



Everything you have been waiting for in a Flow-Based Network Management solution.

Built in Baselining, Event Alerting, Root Cause Analysis, Traffic Accounting and more...

NetFlow Auditor Product Features

From the moment NetFlow Auditor collects NetFlow data it uses unique patent pending collection methodology that highly reduces storage and aggregation overheads whilst enabling superior analysis and insight of your Network and its connected systems in both real-time and over the long-term.

NetFlow Auditor provides granular, scalable and flexible NetFlow analysis.

NetFlow Auditor can suit various requirements regarding a networks usage or the specific communications of connected locations, systems, devices or users. The information is targeted to various levels within an organization ranging from network performance and security specialists to data-centre managers, capacity planners, network architects and business decision makers.

The base features of NetFlow Auditor:

1. NetFlow Monitoring

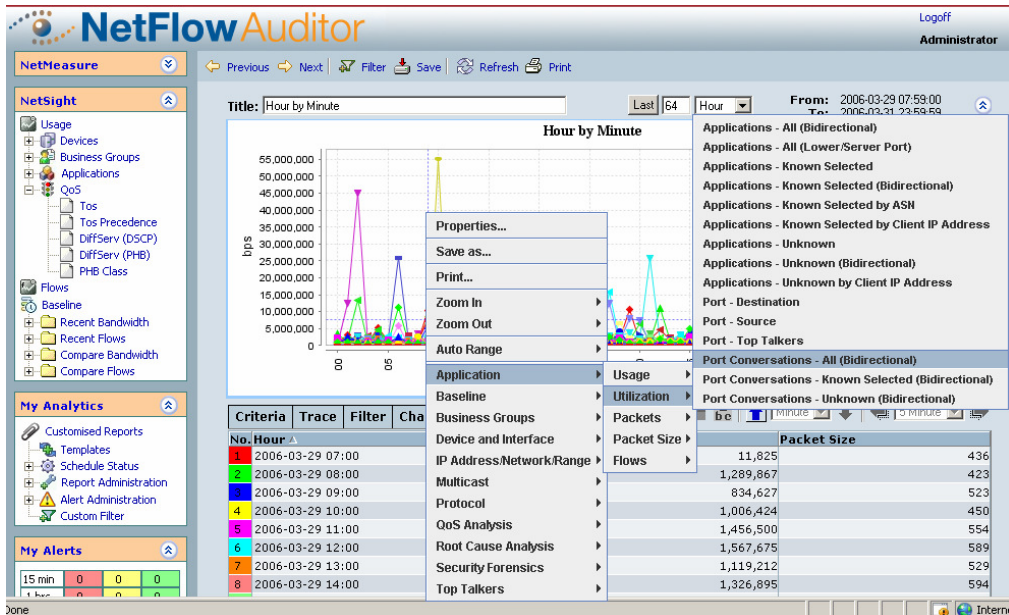
- **Monitoring without probes:**
NetFlow Auditor utilizes NetFlow (version 1, 5, 7, 9) and IPFIX. There is no need for probes or other intrusive methods to detect traffic.
- **Network bandwidth monitoring**
Provides reports of current, average and peak bandwidth utilization across NetFlow-enabled devices or interfaces, on all IP's, all protocols, all port/application, all QoS/DSCP, etc...
- **Network usage monitoring**
Be capable of doing analysis on current, average and peak usage of all IP, all protocol, all application, all QoS/DSCP, etc...
- **Filtering ability**
Capable of creating filtered reports based on any supported NetFlow field
- **Real-time and long-term analysis and data storage**
Provides both real-time, high-definition analysis as well as long-term, panoramic report on traffic
- **Seamless integration between real-time and long-term analysis**
Drill down feature allows the users to tour from a long-term trend report to the detailed root cause of this trend smoothly.

- Abundant information
Fields of traffic information collected from NetFlow includes IP, port/application, protocol, DSCP, interface, autonomous system number, etc...
2. Ancillary features
- Automatic device refresh
Detects new routers or switches automatically from a NetFlow stream.
 - SNMP probing
Interrogates routers for the router and interface information with SNMP
 - Domain name resolving
Resolve IP address to domain name in an efficient way.
 - Flexible licensing
Provides flexible Device based licensing to suit customers with all level of budgets.

The unique advantages 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 like 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. E.g. 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 ability

NetFlow Auditor can do analysis on any combination of data fields simultaneously (e.g. usage, packages, flows, utilization, etc), sort data by any field, and display by any top items (i.e. top 10, top 20, etc). At the same time menu bars and shortcuts provide abundant while easy ways to do quick analysis.

- Packet Size analysis - Network team 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. Count all

internal IP's with number of IP or port conversations enables quick identification of P2P users or other multithreaded conversations or 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 conversation 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 want to watch that only known ports (services/applications) 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 would 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 analysis, alerting and reporting flexibility
- Reporting - Ability to create any combination of analysis and automate the output as 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 disk or emailed to one or more recipients. A report sent to a disk destination can be repeatedly overwritten or time stamped e.g. A data centre 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 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 drilldown menu.

4. Data Collection Tuning:

- Sometimes it is not always necessary to collect all the data - e.g. a switch running in Hybrid mode reports all the data from all the interfaces. NetFlow Auditor can be tuned to collect only the data required.
- Collection over the long-term is limited in most applications - NetFlow Auditor can be set to keep all info down to the hour or just the info required. E.g. for long term capacity planning in a data center. It would be sensible to store each of the key servers (or all the servers) but to ignore the client IP while retain the location information of the client. Store the Server Port but not retain the client Port. This enables the customer to store years of relevant data on his environment without unnecessary overhead. Fully tunable for those folks (like defense) that do want to keep it all
- Self maintaining rules that enable levels of granularity to be set to "protect" the collectors without "kludging up" with data in the event of a major worm outbreak that can cause NetFlow data to become excessive. Our default settings for example collect all data but in event of 100000 flow records per second we ignore client port. (Also useful for Sales deployments where unknown variables exist when customers choose to deploy on low grade computing equipment)

5. Scalability:

- Collector process can be run using "Standard version" or "Enterprise version". In Standard version, data collection, processing and aggregation are performed by Java codes, while Enterprise version has a loosely coupled high-speed primary collector written in C language. Data is collected, tagged and dumped to disk for later "Java" Processing. This enables data to be collected at points where:
 - a) the customer data volume is huge (e.g. a core), or
 - b) the customer is required by law/process to separate any identifiable information/database from collection point, or
 - c) where Netflow does not exist the "Enterprise collector" can run as an Ethernet Sniffer and sniff directly from a mirror port or a tap.
- NetFlow Auditor is made up of two tightly bundled collection mechanisms (i.e. real-time and long-term). For some very large Telco environments real-time collection does not make sense and thus long-term collection can be run on its own in "Telco mode".
- High-fault tolerance and self-healing capability: software is "intelligent-agent" based technology. Each process and function/thread is monitored for health and NetFlow Auditor and other DigiToll products heal themselves. Data recorded in an anomaly is handled "nicely" ensuring minimal loss (a minute or two). If running Enterprise usually no loss. This means very high-fault tolerance.