest DDoS alert.
- **Rate of largest DDoS alert** – Speed of the largest DDoS alert.
- **Duration of longest DDoS alert** – Longest DDoS alert (will be equal to longest DDoS mitigation).

Rate of DoS alert traffic over time

The rate of DoS alert traffic over time graph displays the rate of traffic that triggered any DDoS alert (high, medium, or low) over the previous 28 days. Spikes in traffic rates indicate a potential DDoS attack.

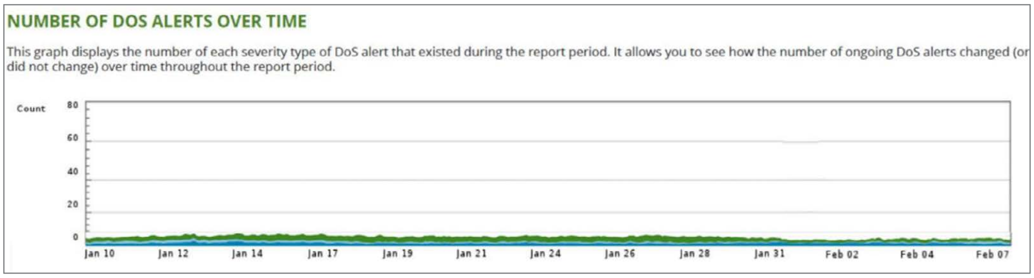


RATE OF DOS ALERT TRAFFIC OVER TIME

This graph displays the rate of traffic that triggered DoS alerts. It allows you to see how the rate of DoS alert traffic changed (or did not change) over time throughout the report period.

Number of DoS alerts over time

The number of DoS alerts over time graph displays the number of high, medium, and low alerts that were triggered over the previous 28 days.



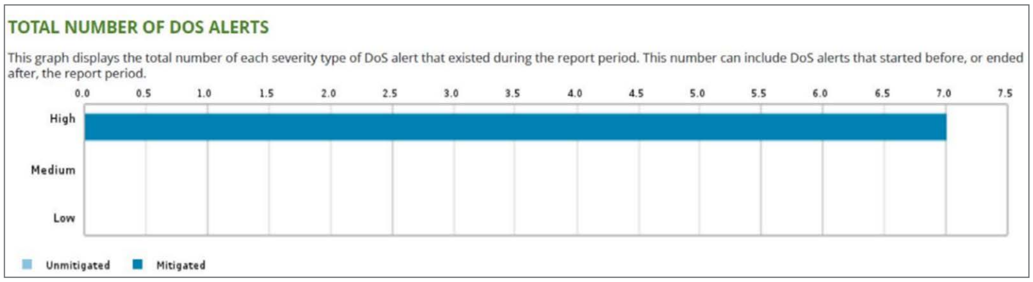
NUMBER OF DOS ALERTS OVER TIME

This graph displays the number of each severity type of DoS alert that existed during the report period. It allows you to see how the number of ongoing DoS alerts changed (or did not change) over time throughout the report period.

Clients are notified only when a high alert is detected. High alerts are considered business impacting. Medium / low alerts are monitored by Spectrum Enterprise, but clients are not notified of an event until the volume or duration of the event is high enough to impact access to business resources.

Total number of DoS alerts

The total number of DoS alerts graph displays the quantity of alerts for each alert type (high, medium, or low) as well as the quantity of each alert type that was mitigated or unmitigated.

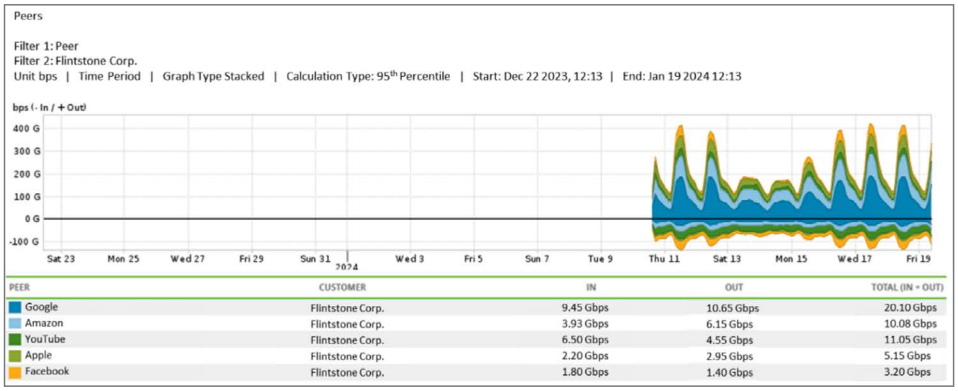


TOTAL NUMBER OF DOS ALERTS

This graph displays the total number of each severity type of DoS alert that existed during the report period. This number can include DoS alerts that started before, or ended after, the report period.

Peers summary

- The peers summary graph is a visual display of the top 5 traffic types traversing the service monitored for DDoS activity.
- The peers activity table displays the top 5 traffic types and volumes traversing the service monitored for DDoS activity.



Peers

Filter 1: Peer
Filter 2: Flintstone Corp.
Unit bps | Time Period | Graph Type Stacked | Calculation Type: 95th Percentile | Start: Dec 22 2023, 12:13 | End: Jan 19 2024 12:13

PEER	CUSTOMER	IN	OUT	TOTAL (IN + OUT)
🟦 Google	Flintstone Corp.	9.45 Gbps	10.65 Gbps	20.10 Gbps
🟦 Amazon	Flintstone Corp.	3.93 Gbps	6.15 Gbps	10.08 Gbps
🟩 YouTube	Flintstone Corp.	6.50 Gbps	4.55 Gbps	11.05 Gbps
🟩 Apple	Flintstone Corp.	2.20 Gbps	2.95 Gbps	5.15 Gbps
🟧 Facebook	Flintstone Corp.	1.80 Gbps	1.40 Gbps	3.20 Gbps

About Spectrum Enterprise

Spectrum Enterprise, a part of Charter Communications, Inc., is a national provider of scalable, fiber technology solutions serving many of America's largest businesses and communications service providers. The broad Spectrum Enterprise portfolio includes networking and managed services solutions: Internet access, Ethernet access and networks, Voice and TV solutions. The Spectrum Enterprise team of experts works closely with clients to achieve greater business success by providing solutions designed to meet their evolving needs. For more information, visit enterprise.spectrum.com.