NetFlowAuditor

NetFlow Auditor Product Features and Unique Capabilities

NetFlow Auditor collects NetFlow data using a unique patent pending collection methodology that highly reduces storage and overheads while enabling full-flow forensics analysis and insight of your Network.

NetFlow Auditor provides granular, scalable and flexible NetFlow Analysis providing benefits to various levels within an organization ranging from network performance and security specialists to data-center managers, capacity planners, network architects and business decision makers.

The base features of NetFlow Auditor:

<u>NetFlow Monitoring</u>

- Monitoring without probes:
  NetFlow Auditor utilizes NetFlow (version 1, 5, 7, 9) and IPFIX. There is no need for probes or other intrusive methods to detect traffic.

- Network bandwidth monitoring:
  Provides reports of current, average and peak bandwidth utilization across NetFlow-enabled devices or interfaces, on all IP's, all protocols, all ports/applications, all QoS/DSCP and many other parameters.

- Network usage monitoring:
  Provides detailed short term and long term usage information of all IP's, all protocols, all applications, all QoS/DSCP, etc…Fields of traffic information collected from NetFlow include source/destination IP's, port/application, protocol, DSCP,interface, AS numbers and many other parameters.

- Filtering ability
  Capable of creating filtered reports based on any supported NetFlow field (show me traffic between certain subnets, certain servers, using certain applications...).

- Real-time and long-term analysis and data storage
  Provides both real-time, high-definition analysis as well as long-term, panoramic reporting and trending on traffic.

- Seamless integration between real-time and long-term analysis
  Drill down feature allows the users to easily tour from a long-term trend report to the detailed root cause of the trend.

The 5 Unique Capabilities of NetFlow Auditor:

1. **Baselining**

• Short term and long term comparative analysis of any and every element. e.g. interface/IP/Location/Application or a combination thereof for a particular period compared against a previous period:

- this minute versus last 20 minutes;
- this hour versus last 6 hours;
- this day of the month versus other days of the month or this day every month;
- this weekday versus each other weekday or this weekday versus every other same weekday for last 12 months;
- this week versus last 4 weeks;
- this month versus last 12 months;
- this quarter versus last 4 quarters;
- this year versus last year;
- what was my Server Farm usage this quarter compared to last quarter?

• Comparative analysis of each element across the time line. Gives the ability to identify which element caused the change and when.

2. **Powerful and Flexible Analysis**

NetFlow Auditor can do analysis on any combination of data fields simultaneously (e.g. usage, packets, flows, utilization, etc) and sort data by any field. Menu bars and shortcuts facilitate rapid analysis.

• Packet Size analysis - Network teams can use this to create reports such as DSCP, Application and Packet Size to identify anomalies.

• Full Flow analysis - (Not just Usage or Utilization or simple conversations) Flow analysis enables the Network Specialist to identify "noise".

• Ability to count records as part of a result to quickly identify excessive flows or change. Any record combination can be counted, e.g. Counting all internal IP's with number of IP or Port conversations enables quick identification of P2P users or other multi threaded conversations and Denial of Service attacks.

• Ability to analyze by standard deviation to identify what aspect has changed the most in a specific period, e.g. what application has changed the most in the last 2 hours can lead to early detection of issues. Coupled with a threshold SNMP trap enables identification of usage that can grow dynamically over time via any "application/service port". Identify Worms/ increasing flows/ data floods.

- Bi-directional analysis - show forward and reverse conversations and In vs. Out conversations to quickly identify which side of the conversation is responsible for traffic usage/flows.

- Stacked graphs - enable cross over of various data, e.g. report on key business servers and watch only known ports (services/applications) that are used on those servers. A stacked bar analysis shows each IP and the "layers" of applications stacked will show the number of applications being used on each server. The opposite is also possible - show my key business servers where "unknown" applications are trying to communicate with servers.

- Business group analysis: IP addresses can be categorized into business groups and accordingly traffic associated with an IP address can be stamped with the business group information of this IP address. This feature provides the capability of splitting traffic by business groups, which is particularly useful in billing.

3. **Unattended (proactive) Analysis, Alerting and Reporting**

- Reporting - Ability to create any combination of analysis and automate the output as a report periodically. E.g. end of a week, end of a quarter, end of a month, end of an hour, every 23 days etc… Reports can be written to saved and/ or emailed to one or more recipients. A report can be repeatedly updated or time stamped e.g. A data center manager wants to know the server usage trends in his environment over time and monitors this every week, month and quarter to make decisions on how to position his servers and provision services. Reports can take the format of CSV file to record events that occur for input into other systems. For example collecting when unknown IP’s use key business services will enable the compliance team to identify risk over the long term.

- Alerting - Ability to create any combination of analysis and automate the output as as an alert once certain criteria are met e.g. bandwidth utilization is over a certain threshold. Alerts can be tuned to reduce or eliminate false positives. Alerts can take the format of SNMP trap to a trap receiver to raise a trouble ticket with the correct team/person.

- Templates - Creation and customization of any analysis combination into a template to be used in the drill down menu.

4. Data Collection Tuning

- NetFlow Auditor can be tuned to collect only the data required. For example NetFlow Auditor can collect all network conversations with per minute granularity in one part of the network where detailed forensic information is required and/or can be configured to collect traffic information at a one hour granularity/view where only high level reporting is required.

- Self maintaining rules enable levels of granularity to be set to "protect" the collector/server in the event of a major worm outbreak that can cause NetFlow data to become excessive.

5. Scalability, Fault Tolerance, and “Self Healing”

- NetFlow Auditor scales to collect at rates up to 1 Million flows/second.

- High-fault tolerance and self-healing capability: Each process and function/thread is monitored for health and NetFlow Auditor heals itself.

NetFlow Auditor

www.netflowauditor.com