

УДК 004

Kolodka A.¹, Snizhnoi G.²

¹ Consultant “Easy Online Solutions” LTD

² Doctor of Technical Science, head of chairs MNE NU “Zaporizhzhia Polytechnic”

METHODS FOR REPELLING DDOS ATTACKS AND NETWORK OPTIMIZATION UNDER HIGH LOADS

With the constantly growing volume of transmitted information in the world, the problem of its high-speed transmission is acute. Network devices have both software and hardware limitations for transmitting network traffic. Quite often, these limits can cause collisions and interfere with each other. In order to avoid such situations, it is required to clearly understand the network construction model, the type of transmitted data, the data transfer rate. Correct determination of the parameters of incoming and outgoing data streams allows you to optimize the software and hardware by changing the parameters of their operation by configuring the limits and buffering parameters.

Consider a data center with an edge router connected to the Internet at a bandwidth speed of 100 Gbps. To analyze data flows, we will use ElasticFlow software, which consists of a bundle of Elasticsearch, LogStash, and Kibana packets. This complex allows you to fully assess the load on any flow or on the total flow interactively or over a period of time. Also, these complex can be attached to the Grafana or other data collection tool to provide a wider list of alerting and informing options.

During this software package usage, the analysis showed suspicious data streams transmitted over UDP protocol for the NTP service and it exceeds more than 6Gbps of bandwidth speed usage. Although this protocol is used only for time synchronization on devices and the bandwidth speed as well as the amount of such data should be several times less. With the help of this software package, we make a selection by the addresses of devices that produce illegitimate data transfer and block the streams with firewall rules. Thus, we eliminate the problem caused by the DDOS attack.

However, for a legitimate data stream, some devices may be overloaded with the number of interrupts due to the fragmentation of data packets. This problem can cause a denial of access to the device and its complete blocking. So we've used the provided software package to analyze the packet fragmentation for different protocols and data sources. To resolve this issue, we've re-configured the device operating system kernels to enable bundling of multiple packages - pooling, before making a request to the kernel. This prevents CPU time over-usage for simple data translation requests.

Applying such an analysis and network optimization, it was possible to eliminate the illegitimate data flow of 6 Gbps, which is 6 % of whole data traffic, which can be seen on the incoming (fig. 1) and outgoing (fig. 2) bandwidth speed graphs at the time between 11:00 and 11:30. Also, such analysis reduced the load on devices by 50-70 %.

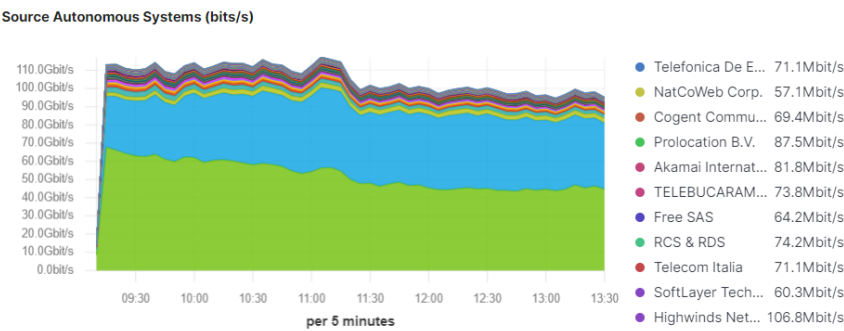


Figure 1 – Incoming data bandwidth utilization

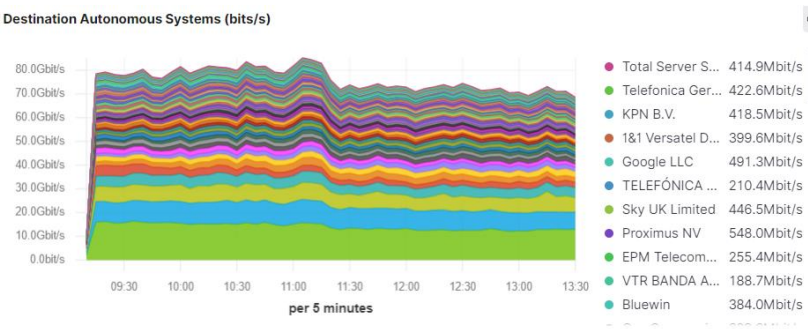


Figure 2 – Outgoing data bandwidth utilization

Such data flow analysis systems make it possible to quickly identify and eliminate network attacks and collisions. Data collection can be performed from multiple sources and aggregated into a single database, which allows to consolidate and visualize the data flow, as well as configure the system of notifications, warnings, and alerts about network events at all levels of the OSI model.