Pluribus Insight Analytics

Real-time Network Performance Monitoring and Analytics

End-to-End Network Visibility

Deploying network visibility and analytics shouldn't be thought of as an unaffordable luxury. Rather, you should be able to extract more business value from your existing network, without any rip-and-replace, forklift upgrade to your network.

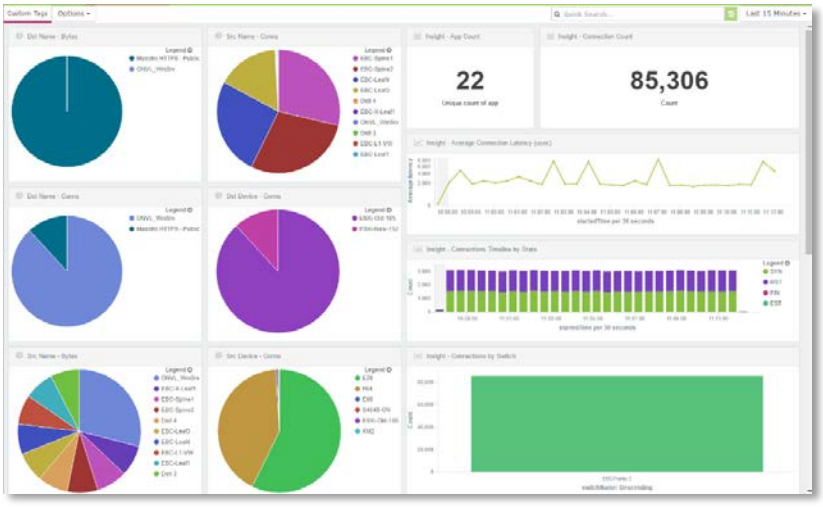
Pluribus Insight Analytics eliminates the economic and operational barriers associated with traditional monitoring infrastructure bringing flow and packet analytics to the network. Pluribus Insight Analytics can be used for broad Enterprise networking deployments extending from the data center to the campus and the branch.

Easy to deploy – inline or through a span/mirror port, it's compatible with your existing networking gear.

Cost Effective – no additional probes needed.

Easy to Use – our graphical user interface is highly intuitive; starts collecting flow and packet data in minutes.

Pluribus Insight Analytics not only has packet and flow analytics, but has the reporting and alerting you'd expect from any network performance monitoring (NPM) and analytics tool.



Easy-to-use – click any aspect to filter and drill-down, intuitively.

Network Troubleshooting

With Insight Analytics, you can quickly identify the root cause of virtually all issues in a matter of clicks, including:

- Network connection issues
- Concurrent Connections
- Connections between applications and servers

Capacity Planning

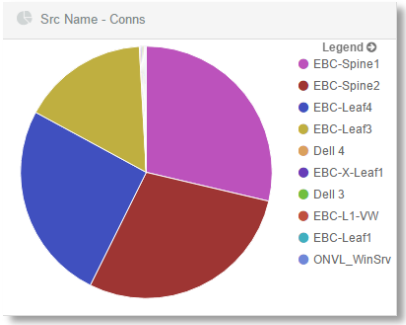
Using Insight Analytics, you can easily determine the applications, locations, users and user groups that your traffic is coming from including:

- Locations, datacenters, clouds or geography traffic is coming from
- Top talkers by total bytes or connections
- Server load balancing behavior
- Switch port load and packet integrity

Security and Incident Response

Using our dashboards, you can greatly improve your visibility and detect security-related issues within your network including:

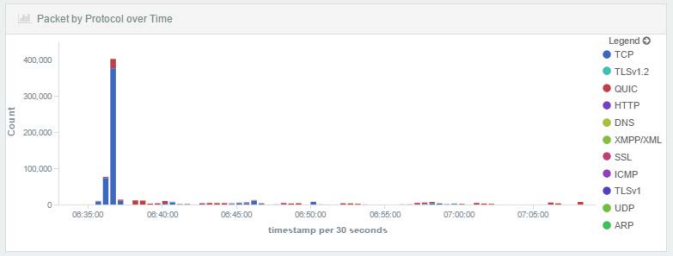
- Rogue remote desktop protocol (RDP) traffic
- DDoS attacks and traffic
- Port scan attacks
    - North/South (exteral)
    - East/West (internal)
- Non-authorized protocols for server access
- Rogue user or device access

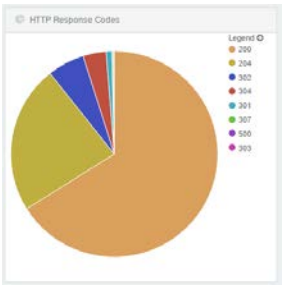


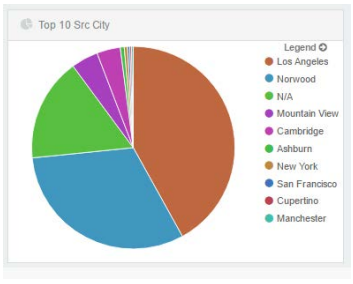
Visualize – sources by number of connections, with custom tagging to make troubleshooting a breeze.

Packet Analytics

Sample Dashboard Windows: Protocol

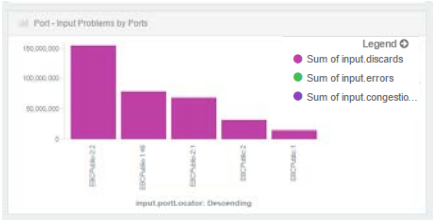






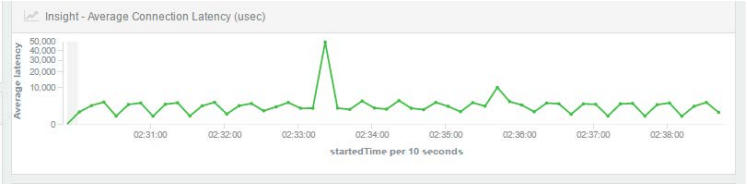
Port Data

Sample Dashboard Windows: Input Traffic, Problems



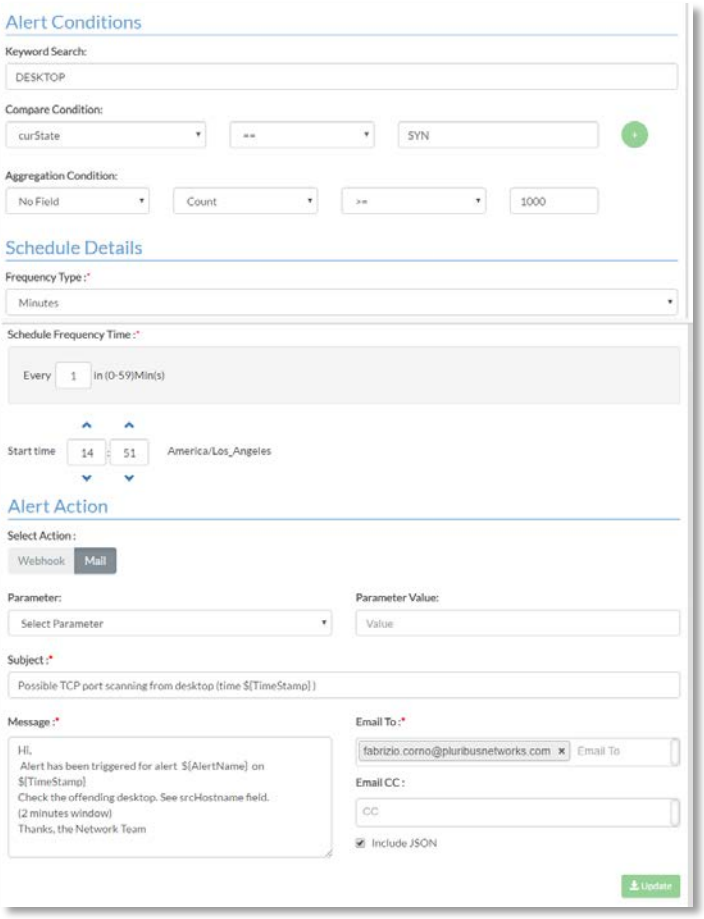
Flow Data

Sample Dashboard Windows: Latency, State



Alert Configuration

Security Example: Desktop Malicious Port Scanning



Pluribus Insight Analytics

Pluribus Insight Analytics eliminates the economic and operational barriers associated with traditional monitoring infrastructure bringing flow and packet analytics to the network. Pluribus Insight Analytics can be used for broad Enterprise networking deployments extending from the data center to the campus and the branch.

Learn more at **www.pluribusnetworks.com/network-performance-monitoring/** and **@pluribusnet**.

March 2017

Pluribus Networks, Inc., 2455 Faber Place, Suite 100, Palo Alto, CA 94303
1-855-GET-VNET / +1 650-289-4717