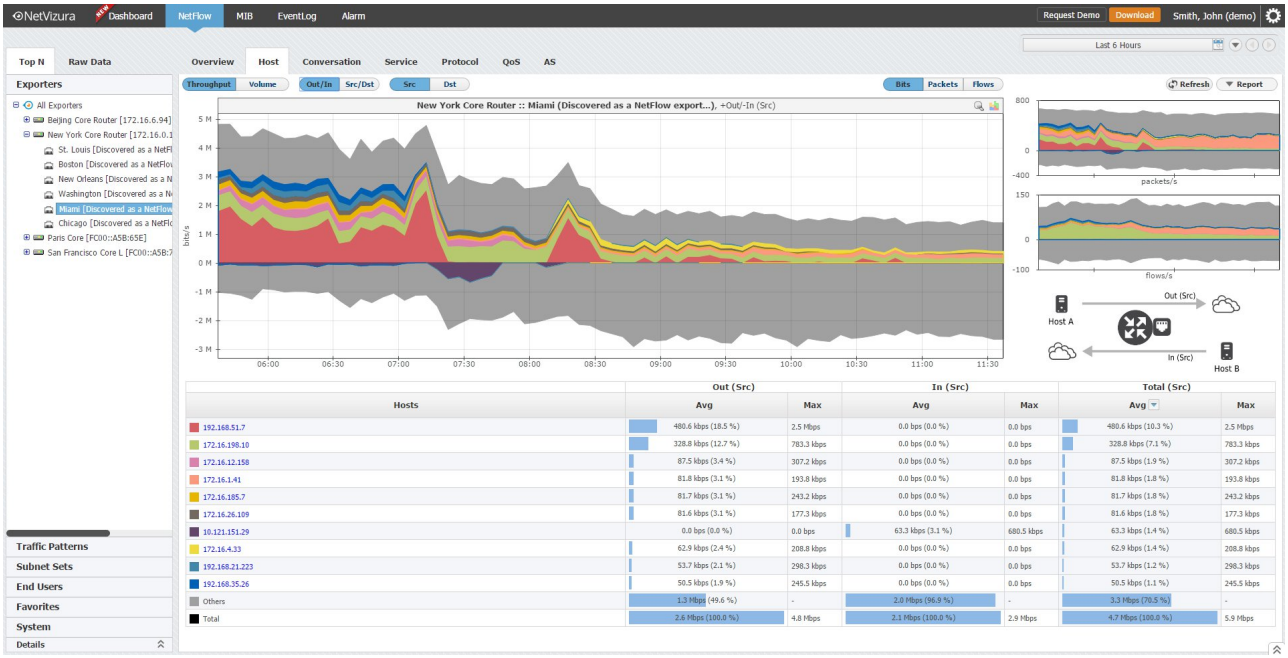
NetFlow Analyzer

DATASHEET



NetVizura NetFlow Analyzer enables you to collect, store and analyze network traffic data by utilizing Cisco® NetFlow, IPFIX, NSEL, sFlow and compatible netflow-like protocols. It allows you to visualize traffic per network devices, interfaces and subnets, and to better understand bandwidth consumption, traffic trends, applications, host traffic and traffic anomalies. This in turn lets you optimize your network and applications, plan network expansion, save time required for troubleshooting and diagnostics and improve security.

Key Features

- Monitoring network bandwidth on routers and interfaces;
- Monitoring custom traffic on IP subnets and IP subnets groups;
- Monitoring end user traffic;

- Highlighting traffic structure with top talkers: hosts, services, protocols, conversations, QoS, AS;
- Exploring historical data: charts and flow records;

- Collecting and analyzing Cisco® NetFlow v5 and v9, NSEL, sFlow and standardized IPFIX (exported by devices from Cisco, Juniper, HP and other vendors).
- Available for Windows and Linux servers;

Feature Highlights

Bandwidth Utilisation

Bandwidth Top Consumers

Provides insight into hosts, services, conversations, protocols, QoS, and AS that consume most of the interface bandwidth.

Bandwidth Threshold Alarms

Sends an instant alarm message via email when traffic (total, host traffic etc.) on a particular router or interface exceeds its bandwidth utilization threshold.

Custom Traffic & IP Subnets Monitoring

Custom Traffic Monitoring

Allows creation of a Traffic Pattern that monitors a specific part of the total traffic. It can be customized to match traffic of certain features, such as the traffic between two networks (e.g. corporate network and Internet, or data centre and remote offices), exporter IP, interfaces, and source and destination ports.

IP Subnets Traffic Monitoring

Provides insight into hosts, services, conversations, protocols, QoS, and AS that generate the most of the IP subnet traffic. IP subnets and their groups can be used for department, site-to-site or office group monitoring. The IP subnet hierarchy is automatically applied to any defined Traffic Pattern.

Traffic Threshold Alarms

Sends an instant alarm message via email when traffic (total, host traffic etc.) in a particular Traffic Pattern or its IP subnet exceeds its traffic threshold.

End User Traffic Monitoring

End User Traffic Traffic Structure

Provides insight into traffic structure of end users traffic allowing understanding of their network usage and investigating security risks. End user (username) is automatically mapped to traffic belonging to IP addresses he/she used over time. Mapping is done by sending logon events as syslog to NetVizura server.

Traffic Threshold Alarms

Sends an instant alarm message via email when traffic (total, host traffic etc.) of a particular End User exceeds its traffic threshold.

Network Traffic Forensics

Multi-Perspective Charts

Enables you to drill down into traffic of any monitored node (router, interface, Traffic Pattern, and subnet), by using multiple views to gain full perspective. It gives you an option to view traffic as either throughput or volume for top talkers, which you can then additionally break down into bits, packets and flows. Host and Services charts also provide additional view of the source and destination IPs and ports. Identifies top hosts, services, conversations, protocols, QoS and AS.

Flow Records Archive

Allows the analysis of flow records (NetFlow raw data) even if months old. Offers extensive data on each flow: time stamp, duration, source and destination IPs and ports, TCP flags etc. Flows can be filtered, sorted and grouped by almost any table column. This enables detailed forensics, allowing you to identify the type of security issues (address scan, port scan, DoS attack etc.), hosts participation and used or compromised service ports.

Flow Based Reporting

Reports

Allows you to export charts and tables for any monitored node as a PDF file. PDF reports can also be scheduled and emailed. Flow records can be exported to CSV files.

Multi-Vendor Device Support

Analyzes NetFlow v5, NetFlow v9, NSEL and IPFIX data from any device capable of exporting to these formats. These include Cisco, Juniper, HP and other vendors' devices.

NetFlow Statistics without NetFlow Capable Device

Allows NetFlow data generated by free NetFlow probes, such as SoftFlowd, to be collected and segmented into IP subnets so that traffic can be analysed by sites, departments etc. This provides for an effective way of monitoring network traffic even without NetFlow capable devices.

Dashboard Overview

Real-time Alarms

Reduces significantly response and troubleshooting time by having all active alarms presented and prioritized clearly.

Key Network and Security Monitors

Improves network visibility, understanding, and contextual awareness by showing

System Reqirements

HARDWARE	RECOMMENDED REQUIREMENTS
CPU	Dual Core 2.0GHz
Memory	4 GB
HDD Space	120GB - SAS or SSD in RAID 0 or similar set-up with striping Additional external storage is recommended for archiving old flow records
SOFTWARE	**MINIMUM REQUIREMENTS**
OS	**Server**: CentOS 6 (64 bit), CentOS 7 (64 bit), Debian Wheezy 7 (64 bit), Debian Jessie 8 (64 bit) Ubuntu Trusty Tahr 14.04 LTS (64-bit), Ubuntu Xenial Xerus 16.04 LTS (64-bit) Windows Server 2008 (64-bit), Windows Server 2012 (64-bit), Windows Server 2016 (64-bit) **Workstation:** any OS supporting recommended web browsers
Database	PostgreSQL 9.2+ (free) Detailed installation and repository links provided in the installation guide
Web Browser	Chrome 35.0+, Firefox 26.0+, Internet Explorer 11
Other	Oracle Java 8, Apache Tomcat 6, 7 and 8 (free)
INTEGRATION WITH OTHER NETVIZURA PRODUCTS	
Deployment	Stand alone product, no additional products required
Other Products	Other products are enabled via license key. Certain NetFlow Analyzer features are enhanced by other products.

NOTE: The recommended server requirements assume default configuration: 2,000 fps on avarage, 5,000 fps max, 500 monitored nodes, 30 days or archive data and 365 days of aggregated data.

Significant increase in the number of flows processed or nodes monitored can lead to an increase in the CPU and memory requirements. Significant rise in the number of flows and extension of the flow archive storing time will increase flow archive size and require more HDD space and/or additional external storage.

For more examples and up-to-date system requirements, please visit our online guide.

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 recognisable clients.

Soneco d.o.o.
Makenzijeva 24/VI, 11000 Belgrade, Serbia
Phone: +381116356319
Email: info@soneco.rs

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