УДК 004.056.53

N. Yerzhanov[a], M.Y. Polushin, A.N. Kozhakhmetov
Academy of the NSC, Almaty, Kazakhstan
[a]nurasyl.yerzhanov@gmail.com

DETECTION OF ANOMALY NETWORK ACTIVITIES BY USING FLOWMAN NETWORKS SOLUTION

Аннотация. Чтобы обнаружить сетевые аномалии, в исследовании были рассмотрены подходы к обнаружению аномалий, основанные на поведении, путем сравнения текущего сетевого трафика. Сетевой метод Flowman обеспечивает гибкий и быстрый метод оценки базового распределения, а также широкую перспективу сетевого трафика для администратора сети. Мы можем идентифицировать аномалии, которые изменяют трафик быстро или медленно, вычисляя меру, связанную с относительной энтропией отслеживаемого сетевого трафика по сравнению с базовым распределением. Кроме того, наш метод собирает информацию об аномалии, и виджеты начнут отображать информацию.

Ключевые слова: аномальная сетевая активность, сетевая безопасность, связь, сеть Flowman

Аңдатпа. Желілік ауытқуларды анықтау үшін зерттеу ағымдағы желілік трафикті салыстыру арқылы мінез-құлыққа негізделген ауытқуларды анықтау тәсілдерін қарастырды. Flowman желілік әдісі базалық үлестіруді бағалаудың икемді және жылдам әдісін, сондай-ақ желі әкімшісі үшін желілік трафиктің кең перспективасын қамтамасыз етеді. Негізгі таратумен салыстырғанда бақыланатын желілік трафиктің салыстырмалы энтропиясымен байланысты өлшемді есептеу арқылы трафикті тез немесе баяу өзгертетін ауытқуларды анықтай аламыз. Сонымен қатар, біздің әдіс аномалия туралы ақпаратты жинайды және виджеттер ақпаратты көрсете бастайды.

Түйінді сөздер: желіден тыс белсенділік, желі қауіпсіздігі, байланыс, Flowman желісі

Abstract. In order to discover network anomalies, the research examined anomaly detection approaches based on behavior by comparing current network traffic. The Flowman Network technique provides a flexible and fast method for estimating the baseline distribution, as well as a wide perspective of network traffic for the network administrator. We can identify anomalies that change traffic either quickly or slowly by computing a measure related to the relative entropy of the network traffic under monitoring in comparison to the baseline distribution. Additionally, our method collects information about anomaly and widgets will start displaying information.

Key words: anomaly network activities, network security, communication, Flowman Network

Introduction.

Nowadays, detecting attacks on computer systems and networks is currently an important task in the field of information security. A well-executed computer attack can result in data loss, unauthorized access to information resources, and significant data distortion. This emphasizes the importance of developing and employing effective methodologies and techniques for detecting network attacks in order to protect data in computer systems and networks.

An attack detection system is typically defined as a software, hardware, or software-hardware device that detects illegal access to a computer system or network, as well as unauthorized control of those systems or networks. Attack detection systems are used to detect specific types of harmful activities that could compromise a computer system's security. Network

attacks against vulnerable services, attacks designed to expand privileges, unauthorized access to key files, and malicious software actions are examples of such behavior. Scanning computer ports for vulnerabilities used to obtain unauthorized access is an example of a network attack.

All network attacks can be categorized to anomalies and abuses. Activities that differ from the templates specified for users are highlighted when anomalies are observed. For the content of the profile of the controlled activity creates a special database.

A network anomaly is a sudden and brief departure from the network's regular operation. Some anomalies are purposefully generated by malicious attackers, such as a denial-of-service attack in an IP network, while others are totally accidental, such as an overpass falling in a busy road network.

Local computer networks of modern enterprises are filled with various applications and solve many problems. Network behavior is formed by users, software and hardware services, and other network devices. The normal functioning of the network means the following: guaranteed supply of services and stability to various stressful influences, which in the most general consideration can be divided into forced (equipment failure, errors in programs) and random (targeted attacks).

Background knowledge and literature review.

In this section, we provide relevant background to understand anomaly network activities and how to prevent it, as well as discuss previous studies on the topic.

Observed events

As a rule, it is impossible to prevent an attack, so it makes sense to concentrate all efforts on monitoring the consequences of the attack. Attacks can be divided into three levels:

- Transport. By attacks on the transport layer, we will understand attacks on the protocols of the channel, network and transport layers of the TCP/IP stack. This level includes, for example, various types of scanning, arp-spoofing, ip spoofing;
- Applied. By this level we will understand attacks aimed at errors in the implementation of various protocols of the TCP/IP stack application layer. Examples of such attacks can be DNS cache-poisoning, smb-die, http-response splitting;
- The level of service. Attacks of this level include all kinds of attacks caused by errors in incorrect processing of user data. Examples of such attacks are XSS, SQL injection, various overflows, etc.

There are two ways to detect an attack:

- Signature. This method boils down to searching for signs of already known attacks. The advantage of the signature method is that it is practically not susceptible to false positives. The disadvantage of this method is the inability to detect attacks that are not embedded in the system.
- Abnormal. It is known in advance what functional parameters a particular application or service has in a normal state, and any deviation from it is considered an attack. The anomaly search method allows you to respond to previously unknown attacks, but is prone to false positives and requires fine tuning for each observed object.

Both methods of detecting attacks can work at all three levels.

The result of any attack, if successful, is an information leak, for example, an ether-leak attack, or a change in any parameters of the attacked system, for example, opening a port, stopping the operation of some program, a significant change in the amount of use of some system resource by the program (for example, memory, processor time, etc.), launching a new program for execution. Similar events occurring in the system can be monitored using software tools.

Because a large shift in resource usage might occur during normal system operation (for example, an increase in requests to the mail server at the start of the working day), the difficulty of evaluating whether the program's behavior is normal or anomalous emerges. The solution of this problem is proposed on the basis of statistical methods of analysis.

Anomaly Detection.

The idea is as follows. Basically, all real automated information systems have a cyclical nature of functioning, which is determined by the working week or the production technological process.

Let's assume that there is a separate period at the initial stage of the system operation, during which we can assert that the system is operating normally. If such a time interval exists, then we will call it the training period. During the training period, we will monitor the use of various program resources and, based on the accumulated information, we will be able to build a function for predicting the further behavior of programs. During the operational operation of the system, we will continuously monitor the use of various resources by programs.

We will compare the actual results to the predictions. When the disparity between the expected and actual consumption of resources reaches a certain threshold, the program's behavior is termed abnormal. Simultaneously, a decision is made to modify the program's mode of operation in order to avoid a disturbance in the overall system's stability.

Literature review.

There are different ways and technologies detecting network anomalies, such as using neural network security, maximum entropy estimation.

The technology of neural networks can be used to solve the problem of diagnosing anomalous network activity. It is suggested that data on network activity be collected and a training sample be formed. The values of the parameters of network packets, along with the values of the sign of network activity, make up a sample for training a neural network. The structure is proposed, the neural network is trained, and the adequacy and classification ability of the neural network are assessed. It is demonstrated that a neural network model can be used effectively as part of an intelligent diagnostic system to detect anomaly network activity.[4]

The following methodology has been devised to collect network activity data and construct a training sample for a neural network:

1. allocation of a local network segment;
2. software installation;
3. network monitoring in conditions of normal network activity;
4. network monitoring in conditions of anomaly network activity;
5. data processing and formation of an educational sample.

The values of the parameters of the network packets that make up the traffic of the local computer network are received at the input of an intelligent system, the core of which is a trained neural network. The decision-making module analyzes the input values and generates a system response about the type of network activity. Within the framework of this algorithm, the problem of neural network diagnostics of abnormal network activity is solved.

It's important to note that the adaptive intelligent method for diagnosing irregular network activity is based on a neural network. Information about errors can gather in a specific database if activity in the local computer network is incorrectly determined. The system may retrain the neural network on a regular basis, taking into account the data from the incorrect network packet categorization.

Methods.

Network monitoring using Flowmon Networks solutions.

Flowmon is positioned as an A-class brand. Develops premium solutions for corporate customers and is marked in Gartner squares in the direction of Network Performance Monitoring and Diagnostics (NPMD). Moreover, interestingly, of all the companies in the report, Flowmon is the only vendor noted by Gartner as a manufacturer of solutions for both network monitoring and information protection (Network Behavior Analysis).

What are the tasks this technology is able to solve?

1. improving the stability of the network, as well as network resources by minimizing their downtime and unavailability;

2. improving the overall level of network performance;
3. improving the efficiency of the administrative staff, due to:
   - the use of modern innovative network monitoring tools based on information about IP streams;
   - providing detailed analytics about the functioning and state of the network – users and applications running on the network, transmitted data, interacting resources, services and nodes;
   - responding to incidents before they occur, and not after the loss of service by users and customers;
   - reducing the time and resources needed to administer the network and IT infrastructure;
   - simplify troubleshooting tasks.
4. increasing the level of security of the network and information resources of the enterprise, through the use of non-signature technologies for detecting abnormal and malicious network activity, as well as "zero-day attacks" (zero-day);
5. providing the required SLA level of network applications and databases.

Flowmon Networks product portfolio.

The kernel of the system is a collector responsible for collecting data on various flow protocols, such as NetFlow v5/v9, jFlow, sFlow, NetStream, IPFIX... The collector is available both as a hardware server and as a virtual machine (VMware, Hyper-V, KVM). By the way, the hardware platform is implemented on customized DELL servers, which automatically removes most of the issues with warranty and RMA. Its own hardware component is, perhaps, FPGA traffic capture boards developed by a subsidiary of Flowmon, and allowing monitoring at speeds up to 100 Gbps.

Figure 1 - Flowmon Collector

The collector is available both as a hardware server and as a virtual machine (VMware, Hyper-V, KVM). The hardware platform is implemented on customized DELL servers and allows monitoring at speeds up to 100 Gbps.

To prevent the load on the equipment and generate high-quality flow, Flowmon Networks suggests using its own probes (Flowmon Probe), which are connected to the network via the SPAN port of the switch or using passive TAP splitters.

Figure 2 - Flowman Probe

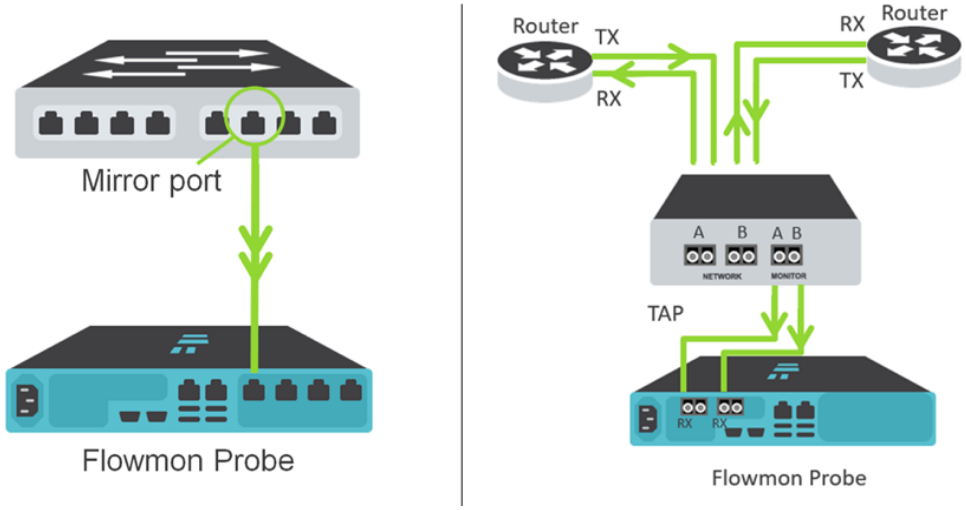


Figure 3 - SPAN (mirror port) and TAP implementation options

In this case, the "raw" traffic coming to Flowmon Probe is converted into an extended IPFIX containing more than 240 metrics with information. While the standard NetFlow protocol generated by network equipment contains no more than 80 metrics. This makes it possible to ensure the visibility of protocols not only at levels 3 and 4, but also at level 7 according to the ISO OSI model. As a result, network administrators can monitor the functioning of applications and protocols such as e-mail, HTTP, DNS, SMB…

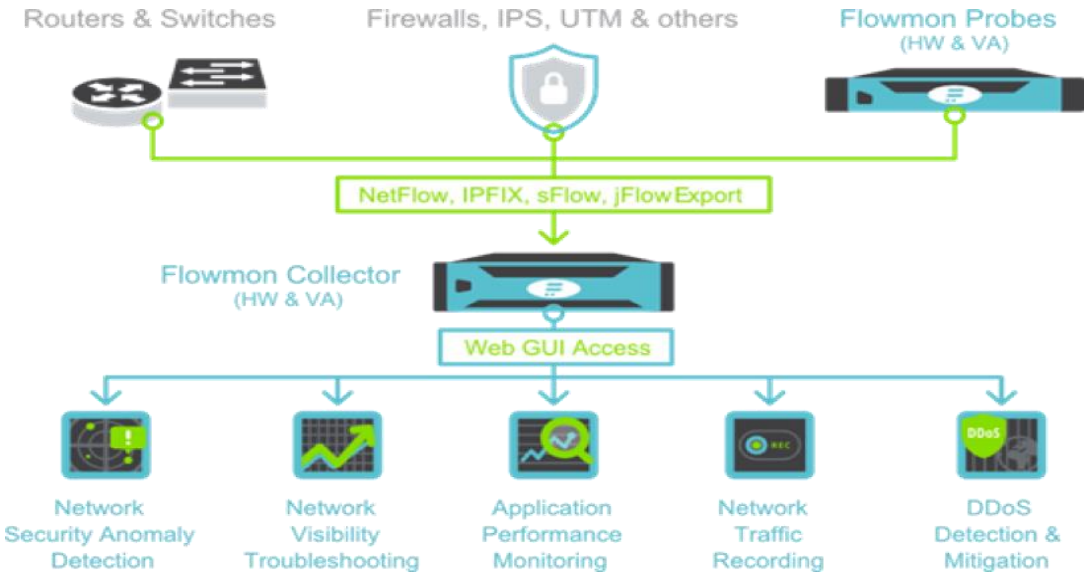


Figure 4 - Flowman Collector (HW \& VA)

The Collector, which accepts traffic from existing network equipment or its own probes, is at the heart of the entire Flowmon Networks ecosystem (Probe). However, it would be far too simple for an Enterprise solution to provide capability solely for network traffic monitoring. Open-source solutions can do the same thing, albeit not as well. Additional modules that enhance the core capabilities of Flowmon offer value to the product:

The value of Flowmon is additional modules that extend the basic functionality:

- Anomaly Detection Security module - detection of abnormal network activity, including zero-day attacks, based on heuristic traffic analysis and a typical network profile.

- Application Performance Monitoring module - monitoring the performance of network applications without installing "agents" and affecting target systems.
- Traffic Recorder module - recording fragments of network traffic by a set of predefined rules or by a trigger from the ADS module, for further troubleshooting and/or investigation of information security incidents.
- DDoS Protection module - protection of the network perimeter from volumetric denial of service DoS/DDoS attacks, including attacks on applications (OSI L3/L4/L7).

The practical part of detecting network traffic anomalies.

In this article, we will look at how everything works live using the example of 2 modules - Network Performance Monitoring and Diagnostics and Anomaly Detection Security.

1st step Installation of Flowmon Collector

The OVF template is used to deploy a virtual machine on VMware in a completely standard manner. As a consequence, we have a virtual computer running CentOS with ready-to-use applications. Humane resource requirements:

- We perform basic initialization using the sysconfig command.
- We configure the IP on the management port, DNS, time, Hostname and can connect to the WEB interface.

2nd step Installing a license

3rd step Setting up the receiver on the collector

It is vital to specify how the system will receive data from sources at this level. It might be one of the flow protocols or a switch's SPAN port.

In this example, we'll use the NetFlow v9 and IPFIX protocols to receive data.

The IP address of the Management interface - 192.168.78.198 - is used as a target in this situation. The Monitoring interface type is used on the eth2 and eth3 interfaces to get a copy of the "raw" traffic from the switch's SPAN port. We miss them, but not in our situation.

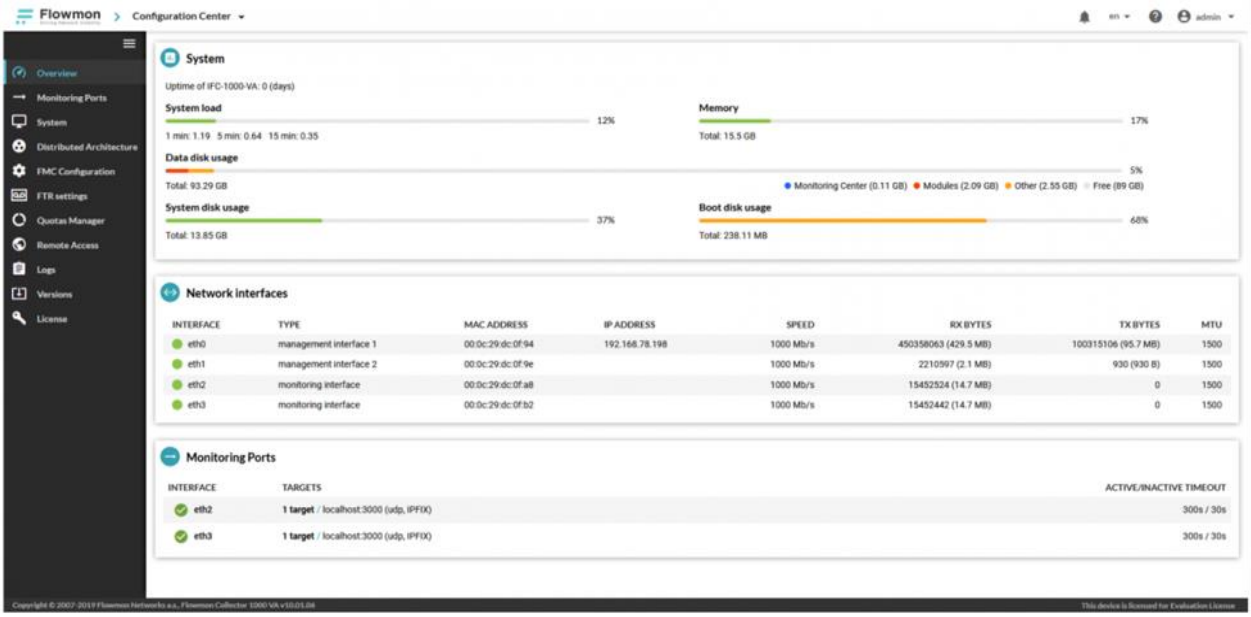


Figure 5 - Monitoring interface

Then we look at the collector port, which is where the traffic should be arriving.

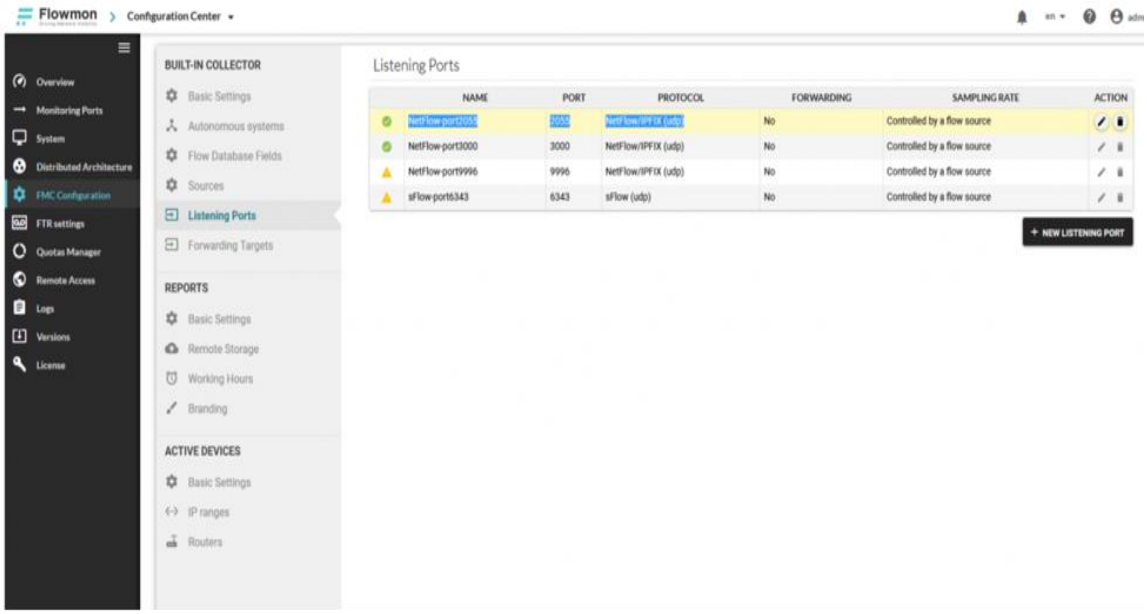


Figure 6 - In our case, the collector is waiting for traffic on the UDP/2055 port

4th Configuring network equipment for flow export

For our example, we'll take something more unusual. For example, the MikroTik RB2011UiAS-2HnD router. In the settings, set the target (collector address 192.168.78.198 and port 2055):

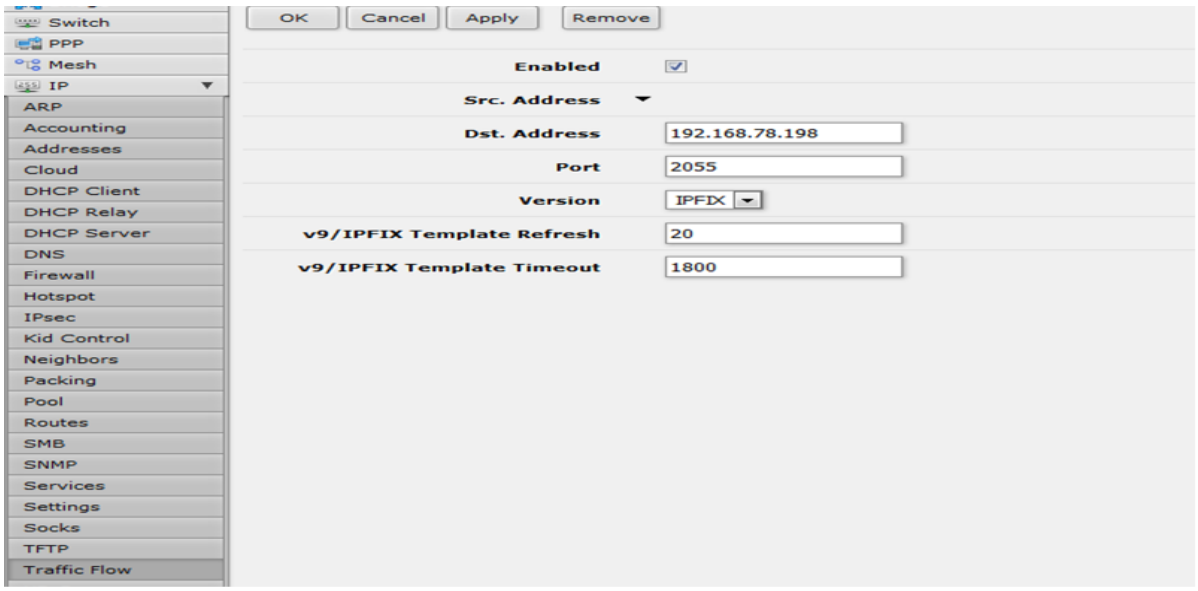


Figure 7 - MikroTik RB2011UiAS-2HnD settings.

5th Testing and operation of the Network Performance Monitoring and Diagnostics module

We can observe that data is entering the system. Widgets will begin to display information after the collector has accumulated traffic:

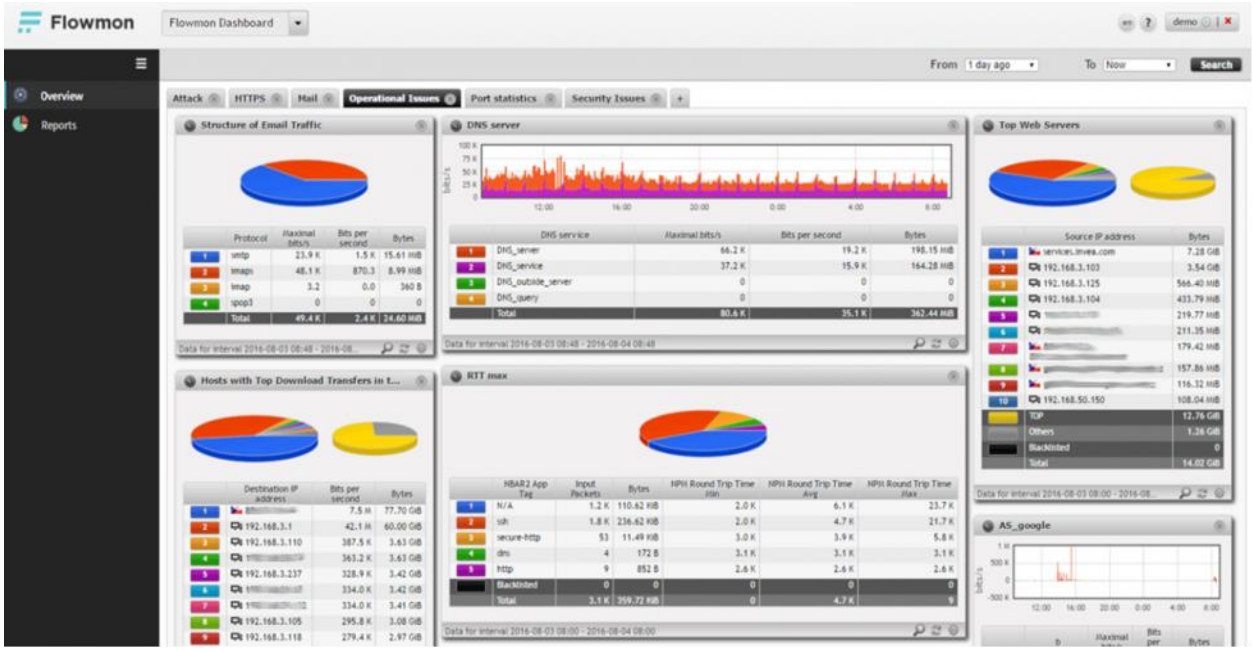
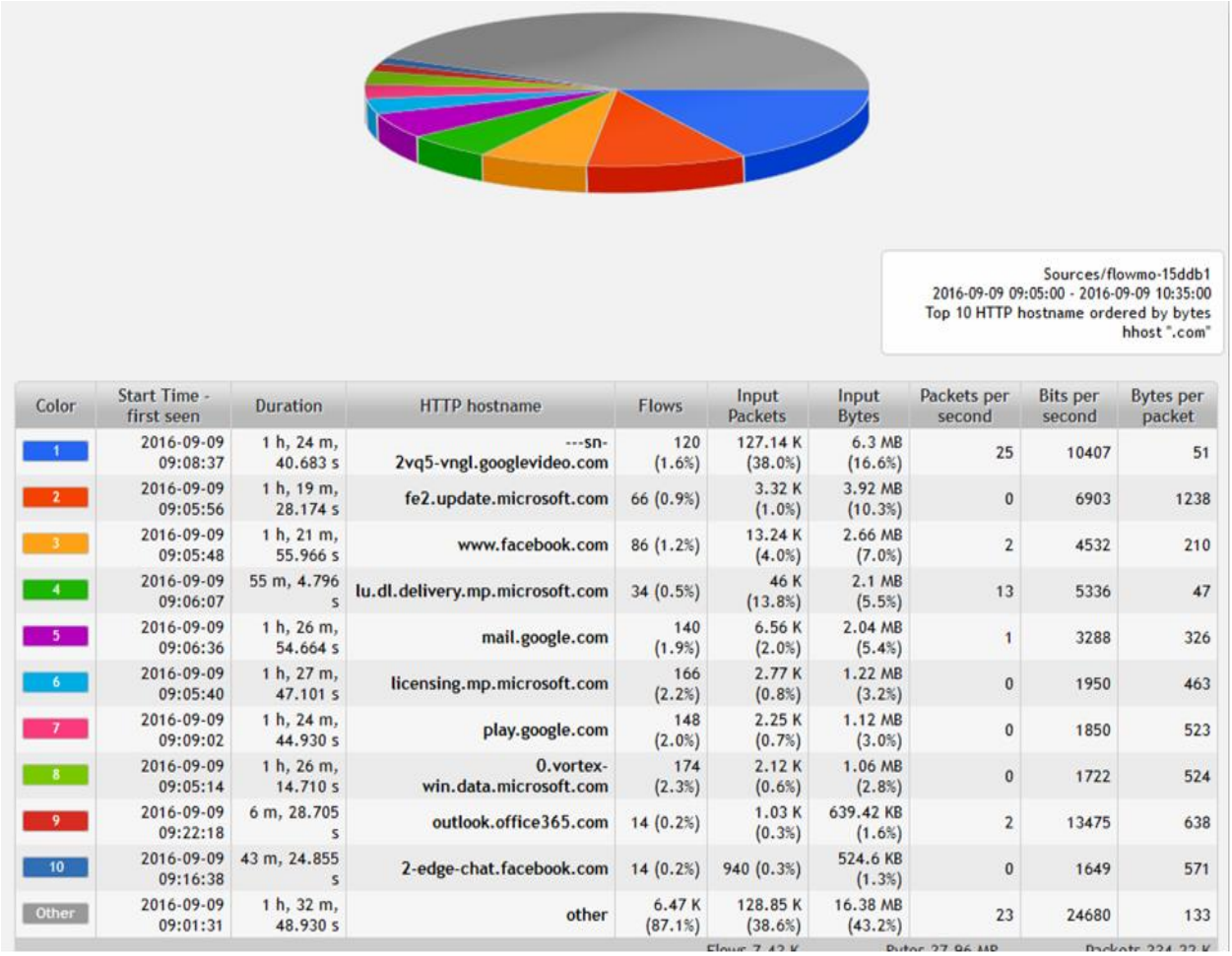


Figure 8

The system is built on the drill down principle. That is, the user, choosing a fragment of interest to him on a diagram or graph, "falls through" to the level of data depth that he needs:



Sources/flowmo-15ddb1
2016-09-09 09:05:00 - 2016-09-09 10:35:00
Top 10 HTTP hostname ordered by bytes
hhost ".com"

Color	Start Time - first seen	Duration	HTTP hostname	Flows	Input Packets	Input Bytes	Packets per second	Bits per second	Bytes per packet
1	2016-09-09 09:08:37	1 h, 24 m, 40.683 s	---sn-2vq5-vngl.googlevideo.com	120 (1.6%)	127.14 K (38.0%)	6.3 MB (16.6%)	25	10407	51
2	2016-09-09 09:05:56	1 h, 19 m, 28.174 s	fe2.update.microsoft.com	66 (0.9%)	3.32 K (1.0%)	3.92 MB (10.3%)	0	6903	1238
3	2016-09-09 09:05:48	1 h, 21 m, 55.966 s	www.facebook.com	86 (1.2%)	13.24 K (4.0%)	2.66 MB (7.0%)	2	4532	210
4	2016-09-09 09:06:07	55 m, 4.796 s	lu.dl.delivery.mp.microsoft.com	34 (0.5%)	46 K (13.8%)	2.1 MB (5.5%)	13	5336	47
5	2016-09-09 09:06:36	1 h, 26 m, 54.664 s	mail.google.com	140 (1.9%)	6.56 K (2.0%)	2.04 MB (5.4%)	1	3288	326
6	2016-09-09 09:05:40	1 h, 27 m, 47.101 s	licensing.mp.microsoft.com	166 (2.2%)	2.77 K (0.8%)	1.22 MB (3.2%)	0	1950	463
7	2016-09-09 09:09:02	1 h, 24 m, 44.930 s	play.google.com	148 (2.0%)	2.25 K (0.7%)	1.12 MB (3.0%)	0	1850	523
8	2016-09-09 09:05:14	1 h, 26 m, 14.710 s	0.vortex-win.data.microsoft.com	174 (2.3%)	2.12 K (0.6%)	1.06 MB (2.8%)	0	1722	524
9	2016-09-09 09:22:18	6 m, 28.705 s	outlook.office365.com	14 (0.2%)	1.03 K (0.3%)	639.42 KB (1.6%)	2	13475	638
10	2016-09-09 09:16:38	43 m, 24.855 s	2-edge-chat.facebook.com	14 (0.2%)	940 (0.3%)	524.6 KB (1.3%)	0	1649	571
Other	2016-09-09 09:01:31	1 h, 32 m, 48.930 s	other	6.47 K (87.1%)	128.85 K (38.6%)	16.38 MB (43.2%)	23	24680	133

Figure 9

6th Anomaly Detection Security Module

The module's "training" is the first step in using it. To do so, a specific wizard is used to specify all of the network's major components and services, including:

- gateway addresses, DNS, DHCP and NTP servers,
- addressing in user and server segments.

After then, the system enters training mode, which lasts anywhere from two weeks to a month on average. The system creates a baseline of traffic that is peculiar to our network during this time.

- what behavior is typical for network nodes?
- what amounts of data are usually transmitted and are normal for the network?
- what is the typical operating time for users?
- what applications are running on the network?

As a result, we now have a tool that can detect any anomalies in our network as well as departures from normal behavior.

- distribution of new malware on the network that is not detected by antivirus signatures;
- building DNS, ICMP or other tunnels and transmitting data bypassing the firewall;
- the appearance of a new computer on the network, posing as a DHCP and/or DNS server.

After your system has been trained and a network traffic baseline has been established, it begins to detect incidents:

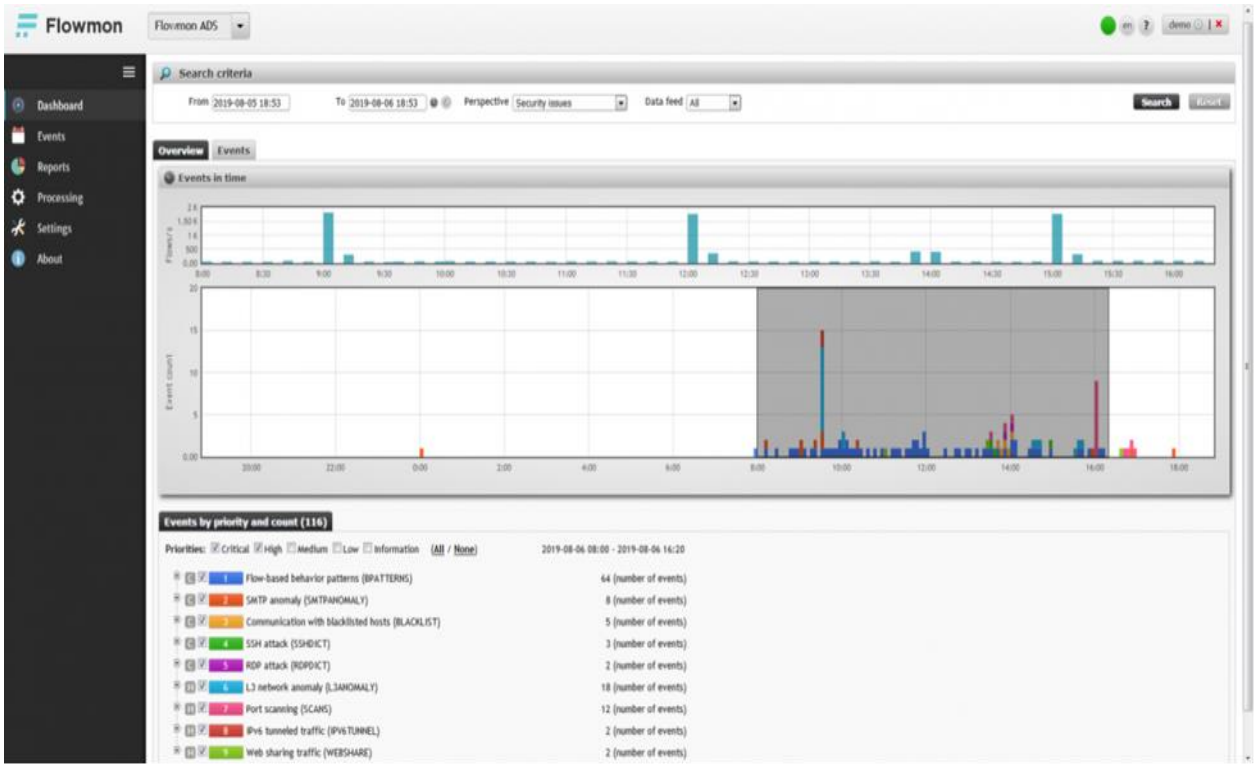


Figure 10

It is obvious, that anomaly behavior of the attacker in the network exists. It all starts with a horizontal network scan on port 3389 (Microsoft RDP service) by the host with the IP 192.168.3.225, which detects 14 possible "victims":

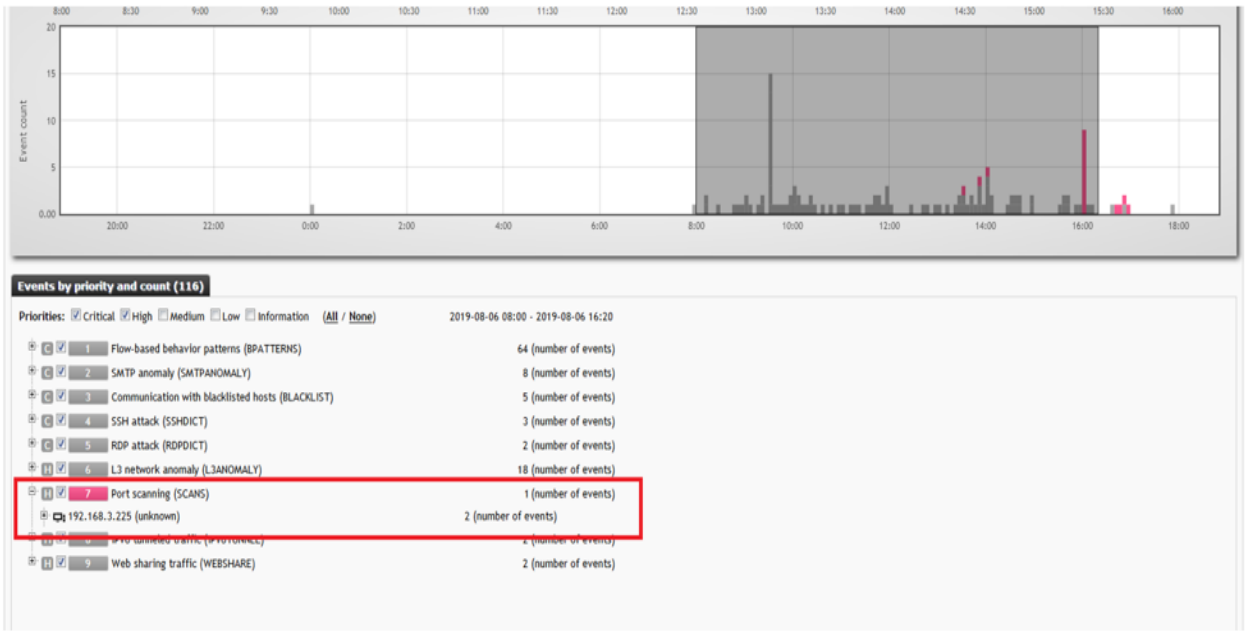


Figure 11

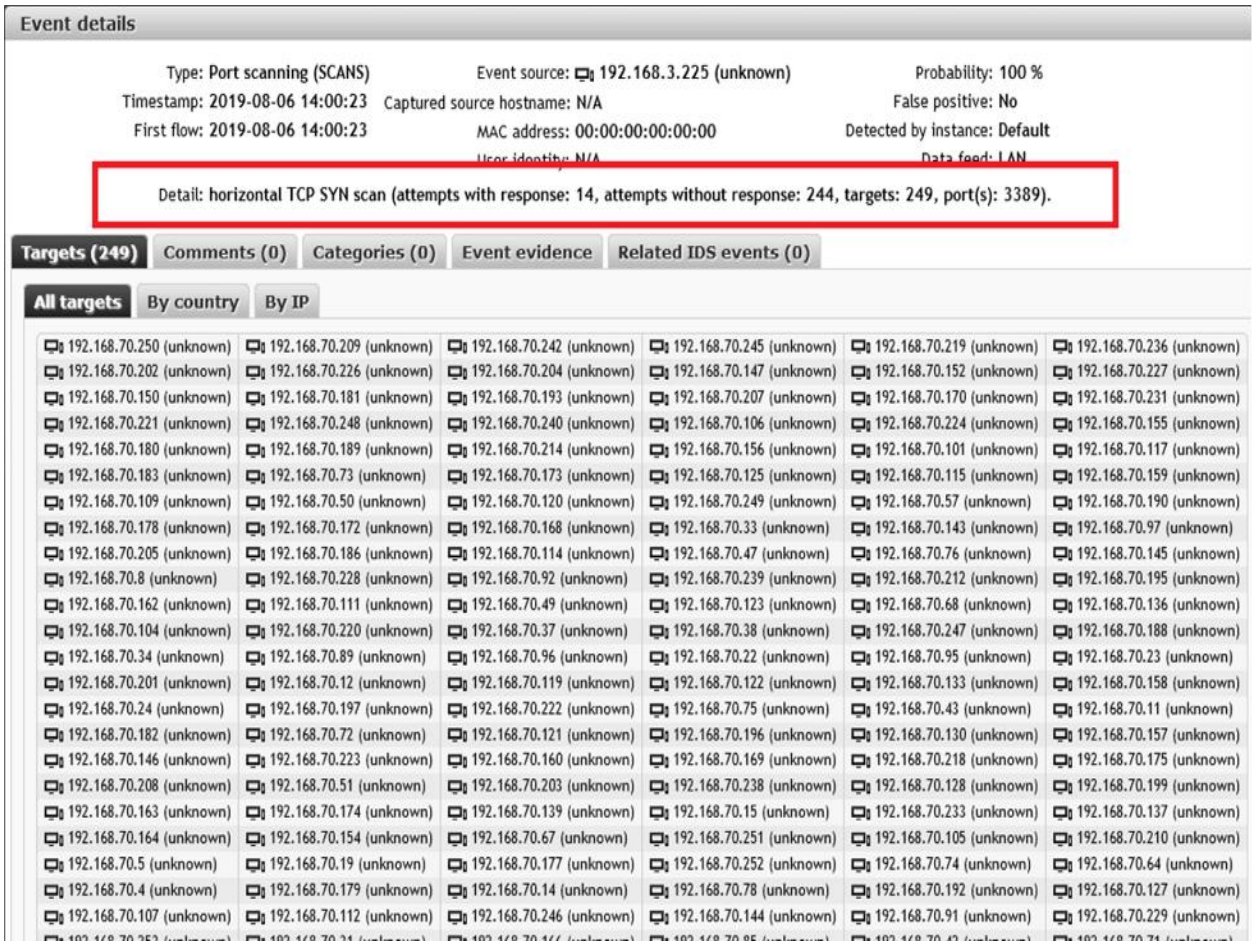


Figure 12

The next recorded incident - host 192.168.3.225 begins a brute force attack on brute-force passwords to the RDP service (port 3389) at previously identified addresses:

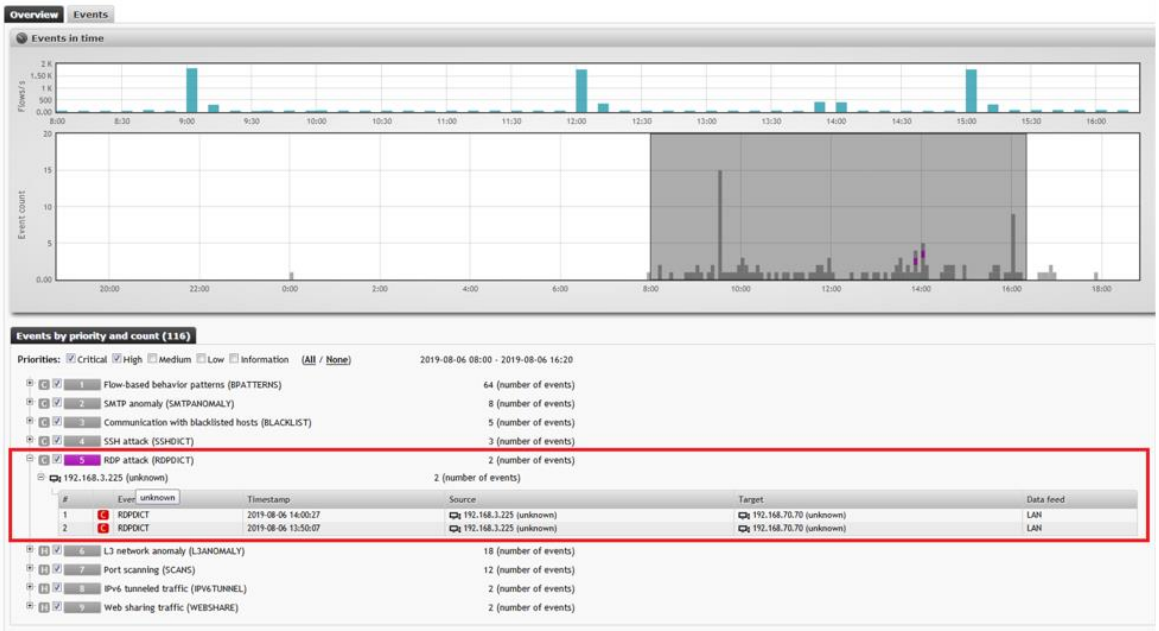


Figure 13

An SMTP issue has been fixed on one of the hacked hosts as a result of the attack. To put it another way, SPAM has begun:

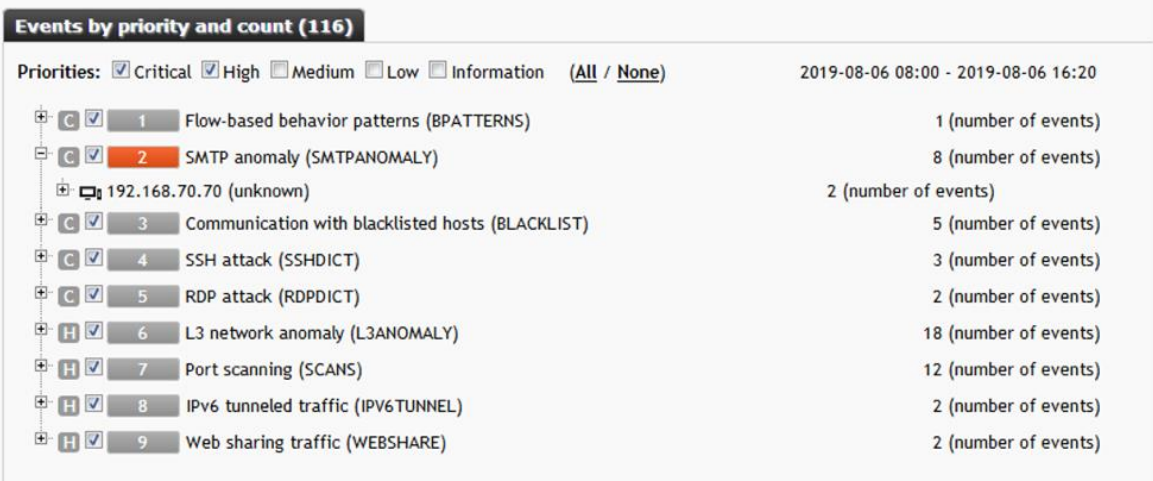


Figure 14

This is a visual illustration of the system's and the Anomaly Detection Security module's capabilities.

Discussion and Conclusion.

Flowmon is a premium level solution for corporate customers:

- due to versatility and compatibility, data collection is available from any sources: network equipment (Cisco, Juniper, HPE, Huawei...) or proprietary probes (Flowmon Probe);
- the scalability capabilities of the solution allow you to increase the functionality of the system by adding new modules, as well as increase productivity thanks to a flexible approach to licensing;
- due to the use of technologies without signature analysis, the system allows detecting even zero-day attacks unknown to antiviruses and IDS/IPS systems;

- due to full "transparency" in terms of the installation and presence of the system on the network, the solution does not affect the operation of other nodes and components of your IT infrastructure;
- Flowmon is the only solution on the market that supports traffic monitoring at speeds up to 100 Gbit/s;
- Flowmon is a solution for networks of any scale;
- the best price / functionality ratio among similar solutions.

This development is a tool that allows to increase fault tolerance and facilitate the administration of automated systems. The consequence of this is a reduction in the maintenance costs of the AU as a whole. In addition, a short-term malfunction of most existing information systems can lead to the loss of important information, significant economic damage, a decrease in the number of customers, etc..

As a result, we get a tool that detects any anomalies in our network and deviations from the characteristic behavior. Here are a couple of examples that the system allows you to detect:

- distribution of new malware on the network that is not detected by antivirus signatures;
- building DNS, ICMP or other tunnels and transmitting data bypassing the firewall;
- the appearance of a new computer on the network, posing as a DHCP and/or DNS server.

REFERENCES

[1] Belov E.B. Fundamentals of information security: textbook. handbook for universities / E.B. Belov, V.P. Los, R.V. Meshcheryakov, A.A. Shelupanov. - M.: Hotline - Tele-com, 2006– - 544 p.

[2] Gaidamakin N.A. Differentiation of access to information in computer systems. - Yekaterinburg: Publishing house of USU, 2003. - 328 p.

[3] Shcheglov A.Yu. Protection of computer information from unauthorized access. - St. Petersburg: Science and Technology, 2004. - 384 p.

[4] A. S. Katasev, D. V. Kataseva, A. P. Kirpichnikov, Neural diagnosis of anomaly networks activities, Bulletin of the Technological University. 2015. Vol.18, No 6.

[5] Garfinkel S. Practical security of Unix and the Internet, O'Reilly / S. Garfinkel, A. Schwartz, G. Spafford. ISBN 0-596-00323-4. - 2003– - 984 p.

[6] Hoglund G. The use of software. How to crack the code / G.Hoglund, G. McGraw, A. Wesley. - 2004– - 512 p.

[7] https://www.slideshare.net/CiscoRu/ss-47809598

[8] https://habr.com/ru/company/tssolution/blog/463625/

UDC.656.25(075).

S. Kanibek[a], D. Sagmwdinov[b], K. Synbat[c]
Academy of Logistics and Transport, Almaty, Kazakhstan
[a]d.sagmedinov@alt.edu.kz, [b]zhanmuratov@gmail.com, [c]simbat.alibek12@mail.ru

DEVELOPMENT OF THE BASE STATION COVERAGE MODEL OF THE RAILWAY TRUNK CHANNEL

Abstract. This article considers methods of data transmission over the radio channel for information security, the issues of communication of the radio locking center and the TETRA switching center, linking the radio locking center with electrical interlocking systems. A model