SOLANA NETWORKS *Visible Intelligence*

SMARTFlow

Network Anomaly Detection

Features

- Flow-based monitoring and data collection
- Flow-based data storage
- Pinpoint security threats such as address scans, Botnets and DoS attacks.
- Identify Network Anomalies
- Supports Netflow, Sflow, Jflow
- Quick diagnosis of Network traffic issues
- Charting and Reporting
- Alarms & Email notification
- Available as a software or hardware solution

Benefits

- Protect the network
- Safeguard information
- Reduced network downtime
- Network-wide visibility
- Scalable solution
- Detect zero-day threats
- Identify top talkers

Flow-based Network and Security Monitoring

SMARTFlow software utilizes network analysis and anomaly detection technology to detect security threats and network performance issues. Botnets, Address Scans, Denial of Service (DoS) attacks are but a few of the threats that SMARTFlow can detect.

SMARTFlow software collects flow-based data from routers and probes, storing the traffic summaries in a database. It applies Solana algorithms to the flow data to characterize network application usage, pinpoint application performance issues and security threats.

SMARTFlow's rich visualization and GUI allows the user to navigate analysis results and reports. Integration of SMARTFlow with Solana's SMARTHawk Network Mapping and Route Analytics product enables powerful new features.

SMARTFlow's distributed architecture allows it to scale seamlessly to support enterprise networks of varying sizes.

Flow-based Data Collection

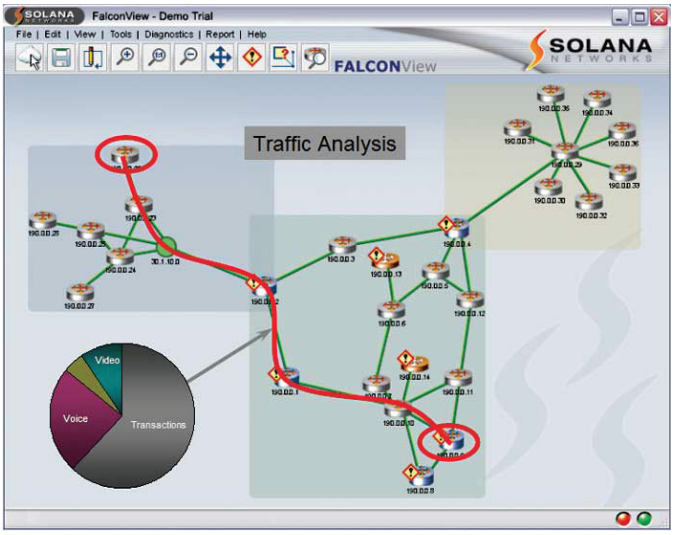
SMARTFlow collects flow-based data such as Netflow, Sflow or Jflow from network routers and switches. It supports Netflow v5 and v9. The collected flow data is stored in distributed databases on various SMARTFlow sensors.

Network Anomaly Detection

SMARTFlow applies intelligent network anomaly detection algorithms on the collected flow data. These algorithms detect anomalous network traffic from Gigabytes and Terabytes of network traffic. Security threats such as Address Scans, Botnets and Trojans can be detected.

Application Analysis

SMARTFlow's application classification algorithms allow it to map network flows to applications. It provides information on which applications are consuming the most network resources. The analysis greatly aids network planning and troubleshooting.



Custom Charts and Reporting

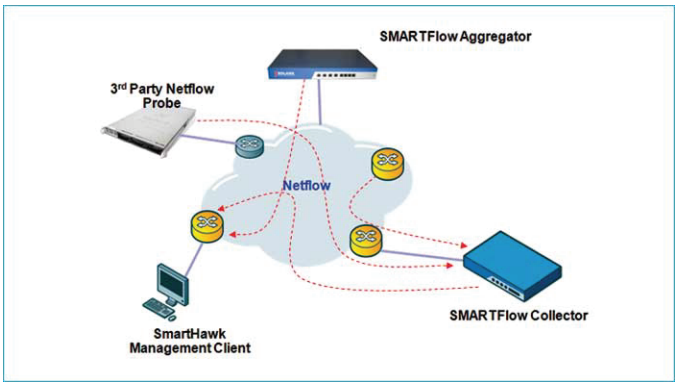
SMARTFlow's reports provide insight into: (i) Top Talkers (ii) Geographic traffic breakdown (iii) Traffic breakdown by subnet (iv) Application traffic breakdown (v) Bandwidth accounting and (vi) Class of Service (CoS) Traffic breakdown. Analysis can be undertaken with current or historical data.

Alarming & Notification

Network events and security incidents detected by SMARTFlow result in a GUI alarm being raised. SMARTFlow's event notification can also be raised via customized email alerts.

Integration with Network Map

SMARTFlow can be integrated with Solana's flagship Route Analytics product SMARTHawk, thus providing a powerful perspective on network topology and traffic. As an example it can provide traffic breakdown on a specific network path.



Multiple SMARTFlow Devices

SMARTFlow scales seamlessly to collect flow-based data from large numbers of routers. Distributed SMARTFlow collectors send analyzed Flow data to an aggregator. Sampled Netflow is also supported.

Deployment with Probes

SMARTFlow can collect flow data from Routers or probes that support Netflow/Sflow. The probes can be deployed inline with traffic or on TAP ports

Specifications For Appliance Hardware Version

Protocols	Netflow, Sflow, Jflow
Form Factor	1U Rackmount
GUI	Windows, Linux, Solaris
Dimensions	426 x 305 x 43.5mm
Certification	CE/FCC Class A
Net Weight	8 kg
Power	90-260VAC, 50-60 Hz, 180 Watts
Network Interface	4-port 10/100/1000 Base T
Operating Temp.	0 to 40 C
Storage Temp.	-20 to 80 C
Relative Humidity	10 to 90% (non-condensing)

SOLANA NETWORKS

T 613-596-2557
F 866-647-2429
web www.solananetworks.com
email info@solananetworks.com

GET PLUGGED IN.