Trisul Network Analytics - Traffic Analyzer

Using this information the Trisul Network Analytics Netfllow for ISP solution provides information to assist the following operation groups:

- Network Operations
    - Network Visibility- Monitor network traffic for network analysis
    - Network Performance Monitoring- Network traffic and analysis for performance related issues
    - Improved Triage
- Security Operations
    - Intrusion Detection
    - Identification of Unknown Threats
    - Incident Mitigation & Forensics
- Architecture and Planning
    - Understand Client-Server Relationships- VMWare Virtual and security level mapping for both network and application level application identification
    - Physical and Virtual Host Visibility
    - Trend Reporting

System Security

Traffic Analyzer handles all Malicious Hosts, Traffic spikes, Worm Activity, Alarms associated to these security concerns, Host Information, Identify infected machines on your network, Measure malware and botnet activity, Alert when users access blacklisted websites, Monitor intrusion attempts into your network, Post compromise analysis

For Network Troubleshooting, Router and Switch Interface utilization, User Activity, Traffic entering and leaving the network, quality of service utilization, Round trip time (RTT) and Server response time (SRT) deviations, Application identification through

- Network Monitoring
- Application Monitoring and Profiling
- User Monitoring and Profiling
- Network Planning
- Accounting/Billing

Router Traffic: Displays the list of configured router IPs with traffic rate of Maximum, Average and Total traffic per second. The Total field shows the summary of flow data in selected time range. Click the Total value to view total router traffic graph and an option for analysis. Similarly, click Router IP to view router specifications.

Protocol Traffic: Displays the list of protocols with the router IPs, the protocol name, the traffic rate of Maximum, Average and Total traffic per second. The Total field shows the summary of flow data in selected time range. Click protocol name or number field to navigate to Protocol Summary page to view details of device flow using corresponding protocol.

Application Traffic: Displays the list of application with the router IPs, the port number, the total In traffic, Maximum traffic, the total Out traffic, Maximum Out traffic, Total traffic per second. Click values under “In” heading to navigate to the Source Summary page, and on “Out” leads to Destination Summary and click Total field to navigate to application report graph.

Interface Traffic: Displays the list of interface with the router IPs, the total In traffic, Maximum traffic, the total Out traffic, Maximum Out traffic, Total traffic per second. By clicking the interface the user can navigate to the interface summary page, clicking on the In or Out takes to the source summary page or Destination summary page respectively and clicking on the total it will take to the interface report graph.

Router Traffic: Displays the configured router IPs by traffic in a Graph. The graph shows the total traffic along the Y-axis and the time in the X-axis.

Source Device Traffic: Displays the list of Top N traffic source devices with the router Ips, and traffic rate of Maximum, Average and Total traffic per second.

Destination Device Traffic: Displays the list of Top N traffic destination devices with the router IPs, and traffic rate of Maximum, Average and Total traffic per second.

Top Conversation Traffic: Displays the list of Top N traffic source and destination devices with the router IPs, and traffic rate of Maximum, Average and Total traffic per second.

Routing Traffic : Traffic going to each Autonomous system at direct peering points, Traffic going to each Application Cache such as Google/ Facebook/ YouTube. Raw BGP analysis capability.

SOLUTION FEATURES

This section describes the key features of the proposed solution with reference to the compliance documents.

Autonomous system based traffic mapping

More Link: https://www.trisul.org/docs/ug/ui/dashboards.html#asn_monitoring

By Enabling Netflow on Gateway Router and Switches at Peering Points you can get detailed break up of Traffic flowing to each AS Peer on a per gateway router or per-Interface level. The AS information can be obtained directly from the Router Netflow records or by the included high quality IP Prefix database.

Busiest UPLOAD and DOWNLOAD ASN on Gateways

The following screenshot shows how much Traffic is flowing TOWARDS and FROM each Autonomous System connected to a Gateway Router. You can also monitor on a per country basis (next section) on each Gateway Router. You can create alerts when unexpected traffic is routed through the gateway routers such as when Country

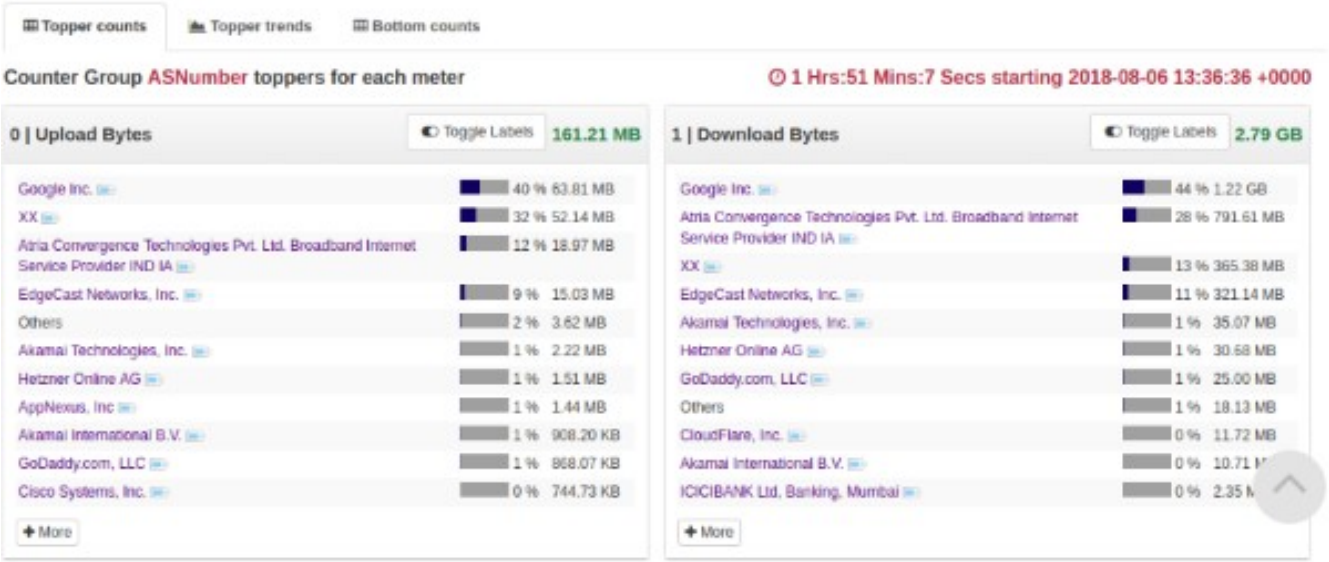


Illustration 1: Showing Traffic going to each ASN from a Gateway Router

Capacity planning and trending of ASN Traffic on Gateway Routers

Long term monitoring and trending of every single ASN traffic profiles over days, and months help you

forecast traffic growth of important Peers and Caches. This allows you to plan ahead of time with increased capacity. The following screenshot shows ASN Traffic over time no Gateway Interfaces.

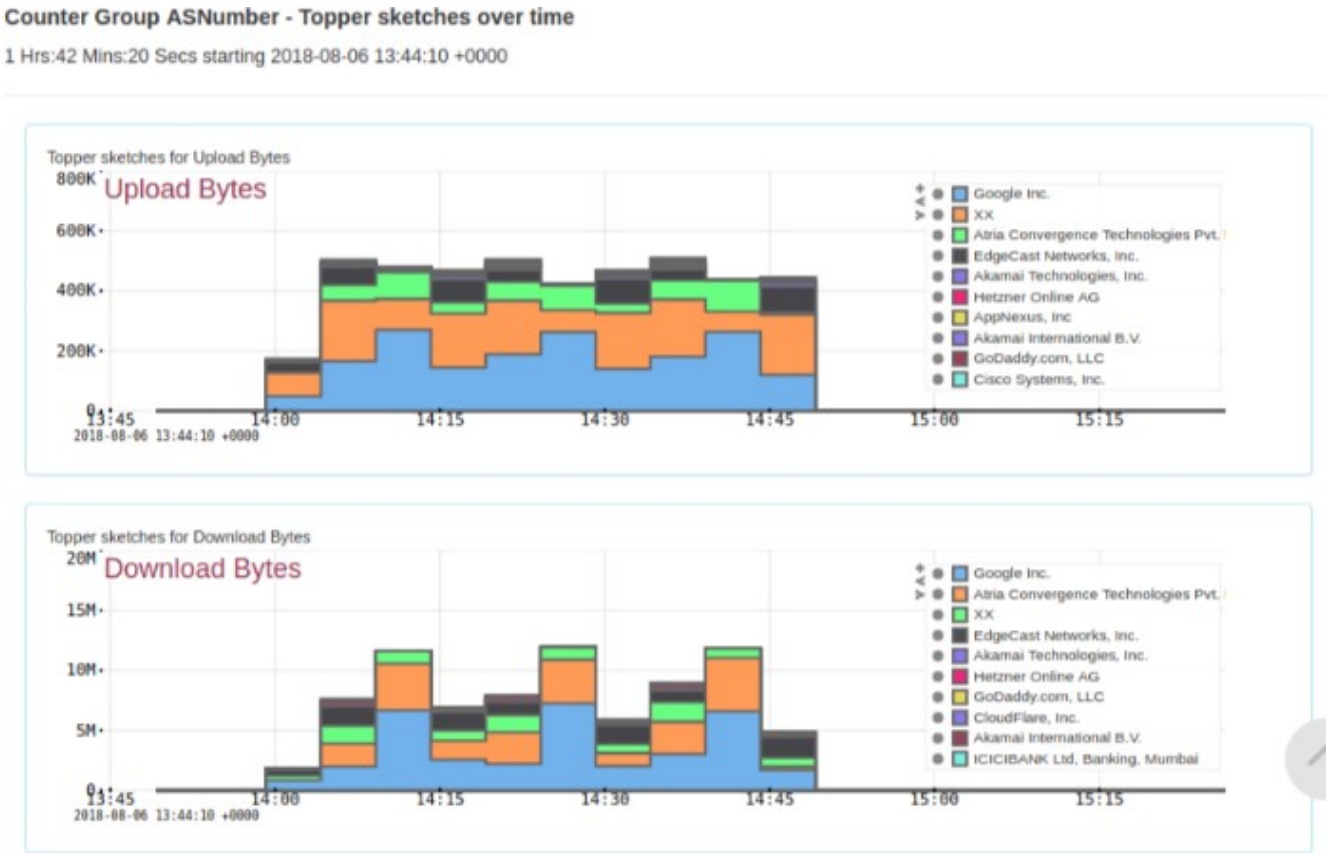


Illustration 2: Traffic Trend per ASN and Google Caches for planning

Troubleshooting and security for ASN

Trisul includes powerful graph analytics functions that help you discover relationships between various entities. If you have unexpected traffic on AS:8388 and then if you wish to see what actual IP Addresses are involved you can simply click the AS and expand it to reveal the IP , Host names, Countries etc. Without this capability you will find it very hard to reveal this information. This is invaluable for troubleshooting, network management and security.

The following screenshot shows as AS which was seen on a particular Gateway node. By clicking it we are able to reveal the hosts on that AS for further action.

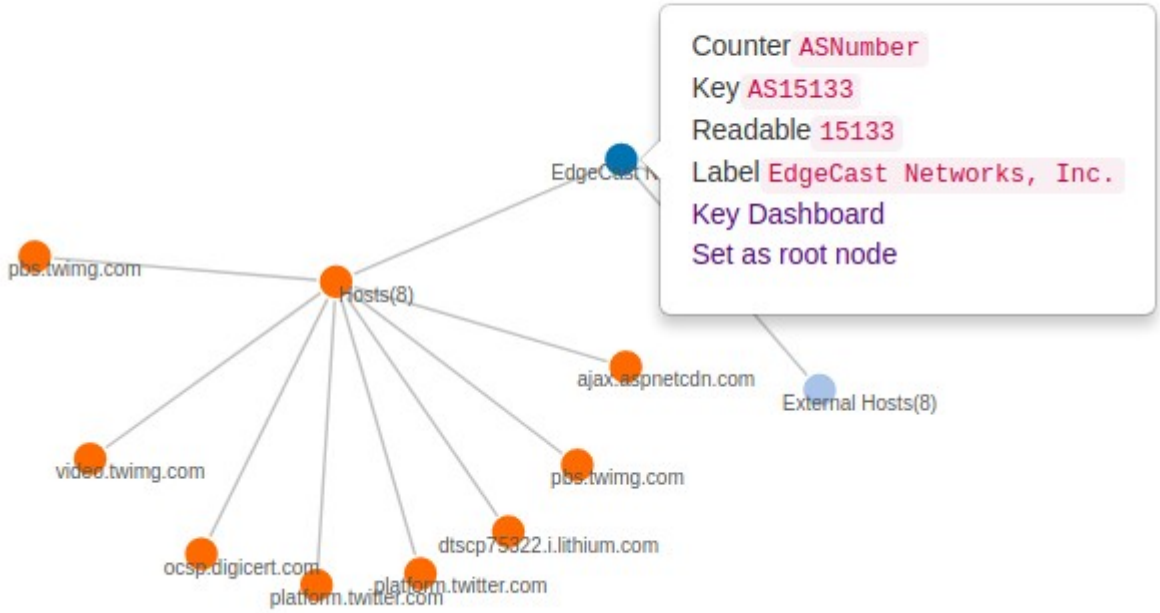


Illustration 3: EDGE Graph Analytics showing Hosts inside an AS

Prefix based traffic mapping

Link : https://www.trisul.org/docs/ug/ui/interesting_dashboards.html#key_space_explorer

Trisul provides very flexible tools to load your own IP Prefixes into the solution. This way you can monitor on a Prefix level per Gateway , per Circle, or nationwide. For your internal traffic you can group all your IP Endpoints into prefixes and monitor at that level. For example you can monitor 115.28.2.0/24 nationwide as one group in addition to each individual endpoint. This lets you build a high level Prefix Mapping of Traffic at country, circle, and gateway level.

Prefix based monitoring tools

All the previous tools such as Topper Monitoring, Trending, and Edge are also available for IP Prefix based monitoring. In addition, there are some additional tools we can see here.

Prefix Space Monitoring

The Prefix Space monitoring tool known as KeySpace Monitor lets you drill down into any internal or

external IP Prefix range to show usage of Ips within in. The following screenshot shows the usage ratio of IP endpoints in the Prefix 192.168.0.0/16 For ISP this allows them to track density of IP Prefix and then use to plan routing and IP Space allocation.

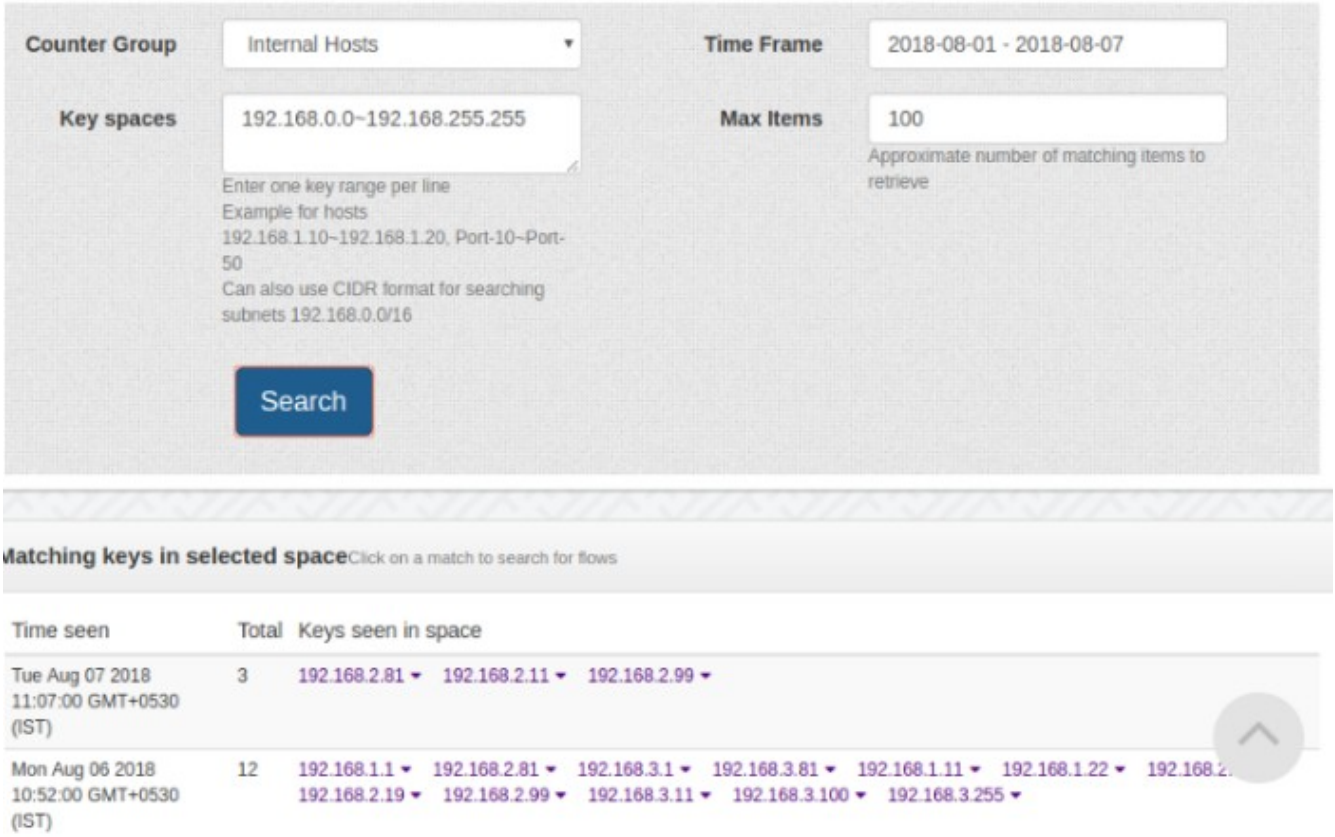


Illustration 4: KeySpace monitor shows which IPs are used in a Prefix

Prefix Traffic Mapping

Prefix based traffic monitoring allows you to not only track the inside IP but also the usage of each block or sub-prefix within the prefix. The following screenshot shows the usage of Total, Transmit, Receive of each point with a Prefix Range. This feature is called Prefix Key-Space Explorer.

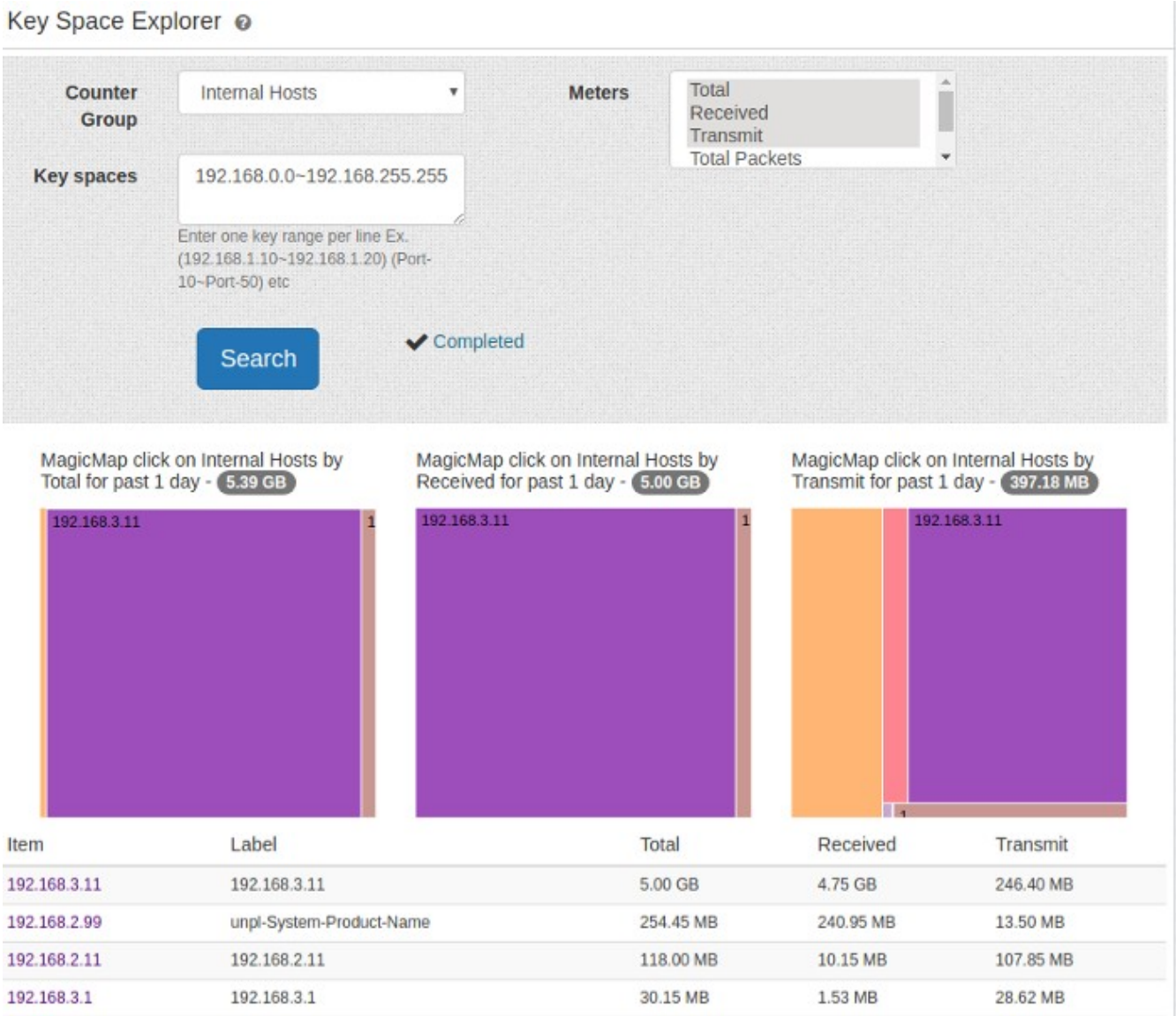


Illustration 5: Traffic mapping of each IP within a Prefix

Location based traffic mapping

More Link : https://www.trisul.org/docs/ug/ui/dashboards.html#country_location_based_traffic_monitoring

Tracking traffic per country, region, or city is a crucial capability of any Network Analytics solution. Trisul allows you to maximum flexibility to track traffic down to the City or area level. This feature can be enabled at the national, circle, or gateway level or even per-interface.

Location traffic per Gateway Interface

The following screenshot shows upload and download bytes on a per Country Basis on a particular Gateway. This allows you to verify your routing policies. You can click on any country to drilldown into it or view trends.

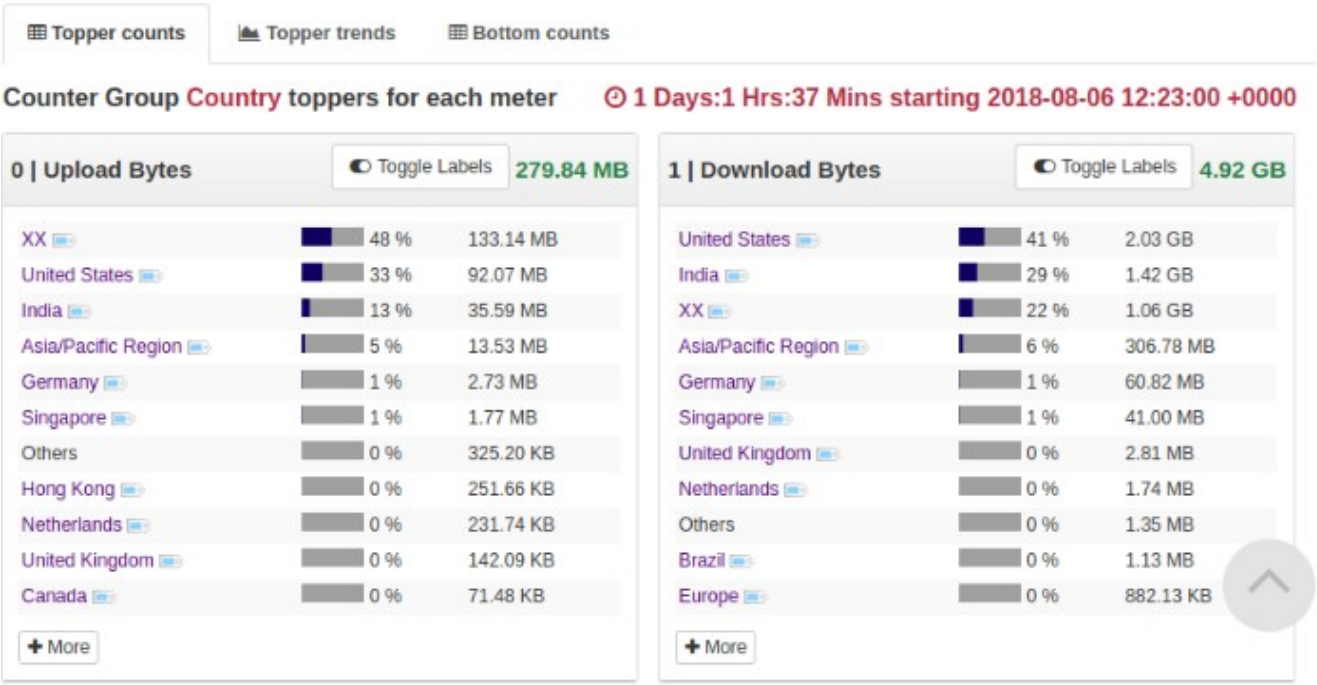


Illustration 6: Traffic upload and download per Country / Gateway

Long term Trends per Location for capacity planning

The following image shows Traffic per location. You can observe which City (Chennai, Delhi, Kochi, etc.) are growing and use that for business planning or capacity planning.

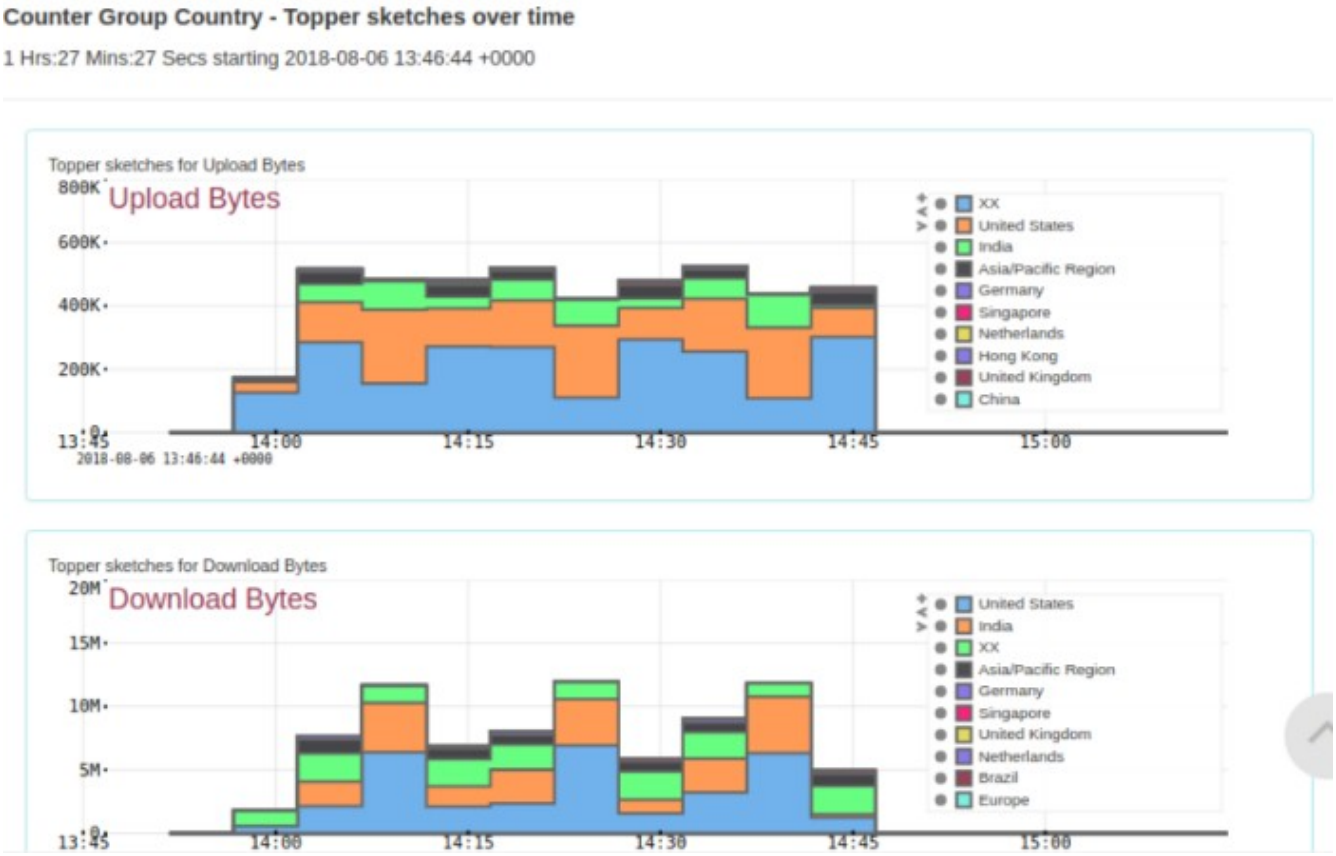


Illustration 7: Traffic Trends per Country

Showing High Traffic endpoints on Geo MAP

This map shows you where the top Location wise traffic IP sources and destinations are for a gateway or for the entire network.

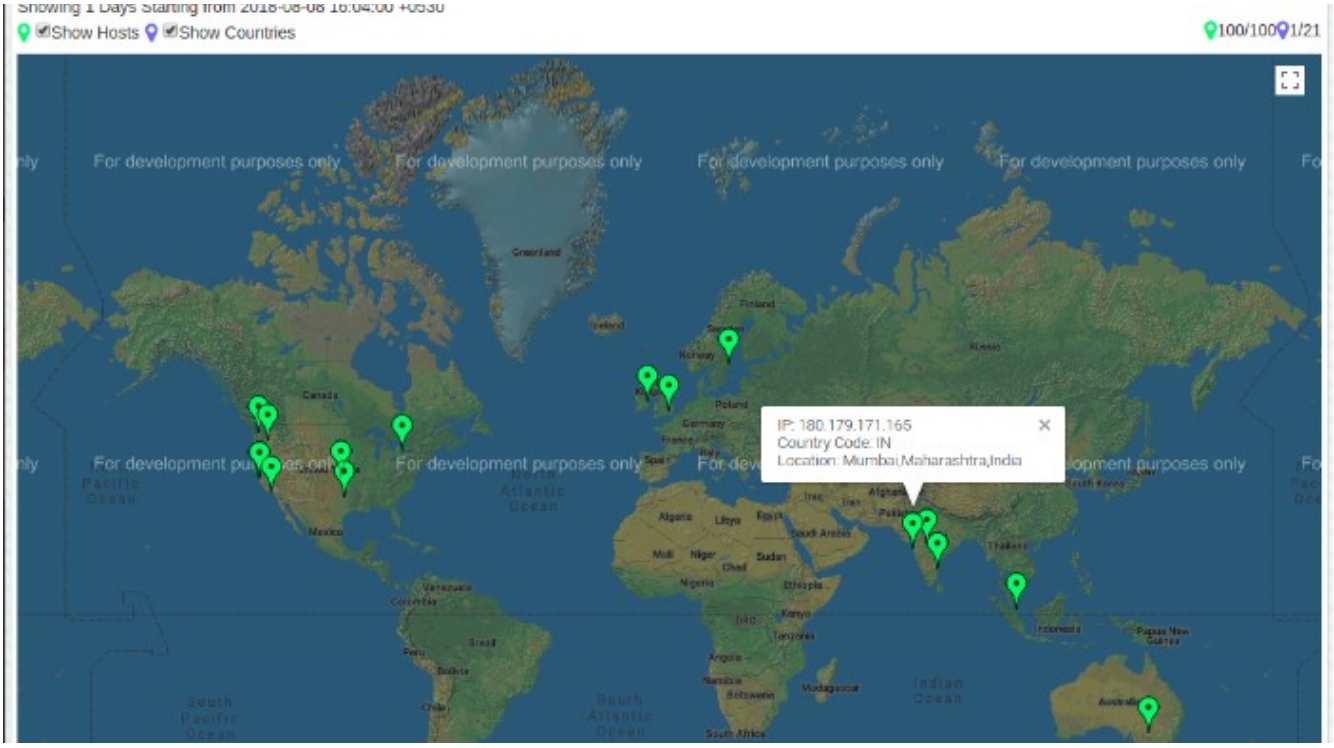


Illustration 8: Traffic shown on Geo Map

Dashboards

Link: https://www.trisul.org/docs/ug/ui/dashboards.html#default_dashboards

Features very powerful dashboarding for all Time-Series measurements, Top-N lists, alerts, summary pages, live views. Users can easily create their own dashboards showing their preferred event counters, time-series charts. Trisul out of the box supports 150-200 metrics. Metrics like TCP round trip time, latency. Custom QoS metrics requested like can be monitored by IP SLA features on routers. The following metrics monitored by IP SLA compatible networks can be added to any dashboard.

•Delay (both round-trip and one-way)

•Jitter (directional)

•Packet loss (directional)

•Packet sequencing (packet ordering)

•Path (per hop)

•Connectivity (directional)

•Server or website download time

This can be shown for paths containing audio (VoIP) or Video traffic. Video duration played from sources like YouTube, Netflix, Amazon Prime can be monitored by flow based techniques. The solution allows customized monitoring depending on the video platform.

Some sample dashboards are shown in the next section.

Events and counters

The Totals dashboard shows all the various event counters over a selected time period. The items include Unique AS, Unique Countries, Unique Hosts, Router Interfaces, and dozens of other counter groups. You can also see security related counter like IDS alerts, threshold crossing alerts, threshold band alerts. Etc

Illustration 9: Events and counters dashboard

Network summary dashboard.

https://www.trisul.org/docs/ug/ui/dashboards.html#live_network_summary_dashboard

A Live Network Summary dashboard showing KPI at the top level for management and high level NOC operations. It shows live usage, bandwidth, security event counts, top hosts, top Apps. This can be customized to show any relevant KPI of importance to the teams using it.

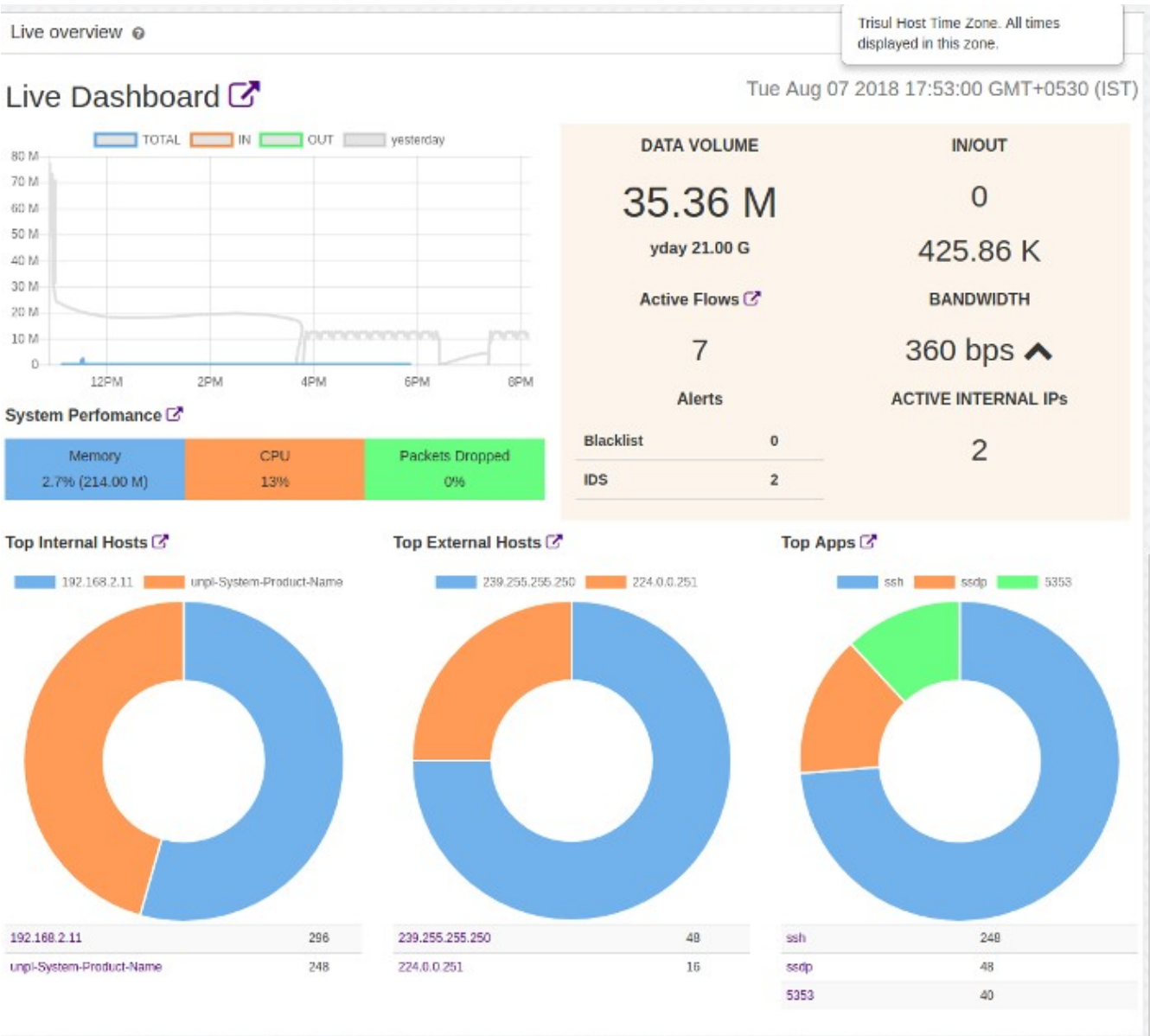


Illustration 10: Network summary dashboard

Routing Efficiency Dashboards

40 (f) Routing Efficiency Dashboard: Control network costs and build business cases for capital projects to gain a complete understanding of interconnect relationships. YES ASN, IP, dashboards

Routing efficiency consists of monitoring IGP and EGP link traffic and also traffic at the interconnects. The solution will monitor IGP links between interconnects, inter-circle, for traffic utilization. The interconnect links with peers are also monitored for long time trending and storage. All the links on routers are autodiscovered from Netflow traffic exported from them. This information can be combined with tools like BGPPlay to simulate and build business cases.

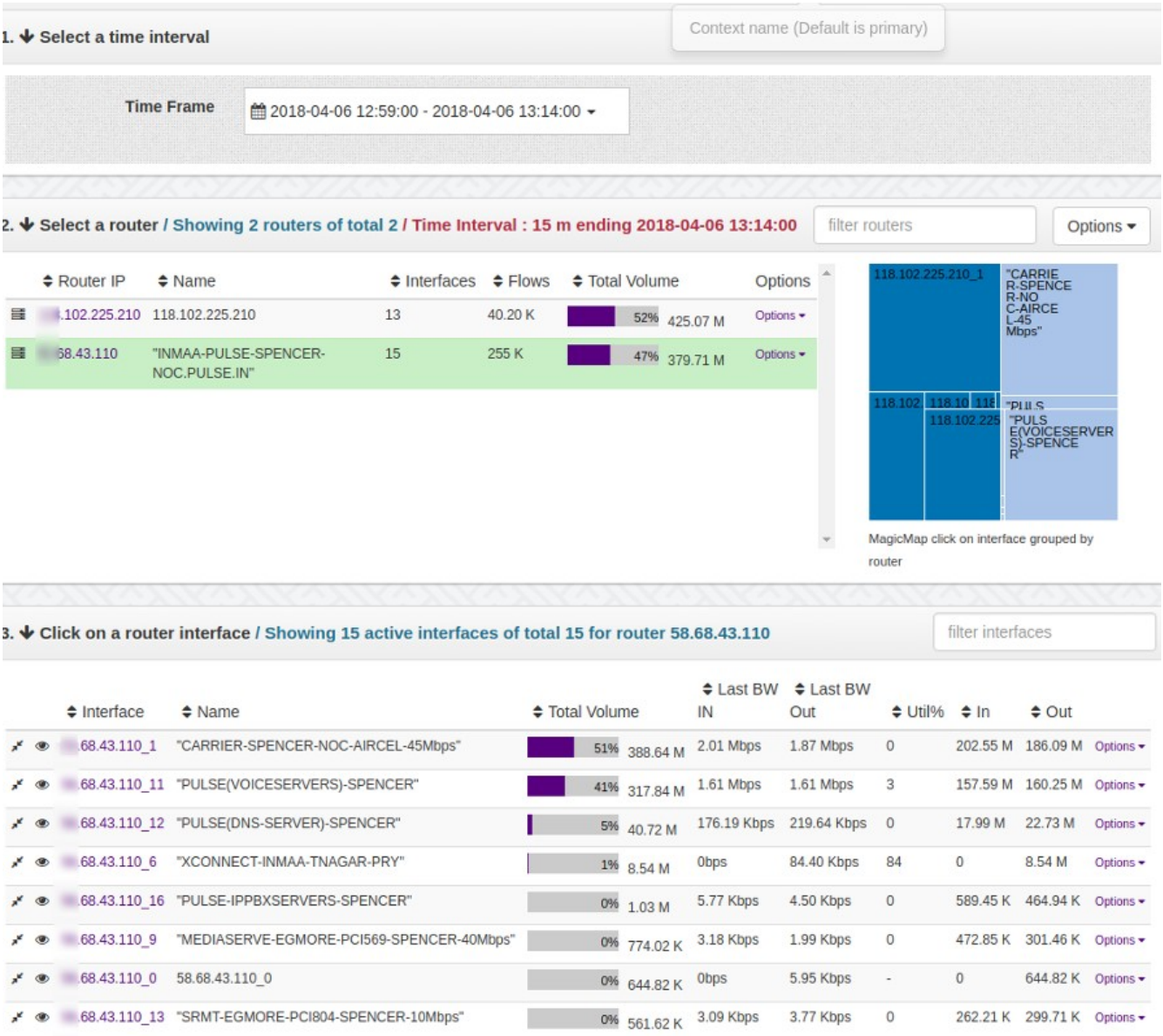


Illustration 11: Showing utilization and KPIs of router IGP and EGP links

Real Time Dashboards

https://www.trisul.org/docs/ug/ui/dashboards.html#real_time_traffic

Powerful real time views are available for all metrics in Trisul at 1-sec, 5-sec, and 1-min duration. There are over 150-200 metrics available out of the box in Trisul to view in real time. Additional metrics like Video views, or any type of content based policy views can be easily added.

Real Time traffic view

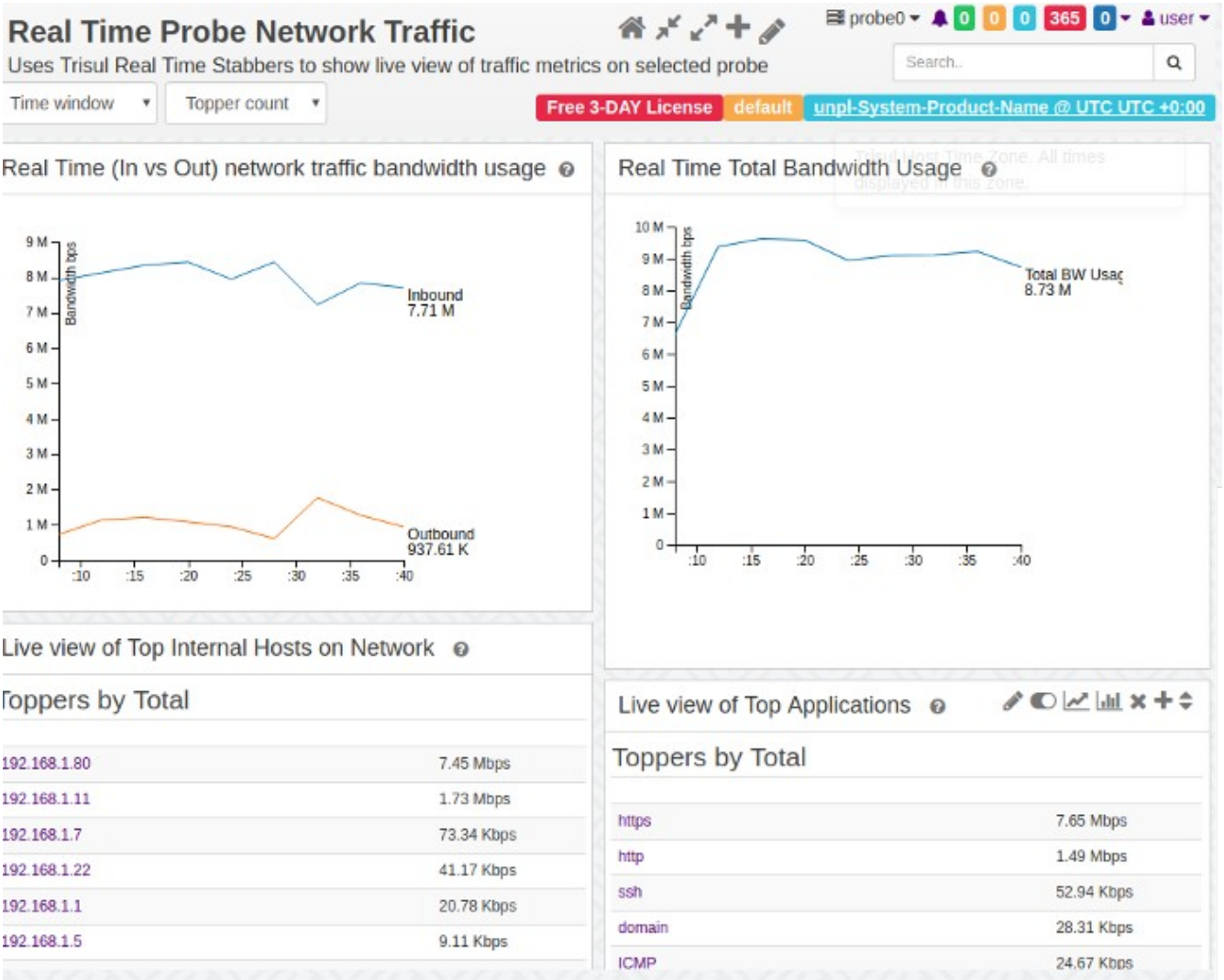


Illustration 12: Real time network traffic view

IPv6 Transition Dashboards

IPv6 is fully supported based on Packet Capture and Netflow v9. Top internet applications adopting IPv6 are monitored and show. The IPv6 adoption internal to the ISP network is also shown. The following screenshots show IPv6 adoption rate showing top IPv6 users as well as the top flows (video, apps, chat) using IPv6.

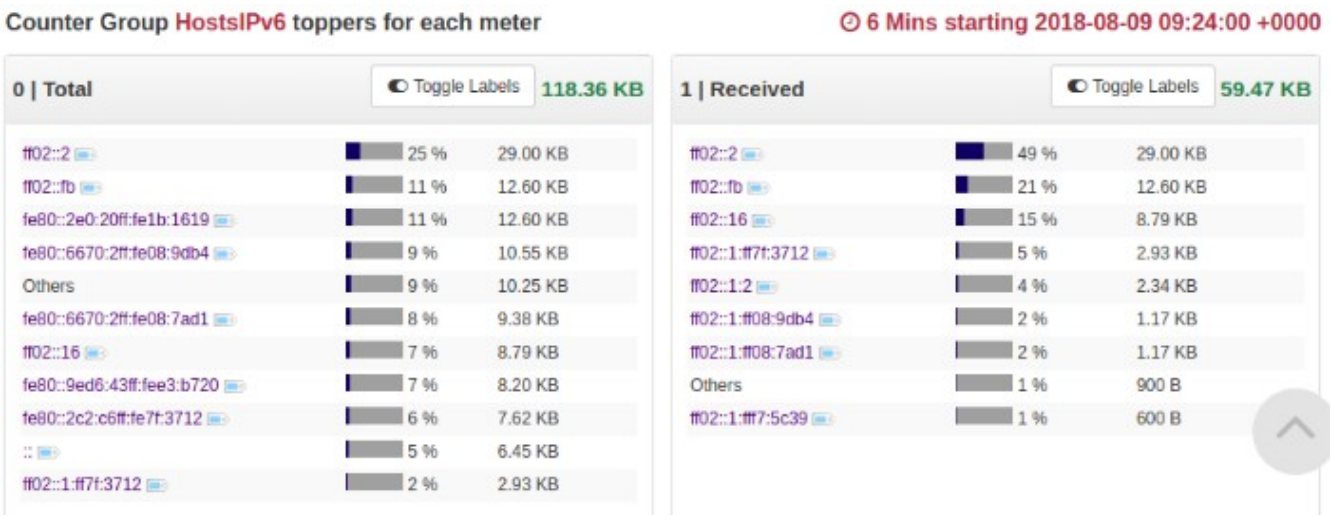


Illustration 13: IPv6 Adoption Top users

TOP IPv6 Flows APPS can be video, apps, file transfers etc.

Cols

Proto	Src IP	Src Port	Dst IP	Dst Port	Volume	StartTime	Duration	Probe	Tags	
IPv6-ICMP	fe80::429b:cdff:fe75:7e0d	0	ff02::1	0	54.09 K	Thu Aug 09 2018 11:07:24	4 h 29 s	probe0		options
IPv6-ICMP	ff02::1	0	fe80::429b:cdff:fe75:7e0d	0	774	Thu Aug 09 2018 11:05:10	6 m 23 s	probe0		options
UDP	fe80::429b:cdff:fe75:7e0d	5353	ff02::fb	5353	394	Thu Aug 09 2018 11:06:22	0 s 0 us	probe0		
IPv6-ICMP	ff02::1	0	fe80::429b:cdff:fe75:7e0d	0	86	Thu Aug 09 2018 11:24:13	0 s 0 us	probe0		

Illustration 14: IPv6 Top Application flows

Traffic Management Dashboards

40i) Traffic Management Dashboard: To plan congestion management policies based on the granular insight provided by the Traffic Management Dashboard, then view the positive impact.

https://www.trisul.org/docs/ug/ui/interesting_dashboards.html#monthly_summary_dashboard

Trisul monitors 200+ KPI of traffic metrics at 1 minute resolution without any roll ups or summarizations for long term analytics. Advanced statistical metrics like cardinality counters (eg unique applications per host) and top-N snapshots are all enabled out of the box. A few of the hundreds of metrics are Hosts, Applications,, Countries, AS Numbers, Routers, Ports, etc.Network flows are analyzed and stored in a custom built database engine designed for very fast storage and retrieval. The Netflow Interface Tracker is a streaming analytics algorithm that lets you generate long term accurate drilldowns of interface usage.

MONTHLY Traffic Management

This can be used for planning or billing activities on a monthly basis.

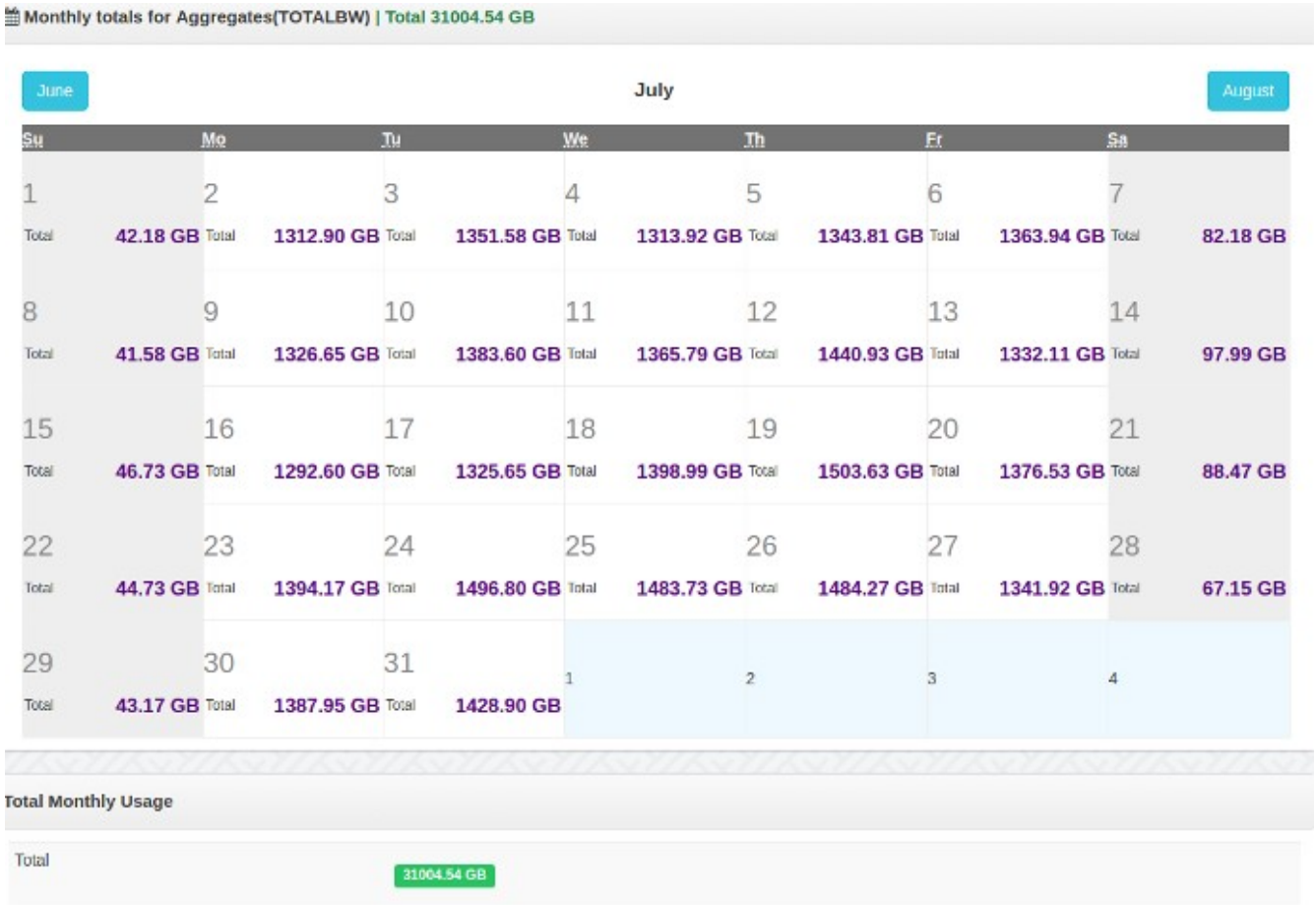
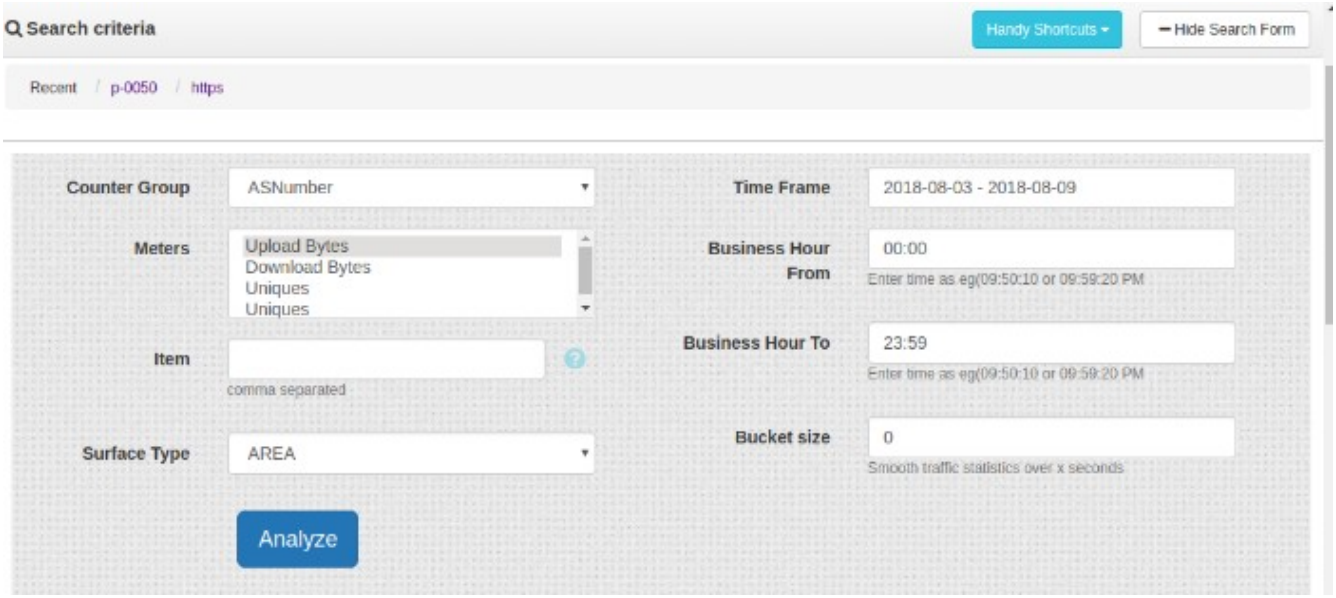


Illustration 15: Monthly traffic managment totals on a calander tool

Long term traffic management chart

Study the congestion of any parameter on any link on long term basis by the Long Term Charts tool.



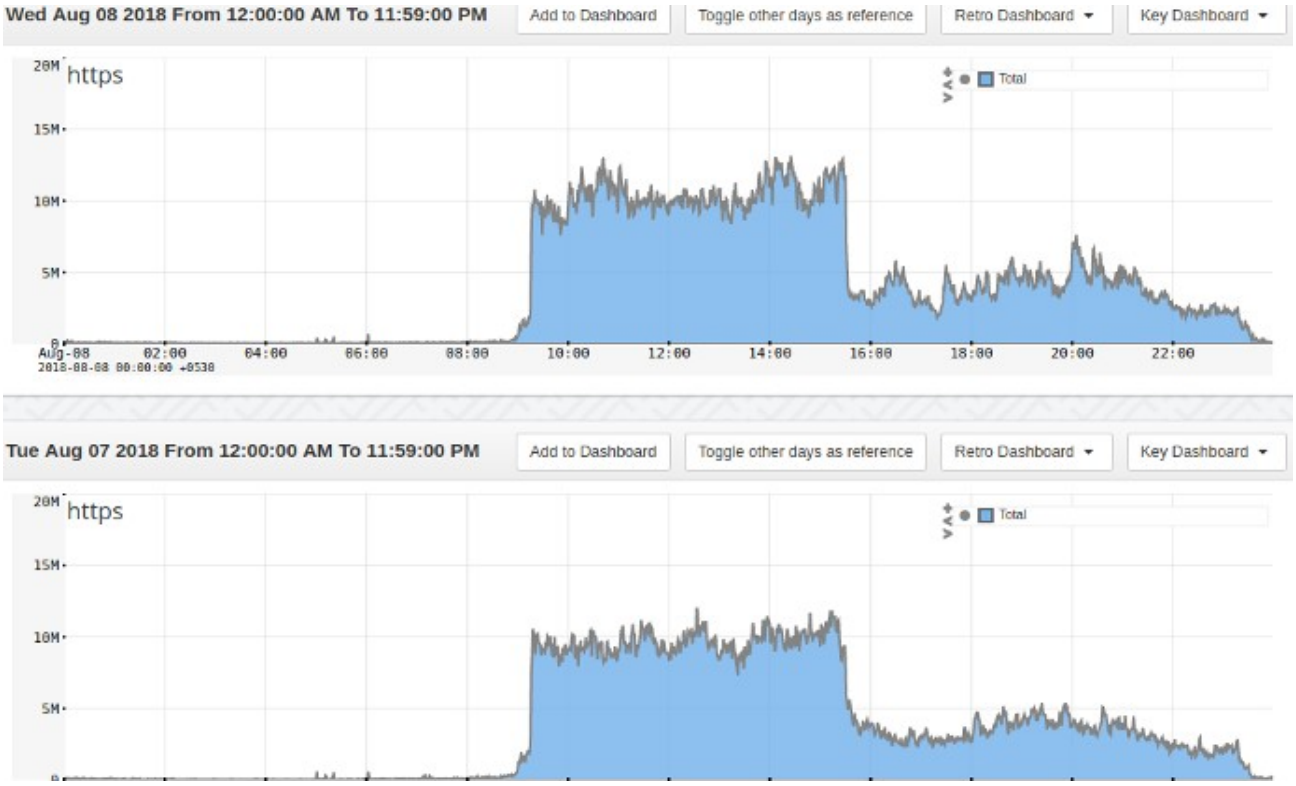


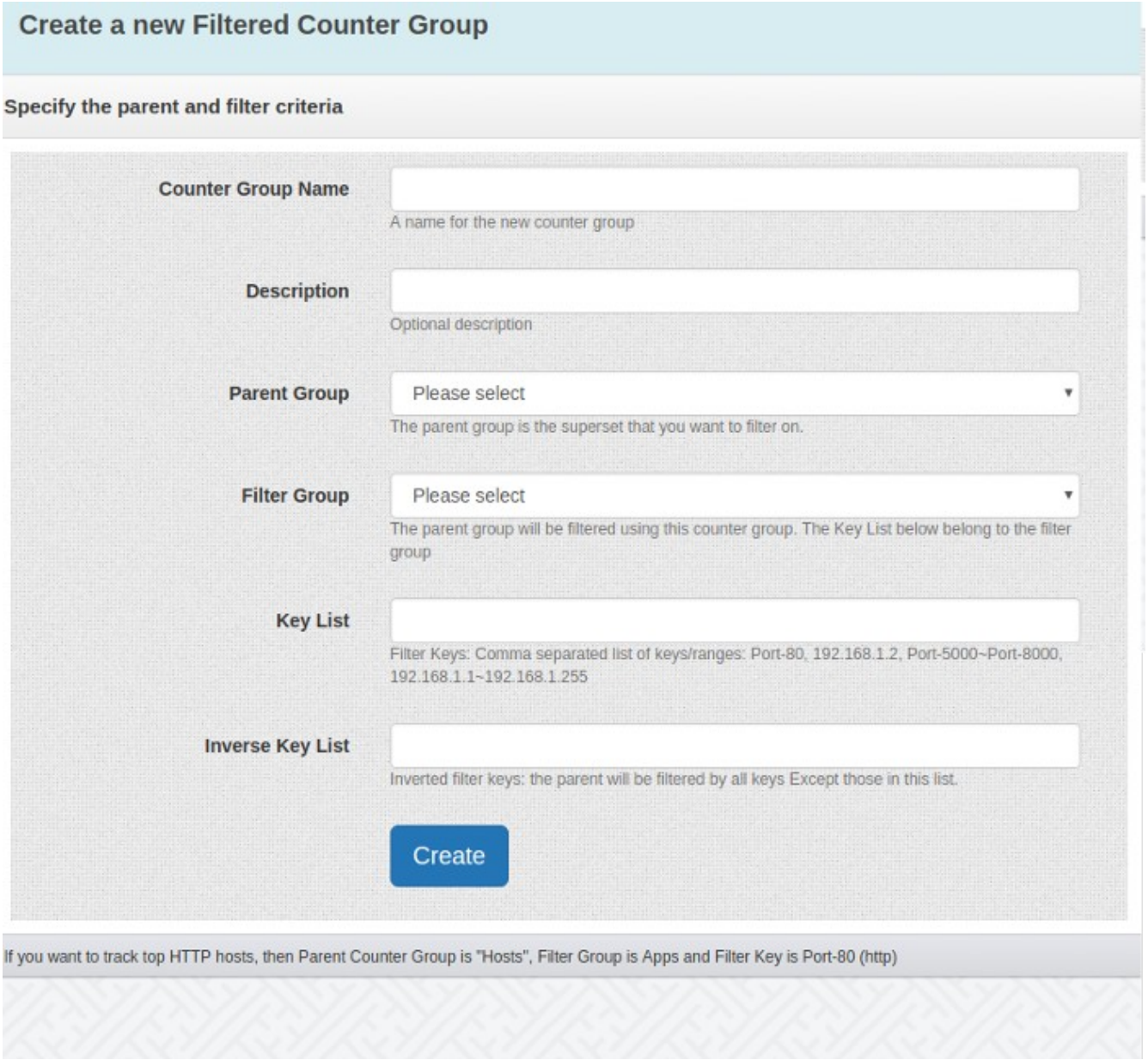
Illustration 16: Long Term traffic charts

Usage management dashboard and segmentation features

https://www.trisul.org/docs/ug/cg/custom.html#filtered_counter_groups

Traffic segmentation refers to the process of setting up filters and groups so you can see where traffic sources and destinations are and this can help tailor your services. Trisul includes various segmentation tools – such as Filtered Counters , Key Set Counters, and Rule Based Counters.

Filtered Counters – segment based on one filter



KEYSET Counter Group

Monitor traffic based on a group criteria. Such as a set of IP ranges, Locations, Services, Traffic Sources, Destinations and monitor as one group.

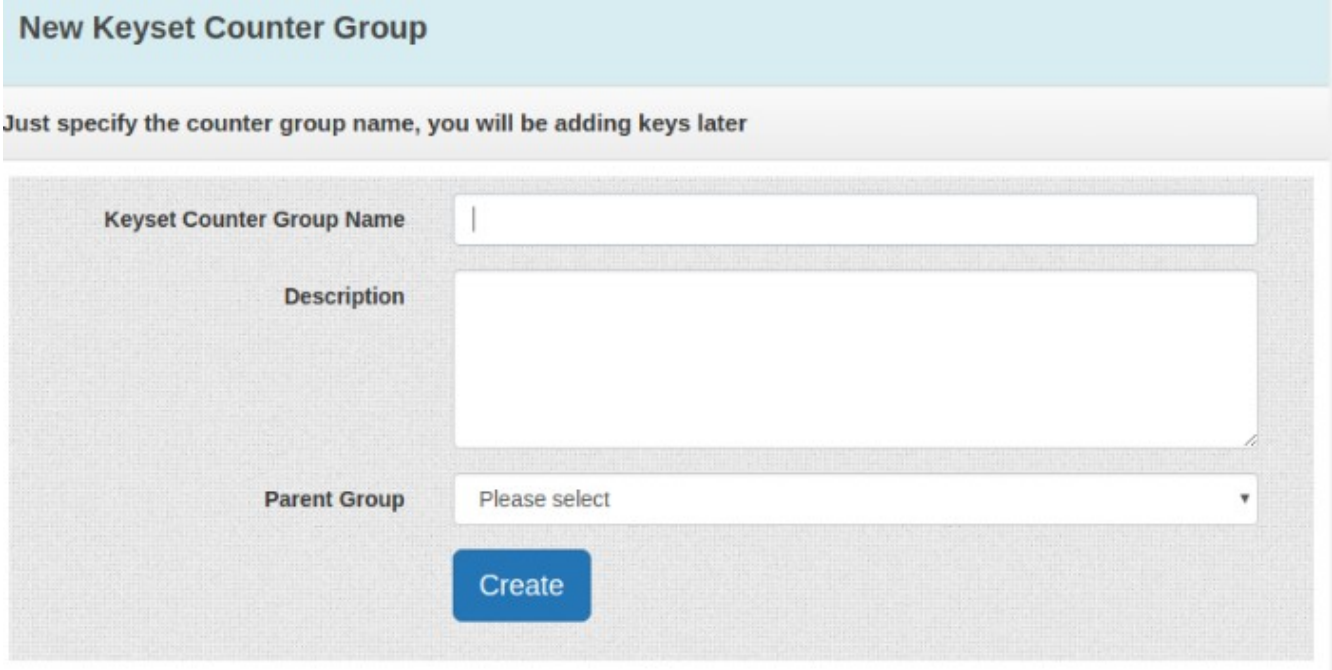
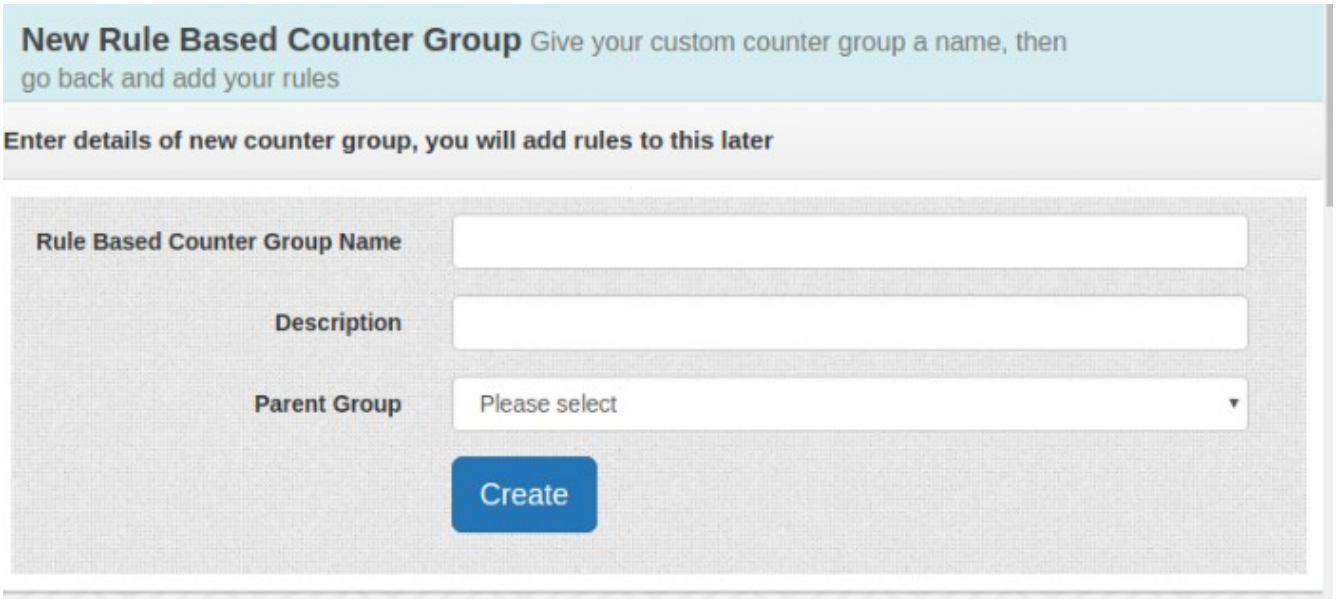


Illustration 17: Create monitoring groups using KeySets

Rule Based Counter Groups

Most flexible , specify any arbitrary rule to meter traffic. Such as Port Ranges applicable to a set of IP Addresses as Video Traffic.



Capacity planning dashboards

40 l) Capacity Planning Dashboard: Gain insight into your Traffic Management deployment to manage congested resources and measure overall business benefit with the Capacity Planning Dashboard

YES

Trisul includes over 20 tools to analyze traffic for long term capacity planning. Keey track of usage growth of all KPI and set alerts when they cross a certain threshold.

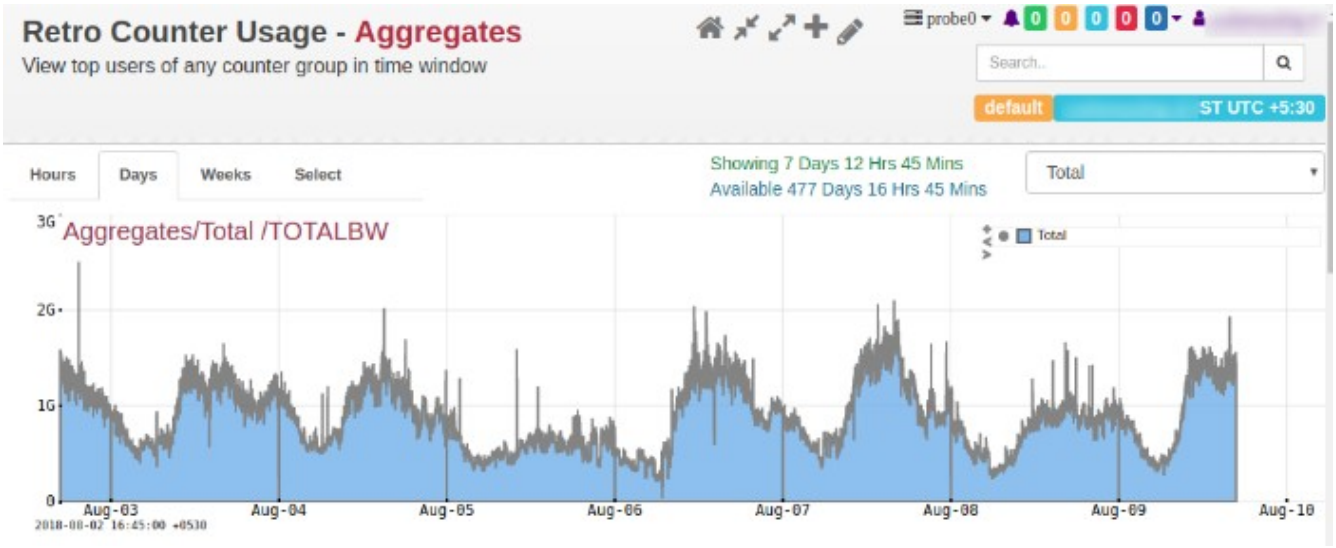


Illustration 18: Long term capacity planning by Retro Tools

Latency measurement from customers to different destinations

There are two methods to calculate latencies supported by Trisul. The first is the built in PING monitor which measures latency and uptime of several destinations and also customer IP You can also use Cisco compatiable IP SLA features to setup SLA monitoring and then report on them using SNMP from Trisul.

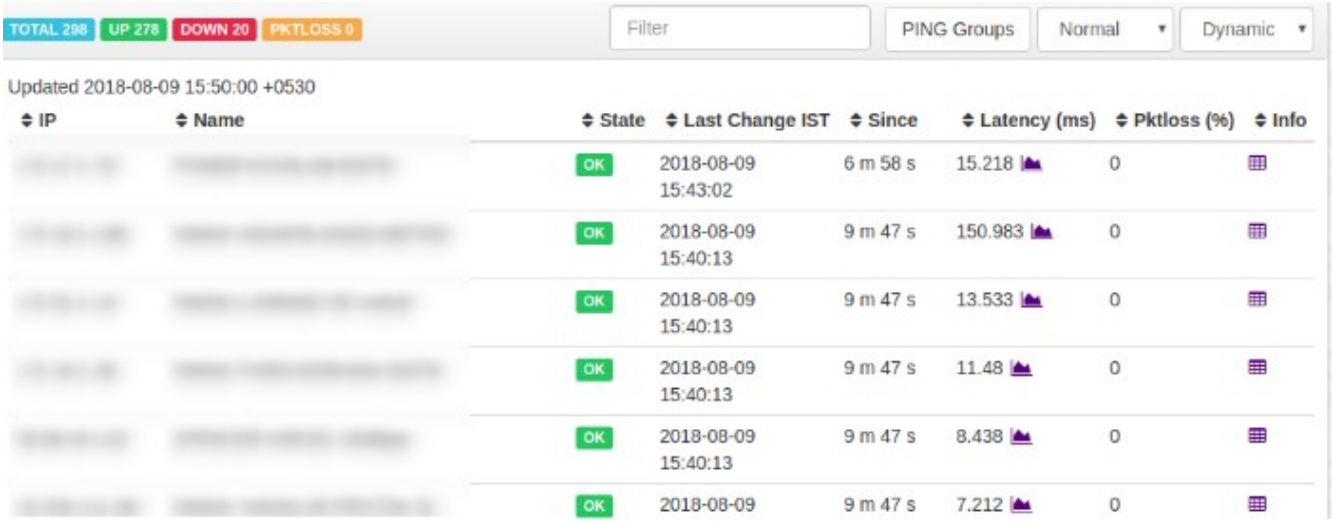
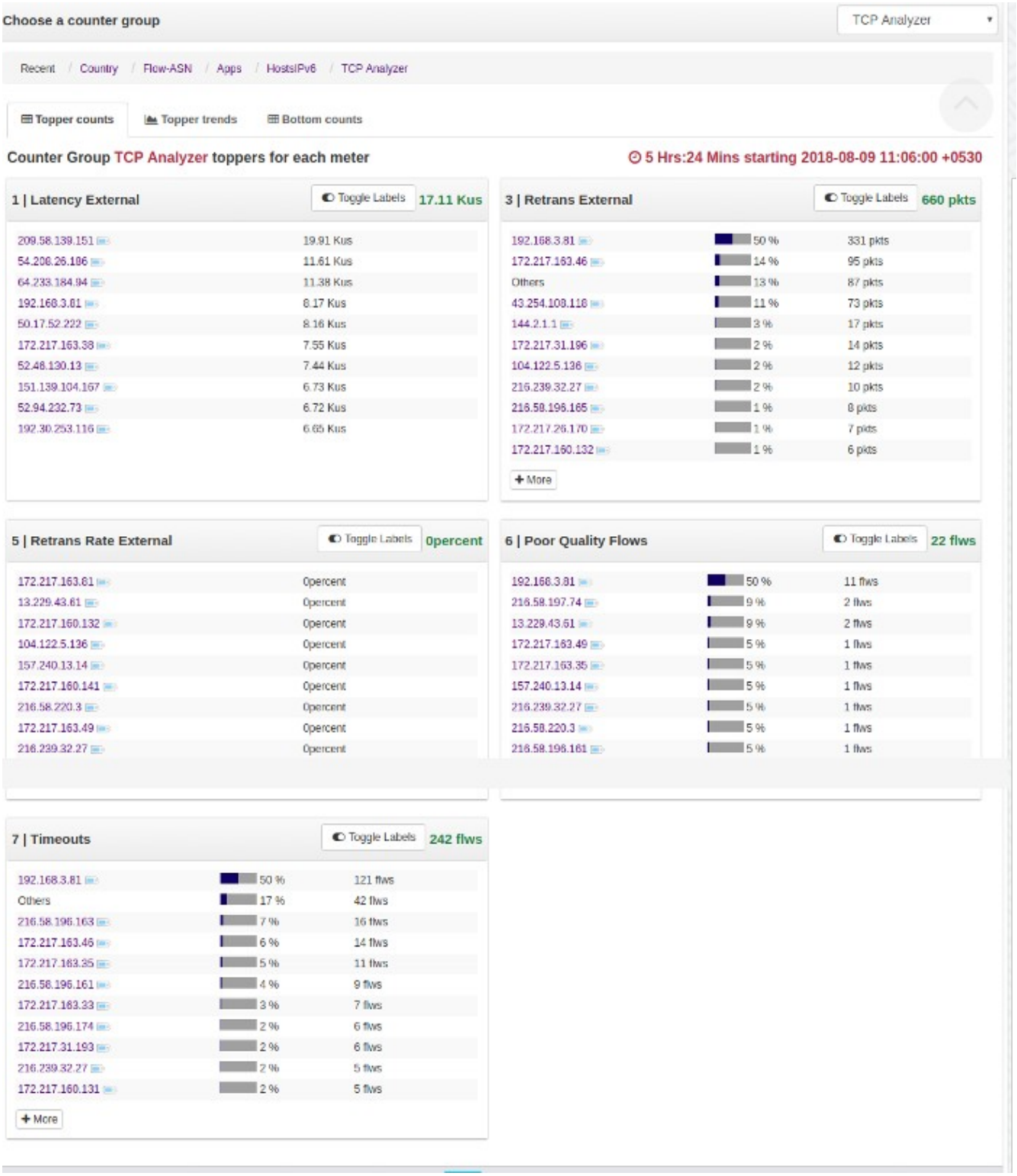


Illustration 19: Latency and Uptime from Trisul BULKPING monitor

TCP Quality Analysis

The TCP Analyzer provides per session monitoring of Round Trip Latency, Retransmissions, Timeout counts, and highlights the Ips and Segments facing the worst experience.



APPENDIX

Added advantage using flow analysis:

- Added Layer of Security
- Increased Application Awareness
- Verify bandwidth Utilization
- Improved Troubleshooting
- Capacity Planning

Analytics Dashboard

Top Bandwidth Servers, Consumers and services both inbound and outbound: This is a view of our Threats overview with Top Bandwidth:

Traffic Monitoring and Reporting

Real time monitoring of traffic over 100 KPIs tracked. It provides, complete visibility of network users, Alert on thresholds, Hosts/ ISP/ App/ Layer 2/ HTTP meters/ and Country – over 100 ways to analyse.

There are numbers of inbuilt reports and dashboards for flow analysis, if still user doesn't satisfy then Report Designer is available to build it yourself or with help from our technical support.

IP or Application Investigation

Investigate any activity of the IP and track down other hosts that might be infected and visibility of alerts and Malware affected IPs in single page,

Netflow Summary