7 REASONS FOR USING NETFLOW

NetVizura

WHY NETFLOW?

Globalization, virtualization, widespread use of personal devices (BYOD), DDoS attacks and similar trends have substantially increased network traffic and network complexity. They have also brought new security issues making it more difficult than ever to manage the network, ensure quality of service and enable smooth business running.

01 OPTIMIZE BANDWIDTH UTILIZATION

02 PLAN CAPACITY UPGRADES

03 MONITOR WHOLE TRAFFIC

04 MANAGE APPLICATION DISTRIBUTION

05 UNDERSTAND NETWORK USERS

06 REDUCE RESPONSE TIME

07 BE SECURITY AWARE

In these circumstances traditional approaches to network monitoring prove to be highly expensive, as they involve purchasing massive networking equipment. Furthermore, managing all these new devices can prove to be a big headache. Some enterprises have resorted to simply over-sizing bandwidth which merely masks the underlying concerns. New services and more personal devices in the network cause latency as personal and non-critical applications compete with business ones. At the same time, the security of connections is bypassed thus giving rise to security risks. To put it simple, more bandwidth is not a sustainable solution to these problems.

On the other side, NetFlow technology helps network engineers solve problems efficiently by utilizing existing infrastructure in the network. It provides a quick and comprehensive insight into the reasons behind existing network problems. This, in turn, leads to optimal use of network resources, more reliable business applications, better situational awareness and faster troubleshooting.

By providing a network-wide analysis of traffic at a fraction of the cost, NetFlow is recognized as a proven cost-effective solution for the issues network, system and security people face nowadays.

OPTIMIZE BANDWIDTH UTILIZATION

With recent trends, such as the increase in media traffic (VoIP, conferencing, video streaming etc.), larger number of tools employees use and even personal applications used on Bring Your Own Devices (BYOD), critical business applications compete with all of them for bandwidth consumption. This can, and often does, make a serious impact on employee performance, reduced service value delivered to customers and results in financial losses. This is why traffic shaping is done – implementing QoS and ToS policies in order to prioritize critical applications (like VoIP) to the expense of non-critical ones (like YouTube). NetFlow data can help network engineers visualize traffic for each QoS and service used on single interface in the network, allow quick analysis and suggest better QoS policy implementation – and then verify if they are implemented properly.

Interface traffic visualization allows network engineers to spot the needs and opportunities for traffic rerouting and thus optimize usage of the overwhelmed resources. Some NetFlow solutions offer the possibility of grouping interfaces and devices into logical entities that represent different functions, remote offices or departments in the enterprise, empowering more personalized network monitoring, analysis and management.

In case routing is based on threshold throughput or volume rates, it may happen that good traffic is discarded or that the bad traffic is not discarded (sent to Null interface). NetFlow charts could provide verification of traffic filtering and suggest how to fine-tune firewall thresholds, i.e. if they are actually too high or too low, in order to keep the wrong traffic out and right traffic in.

PLAN CAPACITY UPGRADES

NetFlow is a neat solution that can help you to accurately plan you network scaling. Historical data (charts) show total, service and host traffic over time and help you recognize trends – therefore they also indicate better traffic prediction. If NetFlow predicts that the bandwidth limit will soon be reached, this will make a clear argument for a bandwidth increase.

Every successful business seeks ways to cut costs by effectively utilizing existing infrastructure. However, expanding businesses know that new device purchase may eventually be crucial for prevention and mitigation of major service drops and related financial losses.

In case simple bandwidth increase or even new device purchase is not sufficient to solve more complex networking demands, NetFlow may suggest the need and help in preparation of the overall network architecture redesign.

MONITOR WHOLE TRAFFIC

You cannot solve a problem if you do not understand the whole picture. With NetFlow exported from a few core or distribution devices and deduplication enabled, you can get a view your network's total traffic – including internal (between hosts from your network), external (with hosts outside your network) and even transit traffic of ISPs (between hosts outside your network).

As one of the biggest advantages of NetFlow, you are able to customly define traffic segments you would like to specially monitor, based on the fields provided by NetFlow dataset. For example, you are able to separate Internet HTTP/HTTPS traffic by services (ports) used or separate atypical GRE traffic by protocol used.

As local and international presence is needed for the business, many enterprises have set up remote offices (regional centers or locations). 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. NetFlow offers a cost-effective solution to remote office monitoring. 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. By showing traffic based on the network's IP address ranges (subnets), NetFlow makes traffic by regional centers, locations or even departments quite easy.

Bring Your Own Devices (BYOD) trend also creates new complexity and issues in the network. Despite clear benefits of using a smart-phone for telecommuting, business related messaging, emails, mobility etc., it also causes additional traffic generated by non-critical 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 analyzing the applications used.

MANAGE APPLICATION DISTRIBUTION

SNMP reports are good for showing total traffic, but they do not show who and how much is using the traffic. On the other hand, NetFlow can show if your critical application is getting the bandwidth it needs and providing required availability. You can even setup an alarm based on the bandwidth utilization of a single application traffic instead of total link usage. This will ensure that you will be notified before application is out of bandwidth and that congestions are prevented. This leads to a more reliable application and SLA fulfilled.

Network engineers can also use NetFlow for monitoring the application used and identifying who is talking to it (source and destination of traffic), thus allowing proper application QoS policy implementation.

Reviewing application communication by hosts or users can clearly point out if there is any unwanted communication, indicating unrestricted access and thus supporting restriction policy implementation or addressing any possible security issues.

UNDERSTAND NETWORK USERS

Mapping IP addresses to usernames is a time consuming activity prone to errors. Statically allocated IP addresses need to be manually maintained while dynamically allocated IP addresses require DHCP logs analysis, too. It is also possible that one user uses several IP addresses or one workstation is used by several users in specific time interval. NetFlow enhances the efficiency of this process by automatically correlating IP addresses usage in specific time interval with specific user name.

Employees have different needs regarding network utilization. Some will predominately use email and have very light impact on network resources. Others will need high throughput and quality in order to fulfill business requirements like hosting a web conference or remotely connecting to client networks. High consumption of network resources and even usage of personal devices (BYOD) can be legitimate, but it could also be a sign of using company resources for non-business purposes. With this information engineers can easily project QoS policies and optimize resources per user.

Employees' unwanted content visits indirectly expose network to a risk of malware and device hijack. NetFlow can provide Insight into end user traffic can show with which IP address did the user communicate (Facebook, YouTube etc.), which services did the user use (slack, torrent etc.) and similar, and in this way support company's network content policy implementation.

BE SECURITY AWARE

Perhaps the biggest challenges to enterprise networks nowadays are in the area of network security. As complexity of the network and services increase, so do security risks. Attacks like Distributed Denial of Service (DDoS) and Data Leakage, are increasingly sophisticated, may come both from outside and inside of the network and are consequently more difficult to detect. Traditionally, Intrusion Detection System (IDS) is used to filter out malicious traffic relying on Malware signatures. This leaves room for network penetration since signatures may not be up-to-date (zero day attacks). Such an attack can be recognized as a traffic anomaly – but to do so you need to analyze traffic and indicate it, which is where NetFlow comes to work. 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, all involved hosts, time stamps etc.

Besides reacting to attacks, NetFlow can be used more proactively for network preparation for potential attacks. For example, port scanning probes network defenses by discovering running services and revealing how to penetrate weak points. NetFlow can easily spot atypical port usage (e.g. SSH) and then show if multiple IPs received atypical protocols (e.g. TCP flag S), confirming scan.

For the reasons mentioned above, NetFlow is also a practical solution to remote offices security. As they are usually 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 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.

Personal, Bring Your Own Devices (BYOD) also bypasses network security thus exposing the network to untrusted access. NetFlow is used for identifying who is talking to whom (source and destination of traffic) and thus addressing any possible security issues.

REDUCE RESPONSE TIME

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 response requires time: to gather right information (alert), make forensics do discover a root cause (analyze), assess options to choose a course of action (decide) and solve a problem (troubleshoot). The first and crucial step is to gather relevant information to get a solid foothold for consecutive steps.

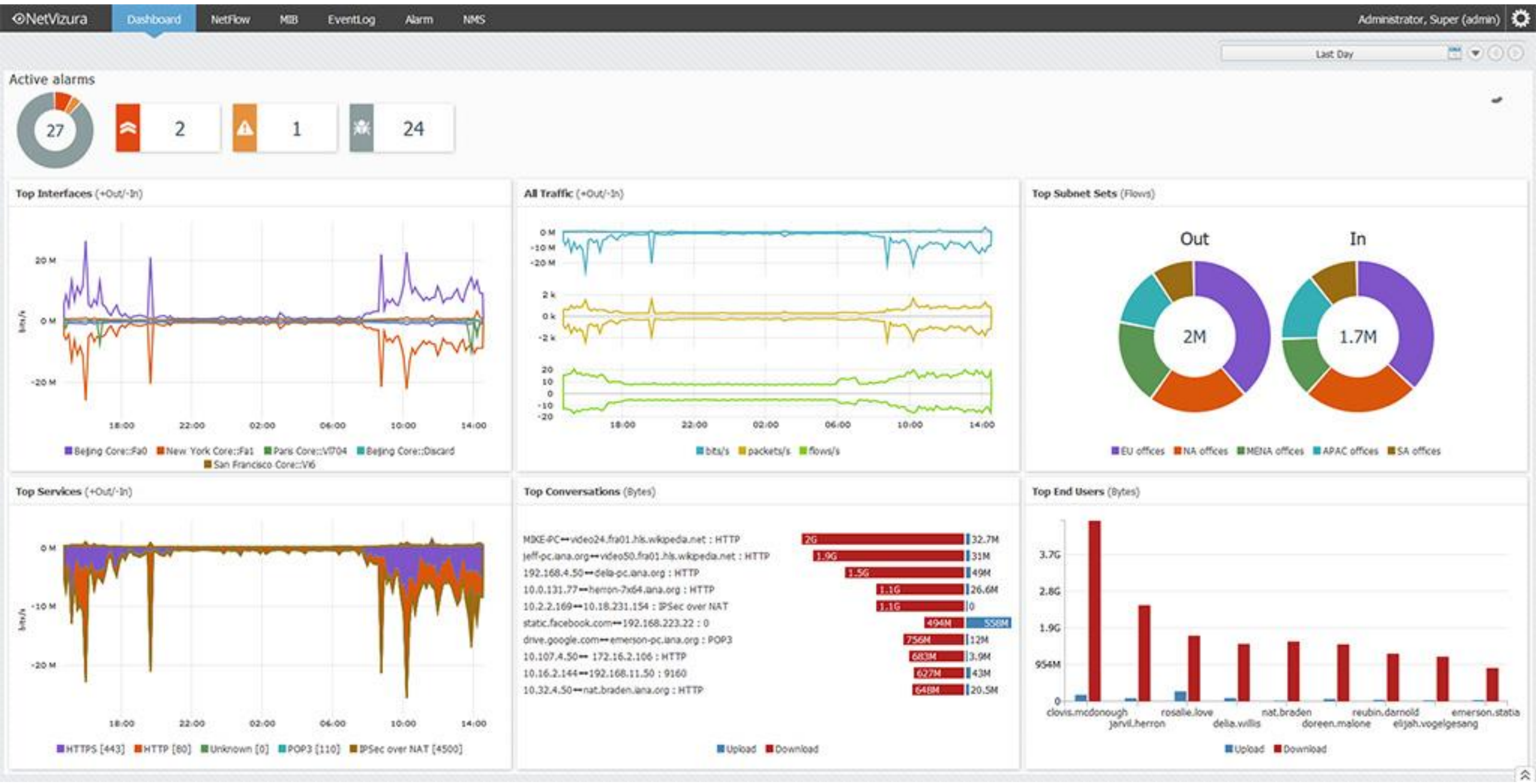
SNMP-based monitoring tools show spikes in total traffic and if a link or a service is down - the where and the when. NetFlow, on the other hand, gives an insight into the causes of network problems by providing a visibility to what is happening in the network – hosts (who is using the bandwidth) and their conversations (what are they doing) and over which routes ports and protocols (how). This allows better understanding of applications and services in the network. Historical data in the form of charts and flow records helps network team in analyzing incidents recorded in the past.

To allow the network team to act preventively, traffic-based alarms can also be set to signalize a critical amount of specific traffic on interfaces, important services or by single end users.

NetFlow solutions also complement other monitoring tools in order to gain a greater contextual awareness of the event. For instance, an SNMP tool can signal a high CPU or memory utilization of a router, while NetFlow can discover a large amount of packets passing through vital link by a multiple hosts – indicating a DDoS attack. In addition to this smokescreen operation, EventLog can show that there is an unauthorized access on a vital server happening at the same time.

NetVizura NetFlow Analyzer

NetFlow Analyzer helps network, system and security admins with network traffic investigation, analysis and reporting. By visualizing the traffic by network devices, interfaces and subnets, they gather right information-alert can better understand bandwidth consumption, traffic trends, applications, host traffic and traffic anomalies. This enables companies to optimize their networks and applications, plan network expansion, save time needed for troubleshooting and diagnostics and improve security – in turn considerably lowering company operational costs. Learn more at www.netvizura.com



[NetFlow Analyzer DATASHEET]()

[NetFlow Analyzer FEATURES]()

ABOUT SONECO

Soneco is a company based in Serbia that specializes 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 recognizable clients. Learn more today at www.soneco.rs.

SONECO DOO

Makenzijeva 24/VI
Belgrade, Serbia
Tel: +38111 635 6319;
For additional information, please contact us at sales@netvizura.com or visit www.netvizura.com