3. ГОСТ Р ИСО 10012-2008. Менеджмент организации. Системы менеджмента измерений. Требования к процессам измерений и измерительному оборудованию;

4. ГОСТ Р 8.892-2015 Государственная система обеспечения единства измерений (ГСИ). Метрологическое обеспечение. Анализ состояния на предприятии, в организации, объединении;

5. ГОСТ ISO 9000-2011 Системы менеджмента качества. Основные положения и словарь;

6. ГОСТ ИСО/МЭК 17025-2009. Общие требования к компетентности испытательных и калибровочных лабораторий

NETWORK TRAFFIC ANALYSIS TOOLS

DOI: 10.31618/ESU.2413-9335.2020.5.81.1171

[1]***Boranbayev S.N.,*** [2]***Kuanyshev D.D.***
[1,2]L.N. Gumilyov Eurasian National University, Nur-Sultan, Kazakhstan

ANNOTATION

The article studies network traffic analysis tools. Various aspects of network traffic analysis are considered algorithms and approaches to network traffic analysis, as well as software and hardware tools for effectively solving this problem. The article studies the current state of this area. It is given recommendations on what to pay attention when using network traffic analysis tools.

Key words: network traffic, algorithm, analysis, packet, network.

1.Introduction

Today network traffic analysis is a very broad topic. By «network traffic analysis» we mean the aggregate name of technologies and their implementations, allowing accumulate, process, classify, control and modify network packets depending on their content in real time. The active development of network technologies and the expansion of the volume of information services provide constant growth of new users, which has a pronounced dynamic character. At the same time, there is an increase of the volume of network traffic. According to the research [1], the approximate dynamics of the growth of traffic transmitted through the World Wide Web is 70% -150% per year (over the past few years), so on average the amount of transmitted information doubles every year.

On the one hand network traffic analysis is the development of algorithms and approaches to analysis, on the other hand it is the development of software and hardware tools for an effective solution of this problem. At the time it leads to both confusion in terminology and the deliberate manipulation of facts and figures for marketing purposes. In this article it is made an attempt to reflect the current state of this area and on what to pay attention when using network traffic analysis tool [1].

In a simpler market segment you can find packet analyzers that copy passing traffic into files. Then this information needs to be processed to get an accurate picture of the traffic patterns. Also, you can find complex systems that measure traffic from several points in the network at the same time. They can also combine this source material to detect unusual user behavior.

Although the network offers real-time data, network traffic analysis tools rarely work in real time. Packet headers are the main source of information for analysis, but traffic analyzers wait until series of packets will not be captured and saved. Thus, it can be said that NTAs (Network traffic analysis) operate at the apps level and not at the network level.

Analysis gives NTA a better overview of network activity at the apps level. The information available at the network level is not sufficient to identify common traffic patterns, and it allows malicious traffic that is deliberately spread across multiple packets or aggregates activities from different sources.

Network traffic analysis can provide quick feedback, but in the fastest mode it is «almost done». Security applications cannot detect threats until they don't have data streams to work with. With opportunity analysis, there is less urgency, accuracy of forecasts is more important than efficiency.

The NTA utility depends on the reason why you want to analyze the network. We consider some traffic analysis tools [2].

2.SolarWinds NetFlow Traffic Analyzer

The SolarWinds NetFlow Traffic Analyzer (Picture 1) is available as an autonomic monitor or as part of a Network Bandwidth Analyzer package that also includes a Network Performance Monitor. The NetFlow Traffic Analyzer uses packet sniffing utilities built into network equipment to obtain packet samples and throughput metrics. These systems include Cisco NetFlow, Juniper Networks J-Flow and Huawei's NetStream, as well as sFlow and IPFIX systems. The tool also interprets NBAR2 data from Cisco devices.

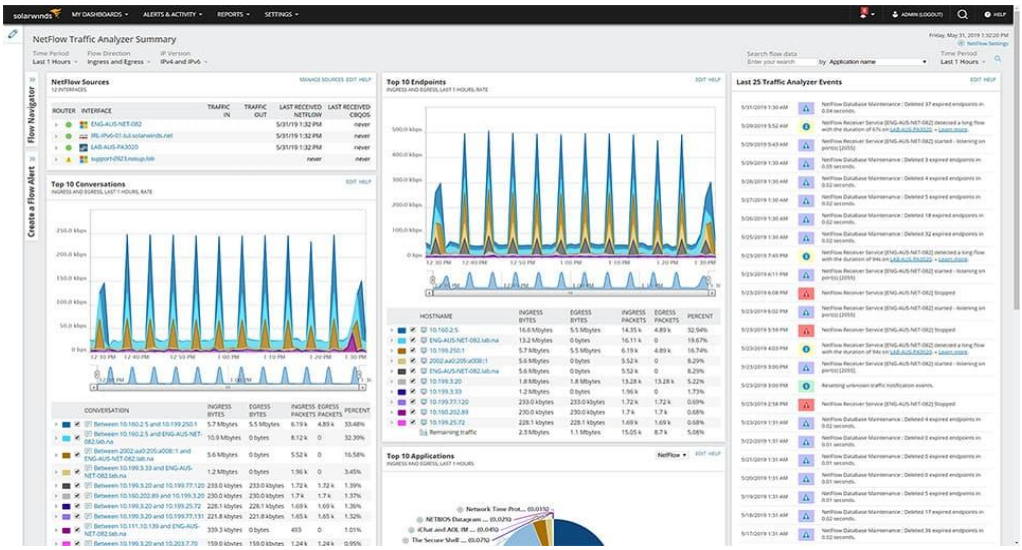
This collected data can be viewed in real time on the screen. However this analysis only takes place on stored data. The utility can detect VLAN (Virtual Local Area Network), such as simultaneous voice traffic on the network. Real-time data features include bandwidth streams that will alert you if traffic begins to exceed your network bandwidth limit.

Data analysis screens will show the applications generating the most traffic and can also segment data by source and protocol / port. Timeline charts show peaks and troughs in traffic volumes over hours, days or months. This will allow you to estimate the time of peak demand so that you can move batch jobs and downloads to less important hours [3].

The fix tools in the utility include traffic shaping measures that you can implement and manage queue

based traffic shaping measures such as class-based QoS.

SolarWinds NetFlow Traffic Analyzer software is a real-time network load and bandwidth monitoring tool. SolarWinds NetFlow Traffic Analyzer collects data from continuous streams of network traffic and converts those numbers into easy-to-interpret graphs and tables that show exactly how, by whom, and for what a corporate network is being used.



Picture 1 - SolarWinds NetFlow Traffic Analyzer

Network Performance Monitor and NetFlow Traffic Analyzer can cover LAN, WLAN, WAN, and connect with cloud services connections. Both of these tools are installed on Windows Server and are written on a common platform so they can interoperate. This communication allows to use a number of common modules, including PerfStack which shows basic resources supporting each app, and their current statuses.

Key features of SolarWinds NetFlow Traffic Analyzer:

– Traffic analysis tools. A comprehensive and flexible dashboard allows you to get a complete overview of network traffic on one page.

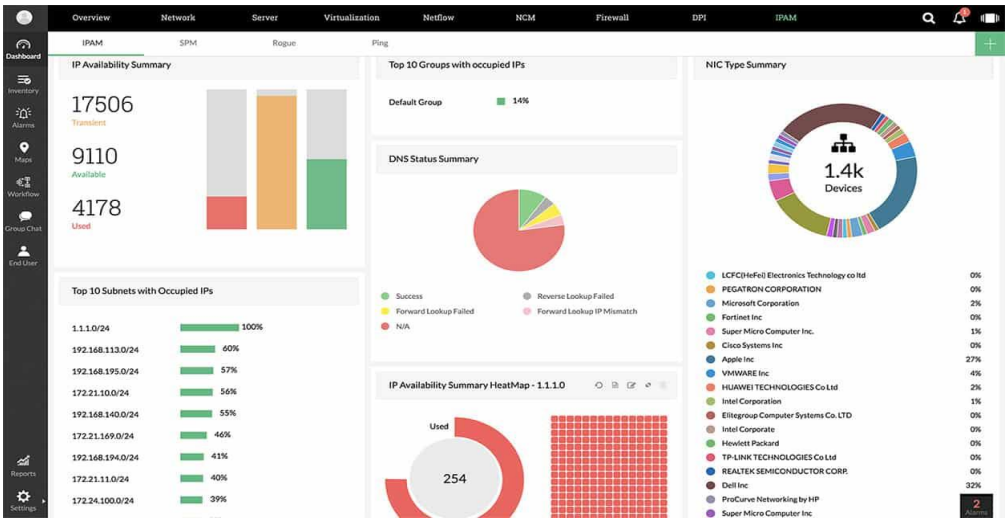
– Support for equipment from different vendors. SolarWinds NetFlow Traffic Analyzer analyzes NetFlow, J-Flow, sFlow, IPFIX and Huawei NetStream data on devices from Cisco Systems, Extreme Networks, HP, Juniper, Nortel Networks and other leading equipment manufacturers.

– Bandwidth analysis by apps. Advanced application research features provide valuable insight into which programs are causing the most bandwidth consumption.

–Notifications when bandwidth reaches streams. SolarWinds NetFlow Traffic Analyzer instantly alerts administrators when network traffic exceeds bandwidth streams. Notifications contain lists of the most active users and apps [4].

3. ManageEngine OpManager Plus Traffic Analyzer

ManageEngine OpManager Plus (Picture 2) includes all the monitoring capabilities required for an IT infrastructure work. This includes utilities for monitoring the operability of network devices and analyzing traffic flow.



Picture 2 – window of ManageEngine OpManager Plus

OpManager Plus scans the network, creates topology maps and device inventories. You can then work on testing traffic on each link or between two nodes on the network. Every time the network layout changes, equipment is moved, added or removed, the topology map and inventory are updated automatically. The map shows the status of each device and the load on each link.

The traffic flow capture system in the monitor can communicate with network devices via NetFlow. Network traffic indicators are displayed on the screen in real time. However, packets captured by the system are saved in files for analysis.

Daily traffic monitoring system allows you to set stream alerts to warn of potential resource depletion. These alerts can be sent via email or SMS, so there is no need to constantly monitor the monitoring screens.

System Analysis screens help you examine traffic sources by app, IP address, or interface. It implements NBAR (Network Based Application Recognition). The tool includes forecasting assistance so that capacity planning can be performed. The system also includes traffic shaping tools such as queuing and prioritization with class-based QoS (Quality of Service) to help squeeze value out of the network infrastructure.

OpManager Plus can monitor wireless networks as well as standard LANs. It can span Internet links between sites if WAN (Wide Area Network) is used, and can also integrate links to cloud servers.

4. Plixer Scrutinizer Traffic Analyzer

Plixer Scrutinizer (Picture 3) is an autonomic traffic analyzer, which available as a device, virtual device, or cloud service. This tool is designed to identify security threats, and its full name is Scrutinizer Incident Response System.

Scrutinizer collects packets and metrics using NetFlow. The system interacts with switches, routers, firewalls, servers, and wireless access points. Data collection occurs simultaneously at many points in the network. All transmitted data are displayed as live graphs as they appear, but they are also saved for security analysis. Multiple viewpoints can be useful for traffic analysis as well as for security processes as they detect bottlenecks in the system [5-6].

Picture 3 - window of Plixer Scrutinizer

All this data collection gives very large amounts of information up to 10 million streams per second. When a source tries to transmit a stream of packets, it may not know exactly what its stream looks like. If a source wants to ensure that the stream it generates is equipment conformal, it must first change the stream. Traffic shaping refers the process of modifying a stream to ensure its conformity. However the Scrutinizer interpolation engine is designed to handle such a large volume. Despite the fact that the system is designed to work with saved data, it works in a sliding window and starts working, including new data as soon as it arrives. This gives it a near-live capability that is able to detect security breaches almost immediately. Override warnings appear on system performance monitoring screens.

5. Conclusion

In this article there are two main reasons for analyzing network traffic: improving network performance and security checks.

SolarWinds NetFlow Traffic Analyzer editor`s choice is the leading network traffic analyzer. It works with NetFlow, J-Flow, sFlow, NetStream and IPFIX for packet capture.

ManageEngine OpManager Plus is an extension of the standard OpManager network performance monitor that includes traffic analysis.

Plixer Scrutinizer traffic analyzer used for network security that simultaneously scans traffic from multiple network locations. The traffic analyzer features are shown in Table 1.

Table 1

Traffic Analyzer Features

Name of analyzer	Type	Platform	Scalability
1. SolarWinds Real-Time NetFlow Analyzer	Free Download	Windows	SOHO
2. SolarWinds NetFlow Traffic Analyzer	Free Trial	Windows	SMB for large enterprises
3. ManageEngine NetFlow Analyzer	Free Trial	Windows, Linux	SMB for large enterprises
4. Plixer Scrutinizer	An inexpensive tool with a free starter version for small stores	hardware, virtual machine Windows or Linux, SaaS	SMB for large enterprises

REFERENCES

1.Seilov Sh.Zh., Boranbayev S.N., Kasenova M.N., Seilov A.A., Shingisov D.S. Intelligent analysis of information and communication traffic. Bulletin of the L.N. Gumilyov Eurasian National University. Technical science and technology series. –2019, №3 (128), 76-87 p.

2.https://www.opennet.ru/base/sec/arp_snif.txt.html

3.T. Yu. Lushnikova. Outstanding characteristics of campus traffic, Telecommunications, №4, 2017, 51-55 p.

4.https://itpro.ua/product/solarwinds-netflow-traffic-analyzer-4/?tab=description

5.Wan Optimizations.http://searchenterprisewan.techtarget.com/definition/WAN-optimization

6.A.I. Geltman, E.F. Evstropov, Yu.V. Markin. Analysis of network traffic in real time: an overview of applied problems, approaches and solutions, http://www.ispras.ru/preprints/docs/prep_28_2015.pdf

ГРАДИЕНТОМЕТРЫ ДЛЯ ПОИСКА ЛОКАЛЬНЫХ ФЕРРОМАГНИТНЫХ ОБЪЕКТОВ

DOI: 10.31618/ESU.2413-9335.2020.5.81.1169

Любимов Владимир Валерьевич
старший научный сотрудник
Федеральное государственное бюджетное учреждение науки
Институт земного магнетизма, ионосферы и распространения радиоволн им. Н.В. Пушкова Российской академии наук,
г. Троицк

АННОТАЦИЯ

Настоящая работа посвящена описанию магнитометров-градиентометров, созданных на основе феррозондовых компонентных датчиков магнитного поля. Приборы предназначены для проведения геомагнитных и поисковых работ в различных условиях и средах с возможностью использования различных средств их перемещения в пространстве.

ABSTRACT

This work is devoted to the description of magnetometers-gradientometers, created on the basis of luxgate component sensors. The devices are designed to conduct geomagnetic and search operations in different conditions and environments with the possibility of using different means of their movement in space.

Ключевые слова*:* магнитное поле, магнитные измерения, компонентные измерения, феррозондовые магнитометры, градиентометры, поиск ферромагнитных объектов.

Keywords: magnetic field, magnetic measurements, component measurements, fluxgate magnetometers, gradientometers, search for ferromagnetic objects.

ВВЕДЕНИЕ

Градиентометрический метод изучения магнитного поля Земли (**МПЗ**) является одним из основных методов, который используется как при проведении геофизических исследований в различных условиях и средах, так и в процессе проведения рекогносцировочных и специальных работ, связанных с поиском ферромагнитных масс и скрытых объектов. Этот метод реализуется при синхронном измерении значений модуля или составляющих вектора магнитной индукции (**ВМИ**) поля Земли датчиками, разнесёнными на некоторое расстояние («измерительную базу» - **ИБ**), и последующего вычисления градиента поля в направлении этой ИБ.