UDC 004.056.5
DOI: 10.15587/1729-4061.2021.242993

ANALYSIS OF NETWORK SECURITY ORGANIZATION BASED ON SD-WAN TECHNOLOGY

Gulzinat Ordabayeva
Corresponding author
Senior Teacher
Department of Information Systems
Al-Farabi Kazakh National University
Al-Farabi ave., 71, Almaty, Republic of Kazakhstan, 050040
E-mail: gulzi200988@mail.ru
Abdizhapar Saparbayev
Doctor of Economic Sciences, Professor, Vice-rector for Science
Department of Economics and Business
Kainar Academy
Satpayev str., 7A, Almaty, Republic of Kazakhstan, 050013
Bibinur Kirgizbayeva
PhD, Professor
Department of «IT technology and automation»
Kazakh National Agrarian Research University
Abai ave., 8, Almaty, Republic of Kazakhstan, 050010
Gulzat Dzhsupbekova
PhD
Department of Information Technology
M. Auezov South Kazakhstan*
Nazira Rakhymbek
Senior Teacher
Department of Information Technology
M. Auezov South Kazakhstan*
*State University
Tauke khan ave., 5, Shyment, Republic of Kazakhstan, 160012

A Software-Defined Network (SDN) on a Wide Area Network (WAN) is a computer network that is controlled and created by software.

SD-WAN is an emerging research area that has received a lot of attention from industry and government. This technology offers tremendous opportunities to support the creation of consolidated data centers and secure networks. This is an innovation that allows the network to be monitored and programmed so that it can respond to network events caused by security breaches.

This solution provides network security, offers a single network management console, and provides complete control over the network architecture. Also controls security in the cloud software-defined infrastructure (SDI), such as dynamically changing the network configuration when forwarding packets, blocking, redirecting, changing Media Access Control (MAC) or Internet Protocol (IP) addresses, limiting the packet flow rate etc.

Using SD-WAN technology, it is possible to reduce the cost of dedicated bandwidth channels, achieve a high-quality Virtual Private Network (VPN), and the ability to automatically select a channel for certain channels.

The main advantages of SD-WAN are the management of an unlimited number of devices from a single center, reducing the cost of deploying branch infrastructure.

According to the results of the survey, 7 % of respondents use SD-WAN for security solutions, 14 % at the piloting stage.

As a result of the research, it was revealed that by 2024, to increase the flexibility and support of cloud applications, more than 60 % of SD-WAN customers will implement the SASE (Secure Access Service Edge) architecture, which is 30 % more than in 2020 and the main concept – application security and cloud functions

Keywords: OpenFlow, Software defined wide area network (SD-WAN), architecture, DDoS attack, WAN network

Received date 23.08.2021
Accepted date 17.10.2021
Published date 29.10.2021

***How to Cite**: Ordabayeva, G., Saparbayev, A., Kirgizbayeva, B., Dzhsupbekova, G., Rakhymbek, N. Analysis of network security organization based on sd-wan technology. Eastern-European Journal of Enterprise Technologies, 5 (9 (113)), 56-69. doi: https://doi.org/10.15587/1729-4061.2021.242993*

1. Introduction

Deploying SD WAN is an important task to ensure network management. This technology is becoming popular in the problem of security and in determining the vulnerability of networks.

In the study [1], the possibilities of testing SDN in laboratory conditions on the graphical network simulator Graphical Network Simulator 3 (GNS3) and the advantages of the technology are considered:

– low costs of the functionality of network devices;

– minimal operating costs due to the configuration of services from one point of management;

– high reliability of automation of low-level network management operations;

– centralized network statistics and integration with network analytics.

SD-WAN has grown in popularity over the past few years, but the ideas for this technology have been evolving for twenty years or more. This network separates the control and data layers, controlling the network infrastructure through application programming interfaces (API – Application Programming Interface). The SD-WAN architecture consists of the following components:

1) application layer – intrusion detection and prevention systems (Intrusion Detection System, IDS/Intrusion

Prevention System, IPS), quality of service (QoS) function, other proxy server that determine the behavior of the network are implemented;

2) control level – the main element is the SDN controller, which coordinates the network devices located at the infrastructure level;

3) infrastructure layer – provides processing and forwarding of packets based on the received instructions from the control layer;

4) north APIs – allow applications to use network security services, load balancing, traffic management, quality of service and dynamically configure the network;

5) southern APIs – provide efficient network management;

6) East/West interfaces – provide communication between objects of the control level and exchange of information for processing traffic at the level of infrastructures [2].

An important component of the SD-WAN architecture is a controller that centralizes and monitors the state of the network. Main characteristics of the controller:

– performance – the number of threads processed by the controller per unit of time (threads/s);

– processing time – the amount of time spent by the controller to process the request from the switch (c);

– reliability – the number of failures at a given load profile;

– resource intensity – utilization of the physical server's RAM by the controller, and the load on the processor cores;

– scalability – multithreading support by the controller [3].

SD-WAN is based on the L2/L3 architecture, in which a centralized controller controls the data transfer of a set of distributed switches using a control protocol, for example, OpenFlow. OpenFlow is an open standard that allows developers to work with experimental protocols on a local area network [4–6].

Leading companies are moving to virtualized environments, so network architectures are needed that integrate seamlessly with SD-WAN controllers. One of the leading vendors in the implementation of SD-WAN technology is Juniper Networks (Sunnyvale, USA), which ensures full compatibility of the network infrastructure with existing resources.

SD-WAN is designed to address constraints such as high bandwidth costs, the cost of adding new nodes to the network, the cost of changing security policies, and the lack of network management automation. More than 90 % of enterprises will be using SD-WAN technology by the end of 2023, according to Gartner's analysis.

The developed models of SD-WAN technology indicate the relevance of research on methods of mathematical analysis for the classification of processing time of flows and rational planning of the placement of network elements at the stage of deployment and scaling.

2. Literature review and problem statement

The work [7] analyzed the security of embedded Dynamic Host Configuration Protocol (DHCP) services on three popular SDN controllers: Python and Apache licensed (POX), Open Network Operating System (ONOS) and Floodlight (an Apache licensed, Java-based OpenFlow controller). Vulnerabilities have been identified for overloading controllers when launching denial-of-service attacks. Studying modern methodologies, a DHCP security module on the POX controller was developed, the Dynamic Host Configuration Protocol Guard feature (DHCPguard). According to a study, DHCPguard increased throughput by up to 94 % and reduced CPU utilization by up to 92 %.

SDN provides a flexible way to manage traffic on networks. The deep Reinforcement Learning (DRL) algorithm was used to determine the traffic management method for QoS optimization in hybrid SDN. The simulation results showed that the method of this work can lead to a significant improvement in the optimization of the network QoS performance [8].

SD-WAN for Internet of Things (IoT) devices provides robust security solutions. IoT and SD-WAN edge devices communicate with a common controller. The cloud controller, in turn, informs and allows IoT and SD-WAN edge devices to take action to provide protection, especially at the edge of the enterprise, where large datasets are aggregated [9].

In [10], the Fake Link Layer Discovery Protocol (LLDP) Injection and LLDP replay methods are considered, which are used to create fake links on the controller. The results revealed that the Floodlight controller is vulnerable to attacks based on the use of LLDP. When receiving invalid routes, access to the network is lost and the network performance is underestimated.

In [11], the results of studies of a Distributed Denial of Service (DDoS) attack in SDN, detected using machine learning-based models, are presented. Feature selection methods are shown to be preferable for simplifying models and providing shorter training times. Classification models were built for Support Vector Machine (SVM), Naive Bayes (NB), Artificial neural network (ANN), and K-Nearest Neighbors (KNN). Based on the test results, it was shown that the use of the shell function selection with the KNN classifier allowed to achieve the highest level of accuracy (98.3 %) in detecting DDoS attacks.

[12] describes a security architecture for the Internet of Things (IoT) based on software-defined networks (SDN) and discusses a new architecture of the IoT system. But there are still unresolved issues related to the analysis of the organization of network security based on SD-WAN technology.

The work [13] considers the preservation of the traditional network infrastructure and the gradual upgrade of this infrastructure to a hybrid SDN (hybrid SDN, hSDN). The authors examined hSDN models in the control and data planes, considered the optimization of the control plane of placement, scalability and security issues, privacy, as well as existing vulnerabilities and threats. An option to overcome the corresponding difficulties may be to update the network in both the outdated and SDN settings. This is the approach used in [13], however, modeling tools and public test benches are a completely undisclosed topic. All this suggests that it is advisable to conduct a study on the use of hSDN in 5G mobile networks, cloud and data centers, IoT connectivity, blockchain, SD-WAN and SD-Branch. In addition, network reliability, resiliency and load balancing are also investigated.

Study [14] discusses SD-WAN Flood Tracer to facilitate tracking of DDoS attacks on SD-WAN. Also, to track and prevent other sources of anomalies on legitimate traffic, the tracing scheme is divided into two parts. This scheme effectively monitors internal, external anomalies and prevents damage to communications in the network.

The growth in the volume of network traffic, the need to configure large-scale data transmission networks and the analysis of the above materials suggest that conducting a study on SD-WAN technology is promising.

3. The aim and objectives of research

The aim of research is to analyze the organization of network security based on SD-WAN technology.

To achieve this aim, the following objectives are being solved:

– investigate methods and algorithms for complex protection against threats based on SD-WAN technology;

– create an algorithm that provides protection against threats without sacrificing bandwidth, taking into account the possibility of protection against various types of attacks;

– create a testing algorithm to optimize the network security system based on SD-WAN technology;

– analyze the implementation of SD-WAN technology.

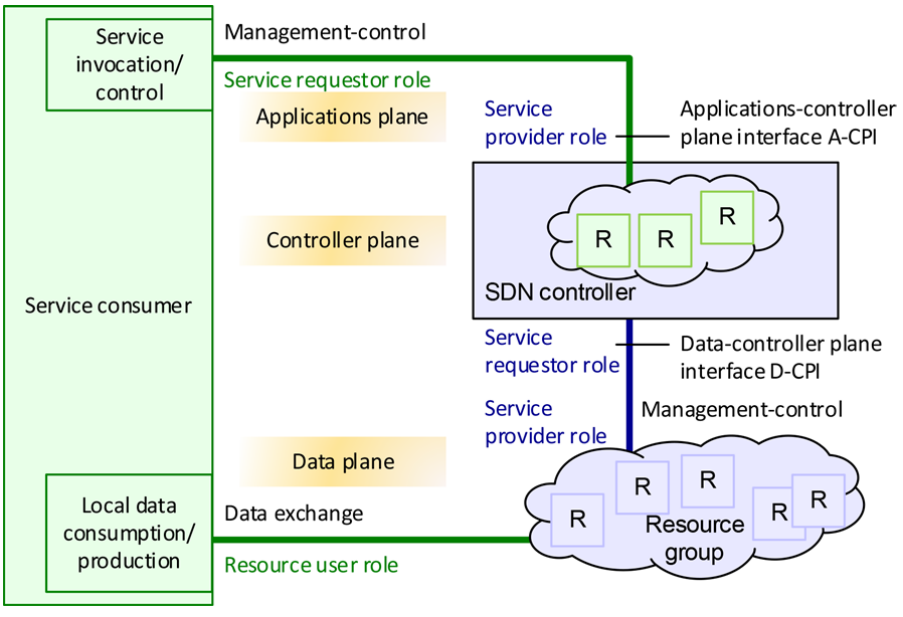


Fig. 1. Basic Service Model SD-WAN [16]

4. Materials and methods of research

The SD-WAN architecture consists of the following planes: data plane, control plane and application. The transmitted data packet is processed in the control plane of the router and goes to the second level. The packet travels along this route to the output port. All operations performed on packet transmission are embedded in the router [15].

The study [16] shows the basic model of SD-WAN service using the D-CPI (Data-Control Plane Interface) interface, the application and control plane – the A-CPI (Application-Control Plane Interface) interface (Fig. 1).

SD-WAN is an integral part of cloud services because it provides flexible management capabilities for monitoring and analyzing network traffic using programmable objects. The main vulnerability of SD-WAN is a distributed denial of service (DDoS) attack. The work [17] proposes a scheme for detecting and protecting DDoS attacks using time series analysis for SD-WAN (Fig. 2). The obtained experimental result showed that the obtained algorithm has a high detection rate and a low false alarm.

In [18], the main design principle of the proposed method is to extract embedded OpenFlow messages in SDN to represent the state of the network and further detect the network anomaly. This method does not need to collect and add additional messages from the core switches. The results of attacks assessment (DDoS, Worm, Port Scan) show that the proposed method for detecting network anomalies can provide high detection accuracy and reduce SDN controller overhead (Fig. 3).

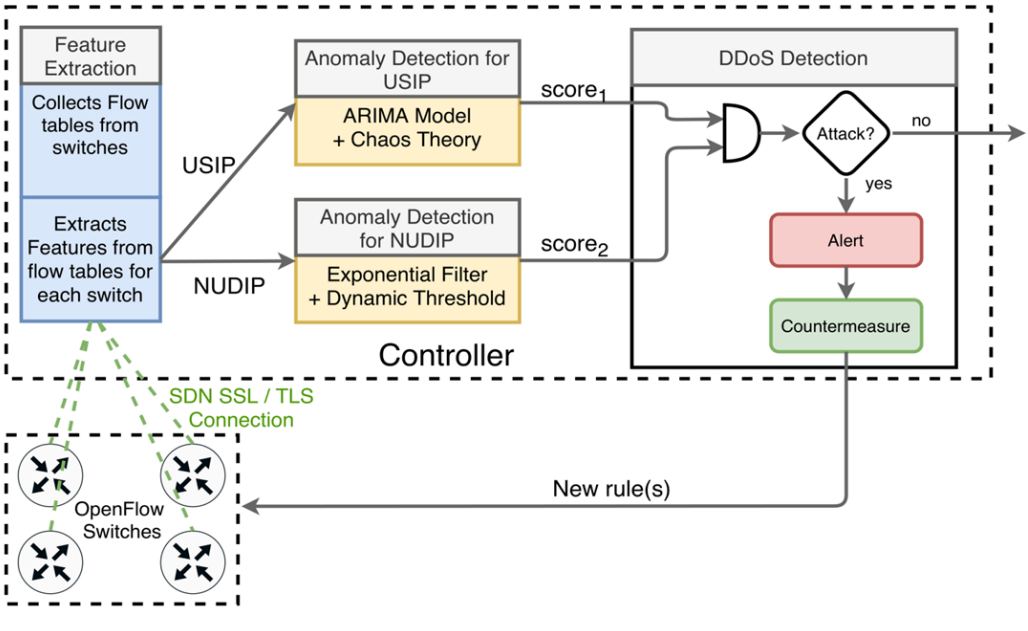
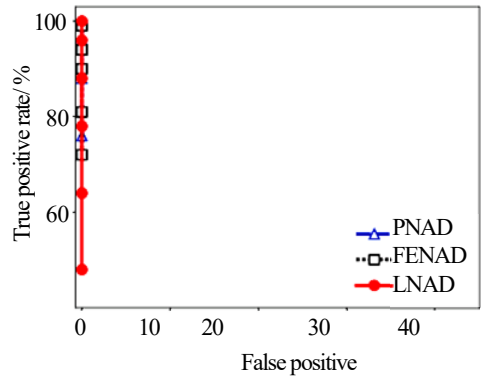


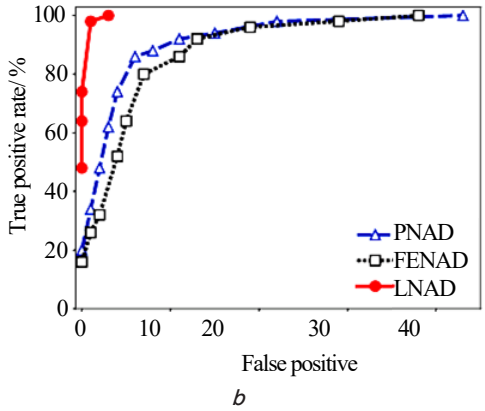
Fig. 2. Proposed DDoS detection and protection model for SDN [17]

One of the areas of SDN security is the use of blockchain for solving forensic problems. Blockchain is a distributed peer-to-peer network that can be used in SDN-based Internet of Things (IoT) environments for security. In [19], event logs are stored in the blockchain of the SDN-IoT architecture. Based on the results of the evaluation, the performance gains were derived from latency caused by the increase in the number of devices and requests (Fig. 4).

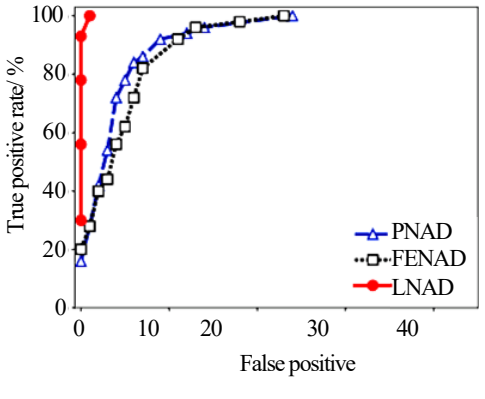
Comparison of latencies shows that Forensic SDN-IoT has the lowest latency, SDN-Fog latency variation is 0.2 milliseconds. The latency value gradually increases as the number of devices increases.



a

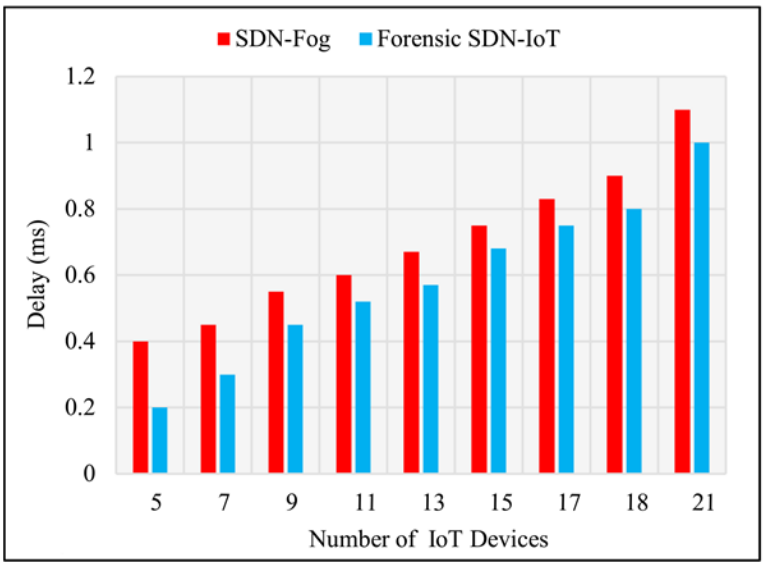


b

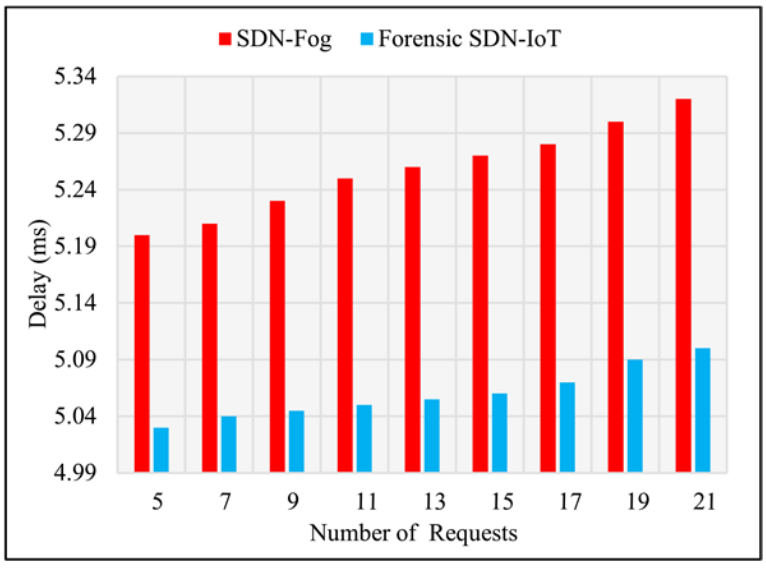


c

Fig. 3. Results of attacks assessment: *a* – DDoS; *b* – Worm; *c* – Port Scan [18]



a



b

Fig. 4. The results of the delay: *a* – an increase in the number of devices; *b* – an increase in the number of requests [19]

5. Results of the study of the SD-WAN technology testing algorithm

5. 1. Research of methods and algorithms for complex protection against threats based on SD-WAN technology

The Open Network Foundation (ONF), a nonprofit organization, has developed a standards compliance certification program to advance the SDN vision. The main goal of SDN is to provide open software development interfaces for controlling the flow of network traffic with the ability to check and modify the network (Fig. 5) [20].

SDN has been researched in the field of road engineering and the following benefits have been identified:

– a global controller that has an idea of the topology and state of the network, as well as the requirements for applications;

– programmability – the data plane can be programmed to improve the allocation of network resources;

– openness – the controller and forwarding devices do not depend on the device suppliers (Fig. 6) [21].

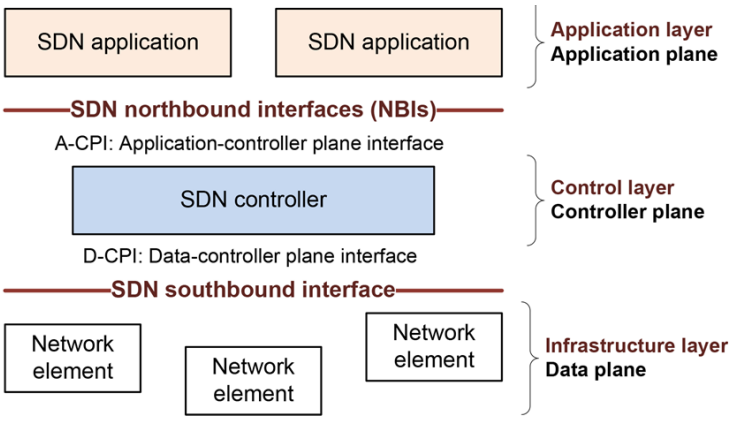


Fig. 5. The main components of the Software-Defined Network (SDN) [20]

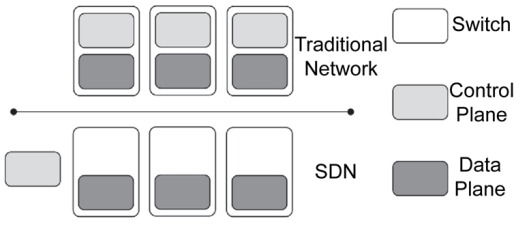


Fig. 6. Deployment of control planes and data transmission in traditional networks and SDN [21]

In the study [22], the DELTA tool is proposed for disclosing SDN vulnerabilities. Based on the testing results, the authors identified 26 known attack scenarios on SDN controllers, as well as 9 new attacks for SDN applications.

The work [23] examines the development of SDN, as well as the introduction of this technology over the years in companies – Google, Cisco (Table 1).

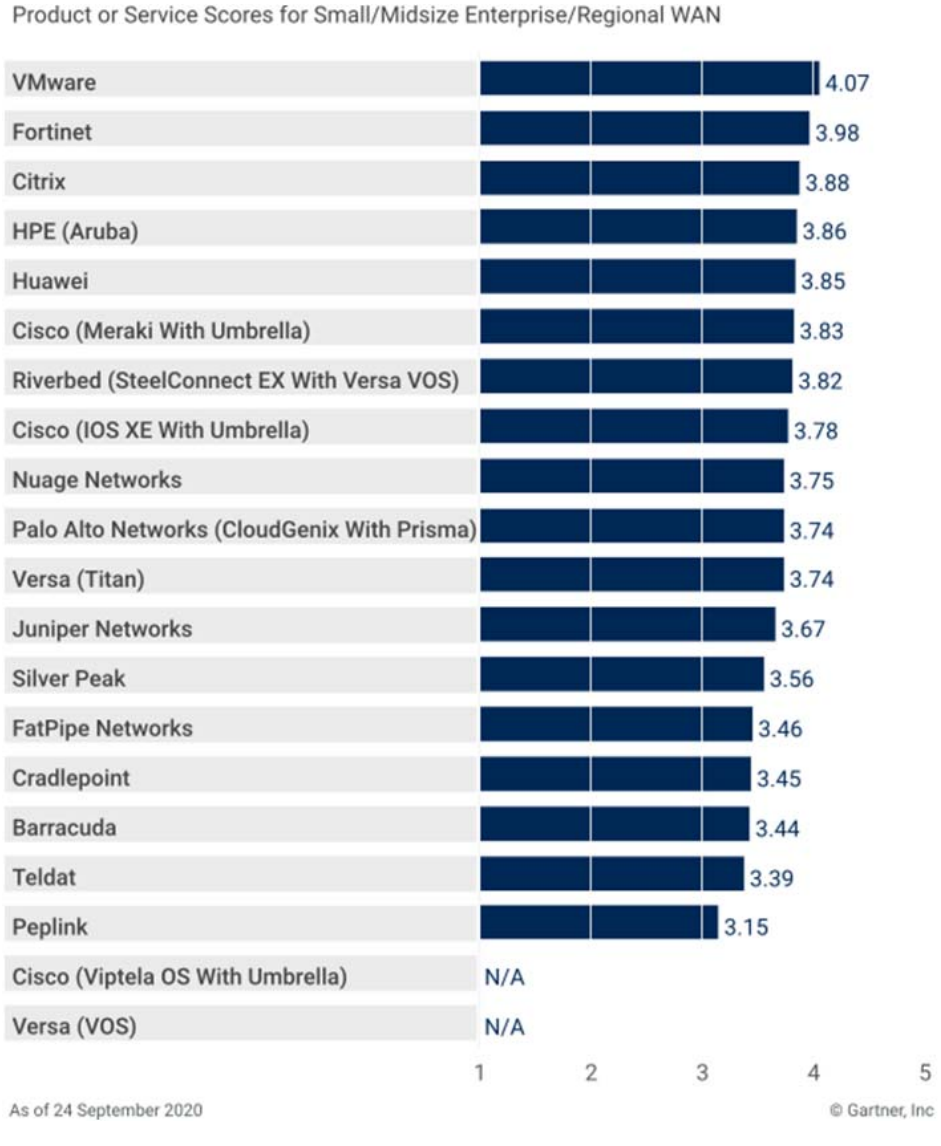


Fig. 7. SD-WAN Market [24]

Table 1

SDN development [23]

Years	Technology	Description
2011	SDN	Movement to separate control and forwarding planes to drive innovation
2012	OPEN FLOW	The first standard interface for separating the network and data control layers.
2014	ONOS	Leading Open Source SDN Controller for Operators
2017	CORD	Edge Cloud Solution: 70 % of carriers plan to deploy CORD to transform their networks

Gartner estimates that there are about 80 vendors providing technology solutions based on SD-WAN (Fig. 7) [24].

According to Gartner researchers, the main leaders of SD-WAN are VMware (Palo Alto, USA), Fortinet (Sunnyvale, USA), Citrix (Fort Lauderdale, USA), HPE (Aruba) (Sunnyvale, USA), Huawei (Shenzhen, China) and others. SD-WAN product differentiation is based on security, application performance optimization and cloud functions.

In a study [25], to achieve robustness and low cost in controllers, RetroFlow is proposed, which maintains flow programmability in the event of failures. Simulations show that RetroFlow reduces communication costs by up to 52.6 % during moderate controller failure. Also, it recovers 90 % of the traffic from standalone switches, reducing costs by up to 61.2 % in the event of a severe controller failure.

Switches with OpenFlow support provide SNMP protocol operation and also support local controller operation.

The following information is defined for routing and network management:

– the number of packets passed through the port;
– the number of bytes transmitted through the port;
– average speed in packets/s;
– average speed in bytes/s;
– load of the processor and memory of the switch;
– port queue lengths [26].

Calculating the average time between packets is needed for routing and network management:

$$\overline{\tau} = \frac{t}{\overline{N}}, \tag{1}$$

where t – observation time; $\overline{N}$ – average number of packages.

Calculating variance for the distribution of time between packets:

$$D_{\tau} = D_N \cdot \frac{\overline{\tau^3}}{t}. \tag{2}$$

Using the above formulas, the number of packets per stream is calculated accurately, but according to manufacturers, it can differ from reality by up to 20 %.

Research data on SD-WAN technology methods and algorithms improves performance that accelerates security and network connectivity tasks. The cost-effectiveness of SD-WAN technologies is a key driver for the development of the network structure and provides a quick return on investment.

5. 2. Development of an algorithm for throughput, taking into account the possibility of protection against various types of attacks

The formulas of mathematical statistics determine the characteristics of time intervals. In the study [26], statistics up to the third order were used, which allow one to judge the nature of the distribution of intervals.

The calculation of the average value of the packet interval is carried out according to the formula:

$$\overline{\tau} = \frac{1}{N}\sum_{k=0}^{N}\left(t_{k+1} - t_k\right), \tag{3}$$

where, t_k – time of packet arrival, N – the number of analyzed intervals.

The sample variance is:

$$D_{\text{в}} = \overline{t^2} - \overline{\tau^2}, \tag{4}$$

where $\overline{t^2}$ – the second initial moment.

$$\overline{t^2} = \frac{1}{N}\sum_{k=0}^{N}\left(t_{k+1} - t_k\right). \tag{5}$$

The coefficient of variation

$$c = \frac{\sigma_{\text{в}}}{\overline{\tau}}, \tag{6}$$

where $\sigma_{\text{в}} = \sqrt{D_{\text{в}}}$.

Asymmetry is calculated:

$$A_s = \frac{\left(\overline{t^3} - 3\overline{t^2}\cdot\overline{\tau} + 2\overline{\tau^3}\right)}{\sigma_{\text{в}}^3}, \tag{7}$$

where $\overline{t^3}$ – the third initial moment

$$\overline{t^3} = \frac{1}{N}\sum_{k=0}^{N}\left(t_{k+1} - t_k\right)^3. \tag{8}$$

Using the above formulas, certain data showed the difference between the analyzed traffic and the Poisson one, since the coefficient of variation c>1, and the asymmetry value A_s>2. Taking into account the ratio of the lengths of the packets of reverse requests (64 bytes) and the main packets (1500 bytes), reverse requests increase the load on the channels by about 4 %.

5. 3. Development of a testing algorithm to optimize the network security system based on SD-WAN technology

In the study [16], applying the Poisson distribution formula over the time interval $[T_0, T_f]=mT_i$ to estimate the probability of k-requests from the switch to the controller, we obtained:

$$P_{d\tau_{NF}} = \frac{\left(\lambda m T_i\right)}{k!} e^{-\lambda m T_i}. \tag{9}$$

The probability of n events on the switch is determined by the formula:

$$P_{dr} = 1 - P_{d\tau_{NF}}. \quad (10)$$

The total delay D, according to [9], is calculated by the formula:

$$D = l \cdot d\tau_{NF} + n \cdot d\tau, \quad (11)$$

where l and n are the number of time intervals.

The network administrator who needs to upgrade the hardware in the SD-WAN can obtain specific packet processing times based on the latency formula.

The use of SD-WAN allows to more efficiently and economically use all available resources of traditional WAN networks within geographically distributed enterprises and optimize business processes. The optimal solution for corporate SD-WANs must align with security priorities.

The main types of security architecture for SD-WAN technologies:

– SD-WAN with built-in firewall;

– firewall with integrated SD-WAN facilities;

– SD-WAN and next generation firewall from independent vendors;

– SD-WAN with cloud security services [27].

To develop a testing algorithm to optimize the network security system based on SD-WAN technology, the Ubuntu distribution kit (South Africa) was chosen as the operating system for the server whose security is required. This operating system belongs to the Linux operating system family and consists of free and open source software. The server has the latest current version of this operating system – Ubuntu 20.04.3 LTS, obtained from the official repository. Recommended system requirements: 2 GHz dual-core processor, 4 GB of system memory, 25 GB of free hard disk space, Internet access (Fig. 8–11).

Based on the data obtained from the access.log files, scripts were created for carrying out load tests, which are reduced copies of real DDoS attacks. Before starting the experiments, the values of the resources used were fixed. At zero load, that is, in the absence of active connections with the server, the processor load was about 0 %, the memory use was 457 Mb, the response time was less than 1 ms. With an average daily load, the resource utilization was: processor – 31 %, RAM – 514 Mb, response time – less than 1 ms.

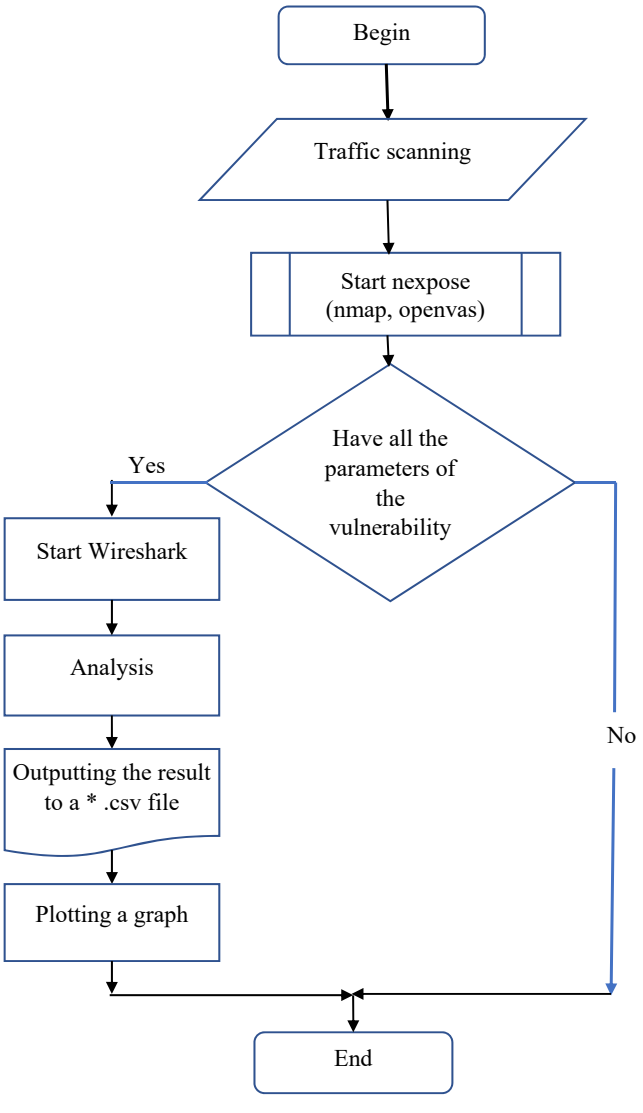


Fig. 8. Testing algorithm

```
[111]
import pandas as pd
import numpy as np
import matplotlib.pyplot as plt
import math

[121]
df = pd.read_csv('capture.csv')
df
```

	No.	Time	Source	Destination	Protocol	Length	Info
0	1	0.000000	HewlettP_c1:ad:e1	HewlettP_09:13:a6	IEEE802a	60	OUI 08:00:09 (Hewlett Packard), PID 0x0003
1	2	0.808452	desktop-2nqkmiq.kaznitu.kz	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
2	3	1.322187	HOME-PC.local	dc1.kaznitu.kz	DNS	83	Standard query 0xf4f0 PTR 80.20.0.10.in-addr.arpa
3	4	1.322679	HOME-PC.local	dc1.kaznitu.kz	DNS	88	Standard query 0x6cf3 PTR 250.255.255.239.in-a...
4	5	1.323119	dc1.kaznitu.kz	HOME-PC.local	DNS	123	Standard query response 0xf4f0 PTR 80.20.0.10....
...	...	...	...	...	...	...	...
82594	82595	598.218695	16.149.211.35.bc.googleusercontent.com	HOME-PC.local	TCP	60	443 > 50005 [ACK] Seq=2945 Ack=4455 Win=729 ...
82595	82596	598.321019	HOME-PC.local	dc1.kaznitu.kz	DNS	84	Standard query 0x7a8b PTR 76.125.9.37.in-addr....
82596	82597	598.467481	dc1.kaznitu.kz	HOME-PC.local	DNS	123	Standard query response 0x7a8b PTR 76.125.9.37...
82597	82598	599.175858	HOME-PC.local	r4.sn-35153iuxa-unxd.googlevideo.com	TCP	55	[TCP Keep-Alive] 51125 > 443 [ACK] Seq=6924 ...
82598	82599	599.191782	r4.sn-35153iuxa-unxd.googlevideo.com	HOME-PC.local	TCP	66	[TCP Keep-Alive ACK] 443 > 51125 [ACK] Seq=2...

Fig. 9. Output of the result

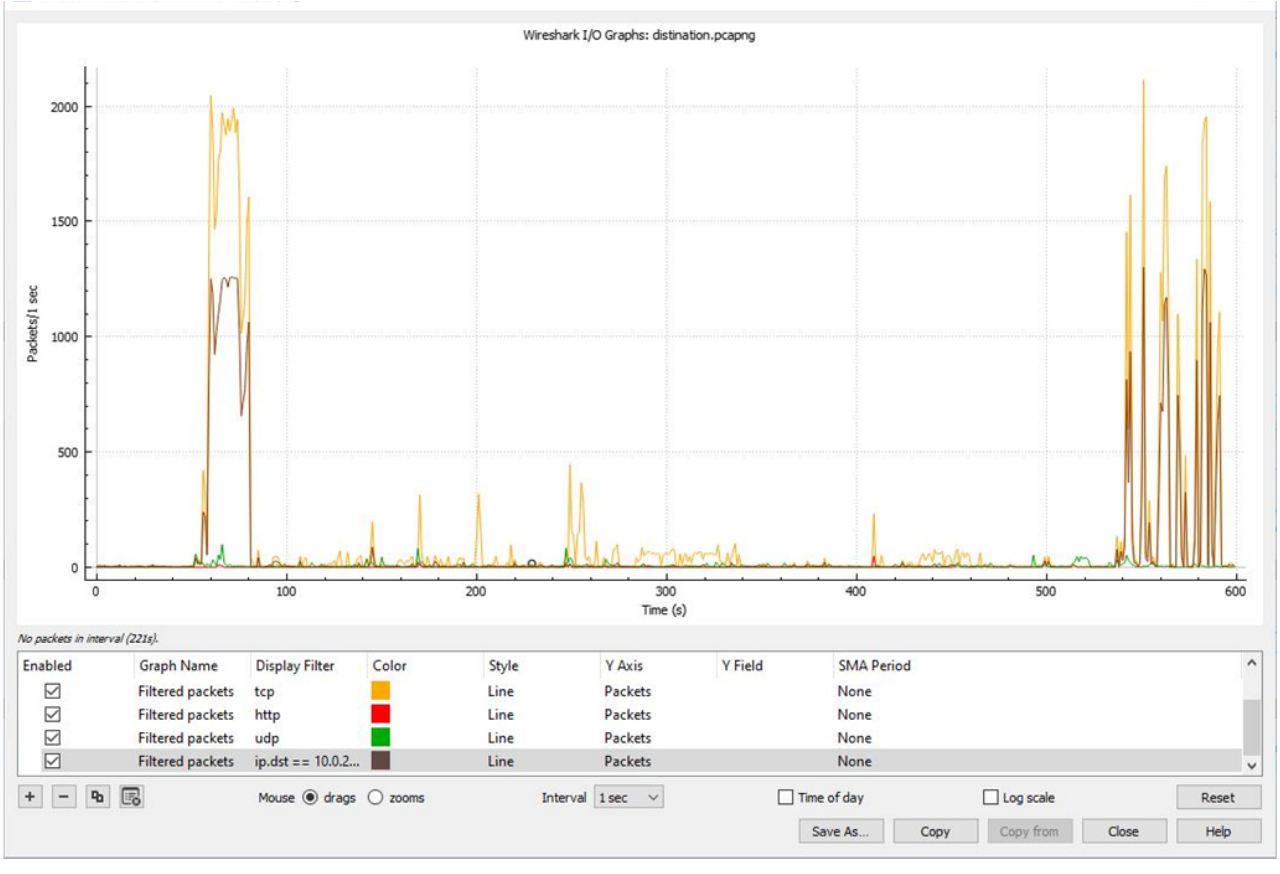


Fig. 10. Length of incoming packets generated by Wireshark

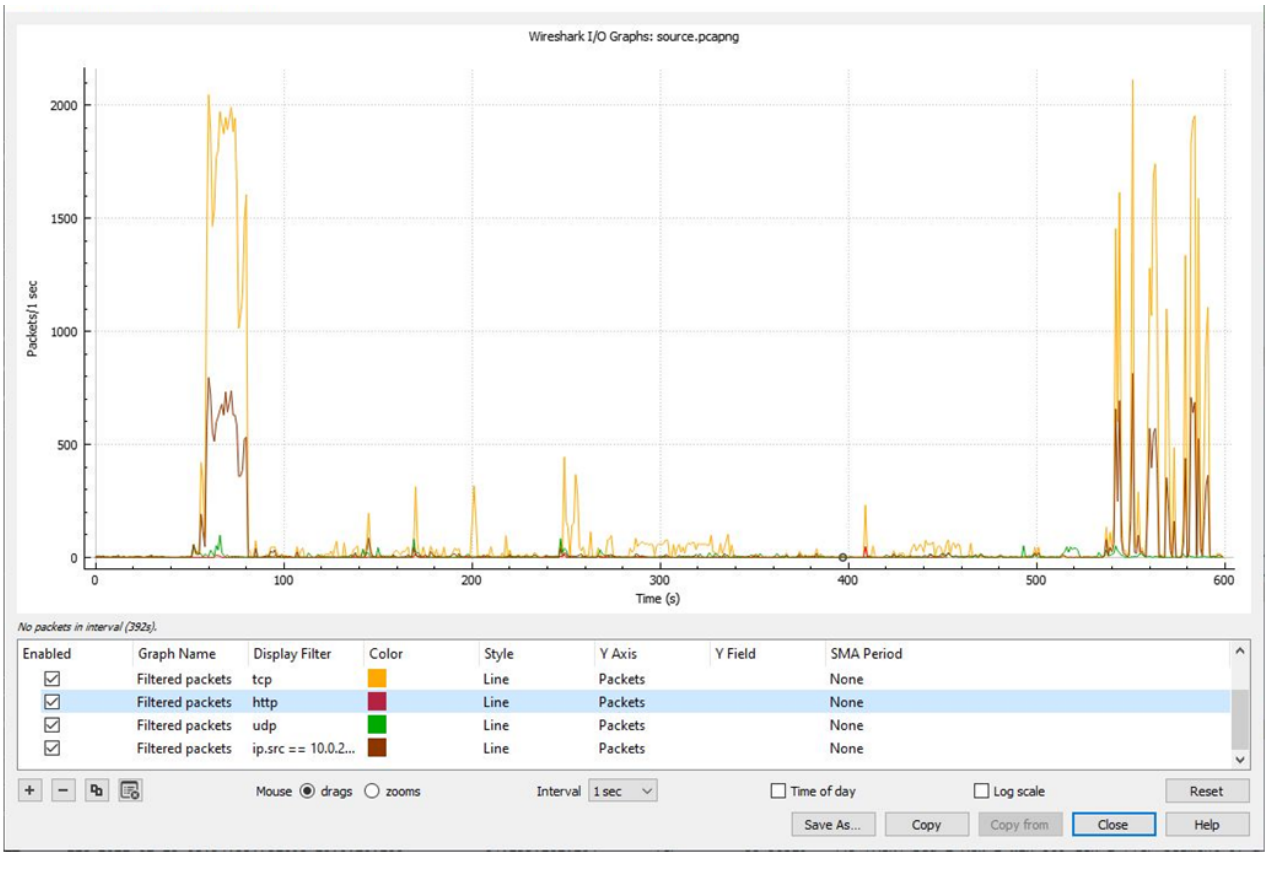


Fig. 11. Length of outgoing packets generated by Wireshark

5. 4. Analysis of the implementation of SD-WAN technology

SD-WAN is a new paradigm in network design and management that enables network programmability and separation of control planes.

The research paper [28] deals with the Controller Placement Problem (CPP) and defines the Quality of Service (QoS) requirements. The proposed algorithms use graph theory to heuristically search for high-quality solutions. The SD-WAN topology is represented by a connected graph $G(V,E)$, $V=S\cup C$, where S is a set of switches with OpenFlow support, and C is controller locations, E is a set of weighted links.

Weighted links are propagation delays between nodes depending on their geographic location. Assuming the controllers can be in the same location as the switches, the potential controller locations are equal to the switch set ($C=S$).

In [28], two binary variables are defined, namely y_j and x_{ij}, to determine decisions about the location and assignment of controllers.

$$\sum_{j\in C} y_i \ . \tag{12}$$

$$y_i \geq x_{ij}, \forall i \in S, \quad j \in C. \tag{13}$$

$$\sum_{j\in C} x_{ij} = r, \quad \forall i \in S. \tag{14}$$

$$\sum_{i\in S} l_i \cdot x_{ij} \leq u_c, \quad \forall j \in C. \tag{15}$$

The specified limit (15) prevents the total load put on by the switches on the controller from exceeding its u_c bandwidth.

$$d_{ij} \cdot x_{ij} \leq sc_{\max}, \quad \forall i \in S, \quad \forall j \in C. \tag{16}$$

The constraint in (16) expresses that the propagation delay between the switch and its assigned controllers satisfies the $sc_{\max}$ delay constraint.

$$d_{j'j''} y_{j'} y_{j''} \leq cc_{\max}, \quad \forall j', j'' \in C \ . \tag{17}$$

The maximum allowable delay among open controllers is provided by the constraint in (19).

$$x_{ij}, y_j \in \{0,1\}, \quad \forall i \in S, \quad \forall j \in C. \tag{18}$$

(18) provides integrality constraints.

[29] defines SD-WAN tasks such as the topology mechanism performed by the processor to obtain appropriate routing information and the definition of Internet Protocol Security (IPSec) tunnels among multiple network nodes. Non-limiting examples of routing information might include information related to IPSec tunnels and Virtual Local Area Network (VLAN) subnets. IPSec tunnels can contain information such as tunnel name, tunnel source and destination ID, cost, and role. In the example, the information related to IPSec tunnels might contain information related to IPSec tunnels that are used for load balancing.

SD-WAN provides real-time intelligent control and management to improve performance and efficient use of network resources through management. Experiments have shown that the approach successfully demonstrates robustness and efficiency through the use of SDN programmability for the global network [30, 31].

Using the Hurst coefficient, the regularities of the length of transmitted packets in our network are determined.

First, the average mathematical expectation of the packet length is calculated:

$$M = \frac{1}{N}\sum_{i=1}^{N} X_i. \tag{19}$$

Calculation of the average standard deviation of the size of the packet length:

$$S = \frac{1}{N}\sum_{i=1}^{N} (X_i - M)^2. \tag{20}$$

Calculation of deviations from the mathematical expectation:

$$D_i = \sum_{j=1}^{i} X_i - M. \tag{21}$$

Calculation of the range (amplitude) of the change in D values:

$$R = \max\{D\} - \min\{D\}. \tag{22}$$

Calculation of the Hurst coefficient:

$$H = \frac{\ln\left(\frac{R}{S}\right)}{\ln(N)}. \tag{23}$$

The result of the calculation in PHP (Fig. 12)

```
[126]
N = len(lens)
M = lens.mean()
S = lens.std()

D = [(lens.head(k)-M).sum() for k in range(0, N)]
R = max(D) - min(D)

H = math.log(R/S)/math.log(N)
print(H)
```

```
0.7523179736409876
```

Fig. 12. The value of the Hurst coefficient

The result of the testing algorithm showed that the most resource-intensive process is the web server process. This process creates the main load when generating dynamic pages using the PHP language interpreter.

According to analyzes, if the Hurst coefficient is greater than 0.5, it means that the process is self-sustaining, i.e. if the value of the quantity increases over time, then after that it continues to increase.

According to the results of Gartner (Fig. 7, Table 2), the leading companies are VMware, Cisco, Fortinet, Palo Alto Networks, Huawei and Oracle.

An anonymous online survey was conducted among the employees of IT companies of the Republic of Kazakhstan. As shown by its results, 34 % of respondents know the general principles of SD-WAN operation, have not heard – 45 %, try to pilot –14 %, use – 7 % (Fig. 13).

According to expert analysis, SD-WAN implements cases of guaranteed connection of many geographically distributed points and is part of SASE (Secure Access Service Edge) (Fig. 14).

According to a report by analyst firm Dell'Oro Group, the global SD-WAN market grew by 39 % in 2021. Cisco is the leader in technology adoption, Fortinet is second, and VMware, Versa and HPE Aruba are also in the top five [32]. A survey by vendors showed that 21 % of respondents trusted Fortinet, Cisco was chosen by 18 %, VMware (13 %) and Oracle (11 %) ranked third and fourth. Closing in the top five Palo Alto Networks (9 %) (Fig. 15).

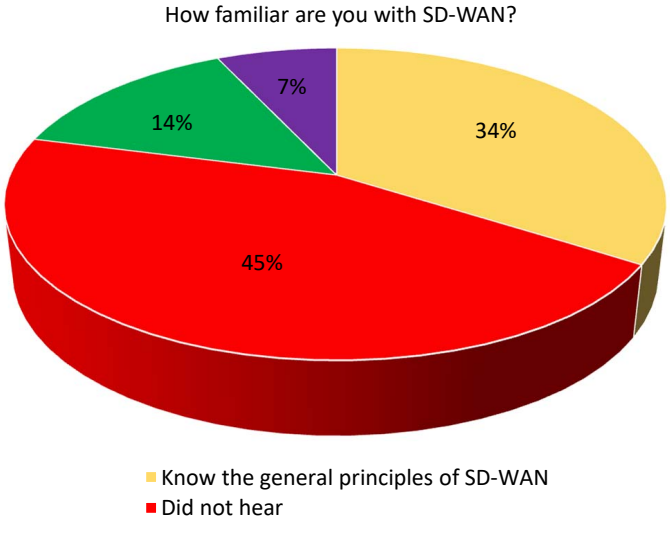


Fig. 13. Result of the online survey

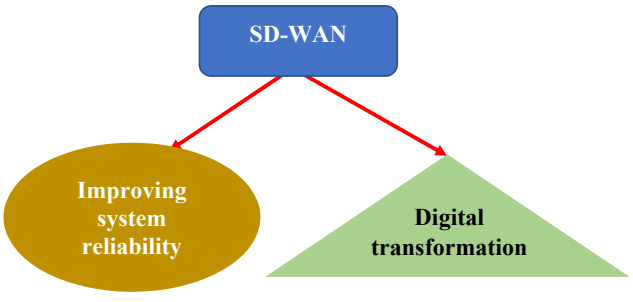


Fig. 14. SD-WAN Application Scenario

For the experiment of implementing SD-WAN, a laboratory bench from Cisco Viptela (San Jose, USA) is considered (Fig. 16).

Used for the software:

– SD-WAN controllers – vManage, vSmart, vBond, version 20.1.1;

– SD-WAN routers – CSR1000v, version 17.2.1r;

– WAN emulator – WANem, version 3.0;

– WMvare platform, version 16 Player.

According to analysis by Shin Umeda, Vice President at Dell'Oro Group, SD-WAN adoption in Europe and Asia is growing strongly. In the first half of 2021, 70 % of the market share was taken by the leading suppliers.

A subsidiary of Halyk Bank of Kazakhstan, Kazteleport Joint Stock Company and a large innovative construction holding BI Group are leaders in the implementation of SD-WAN technology. According to Kazteleport JSC, the introduction of SD-WAN technology has reduced the cost of dedicated channels with a bandwidth of 5 Mbit/s 3 times, received savings in administration and maintenance of the network.

As a result of the implementation of SD-WAN in the BI Group holding, the number of connection points has doubled – from 80 to 150 objects. The use of this technology is an indicator of high productivity growth and obtaining a fault-tolerant network with wide scalability [33, 34].

Table 2

Comparison of SD-WAN solutions

Manufacturers	The main characteristics							
	Own hardware and virtual	Hypervisor support	Cloud support	Lack of risks	High-quality documentation and training system	High quality service support	Subscription and perpetual licensing	Flexible building of configurations based on templates
VMware	√	√	√	√	√	√	√	√
Cisco	√	√	√	√	√	√	√	√
Fortinet	√	√	√	√	√	√	√	–
Palo Alto Networks	√	√	√	√	√	√	√	–
Silver Peak	–	–	√	–	√	–	–	–
Aryaka	√	√	√	√	–	–	–	–
Nokia	√	√	√	–	√	√	–	–
Versa Networks	√	–	√	√	√	–	√	√
Citrix	√	√	√	√	√	√	√	–
Huawei	√	√	√	√	√	√	√	√
Juniper	√	√	√	√	√	√	√	–
Oracle	√	√	√	√	√	√	√	√
Riverbed	√	√	√	–	√	–	–	–
Zyxel	√	√	√	√	–	–	–	–

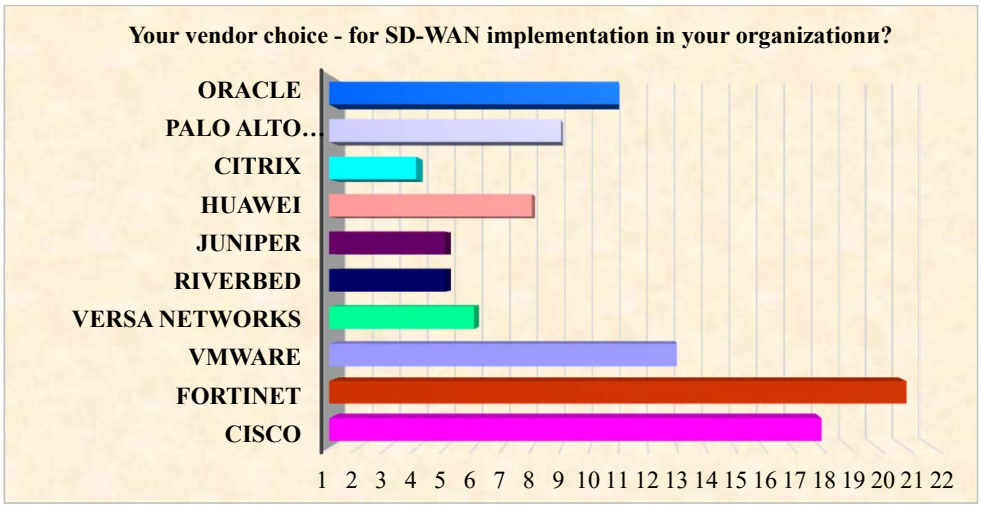


Fig. 15. Choosing a vendor for SD-WAN implementation

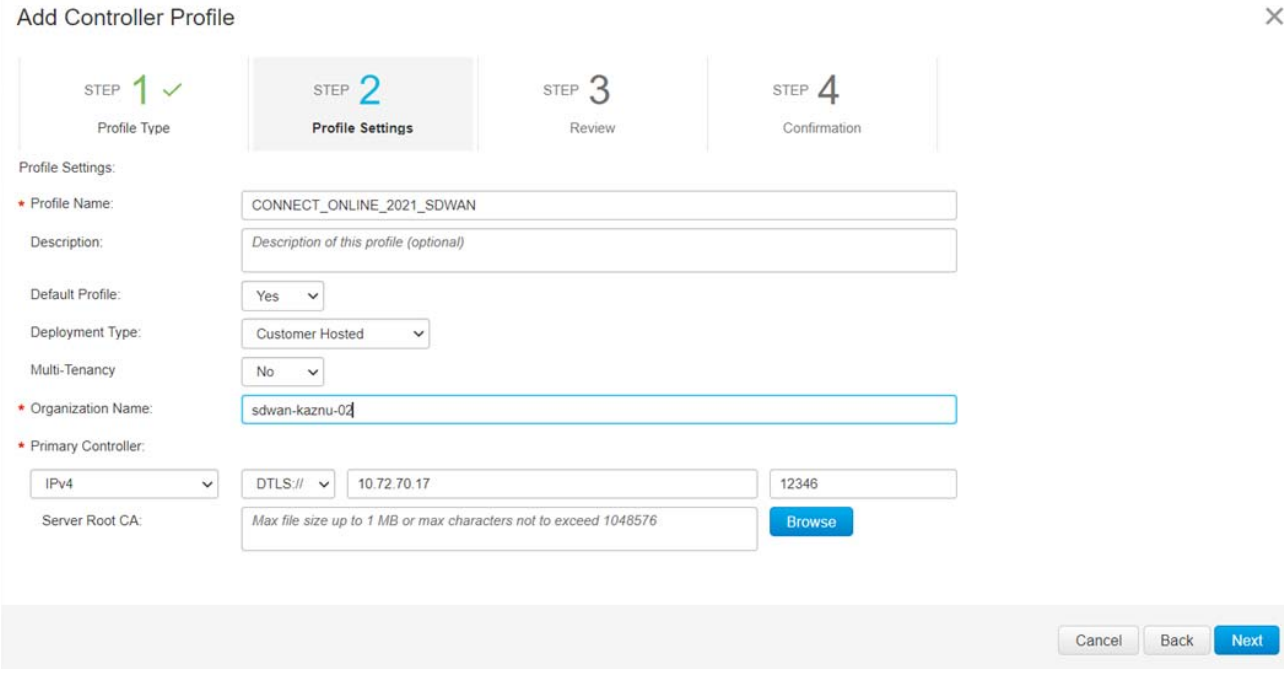


Fig. 16. Adding Controller Profile

The SD-WAN concept is a technology for distributing network traffic over data network channels to automatically determine the most efficient route for traffic between an office and a data processing center (DPC). In the process, the network administrator determines the appropriate security policies. SD-WAN components are:

– terminal devices that replace WAN routers;

– orchestrator – configuring traffic routing policy and security functionality;

– Analytics tools are reports based on data collected from endpoints, such as channel history, network application history, and node availability.

The SD-WAN security solution for on-premises and cloud-based security includes the following categories: network segmentation, corporate firewall, secure web gateway, and DNS-compromised security [35].

In the discussion, experts noted three SD-WAN security models, such as SD-WAN with built-in security, SD-WAN using a chain of services and cloud security, SD-WAN with a corporate firewall [36].

The head of the BI Group holding reports that, since the introduction of SD-WAN, the load on the information security department has dropped sharply, and this despite the fact that there are more objects, also, the quality of the network has dramatically improved [34].

One of the leading SD-WAN solution providers is Fortinet, which has received Recommended status from NSS Labs for the implementation of the next generation firewall (NGFW). NGFW provides ISO Level 3 through 7 security using its own security processor. The SD-WAN solution also monitors firewall rules and policies and offers recommendations for optimizing the entire security system [36].

6. Discussion of the results of the study of the throughput of controllers based on SD-WAN technology

One of the main goals of SD-WAN is to provide robust network management. SD-WAN performance depends on the operation of centralized controllers, which, when one controller fails, reassign to other active controllers.

In this paper, methods and algorithms for complex threat protection tools based on SD-WAN technology were investigated.

A model for detecting and protecting against DDoS for SDN [17] is considered, as well as the basic principles of designing a network state [18].

The results of the testing algorithm can be used in traffic control, when optimizing the network security system based on SD-WAN technology.

The unresolved issues in the analysis of the organization of network security based on SD-WAN technology are related to the choice of access policy. Since the implementation of SD-WAN simplifies the connection of branch offices and contributes to the growth of the overall network security using the IPSec protocol.

Implementation of SD-WAN improves control of access rights to the network and applications, qualitatively monitors the operations performed by the connected clients.

SD-WAN controllers – vManage, vSmart, vBond can be deployed both in a corporate network and in a public cloud environment.

The main characteristics of vBond:

– provides connectivity between the planes of administration, control and data transfer;

– starting point of authentication;

– high resiliency;

– authorizes all control connections ("whitelisting" model).

Key features of vManage:

– a single management console for operations Day0, Day1 and Day2 (deployment, configuration, operation);

– the formation of policies and templates;

– monitoring and troubleshooting.

Key features of vSmart:

– provides discovery of devices in the factory;

– propagates control plane information to vEdge devices;

– applies control plane policies;

– reduces the complexity of the control plane.

In the work, an experimental test bench was developed as a corporate network for analyzing the organization of network security over broadband Internet using SD-WAN. To measure the performance of the proposed solution, we used Cisco SD-WAN controllers – vManage, vSmart, vBond.

7. Conclusions

1. Results of research of methods and algorithms for complex protection against threats based on SD-WAN technology allows to manage large-scale corporate networks without manual configuration and high-security connections built-in security functions with the ability to redirect traffic to centralized protection services. This technology comprehensively solves the modernization of the network infrastructure of telecom operators, data centers and distributed corporate networks. Also, the platform includes orchestration of network services, organization of high-speed traffic processing and virtualization of network functions.

2. Development of a protection algorithm for bandwidth against various types of attacks optimized the use of communication channels, increased resiliency and accelerated network reconfiguration. Based on the calculation results, it was obtained: the Hurst coefficient is greater than 0.5. This proves that this process is self-sustaining.

3. The testing algorithm and the analyzes carried out revealed the leaders of the SD-WAN market, and according to Dell'Oro Group research, in the first half of 2021, the global SD-WAN market grew by 39 % and the share of growth will only increase. The application of SD-WAN technology to secure management of the cloud or on-premises environment can be tailored to meet the following needs:

– providing local access to the Internet at remote sites;

– SSL inspection with high bandwidth;

– filtering web content for Internet security without using a separate Secure Web Gateway (SWG);

– IPSec encryption;

– centralized supervision and control of all internal, incoming and outgoing traffic.

The developed algorithm showed that at zero load, that is, in the absence of active connections with the server, the processor load was about 0 %, the memory use was 457 Mb, the response time was less than 1 ms. With an average daily load, the resource utilization was: processor – 31 %, RAM – 514 Mb, response time – less than 1 ms.

Centralized policy-based management allows the network engineer to send more (or less) traffic over broadband links at any time, without having to reconfigure routers on an individual basis. Vendors are increasingly using security features to differentiate their SD-WAN solutions in a competitive marketplace. Implementing SD-WAN improves performance, reduces the number of hardware devices in branch offices, and provides secure Internet access.

4. The SD-WAN is being implemented on the existing corporate network as part of the equipment upgrade. Initially, it is necessary to test the SD-WAN solution in a multi-site pilot zone. Also, it is necessary to configure the exchange of information with the existing corporate network and multiple terminal devices.

References

1. Laponina, O. R., Sizov, M. R. (2017). Laboratory bench for testing the integration capabilities of SDN networks and traditional networks. International Journal of Open Information Technologies, 5 (9).
2. Mukhizi, S., Mutkhanna, A. S., Kirichek, R. V, Kucheriavii, A. E. (2019). Issledovanie modelei balansirovki nagruzki v programmno-konfiguriruemykh setiakh. Elektrosviaz, 1, 23–29
3. Sallent, O., Perez-Romero, J., Ferrus, R., Agusti, R. (2017). On Radio Access Network Slicing from a Radio Resource Management Perspective. IEEE Wireless Communications, 24 (5), 166–174. doi: http://doi.org/10.1109/mwc.2017.1600220wc

4. OpenFlow Management and Configuration Protocol (OF-CONFIG 1.2). ONF TS-016. Available at: https://www.opennetworking.org/wp-content/uploads/2013/02/of-config-1.2.pdf Last accessed: 15.08.2021
5. Google's Inter-Datacenter WAN Using SDN and OpenFlow. Available at: https://opennetworking.org/sdn-resources/customer-case-studies/google/
6. OpenFlow. Available at: https://lvk.cs.msu.su/~sveta/SDN_OpenFlow_basics_lecture1_v2.pdf Last accessed: 15.08.2021
7. Tok, M. S., Demirci, M. (2021). Security analysis of SDN controller-based DHCP services and attack mitigation with DHCPguard. Computers & Security, 109, 102394. doi: http://doi.org/10.1016/j.cose.2021.102394
8. Huang, X., Zeng, M., Xie, K. (2021). Intelligent traffic control for QoS optimization in hybrid SDNs. Computer Networks, 189, 107877. doi: http://doi.org/10.1016/j.comnet.2021.107877
9. Pamplin, S. (2021). SD-WAN revolutionises IoT and edge security. Network Security, 2021 (8), 14–15. doi: http://doi.org/10.1016/s1353-4858(21)00090-8
10. Tok, S., Demirci, M. (2021). An Investigation of Topology Poisoning Attacks in Software Defined Networks Through Exploiting Link Layer Discovery Protocol, 589–608. Uludağ University Journal of The Faculty of Engineering, . doi: http://doi.org/10.17482/uumfd.769939
11. Polat, H., Polat, O., Cetin, A. (2020). Detecting DDoS Attacks in Software-Defined Networks Through Feature Selection Methods and Machine Learning Models. Sustainability, 12 (3), 1035. doi: http://doi.org/10.3390/su12031035
12. Olivier, F., Carlos, G., Florent, N. (2015). New Security Architecture for IoT Network. Procedia Computer Science, 52, 1028–1033. doi: http://doi.org/10.1016/j.procs.2015.05.099
13. Khorsandroo, S., Sánchez, A. G., Tosun, A. S., Arco, J., Doriguzzi-Corin, R. (2021). Hybrid SDN evolution: A comprehensive survey of the state-of-the-art. Computer Networks, 192, 107981. doi: http://doi.org/10.1016/j.comnet.2021.107981
14. Dayal, N., Srivastava, S. (2021). SD-WAN Flood Tracer: Tracking the entry points of DDoS attack flows in WAN. Computer Networks, 186, 107813. doi: http://doi.org/10.1016/j.comnet.2021.107813
15. Smelianskii, R. L. (2014). Tekhnologii SDN i NFV: novye vozmozhnosti dlia telekommunikatsii. Vestnik Sviazi, 1, 43–47. Available at: https://www.arccn.ru/media/1132/ Last accessed: 29.08.2021
16. Galich, S. V., Deogenov, M. S., Kartashevskii, V. G., Pasiuk, A. O., Semenov, E. S. (2016). Issledovanie proizvoditelnosti PKS-kontrollera OpenDaylight na setiakh raznykh masshtabov. Izvestiia IUFU. Tekhnicheskie nauki, 9, 121–133.
17. Fouladi, R. F., Ermiş, O., Anarim, E. (2020). A DDoS attack detection and defense scheme using time-series analysis for SDN. Journal of Information Security and Applications, 54, 102587. doi: http://doi.org/10.1016/j.jisa.2020.102587
18. Cui, Y., Qian, Q., Xing, H., Li, S. (2020). LNAD: Towards Lightweight Network Anomaly Detection in Software-Defined Networking. 2020 IEEE 22nd International Conference on High Performance Computing and Communications; IEEE 18th International Conference on Smart City; IEEE 6th International Conference on Data Science and Systems (HPCC/SmartCity/DSS), 855–860. doi: http://doi.org/10.1109/hpcc-smartcity-dss50907.2020.00113
19. Pourvahab, M., Ekbatanifard, G. (2019). An Efficient Forensics Architecture in Software-Defined Networking-IoT Using Blockchain Technology. IEEE Access, 7, 99573–99588. doi: http://doi.org/10.1109/access.2019.2930345
20. ONF TR-502: SDN Architecture (2014). Open Networking Foundation. Available at: https://www.opennetworking.org/images/stories/downloads/sdn-resources/technical-reports/TR_SDN_ARCH_1.0_06062014.pdf Last accessed: 20.08.2021
21. Queiroz, W., Capretz, M. A. M., Dantas, M. (2019). An approach for SDN traffic monitoring based on big data techniques. Journal of Network and Computer Applications, 131, 28–39. doi: http://doi.org/10.1016/j.jnca.2019.01.016
22. Lee, S., Kim, J., Woo, S., Yoon, C., Scott-Hayward, S., Yegneswaran, V. et. al. (2020). A comprehensive security assessment framework for software-defined networks. Computers & Security, 91, 101720. doi: http://doi.org/10.1016/j.cose.2020.101720
23. Rana, D. S., Dhondiyal, S. A., Chamoli, S. K. (2019). Software Defined Networking (SDN) Challenges, issues and Solution. International Journal of Computer Sciences and Engineering, 7 (1), 884–889. doi: http://doi.org/10.26438/ijcse/v7i1.884889
24. Critical Capabilities for WAN Edge Infrastructure. Available at: https://www.gartner.com/doc/reprints?id=1-1XWDQO33&ct=191210&st=sb Last accessed: 24.08.2021
25. Guo, Z., Feng, W., Liu, S., Jiang, W., Xu, Y., Zhang, Z.-L. (2019). RetroFlow: Maintaining Control Resiliency and Flow Programmability for Software-Defined WANs. IEEE/ACM International Symposium on Quality of Service (IWQoS '19). Phoenix, New York. doi: http://doi.org/10.1145/3326285.3329036
26. Malakhov, S. V., Tarasov, V.N. (2015). Teoreticheskoe i eksperimentalnoe issledovanie zaderzhki v programmnogo-kofiguriruemykh setiakh. Infokommunikatsionnye tekhnologii, 4, 409–413.
27. Maltsev, A. (2018). Postroenie zaschischennoi i adaptiruemoi seti SD-WAN. Available at: https://www.osp.ru/lan/2018/04/13054564 Last accessed: 29.08.2021
28. Tanha, M. (2019). Resilient Controller Placement Problems in Software Defined Wide-Area Networks. University of Victoria, 130.

29. Kodavanty, V., Sen, S., Kamsetty, S., Arumugam, P. V. (2019). Pat. No. US 2019/0207844 A1 USA. Determining routing decisions in a software – defined wide area network. Pub. Date: 04.07.2019.
30. Golani, K., Goswami, K., Bhatt, K., Park, Y. (2018). Fault Tolerant Traffic Engineering in Software-defined WAN. 2018 IEEE Symposium on Computers and Communications (ISCC). doi: http://doi.org/10.1109/iscc.2018.8538606
31. Sarychev, D. (2021). Kak obespechit bezopasnost programmno-opredeliaemykh setei (SD-WAN). Available at: https://www.anti-malware.ru/analytics/Technology_Analysis/Secure-SD-WAN Last accessed: 05.09.2021
32. SD-WAN Market Recorded 39 Percent Growth for 1H 2021, According to Dell'Oro Group. Available at: https://www.delloro.com/news/sd-wan-market-recorded-39-percent-growth-for-1h-2021/ Last accessed: 05.09.2021
33. Galiev, A. (2021). Kak «Kazteleport» v razy sokratil izderzhki na vydelennye kanaly s pomoschiu SD-WAN. Available at: https://profit.kz/articles/14657/Kak-AO-Kazteleport-v-razi-sokratil-izderzhki-na-videlennie-kanali-s-pomoschu-SD-WAN/ Last accessed: 05.09.2021
34. BI Group modernizirovala set s pomoschiu resheniia SD-WAN ot Fortinet (2021). Available at: https://profit.kz/articles/14700/BI-Group-modernizirovala-set-s-pomoschu-resheniya-SD-WAN-ot-Fortinet/ Last accessed: 05.09.2021
35. Razbor rynka SD-WAN: kakie suschestvuiut resheniia i komu oni nuzhny (2019). Available at: https://safe.cnews.ru/articles/2019-11-06_razbor_rynka_sdwan_kakie_sushchestvuyut Last accessed: 06.09.2021
36. Rukovodstvo po sredstvu zaschity SD-WAN dlia rukovoditelei v sfere setevykh tekhnologii. Available at: https://www.fortinet.com/content/dam/fortinet/assets/white-papers/ru_ru/eBook-The-Network-Leaders-Guide-to-Secure-SD-WAN.pdf Last accessed: 06.09.2021