

NetFlow Analyzer from NetVizura



PRODUCT REVIEW

Cisco's NetFlow is the network administrator's best friend, as it provides a wealth of information concerning IP traffic, interfaces, ports, services and much more. However help is needed, as its true value can only be realised if your choice of NetFlow collector provides the tools required to make sense of it.

NetVizura is an expert in the field of network analysis and its NetFlow Analyzer software provides an unbeatable range of tools for collecting, processing, analysing and archiving NetFlow data. Its capabilities outstrip many competing products as, along with its in-depth forensics and reporting, it offers traffic threshold and volume alarms, end user analysis and custom data collection options.

This latest version adds significant capability. Its web console seamlessly integrates the NetVizura EventLog Analyzer and free MIB browser tools, and with these onboard, you have access to Syslog and SNMP trap collection, analysis and search facilities, plus options to view SNMP data and MIBs.

Host system requirements are modest. We used a low-cost HPE ProLiant DL20 Gen9 rack server equipped with a 3.4GHz E3-1230 v5 Xeon, 16GB of DDR4 and a cheap 4TB SATA hard disk. We ran the Windows version of NetFlow Analyzer, and there was some preparatory work required which was covered clearly in the manual. With this complete, the slick web console wowed us with its new

Dashboard Overview. This presents a colour-coded alarm overview with hotlinks along with six graphs below showing all NetFlow action for the selected time period.

The graphs provide at-a-glance views of all traffic plus the top interfaces, services, conversations, subnets and end users. Time periods can be customised at the top of the screen and each graph can be drilled into for greater detail.

To create plenty of flows for the host system we used the excellent MIMIC NetFlow Simulator from Gambit Communications. We configured it to generate a wide range of protocols, ports, interfaces, sources and destinations and then sat back to observe. We didn't have to wait long however, as NetFlow Analyzer spotted the NetFlow sources and automatically added them to its list of exporters along with the discovered interfaces. The console's NetFlow tab provides an overview of all exporters and we could select individual ones and observe everything being sent.

The level of information presented by the console is quite remarkable with big pie charts for interfaces, hosts, conversations, services, protocols, QoS, as well as traffic graphs for each element in a lower pane. Once we'd added our subnets, we used Traffic Patterns to view activity for specific areas of interest.

To identify the heaviest users we created custom patterns for a range of services and

could view traffic distribution across multiple exporters. Selected exporters can also be placed in the console's Favorites pane for quick access to related traffic views, avoiding the need to search the entire exporter list. Alarms can be used to alert on excessive usage, service abuse or suspect activity, including malware. They're extremely versatile as they can monitor exporters, interfaces, patterns, subnets or individual users, watch out for objects such as hosts, services or conversations, and assign one of eight available alarm levels.

To test this we created alarms to monitor specific services and then applied thresholds based on traffic throughput or volume. Triggered alarms were posted in the dashboard, and we also set NetFlow Analyzer to issue email alerts to multiple recipients.

The NetVizura NetFlow Analyzer is the perfect partner for busy support departments as it provides sophisticated NetFlow monitoring and analysis. It's capable of presenting a wealth of valuable information in a meaningful and user-friendly way, and its flexible licensing schemes make it a very affordable asset. **NC**

Product: NetFlow Analyzer

Supplier: NetVizura

Web site: www.netvizura.com

Sales: sales@netvizura.com

Tel: +381 (0)11 785 4824

Price: Enterprise package: Perpetual \$4,995 or \$2,345 yearly