

Getting started with the DDoS Mitigation and Reporting portal

November 2020

Contents

Signing in to the portal.....	3
DDoS Mitigation and Reporting dashboard	5
Navigating Through the DDoS Mitigation portal.....	7
Clicking through.....	7
Using the navigation bar	9
Reports	11
Additional resources.....	14

Signing in to the portal

Your Lumen® DDoS Mitigation service comes with a portal containing an extensive set of dashboards and reports. Use this guide to acquaint yourself with the information available and how to navigate through the various pages.

When your service was activated, you received an email with instructions on how to activate your portal account. To summarize, you should have access to the following things:

The link to the service: <https://globalview.centurylink.com> (changing to <https://globalview.lumen.com> in the near future)

Login credentials established during service activation:

- Username
- PIN
- The RSA SecurID app – available from your app store
- A token for the RSA Secure

Each user has a unique username and will use an auto-generated token for the password, combined with a PIN that you specify. You will need access to the RSA token-generation app that can be found at your app store.

Once you have your username, PIN and RSA token app, you are ready to sign in. When you click the portal link you will be provided with the following dialog.

Your Unique User Name

Welcome to Lumen®
Authorized Users Only

Username

Password

Log In

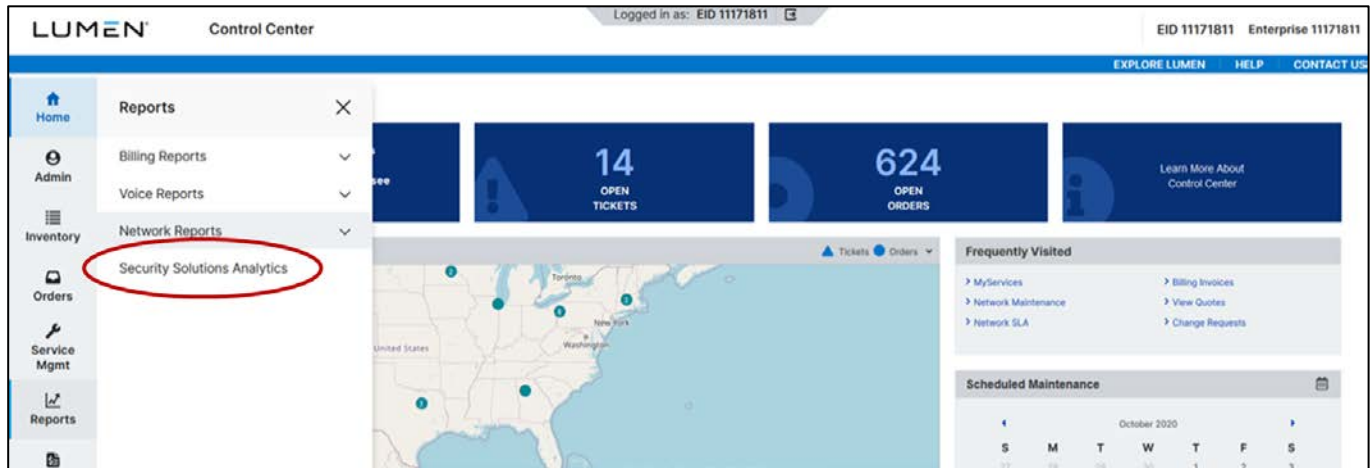
XXXXYYYYYYY

XXXX: Your unique PIN
YYYYYY: RSA Token Code

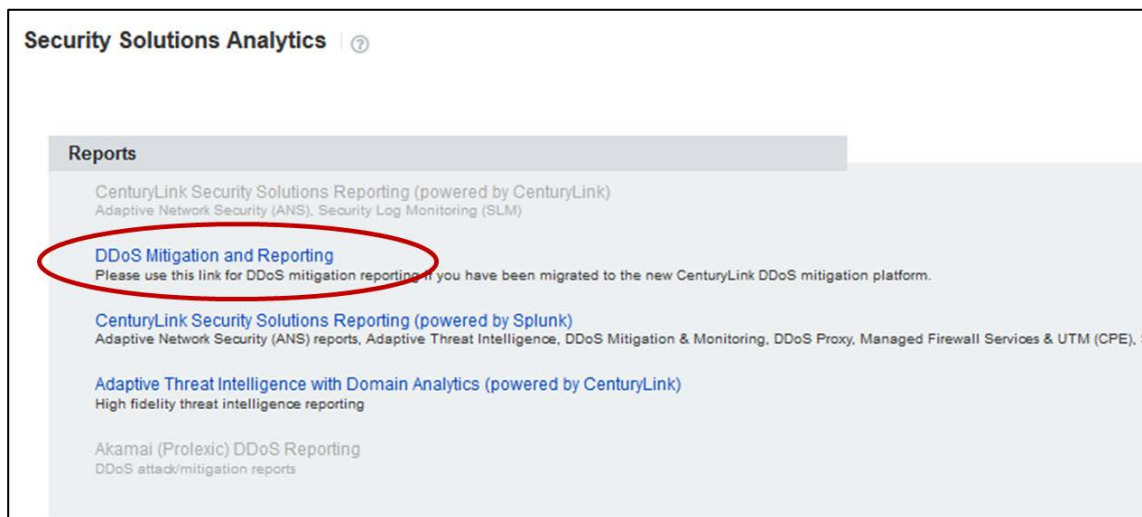
Enter your unique username in the top box. Your password will be the 4-digit PIN number you have established concatenated with the number generated by the RSA token app.

Once logged in, you have access to all the DDoS Mitigation portal information that is applicable to your business.

If you are already signed in to Control Center, you can navigate to the DDoS Mitigation portal by clicking **Reports**, then select **Security Solutions Analytics**.



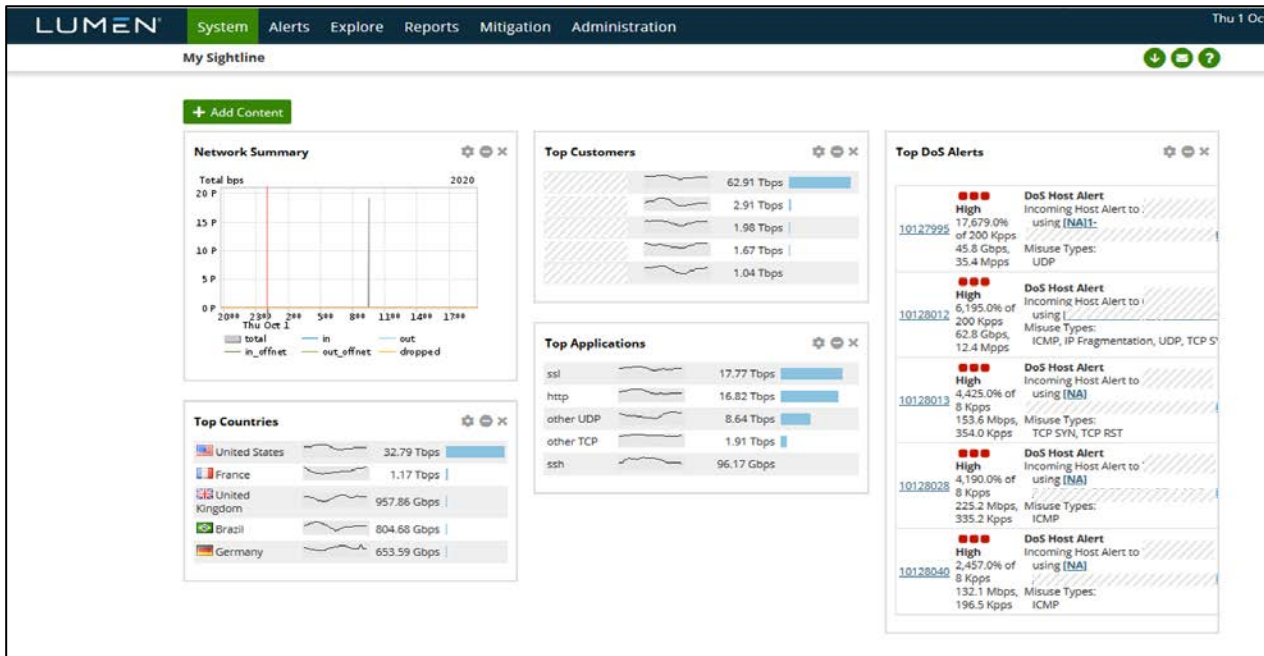
From the Security Solutions Analytics page, select **DDoS Mitigation and Reporting**.



You will need to sign in to the DDoS Mitigation and Reporting portal separately as described above, using your unique username, RSA PIN and RSA token-generated code.

DDoS Mitigation and Reporting dashboard

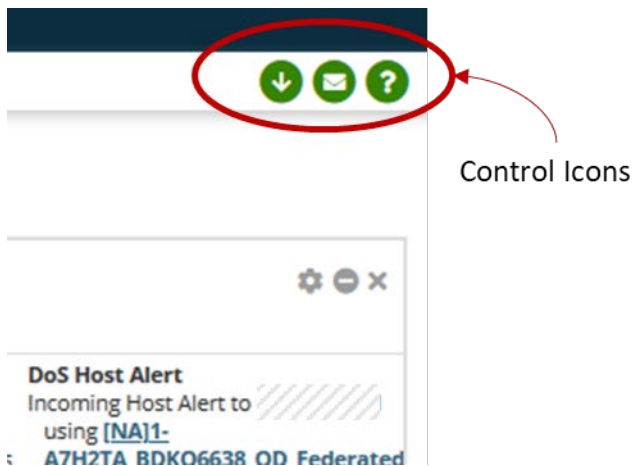
When you sign in, the first page that appears in the DDoS Mitigation and Reporting dashboard:



Many of the widgets on this page have “drill down” capabilities. To focus in on the per country data, for instance, click on the widget to get a more comprehensive data. Of note is the Top DDoS Alerts widget, where clicking on any entry in the widget will bring up details of that alert.

This dashboard is highly customizable. Click the “Add Content” button in the upper-right to add more widgets to this page.

In the upper-right, note three control icons, illustrated below.



The down-arrow icon is used to download this page to a PDF document. The mail icon is used to mail an image of the page. The question mark icon brings up an extensive, detailed online manual for the entire portal. Please note that not all features described in the manual are available to you as a user. A snapshot is below.

NETSCOUT | Arbor Sightline and Threat Mitigation System Search All

Contents | Index

- > Preface
- > Sightline and TMS User Guide
 - > Introduction to Sightline and TMS
 - > System Administration
 - > Configuring Sightline Appliances
 - > Configuring Sightline to Learn about Y
 - > Configuring Monitored Network Device
 - > Configuring Managed Objects
 - > Configuring Other Network Resources
 - > Configuring Notifications
 - > Configuring User Interface Settings
 - > Configuring User Accounts, Account C
 - > Configuring ATLAS Services
 - > Monitoring the System
 - ▣ **About the My Sightline Dashboard**
 - ▣ About Monitoring APS Cloud Signa
 - ▣ Monitoring Your Deployment
 - ▣ About the Appliance Status Page
 - ▣ Viewing General Appliance Statist
 - ▣ Viewing Web UI Statistics
 - ▣ Viewing Managed Services UI Stal
 - ▣ Viewing TMS Appliance Statistics
 - ▣ Monitoring Your Arbor Networks Ap
 - ▣ About the Summary Tab on the Ap
 - ▣ About the Per Appliance Metrics Ta
 - ▣ About the Metric Comparison Tab
 - ▣ Viewing ArborFlow Statistics
 - ▣ Monitoring Account Status

For information about capabilities, see [Configuring Capability Groups](#).

> **Default content of your My Sightline dashboard**
By default, your My Sightline dashboard contains the following gadgets:

My Sightline dashboard default gadgets

Gadget	Description
<i>Introduction</i>	A welcome gadget that describes how to use and customize the My Sightline dashboard.
<i>Top DoS Alerts</i>	A summary of the top five ongoing DoS alerts on the network. Only high or medium alerts are displayed.
<i>Network Summary</i>	A summary of your network's traffic over the last 24 hours.
<i>Top Customers</i>	A summary of the top five customers consuming bandwidth on your network.
<i>Top Applications</i>	A summary of the top five applications detected in your network's traffic.
<i>Top Countries</i>	A summary of the top five countries consuming bandwidth on your network.

Note
IP Location data is only available when you deploy appliances that have the traffic and routing analysis role or Flow Sensor appliances with appliance-based licensing.

> **Adding content to your My Sightline dashboard**
To add content to your My Sightline dashboard:

1. Navigate to the My Sightline page (**System > My Sightline**).
2. Click **Add Content**.
3. Hover your mouse pointer over the gadget that you want to add, and then click **Add to Report**.
4. Repeat Step 3 for each gadget that you want to add, and then click **Hide**.

Navigating Through the DDoS Mitigation portal

There are a couple of key ways to navigate through this portal. Clicking through on clickable widgets will typically bring the user to specific information on the widget selected. Using the navigation bar is a quick way to get to specific spot in the portal.

Clicking through

Dashboard views are typically designed to give the user a general landscape of available information. Typically to make that information actionable, the user needs to get to something more specific. For example, on the DDoS Mitigation and Reporting portal landing page, there is a widget that contains the top DDoS Alerts. To get to something more specific, select an alert and click on the alert incident identifier associated with it as illustrated below.

The screenshot shows a widget titled "Top DoS Alerts" with three entries. Each entry is a "DoS Host Alert" with a "High" severity. The first entry has an incident ID of 10127995, which is circled in red. An arrow points from the text "Alert Incident ID" to this circled ID. The second entry has an incident ID of 10128012, and the third has 10128013. Each entry includes details such as "Incoming Host Alert to using [NA]1-", "Misuse Types", and traffic volume information.

Alert Incident ID	Severity	Alert Type	Details
10127995	High	DoS Host Alert	Incoming Host Alert to using [NA]1- Misuse Types: ICMP, IP Fragmentation, UDP 27,567.0% of 200 Kpps 77.3 Gbps, 55.9 Mpps
10128012	High	DoS Host Alert	Incoming Host Alert to using [Misuse Types: ICMP, IP Fragmentation, TCP RST, UD 6,195.0% of 200 Kpps 62.8 Gbps, 12.4 Mpps
10128013	High	DoS Host Alert	Incoming Host Alert to using [NA]1- Misuse Types: TCP SYN, TCP RST 4,726.0% of 8 Kpps 165.0 Mbps, 378.1 Kpps

This click will bring in all the detailed level information for the selected alert. A snapshot is below.

Duration: Oct 1 18:48 - Ongoing (3:27)
Explore with Insight
View Scratchpad (0)
Mitigate Alert

Summary | Traffic Details | Routers | Annotations

DETAILS | Period: Alert Timeframe | Units: pps | View: Network Boundary | Update

KEY INFORMATION

Severity Level	Max Severity Percent	Top Misuse Type	Max Impact of Alert Traffic	Direction	Misuse Types	Managed Object	Target
●●● High	27,967.0% of 200 Kpps	UDP	77.3 Gbps/55.9 Mpps at Managed Object Boundary	Incoming	ICMP, IP Fragmentation, UDP	[NA]1.A7H2T...	//////

[View Raw Flows](#)

ALERT TRAFFIC

Misuse Types

* Misuse Types Exceeding Trigger Rate

Loading

Alert Characterization

- Misuse Types: UDP (9) 100.00%
- Destination IP Addresses: 100.00%
- Protocols: udp (17) 100.00%
- Destination UDP Ports: 4501 100.00%
- Source Countries: United States 99.92%
- Source ASNs: NULL (0) 100.00%
- Destination ASNs: NULL (0) 100.00%

Packet Size Distribution

Top Traffic Patterns (last 5 min of selected timeframe)

[Download All Patterns](#)

	Source	Protocol	Flags	Src Port	Destination	Dest Port	Router	Alert Traffic
1.	//////	UDP	--	63147	//////	4501	//////	1.50 Mpps
2.	//////	UDP	--	62427	//////	4501	//////	214.30 Kpps
3.	//////	UDP	--	53462	//////	4501	//////	206.40 Kpps
4.	//////	UDP	--	58313	//////	4501	//////	179.73 Kpps
5.	//////	UDP	--	62132	//////	4501	//////	177.37 Kpps
6.	//////	UDP	--	51893	//////	4501	//////	175.20 Kpps
7.	//////	UDP	--	59711	//////	4501	//////	146.03 Kpps
8.	//////	UDP	--	63335	//////	4501	//////	114.03 Kpps
9.	Highly Distributed	UDP	--	1024 - 65535 (Dynamic)	//////	4501	//////	34.05 Kpps
10.	//////	UDP	--	63482	//////	4501	//////	11.40 Kpps

Top Interfaces

Interface	Router	Router Severity	Direction	Boundary	ASNs	Max Observed	Average Observed
<input type="checkbox"/> Untracked Aggregate Untrac...ace	//////	●●● High	IN	Network	28121	75.6 Gbps 55.3 Mpps	14.6 Gbps 9.2 Mpps
<input type="checkbox"/> Untracked Aggregate Untrac...ace	//////	●●● Low	IN	Network	28121	261.5 Mbps 162.1 Kpps	110.5 Mbps 54.5 Kpps

Recent Annotations

[View All Annotations](#)

Using the navigation bar

The navigation bar at the top of the screen brings the user to all the detailed pages in the portal. Hovering over the stop selection generates a dropdown to one of the many selections in each top category, as illustrated here.

The screenshot shows the LUMEN portal interface. The navigation bar at the top includes 'System', 'Alerts', 'Explore', 'Reports', 'Mitigation', and 'Administration'. The 'Alerts' menu is expanded, showing options: Summary, All Alerts, Ongoing, Activity Report, DoS, Smart, Fingerprints, Services, and System Error. A red circle highlights the 'Alerts' menu, and a red arrow points to the 'DoS' option. The dashboard displays several widgets: 'My Sightline' with an 'Add Content' button, 'Network Summary' with a line chart showing traffic from 2019 to 2020, 'Top Customers' with a bar chart, 'Top Applications' with a bar chart, and 'Top DoS Alerts' with a list of alerts. A footer note states 'Page generation took 2.79 seconds (Details)' and 'About'.

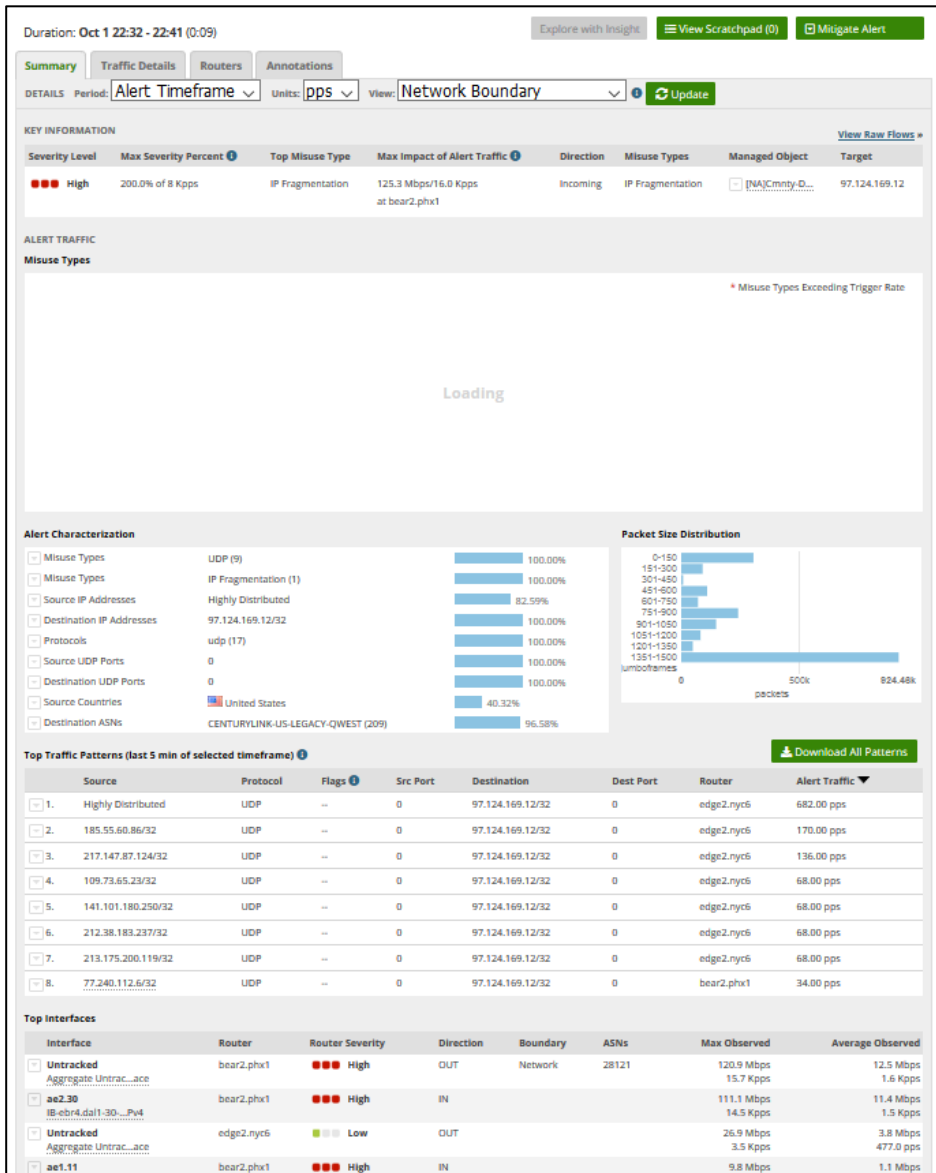
Navigation Bar with
Pulldown Selection

For assistance with this product, please contact DDoSOpsEng@centurylink.com. [About](#)

From this menu pulldown, we can select from a variety of Alert views. Selecting DoS will focus on Denial-of-Service alerts, shown here.

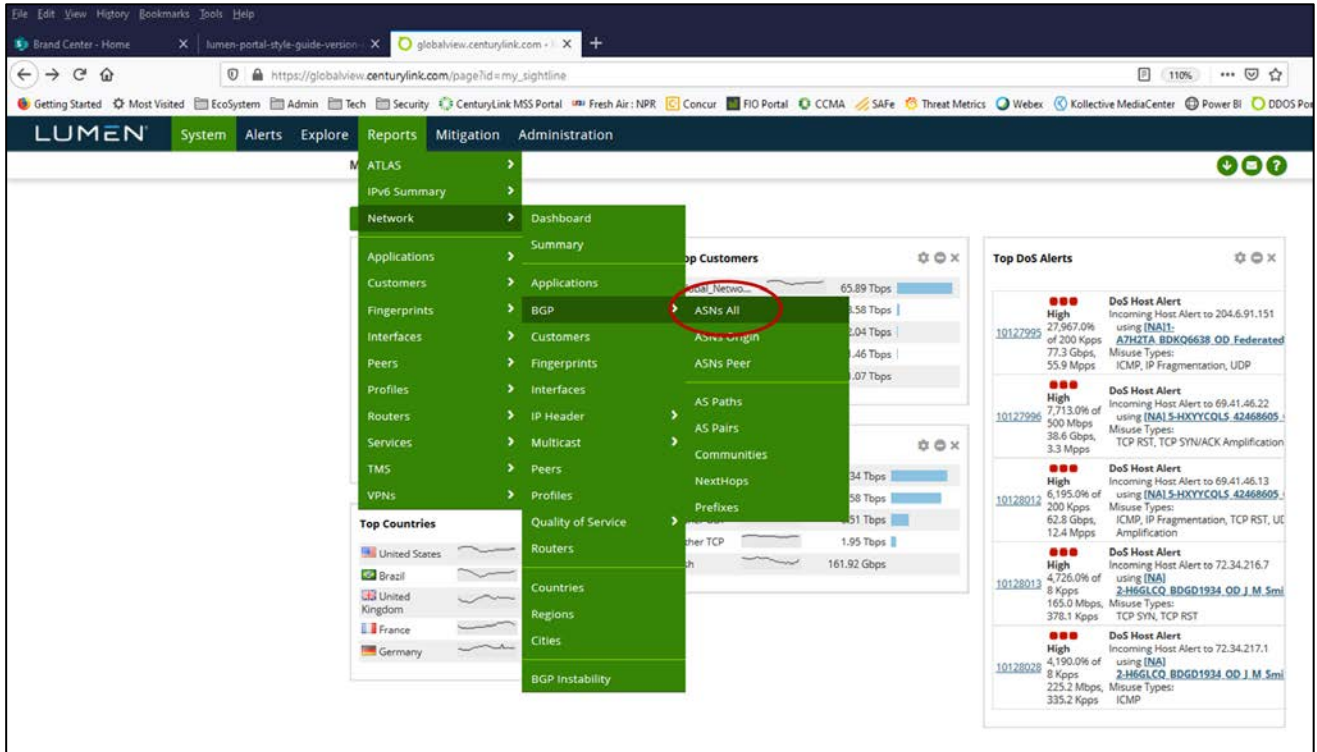
DoS Alerts					
ID ↓	Max Impact	Importance ⓘ	Alert	Start Time	Classification & Annotations
10128991	No Data	Low 25.0% of 8 Kpps 841.3 Kbps, 2.0 Kpps	DoS Host Alert Incoming Host Alert to 55.49.0.0 using ddos-23939295_DISA-BEF6_A Misuse Types: TCP SYN	Oct 1 22:34 - Ongoing (Less than 1 minute)	Possible Attack The "TCP SYN" host alert signature has been triggered at router "abx3-edge-01". (expected rate: 2.00 Kpps, observed rate: 2.02 Kpps) <i>(by auto-annotation)</i>
10128990	No Data	Medium 156.8% of 499.5 Mbps	DoS Alert Incoming IPv4 DoS Profiled Router Bandwidth Attack to S-FCTSXFMX.41794814_OD_HEALTH_AND_HUMAN_SERVICES_FBM	Oct 1 22:34 - Ongoing (0:01)	Possible Attack The alert was generated because the incoming expected rates have been exceeded (baseline: 34.15 Mbps, observed: 783.14 Mbps; baseline: 3.07 Kpps, observed: 65.35 Kpps) <i>(by auto-annotation)</i>
10128989	No Data	Medium 235.0% of 8 Kpps 169.7 Mbps, 18.8 Kpps	DoS Host Alert Incoming Host Alert to 75.174.250.168 using [NA]Cmnty-DSL-BOID Misuse Types: IP Fragmentation	Oct 1 22:34 - Ongoing (Less than 1 minute)	Possible Attack The "IP Fragmentation" host alert signature severity rate configured for "[NA]Cmnty-DSL-BOID" has been exceeded, changing Severity Level from low to medium (expected rate: 8.00 Kpps, observed rate: 18.78 Kpps) <i>(by auto-annotation)</i>
10128987	No Data	Low 77.0% of 8 Kpps 38.4 Mbps, 6.1 Kpps	DoS Host Alert Incoming Host Alert to 67.7.83.240 using [NA]Cmnty-DSL-FTMY Misuse Types: IP Fragmentation	Oct 1 22:33 - Ongoing (0:01)	Possible Attack The "IP Fragmentation" host alert signature has been triggered at router "bar3.tmp1". (expected rate: 2.00 Kpps, observed rate: 6.12 Kpps) <i>(by auto-annotation)</i>
10128985	No Data	Medium 200.0% of 8 Kpps 125.3 Mbps, 16.0 Kpps	DoS Host Alert Incoming Host Alert to 97.124.169.12 using [NA]Cmnty-DSL-PHN4 Misuse Types: IP Fragmentation	Oct 1 22:32 - Ongoing (0:02)	Possible Attack The "IP Fragmentation" host alert signature severity rate configured for "[NA]Cmnty-DSL-PHN4" has been exceeded, changing Severity Level from low to medium (expected rate: 8.00 Kpps, observed rate: 16.00 Kpps) <i>(by auto-annotation)</i>

Now we can use the “click through” method to get the details on a single alert, as shown.

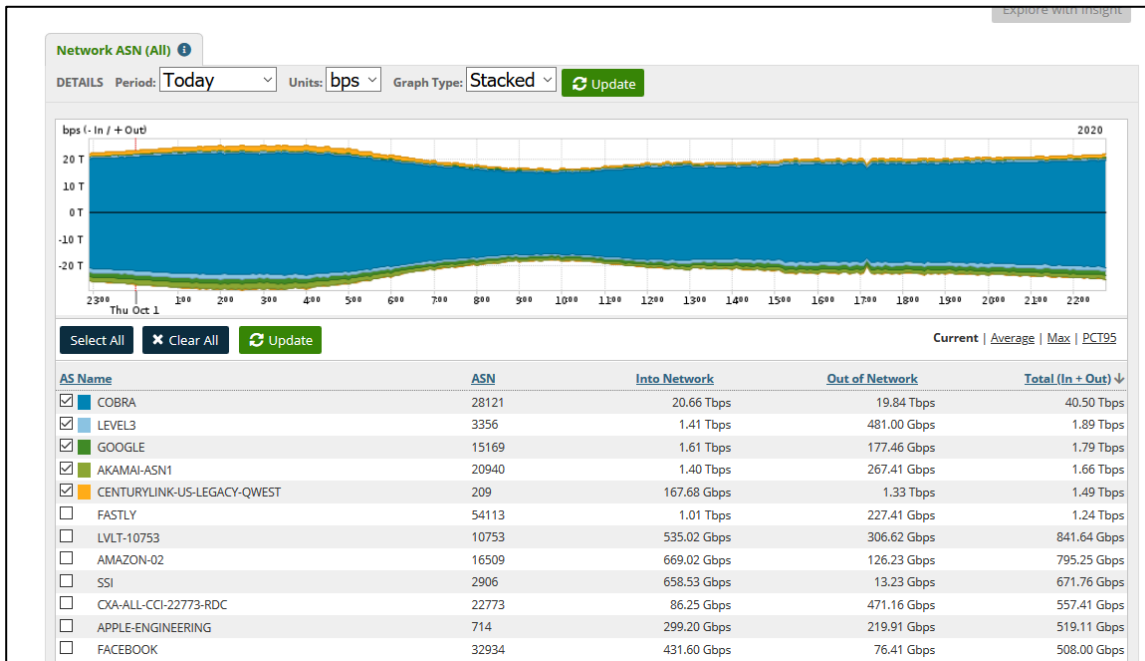


Reports

The DDoS Mitigation and Reporting portal has many reports to choose from. Hovering over “Reports” in the navigation bar reveals numerous selections, many of which have sub-selections. In this example, we start with Network and drill down to select All ASNs by selecting the following path Reports > Network > BGP > All ASNs as shown here.



This selection brings up the following report which illustrates the amount of traffic traversing your network from other ASNs, as depicted below.



For this next example, select a report via the path Reports->Applications->Countries as follows.

The screenshot shows the Lumen GlobalView interface. The navigation menu is open, highlighting the path: Reports > Applications > Countries. The main content area displays a traffic report for a selected application. The report includes a stacked area chart showing traffic volume over time (from 800 to 2200) and a table summarizing network-boundary traffic by external country of origin.

AS Name	ASIN	Into Network	Out of Network	Total (In + Out)
<input checked="" type="checkbox"/> COBRA	28121	20.66 Tbps	19.84 Tbps	40.50 Tbps
<input checked="" type="checkbox"/> LEVEL3	3356	1.41 Tbps	481.00 Gbps	1.89 Tbps
<input checked="" type="checkbox"/> GOOGLE	15169	1.61 Tbps	177.46 Gbps	1.79 Tbps
<input checked="" type="checkbox"/> AKAMAI-ASN1	20940	1.40 Tbps	267.41 Gbps	1.66 Tbps
<input checked="" type="checkbox"/> CENTURYLINK-US-LEGACY-4	209	167.68 Gbps	1.33 Tbps	1.49 Tbps
<input type="checkbox"/> FASTLY	54113	1.01 Tbps	227.41 Gbps	1.24 Tbps
<input type="checkbox"/> LVL1-10753	10753	535.02 Gbps	306.62 Gbps	841.64 Gbps

This selection brings up the following report which displays the amount of network-boundary traffic that flows into or out of a selected application, by external country of origin as shown herein.

Additional resources

The DDoS Mitigation and Reporting portal offers excellent visibility into your DDoS Mitigation service. Make sure to use the Help selection often by selecting the “?” icon in the upper-right of every page for detailed descriptions of each page.

Additional information on DDoS Mitigation and other products can be found at the following locations

Lumen Security Solutions: <https://www.lumen.com/en-us/solutions/connected-security.html>

DDoS Mitigation and Application Security: <https://www.lumen.com/en-us/security/ddos-and-web-application.html>

Black Lotus Labs, the Lumen Threat Research Lab: <https://www.lumen.com/en-us/security/black-lotus-labs.html>

Lumen Product Finder: <https://www.lumen.com/en-us/resources/product-finder.html>

Sign in to your Command Center account here: <https://business-signin.centurylink.com/oxauth/business/login.htm>

All things Lumen: www.lumen.com