ManageEngine

networks unlimited
ManageEngine UK Distributor

Summary

Today, Enterprises know that the WAN is one of their most important assets. It needs to be up and running 24x7 for the enterprise to function smoothly.

To make this possible, IT administrators need to have a clear understanding of where WAN traffic is headed across the network and who's responsible for it.

Traditional traffic analysis uses hardware probes or packet analyzers to offer granular and detailed information on network traffic. However, hardware probes require complex deployment procedures, and typically do not account for IPsec traffic. Packet analyzers produce copious results that do not offer direct insight into application-specific traffic.

As a result, IT managers are faced with an increased troubleshooting cycle, and an extended time to make critical decisions affecting the network.

Today with Cisco's Netflow innovation, traffic analysis takes far less time and effort and yields much bigger benefits to the enterprise. Netflow makes it possible to collect granular details on IP traffic continuously, without affecting device performance or increasing costs.

Using exported NetFlow data, ManageEngine NetFlow Analyzer from Networks Unlimited, gives IT managers the visibility they need in order to understand the WAN. Armed with powerful instant reports on top talkers, conversations, and more, NetFlow Analyzer tells IT exactly what they need to know in order to troubleshoot, or forecast capacity on the WAN.

ManageEngine White Paper:

Traffic Analysis With Netflow. The Key to Network Visibility

The Need For Network Visibility

The distributed nature of today's enterprise presents network administrators with a series of operational and infrastructure challenges. IT teams are constantly required to troubleshoot network problems on the WAN quickly, and restore performance levels whenever low, but they typically lack the visibility needed to find the root cause of the problem.

To overcome these challenges, IT needs complete visibility of the traffic traversing the WAN – detailed insight that allows them to monitor and record activity to understand how the network, applications, and users, are interacting. Complete network visibility is possible only when an effective traffic analysis solution is in place.

> According to a recent study by independent research firm Nemertes Research, the average 1000-person company spends more than $216,000 per year troubleshooting outages on fixed remote-access services – and that's just to identify the trouble.

Traffic Analysis: The Key To Network Visibility

Traffic analysis helps IT managers answer important questions about their network including:

- Are critical business applications getting a fair share of available bandwidth?
- How to identify rogue applications and viruses on the network?
- Why is this WAN link congested?
- Which applications and users are using bandwidth

Effective traffic analysis needs to be fast, simple, and efficient. It needs to be comprehensive and, at the same time, should not tax the device from which traffic data is collected. This is where the power of Cisco NetFlow comes in

Cisco Netflow: Powering Traffic Analysis

Cisco offers an innovative approach to traffic analysis by adding the Netflow feature set to its devices. Netflow gives a Cisco router the ability to collect IP network traffic data as it enters an interface. Since the router itself is used as a probe, Netflow data is gathered with no capital investment, and low deployment costs.

Netflow measures and analyzes network traffic whilst offering several advantages over hardware probes and other traditional traffic analysis tools.

- **Low capital investment: S**ince most enterprise networks are already instrumented with Cisco routers
- **Simple configuration:** To set up Netflow on a router interface
- **Completeness of data:** As Netflow measures and reports automatically on all application traffic (most probes need to be configured for each traffic type)
- **Low lifecycle maintenance:** Since Netflow capabilities are tied to the Cisco router hardware/software maintenance

Netflow does introduce a small increase in the CPU utilization of the configured routers, (the amount of increase on router CPU utilization varies by router platform and the number of flows traversing the router) but the level of detail offered, coupled with the low-cost and ease of deployment make it the best choice for in-depth traffic analysis.

Once collected, Netflow data needs to be analyzed and reported on, in order to enable quick and efficient traffic analysis. Netflow data analysis tools are abundant in the market, but NetFlow Analyzer offers several advantages for simple and affordable traffic analysis.

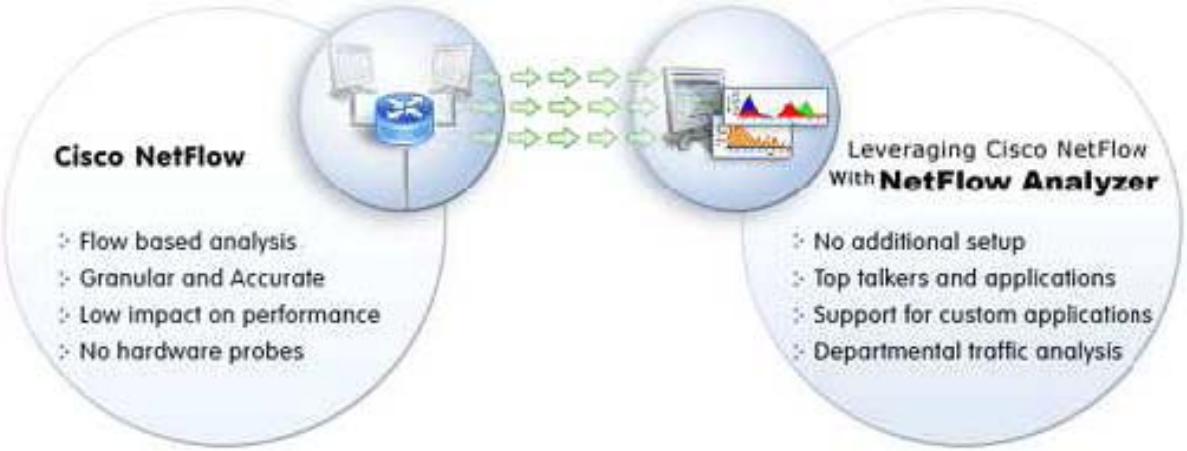
Netflow Analyzer: Effective Netflow Analysis

ManageEngine NetFlow Analyzer, is a web-based tool that analyzes Netflow exports from Cisco routers to provide in-depth information about network traffic including, traffic volume, top talkers, bandwidth consumption, and high usage times.

The information provided by NetFlow Analyzer helps IT in the following tasks:

1. **Identifying Top Talkers and Conversations:** Determine which users and what applications are using maximum bandwidth, and drill down for conversational details
2. **Projecting Traffic Trends and Usage Patterns:** View trends in network traffic, and determine top applications and peak usage times
3. **Defining Applications to Recognize Specific Traffic:** Use a combination of ports and protocols to define unlimited applications, and recognize this traffic exclusively in traffic reports
4. **Determining Bandwidth Usage per Department:** Define departments based on IP addresses, and identify bandwidth usage and application usage for each department.
5. **Managing Netflow Devices Exclusively:** Categorize devices exporting Netflow data into logical groups, and view traffic reports exclusively
6. **Increasing Accounting Accuracy:** Improve resource utilization accounting with real-time bandwidth and network usage statistics

Working Together: Cisco Netflow with Netflow Analyzer



NetFlow Analyzer and Cisco Netflow work together to enable complete network visibility through efficient traffic analysis

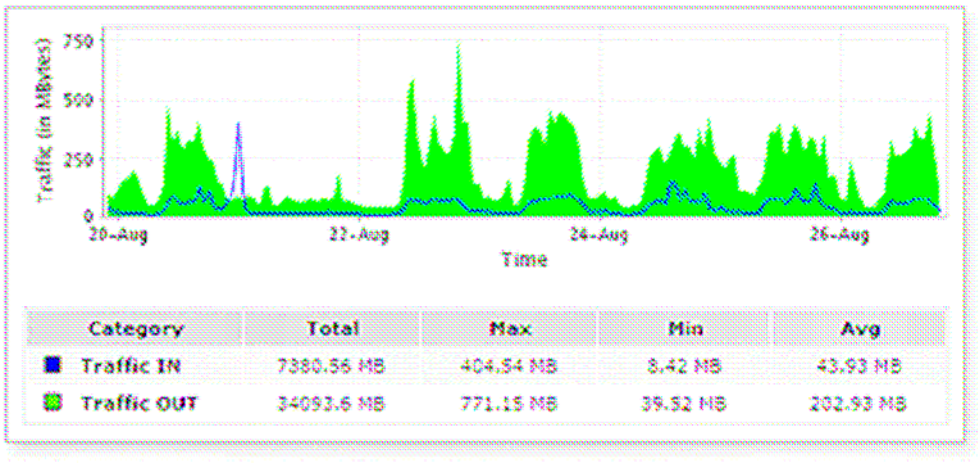
Netflow Analyzer at Work: Increasing Visibility with Effective Traffic Analysis

The analysis capabilities in NetFlow Analyzer enable IT to improve overall WAN performance. Scenarios can best illustrate how NetFlow Analyzer isolates performance problems, and aids in troubleshooting.

Scenario 1: Ending The Blame Game

Setting: A large national corporation with a central campus supporting multiple remote offices throughout the U.S. The helpdesk receives a call from one of the remote sites complaining that users cannot reach the email server. The caller's initial diagnosis is that "the WAN is down".

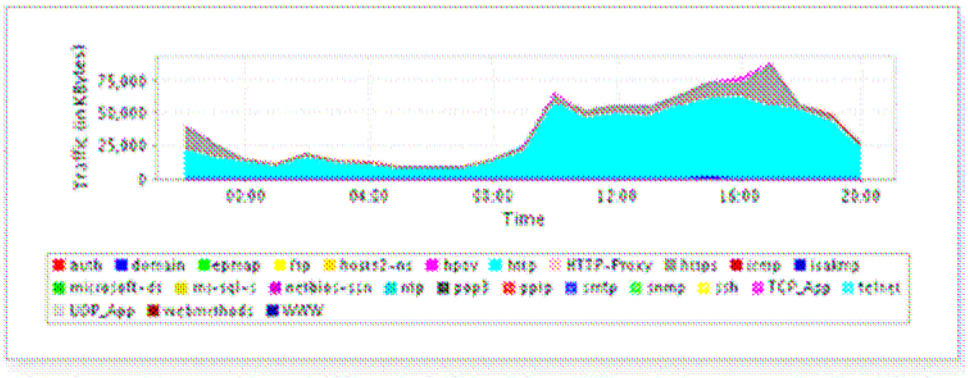
For IT, the first step is to determine whether the problem is indeed with the respective WAN link. A quick glance at the traffic reports tells the IT technician that traffic peaks are within acceptable limits, eliminating the WAN as the culprit. Next, IT must narrow down the search and determine if all applications at the remote site are affected, or just e-mail is failing.



Category	Total	Max	Min	Avg
Traffic IN	7380.56 MB	404.54 MB	8.42 MB	43.93 MB
Traffic OUT	34093.6 MB	771.15 MB	39.52 MB	202.93 MB

Traffic reports for the WAN link show that traffic peaks are within acceptable limits

By pulling out the Top Applications report, the technician gets an at-a-glance view of current traffic levels for the top hundred applications running to the remote site. Surprisingly, e-mail traffic is not counted as a significant contribution. He suspects the problem could be with the mail server.



The Top Applications report shows current traffic levels for top applications running to the remote site

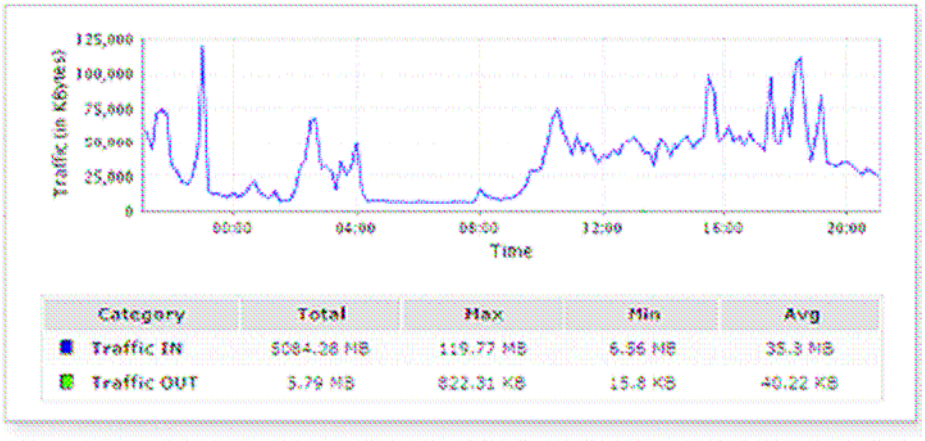
Now the technician approaches the e-mail team, which performs its own investigation, and discovers that the e-mail process on the server supporting the remote site in question has failed. The problem is quickly resolved, and e-mail service at the site is promptly restored.

> Using NetFlow Analyzer, IT was able to quickly end the finger pointing by eliminating the WAN as a suspect and narrowing the search to the e-mail server. By providing the e-mail team with detailed performance information, IT helped them identify and fix the problem.

Scenario 2: Troubleshooting

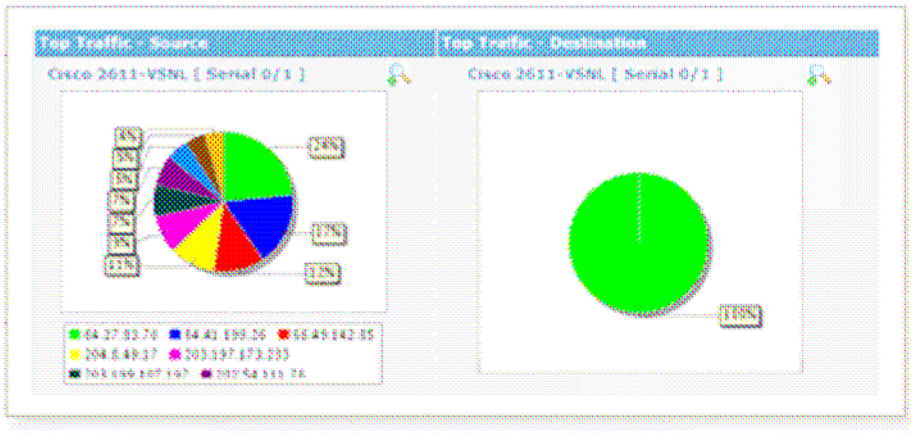
Setting: A distributed international organization with many remote sites around the globe. Users across the Asia-Pacific link can't gain access to key financial applications or server resources.

The IT operator receiving the call needs to first know what is on the network now. She opens the real-time traffic report on the corresponding network interface and notices a curious spike in traffic rate occurring ten minutes ago. She wants to investigate further into this spike.



Curious spike in traffic report indicates suspicious activity

Opening the Top Applications report for that time interval, the operator finds an unusually high percentage of ms-sql traffic, indicating that the SQL Slammer virus is active on the network. She now wants a comprehensive list of all the hosts infected with the virus, and so drills down from the Top Applications report to see the Top Conversations report.



The Top Applications drill down report shows the top conversations that have used that application

This report shows the top conversations that have used the ms-sql protocol. In a matter of minutes, the operator has identified the problem and the hosts that have been affected. From this point, the operator alerts the security team that quarantines the infected hosts and proceeds to stop the virus from spreading.

> Thanks to NetFlow Analyzer, the operator was able to identify a virus and track down the infected hosts within minutes, saving valuable network downtime and security compromises.

WAN Traffic Analysis – Key To Network Optimisation

WAN traffic analysis plays an important role in today's enterprise, providing critical centralized visibility into how the WAN, applications, and remote users are operating. By allowing IT to observe WAN behavior as it relates to business operations, WAN traffic analysis solutions can help locate where a problem originated, isolate the cause and source of the problem, and provide historical performance information that allows IT to optimize current performance while effectively planning for future growth and expansion.

NetFlow Analyzer is an in-depth WAN traffic analysis solution that helps IT end the blame game, focus and streamline their troubleshooting efforts, and optimize WAN performance through effective capacity planning. Complementing the level of granularity and accuracy that Cisco Netflow provides, NetFlow Analyzer provides an affordable, yet powerful solution for tapping this information with least impact on the performance of devices and the network.

Using the Cisco Netflow and NetFlow Analyzer combination, an enterprise can maximize their infrastructure investments, address the multitude of WAN challenges, and reduce complexity by eliminating the need for multiple point products.

Other Information

NetFlow Analyzer is available for purchase immediately, with prices starting at £520 for a 10-interface pack. A Free Edition is available that can report on NetFlow data exported from a maximum of two routing interfaces. A free 30-day evaluation can be downloaded from the website.

For more details on ManageEngine Netflow Analyzer visit http://www.manageengine.co.uk
To understand how it can help you manage your network, systems, and applications seamlessly, please contact Networks Unlimited on +44 (0)1798 873001 or at sales@manageengine.co.uk