Flowmon
Driving Network Visibility

Handbook
July 25, 2016

HOW TO ANALYZE AND UNDERSTAND YOUR NETWORK

Part 1: Infrastructure Monitoring vs. Network Traffic Monitoring

by

Pavel Minarik, Chief Technology Officer
at Flowmon Networks

1 Introduction

When it comes to monitoring, the majority of IT professionals most likely think of server and service availability, CPU and RAM utilization, the status of a particular network interface or a number of transferred packets. This should be seen as mandatory for every responsible network administrator. But let's face the truth – this is not how you can manage network in the 21st century.

In the first part of this handbook, we will describe the difference between traditional infrastructure monitoring and next generation network monitoring that helps to deal with issues that arise in the modern IT environment.

The traditional concept of monitoring, as described above, is performed by a SNMP (Simple Network Management Protocol) that delivers an overview of the IT infrastructure; giving network administrators information about the availability of its components. Such monitoring is considered a "must have" for every responsible data network administrator.

> Imagine a situation where an unexpected traffic anomaly occurs and network traffic increases significantly - the administrator gets the information about the increased number of packets and volume of the transferred data on network interfaces. But what else? What is the origin of this anomaly? Which device is responsible for the traffic increase? What protocols and services are involved in this situation? These are the questions that traditional infrastructure monitoring is not able to answer. It doesn't look into the network traffic itself, and therefore has no information about its structure.

2 Network Traffic Monitoring

Modern corporate infrastructure cannot be efficiently managed by tools that have remained practically unchanged since the nineties and are not able to cope with the current robustness, reliability or security issues of the time. Network traffic monitoring tools were developed for this reason (in addition to providing administrators with appropriate answers). These tools are usually referred to as **"next generation monitoring"**.

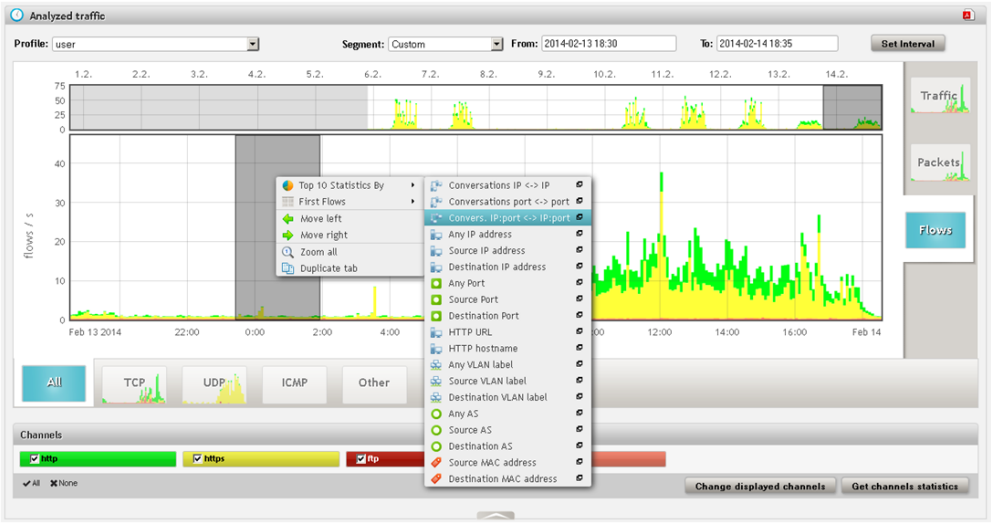

Figure 1: Monitoring capabilities and advanced traffic analysis

Network traffic monitoring generates statistics both on the underlying data transfers when abstracting from packets, and the subject of the communication itself (the content of the communication is not stored). These statistics represent the flow data in the network, which can be thought of as similar to a list of telephone calls. We know who communicates with whom, when, how long and how often; but we do not know what the subject of the conversation is. In the language of a data network environment, we monitor IP addresses, data volumes, time, ports, protocols and other technical characteristics of TCP/IP communication in the third and fourth network layer.

> To go back to the aforementioned anomaly; by a simple query of the data flows we can immediately get information that it is in communication with the FTP service (TCP protocol, port 20 – see figure 1 when the local PC (with IP address 192.168.34.78) stores large volume of data on a public server.

3 Flow Data

There are a number of different flow data standards and formats encountered in practice, and the Cisco standard NetFlow is one of the most important ones. The NetFlow standard is available in several versions. The original NetFlow v5 is today considered obsolete as it does not support IPv6 traffic, VLAN numbers or MAC addresses. These imperfections have been overcome by the NetFlow v9, which is based on certain templates and enables flexible settings of monitored traffic information. The current standard is known as the IPFIX (also known as NetFlow v10) and was developed as a result of the NetFlow standardisation process by IETF (RFC 5101, RFC 5153).

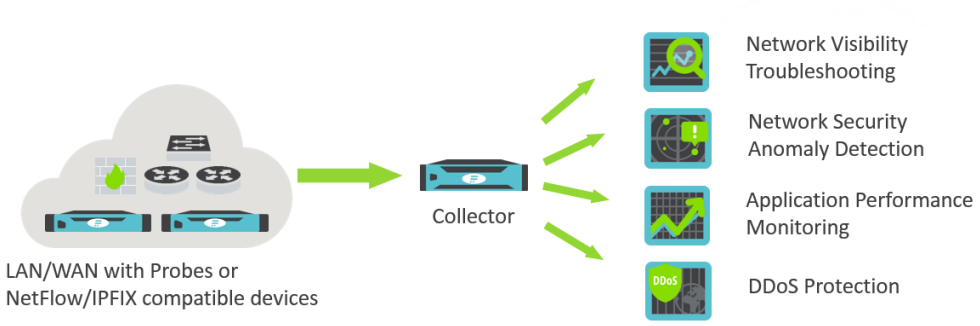

Figure 2: Architecture of flow data collection

NetFlow statistics are provided by network elements (routers, switches) or by specialized standalone hardware probes. The probes are transparently connected to the monitored network as passive appliances, creating a precise and detailed flow of statistics from the copy of network traffic. This approach is used to overcome various performance and feature limitations of router-based NetFlow monitoring.

> It is always important to check the router/switch documentation to ensure it supports NetFlow and if so which version. It is usually necessary to test if it does – older nodes can sometimes suffer from performance issues, do not provide precise statistics or have limited scope for monitored network traffic characteristics. Flow data is not only the domain of Cisco as there are a number of compatible alternative standards, for example jFlow, cFlow or NetStream.

4 Processing Flow Data

For the full utilization of flow data, we need a tool that is capable of collecting, storing, displaying, reporting and analyzing network statistics. The NetFlow collector is one such tool. It is a specialised software or hardware appliance which is equipped by the appropriate software. The collector ensures that data traffic statistics are stored, reported and analysed centrally. Thanks to this, the network administrator is provided with an immediate overview of traffic structure, reporting on data network utilization, as well as a powerful troubleshooting tool.

Imagine this situation: a user from one branch has recognized a poor response from the internal systems located in a distant company headquarters, as well as the slow loading of websites. He notifies the administrator at the headquarters that "something" has gone wrong. After only a quick look into the monitoring system, the administrator can identify the end station that has been transferring a huge amount of data from the internet. Moreover, the administrator can easily and immediately respond to that situation, i.e. by notifying the user to reduce or even stop downloading from the internet.

5 Behavior Analysis

An important benefit of network traffic monitoring technology is data protection and IT security. When we analyze network statistics, we gain a completely new perspective on the monitored infrastructure, so that we can automatically detect infected devices, malicious activities, attacks or network traffic anomalies in general. This technology is known as a network behavior analysis (NBA). Unlike signature-based solutions, NBA is able to detect new and advanced threats against which other security tools are ineffective.

Let's imagine another scenario. A curious user opens an attachment in his e-mail, which installs a malicious code onto his computer. This code will find the internal network servers running Windows and then start to try different combinations of credentials for Remote Desktop Services. From time to time, it encrypts sensitive data and uploads the data to a server somewhere on the other side of the world. How would current security tools respond to such a situation? The antivirus program can be taken for granted; however, it is not a measure against targeted attacks and custom-made malware. If the antivirus program allows the user to run an infected attachment, it will hardly be able to prevent consequent activities. A secured perimeter and advanced firewall will not help us, since the described activity will not even appear at the perimeter.

How does the monitoring system equipped with NBA respond? The monitoring system automatically reveals the attack when the malicious code starts seeking servers in the internal network (i.e. a horizontal port scan), followed by the attempt to connect to Windows Remote Desktop (i.e. a dictionary attack). It reports the malware communication to the control centre, which is located on the other side of the world, as suspicious.

6 Conclusion

We have introduced network traffic monitoring technology which utilizes information from the flow data. This technology delivers detailed network traffic visibility in order to provide effective network administration, troubleshooting and the detection of security issues and threats. Therefore it can be fairly described as a tool which helps you to get the network under control.

Author

Pavel Minarik, CTO at Flowmon Networks

Pavel Minarik has worked in the area of cyber security since 2006. During this time he has participated in several research projects as a senior researcher at the Institute of Computer Science at Masaryk University. He is the author of more than ten publications in the domain of behavior analysis and numerous algorithms for traffic processing and anomaly detection. As Chief Technology Officer at Flowmon Networks, Pavel is responsible for the technology roadmap, product design and development, as well as technical support and customer projects worldwide.

About Flowmon Networks

Flowmon Networks empowers businesses to manage and secure their computer networks confidently. Through our high performance network monitoring technology and lean-forward behavior analytics, IT pros worldwide benefit from absolute network traffic visibility to enhance network & application performance and deal with modern cyber threats. Driven by a passion for technology, we are leading the way of NetFlow/IPFIX network monitoring that is high performing, scalable and easy to use. The world's largest businesses, internet service providers, government entities or even small and midsize companies rely on our solutions to take control over their networks, keep order and overcome uncertainty. With our solution recognized by Gartner, recommended by Cisco, Check Point and IBM, we are one of the fastest growing companies in the industry.

Learn more at www.flowmon.com