Using NetFlow Auditor to assist in identifying Distributed Denial-of-service (DDoS) attacks and other network behavior anomalies.

Rafi Sabel, IdeaData (August 2009)

Abstract

This Paper covers how denial of service attacks (DoS) and distributed denial of service attacks (DDos) can be identified early to mitigate and attack. We will reflect a method to alert when changes occur outside of learnt baselines and how new patterns can be recognized when security analysts have access to technology that provides high visibility of traffic from utilization, conversation, packet analysis, packet size distribution analysis and byte usage and standard deviation methods.

A game-changing Network Auditing technology called NetFlow Auditor has the potential to enhance the security, reliability, resilience, and trustworthiness of your digital infrastructure which can be used to assist in identifying a DDoS flood or a slow Denial of Service attacks and other network behavior anomalies including Peer-to-Peer (P2P) usage. At the end of this paper we will focus on the various forensic methods available in NetFlow Auditor that can be used for Baselining, Alerting and Tracking an attack.

We will show you how to apply NetFlow Auditor filters for high scale collection environments. We will also cover some of the key architectural benefits of the NetFlow Auditor design.

Introduction

A denial-of-service attack (DoS) is an attempt to make a computer resource unavailable to its intended users. The reasons for such an attack may vary and can take many forms. The attack can be from a single source or may be a widely distributed denial-of-service attack (DDoS).

Targets

High-profile sites or services are usually the typically target such as financial organizations and critical infrastructures such as electricity or water or in telecommunications such as the “root nameservers” that are used to manage the internet infrastructure. As tools become easier to use and more accessible, attacks are being made on even small business by disgruntled employees, competitors or extortionists. Even if the attacker causes the systems to run inefficiently it may cause other negative consequences. The need to identify DoS and DDoS attacks is vital as key systems become increasingly more interconnected and open to attack by increasing organized ecrime that includes data-theft, fraud, international crime syndicates and cyber terrorism as well as politically motivated attacks.

Methods

Various methods can be used to create a denial-of-service and tools are freely available that allow an attacker to creatively flood or overload a receivers computer. The intention is to overload the victim’s computer to the point where the computer or the associated communications infrastructure cannot correctly function or respond to valid traffic.

The list of DoS/DDoS attack methods are varied and continue to grow. Attacks can be directed at any network device, including attacks on routing devices and web, electronic mail, or Domain Name System servers. Some well known methods of attack include ICMP flooding, Teardrop, Peer-to-peer, Permanent denial-of-service, Application level floods, Nuke, Distributed, Reflected, Degradation-of-service, Un-intentional, Denial-of-Service Level II and Blind Denial-of-Service. These methods usually depend on flooding of some sort.

Some newer attacks include slow denial of service attacks where connections are held

open by sending partial HTTP requests and subsequent headers are continually sent at regular intervals to keep the sockets from closing.

Slow denial of service attacks are much harder to detect because other users of the system can continue to use the system whilst sockets are slowly cannibalized until it is too late and the system is fully used by bogus clients. This is not a TCP DoS attack, because it is actually making a full TCP connection and not a partial one. However it is making partial HTTP requests. It's the equivalent of a SYN flood but over HTTP.

In some cases a slow DoS attack on a web server can be used as a diversionary tactic and can return to normal almost instantly. The nature of these connections is that they remain connected for a much longer period than normal, they may only require a few hundred requests but these are at long term and regular intervals, as opposed to tens of thousands on an ongoing basis, various alerts can be created to address slow denial of service attacks and the ability for a NetFlow Auditor professional to see them.

Other kinds of DoS attacks can be as a result of Infections from worms, spyware, malware introduced by email, web surfing or guest PCs, as well as the installation of unapproved applications, are examples of how threats can infiltrate a network. Others can be created as a result of unintentional oversights such as installing personal firewalls on every laptop in an organization where a firewall update from hundreds of laptops at once can affect the communications infrastructure.

Today, attacks often involve many hacked computers that allow the compromised computer to unwittingly become part of a networked group of computers called a botnet. A single computer on its own sending out a small attack on an infrastructure may do little damage and may even go unnoticed. However, multiply that by 500,000 times where computers in the form of a botnet send out the same or varied attacks from all over the world at the same time to a single point and you've got a real problem. This is the nature of a Distributed Denial of Service Attack (DDoS).

A botnet is made up of computers that have been compromised. Computers are currently compromised by Trojan viruses distributed via email or transferred from websites that appear to carry useful information but instead are traps set to infect unsuspecting web surfers. Antivirus software today is believed to have about a 50:50 chance of being able to pick up a new Trojan.

Once a computer becomes infected it begins to communicate with a botnet master via IRC, P2P or another protocol. Each of these zombie computers once connected to the Internet try to self replicate and extends its reach to try and infect as many computers as it can. The Zombie may forward transmissions (including spam, viruses or DDoS attacks) to other computers on the Internet, without the knowledge of the computer owner. The numbers of computers compromised with bot software are in the hundreds of thousands and have become known as a zombie army. Botnet software enables attackers to rent or directly control a botnet and can command the bots to attack other computers and organizations and steal information from infected systems.

Detection

It is difficult to distinguish between a P2P and a DDoS attack as both can display a similar inbound connection profile. The ability to identify P2P traffic profiles is important as P2P systems can be vulnerable to index poisoning or to routing poisoning, and can thus be exploited as a massive DDoS flooding engine. P2P activity therefore may be the result of an attack.

P2P acts as both a client and a server. Its profile is that it downloads data from multiple IP's simultaneously and makes search requests from multiple peers for a

file. The result is a "flood" of peer broadcaster IP's to a single destination peer. Port monitoring is almost pointless as most P2P software port hops. Initial P2P traffic may begin with TCP requests to root servers but can instead communicate with known peer neighbors for search requests.

In the case of a P2P DDoS created by index or routing poisoning peers will attempt to download data from a computer that may be a key server in a target IP Range such as a web server or mail server. The server will respond with an error but the poisoned peers will continue to retry and depending on the popularity of the file the number of attempted connections will increase as long as peers continue to swap the IP locations published in the poisoned indexes. Even internet phone services such as Skype that use P2P technologies and Vonage could provide a means for cybercriminals to send spam and launch attacks. The packet distribution signature profile of a P2P DDoS attack at least has the benefit of being more structured and therefore less stealthy and therefore manageable if detected early.

Using NetFlow Auditor detection methodologies

Each attack has its own signatures and generation of general and specific traffic patterns. A Network Security Analyst and Performance Engineers need to have full traffic visibility to be able to analyze data from all perspectives to identify new kinds of attack signatures and to set up baselines on devices, interfaces, servers or locations to alert when changes occur.

NetFlow Auditors ability to scale in Flow collection and flexibility makes it an ideal solution for various network usage auditing requirements. The NetFlow Auditor framework has Data Collection Tuning options that allow simultaneous collection of Real-Time and Long-Term data recording. The Long-Term data recording mechanism can be configured to store data in either increments of 5, 10, 15 30 and 60 minutes and Real-Time data is stored down to the minute for as long as disk space will allow. This enables NetFlow Auditor to be used for trending and baselining identification methods to find either short term attacks or longer slow denial of service attacks or other stealthy attacks.

NetFlow Auditor can perform analysis on any combination of data fields and measurement criteria; usage, packets, flows, packet size, utilization and record counts. Menu bars, right click drilldowns, baseline alerting, automated reporting template shortcuts all facilitate in providing rapid analysis to effectively measure usage, trending patterns, baselines, averages, peaks and troughs, and standard deviations so that fast and appropriate action can be taken to reroute the packets that fit the attack profile.

Peer-To-Peer content detection methodologies - IdeaData have invented new methodologies that leverage NetFlow Auditor's flow recording technology with the original objective to assist in profiling users that trade in illicit or Copyrighted content on P2P networks. This new technology can also be used to the advantage of organizations that need to identify DDoS profiles that occur over multiple disparate points and pass back top profiling details to a central NetFlow Auditor for auto discovery of common attacks to multiple points.

Packet Size analysis - Provides a detailed view of network traffic by packet sizes. Use this information to optimize VoIP traffic as well as to identify packet size anomalies.

Count analysis - 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 Port Scanners, P2P users, DDoS attacks or other multi threaded conversations. Identify long lasting flows or conversations.

NetFlow Auditor Count Analysis enables fields to be grouped in order to count the number of connections (flows), packets or physical file records to trigger an alert and assist the security forensic analyst to analyze the pattern of the attack.

Standard Deviation analysis - Analyze traffic patterns by standard deviation to identify what aspects have changed the most in a specific period, e.g. knowing what application has changed the most in the last 2 hours can lead to early detection of issues. Identify Worms, increasing flows or data floods.

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

Cross section analysis - Stacked graphs enable comparison of any two network traffic parameters. As an example, a stacked bar QoS analysis can graphically show the details of each application running within every class of service.

Custom Group analysis - IP addresses can be grouped by Location, Customer, Application and Services. Network traffic detail can now be categorized in logical groups for reporting, billing and capacity planning.

Baselining analysis - Short term and long term comparative analysis can be performed on any and every element. For example, interface/IP/Location/Application or a combination thereof for a particular period compared against a previous period. Comparative analysis of each element across the time line gives the ability to identify which element caused the change and when.

Baseline Alerting can then be activated to learn and watch.

Percentile analysis - Short term and long term percentile analysis can be calculated. Most commonly known for its benefit in Billing also has a large benefit for security and alerting. For example a burst may occur once or may occur in ever increasing frequency. A percentile analysis of a threshold event will provide an indication of change. This should be set in conjunction with Baseline analysis.

QoS analysis - A network provider can change QoS markings to make it more difficult to conduct DoS attacks. QoS policies can help to reduce the effects of Dos and DDoS traffic floods and keep key applications available during attacks. The first step in deploying QoS is to profile applications to determine what constitutes a normal versus an abnormal flow.

NetFlow Auditor does not make claims that it can identify every DoS attack or network anomaly as this will depend on the environment, the load and the dynamic nature of attacks. NetFlow Auditor in its out of the box setting may not be ideal for your immediate flow and may need to be tuned. This process is easy to learn and allows you to scale the NetFlow Auditor Collection Tuning to best fit your objectives and flow size.

In environments with many flows, it is always advisable to use sampling on the routing/switching device and to set the corresponding sampling ratio in NetFlow Auditor. This substantially reduces the number of flows NetFlow Auditor has to collect and store and allows higher granularity of the data providing substantially greater visibility. NetFlow Auditor should be considered as part of a total defense in depth solution and can be run concurrently with other NetFlow Auditor configurations and 3rd Party tools. Where high compliancy of flows is required consider deploying two NetFlow Auditors; one for full flow collection and a second aggregated collection for fast analysis.

Upcoming NetFlow Auditor version 4 includes full TCP Flag analysis that includes the ability to analyze flags in detail further

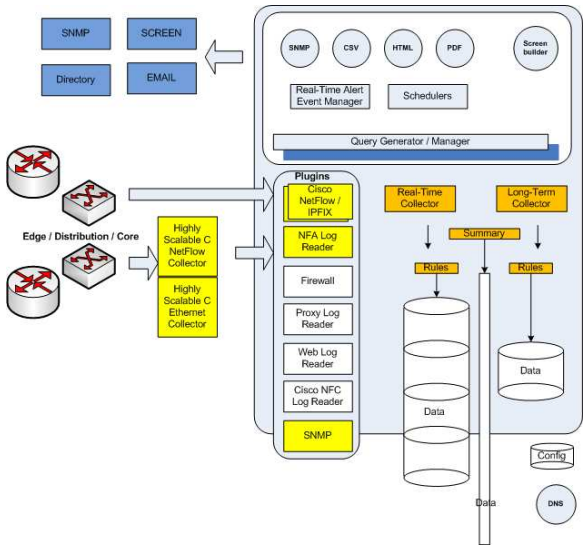
thereby improving the ability to analyze what kind of DoS attack is occurring. ECN flags are also included to provide early analysis of congestion caused by an attack.

Flow analysis systems themselves can be vulnerable to meltdown in DDoS attacks where the number of unique flows soon become too unwieldy for a system to manage and the Flow analysis systems becomes useless.

NetFlow Auditor has a number of methodologies that enable it to be highly fault tolerant and limit exposure to Flow floods including Collection Tuning, Self Maintaining Collection Tuning Rules and Self-Healing Capability.

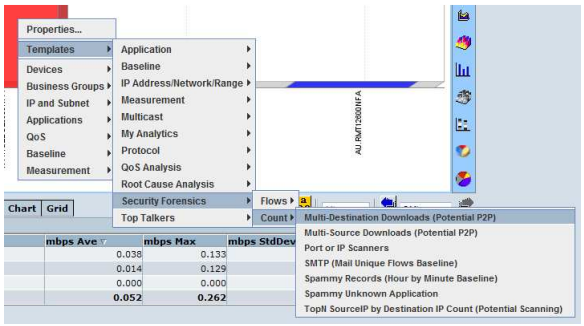
Various best practice collection strategies can be also adopted to increase the security of a NetFlow Auditor deployment in high load or very high security environments.

NetFlow Auditor allows collection of NetFlow to be separated from the database aggregation. This is useful in high security environments and ensures the database is not rendered inaccessible during an attack.



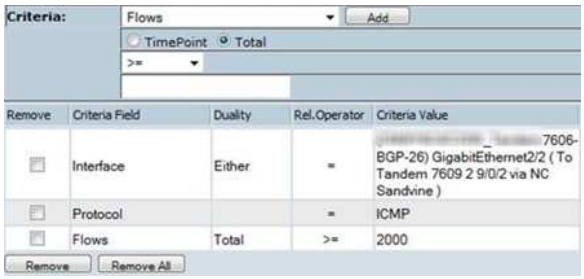
DDoS identification

A good example of setting up an alert based on "Count" Groupings can be seen below. The examples below are for DoS/DDoS attacks but the same principle applies for P2P. Count templates should be changed to sort by flows_sum or packets_sum and "Save New" to extend DDoS analysis. We are concerned with two major classes of flooding DDoS attacks. The first type, which we call TCP connection DDoS attack, is to overwhelm the victim's connection resources with fully-open TCP connections, thereby hampering legitimate users from making connections to the victim host. The second type, which we call the bandwidth DDoS attack, is to generate enough traffic to tie up the bandwidth of the victim's access link (either downstream or upstream). UDP, TCP SYN or ICMP packets can be used as the raw material in a bandwidth DDoS attack.



Extending current Templates

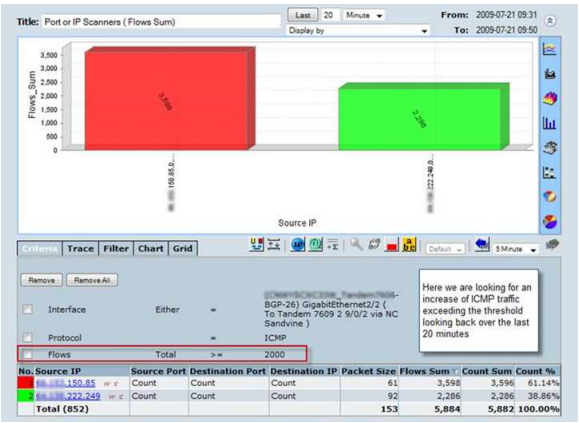
As an example to build a Template with Threshold criteria to watch for ICMP floods simply click on the Custom Filter and add the criteria that suits your need.



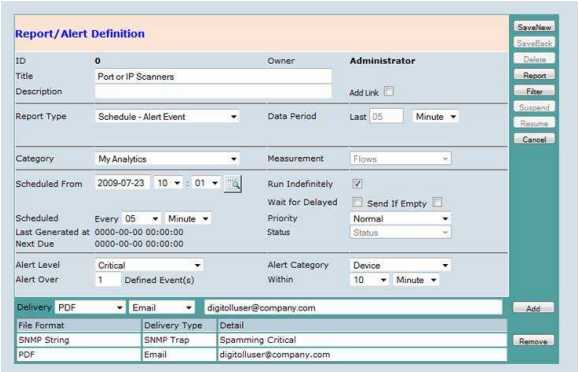
The same methodology can be used to find P2P users. In this case ignore protocol. If you want to set alerts then show top 1-5 and

set flow threshold for a normal period in your environment accordingly. Use Flow Sum, Packet Sum, Packet Size or Bytes Sum Descending to cater for various types of ICMP/P2P.

Here we are looking for an increase of ICMP traffic exceeding the threshold looking back over the last 20 minutes. The Threshold has been set to show data from IP Addresses that exceed 2000 flows over 20 minutes.



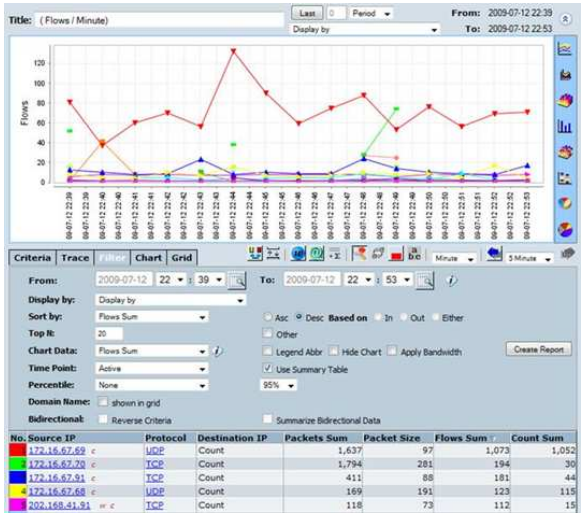
Lets Save this as an Alert / Report. Click on the Save icon at the top of the "Traffic Analysis" page.



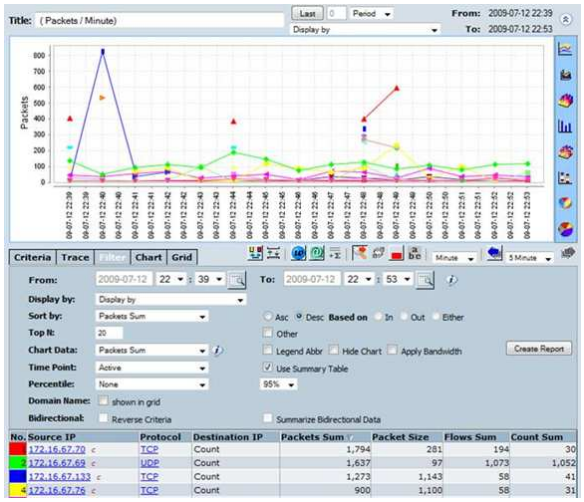
Other anomalies can be identified by burst analysis, rising threshold or standard deviation

As an example you can use NetFlow Auditor to provide the visibility to identify all computers who are communicating on IRC channels to IRC Servers. This will enable organizations and Internet service providers to block traffic to the IRC servers used by zombies in order to thwart attacks.

In the Graph below we are analyzing by the amount of Times a Conversation with a DestinationIP occurred from a SourceIP and Protocol. Physically constant connections can be easily seen. You can exclude IP Addresses as needed to reduce false positives.



Here we are analyzing the amount of Packets generated by a Top SourceIP and Protocol and counting the number of Destination conversations. In the graph below you can physically see the constant connections to a single source with a focus on Packets.

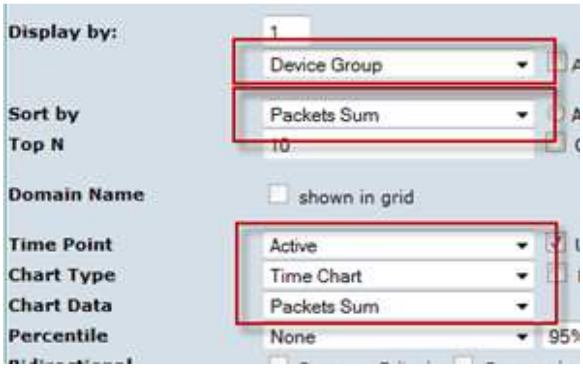


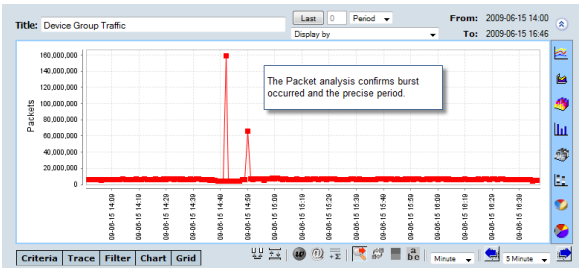
Case Study – Post Analysis of a DoS attack

We had an emergency/DoS attack today at 15:06:02 Eastern. It lasted until 15:14:25. What is the best way to look at the Netflow history to determine the source and destination of this attack? The bandwidth was relatively small but the packets per second were over 80,000.

Identify the time period. Choose Device Group, Device or Interface as the "Display By" this will enable the query engine to make use of summary tables. Use the Timepoint "Active" and TimeChart.

Order Chart and Data by the Analytic you need to understand, in this case Sum of Packets to identify a possible DoS attack.

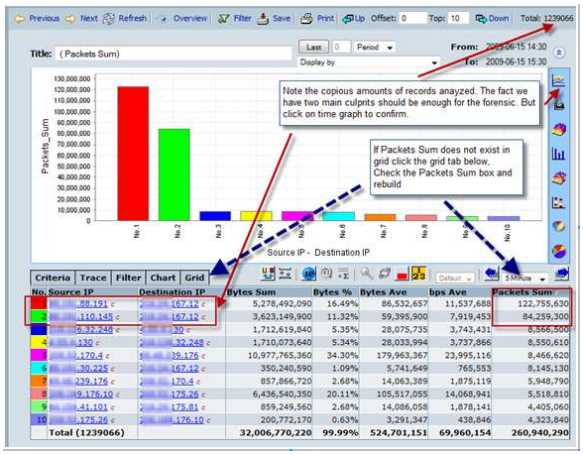




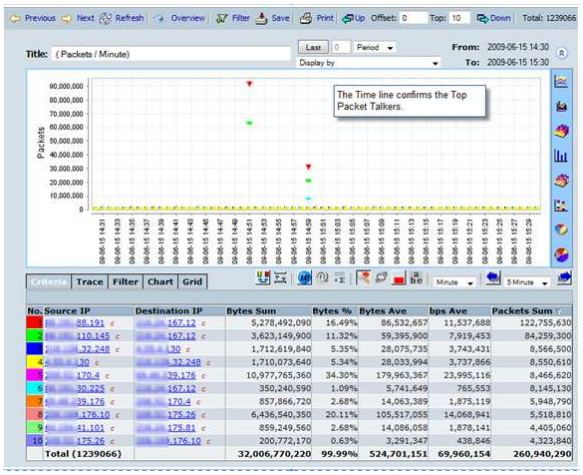
The Packet analysis confirms that bursts occurred at the precise periods.

Now analyze the conversations by the top packet generators for the period.

Hint: A Barchart with Time Point set to "None" provides the analysis much faster than building a time series analysis and therefore may enable faster reaction time.



Note the redline arrows show copious amounts of records in this query are 1249066 results. Two main culprits out of this huge dataset were found. Further analysis is performed using the time graph to see the burst frequency. Packets, flows, bytes or utilization sums can be placed on the grid just by ticking the desired measurement option and rebuilding.

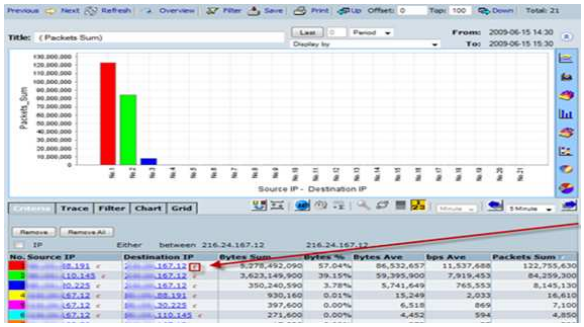


The Timeline confirms the Top Packet Talkers. Click "Other" if required to see all the remaining data in the timeline.

Let's take a quick look at the IP connections first for the IP Address in question X.X.167.12. We see it is DNS (UDP/53). Bytes Sum is also very high and is unusual for port 53 UDP. It does not appear to be P2P as otherwise the other side would reflect multiple IP connections. It currently feels more like a mass email campaign where the email server or mailer software on the X.X.88.191 side did most of its resolves

over the period. It could also be a worm/virus on the X.X.88.191 side seeing as it occurred from three IP addresses but does not appear to be X.X.167.12.

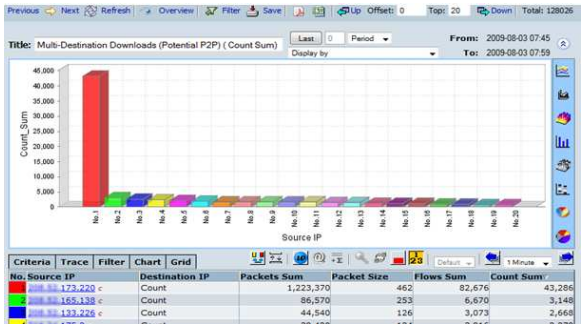
In this report we have isolated the range. By clicking the little “c” next to an IP Address shows the complete conversation flow for that data based on the current data collection tuning granularity.



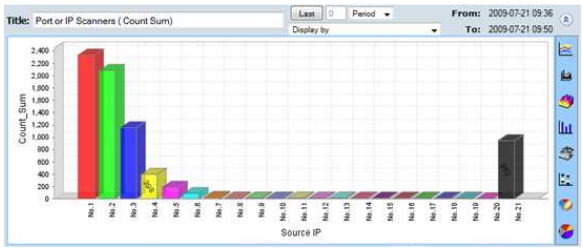
The conversation flows reflect suspicious IRC communications.

Use Count to group values to sum flows/packets/bytes/file records

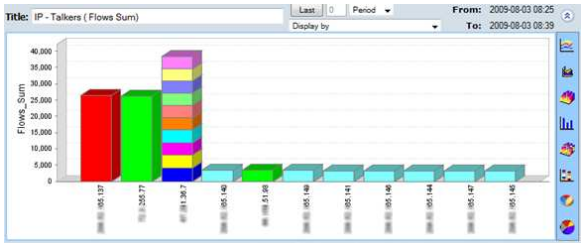
An IP is attempting to converse with multiple Destinations. This could be as a result of normal traffic from a web server. A baseline analysis will confirm the conversation profile. Thresholds can be set and exclusions can be made to fine tune.



The amount of ICMP from the top devices is excessive and worth investigating!

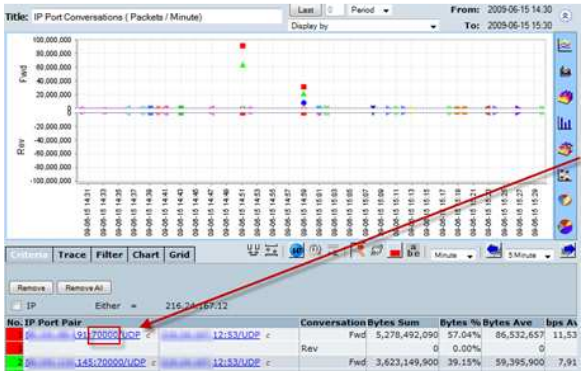


A visual example of an IP with multiple connections.

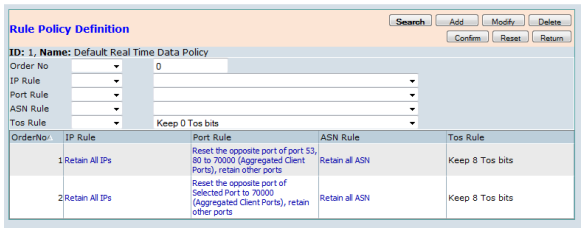


Data collection tuning

Data collection tuning rules can be used to reduce the amount of data stored while still providing high granularity and ability to track and trace. The Rules of the data collection policies will dictate the granularity of data collection depending on the number of flows. The Netflow Auditor Administrator can remove all rules or tune for an environments specific needs. In this case the client ports of the DNS queries are sent to this server are grouped to Port 70000. The frequency of flows will indicate if multiple connections are occurring.



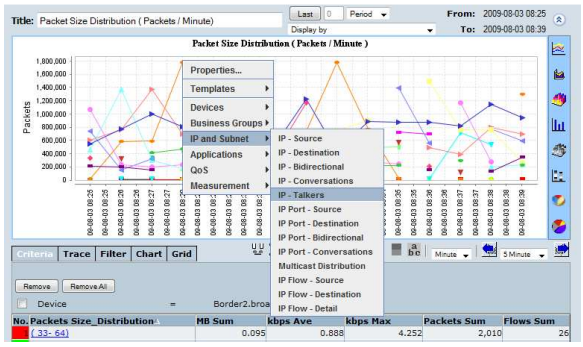
Collection Tuning Rules are configured by default to limit storage requirements in very large environments. All rules can be removed for full flow collection and should be used subject to sampling being enabled.

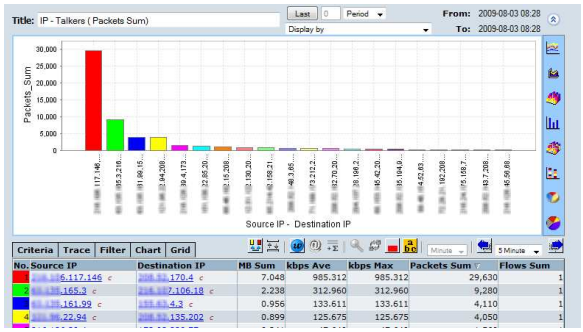


Network Auditing Examples

Drilldown Analysis

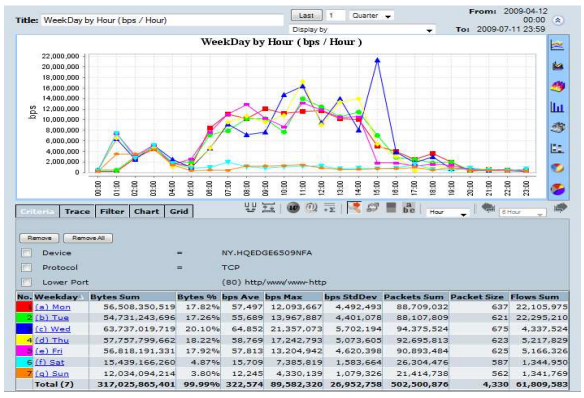
Once an area of concern is identified drilldown into it for as much detail as required.



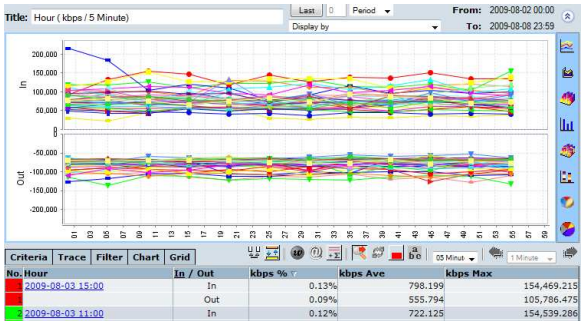


Baseline Analysis

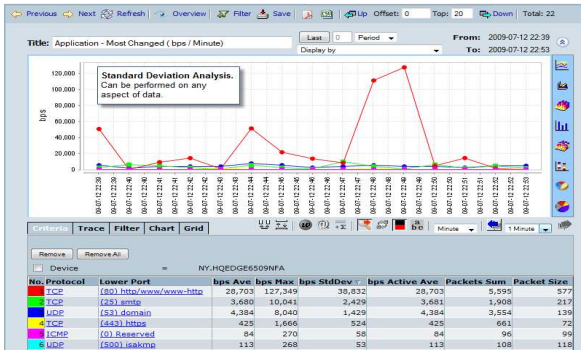
Baselines can be performed over long term or real time for any element. Knowledge of baselines provides the intelligence to create alerts.



In the graph below a single Interface has been analyzed for the last week by minute. Intelligent Baseline Alerting can then be set to automatically identify and alert on change. The longer NetFlow Auditor has been deployed the smarter it becomes.

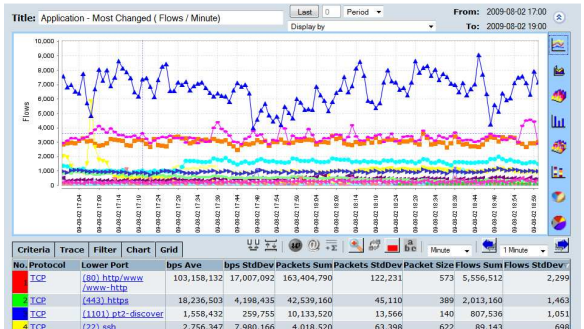


Standard Deviation Analysis

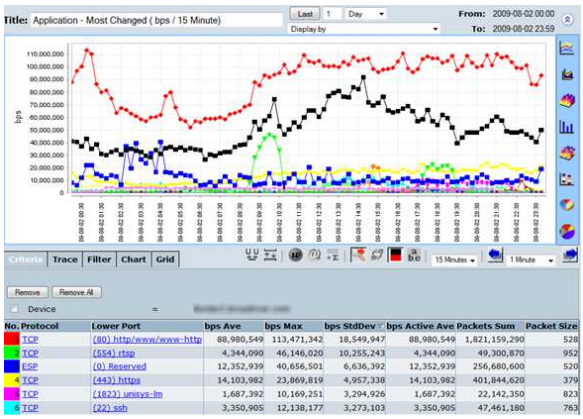


Standard Deviation Analysis can be performed on any aspect of data

Looking for change in an environment is often like looking for a needle in a haystack. NetFlow Auditor can calculate a standard deviation on bps, packets, flows or bytes. This provides the ability to see new sudden or slow changes that would otherwise remain hidden.



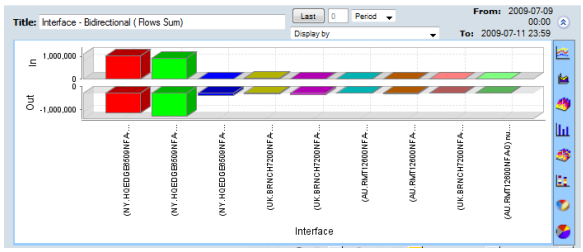
Note the sudden change in rtsp traffic and the increasing 443 traffic.



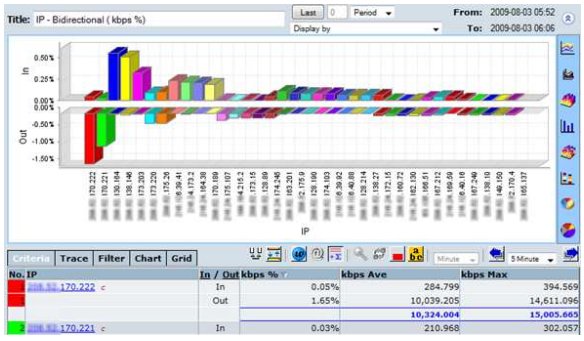
Bidirectional Analysis

Any aspect of data such as Interfaces, IP Addresses, Baselines, Ports, QoS values, or Accounts can display a Bidirectional view. Various graph types assist understanding:

Example 1. Interfaces

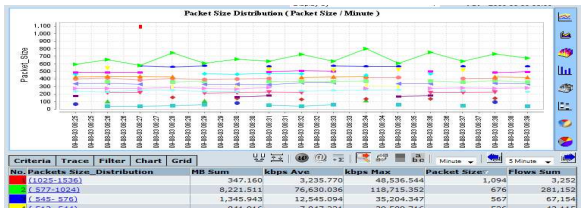


Example 2. IP Addresses.

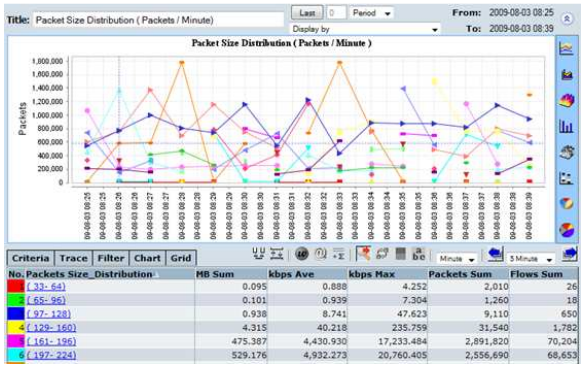


Packet size distribution

Various Packet Size Distribution analyses can be performed. The graph below shows continuing conversations split by packet size. There appears to be one very large packet.

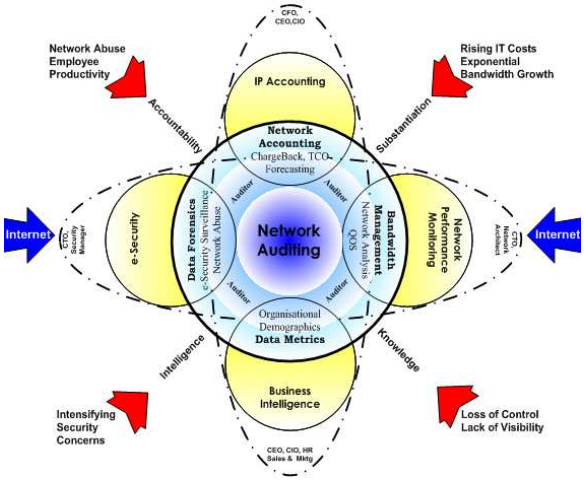


The graph below shows the data by the amount of packets for each packet size.



IdeaData

IdeaData has been focused on developing Network Traffic Forensics and Network Performance Management software for over 12 years. IdeaData has built a number or Network Auditing software products for Total Network Traffic Visibility including NetFlow Auditor, ProxyMate and DigiToll.



NetFlow Auditor software provides an entire team in a box and is focused on delivering total traffic visibility for IP based networks. It provides a complete and flexible toolkit for flow based network analysis.

From the same core NetFlow Auditor product we provide:

- Real-time analysis, long-term trending and baselining.
- 20:20 vision for Network Security forensics, DDoS and Network Behavior Anomaly detection.
- Intelligent Baselining detection for Network Performance and Security.
- Trending of any network traffic for capacity planning to Data Center managers and Network Architects.
- Ability to convert bits to usage totals or to 95th percentiles to enable ISP's to Invoice and substantiate Billing or turn IT Cost centers into Profit centers.

(See Gallery for various views of NetFlow Auditor capabilities).

NetFlow Auditor is unique in the global market in being able to capture, retain and present more network data intelligence than any other software currently in the genre allowing near real-time monitoring and profiling of Network activity and the ability to record and automatically report and alert on point to point data transactions at various degrees of grouping and granularity. Our methodology is preferable for a number of reasons most importantly it is non-intrusive, reduces the need for multiple probes or other intrusive methods to detect traffic and is highly fault tolerant.

Our customers range from SME businesses to large enterprises, Government and ISP's and we service the data visibility needs of Network professionals of varying backgrounds and skills. License Options are available to cater for full forensic analysis, simple top traffic only Performance management requirements or highly scalable options for service providers such as ISP's Telco's, Government or Campuses who need a highly fault tolerant solution for environments that have millions of flows per minute and for those that need the ability to measure 95th percentile to 5 minute intervals for a month. Whatever your needs to supply permanent solutions, managed services or part time projects you can be sure we have a quality solution that can fit your requirements and budgets as either a Capex purchase, a Basic or Support Bundled Subscription, Managed Service or a Consultancy.

Our Peer-to-Peer Behavior Detection technology and methodologies for filtering P2P traffic and are designed around our existing Flows Analysis methodology with new areas being added to our Deep Packet Inspection technology. We are sensitive to the issues surrounding file sharing networks and have developed methodologies to provide profiling forensic solutions for P2P traffic content.

P2P traffic is today the largest consumer of bandwidth representing as much as 80% of all the traffic on the public internet and over 50% of P2P traffic is believed to be illegal content. We believe our Peer-to-Peer Behavior Detection methodology can provide tremendous benefit to globally monitoring, filtering and managing P2P activity copyright and illicit content and be a major benefit to society.

Some Unique Perspectives are:

- Ability to represent multiple variables on a single graphs (subnets, protocols, traffic to endpoint, etc)
- Ability to learn and baseline traffic profiles to produce trend information then use this to formulate alerts.
- Provide exception and/or threshold alerts on a wider range of events such as rising/dropping traffic to particular end

point, rising/dropping protocol to end point, idle period to end point, etc.

- Time of day event alerting and thresholds
- Ability to email and store PDF, CSV. HTML and flexible SNMP trapping alerts.
- Ability to perform a packet capture on a time interval as well as number of packets.
- Ability to apply filters when performing a packet capture.
- Correlation and analysis of feeds from multiple appliances.
- Application protocol real-time alerting based on specific pre-defined groups or targets.
- Ability to set global real-time alerting thresholds based on changes in volume, destination, source or port.
- Ability to create 95th Percentile (Or any percentile) for any measurement such as bps, packets, packet size distribution or flows for use in Billing or Security analysis.

There are a number of key features where NetFlow Auditor stands above other solutions such as Scalability, Flexibility, Granularity, Comparative Baselining, Reporting and Alerting.

- Don't underestimate scaling needs when capturing flow data. Scalability is an important aspect to appreciate when comparing tools. Even our most basic NetFlow Auditor license can handle hundreds of thousands of flows per second and therefore you won't miss key data that others lose when pipes burst or when flows increase beyond their unpublished physical capabilities.
- An inflexible tool limits your ability to create relevant outputs for engineers, management and customers and can increase your workload rather than decrease it. That's why NetFlow Auditor effortlessly allows you to customize every aspect of the system from tuning data capture to producing templates and automated reports exactly as you need them.
- When analyzing network traffic details it is critical to have the ability to see the data in all perspectives and create dynamic Reports and Alerts. Network traffic is very dynamic and new traffic behavior can be tricky to track. Be careful that the product you buy doesn't just talk the visibility message and provides a tool set that won't leave you handicapped. NetFlow Auditor provides complete drilldown tools to fully explore the data.

NetFlow Auditor is unique in overall architecture:

- Baselining - Comparative analysis of each element across the time line. Gives the ability to identify which element caused the change and when.
- Powerful and Flexible Analysis: Packet Size, Full Flow, Count, Deviation, Bi-directional, Cross-sectional and Business group analysis.
- Unattended (proactive) Analysis, Alerting and Reporting or create drilldown templates for quick analysis of your specific needs.
- Data Collection Tuning - Collect only the data required.
- Scalability, Fault Tolerance, and "Self Healing" - Scales to collect at rates above to 1 Million flows/minute when using NetFlow Auditor Enterprise.

IdeaData Network Intelligent Agent Auditing Technologies. Saving you time and money. Flow-Based Network Monitoring you can depend on.