NetFlow Analyzer

highlighted feature:
end user traffic statistics

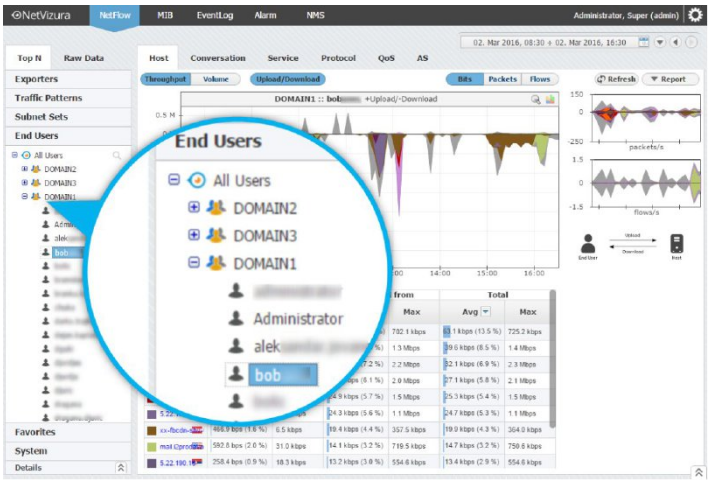
NetVizura NetFlow Analyser enables you to collect, store and analyse network traffic data by utilising Cisco® NetFlow, IPFIX, NSEL, sFlow and compatible netflow-like protocols. It allows you to visualise traffic per network devices, interfaces and subnets, and to better understand bandwidth consumption, traffic trends, applications, host traffic and traffic anomalies. This in turn allows businesses to optimise their network and applications usage, plan network expansion, save time required for troubleshooting and diagnostics and improve security.

Key Features

- Detailed statistics for:
  - router and interface bandwidth
  - custom traffic on IP subnets
  - end user traffic.
- Highlighted biggest traffic contributors (*top talkers*) per hosts, services, protocols, conversations, QoS and AS.
- Archive of all flow records in the network, searchable historical data and report generation.
- Threshold based alarming.
- Supported protocols: Cisco® NetFlow v5 and v9, IPFIX (standard), NSEL, sFlow v5 and netflow compatible protocols of other network device vendors.

Highlighted Functionality:

End user traffic statistics



Traditionally, traffic analysis is focused on IP addresses, but in certain situations it is necessary to correlate traffic to a specific user. For example, while investigating security breaches and atypical network behavior, engineers need to check the activity of specific users in order to determine is it an internal security flaw or external attack.

Mapping IP addresses to usernames is a time consuming activity prone to errors. Statically allocated IP addresses need to be manually maintained while dinamically allocated IP addresses requires for DHCP logs analysis, too.

NetVizura enhances the efficiency of this process by automatically correlating IP address usage during specific time with specific user name. This is done by mapping login events sent over syslog messages from domain controllers or worstations to NetVizura server. With this, traffic statistic of each user (username) is available regardless of how IP address is allocated. It is also known if a user used several IP addresses or one workstation is used by several users during different times.

As with traffic statistic on exporters, interfaces and IP subnets, NetVizura allows visualization of traffic structure by host, services, conversations, protocols, QoS and AS for each end user at any given time.

Use Cases

Identifying user's needs and illegitimate network usage

Employees have different needs in regard to 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 can be legitimate, but it could also be a sigh of using company resources for non-business purposes. Insight into end user traffic allows fast identification of top consumers in the whole network or network domain. After identification of such users, one can analyze what is the cause of high traffic – with which IP address did the user communicate (does it belong to Facebook, YouTube etc.), which services did the user use (jabber, torrent etc.) and similar. With this information engineers can easily project QoS policies and optimize network resources.

Investigating security risks

Atypical network traffic (peak in traffic, atypical protocols, activity outside work time etc.) can indicate security risks and breaches such as misuse of credentials, compromised work station (zero-day attack), unauthorized access or data leakage. Insight into end user (username based) traffic, engineers can accelerate checkup processes and problem diagnostics therefor mitigate security risks faster.

About NetVizura

NetVizura brings easy-to-use, flexible and affordable network monitoring solutions. Our goal is to help network teams be more efficient thus making your business more effective. For more info, visit us at www.netvizura.com/about-netvizura.

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

About Soneco

Soneco is 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. Cisco Solutions Partner since 2011. Oracle Gold Partner since 2010. ISO 9001 i ISO/IEC 27001.

Soneco d.o.o.
Makenzijeva 24/VI, 11000 Beograd
Tel: +381116356319
Email: info@soneco.rs

Copyright © 2016 Soneco.All Rights reserved. NetVizura and NetVizura logo are trademarks of Soneco d.o.o. company.
All other trademarks are poperty of their respective owners.