УДК 004.056
https://doi.org/10.47533/2020.1606-146X.218

A. M. NURUSHEVA, A. K. AMRENOV*

L.N. Gumilyov Eurasian National University, Astana, Kazakhstan

USE AND ANALYSIS OF NEXT GENERATION FIREWALL TO ACHIEVE SECURITY OF INFORMATION AND COMMUNICATION INFRASTUCTURE

The article is devoted to the investigation of the problem of the security of information and communication infrastructure functioning. The next generation firewall which was named UTMsense (UTM box) was tested. The results of testing are considered in the article. The comparing review of UTM box and other products was made. The possibility of using the tool for CERTs and SOCs is also considered.

Keywords*: Next Generation Firewall, Next Generation Threat Prevention, Information and Communication Infrastructure, Security.*

Introduction. The quality of succulent feed for animal husbandry is determined by the availability of full seeds, which in turn is determined by the level of equipment of seed farms with effective seed-cleaning unit for cleaning seed material from seeds of quarantine and hard-separable weeds. Today, seed producers of fodder crops in the country are import-dependent for clover seeds, about 60% of seed material is purchased abroad [1].

In world practice, the highest results of cleaning seeds of quarantine and hard-separable impurities are achieved by separating machines, the operating principle of which is based on optical-electronic recognition of seeds of impurities. More than 15 machine manufacturing companies produce these color sorting machines in the world [2]. Their cost varies from 15 to 120 thousand US dollars, which is unbearable for small producers of fodder crops in the country.

As part of our project, we have set a goal - to improve the design and technological parameters of the color sorter, achieving a reduction in its cost.

Problem statement. Today, many organizations develop and use their information and communication infrastructure without due regard for their information security and fault tolerance. The organizations save their time and do not spend their financial resources on tools for information security risks and threats analysis. As a result, such organizations often have information security incidents on their information and communication infrastructure.

One of the layers of security against external threats and attackers to networks is a firewall [13]. It can help to minimize the information security risk and threat to an acceptable level. Firewall technology is a set of mechanisms that collectively enforce a security policy on communication traffic entering or leaving the guarded network domain [14-16].

So the firewalls can protect materials such as stored data, information computation, and communication resources. They can guard against unauthorized access, browsing, leaking, modification, insertion, deletion and other. In addition, they can provide protection from “denial-of-service” attacks in which users are prevented from accessing the network by

* E-mail корреспондирующего автора: askhat.amrenov@gmail.com

a message that disables the equipment or by a flood of messages that clogs the internal network [14-17].

When they are used, the network administration and management become more efficient, as they limit the exposure of the internal network.

Related Work. Considering the priority use of domestic IT products in the country, next generation firewall was tested. It was named UTMsense (UTM box).

Some pictures of UTM box are shown in Figure 1.

Figure 1 – UTM box (UTMsense)

Let's consider some advantages of the UTM box:

1) Unique functionality: Combined in one solution, various functional modules allow avoiding the cost of additional equipment to protect against network intrusions. This solution supports integration with existing infrastructure solutions and security systems.

2) Improved performance: It was reached a level of performance that allows you to use all the existing functionality of the product without losing data processing speed.

3) Increased efficiency: The advanced traffic monitoring system allows you to block up to 99.4% of network threats and provides security system flexibility, allowing you to customize security policies in accordance with the requirements of regulators and internal regulations.

4) Scalable functionality: The IT product is suitable for small businesses, combining the necessary basic functionality to provide comprehensive protection against network intrusions at an affordable price.

Advanced functionalities suitable for protecting medium-sized enterprises include a DNS server, a fault tolerance function, a Captive Portal, and provide a greater number of network connections.

The Enterprise level device has enhanced performance for processing large amounts of data and a full set of functionality necessary to protect large infrastructure:

- Fault tolerance;
- Support;
- Integration;
- DNS;
- Captive Portal;
- SSL;
- Balancer.

Comparison of UTM-box with alternative solutions is given in Table 1.

Table 1 – Comparison of UTM-box (UTMsense) with alternative solutions

	UTMbox	Cisco ASA	Fortinet Fortigate	Check Point	Palo Alto
NGFW	+	+	+	+	+
IPS	+	+	+	+	+
Antivirus	+	+	+	+	+
URL filtering	+	+	+	+	+
Remote Access VPN	+	+	+	+	+
Site-to-site VPN	+	+	+	+	+
Integration with Snort and Open AppID	+	+			
Captive Portal	+		+	+	+
High Availability	+	+	+	+	+
Inbound Load Balancing	+		+	+	+
Full-fledged configuration from Web-interface	+		+		+

The base features of the IT-product are:
• Firewall;
• Routing;
• VPN;
• User Authorization;
• Network Services;
• Management.
Extended features:
• URL filtering;
• High availability;
• Extended DNS server;
• Captive portal;
• SSL inspection;
• Inbound load balancing.
The base features components of the UTM-box are given in Table 2.

Table 2 – The base features components of the UTM-box (UTMsense)

The base features of the IT-product	Components
Firewall	Statefull Firewall Aliases NAT Schedules Traffic Shaper Virtual IP Virtual interfaces Bridges
Routing	BGPD OSPF RIP
VPN	IP sec Open VPN L2TP
User Authorization	Local Radius LDAP
Network Services	PPoE server NTP server/client DHCP (IP v4/6) server/client/relay DNS resolver/forwarder Radius UPnP SNMP
Management	Web-based configuration SSH RJ45 Console

UTM box can be divided into three types:
• For small business;
• For medium business;
• For large enterprises.
The technical specifications of UTM-box for small business are given in Table 3.

Table 3 – Technical specifications of UTM-box for small business

	UTMbox
Gbit Ethernet	More than 4
Firewall throughput	
Max. connect.	More than 1800000
Max. connect.states	More than 3600000
Max.throughput (1400 b. packets), PPS/Mbit/sec	*
VPN throughput, Mbit/s	
Open VPN/AES-128+SHA1	More than 60
Psec/IKEv2+AE S-GCM	More than 200
Recommended workload	
User	More than 10
Wan speed, Mbit/sec	More than 10

The comparing between traditional firewall and next generation firewall is presented in Table 4.

Table 4 – The base features components of the UTM-box (UTMsense)

Parameter	Traditional Firewall	Next Generation Firewall
1	2	3
Traffic filtering (Port, IP Address and protocol based	Supported	Supported
Application Visibility and Application Control	Partial	Detailed
CAPEX and OPEX (considering all feature requirement)	Higher since separately need to buy and maintain	Considerable reduction since all services will be bundled into single box
IPS (Intrusion Prevention System)	Not Supported	Supported
NAT	Supported	Supported
VPN	Supported	Supported
Application level awareness	Not Supported	Supported

1	2	3
Reputation and identity services	Not Supported	Supported
Working Layer	Layer 2 to Layer 4	Layer 2 upto Layer 7
Throughput and performance	Lower than NGFW and drastically reduces when additional services introduced.	Much higher than traditional Firewall and doesn't change much on introduction of additional services.
Reporting	Standard reports	Customized reporting upto user level giving near real time detail with plenty of additional reporting options like download format etc.

The data presented in Table 4 also show the advantages of next generation firewall.

Thus, we propose the use of the domestic IT product as a Kazakhstan solution aimed at the full import substitution of foreign manufacturers in different sectors of the Republic of Kazakhstan, including the critical informatization objects protection.

Conclusion. In this article, we describe the next generation firewall to protect information, and communication infrastructure. It was considered some goals, functionality and advantages of the IT product.

The use of domestic product allowed significantly improving the level of information security in the Republic of Kazakhstan. It was reducing the level of information threats due to identifying and neutralizing the threats in the information and communication infrastructure. In addition, the product has several advantages. In the future, it is planned to modify the UTM box: add new functions using new methods, updating databases, etc.

Therefore, the use of such a tool is a priority for CERTs and SOCs.

REFERENCES

1 S.Boranbayev, N.Goranin, A.Nurusheva. "The methods and technologies of reliability and security of information systems and information and communication infrastructures" Journal of Theoretical and Applied Information Technology, vol.96, pp. 6172-6188, 2018.

2 Z. Turskis, N. Goranin, A. Nurusheva, and S. Boranbayev, "A Fuzzy WASPAS-Based Approach to Determine Critical Information Infrastructures of EU Sustainable Development", Sustainability, vol. 11, no. 2, p. 424, 2019.

3 A. Boranbayev, S. Boranbayev, A. Nurusheva, K. Yersakhanov and Y. Seitkulov, "Development of web application for detection and mitigation of risks of information and automated systems", Eurasian Journal of Mathematical and Computer Applications, vol. 7, no. 1, pp. 4-22, 2019. Available: 10.32523/2306-6172-2019-7-1-4-22

4 A. Boranbayev, S. Boranbayev, A. Nurusheva, Y. Seitkulov and N. Sissenov, "A method to determine the level of the information system fault-tolerance", Eurasian Journal of Mathematical and Computer Applications, vol. 7, no. 3, pp. 13-32, 2019. Available: 10.32523/2306-6172-2019-7-3-13-32

5 Z. Turskis, N. Goranin, A. Nurusheva, and S. Boranbayev, "Information Security Risk Assessment in Critical Infrastructure: A Hybrid MCDM Approach", Informatica, vol. 30, no. 1, pp. 187–211, 2019.

6 Decree of the President of the Republic of Kazakhstan "On measures to implement the President's Address "Third Modernization of Kazakhstan: Global Competitiveness" dated 15th February, 2017 No422 dated 31st January, 2017

7 Decree of the Government of the Republic of Kazakhstan the Cybersecurity Concept ("Cybershield of Kazakhstan") until 2022 dated 30th June, 2017 No 407.

8 S.N. Boranbayev, A.M. Nurusheva, K.B. Yersakhanov. "The modern state and the further development prospects of information security in the Republic of Kazakhstan." Herald of ENU, №1. 119, Astana, 2017, pp. 52-62.

9 S.N. Boranbayev, A.M. Nurusheva, K.B. Yersakhanov. "Analysis of the state of information security of the Republic of Kazakhstan and prospects for its development". A collection of reports of the IV International Scientific and Practical Conference - Astana: ENU, 2017, p.341-344.

10 Information security incidents for the II quarter of 2018 http://kz-cert.kz/en/page/698. Accessed 15 November 2018.

11 J. Juknius, N. Goranin. "Botnet spreading detection and prevention via website". Journal of young scientists. Šiauliai: Šiaulių universitetas. Nr. 1(26), priedas 2010, p. 293-298.

12 A.Boranbayev, S.Boranbayev, A.Nurusheva, K.Yersakhanov. "The Modern State and the Further Development Prospects of Information Security in the Republic of Kazakhstan" // 15th International Conference of Information Technology, Information Technology – New Generations, 2018, pp. 33-38.

13 S.Lodin Ernst, Young LLP & Christoph L Schuba, "Firewalls tend off invasions from the net", IEEE Spectrum, pp 26-34, February 1998.

14 G.Athisha Miete & K.Sankaranarayanan. "Key Technologies in Information Security—A Review", IETE Technical Review, 22:3, pp. 173-181, 2005. DOI: 10.1080/02564602.2005.11657899.

15 Shao Yiyang, Xue Yibo, Li Jun. PPP: Towards Parallel Protocol Parsing. China Communications. 11/10. pp.106-116. 2018. DOI: 10.1109/CC.2014.6969799.

16 E.S.Yusuf, G.Mengmeng, H. B. Jin, A.Hani, K.D.Seong. A systematic evaluation of cybersecurity metrics for dynamic networks. Computer Networks, Vol. 144 pp. 216-229. 2018. DOI: 10.1016/j.comnet.2018.07.028

17 A.Householder, K.Houle and Chad, Computer Attack Trends Challenge Internet Security, IEEE Security and Privacy, pp 5-7,2002.

А. М. НУРУШЕВА, А. К. АМРЕНОВ*

Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан

АҚПАРАТТЫҚ-КОММУНИКАЦИЯЛЫҚ ИНФРАҚҰРЫЛЫМНЫҢ ҚАУІПСІЗДІГІН ҚАМТАМАСЫЗ ЕТУ ҮШІН КЕЛЕСІ БУЫНДАҒЫ ЖЕЛІАРАЛЫҚ ЭКРАНДЫ ПАЙДАЛАНУ ЖӘНЕ ТАЛДАУ

Мақала ақпараттық-коммуникациялық инфрақұрылымның жұмыс істеу қауіпсіздігі мәселесін зерттеуге арналған. UTMsense (UTM box) деген атау алған келесі буынның желіаралық экранын тестілеу жүргізілді. Мақалада тестілеу нәтижелері қарастырылған. UTM box және басқа өнімдерге салыстырмалы шолу жасалды. Сондай-ақ, мақалада CERT және SOC үшін құралды пайдалану мүмкіндігі қарастырылған.

Түйін сөздер: *жаңа буынның желіаралық экраны, жаңа буынның қауіп-қатерді алдын алу құралдары, ақпараттық-коммуникациялық инфрақұрылым, қауіпсіздік.*

А. М. НУРУШЕВА, А. К. АМРЕНОВ

Евразийский университет имени Л.Н. Гумилева, Нур-Султан, Казахстан

ИСПОЛЬЗОВАНИЕ И АНАЛИЗ МЕЖСЕТЕВОГО ЭКРАНА СЛЕДУЮЩЕГО ПОКОЛЕНИЯ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННО-КОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЫ

Статья посвящена исследованию проблемы безопасности функционирования информационно-коммуникационной инфраструктуры. Осуществлено тестирование межсетевого экрана следующего поколения, получившее название UTMsense (UTM box). В статье рассмотрены результаты тестирования. Выполнен сравнительный обзор UTM box и других продуктов. Также в статье рассмотрена возможность использования инструмента для CERT и SOC.

Ключевые слова: *межсетевой экран нового поколения, предотвращение угроз нового поколения, информационно-коммуникационная инфраструктура, безопасность.*