International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-11, September 2019

Methods for Applying of Scheme of Packet Filtering Rules

Yusupov Bakhodir, Nasrullaev Nurbek, Zokirov Odiljon

Abstract: ***This article is devoted to research methods for applying of scheme of packet filtering rules. The scheme of the Firewall is developed on corporate network to allow protect the network system from information security threat. Use of Firewall in different mode of protection in the corporate networks is given which is accessed to segment information resources under the administrator's rules. Filtering packets rule is worked out according to the state of the virtual connection that the process moving of packets is determined by flags and sequence numbers of head IP addresses. The system logging log is designed to record a message about events that involve firewall operating system management activities and events that are fraught with an intersection-related event log. Consequently, the offered rules of packet filtering protected the network traffic from unwanted action. Furthermore, the rules of packet filtering is formed, allowing to observe and management access to resource users on the Web content.***

Index Terms: Firewall, TCP/IP protocol, network traffic filtering, virtual connection, filtering rule, flood-related attacks, Network Time Protocol (NTP), balancing mode, full control.

I. INTRODUCTION

Under increase the vulnerabilities information security on computer network and the development of modern technologies put new requirements to network security and security systems. The data transmission through the Internet indicates the relevance of information security issues such as confidentiality, integrity and availability of information. All processes related to unrestricted change and unrestricted use of information indicate that organizational and legal methods of protection should also be used together with hardware and software solutions. However, the development of network technologies, the emergence of new interactive applications, and the emergence of a large number of network resources, lead to the emergence of new issues related to the limitation of access to certain resources to protect against unauthorized access to information using remote access control systems.

II. TYPES OF USING FIREWALLS

Therefore, the development of tools to limit access to network resources is crucial for software and hardware utilization. Typical wide-bandwidth limitations are multi-channel firewall on the form of software or software intended for network traffic control based on packet filtering in accordance with the rules set by network administrators. Effective use of an interactive display involves the use of firewall for secure functioning and the formation of filtering rules that take into account security policy requirements [1].

There are several schemes for packet filtering

1) An ordinary scheme of the firewall for the protection of the corporate network is given in Figure 1.

The on-firewall is placed between the corporate network routers and the external routers where their addresses do not change. Interface firewall saves internal network and local network routers from external threats.

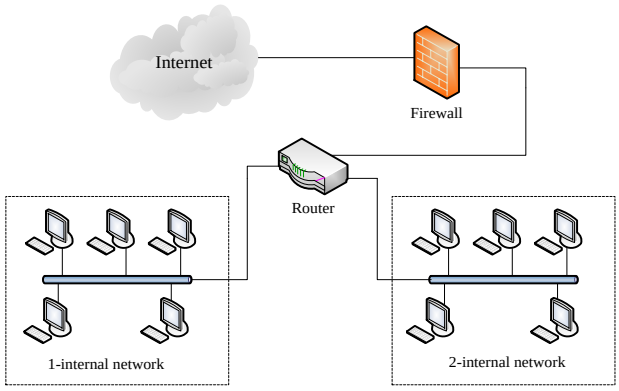

Figure 1 - An ordinary scheme of the Firewall to protect the corporate network

The on-firewall will display an external access permissions policy for internal network users as needed [2-3].

2) The demilitarized zone (DMZ) firewall diagram is given in Figure 2.

As you know, DMZ-networks will be able to build a protected area, which will be located in the internal segment of the enterprise's local network. The capabilities of the DMZ cannot be directly or indirectly accessible to the internal or external network and can only be accessed in accordance with the predefined rules of the firewall. The demilitarized zone usually serves to prevent the use of external networks, because a special zone of all services requiring external access is removed from the local network. The DMZ part of a local network is designed for systems and resources that are protected from internal and external threats, but must be accessed internally or externally [4]. The reason is that such systems and resources can never be frozen. However, the violation of these systems should not necessarily indicate the availability of other external systems.

Manuscript published on 30 September 2019.
*Correspondence Author(s)
Yusupov Bakhodir Providing Information Security Department, Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Tashkent, Uzbekistan
Nasrullaev Nurbek, Providing Information Security Department, Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Tashkent, Uzbekistan
Zokirov Odil, Providing Information Security Department, Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Tashkent, Uzbekistan

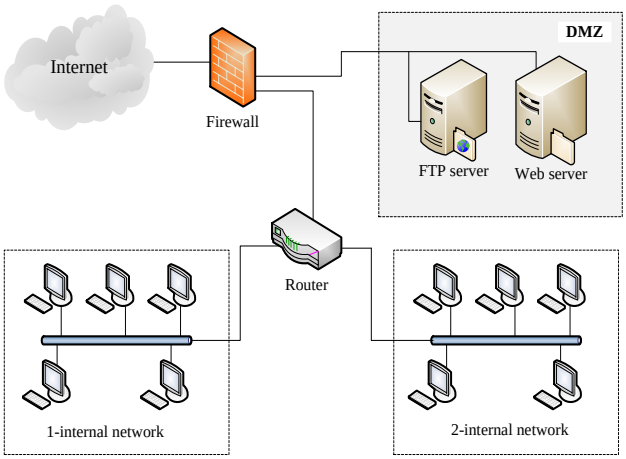

Figure 2 - Demilitarized Regional (DMZ) Firewall Diagram

The offered scheme includes three or more interfaces. The internal network and the DMZ will be disconnected. Interfaces are internal network, DMZ resources, routers protect against external threats, execute external users' access to external resources and DMZ resources [4]-[5].

Figures 1 and 2 shall have equal access to the Firewall interfaces.

3 and 4 figures are analogous to 1 and 2, but they use Firewall functions, such as network address transmissions (NAT). In this case, the firewall performs the role of routers, the internal network has "private" - "closed" network addresses, and DMZ resources use simple "public" addresses [6]-[7]. The scheme of Firewall layout based on NAT mode and the scheme of Firewall with DMZ zone on NAT mode are shown in Figures 3 and 4.

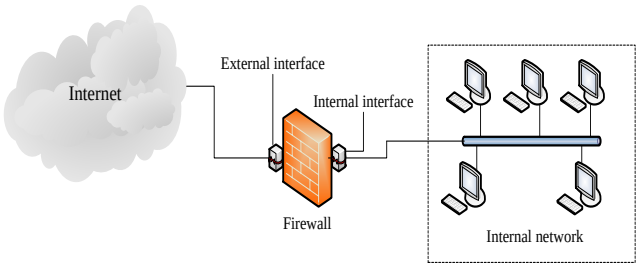

Figure 3 - Scheme of Firewall layout based on NAT mode

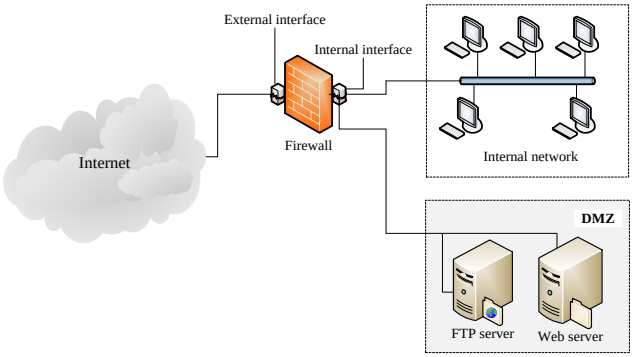

Figure 4 - Scheme of Firewall with DMZ zone on NAT mode

III. USE OF FIREWALL IN DIFFERENT SECURITY MODES

Filtering network traffic.

The packet filtering is focused on Ethernet (10/100/1000 Mbit/s) wired technology and TCP/IP protocols, or IPX/SPX. Firewall divides the local area network into different security-grade segments and restricts access to segment information resources under the administrator's rules. In the normal case, the firewall separates the network from protected and open segments.

Firewall performance can be divided into three main modes [8]-[9]:

1) Packet filtering mode;

2) Session control mode, State Inspection, including the state of the virtual connection;

3) Applied layer data control mode.

In line with the generally accepted classification, it means that the firewall can act as a packet filter, a status analyzer.

IV. PACKET FILTERING MODE

Segment filtering performs then independent filtering (deleting/deactivating) of each packet between segments separated by rules set by the administrator in interactive screen packet filtering mode. Packet filtering is an indispensable part of a complex categorical firewall that forms the basis of any firewall [10].

The packet filtering rule rules allow you to:

• Protection against unauthorized use of the dedicated local area network and its subscribers on external network segments;

• Manage access rights of local network subscribers protected by external network resources.

Firewall performs packet filtering over packet headers on multiple layers of interaction [11]. The following categories of packets will be selected in accordance with the rules given:

• Ethernet cams;
• ARP and RARP packets;
• IPv4 packets;
• ICMP packets;
• UDP diagrams;
• TCP segments;
• IPX packets.

Other packaging headings are filtered without analysis.

V. FILTERING RULES AND ORDER PROCESSING PACKETS

Network traffic filtering could have taken place at different levels of the network. Each layer corresponds to a specific filtering group [12]-[13]. The filtering rules for each group are given in the header parameters of the protocol packets that correspond to the current layer link. As a result, packet filtering is performed on the basis data that is part of the packet header on the firewall.

The following groups of rules are available on the firewall:

• MAC rule - rules of filtering on the Ethernet cadre layer;
• ARP rule - Rules for filtering ARP and RARP packets;
• IP rule - IPv4 protocol packet filtering rules. The IP rules contain additional packets for processing TCP, UDP and ICMP packets. This group also includes specific IP-rules for short network attacks, blocking subscribers, and so on;
• IPX rule - IPX packet filtering rules;

Retrieval Number: I8206078919/19©BEIESP
DOI: 10.35940/ijitee.I8206.0981119
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

• AP rule - Practical layer filtering rules [13].

When creating rules, special structures such as "VLAN Groups" and "Time Span" are used to allow a rule to be bound to a specific time interval and a VLAN identifier.

Any filtering rule will look like this:

IF (rule parameter) - THEN (rule behavior), when the packet header corresponds to the rule policy, the rule must be applied to the packet. The following actions shall be permitted on the packet [14]:

• "conduction" - transmits the packet filtering interface or the next layer of filtering (for MAC rules);

• "pass" - extends the packet to the outbound filtering interface (in the firewall) by passing the next filtering levels;

• "Drop" - block the next packet.

In packet filtering mode, packets are processed in step 2:

1) Filtering by MAC-rules;

2) Filtering by rules of the next layer (ARP, IP and IPX rules).

First of all, each packet received by the filter interface of the firewall is processed on the Ethernet cadres layer according to the filtering MAC rules. If a packet wiping policy is applied, then the packet will stop running without the wrapping. If a packet is used for the packet convention, then the final decision on the transfer or removal of the packet is given to the next level of filtering. If a packet sender policy is applied, then the packet filtering procedure will be aborted and the packet will be issued to the outgoing interface [15].

At the next level of filtering, one of the corresponding cases of ARP, IP or IPX is applied to the packet, depending on the category of protocols that are configured in the current Ethernet frame.

VI. FILTERING PACKETS ACCORDING TO THE STATE OF THE VIRTUAL CONNECTION

By default, when filtering traffic over the state of the virtual connection, an additional check is made that matches the appropriate virtual connection state for each packet. On a firewall, this filtering mode is called the session management mode [16]. The interactive display supports the following session views:

• Virtual TCP connection;

• Virtual UDP access - a binary exchange of UDP packets between a client and a server, an ICMP-message exchange with an "Inbox" and "Inactive Response" (ping session).

In this mode, the firewall consistency of packet sharing between the client and the server that includes the IP address, traffic flow protocol, sender and recipient port numbers, flags, sequence and confirmation numbers, query IDs, and so on [17].

The session management mode provides the following filtering preferences.

It is sufficient to create one rule for each virtual connection (session). There is no need to show the "reverse" rule [17]. Thus, when using this filtering mode, the above IP rules table may not contain some rules:

• Checking the authenticity of the sessions, not just the heading of separate packets.

• Only the client port required for the current session is automatically opened;

• Provide control over practical layer information;

• The NAT mode will be used;

• Flood-related attacks and TCP protocols are blocked by blocking sequence numbers and flags incorrectly;

• The full screening of all filtering rules will only increase the bandwidth capacity of the session because only the first session of the session is available and all other packets open session will be tested in accordance with the session vectors [18]. Figure 5 shows the increased bandwidth capacity of the firewall in line with the session vector.

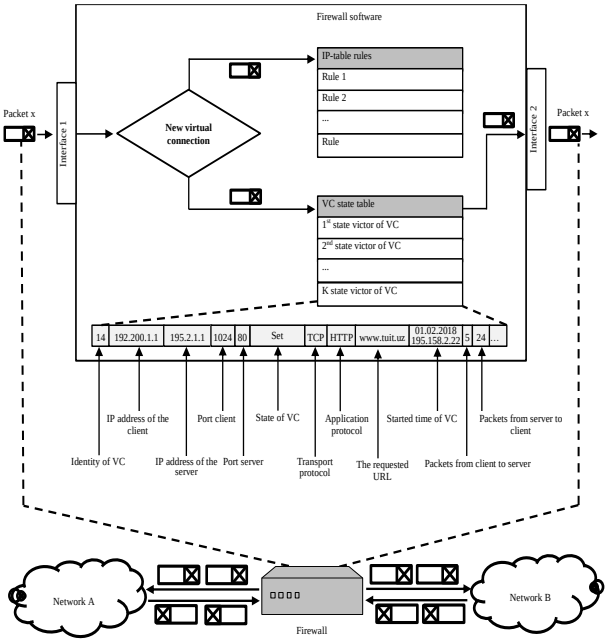

Figure 5 - Increased bandwidth capacity of the firewall in accordance wit

VII. OPERATION LEVEL CONTROL MODE

This applies to "practical" AP rules. Any desired protocol can be filtered by the following parameters:

• Practical protocol name or number (in RFC 1700). The protocol identification for HTTP, SMTP, FTP, Telnet protocols, regardless of port number [19].

• Optional ASCII array of 250 characters long;

• Optional binary information up to 16 bytes.

Additional protocol filtering options are provided for some protocols:

For HTTP protocol:

• Fragment or username of the hostname;

• HTTP request;

• File fragment or name requested from the HTTP server [20].

For FTP protocol:

• The username and password of the FTP server;

• File or fragment file requested from the FTP server;

• FTP protocol command.

For SMTP protocol:

• A fragment or email address of the sender and receiver.

For enterprise database management system protocols:

• SQL queries or query fragments.

The following AP rules explain the filtering based on application layer information. (Practical rules are in the CLI command line interface format)

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

ap: 30 action = drop protocol = SMTP data = information_name

The Rule 30 application prohibits the transmission of messages from the “Information stream” row. Figure 6 illustrates the removal of the packet of SMTP sessions from the "Information Stream" row [20].

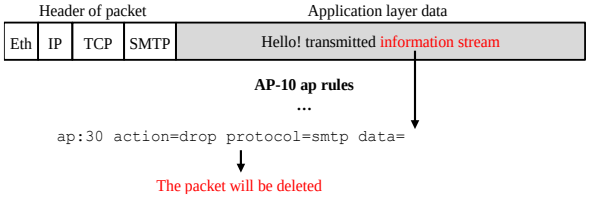

Figure 6 - Blocking outbidding of the “Information stream” row

Version 40 does not block access to sites www.olx.uz, www.daryo.uz and kun.uz.

ap: 40 action = drop protocol = http host = www. olx.uz, www.daryo.uz, * .kun.uz

from-client

Forbidden to send files to the ftp-server, which uses a 50-bit rule

ap: 50 action = drop protocol = ftp cmd = put user = elegant

Reflection of traffic

There are three modes of Firewall:

1) in: The following interface only copies inbound packets;

2) out: The next interface only copies of outgoing packets;

3) all: copies of incoming and outgoing packets will be sent to the next interface, all traffic through the current interface.

The mirror function works in all the Firewall in all filtering modes. In this case, the Outline (Eth0) and Internal (Eth1) interfaces are not supported in the network address transmissions mode, the interface of interfaces, that is, the interfaces to which the packets are copied [20].

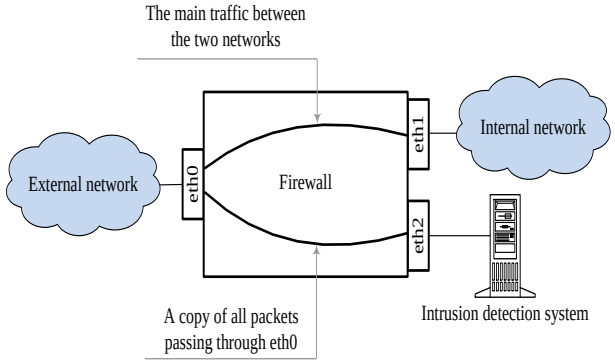

Figure 7 - Traffic mirroring function

Recording of events and traffic on the firewall

It has the capability to record a variety of information that is taking place during the firewall process. The following the registration logs refer to:

1) the registration logs of event;

2) the registration logs of traffic;

3) the registration logs of system information;

The registration logs of event

Event IDs include the change in the status, settings, or profile of the onboard firewall software that has occurred as a result of administrative actions or errors in the operation of a firewall. The event is divided into the following three classes:

1) message - is intended for informing the administrator about events that do not violate the normal operation of the on firewall software [21];

2) warning - is intended for informing the administrator of events that are not logical in the firewall, which do not interfere with the normal operation of the on firewall software;

3) errors are intended to inform the administrator of any interruptions that may affect the normal operation of the onboard firewall software and require special processing operations.

The registration logs of traffic

When registering traffic on a network interface, the following functions are understood:

1) registration of packets;

2) recording sessions.

Registration of packets

Package registration is carried out when the following conditions are met:

1) the parameters of recording of the systems of systematic systems of registration of the firewall are in working condition;

2) at least one of the rules for packaging processing records the packet. Firewall takes several levels of filtering while packaging.

Saving sessions

Session registration is carried out regardless of the parameters of the systematic system packet registration, following conditions are fulfilled:

1) Firewall session management or network address transcoding;

2) If the session has at least one packet of IP rules or rules, this rule implies recording the session.

Events include [21]-[22]:

• Events related to the disconnection and start-up of the system-based system on the firewall;

• Events related to writing or reading a system;

• Events related to the operation of a firewall when there is no possibility to record information from an event log on firewall;

• Time synchronization on the NTP (Network Time Protocol) protocol;

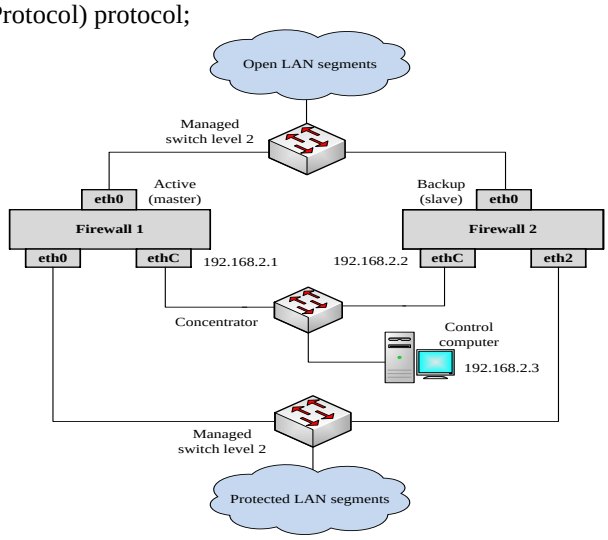

Figure 8 - General scheme of high-efficiency filtering system

Retrieval Number: I8206078919/19©BEIESP
DOI: 10.35940/ijitee.I8206.0981119
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

• Downloading account logs on the FTP server;
• A message indicating that the packet has been received with the given parameters;
• Flood-attack detection and blockage notification.

Use backup mode to improve reliability of the on firewall High-performance filtering system based on firewall [22].

The overall scheme for the high efficiency filtering system is shown in Figure 8.

1) "Active / reserve" mode

In Active / Backup mode, two firewalls are parallel to the local network segment and act as the only logical filtering system [28]-[29]. Firewall will be active and filter the traffic, the second will be backup and will work in the "backup" mode without having to accept all the filtering interface packets. Exchange and synchronization between active and backup firewall can be performed via Ethernet interfaces (ethC), which can be used to detect workflow modes and interruptions.

An interactive filtering logic system, if this firewall duplicates an active packet filter, the firewall will ensure the smooth operation of the filtering system at any disconnection of active hardware or software components.

2) Balancing mode

In a highly effective filtering system, balancing is based on the scheme of combining two physical channels between the switchgears into one logical channel known as trunk. In this system, the two firewalls are connected to the disconnection of the physical channels between the switchgear and act as a single logic filtering system. In this case, both devices on the firewall are active and traffic filtering [30]. The distribution of the load on the physical channels is performed by a set of switch that is properly adjusted. Switching between work modes is done via Ethernet interfaces, which control communication and synchronization between firewall to detect hardware and software failures.

3) Spanning Tree Mode

The highly efficient system of Spanning Tree mode is based on two circuit breakers with two physical channels. In this case, the switch determines whether there is a reserve connection and block the appropriate ports. In this system, the dual firewall is connected to the disconnection of physical channels between the switch and acts as a single logic filtering system. Both firewalls are also active, but only one device filters traffic due to a single physical channel at a time. The channel switching is made by the switch [31]-[33].

The filtering logic built on the firewall ensures that the filtering process stopped for less than 10 seconds in the previous volume due to hardware or software interruption. To ensure high-efficiency mode, both products must have the same configuration settings as the backup module and control interface addresses.

The high-performance scheme envisages filtering rules and configuration synchronization between interlaced firewall included in the scheme [26]. Synchronization can be done on an Administrator's request asynchronous and can only be used and navigated by various firewalls.

Figure 9 shows the scheme of management of firewall. Depending on the type of managed computer connection, the administrator will be able to access the WEB-Interface management or the toolkit interface [26]-[27]. The access level through the team interface is high. Firewall settings are achieved by filling out the Web-Interface form in dialog boxes or by passing commands in teams.

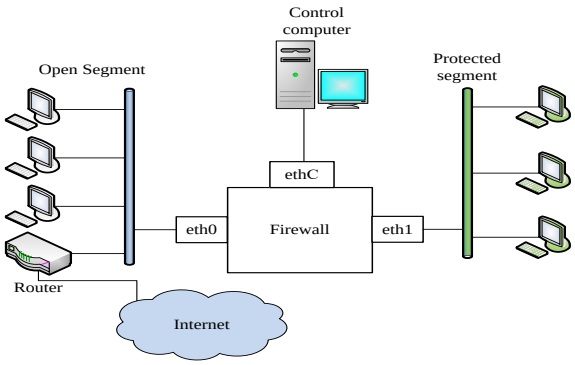

Figure 9 - The scheme of management of firewall

The Administrator setup process has the following capabilities:

• Manage user rights and lists that are allowed to manage the firewall;
• Full control over firewall modes and devices;
• Editing and filing rules;
• Enter any parameters of device operation;
• Registering a firewall saving a systemized system and monitoring your account files.

VIII. CONCLUSION

To summarize, it should be noted that, based on outcome of analysis, schemes of Firewall with automated setting of rules of packet filtering allow to minimize the impact at implementation of attacks associated with overflow is offered. As well, the offered schemes allow decrease information security risks and the number of network anomalies is improved.

REFERENCES

1. G Divya, C J Kavitha Priya and G Kowselya, "Effective Firewall implementation in cloud over virtual environment using speck Firewall restriction", International Journal of Electrical and Electronic Engineering & Telecommunications, Vol. 1, No. 1, pp. 324-328, March 2015.
2. Karimov M. M. Approach Development Accelerate of Process Special Traffic Filtering // Journal of Computer and Communications. USA, 2015. Volume 3. P.68-82.
3. A. Bremler-Barr, Y. Harchol, D. Hay, Y. Koral. Deep packet inspection as a service. In CoNEXT, 2014. - P.271-282.
4. Canini M., Li W., MooreA. W., BollaR. GTVS: Boosting the collection of application traffic ground truth // Lecture Notes Comput. Sci. V.5537. 2009. - P.54-63.
5. Gobika S, Janane T K, Mohana Priya U and C Gnanaprakasam. Detection monitoring of secure packet transfer over network traffic. Journal of Electrical and Electronic Engineering & Telecommunications. Special Issue, Vol. 1, No. 1, March 2015. -P.319-322.
6. Rakhmanova G.S., Boymurodov B.E. Ensuring Se-cure Info-Communication Networks Based on the Special Filtering Mode. International Journal of Engineering Innovation & Research. Volume 5, Issue 1, 2016, ISSN: 2277 –5668, India, -P.16-23.
7. Karimov M.M., Ganiev A.A. Models of Network Processes for Describing Operation of Network Protection Tools // 4th International conference on application of information and communication technology and statistics in economy and education (ICAICTSEE – 2014). University of National and World Economy Sofia. - Bulgaria, October 24 - 25th 2014. - P.226-235.

8. Ma, T., Zhou, Z., Antoniou, C. Dynamic factor model for network traffic state forecast. 2018. Transportation Research Part B: Methodological, 118, pp. 281-317. DOI: 10.1016/j.trb.2018.10. 018
9. Vikash C Pandey, Sateesh K Peddoju and Prachi S Deshpande. A statistical and distributed packet filter against DDoS attacks in Cloud environment. Indian Academy of Sciences. Sadhana 2018. 43:32-P.2-9.
10. William Stallings. Network security essentials: Applications and Standards Fourth edition. Prentice Hall, USA, 2011. - P.417.
11. Ganiev Abdukhalil Abdujalilovich. Methods and models of protecting computer networks from un-wanted network traffic International. Journal of Engineering & Technology, Indexed in Scopus. Vol 7 No 4 2018. Science Publishing Corporation, RAK Free Trade Zone, RAK FTZ Business Park, Business Centre 4, Al Mamourah Area, P.O. Box: 487447, UAE, – P.2541-2545.
12. William Stallings. Data and Computer Communications (10th Edition). International Edition, 2013. P.912.
13. LinY-D., LuCh-N., LaiY- Ch., etal. Application classification using packet size distribution and port association // J. Network Computer Appl. 2009. V.32. - P.1023-1030.
14. Abdurakhmanov A.A., Nasrullaev N.B. Design Method and Monitoring Special Traffic Filtering under Developing «Electronic Government» // International Journal of Emerging Technology & Advanced Engineering. - India, 2015. - Volume 5. - P.66-73.
15. Zouheir Trabelsi, Liren Zhang, and Safaa Zeidan. Firewall Packet Filtering Optimization Using Statistical Traffic Awareness Test. Springer-Verlag Berlin Heidelberg. ICICS 2012, LNCS 7618, pp. 81–92, 2012.
16. Nasrullayev Nurbek Bakhtiyorovich. Method for security monitoring and special filtering traffic mode in info communication systems // 2016 International Conference on Information Science and Communications Technologies (ICISCT). Tashkent University of Information Technologies. Tashkent, Uzbekistan. Applications, Trends and Opportunities 2nd, 3rd and 4th of November 2016. 1-6. 10. 1109/ICISCT. 2016. 7777409.
17. Bhed Bahadur Bista, "Improving Message Deliverability of Opportunistic Network Protocols," International Journal of Electrical and Electronic Engineering & Telecommunications, Doi: 10.18178/ijeetc.180402.
18. Lindgren, A. Doria, E. Davies, and S. Grasic. (August 2012). Probabilistic routing protocol for intermittently connected networks. [Online]. Available: http://www.rfceditor.org/rfc/rfc669 3.txt
19. M. Alajeely, R. Doss, and A. Ahmad, “Routing protocols in opportunistic networks – A Survey,” IETE Technical Review, vol. 0, no. 0, pp. 1–19, 2017.
20. L. Wan, F. Liu, Y. Chen, and H. Zhang, “Routing protocols for delay tolerant networks: survey and performance evaluation,” Int. Journal of Wireless & Mobile Networks, vol. 7, no. 3, pp. 55-69, June 2017.
21. Hao Yu, Ming-Xiang He and Hai-Chun Sun, 2009. The Design of Firewall in Mobile Phone Based on Cross-Layer Collaboration. Information Technology Journal, 8: 1049-1053.
22. Nazrulazhar Bahaman, Anton Satria Prabuwono, Mohd Zaki Mas`ud and Mohd Faizal Abdollah, 2012. Effectiveness of Security Tools to Anomalies on Tunneled Traffic. Information Technology Journal, 11: 191-199.
23. Zijian Cao and Xiaofeng Rong, 2013. A Mechanism of Intrusion Detection System Cooperating with Firewall. Information Technology Journal, 12: 6449-6454.
24. Khatua, M., Safavi, S.H., Cheung, N.-M. Sparse Laplacian Component Analysis for Internet Traffic Anomalies Detection. 2018. IEEE Transactions on Signal and Information Processing over Networks, 4 (4), № 8323201, pp. 697-711. DOI: 10.1109/TSIPN.2018.2818950.
25. Yang, Y.-Y., Yang, C.-T., Chen, S.-T., Cheng, W.-H., Jiang, F.-C. Implementation of network traffic monitor system with SDN. 2015. Proceedings - International Computer Software and Applications Conference, 3, № 7273440, pp. 631-634. DOI: 10.1109/COMPSAC.2015.149.
26. Cereia, M., Bertolotti, I.C., Durante, L., Valenzano, A. Latency evaluation of a firewall for industrial networks based on the Tofino Industrial Security Solution. 2014. 19th IEEE International Conference on Emerging Technologies and Factory Automation, ETFA, 2014. № 7005177, DOI: 10.1109/ETFA.2014.7005177
27. Meng, W., Li, W., Kwok, L.F. Towards Effective Trust-Based Packet Filtering in Collaborative Network Environments, 2017 IEEE Transactions on Network and Service Management, 14 (1), № 7843625, pp. 233-245. DOI: 10.1109/TNSM.2017.2664893.
28. Karimov M.M., Gulomov Sh.R. Analysis challenge protection of information from attacks and construction of a formal model for protecting network traffic. Tenth World Conference “Intelligent Systems for Industrial Automation”, WCIS-2018. Tashkent, Uzbekistan. P.84-88.
29. Gulomov Sh.R., Ganiev A.A. Methods and models of protecting computer networks from un-wanted network traffic. International Journal of Engineering & Technology, Indexed in Scopus. Vol 7 No 4 (2018) Science Publishing Corporation, RAK Free Trade Zone, RAK FTZ Business Park, Business Centre 4, Al Mamourah Area, P.O. Box: 487447, UAE, P.2541-2545.
30. Gulomov Sh.R., Mirzaeva M.B. Security analysis of “Internet of Things”. International conference on importance of information communication technologies in innovative development of sector of economy dedicated to the 1235th anniversary of the birth of Muhammad al-Khwarizmi, 2018, Tashkent Uzbekistan, P.464-467.
31. Gulomov Sh.R., Akhmedov K.S. The Experiment about Providing the Security of the Network with the base of the Special Filtering of the Traffic. International Journal of Advanced Research in Science, Engineering and Technology. India-2017. Volume 4, Issue 10. P.4679-4685.

AUTHORS PROFILE

Nasrullaev Nurbek Bakhtiyorovich was born in 1989 in Tashkent, Uzbekistan. He has more 45 scientific research papers in the field Cyber security and monitoring. Moreover he is parting in a lot of and national projects in variety sphere. Nowadays he works as assistant professor in the department of Providing information security, Tashkent University of Information technologies named after Muhammad al-Khwarizmi.

Yusupov Bakhodir senior teacher was born in July 13, 1988 in Yakkabog region, the Republic of Uzbekistan. In 2012 graduated «Information technology» faculty of Tashkent University of Information Technologies. Has more than 60 published scientific works in the form of articles, journals, theses and tutorials in sphere Computer networks, security mobile systems, malware and as well Cyber Security. Currently works of the department «Providing Information Security» at the Tashkent University of Information Technologies named after Muhammad al-Khwarizmi.

Zokirov Odiljon Yoqubjon ugli Was born February 13, 1992 year in Tashkent city, Republic of Uzbekistan. In 2015 graduated “Computer engineering” faculty of Tashkent University of Information Technologies. Has more 20 published scientific works in the form of articles, journals, theses and tutorials. Currently works of the department «Information Security» in Tashkent University of Information Technologies.