The best real-time NetFlow analysis and collection tool

NetFlow is a protocol developed by Cisco used to gather information about traffic through devices on the network.

NetFlow is a protocol developed by Cisco used to gather information about traffic through devices on the network. Information collected from NetFlow's IP traffic to determine a flow includes:

1. Source IP address
2. Destination IP address
3. Source port
4. Destination port
5. Layer 3 protocol
6. Class of Service (CoS) - how to manage traffic in the network by grouping similar types of traffic (eg e-mail, streaming video, transferring large document files, etc.) together and treating each group is a class with its own priority.
7. Interface Ingress

By collecting this information and analyzing it, users can gain more in-depth information about the network and use it for a number of other purposes, including bandwidth monitoring, network performance troubleshooting. and detect unusual points.

Learn about analyzing and collecting NetFlow

1. NetFlow components
2. NetFlow and partners
3. List of leading NetFlow analysis and collection tools today
    1. 1. Solarwinds NetFlow Traffic Analyzer
    2. 2. PRTG Network Monitor
    3. 3. Scrutinizer
    4. 4. ManageEngine NetFlow Analyzer
    5. 5. nProbe and ntopng

NetFlow components

When NetFlow is deployed on the network, there are usually two main components: Flow Exporter and Flow Collector. Flow Exporter stores flow information to the Flow Collector. Flow Exporter is usually configured on a

device such as a router or switch, and in some cases, there may be several exporters for different flows. On the other hand, Flow Collector receives traffic logs from Flow Exporter, processes them and can analyze this information to present to users in appropriate form.

Note : In some cases, Flow Collector does not perform the analysis of the logs. Instead, Flow Collector only accepts logs and another application will perform this analysis.

NetFlow and partners

The important thing to emphasize here is that although NetFlow is developed by Cisco, it is also supported by other vendors. At the same time, other vendors also have their own NetFlow versions, including Juniper and NetStream's J-Flow. In addition, there is an IETF protocol for transmitting network IP flow information - IP Flow Information Export (IPFIX) - based on Cisco NetFlow 9 version.

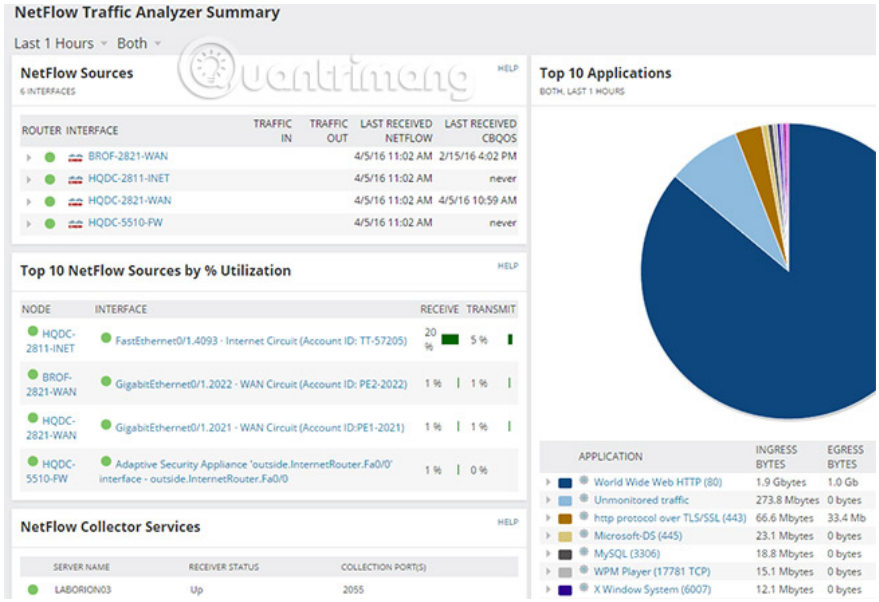
Note : There are several versions of NetFlow that have become obsolete. NetFlow versions 5, 7 and 9 are the most commonly used versions.

Below, a list of the leading NetFlow analysis and collection tools today.

(As mentioned earlier, the Flow Collector receives records from Flow Exporter and analyzes these records to generate reasonable information. More details are available later).

List of leading NetFlow analysis and collection tools today

1. Solarwinds NetFlow Traffic Analyzer



Solarwinds NetFlow Traffic Analyzer (NTA) is a tool for analyzing bandwidth and network traffic, supporting various flow technologies including NetFlow, J-Flow, IPFIX and NetStream.

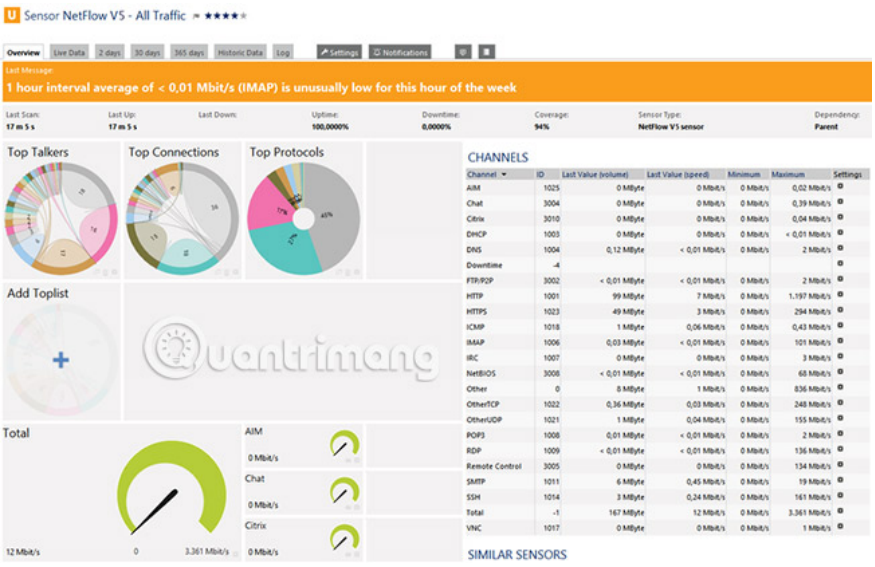
Solarwinds NTA can provide insight into bandwidth usage on the network, such as which IP address or application is consuming the most bandwidth at a given time. It can analyze patterns in traffic at a certain time, so it has the ability to perform network traffic surveys.

Solarwinds NTA has a starting price of $ 1,875 (43,500,000 VND), tracking 100 elements (with a free trial for 30 days). Another note is that Solarwinds NTA needs to integrate with Solarwinds Network Performance Monitor (NPM) to perform its functions.

This means to calculate the cost (and the necessary requirements) of Solarwinds NPM along with the cost of Solarwinds NTA. NPM Solarwinds also have a free trial for 30 days and the cost to buy a license is priced from $ 2,895 (67,150,000 VND), tracking 100 factors.

Download the free trial version of Solarwinds NetFlow Traffic Analyzer for 30 days.

2. PRTG Network Monitor



PRTG Network Monitor is an all-in-one network monitoring solution, including performance monitoring, bandwidth, applications and servers, etc. The biggest plus is the NetFlow tracking feature that is enabled by default in tool - does not require installation of an add-on or upgrade. PRTG Network Monitor can analyze different NetFlow versions (v5, v9), industry standards (Internet Protocol Flow Information Export - IPFIX) and other technologies such as sFlow or J-Flow.

One of the NetFlow monitoring applications available from PRTG Network Monitor is bandwidth usage analysis. For example, users can determine the amount of bandwidth being used by other servers, protocols and applications. This can be very helpful in troubleshooting problems related to network performance.

In setting PRTG NetFlow, Flow Collector differs from analysis software. Flow Collector can be any computer that receives a flow report from exporters and has a PRTG probe installed on it. The analytical software is PRTG Network Monitor, where the Flow Collector (system with PRTG probe) is set as the sensor.

PRTG Network Monitor is available in two versions: Freeware and Commercial. Freeware version is a fully functional PRTG Network Monitor, allowing users to monitor up to 100 sensors. If you want to monitor more than 100 sensors, you will need to purchase a license for the Commercial version (starting price is from $ 1600, equivalent to 37,112,000 VND) to monitor 500 sensors. You can refer to this tool at paessler.com.

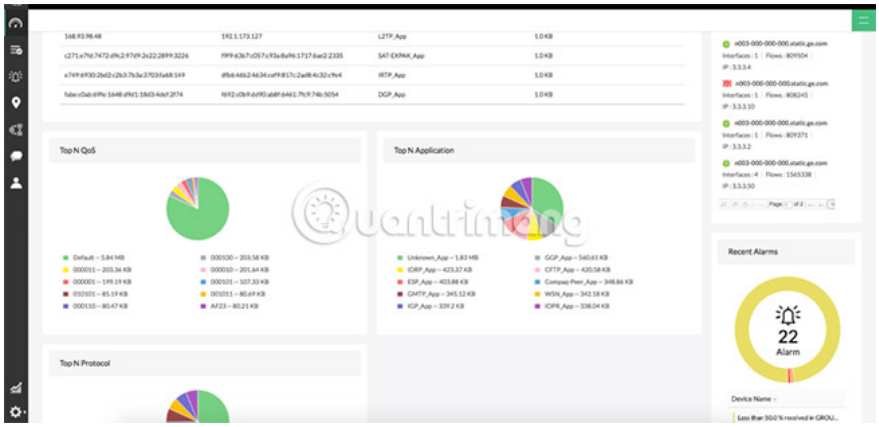
3. Scrutinizer

Not only is a NetFlow analysis tool, Scrutinizer is a fully functional incident response system, which can be used to analyze network traffic and report security incidents. It can collect and analyze data from different flow types including NetFlow, J-Flow, NetStream and IPFIX. This means that Scrutinizer can be used for network devices from Cisco and other providers.

Scrutinizer can provide visibility in both physical and virtual environments. It also has fast and advanced reporting features, support for multiple users and can be expanded due to its distributed structure.

Scrutinizer has 3 deployment options: Hardware, Virtual Machine and Software as a Service (SaaS). You can try Scrutinizer for free for 30 days, then the product downgrades to the free version. The free version allows maximum data collection for 5 hours from unlimited devices before resetting, ie historical data will be lost and everything starts over again.

4. ManageEngine NetFlow Analyzer



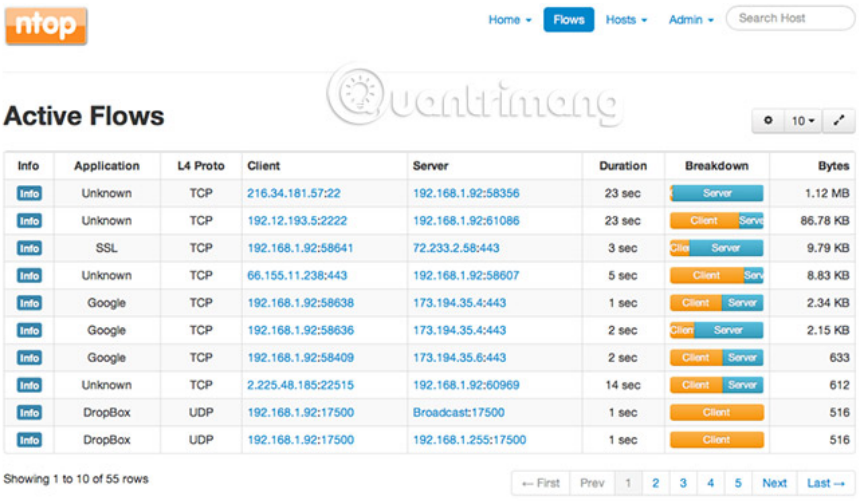
ManageEngine has an analytical tool and collects NetFlow similar to other solutions that the article discussed previously. NetFlow Analyzer also supports many flow technologies such as NetFlow, J-Flow and NetStream, with the main goal of analyzing network traffic and monitoring bandwidth.

ManageEngine NetFlow Analyzer integrates a number of interesting features such as customizable dashboards, iPhone apps for monitoring anytime, anywhere and reporting capabilities on Cisco Medianet and Cisco WAAS.

ManageEngine provides online demo for NetFlow Analyzer tool. This is useful because users can try it out before deciding whether to download or purchase a license. NetFlow Analyzer has two versions: Essential and Distributed. Both versions are free to try for 30 days. The lowest license price for Essential version is $ 495 (VND 11,482,000), tracking 10 interfaces. There is also a free version, which is used to monitor two interfaces without any license.

Download the free version here.

5. nProbe and ntopng



ntopng is an open source tool to monitor network traffic. It works by collecting packages from an interface and analyzing it to provide useful information such as the Top X talker - host and the most bandwidth intensive application.

ntopng can connect to nProbe, a NetFlow / IPFIX crawler. In this way, nProbe acts as Flow Collector, receiving records from the Flow Exporter and sending this information to ntopng for analyzing information, then presenting it in a user-readable format.

Although ntopng has a free version (Community version), a license is required to use nProbe (unless the user is a non-governmental organization or educational institution). nProbe has two versions: Standard and Pro with Plugins. The Standard version costs € 149.95 (VND 3,950,000) and the Pro with Plugins version costs € 299.95 (VND 7,895,000).

This article discussed NetFlow and other flow-related technologies. They are very useful in analyzing network traffic, troubleshooting performance and monitoring bandwidth.

The article also highlights a number of tools that can be used to collect and analyze NetFlow logs including Scrutinizer, PRTG Network Monitor and ntopng / nProbe. Other tools that the article has not mentioned such as NFDUMP or EHNT are open source and free. The reason these tools are not discussed in this article is because they are limited to NetFlow (unlike other tools that can support both NetFlow, J-Flow, NetStream, etc.).

In short, if you are looking for a solution that strictly enforces NetFlow collection and analysis, as well as being able to expand to different platforms and protocols, you should use Solarwinds NetFlow Traffic Analyzer (go included with Network Performance Monitor).

If you are more interested in analyzing NetFlow as an add-on to a network monitoring solution, try PRTG Network Monitor or ManageEngine NetFlow Analyzer. If you are interested in scalability and security analysis, the Scrutinizer may be the choice you are looking for. Finally, if you want a cheap solution with some open source features, consider ntopng or nProbe.

Wish you find the right choice!

See more:

1. Top 10 best bandwidth monitoring software
2. Data analysis with Network Monitor
3. Monitor and save Internet capacity on Windows 10