

# DDoS Portal Overview

CenturyLink Technology Solutions  
Managed Security Services

# Table of Contents

<b>Access.....</b>	<b>3</b>
Status Screen.....	3
<b>Traffic .....</b>	<b>4</b>
Traffic → Summary → Application.....	4
Traffic → Summary → Ports → TCP .....	5
Traffic → Summary → Protocols.....	6
Traffic → Summary → Top Talkers .....	7
Traffic → Profiles → Profile Details.....	8
<b>Alerts .....</b>	<b>9</b>
Alert Summary.....	10
Alert Traffic Details .....	11
DDoS Alert Traffic Details – Summary .....	12
DDoS Alert Traffic Details – Source and Destination Addresses.....	13
DDoS Alert Traffic Details – Source and Destination Ports.....	14
DDoS Alert Traffic Details – Protocol Details .....	15
ACL Generation from an Alert .....	16
<b>Mitigation .....</b>	<b>17</b>
TMS Mitigation Status – Summary .....	18
TMS Mitigation Status – Countermeasures .....	19
<b>Administration.....</b>	<b>22</b>
My Account .....	22
Administration → User Accounts .....	22

# DDoS Portal Overview

This document presents an introduction to the major features in the customer portal for the CenturyLink Technology Solutions DDoS Mitigation service implemented on the Arbor Peakflow SP system.

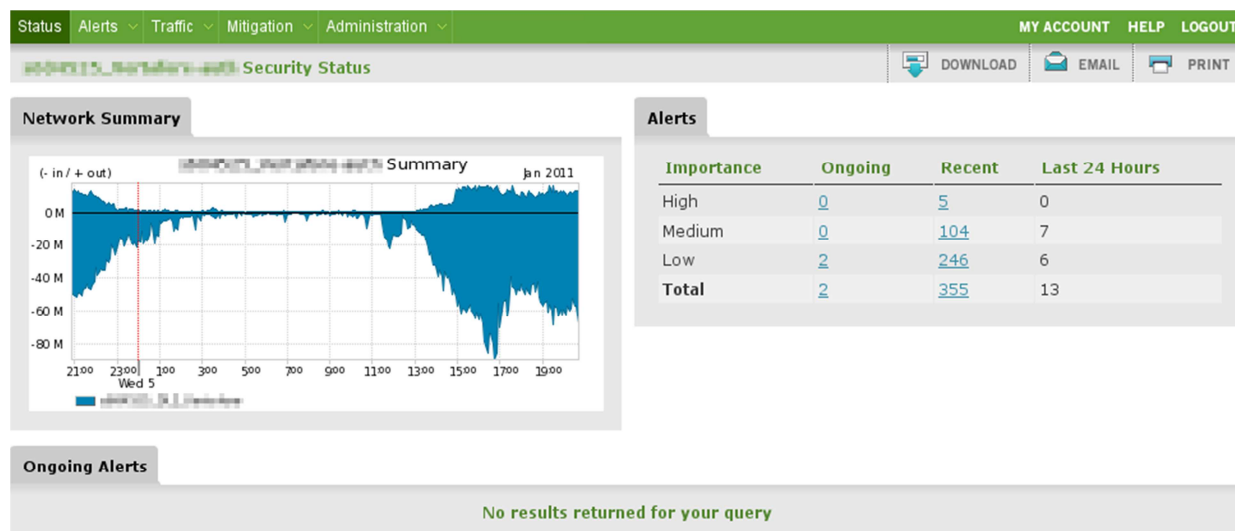
## Access

The DDoS portal is loosely integrated with the SavvisStation portal. Subscribers to the CenturyLink Technology Solutions DDoS Mitigation service will be presented with a link on the Security page of their SavvisStation account that leads to the Arbor-based portal. The Arbor portal can be accessed directly, without using SavvisStation, at <https://adms.savvis.net/>.

Because it is a separate implementation on a third-party device, access to the Arbor-based DDoS portal requires a second login that is distinct from the SavvisStation login.

## Status Screen

Upon successful login, the customer is presented with a status summary view:



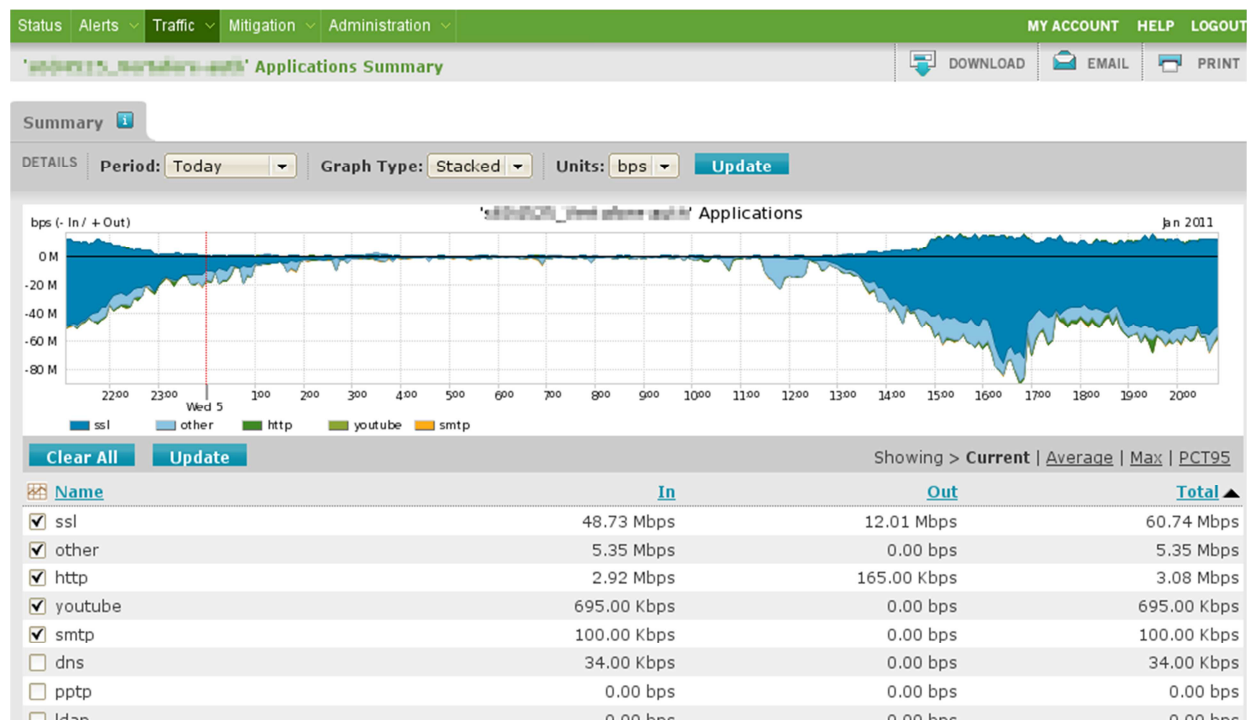
Navigating by means of the top menu bar, portal customers can examine characteristics of their network traffic at any time, independent of DDoS events and alerts. Alerts can be examined through the menu bar or from the Alerts panel in the Status page.

Traffic into and out of the customer network appears on the left of the Status screen. On the right a summary of current and recent DDoS alerts is presented. Any active alerts show below. This example has no active alerts.

## Traffic

### Traffic → Summary → Application

The Peakflow system displays a summary of the traffic for all monitored networks of the customer broken down by application:

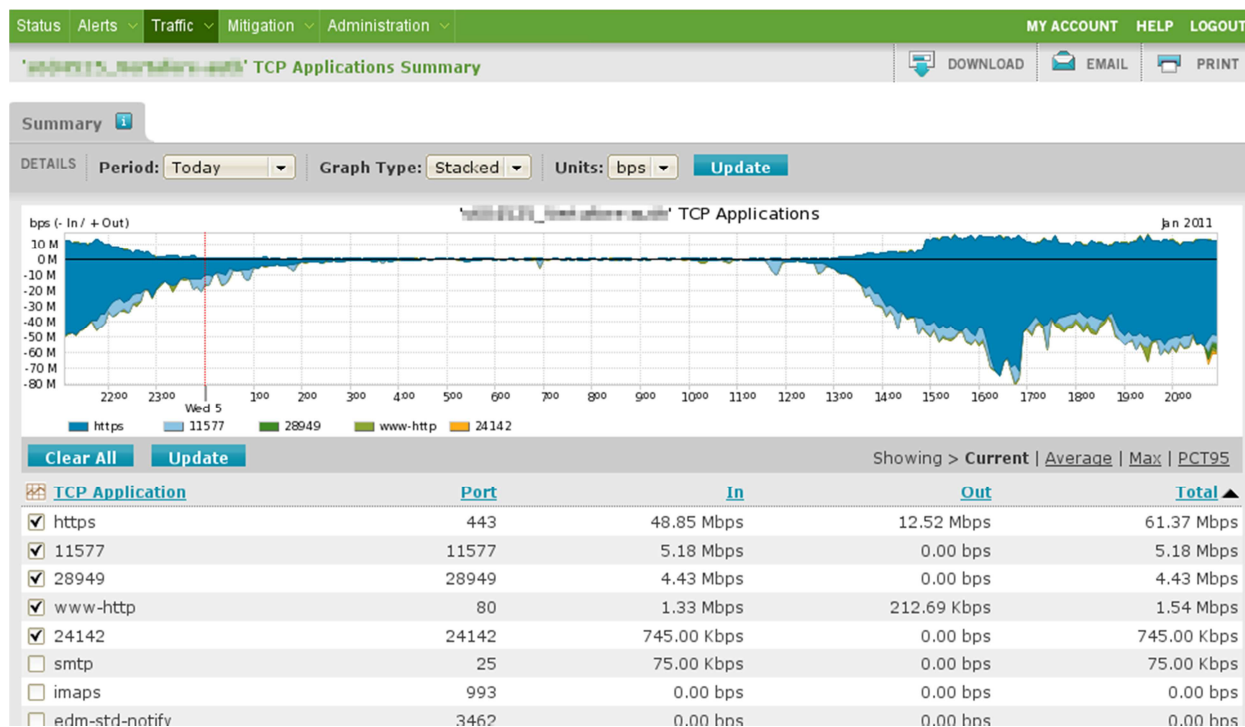


The default period is the previous 24 hours. The period can be changed to various predefined selections or to “other” for a user-defined timeframe. The default display is bits per second (bps) but can be changed to packets per second (pps). Available graph types are Stacked (default, shown), Pie, and Bar.

Any selected applications are shown in the graph with a unique color; any unchecked applications are not represented in the graph. The table can be sorted by clicking on a column header. Click the column header again to reverse the order.

## Traffic → Summary → Ports → TCP

Very similar to the Applications report, this screen constrains the report to TCP traffic broken down by TCP port:



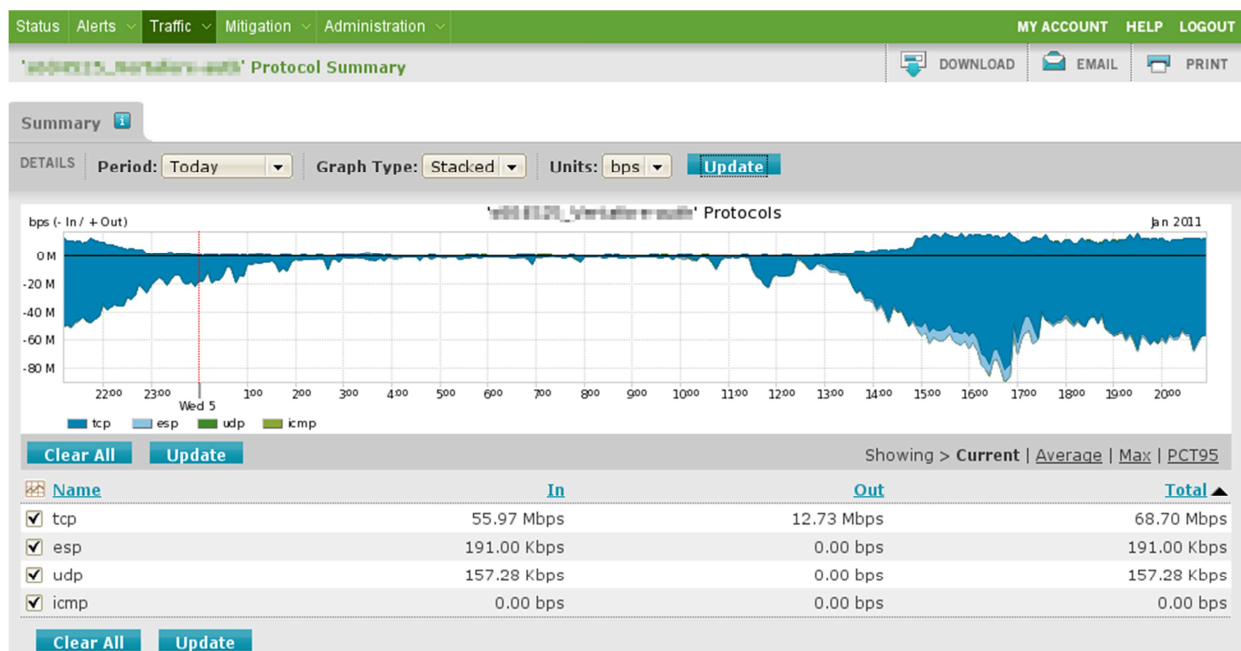
The default period is the previous 24 hours. The period can be changed to various predefined selections or to “other” for a user-defined timeframe. The default display is bits per second (bps) but can be changed to packets per second (pps). Available graph types are Stacked (default, shown), Pie, and Bar.

Any selected ports are shown in the graph with a unique color; any unchecked ports are not represented in the graph. The table can be sorted by clicking on a column header. Click the column header again to reverse the order.

There is a similar report for UDP ports that looks and behaves identically, constraining the report to UDP traffic aggregated by UDP port.

## Traffic → Summary → Protocols

This screen breaks down the customer's traffic by IP-level protocol:



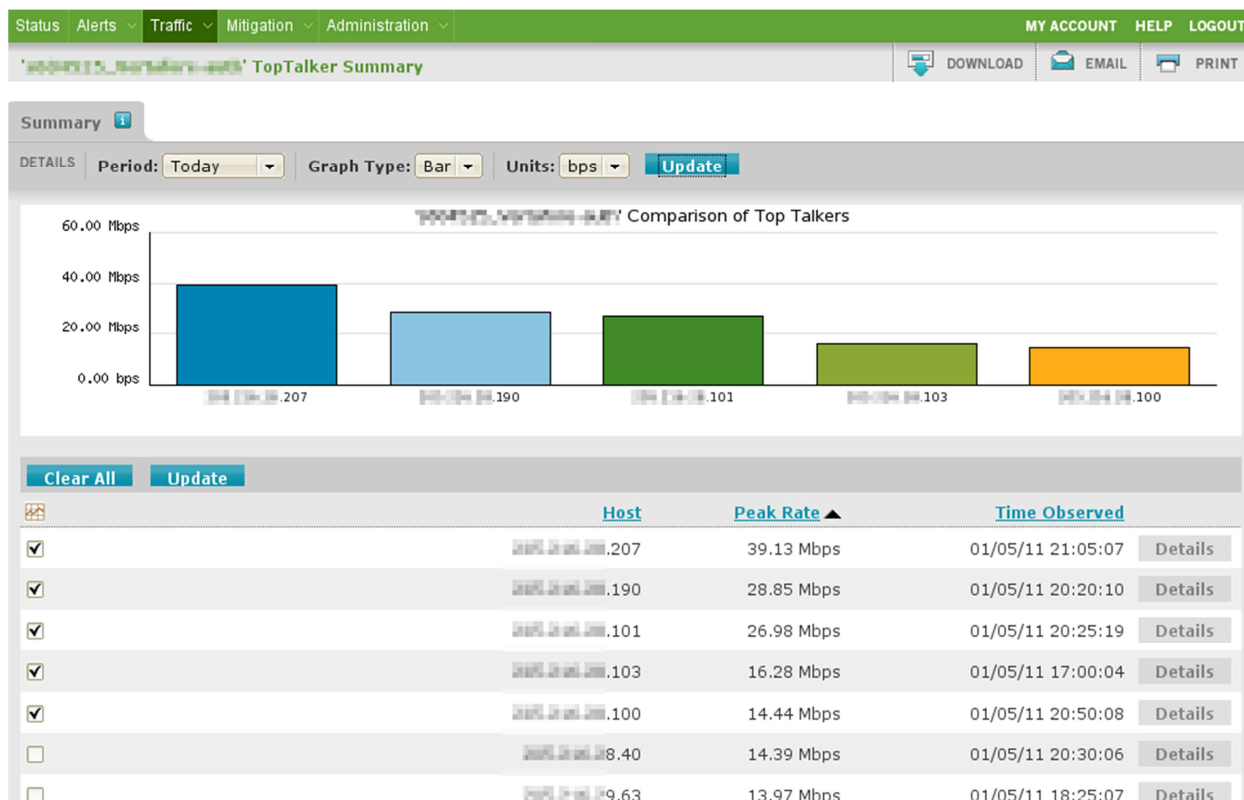
Those shown here, TCP, ESP (for VPN traffic), UDP, and ICMP are the most likely to be seen. This screen is very similar in appearance and function to those discussed previously:

The default period is the previous 24 hours. The period can be changed to various predefined selections or to "other" for a user-defined timeframe. The default display is bits per second (bps) but can be changed to packets per second (pps). Available graph types are Stacked (default, shown), Pie, and Bar.

Any selected protocols are shown in the graph with a unique color; any unchecked protocols are not represented in the graph. The table can be sorted by clicking on a column header. Click the column header again to reverse the order.

## Traffic → Summary → Top Talkers

This screen identifies the systems generating the most traffic in the customer's environment that traverses the CenturyLink Technology Solutions network:



The period is selectable from a pre-defined list. The graph type can be Bar (default) or Pie. Units can be bits per second (default) or packets per second.

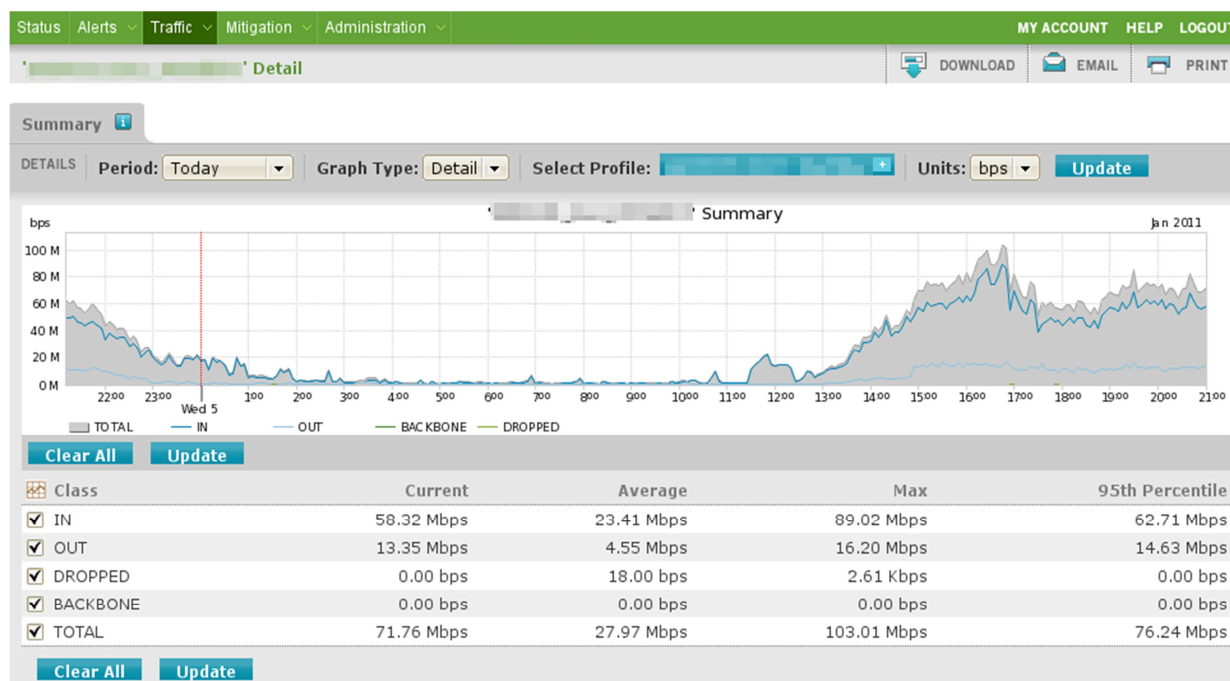
For each of the top-ranked hosts, the time and rate of their individual peak rate is shown. Those hosts that are checked are shown on the graph with a unique color. Those hosts left unchecked are not shown in the graph.

If the DNS name of host can be resolved it is shown to the left of the IP address. None of the addresses in the example above can be resolved; if resolved, the name would appear in the blank space to the left of the address.

The table can be sorted by clicking on a column heading. The order of the sort can be reversed by clicking on the column heading a second time.

## Traffic → Profiles → Profile Details

The summary reports above are for all the networks being monitored for a given customer that are associated with the customer Arbor portal account. Customers with multiple profiles (a.k.a. “managed objects”, a.k.a. “zones”) can view traffic reports restricted to one specific profile with the options under Traffic → Profiles. This is a traffic summary report for one profile:



A different profile can be chosen from the selection box. The time period is selectable and customizable. Graph type can be Stacked (default), Pie, or Bar. Units can be bits per second (default) or packets per second. When any of these options is changed the Update button must be clicked.

Traffic shown as “dropped” is traffic reported as dropped by backbone routers, not by the Arbor TMS DDoS mitigation devices; this data is unrelated to DDoS mitigations.

Only those directions/categories of traffic checked in the table are shown in the graph.

Application, Ports, Protocols, and Top Talker reports, identical to those previously discussed but restrained to a specific profile, are available under the Traffic → Profiles menu. Most subscribers to the CenturyLink Technology Solutions DDoS mitigation service have a single profile, making these identical to the summary reports.



## Alerts

DDoS Alerts can be viewed under Alerts → All Alerts, or by clicking on the number of Ongoing or Recent alerts on the status page. Here is a page resulting from clicking on the number of recent high alerts:

Status	Alerts	Traffic	Mitigation	Administration	MY ACCOUNT HELP LOGOUT		
Alerts Recent					DOWNLOAD	EMAIL	PRINT
<input type="text"/>					Search	Wizard	5 results (0.42 seconds)
ID	Graph	Importance	Alert	Start Time	Classification & Annotations		
<a href="#">878059</a>		<b>High</b> 163.4 Mbps 14.5 Kpps	<b>DoS Alert</b> Incoming Profiled Bandwidth Attack to <a href="#">192.168.1.1</a>	2010 Dec 25 02:17 - 02:32 (0:15)	<b>Possible Attack</b>		
<a href="#">878055</a>		<b>High</b> 165.3 Mbps 14.6 Kpps	<b>DoS Alert</b> Incoming Profiled Protocol TCP Attack to <a href="#">192.168.1.1</a>	2010 Dec 25 02:10 - 02:36 (0:26)	<b>Possible Attack</b>		
<a href="#">851148</a>		<b>High</b> 32.0 Mbps 16.8 Kpps	<b>DoS Alert</b> Incoming Profiled Protocol TCP Attack to <a href="#">192.168.1.1</a>	2010 Nov 22 20:09 - 22:09 (2:00)	<b>Verified Attack</b> TMS mitigation 'DoS Alert 851148' stopped (53) (by auto-annotation)		
<a href="#">839534</a>		<b>High</b> 34.8 Mbps 14.3 Kpps	<b>DoS Alert</b> Incoming Profiled Protocol TCP Attack to <a href="#">192.168.1.1</a>	2010 Nov 8 17:40 - 21:54 (4:15)	<b>Possible Attack</b>		
<a href="#">839364</a>		<b>High</b> 46.1 Mbps 21.1 Kpps	<b>DoS Alert</b> Incoming Profiled Protocol TCP Attack to <a href="#">192.168.1.1</a>	2010 Nov 8 12:43 - 17:40 (4:58)	<b>Possible Attack</b>		

Alerts matching the selection criteria are listed up to 10 per page. They can be sorted in various ways by clicking on the column headers. The small graph shows the traffic rates for the affected destination IPs for the duration of the alert.

The Importance is assigned automatically by the Peakflow system based on various criteria.

The Alert details show the type of Alert (bandwidth, misuse, profiled, e.g.) and the name of the managed object (often called “zone” in CenturyLink Technology Solutions parlance) that is affected.

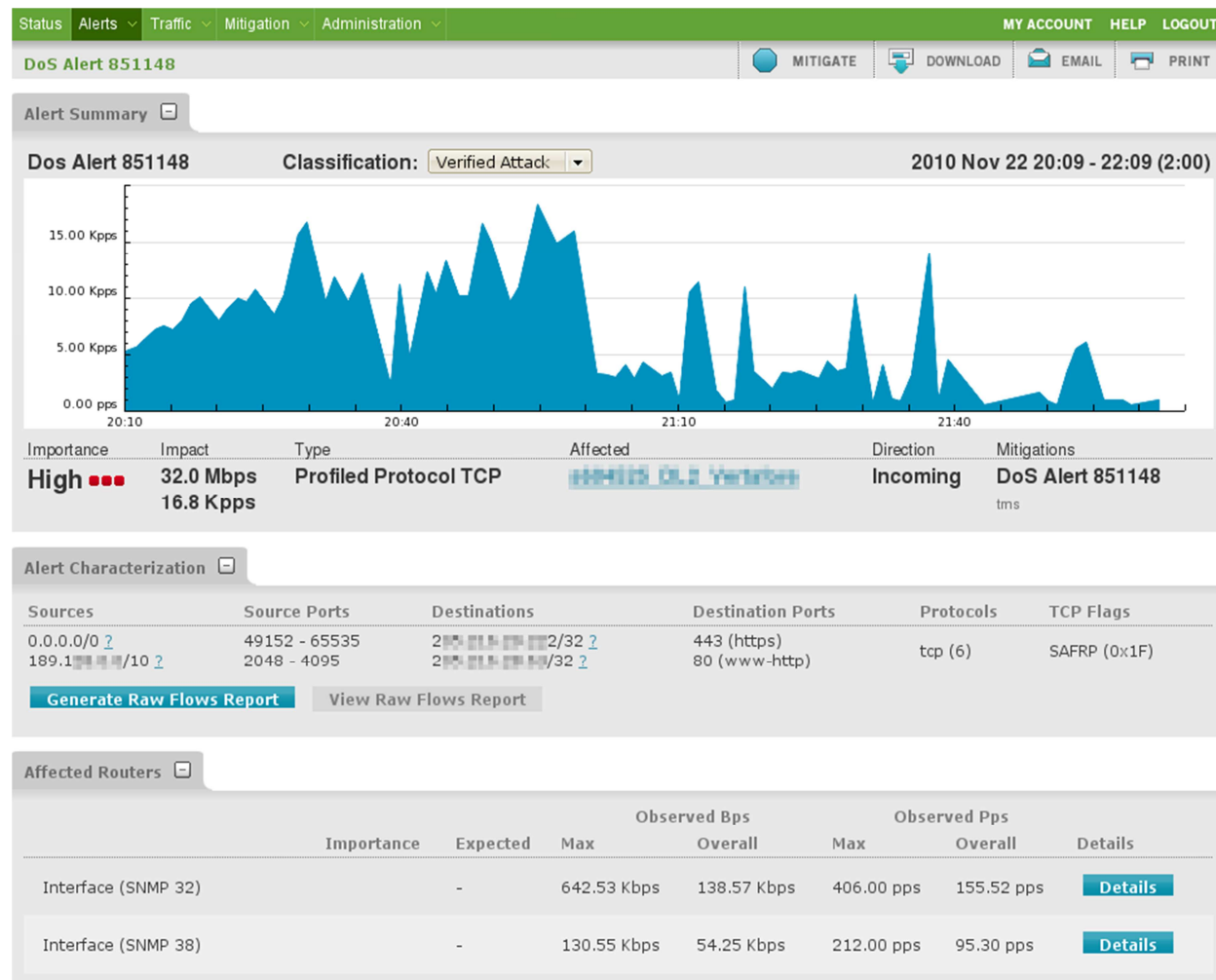
The start time and, if applicable, the end time of each alert is shown in the time zone configured for the portal account (defaults to UTC).

The Classification is initially assigned automatically by the Peakflow system as “Possible Attack”. This can be manually changed by operators to one of None, Flash Crowd, Network Failure, Trivial, or Verified Attack. This is for notational purposes only and has no effect on the operation of the system.

Annotations, shown with the Classification, display the last automatic or manual comment added to the alert. The third line above shows an example of an automatic comment added when a mitigation of that attack was initiated from the alert. (It is possible to initiate mitigations in other ways that don't associate the mitigation with the alert, in which case no annotation such as this would be created.)

## Alert Summary

An alert can be inspected by clicking on the alert ID number:



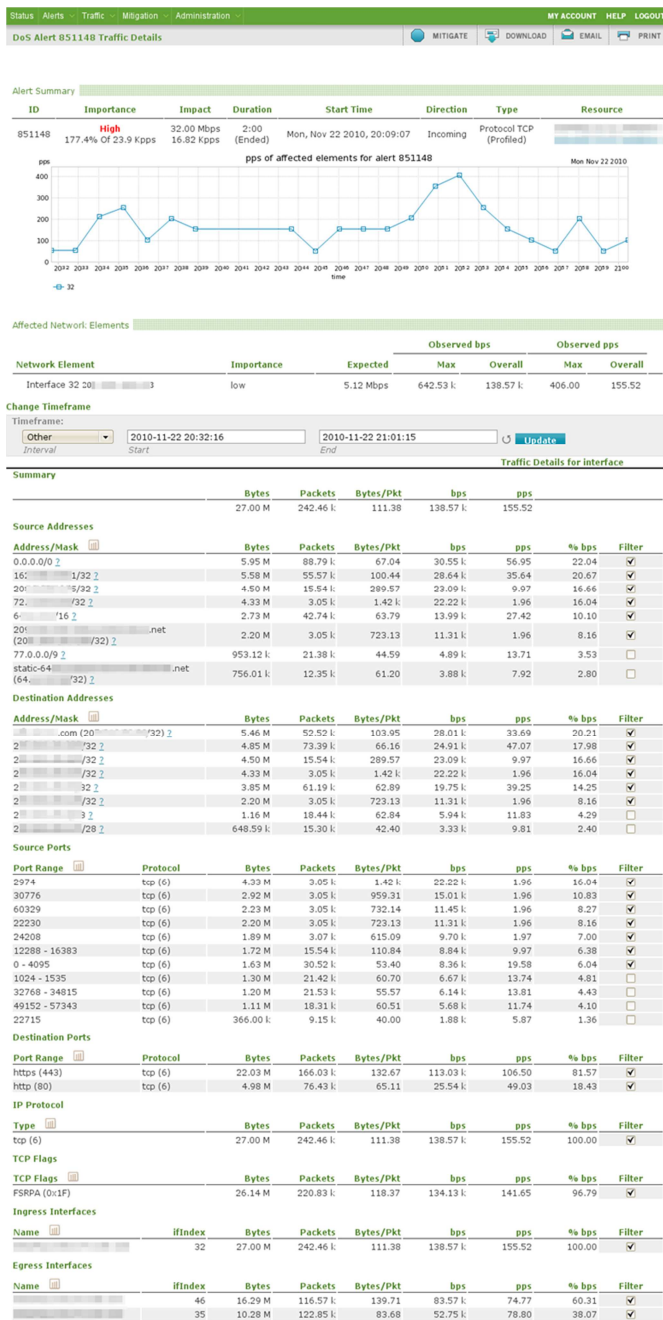
The graph shows the total traffic associated with the affected IPs during the alert along with some information about the alert, such as the data rates, the type of alert, and the affected profile. (Most customers have one profile, a.k.a. zone; some may have multiple.)

The Alert Characteristics panel shows the most relevant source and destination IPs, ports, and protocols. Protocol-appropriate information will also be shown, such as TCP Flags, ICMP codes, etc. The characteristics may be more or less specific, depending on the variation seen in the traffic. In this example, the source IPs are widespread on the Internet; some of the traffic has been narrowed down as coming from the same /10 network, but other traffic cannot be so categorized and is shown as coming from the Internet as a whole (0.0.0.0/0).

TCP Flags list those flags commonly being seen in the traffic flow. These are all normal flags; a SYN Flood, e.g., would likely list only flag "S" as it would predominate.

## Alert Traffic Details

More detail about the traffic generating a DDoS alert is available in the data from individual routers in the CenturyLink Technology Solutions backbone network. The list of affected interfaces on individual routers is shown on the Alert Summary page, and the detail coming from a specific interface is accessed with the Detail button for a specific interface: The detail contained in the different sections of this report is examined in detail in the following pages.

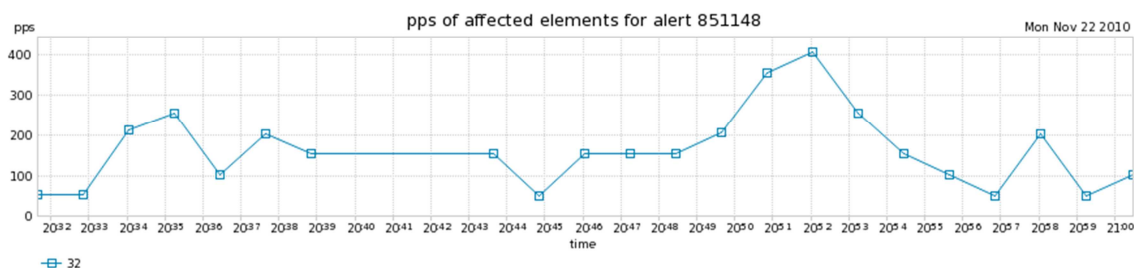


## DDoS Alert Traffic Details – Summary

The summary at the top of the Alert Details screen shows the amount of the customer's monitored traffic that traverses the selected router interface, along with some of the general attack characteristics from the alert summary screen:

### Alert Summary

ID	Importance	Impact	Duration	Start Time	Direction	Type	Resource
851148	<b>High</b> 177.4% Of 23.9 Kpps	32.00 Mbps 16.82 Kpps	2:00 (Ended)	Mon, Nov 22 2010, 20:09:07	Incoming	Protocol TCP (Profiled)	



### Affected Network Elements

Network Element	Importance	Expected	Observed bps		Observed pps	
			Max	Overall	Max	Overall
Interface 32 20 3	low	5.12 Mbps	642.53 k	138.57 k	406.00	155.52

### Change Timeframe

Timeframe:

Other

2010-11-22 20:32:16

2010-11-22 21:01:15

Interval

Start

End

Update

Traffic Details for interface



### Summary

Below the graph the amount of traffic seen vs. the amount of traffic expected. The expected rate is determined from normalized historic averages for Profiled alerts, and from configured thresholds for Misuse alerts. The example is a profiled traffic alert.

By default the entire history of the alert is shown. Different timeframes can be selected (first 10 minutes, last 10 minutes, last minute), or defined by the user ("Other"). More useful information can sometimes be had by examining just the peak of the attack, e.g., or sometimes details of what is happening right now may be more relevant to the task at hand. The details shown on the rest of the page always refer to only the timeframe that is used.

## DDoS Alert Traffic Details – Source and Destination Addresses

The source and destination IP addresses in the traffic are shown in the table with as much specificity as the Arbor Peakflow system can determine:

Traffic Details for interface							
Summary							
	Bytes	Packets	Bytes/Pkt	bps	pps		
	27.00 M	242.46 k	111.38	138.57 k	155.52		
Source Addresses							
Address/Mask 	Bytes	Packets	Bytes/Pkt	bps	pps	% bps	Filter
0.0.0.0/0 <a href="#">?</a>	5.95 M	88.79 k	67.04	30.55 k	56.95	22.04	<input checked="" type="checkbox"/>
16: <a href="#">/32</a> <a href="#">?</a>	5.58 M	55.57 k	100.44	28.64 k	35.64	20.67	<input checked="" type="checkbox"/>
20: <a href="#">/32</a> <a href="#">?</a>	4.50 M	15.54 k	289.57	23.09 k	9.97	16.66	<input checked="" type="checkbox"/>
72: <a href="#">/32</a> <a href="#">?</a>	4.33 M	3.05 k	1.42 k	22.22 k	1.96	16.04	<input checked="" type="checkbox"/>
6: <a href="#">/16</a> <a href="#">?</a>	2.73 M	42.74 k	63.79	13.99 k	27.42	10.10	<input checked="" type="checkbox"/>
20: <a href="#">.net</a> (20: <a href="#">/32</a> ) <a href="#">?</a>	2.20 M	3.05 k	723.13	11.31 k	1.96	8.16	<input checked="" type="checkbox"/>
77.0.0.0/9 <a href="#">?</a>	953.12 k	21.38 k	44.59	4.89 k	13.71	3.53	<input type="checkbox"/>
static-64: <a href="#">.net</a> (64: <a href="#">/32</a> ) <a href="#">?</a>	756.01 k	12.35 k	61.20	3.88 k	7.92	2.80	<input type="checkbox"/>
Destination Addresses							
Address/Mask 	Bytes	Packets	Bytes/Pkt	bps	pps	% bps	Filter
: <a href="#">.com</a> (20: <a href="#">/32</a> ) <a href="#">?</a>	5.46 M	52.52 k	103.95	28.01 k	33.69	20.21	<input checked="" type="checkbox"/>
2: <a href="#">/32</a> <a href="#">?</a>	4.85 M	73.39 k	66.16	24.91 k	47.07	17.98	<input checked="" type="checkbox"/>
2: <a href="#">/32</a> <a href="#">?</a>	4.50 M	15.54 k	289.57	23.09 k	9.97	16.66	<input checked="" type="checkbox"/>
2: <a href="#">/32</a> <a href="#">?</a>	4.33 M	3.05 k	1.42 k	22.22 k	1.96	16.04	<input checked="" type="checkbox"/>
2: <a href="#">/32</a> <a href="#">?</a>	3.85 M	61.19 k	62.89	19.75 k	39.25	14.25	<input checked="" type="checkbox"/>
2: <a href="#">/32</a> <a href="#">?</a>	2.20 M	3.05 k	723.13	11.31 k	1.96	8.16	<input checked="" type="checkbox"/>
2: <a href="#">/32</a> <a href="#">?</a>	1.16 M	18.44 k	62.84	5.04 k	11.87	4.20	<input type="checkbox"/>

Here, 22% of the traffic is coming from “the Internet” (0.0.0.0/0); i.e., from too many disparate addresses and networks to effectively aggregate in smaller netblocks. Of the remaining traffic, a considerable percentage is coming from 5 distinct hosts (/32) and two large netblocks (/16 and /9). Where resolution is successful, the DNS names for individual addresses are shown.

The targets of the traffic are a list of individual servers (/32) in the customer's network.

The sources and destinations which appear to the Arbor Peakflow system to be most relevant to the attack are automatically checked for “Filter”. All characteristics (sources, destinations, protocols, ports) that are checked can be used to generate a router ACL to drop that specific traffic. The ACL is displayed only – it is not automatically applied anywhere. CenturyLink Technology Solutions customers can use this to help generate an ACL to block undesired traffic on their own routers if that seems to be the best way to mitigate a low-bandwidth attack. (Large bandwidth attacks should always be mitigated in the CenturyLink network to prevent saturation of the link to the customer's network.)

An example ACL employing more elements from this alert is shown farther along in this document.

## DDoS Alert Traffic Details – Source and Destination Ports

The source and destination ports used are shown farther down in the details:

2	1.16 M	18.44 k	62.64	5.94 k	11.83	4.29	<input type="checkbox"/>
2	648.59 k	15.30 k	42.40	3.33 k	9.81	2.40	<input type="checkbox"/>

### Source Ports

Port Range	Protocol	Bytes	Packets	Bytes/Pkt	bps	pps	% bps	Filter
2974	tcp (6)	4.33 M	3.05 k	1.42 k	22.22 k	1.96	16.04	<input checked="" type="checkbox"/>
30776	tcp (6)	2.92 M	3.05 k	959.31	15.01 k	1.96	10.83	<input checked="" type="checkbox"/>
60329	tcp (6)	2.23 M	3.05 k	732.14	11.45 k	1.96	8.27	<input checked="" type="checkbox"/>
22230	tcp (6)	2.20 M	3.05 k	723.13	11.31 k	1.96	8.16	<input checked="" type="checkbox"/>
24208	tcp (6)	1.89 M	3.07 k	615.09	9.70 k	1.97	7.00	<input checked="" type="checkbox"/>
12288 - 16383	tcp (6)	1.72 M	15.54 k	110.84	8.84 k	9.97	6.38	<input checked="" type="checkbox"/>
0 - 4095	tcp (6)	1.63 M	30.52 k	53.40	8.36 k	19.58	6.04	<input checked="" type="checkbox"/>
1024 - 1535	tcp (6)	1.30 M	21.42 k	60.70	6.67 k	13.74	4.81	<input type="checkbox"/>
32768 - 34815	tcp (6)	1.20 M	21.53 k	55.57	6.14 k	13.81	4.43	<input type="checkbox"/>
49152 - 57343	tcp (6)	1.11 M	18.31 k	60.51	5.68 k	11.74	4.10	<input type="checkbox"/>
22715	tcp (6)	366.00 k	9.15 k	40.00	1.88 k	5.87	1.36	<input type="checkbox"/>

### Destination Ports

Port Range	Protocol	Bytes	Packets	Bytes/Pkt	bps	pps	% bps	Filter
https (443)	tcp (6)	22.03 M	166.03 k	132.67	113.03 k	106.50	81.57	<input checked="" type="checkbox"/>
http (80)	tcp (6)	4.98 M	76.43 k	65.11	25.54 k	49.03	18.43	<input checked="" type="checkbox"/>

### IP Protocol

Type	Bytes	Packets	Bytes/Pkt	bps	pps	% bps	Filter
------	-------	---------	-----------	-----	-----	-------	--------

Here, as is typically the case, the source ports are fairly random. It is interesting that 27% of the traffic is sourced from two specific TCP ports. That might indicate two very noisy hosts, and/or the use of unsophisticated attack software that does not randomize the source port.

The destination ports show that all the traffic is to the HTTP and HTTPS ports of the servers.

This section of the alert detail varies by the type of attack. This example is a TCP-specific alert. If it was a UDP attack, the UDP ports would be shown, of course. If it was an ICMP attack, the ICMP codes would be detailed.

## DDoS Alert Traffic Details – Protocol Details

Further details are shown depending on the type of traffic:

### Destination Ports

Port Range	Protocol	Bytes	Packets	Bytes/Pkt	bps	pps	% bps	Filter
https (443)	tcp (6)	22.03 M	166.03 k	132.67	113.03 k	106.50	81.57	<input checked="" type="checkbox"/>
http (80)	tcp (6)	4.98 M	76.43 k	65.11	25.54 k	49.03	18.43	<input checked="" type="checkbox"/>

### IP Protocol

Type	Bytes	Packets	Bytes/Pkt	bps	pps	% bps	Filter
tcp (6)	27.00 M	242.46 k	111.38	138.57 k	155.52	100.00	<input checked="" type="checkbox"/>

### TCP Flags

TCP Flags	Bytes	Packets	Bytes/Pkt	bps	pps	% bps	Filter
FSRPA (0x1F)	26.14 M	220.83 k	118.37	134.13 k	141.65	96.79	<input checked="" type="checkbox"/>

### Ingress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% bps	Filter
	32	27.00 M	242.46 k	111.38	138.57 k	155.52	100.00	<input checked="" type="checkbox"/>

### Egress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% bps	Filter
	46	16.29 M	116.57 k	139.71	83.57 k	74.77	60.31	<input checked="" type="checkbox"/>
	35	10.28 M	122.85 k	83.68	52.75 k	78.80	38.07	<input checked="" type="checkbox"/>

This shows that 100% of the traffic is TCP, and that all TCP flags are being used, which is characteristic of the life cycle of TCP connections. Some types of TCP-based attacks may be differentiated by different use of TCP flags. A SYN flood, e.g., would show a predominance of packets with just the SYN flag set: S (0x02).

Knowledge of the ingress and egress interfaces on the router being examined here is not of much use to CenturyLink customers. They could be used by CenturyLink Technology Solutions engineers to generate an ACL specific to those interfaces. A customer using the Peakflow to generate an ACL for their own routers would want to un-check the Filter box for these interfaces.



## ACL Generation from an Alert

An ACL filter can be generated from the checked items in an alert detail by clicking on the “**Mitigate Alert: Generate Filter**” button at the top of the page. In the customer portal this will only present the text of a router ACL that *could* be copy-and-pasted into a router configuration. The Arbor Peakflow system does not actually take any action from the Mitigate Alert button in the customer portal. This would only be useful to customers who manage their own routers and could find it beneficial from time to time to use an ACL to mitigate a small-scale event.

All the elements in the alert detail that have a check in the Filter column will be used in the generation of the ACL. Elements can be added or removed manually by adding or removing Filter checks before generating the filter.

The Arbor Peakflow is programmed with the ACL syntax for several popular router brands. This is an example of an ACL generated for a Cisco router. The text of the ACL is presented for a knowledgeable and capable customer to use via copy-and-paste. It is not applied to any router by the Peakflow system.

Status	Alerts	Traffic	Mitigation	Administration
<b>Generate Filter</b>				

```
# ALERT 851148

no ip access-list extended alert-851148
ip access-list extended alert-851148
deny tcp any eq 2974 host 203.113.136.36 eq 443 fin syn rst psh ack
deny tcp any eq 2974 host 203.113.136.36 eq 80 fin syn rst psh ack
deny tcp any eq 30776 host 203.113.136.36 eq 443 fin syn rst psh ack
deny tcp any eq 30776 host 203.113.136.36 eq 80 fin syn rst psh ack
deny tcp any eq 60329 host 203.113.136.36 eq 443 fin syn rst psh ack
deny tcp any eq 60329 host 203.113.136.36 eq 80 fin syn rst psh ack
deny tcp any eq 22230 host 203.113.136.36 eq 443 fin syn rst psh ack
deny tcp any eq 22230 host 203.113.136.36 eq 80 fin syn rst psh ack
deny tcp any eq 24208 host 203.113.136.36 eq 443 fin syn rst psh ack
deny tcp any eq 24208 host 203.113.136.36 eq 80 fin syn rst psh ack
deny tcp any range 12288 16383 host 203.113.136.36 eq 443 fin syn rst psh ack
deny tcp any range 12288 16383 host 203.113.136.36 eq 80 fin syn rst psh ack
deny tcp any range 0 4095 host 203.113.136.36 eq 443 fin syn rst psh ack
deny tcp any range 0 4095 host 203.113.136.36 eq 80 fin syn rst psh ack
deny tcp any eq 2974 host 203.113.136.36 eq 443 fin syn rst psh ack
deny tcp any eq 2974 host 203.113.136.36 eq 80 fin syn rst psh ack
deny tcp any eq 30776 host 203.113.136.36 eq 443 fin syn rst psh ack
```

Large-scale attacks require mitigation in the CenturyLink Technology Solutions core cleansing centers and cannot be adequately defended against with ACLs on the customer's routers.



## Mitigation

Portal customers can get a view into the detailed operation of DDoS mitigations, both past and present. Only those mitigations that have been specifically enabled for managed-services customer access will be visible. That can be enabled either when a mitigation is initially created, or added after it is running.

Currently running mitigations are listed under Mitigation → Ongoing. The order of presentation is selectable by clicking on the column headers; the default is to list most-recent first:

StatusAlertsTrafficMitigationAdministrationExit Scoped View

MY ACCOUNTHELPLOGOUT

Mitigations Ongoing

DOWNLOAD

EMAIL

PRINT

SearchWizard

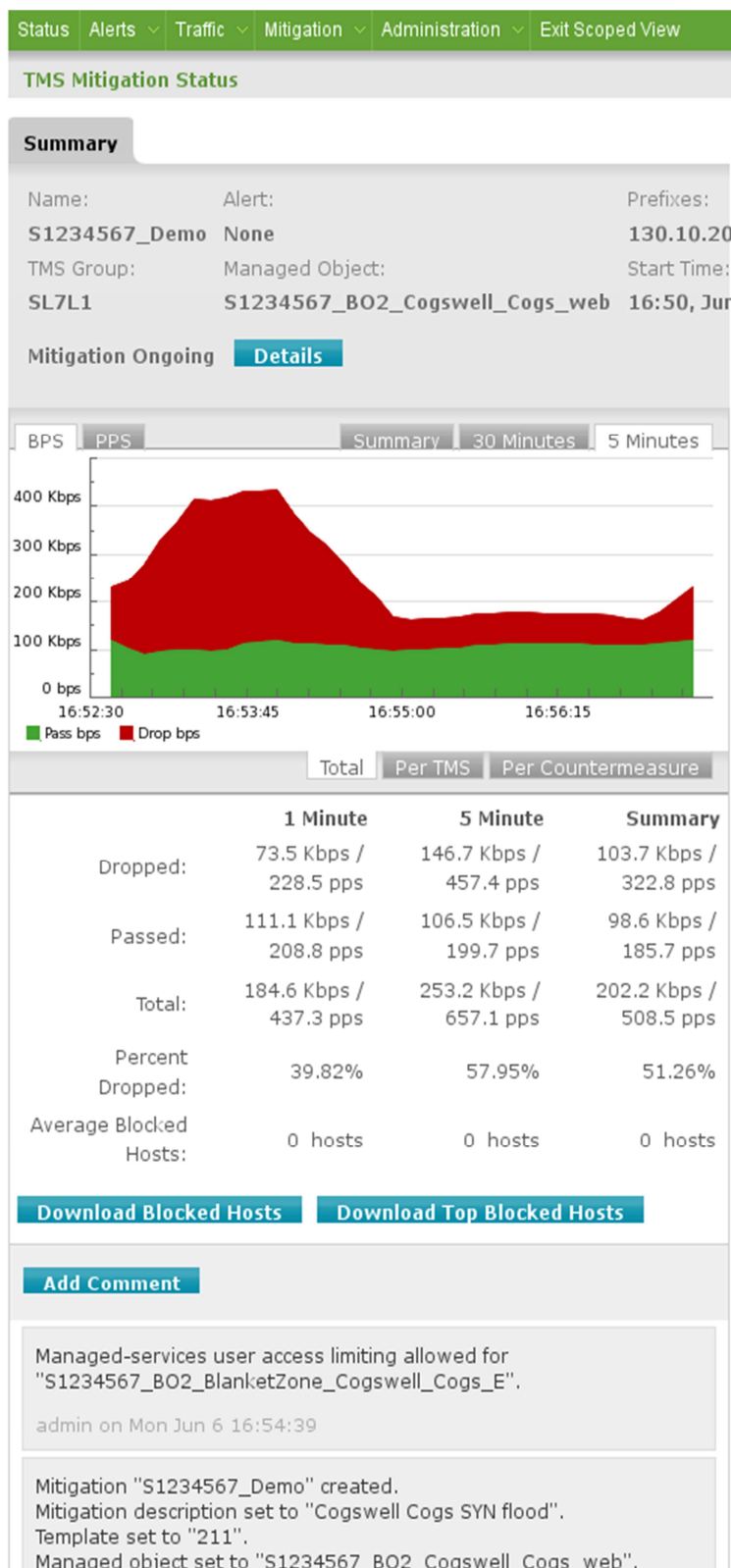
1 results (0.18 seconds)

Graph	Name	Duration	Start Time	User	Type	Annotations
	<a href="#">S1234567_Demo</a>	0:05 (Ongoing)	16:50, Jun 6	admin	TMS	Managed-services user access limiting allowed for "S1234567_BO2_BlanketZone_Cogswell_Cogs_E". (by admin)

- The columns contain this information for each mitigation:
- The small graph is a summary of the traffic being handled by the mitigation, with passed traffic shown as green and dropped traffic shown as red.
- The name is assigned by the operator when the mitigation is created.
- The duration is the length of the mitigation
- Start time is when the mitigation was created, not the time that it was most recently started if it was stopped and subsequently restarted.
- User is the id of the operator that started the mitigation.
- Type will be TMS
- The Annotations column shows the most recent annotation only. Annotations are automatically added by the system when the mitigation is started or when it is modified in any way. Annotations may also be manually added by operators.

View details of the mitigation status by clicking on the graph or the mitigation name.

## TMS Mitigation Status – Summary



Details of the mitigation status are shown in two columns. The left column, shown here, contains the summary information about the mitigation.

The chart depicts the amount of traffic that is passed (green) and dropped (red) in either bits per second (BPS) or packets per second. The time period is selectable. The chart updates automatically while the page is open.

Below the chart are various statistics on dropped, passed, and total traffic. These flash green and red as they update, the color indicating the direction of change – green indicating an increase (even of bad things), and red indicating a decrease since the previous update.

The currently blocked hosts and the most frequently blocked hosts for this mitigation can be downloaded as a .txt file. See the section below on what malicious traffic will and will not be represented in these reports.

At the bottom are all the mitigation annotations in most-recent-first order, and a button for adding an annotation (comment). Any modification to the mitigation will result in an automatic annotation detailing the change. This example shows the portal account being granted access to the mitigation, and before that the creation of the mitigation.

## TMS Mitigation Status – Countermeasures

Details of the operation of individual countermeasures are shown in a panel to the right. Only those countermeasures that correspond to the characteristics of the attack should be enabled, both to avoid overtaxing the system and to avoid the possibility of unintended consequences on non-attack traffic.

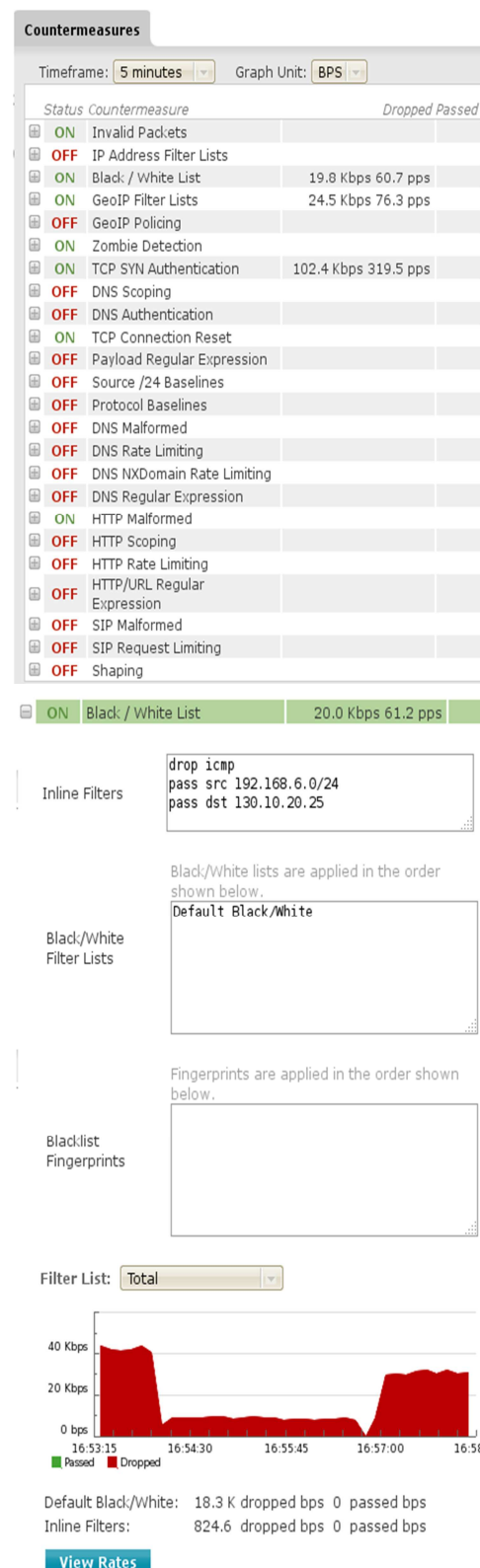
Each countermeasure shows how much traffic it is dropping or explicitly passing in either bits per second (BPS) or packets per second (PPS). The timeframe for the traffic graphs shown in many countermeasures' details is selectable. Details for a specific countermeasure can be examined by clicking the + next to it. Details can be hidden by clicking on the –.

All details of all countermeasures are not covered in this document. This is an overview of some of the most salient features, including those common to many countermeasures.

**Invalid Packets:** This countermeasure is always enabled and drops packets that are incomplete or have invalid checksums. It looks at the IP, TCP, and UDP headers.

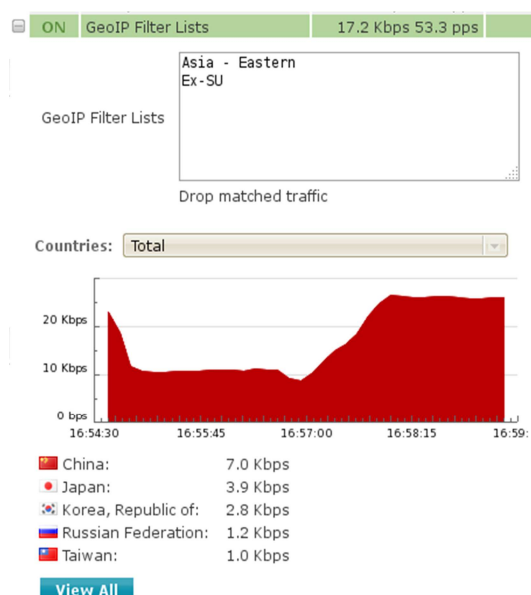
**IP Address Filter Lists:** Named lists of IP addresses and netblocks are maintained outside of the mitigation, and different lists can be defined for traffic that should be immediately dropped or immediately passed with no further inspection. This is the place for long or long-lived lists of IP address space for this purpose. A graph of passed and dropped traffic rates is shown, for this countermeasure as a whole, or for an individual list.

**Black / White List:** Shown at the right, there are three parts to Black/White Lists. **Inline Filters** consist of pass or drop rules in Arbor's FCAP filter notation. This can be used to match a limited number of IP addresses or netblocks. Though the IP Address Filter Lists described above are the better place for large numbers of address-based rules, the Inline Filters are more accessible for modification from within the mitigation. The FCAP rules in the Inline Filters can consist of arbitrarily complex expressions that look at different parts of the protocol headers and which can be combined with AND/OR logic and grouped in parentheses. (FCAP is similar to the PCAP filters used in tcpdump and Wireshark with enhancements.) **Black/White Filter Lists** reference predefined and named lists of FCAP expressions that can be brought into the mitigation. The Default Black / White list contains drop rules for RFC-1918 addresses and illegal TCP flag combinations. **Blacklist Fingerprints** identify potentially troublesome traffic based on predefined



criteria, such as P2P and Botnet C&C traffic.

**GeoIP Filter Lists:** One or more predefined lists of country codes can be selected. The Arbor TMS will drop either all traffic that matches the selected lists, or it will drop all traffic that does not match the selected lists. Several lists are defined for all regions of the globe. The graph shows the total traffic dropped for this countermeasure, or the total from an individual country from the drop-down list. Drop rates for the most frequently matched countries are displayed numerically. The View All button opens a pop-up that shows the numeric drop rates for all affected countries. Note that available GeoIP lists are subject to a certain amount of error, and this countermeasure can misidentify some traffic.



**GeoIP Policing:** Individual countries can be selected to identify traffic to immediately drop or pass (subject to scrutiny by other countermeasures), on a per-country basis. A third option allows traffic from individual countries to be rate-limited on a per-country basis. Unmatched traffic can be dropped, allowed to pass through to other countermeasures, or rate-limited. Rates are reported only for dropped traffic. GeoIP lists are subject to a certain amount of error, and this countermeasure can misidentify some traffic.

**Zombie Detection:** Individual hosts sending abnormally large amounts of traffic are identified as “zombies” and blocked. These are real hosts, not spoofed. The detection is based solely on operator-defined static thresholds. Different thresholds can be established for different traffic types.

**TCP SYN Authentication:** SYN flood attacks are mitigated by testing whether the initial SYN packet used to initiate a new connection was sent from a real host trying to initiate a full connection. The Arbor TMS supports multiple ways of doing this, each of which has advantages and disadvantages in terms of how disruptive it can be to new connections from legitimate remote hosts. A special mechanism can be enabled for HTTP connections and restricted to the port(s) that HTTP normally runs on. Specific ports can be excluded from this countermeasure.

**DNS Scoping** can limit the action of DNS-specific countermeasures to specific domains, which can be useful if an attack targets a specific domain on a DNS server that hosts multiple domains.

**DNS Authentication** attempts to determine whether DNS queries are from real hosts or are part of a spoofed flood of queries.

**TCP Connection Reset** closes idle TCP connections and blocks the offending clients for a period.

**Payload Regular Expression** can drop packets which contain an operator-defined pattern.

**Source /24 Baselines** can drop traffic from netblocks that generate more traffic than what is considered “normal” for them. This is a last-resort type of measure that can easily drop innocent traffic, though it can be useful to keep bandwidth in check when other means fail to thwart attacks.

**Protocol Baselines** drops packets for protocols that exceeds the “normal” rate expected. Here, protocols mean TCP, UDP, ICMP, etc., not application-level protocols. This is a last-resort type of measure than can easily drop innocent traffic.

**DNS Malformed** drops DNS packets that do not conform to the published DNS standards.

**DNS Rate Limiting** drops traffic from hosts that exceed a set number of DNS queries per second.

**DNS NXDomain Rate Limiting** is not applicable to the CenturyLink Technology Solutions DDoS mitigation architecture.

**DNS Regular Expression** can drop DNS packets with content that matches one or more patterns.

**HTTP Malformed** drops HTTP requests that do not fully conform to the HTTP standards.

**HTTP Scoping** can be used to limit HTTP-specific countermeasures to HTTP requests that match certain patterns. It can be used, for example, to focus on one specific website that is under attack when multiple sites are hosted on the same server or behind the same load balancer.

**HTTP Rate Limiting** can block clients that open HTTP connections too rapidly (Object Limit), or which issue HTTP requests too rapidly (Request Limit). The distinction is needed because multiple requests can be made on one connection.

**HTTP/URL Regular Expression** identifies patterns in HTTP requests that can be used either to immediately drop or pass the requests.

**SIP Malformed** blocks traffic from hosts that originate SIP packets that do not conform to RFCs.

**SIP Request Limiting** blocks hosts that generate SIP messages at too high a rate.

**Shaping** limits all traffic passed by the mitigation to a specified limit. It is a last-resort measure if the other countermeasures are unable to prevent the attack from consuming available network bandwidth. Shaping can be restricted to certain traffic so that some bandwidth is available for mail or VPN access, *e.g.*, while an attack is in progress on HTTP.

## Administration

Customers can view the networks included in their profile(s) from Administration→Profiles:

This is a read-only display. Any discrepancies between what is shown here and the customer's current needs will be handled by a CenturyLink Technology Solutions engineer.

### My Account

The user of an Arbor portal account can change the timezone used in the display of data when using the system with that account. The default timezone is UTC.

Users can change their passwords used to access the Arbor Peakflow portal. It is recommended that users change the passwords they receive from CenturyLink Technology Solutions when the account is initially configured.

### Administration → User Accounts

CenturyLink Technology Solutions provides to DDoS portal customers an admin-level portal account that can create additional user accounts within the same scope for other users in the same organization.

User Accounts									
	Username	Real Name	Group	Email	Device	Timezone	UI Menu	Last Login Attempt	
								Location	Time
<input type="checkbox"/>	admin-admin	portal admin	arbor2_dck_authentication-auth	arbor2.dck	Default	Default	00:11:11.58	01:33:00.14	2010
<input type="checkbox"/>	admin21_123	authentication	arbor2_dck_authentication-auth	arbor2.dck	Default	Default	00:11:11.33	20:14:00.14	2010
<div> <a href="#">Create A New Account</a> <a href="#">Delete Selected</a> <a href="#">Disable Selected</a> </div>									

This internal CenturyLink Technology Solutions document is provided to customers under confidentiality restrictions for informational purposes only and nothing herein creates any obligation, contractual or otherwise, between the parties and no third party beneficiaries are intended