ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 4, Issue 10 , October 2017

The Experiment about Providing the Security of the Network with the base of the Special Filtering of the Traffic

Gulomov Sherzod Rajaboevich, Akhmedov Kodirjon Sokhibjon ugli

Senior lecturer, Department of Providing Information Security, Tashkent University of Information Technology named after Muhammad al-Khwarizmi, Uzbekistan

Student, Department of Providing Information Security, Tashkent University of Information Technology named after Muhammad al-Khwarizmi, Uzbekistan

ABSTRACT. In this article packet processing scheme on special packet filtering is offered. A special software packet filtering in the computer networks that will allow protecting network traffic from external influences has been developed. From above experiments, identifying the probability of missing the suspicious enables to assess how it is secured from the outer impacts is defined.

I. INTRODUCTION

At present, in the world information processing, storage and transmission are developing intensively. The modern world has become digital. Currently, the following trends in the development and use of modern information technology (IT) are observed:

- complication of computer system software;
- collection and storage of large information databases on electronic media;
- direct access to the resources of the computer system of a large number of users of different categories and with different access rights in the system;
- combining in the general information array of different access methods;
- increase the cost of resources of computer systems;
- the use by most public and private organizations of special anti-virus programs as a means of security;
- extensive use of the Internet, etc.

The use of information technology requires attention to information security. Unauthorized use of information resources, unauthorized access or infringement of information security causes serious problems for citizens, social groups, companies and states. Therefore, it is important to develop efficient methods and algorithms for special traffic filtering, which protects computer networks against unauthorized use and remains a problem of theoretical and practical problem, which is of national importance.

II. THE EXPERIMENT ABOUT THE PROBABILITY OF MISSING SUSPICIOUS PACKETS

Let's say x_1 – is the source which characters filtering through IP addresses and x_2 – is the source which characters usage from filtering through ports.

$x_1 = 1$, Usage from filtering towards IP addresses;

$x_1 = -1$, Disuse from filtering towards IP addresses;

$x_2 = 1$, Usage from filtering towards ports;

$x_2 = -1$, Disuse from filtering towards ports.

After that $p = (x_1), (x_2)$ – it will be determined probability of missing suspicious packets. $p = (x_1, x_2)$ – must be marked as the probability of missing suspicious packets [1,2]. The model object of the experiment $p = (x_1, x_2) = b_0 + b_1x_1 + b_2x_2 + b_3x_1x_2$ polygon can be used as an analytic model. In the experiment, 1000 type of TPC packet's generation will be modeled through IP addresses and ports. Fig.1.1 illustrates that there is no filtering results through IP addresses and ports, namely, $(x_1 = -1, x_2 = -1)$ sources will receive the same symbols, and the probability of missing the suspicious packets will be equal to $p = 0{,}47$.

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 4, Issue 10 , October 2017

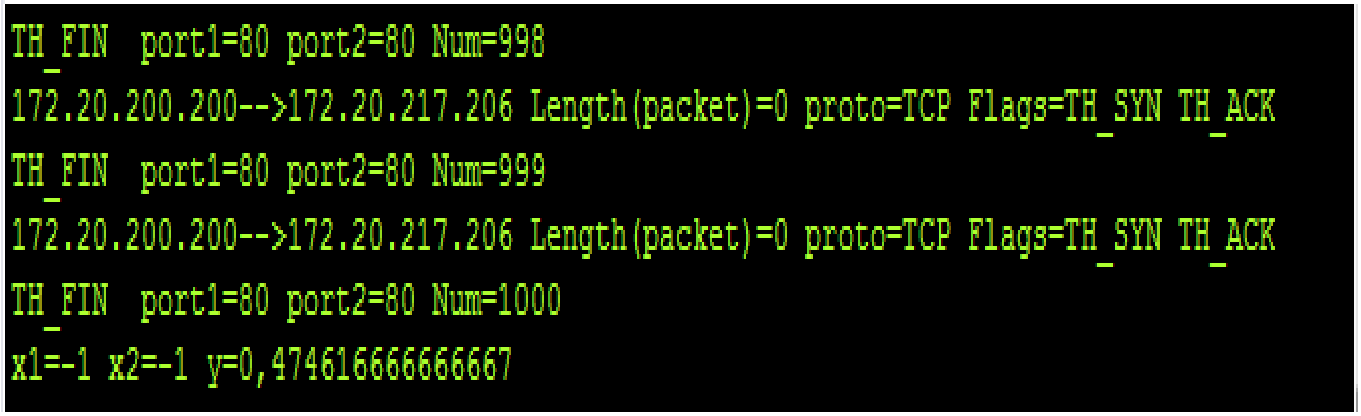

Fig.1.1. There is no filtering results through IP addresses and ports.

Fig.1.2 illustrates that there is no filtering through IP addresses and it is shown that through ports there is existence and a results of filtering towards ports, namely, ($x_1 = -1, x_2 = 1$) sources will receive several symbols and the probability of missing the suspicious packets will be equal to $p = 0{,}33$.

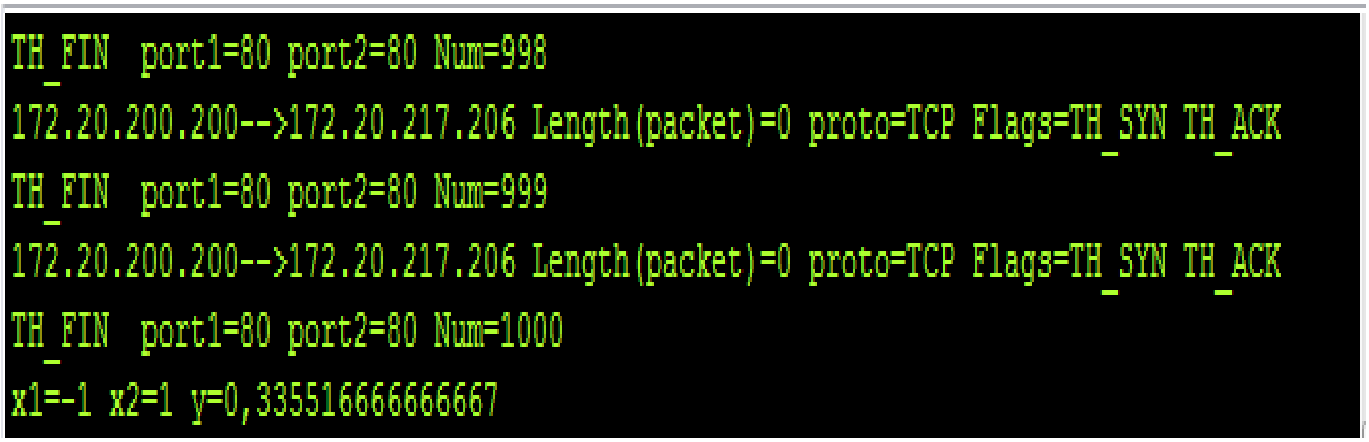

Fig.1.2. There is no filtering towards IP addresses and it is shown that through ports there is existence and results of filtering towards ports.

Fig.1.3 illustrates there is existence of filtering through IP addresses and there is no filtering through Ports namely ($x_1 = 1, x_2 = -1$) sources will receive different symbols and the probability of missing the packets is equal to p = 0.32.

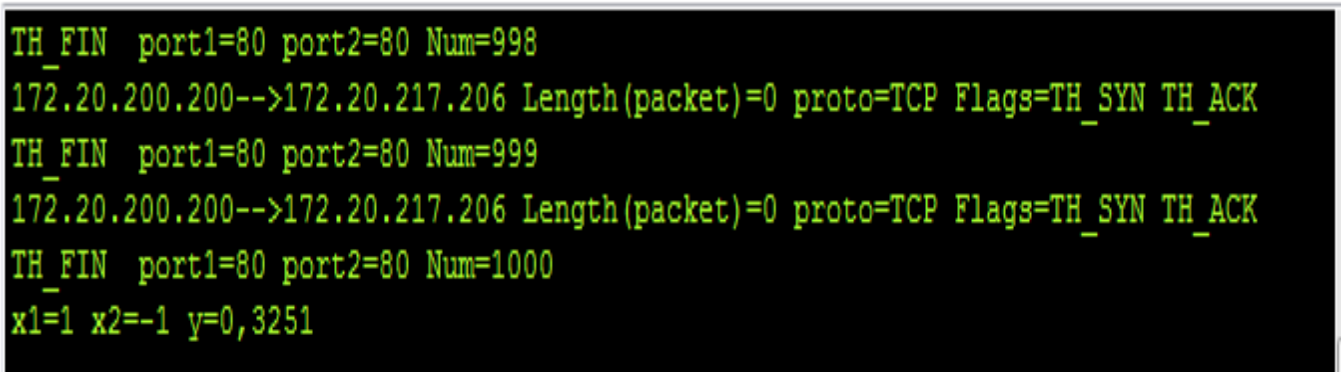

Fig.1.3. There is an existence of filtering through IP addresses and there is no filtering through ports.

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 4, Issue 10 , October 2017

Fig.1.4. shows that there is a existence in both IP addresses and ports, namely ($x_1 = 1,\ x_2 = 1$) will receive the same symbols and the probability of missing the suspicious packets is equal to $p = 0{,}29$

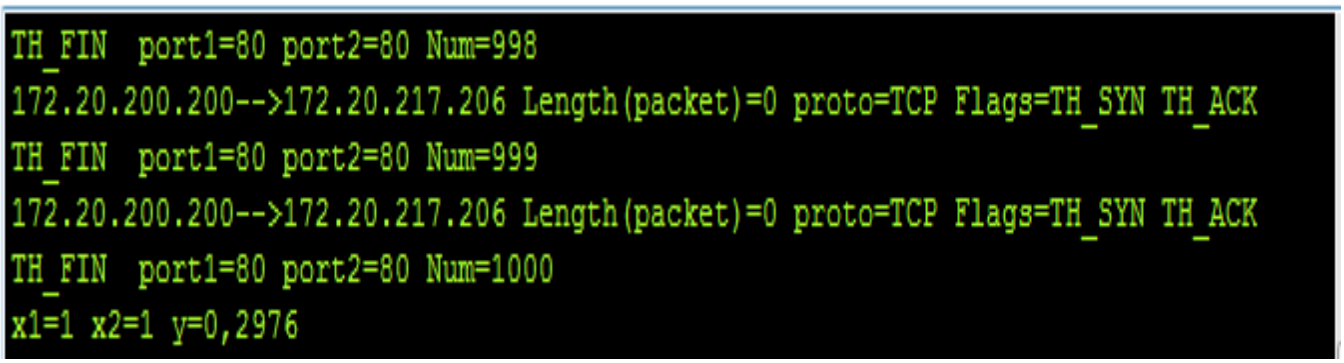

Fig.1.4. There is an existence of filtering through IP addresses and there is filtering through ports.

Table 1 shows the values of the IP addresses and ports.

Table 1.1: Values for IP addresses and ports

Sources / Experiments	x_1	x_2	$p_i = (x_1, x_2)$
There is filtering towards both IP addresses and ports.	-1	-1	$p_1 = (0{,}47)$
There is no filtering towards IP addresses and there is existence of filtering towards ports.	-1	1	$p_2 = (0{,}33)$
There is existence of filtering towards IP addresses and there is no filtering towards ports.	1	-1	$p_3 = (0{,}32)$
There is no filtering in both IP addresses and ports.	1	1	$p_4 = (0{,}29)$

For the experiment that has been done, the linear equation system can be seen like this:

$b_0, b_1, b_2, b_3 -$ model parameters:

$$\begin{cases} p_1 = b_0 + b_1(-1) + b_2(-1) + b_3(1) = 0{,}47 \\ p_2 = b_0 + b_1(-1) + b_2(1) + b_3(-1) = 0{,}33 \\ p_3 = b_0 + b_1(1) + b_2(-1) + b_3(-1) = 0{,}32 \\ p_4 = b_0 + b_1(1) + b_2(1) + b_3(1) = 0{,}29 \end{cases}$$

Below it is described the solution to linear equation system with Matrix and Gauss methods.

$$\left(\begin{array}{cccc|c} 1 & -1 & -1 & 1 & 0{,}47 \\ 1 & -1 & 1 & -1 & 0{,}33 \\ 1 & 1 & -1 & -1 & 0{,}32 \\ 1 & 1 & 1 & 1 & 0{,}29 \end{array}\right) = \left(\begin{array}{cccc|c} 1 & 0 & 0 & 0 & 0{,}35 \\ 0 & 1 & 0 & 0 & -0{,}04 \\ 0 & 0 & 1 & 0 & -0{,}04 \\ 0 & 0 & 0 & 1 & 0{,}02 \end{array}\right)$$

As results we can get these values:

$b_0 = 0{,}35;$

$b_1 = -0{,}04;$

$b_2 = -0{,}04;\ b_3 = 0{,}02.$

$a_1 -$ Filtering towards IP addresses $x_1$the main advantage of factor.

$a_2 -$ Filtering towards Ports x_2 the main advantage of factor.

Considering the experiments of factors formulas, we can write followings:

$$a_1 = \frac{(p_3 - p_1) + (p_4 - p_2)}{2} = \frac{(0{,}32 - 0{,}47) + (0{,}29 - 0{,}33)}{2} = -0{,}095$$

$$a_2 = \frac{(p_2 - p_1) + (p_4 - p_3)}{2} = \frac{(0{,}33 - 0{,}47) + (0{,}29 - 0{,}32)}{2} = -0{,}085$$

It is known from the formula that, factor of filtering towards IP addresses has greater value than factor of filtering towards ports.

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 4, Issue 10 , October 2017

III. ASSESSMENT TO WORK OF THE SPECIAL SOFTWARE PACKET FILTERING

Special software packet filtering and SSP modules which have the higher surface around networking imitation model of the screen is conducted in web page creating Stylemix company in Tashkent: Entering packets with working the rule of exponential for each interface comes with 100 Mbit/sec speed to networking map of the interface. The smallest measurement of packets is 64 byte. For receiving the buffer packets is 48 kilobyte. In the table 1.2, it was shown about special software packet filtering and SSP modules that has higher level in networking screen's filtered and number of filtered entering packets.

Special software packet filtering and SSP modules which have the higher surface Firewall is filtered or not filtered.

Table 1.2: Number of entry packets

№	Special software packet filtering	SSP modules which have the higher surface Firewall
Number of entry packets	1000	1000
Filtered packets numbers	990	984
Not filtered packets numbers	10	16

Fig.1.5 describes special software packet filtering and SSP modules which have the higher surface Firewall filtered and not filtered number of entry packets diagram of the Firewall.

It can certainly be seen that, number of entry packets consists special software packet has SSP model with higher surface Firewall is used mostly and this helps to decrease the outer threats on network traffic [3].

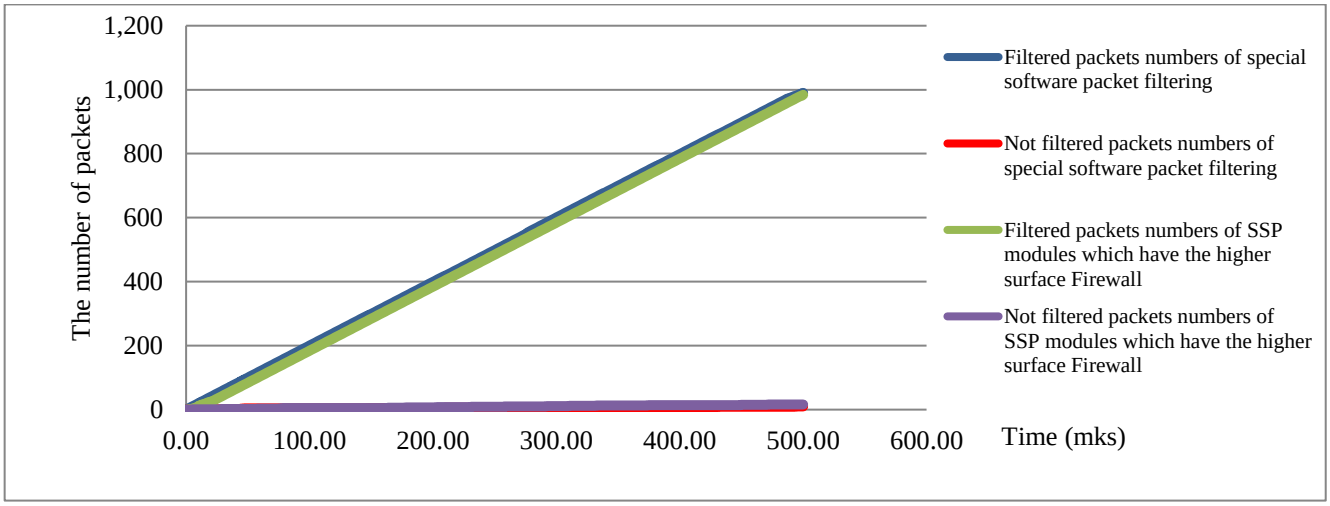

Fig.1.5. Special software packet filtering and SSP modules which have the higher surface Firewall and filtered and not filtered number of entry packets diagram of the Firewall.

IV. ASSESSMENT OF THE SPECIAL SOFTWARE PACKET FILTERING WITH OTHER FIREWALLS

Special software packet filtering for the different personal working with Firewalls for assessment we will look through the row value of the Firewall.

A = the main functions of the Firewall.

Here:

A_1 = Proportional scanning/filtering;

A_2 = Proportional blocking;

A_3 = blocking input/output ports;

A_4 = virtual private network (concealing IP and MAC addresses). Providing the higher level of the security.

A_5 = client-server architecture filtering.

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 4, Issue 10 , October 2017

B = the additional functions of the Firewall.

$$B = B_1, B_2, B_3, B_4, B_5, B_6, B_7, B_8$$

Here, B_1 = Anti-phishing.
B_2 = Antivirus.
B_3 = Anti spy.
B_4 = Monitoring of the current connections.
B_5 = Identifying suspicious packets
B_6 = Incidence journal
B_7 = Controlling the pages which the network can use.
C = Compatibility of the Firewall.

$$C = C_1, C_2, C_3, C_4, C_5$$

Here, C_1 = Windows 10;
C_2 = Windows 8;
C_3 = Windows 7;
C_4 = Windows Vista;
C_5 = Windows XP.

Table 1.3 shows that special software packet filtering in different personal Firewalls and the comparative analysis on that [4]. Fig.1.6 illustrates histogram of that comparative analysis.

Table 1.3: Special software packet filtering in different personal Firewalls and the comparative analysis of them

Private screen in networking / **Rank**		Total evaluation	Assessment	Special software packet filtering	Comodo Firewall	Avast Internet Security	AVG Internet Security	Outpost Firewall Pro	Zone Alarm Free Firewall	Kerio Winroute Firewall
A	A_1	**20**	**3**	3	3	3	3	3	3	3
	A_2		**2**	2	2	2	2	2	2	2
	A_3		**4**	4	4	4	4	4	4	4
	A_4		**5**	5	5	0	0	0	0	5
	A_5		**6**	6	0	0	0	0	0	0
Total				**20**	**14**	**9**	**9**	**9**	**9**	**14**
B	B_1	**24**	**3**	0	3	3	3	0	3	3
	B_2		**3**	3	3	3	3	0	3	3
	B_3		**3**	0	3	3	3	0	3	0
	B_4		**4**	4	0	0	0	0	0	0
	B_5		**4**	4	0	0	4	4	4	4
	B_6		**3**	3	3	3	3	3	3	3
	B_7		**4**	4	4	0	0	0	0	0
Total				**18**	**16**	**12**	**16**	**7**	**16**	**13**
C	C_1	**15**	**3**	3	3	3	3	3	3	3
	C_2		**3**	3	3	3	3	3	3	3
	C_3		**3**	3	3	3	3	3	3	3
	C_4		**3**	3	3	3	3	3	3	3
	C_5		**3**	3	3	3	3	3	3	3
Total				**15**	**15**	**15**	**15**	**15**	**15**	**15**

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 4, Issue 10 , October 2017

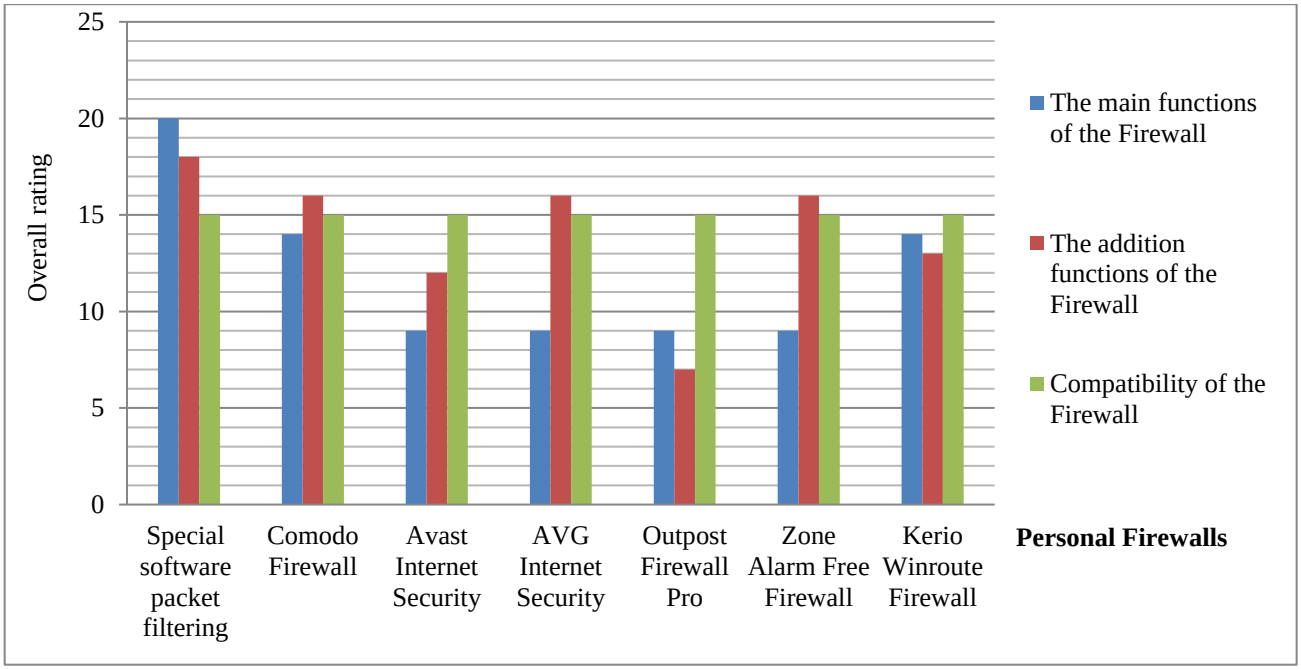

Fig.1.6. Special software packet filtering in different Firewalls assessment of that work and histogram of that comparative analysis

Here:

A_U – Effectiveness relation with different functions of Firewalls.

$$A_U = A_1 + A_2 + A_3 + A_4 + A_5$$

B_U – Effectiveness relation with different additional functions of Firewalls:

$$B_U = B_1 + B_2 + B_3 + B_4 + B_5 + B_6 + B_7$$

C_U – Effectiveness relation in several Firewalls and suitability to each other and relation to functions:

$$C_U = C_1 + C_2 + C_3 + C_4 + C_5$$

S – Overall productivity

$$S = A_U + B_U + C_U$$

S_{max} – Maximal productivity:

$$S_{max} = A_{max} + B_{max} + C_{max}$$

According to the result of the 1.3 table:

$$S_{max} = A_{max} + B_{max} + C_{max} = 20 + 24 + 15 = 59$$

$U(\%)$ – productivity:

$$U = \frac{S}{S_{max}} \cdot 100\%$$

In table 1.4 shows the working effectiveness assessment of special software packet filtering in different personal Firewalls [5,6]. Fig.1.7 shows that histogram of the comparative analysis.

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 4, Issue 10 , October 2017

Table 1.4: The result of effectiveness assessment of special software packet filtering in different personal Firewalls

Private screen in networking / Rank	Special software packet filtering	Comodo Firewall	Avast Internet Security	AVG Internet Security	Outpost Firewall Pro	Zone Alarm Free Firewall	Kerio Winroute Firewall
S	53	45	36	40	31	40	42
S_{max}	59	59	59	59	59	59	59
$U(\%)$	89,830	76,271	61,016	67,796	52,542	67,796	71,186

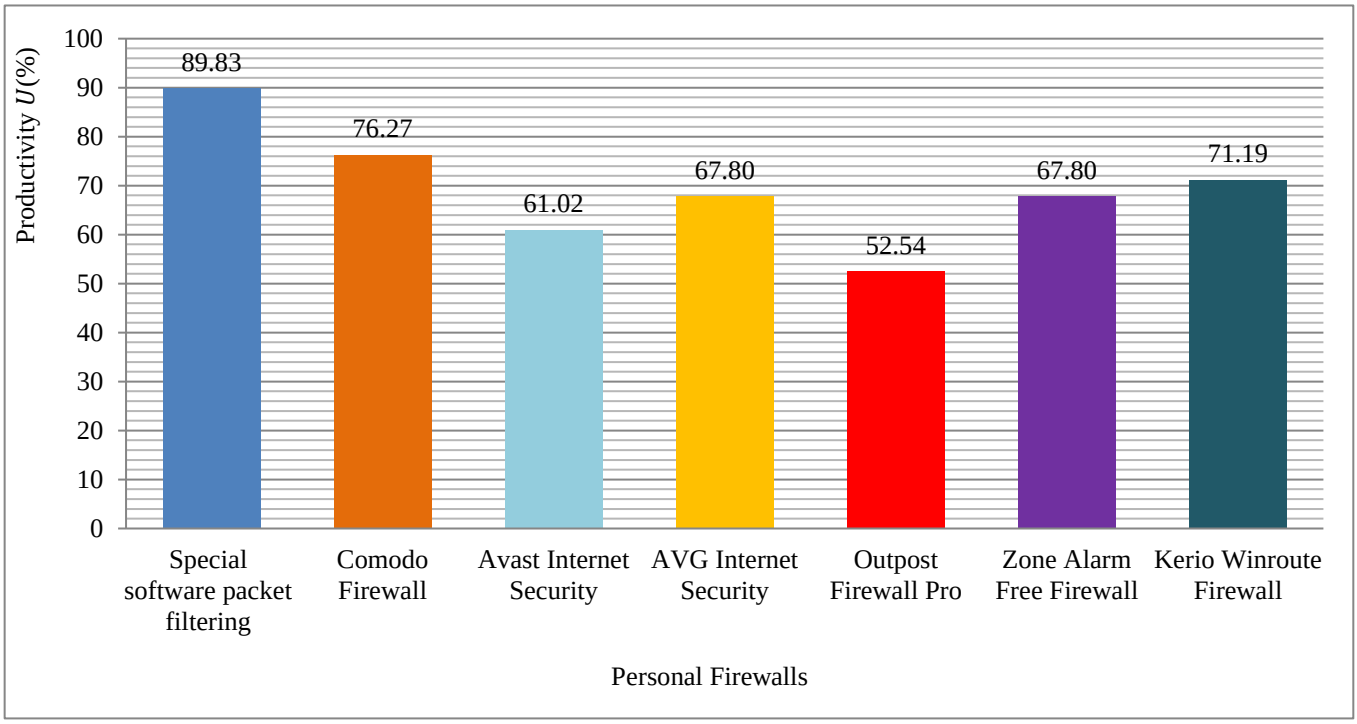

Fig.1.7. The result of effectiveness assessment of special software packet filtering in different personal Firewalls.

V. CONCLUSION

The customized special software packet filtering provides a high level of protection for network traffic over external influences and allows you to control traffic filtering on remote PCs that are not available on any individual Firewalls. Moreover, software packet filtering special has effectiveness of 13 % from the most effective assessment of productivity Comodo Firewall and the least effective assessment is Outpost Firewall Pro has 37 % productivity of the personal Firewalls.

REFERENCES

[1]. Behrouz A. Forouzan. Data communications and networking fourth edition. Publisher: McGraw – Hill. 2007. pp.1171.
[2]. Gulomov Sh.R., Nasrullaev N.B., Yusupov B.K. Tools of protection functioning info communication networks from external attacks. "TUIT xabarlari" journal. № 4(32) 2014, pp.16-24.
[3]. Gulomov Sh.R., Abdurakhmanov A.A., Nasrullaev N.B. Design Method and Monitoring Special Traffic Filtering under Developing «Electronic Government». International Journal of Emerging Technology & Advanced Engineering (ISSN 2250-2459, ISO 9001:2008 Certified Journal), Volume 5, Issue 1, January, 2015, India, pp.66-73.
[4]. Karimov M.M., Ganiev A.A., Gulomov Sh.R. Settings firewalls to implement special filtering mode. Vestnik TSTU, 2015, №1 (89), pp.14-21.
[5]. Karimov M.M., Gulomov Sh.R., Yusupov B.K. Approach Development Accelerate of Process Special Traffic Filtering. Journal of Computer and Communications, Vol.3 No.9, September 2015, USA pp.68-82.
[6]. Gulomov Sh.R., Rakhmanova G.S., Boymurodov B.E. Ensuring Secure Info-Communication Networks Based on the Special Filtering Mode. International Journal of Engineering Innovation & Research Volume 5, Issue 1, ISSN: 2277 – 5668, 2016, India, pp.16-23.