WHITE PAPER

Published on **May 7, 2015**

By **Milos Zekovic**, Chief Customer Officer at Soneco

7 Reasons for Using NetFlow

NetVizura

Table of Content

Executive Summary

Globalisation, virtualisation, widespread use of personal devices and similar trends have substantially increased network traffic and network complexity. They have also brought about new security issues making it more difficult than ever to manage the network, ensure quality of service and enable smooth running of business applications.

In these circumstances traditional approaches to network monitoring prove to be extremely costly as they involve massive purchase of additional network equipment. Furthermore, management of all these new devices proves to be a real headache. Some enterprises have resorted to simply over-sizing bandwidth which merely hides the real issue. New services and more personal devices in the network cause leniency as personal and non-critical applications compete with the business ones. At the same time, the security of connections is bypassed thus giving rise to security risks. Getting more bandwidth is no solution to these problems.

A cost-effective answer to them lies in NetFlow. It is a technology that allows a network-wide analysis of traffic at a fraction of the cost. NetFlow helps network engineers solve problems efficiently by utilising the existing infrastructure in the network. It provides a quick and comprehensive insight into the reasons behind network problems. This in turn leads to optimal use of network resources, reliable business applications and services, faster troubleshooting and heightened security.

1. Whole Network Traffic Visibility

You cannot solve a problem if you do not understand it, nor can you manage something if you cannot measure it. Network traffic not monitored is a black box – you don't know what happens inside and to solve a network problem under such a veil is no more than an educated guesswork – at best.

Traditional methods like sniffer or physical probes installed on each network segment can be rather expensive, not to mention the on-going costs of managing all the probes. NetFlow, however, leverages the company's existing infrastructure – routers and L3 switches. NetFlow capable devices are probes per se so there is no need for an additional expensive hardware.

NetFlow is enabled on selected devices and the traffic data logs are sent to a central location - NetFlow analyser - where they are collected and aggregated into a human-readable format. This allows network engineers to quickly and easily visualise, identify and analyse hosts, service, conversation and protocols for the whole network or its segments.

Some NetFlow solutions offer interface grouping in order to enable network and segment visibility. In addition to device and interface-based segmentation, NetVizura NetFlow Analyzer separates traffic into segments based on the IP subnets. With NetFlow enabled on just a few core routers you get whole network and network segment traffic visibility.

2. Cost-effective Remote Office Monitoring

As local and international presence is needed for the business, many enterprises have set up remote offices. In order to connect them, enterprises often employ the MPLS technology to create the VPN links. Instead of purchasing point-to-point links for each location, the MPLS technology facilitates secured communication through a provider's network, thus ensuring Quality of Service and reducing network complexity. Unfortunately, even these benefits come at a cost. Traditional monitoring and security solutions are not entirely free of difficulties.

Remote offices are normally connected through a central location where an Intrusion Detection System (IDS) ensures the security of all traffic passing through the enterprise network. However, MPLS links allow for traffic to be established between remote offices by bypassing the central location. This means that the IDS and network monitoring solution are bypassed, as well.

NetFlow offers a cost-effective solution to remote office monitoring and security issues. Instead of purchasing and installing a sensor or a probe at each remote office location – which is expensive and difficult to maintain – NetFlow can be enabled on existing routers in the remote offices.

3. Prioritise Mission-critical Applications

Enterprises rely on mission-critical applications to enhance the effectiveness of business and sell value to their customers. Such applications help employees be more efficient and effective when executing daily tasks. They also allow for various services to be offered to customers.

With recent trends, such as the increase in media traffic (VoIP, conferencing, video streaming etc.), Bring Your Own Device (BYOD) and a larger number of tools employees use, business applications compete with each other for bandwidth. Or worse yet they compete with non-critical applications used on workstations and personal devices. This can, and often does, exert a serious impact on performance of the enterprise and result in financial losses.

The solution lies in prioritising mission-critical applications by implementing QoS and ToS policies. These will ensure that important applications (like VoIP) get the necessary bandwidth while non-important applications will get it only if available.

NetFlow shows statistics for each QoS and service used on interface in the network, allowing network engineers to quickly analyse and determine how QoS policies should be implemented – and then to ensure they are implemented properly.

4. BYOD Impact Monitoring & Management

Bring Your Own Device (BYOD) creates new complexity and issues in the network. Despite clear benefits of using a smart-phone for telecommuting, business related messaging, emails, mobility etc., BYOD has certain downsides. Not only does it cause additional traffic, but often bypasses network security thus exposing the network to non-critical and untrusted applications. It is therefore vital to monitor the impact of BYOD in your network.

Network engineers can use NetFlow for understanding the BYOD bandwidth usage by monitoring the applications used and identifying who is talking to whom (source and destination of traffic). This allows to properly implement QoS policies and address any possible security issues.

5. Faster Troubleshooting

Providing mission-critical services to employees and customers is essential for enterprise's revenues. If services are unavailable or "slow", employees' efficiency suffers. More importantly, unavailable or "slow" customer services can harm the existing business and damage the enterprise's reputation. As network is complex and constantly evolving, network problems that cause service unavailability cannot be escaped. The question is – how to troubleshoot faster?

Proper troubleshooting requires time: time to gather information, analyse and solve a problem. The first step is to gather relevant information. Unfortunately, SNMP-based monitoring tools show spikes in total traffic and if a link or a service is down, but not the reasons why.

NetFlow, on the other hand, gives an insight into the causes of network problems related to bandwidth consumption. It can help in resolving certain security issues by providing a clear answer to what is happening in the network – the who, the what and the when.

It provides a quick insight into hosts (who is using the bandwidth) and their conversations (what are they doing) over time (when). NetFlow identifies the most frequently used services, protocols and QoS allowing for a better understanding of applications and services in the network. Historical data in the form of charts and flow records help the network team analyse incidents recorded in the past. To allow the network team to act preventively, traffic-based alarms can also be set to signal a critical amount of specific traffic on interfaces or for important services.

NetFlow solutions also complement other network monitoring tools. For instance, an SNMP tool can signal a high CPU or memory utilisation of a router, while NetFlow analyser can discover a large amount of packets sent to the router by a single host – indicating a Denial of Service attack. Similarly, interface traffic can be analysed to show what had been happening before the interface went down.

6. Heightened Security

One of the biggest threats to enterprise networks nowadays stem from network security. As complexity of the network and services increase, so do security risks. Telecommuting and Bring Your Own Device (BYOD) increase the security risk by providing a direct way for malware to penetrate the network. Attacks like Denial of Service (DoS) are increasingly sophisticated and consequently more difficult to detect. Unknown applications running on well-known ports prove to be a considerable risk, too.

Traditionally, IDS is used to filter out malicious traffic relying on Malware signatures. This leaves room for network penetration since these signatures need to be up-to-date (zero day attack). However, such an attack can be recognised as a traffic anomaly – but to do so you need to analyse traffic, which is when NetFlow comes to work.

Anomalies can be easily identified on charts and statistical patterns can be analysed in raw data (flow record logs). Anomalies are usually shown on the packets and flows charts as a large amount of very small packets sent by or to a single host. Host, protocol and service can be identified on the charts, whereas the whole flow records will provide more detailed information such as the type of an attack (address scan, port scan, Denial of Service etc.), all involved hosts, time stamps etc.

7. Accurate Capacity Planning

Every successful business seeks ways to cut costs by effectively utilising the existing infrastructure. Every expanding business knows that network capacity planning is crucial when preventing and mitigating major service issues and costs. The main difference between a heavy and slight loss caused by the unscaled network and unrecognised service trends is the accuracy of capacity planning.

NetFlow is a neat solution which helps you with accurate capacity planning. Historical data (charts) show total, service and host traffic over time and help with recognising traffic trends – therefore allowing better planning and traffic prediction. Interface charts allow network engineers to optimise the physical and virtual link capacity and adjust traffic if needed. Services, protocols and QoS charts help in optimising bandwidth utilisation thus boosting the efficiency of the existing infrastructure. NetFlow provides quick accessibility of all these statistics for the whole network and per network router and interface.

Some NetFlow analysers allow department and location traffic monitoring by offering the possibility of grouping interfaces and routers into logical entities that represent different departments or remote offices in the enterprise. NetVizura can segment the network based on IP addresses – making the segmentation of traffic by departments and remote offices quite easy.

About NetVizura NetFlow Analyzer

Product Highlights

NetFlow Analyzer helps network admins with deep network traffic investigation, analyses and reporting. By visualising the traffic by network devices, interfaces and subnets, network admins can better understand bandwidth consumption, traffic trends, applications, host traffic and traffic anomalies. This enables companies to optimise their networks and applications, plan network expansion, save time needed for troubleshooting and diagnostics and improve security – in turn considerably lowering company operational costs.

Why NetVizura?

More than bandwidth monitoring

NetVizura does not simply monitor bandwidth consumption – it is a powerful analytic tool that gives your network team more information: extensive flow records, flow and packets charts in addition to standard bits charts, etc. This boosts your capacity to troubleshoot faster and increases your network security.

There is no limit to the size of the flow record archive. The size is limited only by the size of your storage. Flow records are displayed as tables and can be filtered, searched, ordered and exported for advanced analyses. This allows you to inspect past incidents in greater detail, even if they are months old.

More visibility with less NetFlow routers

NetVizura allows you to enable NetFlow export on just a few routers and still get network-wide traffic statistics segmented into IP subnets that represent departments and remote offices.

Why NetVizura (cont.)?

Custom traffic monitoring

Traffic Patterns allow monitoring of specific traffic of interest: traffic between specified subnets with specific characteristics like service, protocol, exporter, interface etc. This allows you to monitor critical traffic separately from the total network traffic.

In addition to monitoring traffic per router and interface, network can be segmented based on IP subnets representing different organisational units in the network. This allows you to monitor traffic per departments, remote offices and collections of regional offices easily.

No NetFlow capable device? No problem!

Get full statistics without any NetFlow capable device by installing a free software for NetFlow capture and export. Traffic will be separated into different segments by IP subnets and monitored via Traffic Patterns.

Simple pricing

NetVizura NetFlow Analyzer license is based solely on the flow rate of your network. There are no limitations to the number of NetFlow routers, interfaces, hosts or users.

Trial download:
www.netvizura.com/download-netflow-analyzer.html

Live Demo:
www.live.netvizura.com/demo/

About Soneco

Soneco is a Serbia based company that specialises in software development and ICT consulting. Since 2006, we have been growing steadily and our solutions have left a significant mark on some of the core ICT transformations in the region, earning us a wider recognition as a reliable partner and software developer of consistent quality. We have been Cisco Solutions Partners since 2011 and Oracle Gold Partner since 2010.

Soneco continues to focus on client satisfaction and building strong relationships with partners. Our best reference is the number of successfully delivered projects implemented in various industry verticals and a strong reference list consisting of recognisable clients. Learn more today at www.netvizura.com

Soneco d.o.o.

Alekse Nenadovica 19/4
11000 Belgrade, Serbia

Tel: +381.11.2455944;
Fax: +381.11.2455210
sales@netvizura.com
www.netvizura.com

NetVizura

For additional information, please contact us at sales@netvizura.com or visit www.netvizura.com