Development of module for neural network identification of attacks on applications and services in multi-cloud platforms

D I Parfenov, I P Bolodurina

Orenburg State University, 13, Pobedy Av., Orenburg, 460018, Russia

E-mail: parfenovdi@mail.ru

Abstract. The article presents the results of developing an approach to detecting and protecting against network attacks on the corporate infrastructure deployed on the multi-cloud platform. The proposed approach is based on the combination of two technologies: a software-configurable network and virtualization of network functions. The approach for searching for anomalous traffic is to use a hybrid neural network consisting of a self-organizing Kohonen network and a multilayer perceptron. The study of the work of the prototype of the system for detecting attacks, the method of forming a learning sample, and the course of experiments are described. The study showed that using the proposed approach makes it possible to increase the effectiveness of the obfuscation of various types of attacks and at the same time does not reduce the performance of the network.

1. Introduction

Today, there is a rapid development of global and local networks. The actual problem of modern networks is the annual growth of convergent traffic. According to the analytical data of the leading network equipment vendors such as Cisco and Huawei, the volume of traffic is increasing annually by 20-35% [1]. This is primarily due to an increase in the number of users and the growth of the services they use. However, avalanche-like traffic growth is mainly due to cyber attacks conducted on these services. Assessing the vector of attacks on the infrastructure that supports the operation of information systems in large companies, it can be concluded that the legitimate users are aimed at restricting access to the main attack to key applications (35%), a violation of the process equipment (35%), destruction or theft of confidential data (23%).

If one considers the actual list of cyber threats in more detail, the list of attacks carried out on the corporate network can be divided into four basic groups [5]. The first group includes attacks such as denial of service for a DDoS attack. The main purpose of such attacks is to restrict legitimate users access to applications and services. The main complexity of protection from this type of attack is to identify and filter malicious traffic in the general flow of requests.

The second place in the ranking of the most common attacks is Remote to Local (User) attack (R2L). A remote to local (R2L) attack is a class of attacks where an attacker sends packets to a machine over network, then exploits the machine’s vulnerability to gain illegally local access to a machine [7]. The problem of protection against such attacks is the need to install a software update designed to fix identified vulnerabilities. In a large corporate network with a variety of heterogeneous devices, this can lead to unpredictable consequences. This is primarily due to the fact that update can cause a stop of the corporate services and applications. To install critical updates, it is necessary to
plan a break in the least busy hours of services and applications. However, such approach to protection is not always acceptable not only in terms of time spent, but in terms of security.

The next group of attacks is User to root (U2R) attack. U2R attacks is a class of attacks where an attacker starts with access to a normal user account on the system and is able to exploit vulnerability to gain root access to the system. The problems of protection against this type of attack are similar to those listed in R2L [8].

The fourth place is occupied by Probing attack. Probing is an attack in which the hacker scans a machine or a networking device in order to determine weaknesses or vulnerabilities that may later be exploited so as to compromise the system [6].

Corporate users use various methods to protect against the listed threats to cyber security. One of the solutions used to protect against undesirable effects on the corporate network infrastructure is the use of modern hardware equipment. The basic set usually includes firewalls, DLP systems and IDS / IPS analyzing the incoming and circulating traffic in the network. However, the cost of such hardware solutions is quite high [10]. Corporate users prefer to take cyber security facilities for rent. To do this, corporate information resources are located in data centers.

In one data center, computing capacities usually rent several companies at once. In this case, each of these companies expects full satisfaction of their requirements from the provider of data center services. In turn, the task of data center operators is to meet the requirements of corporate users to ensure the security of leased infrastructure from external influences, as well as to ensure quality of service (QoS) according to the SLA. However, with the given amount of data entering the data center and the number of users working simultaneously with the same equipment, there is a risk of errors in the configuration of network equipment. This can lead to negative consequences for the data center of the operator, as well as for corporate clients it serves. Therefore, operators of data centers prefer to isolate the infrastructure of corporate users with using multi-cloud platforms. This approach allows to guarantee the required amount of consumed resources and to ensure the proper level of quality of service. However, this approach is not without flaws. When using architecture based on a multi-platform platform, corporate users are deprived of the opportunity to independently configure the network infrastructure and apply non-standard solutions to ensure the security of their own information systems.

In this article, the authors propose some solutions that are responsible for filtering and searching for malicious traffic flows in a corporate infrastructure deployed on the multi-cloud platform.

2. Related work

Today there are many approaches to ensuring the security of applications and services, including the use of technologies for software-defined networks (SDN) and multi-cloud platforms.

So one of the solutions used to protect against denial of service attacks (DOS/DDOS) is the use of load balancing using virtualization tools based on multi-cloud platforms. The proposed solution allows us to scale the instances of applications and services and redistribute the load to free computing nodes. A significant disadvantage of this solution is the high cost of computing resources during the attack on the services. In addition, during times of denial of service attacks, there is a significant violation of QoS policies. This is primarily due to the mechanism of protection. Service providers, who prepare protection against this type of attack, forward all traffic to its own network. This network is used as a filter for identifying legitimate traffic. In this regard, the response time of applications and services is quite strong. The use of such approach is rather a preventive measure aimed at ensuring the operation of services under a high load, rather than protection from specialized attacks. Moreover, this approach does not allow providing protection from other classes of attacks.

The main goal of DOS/DDOS attacks can be not only applications and services, but the data center infrastructure objects that provide network operation. One popular way of disabling the network infrastructure is to attack the controller of a software-defined network. To conduct such attacks, cyber-attackers do not need to investigate vulnerabilities in specific services or applications. As a rule, to limit the access of legitimate users, it is enough to overload the controlling controller with redundant
traffic. To protect against such attacks, scientists from Shiraz University of Technology developed the SLICOTS framework. The proposed solution allows protection against TCP SYN attacks on the SDN network controller. The authors of the study prove the effectiveness of the proposed solution by reducing the response time in the network by 50%, which makes it possible to provide the required QoS. A significant drawback of SLICOTS is the high resource intensity of the solution itself. With limited functionality, it creates significant overhead for infrastructure.

To solve this problem, Ali Hussein in [4] proposed a security architecture based on SDN. The solution is based on the introduction of a security plane between the switches and the network controller. This allows the controller to block attacks in real time without having to process most of the traffic. However, this approach allows one to monitor traffic only within the network and does not provide control of the network perimeter.

To ensure network security on the boundaries of the network, most solutions use the Firewall. But this solution has several drawbacks. In the queue, it significantly reduces the performance of the input link. Secondly, filtering lists have a serious vulnerability in their implementation. All filtering rules on the Firewall are processed sequentially. This vulnerability manifests itself when one accumulates enough active rules in the filter list. The implementation of the vulnerability is possible when attacks are directed at the lower stages of the filtering base. The consequence of implementing an attack on the lower stages of the rules is the long passage of the filter list from the beginning to rule M, which leads to a significant increase in the maintenance time and the increase in the costs of the hardware resources. The exploitation of this vulnerability significantly improves the effectiveness of denial of service attacks: to reach the goal when attacking the lower levels of the rules base, an attacker will need significantly less resources than when attacking a random rule in the list [2]. To solve this problem, researchers are offered various mechanisms for organizing the Firewall, but not one of them does not allow efficient scaling of resources without loss of performance and quality of filtering malicious traffic.

A common disadvantage inherent in all of these approaches to protecting the network from cyber attacks is the lack of functionality for rapid software update of devices, which in turn leaves vulnerabilities in the security system.

Thus, a review of research on the research topic shows that different approaches to the detection of network attacks are currently being used, but in practice these approaches are not always ineffective. For this reason, the authors proposed a solution that would eliminate the listed shortcomings and increase the efficiency of protecting the corporate network.

3. Materials and methods

In the framework of this study, the authors proposed an approach based on the use of a group of components that are the basis for a virtual data center. The developed solution is built using the hybrid synthesis of two breakthrough technologies: software-defined networks and virtualization of network functions. The first component (SDN) allows isolating and implementing efficient traffic flow control based on methods and dynamic routing algorithms [3, 9]. The second component (VNF) allows carrying out a set of activities aimed at monitoring and timely updating of protocols and means of ensuring cyber security on all devices (objects) involved in the operation of a multi-cloud corporate infrastructure.

To improve the quality of services and the security of multi-cloud platforms, one needs to detail the main object, which should give a prediction about the architecture of the network of the virtual data center. The network of the virtual data center can be described as:

\[ VDC_{\text{network}} = (V, e, u, FE), \]

where \( V \) – vertices of the graph (network nodes), \( e \) – arc graphs (network connections), \( FE : E(G) \rightarrow R^* \) - flow of requests in a SDN network; \( u : E(G) \rightarrow R^* \) - the cost of implementing a network connection in the SDN network.
To maintain the required quality of service (QoS) and a given level of uninterrupted operation, let us write the balance equations:

\[ ex_f(u,v) := \sum_{e \in \delta(U,V)} FE(e) - \sum_{e \in \delta(V,U)} FE(e), \forall (u,v) \in E(G). \]  

(2)

The presented description is necessary for transition to modeling at the level of flows of transmitted and analyzed data. Each record of the flow \( FE_{kij}(t) \) is dynamic and changes at times \( t \). Each thread has a set of characteristics that uniquely identify it. In the traffic management system, the flow can be represent as form:

\[ FE_{kij} = (\text{Match}_{kij}, \text{Actions}_{kij}, \text{TimeOut}_{kij}, \text{Flow}_{kij}, \text{CNT}_{kij}(t)), \]  

(3)

where \( \text{Match}_{kij} \) this is a set of fields to check for matches with the headers of the package; \( \text{Actions}_{kij} \) – a set of actions performed on the package, if its headers match \( \text{Match}_{kij} \); \( \text{TimeOut}_{kij} \) – time of fixing the flow in the system; \( \text{Flow}_{kij} \) – the thread to which this OpenFlow rule applies; \( \text{Counters} \) – statistical counters OpenFlow.

In this case, for more efficient traffic analysis, as a rule a signature approach, is used in networks. Within the framework of this research, this approach is supplemented by methods of data mining, which allow reducing the set of characteristics, which significantly speeds up the processing of information. This is important when analyzing Big data flows that occur in networks of virtual data centers because of multiple intersections of communication channels. The flow analysis scheme at the point of connection to the network on the node of the data center can be formalized as follows:

\[ \text{Analyzer}_{ki} = (\text{Node}_{ki}, \text{CurFlows}_{ki}(t), \text{SuspiciousFlows}_{ki}(t)), \]  

(4)

where \( \text{Node}_{ki} \) – the network node on which the signature traffic analyzer works, \( \text{CurFlows}_{ki}(t) = \{\text{CurrentFlows}_{kij}\} \) and \( \text{SuspiciousFlows}_{ki}(t) = \{\text{SuspiciousFlow}_{kij}\} \) – respectively, the set of current and the set of suspicious flows detected by the analyzer at time \( t \).

For the model presented, firewall rules have been developed separately for the L2 and L3-L4 levels of the OSI model. All rules have two parts - the headers that identify the packages, and the action. The headers for L2-level rules include the source port of the packet, the source switch, the MAC addresses of the sender and the receiver of the packet, the type of protocol, etc. The headings for the L3-L4 layer rules contain the IP addresses and ports of the source and destination of the packet, the type of the encapsulated protocol, etc. Possible actions are the removal or resolution of the package.

Such rules can be combined into chains if necessary. Each chain is an ordered list of rules that has an identifier. The entire chain of rules is checked in order of priority, until there is a rule suitable for the parsed packet. In this case, the action specified in this rule is executed, and the subsequent execution of the chain is terminated. In order to transfer the rule to another chain, the corresponding action with its identifier can be specified. The originality of this model lies in the fact that within the rules all OpenFlow headers are supported up to version 1.5, inclusive.

4. Hybrid neural network model for detection anomalous traffic

To search for anomalous traffic, it is proposed to use a hybrid neural network consisting of a self-organizing network of self-organizing map (SOM) and a multilayer perceptron. The architecture of the projected network is shown in Figure 1.
Figure 1. Hybrid neural network model for detection anomalous traffic

By applying the Kohonen map, clustering of network events occurs in the nodes of the matrix, in which events of similar numeric symbols will be grouped. In fact, individual nodes will represent certain attack scenarios. The input vector for the SOM contains the following components: $x_1$ - destination IP address, $x_2$ - source IP address, $x_3$ - destination TCP/UDP port, $x_4$ - source TCP/UDP port, $x_5$ - duration, $x_6$ - number of packets, $x_7$ - number of bytes, $x_8$ - single rate, $x_9$ - rate to the host, $x_{10}$ - multiple rate with the same source host, $x_{11}$ - rate of connections on the same port to a host from other nodes.

After clustering the data on the SOM-based data, packet header data and grouping information are fed to the input of a multi-layer perceptron trained to recognize abnormal traffic, but with the event information in mind, i.e. package belongings to a certain group. This allows one not only to detect anomalies in single packets, but also to reveal the belonging of the packet to a time-based attack.

The input vector format for the multi-layer perceptron is as follows. The input sample is divided into disjoint parts with a length of 150 packets. All packages pass through the Kohonen network. The packet is associated with the cluster number (the number of the winner’s neuron). Clusters are being consolidated - 5 neighboring ones are united together. It turns out 100 enlarged clusters.

By enlarged clusters, a histogram is considered to represent traffic. That is, the first component of the vector is the number of packets that hit the first aggregated cluster (clusters 1-5), and so on. The histogram is normalized, components are reduced to a range of 0-1. After this, the delta between neighboring vectors is calculated.

The proposed method takes into account two types of traffic activity. When analyzing individual cluster nodes, individual attack scenarios are identified. In addition, sharp changes in the power of the network stream are analyzed to detect bursts of load. A joint analysis of these two types of events allows one to respond more accurately to the appearance of malicious traffic, while reducing the number of false positives associated with the legal increase in the use of bandwidth.

The created neural network allows one not only to identify anomalies in the network, but to predict their appearance by collecting data from sensors located on the basis of virtual network functions in the multi-cloud environment of the virtual data center. The information obtained is necessary for training and testing of the neural network. The next step is to determine the optimal scheme for rules of attack identification. This will allow one to adjust the input data sets and improve the quality of the
result at the output of the neural network. The final step is testing the system using examples that are
not included in the training sample.

Another advantage of the Kohonen network is the ability to identify new clusters. The trained
network recognizes clusters in training data and assigns all data to one or another cluster. If the
network then meets a data set that is unlike any of the known samples, it will independently identify a
new cluster of elements. This feature is very relevant, because it allows one to protect the architecture
of a virtual data center without actually changing the algorithms for detecting attacks.

5. Simulation results
For carrying out load testing, scenarios of various infrastructure attacks were implemented. To create
test attacks, a test virtual network was created in OpenStack. It includes 4 OpenFlow switches (2 HP
3500yl, 2 Netgear GSM7200), 8 computing nodes (32Gb RAM, 4 cores), 1 server (32Gb RAM, 8
cores) with OpenFlow controller and 1 server (32Gb RAM, 4 cores) for monitoring the function as a
selected fat tree topology with three levels. Routers connected compounds having the speed 1000 Mbit
/s, and the computers are connected to a third level router via the second level network connections at
100 Mbit/s. In this infrastructure was prepared 100 virtual machines (attacking nodes). Also let us
include one node that controls the attack. Let us select random five attacked virtual machines (service
host). Experiments have shown that the maximum performance of the sensor and the collection
module when working in pairs is limited by two factors: the bandwidth of the channel between the
collector and the sensor, and the power of the server on which the collector is located. The data from
the sensor come in the form of UDP packets, the packet contains the maximum information about 30
threads. If the sensor has processed 240,000 streams per second, then it will send 8000 UDP packets of
1506 bytes each, which will create a load of 92 Mbps. The module was tested at values of up to 4
million input flows per second. With an average stream size of 1 Mbyte, the power value of the flows
will be 3900 GB/s. In all experiments, the time delay introduced by the module did not exceed 300 ms.
This delay is sufficient to generate a timely response to malicious traffic. At the moment, the
maximum registered power of DDoS attack is 300 Gbit/s.

6. Conclusion
Experimental studies have shown that the developed prototype of the system allows one not only to
reduce significantly the response time of applications and services in a multi-cloud platform network
while conducting cyber attacks, but also to maintain the specified quality of service at the required
level.

In the future, it is planned to investigate the work of the prototype for resource intensity, as well as
behavior for various types of cyber attacks.

7. Acknowledgments
The study was carried out with the financial support of the RFBR (projects 16-37-60086, 16-07-
01004, 18-07-01446) and the grant from the President of the Russian Federation for state support of
young Russian scientists - candidates of science - (MK-1624.2017.9).

References
[1] Cisco Visual Networking Index: Forecast and Methodology, 2015-2020 Cisco Systems, Inc.,
White
[2] Salah K, Elbadawi E, Boutaba R 2016 Performance Modeling and Analyses of Network
Firewall IEEE Transactions on network and service management 9(1) 12-21
[3] Parfenov D, Bolodurina I 2017 Methods and algorithms optimization of adaptive traffic control
in the virtual data center Proceedings of 2017 International Siberian Conference on Control
and Communications, SIBCON 2017 (Astana, IEEE) pp 1-6
[4] Avinash Kumar, Srinath N K 016 Implementing a firewall functionality for mesh networks
using SDN controller 2016 Proceedings of 2016 International Conference on Computational
Systems and Information Systems for Sustainable Solutions (IEEE) pp 168-173

[5] Lombardo A, Manzalini A, Schembra G, Faraci G, Rametta C, Riccobene V 2015 An Open Framework to Enable NetFATE (Network Functions At The Edge) Proceedings of the 2015 1st IEEE Conference on Network Softwarization (NetSoft) (IEEE) pp 1-6

[6] Nainesh V. Patel, Dr. Narendra M. Patel, Costas Kleopa 2016 OpenAppID – Application Identification Framework Proceedings of 2016 Online International Conference on Green Engineering and Technologies (Coimbatore, IEEE) pp 1-5

[7] Khaled Salah, Prasad Calyam, Raouf Boutaba 2016 Analytical Model for Elastic Scaling of Cloud-based Firewalls IEEE Transactions on Network and Service Management Journal 14(1) 136-146

[8] Mehdi S A, Khalid J, Khayam S A 2011 Revisiting traffic anomaly detection using software defined networking 14th International Symposium Recent Advances in Intrusion Detection (CA, Springer) pp 161-180

[9] Bolodurina I P, Parfenov D I 2017 Models and algorithm of optimization launch and deployment of virtual network functions in the virtual data center Journal of Physics: Conference Series 913(1) 012012

[10] Braga R, Mota E, and Passito A 2010 Lightweight DDoS flooding attack detection using NOX/OpenFlow IEEE 35th Conference on Local Computer Networks (LCN) (IEEE) pp 408-415