SYSTEMS ANALYSES OF NETWORK TRAFFIC FILTERING BASED ON THE SPECIFIED CRITERIA

M.M. Karimov, Sh.R. Gulomov [1], S.M. Sagatova [2]

[1]Department of Providing information security
Tashkent University of information technologies named after Muhammad al-Khwarizmi, Tashkent, Uzbekistan,
dr.mmkarimov@rambler.ru, sherhisor30@gmail.com

[2]Tashkent State Technical University named after Islam Karimov, Uzbekistan,
mssagatova@mail.ru

Abstract. *The article is investigated the structure of network traffic filtering and filtering algorithms, and traffic control. Set out the structure of software and hardware tools, algorithms of filtering incoming and outgoing traffic, algorithms control integrity and authenticity of updates, provides a conceptual scheme of the server-side database and the scheme to build a dialogue with the system administrator network traffic filtering on the specified criteria.*

Keywords: *Information society, hardware, software, criteria, multi-level, traffic filtering, back-end, front-end, out coming http-traffic filtering, incoming http-traffic filtering, blacklist, availability, scalability.*

1 Introduction

An integral part of the modern information society is the global internet. Nowadays it is difficult to work without the internet company employee progressive or advanced training. But the uncontrolled use of the internet poses a threat to the following: improper use of time and the destruction of moral standards and without that are not yet fully formed.

The trends are clear: network bandwidth continues to increase dramatically, network device applications, such as bridging, switching, routing, firewalls, network address translation, virtual private networks, intrusion detection, and prevention, multicast routing, traffic shaping, etc, are continuing to increase in complexity and the market continues to demand that separate applications be merged into one device. Network utilization continues to increase to match the available bandwidth, and single processors mixed with ASICs, and FPGAs do not meet these demands. So the logical solution to these requirements includes multiple processors. Additionally, a clean division of work effort and functionality is needed to use them. This requires decomposition and repackaging of functions, placing some in hardware and some in software so that the resulting system can scale and adapt more easily to handle increased loads and alternative functionalities and configurations.

2 Multi-level architecture of network traffic filtering on the specified criteria

Multi-level hardware and software architecture of servers used to provide scalability network filtering on the specified criteria that is able to prevent excessive network traffic and data servers, which is the server application. This architecture also allows you to distribute the functions of the server side application on the number of references to them.

Greatest level - the level of front-ends, which is responsible for the execution of the authorization database updates and versions of the client part of application, as well as the treatment system to the site through which the monitoring and remote system administration. If a user requests data statistics or change system settings to traffic filtering on the specified criteria, the server-level front-end proxy server to do any server-level back-ending, which determines the first two characters of the user's login. Thus, carried out between the server level addressing front-end and server-level back-end. In this case, if the server-level front-end overload in a given time, it forwards the request to the user to another less loaded server.

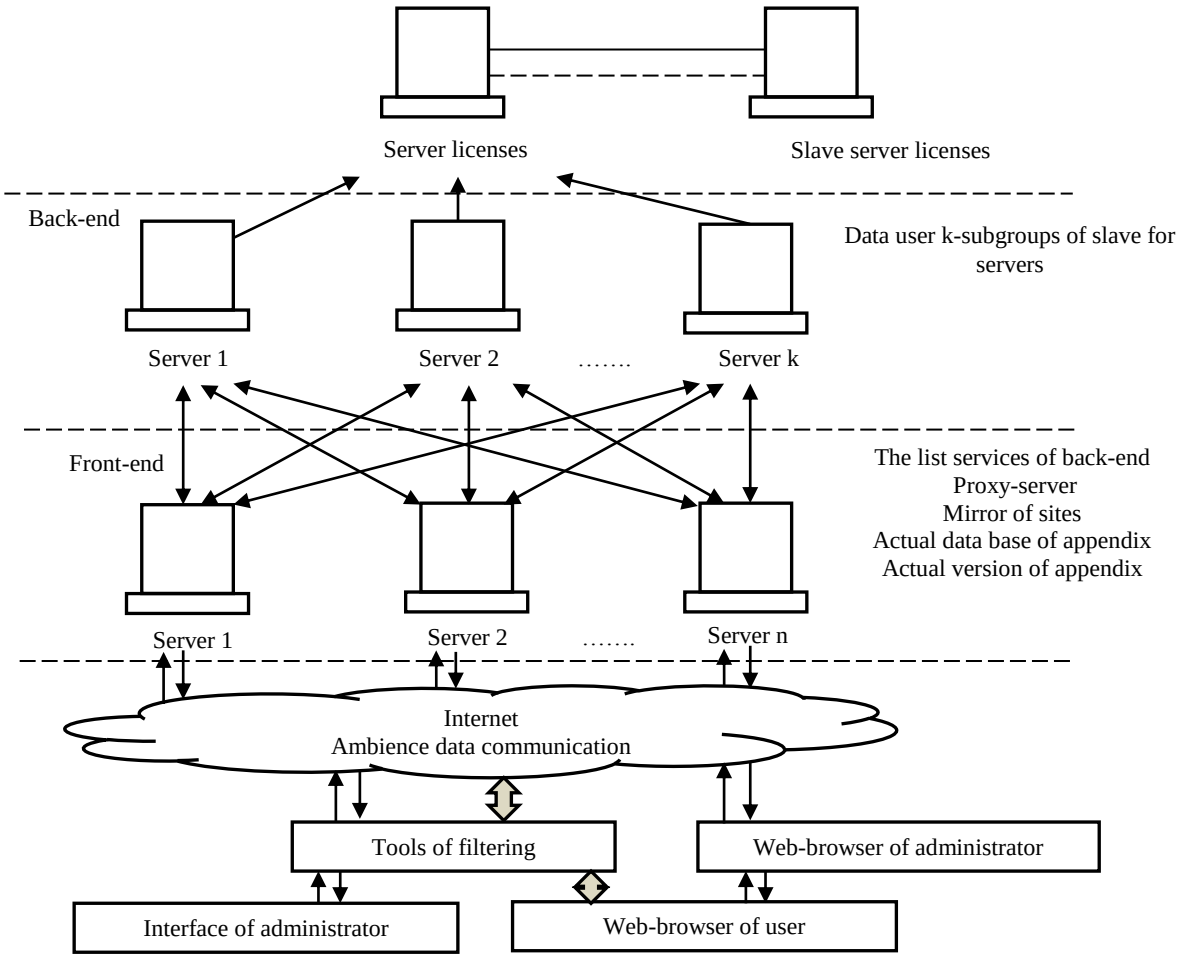

Fig.1 Multi-level hardware and software architecture of the network traffic filtering on the specified criteria

For fault tolerance, the server part of the system of traffic filtering on the specified criteria level servers back-end connected to the ring with each other (Figure 2), which allows you to duplicate a database of users each subgroup [1].

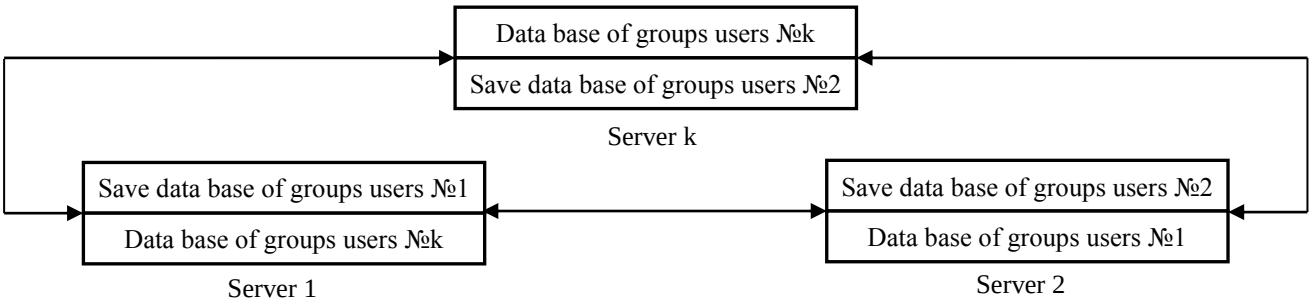

Fig.2 Connection server-level back-end

At last, the third level, multi-level server-side filtering system is the license server that stores information about user licenses and the server that makes it overlaps.

3 Algorithms of traffic filtering

The general scheme of the system of traffic filtering network traffic filtering on the specified criteria is presented Figure 3.

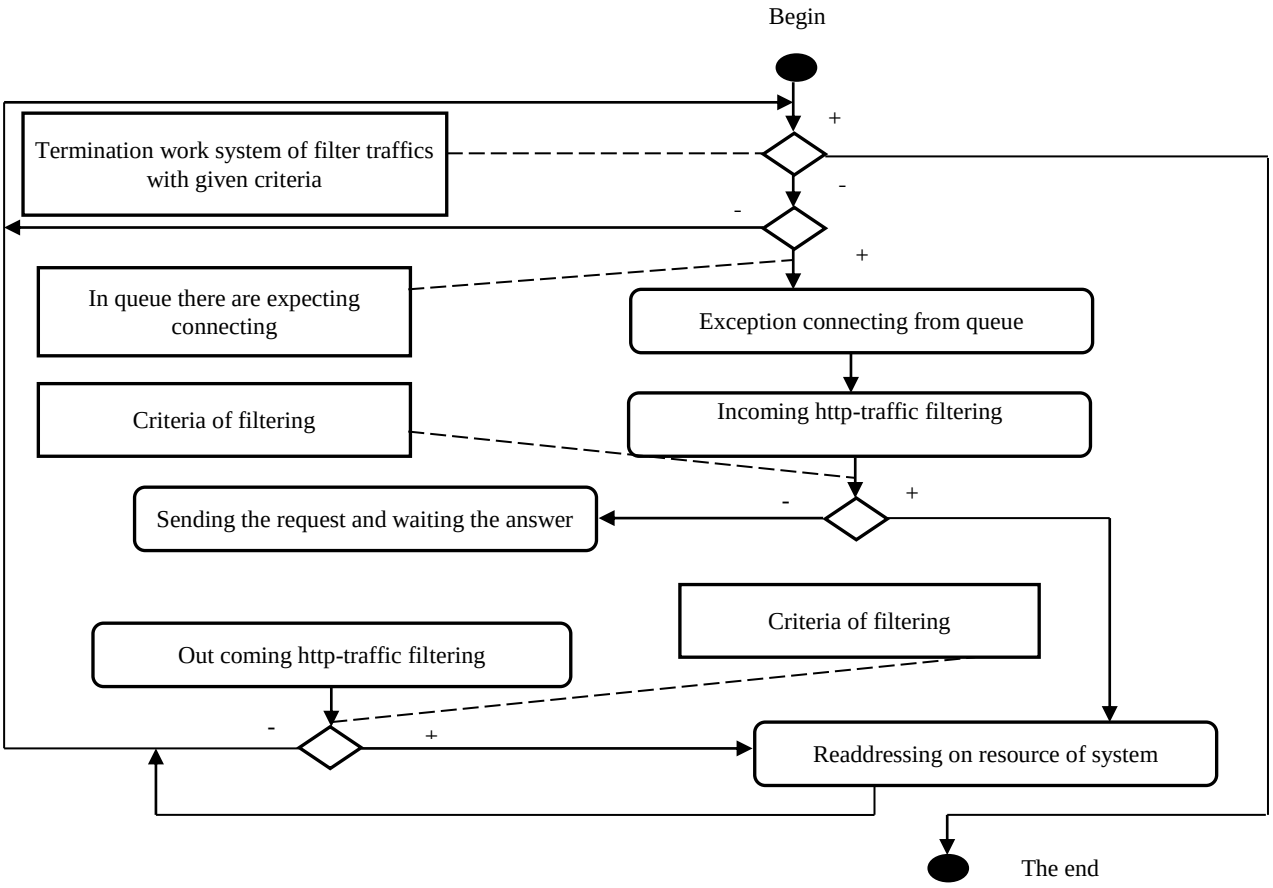

Fig.3 The general scheme of traffic filtering

System network traffic filtering on the specified criteria checks for pending connections queue, if any, we exclude the first of the queue. The analysis of the selected out coming traffic connection (Figure 4), the results of which it is determined whether or not the connection is contrary to criteria filtering system [2]. Unless contrary to the contents of the query on the specified criteria filtering system, then there is a «send request» and then waiting for a response, or is redirected to a system resource.

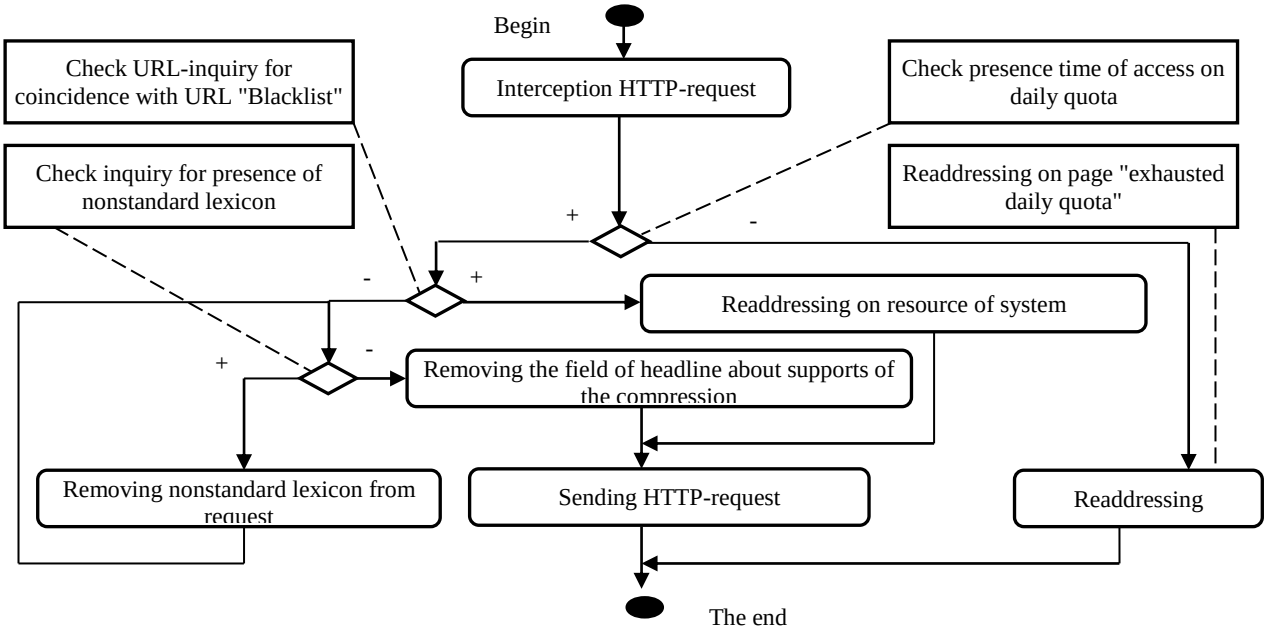

Fig.4 Scheme of out coming traffic filtering

Once the answer comes to the requested resource is a filtration of incoming http-traffic system of network traffic filtering on the specified criteria (Figure 5).

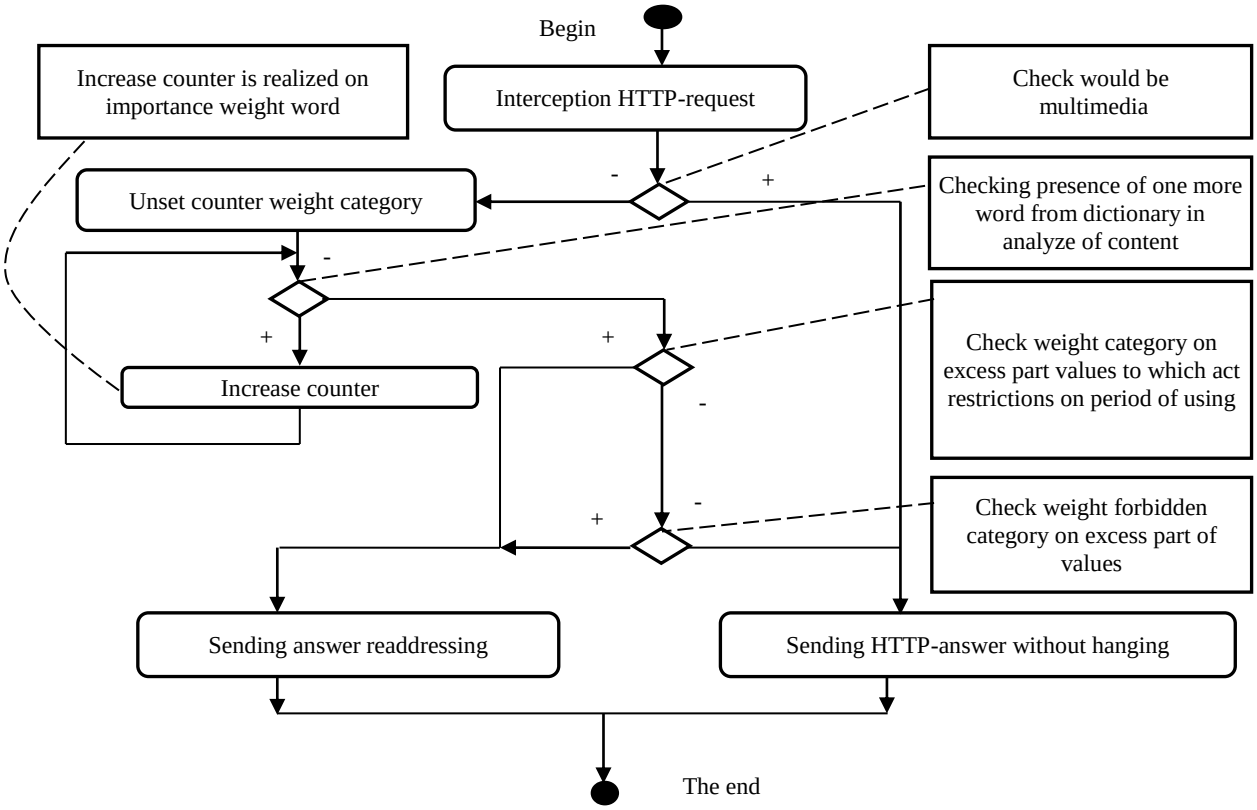

Fig.5 Scheme of incoming traffic filtering

According to the analysis of the incoming content is determined by its compliance with the specified filter on the specified criteria. If the content is found to be negative, it is redirected to a system resource, in the opposite case the content is delivered to the user application.

4 Conclusions

In conclusion it should be noted, that the multi-level hardware and software architecture allows high availability, scalability, as well as the implementation of the function for remote administration and monitoring system network traffic filtering.

References:

1. L. Braun, A. Didebulidze, N. Kammenhuber and G. Carle, “Comparing and Improving Current Packet Capturing Solutions based on Commodity Hardware”, Proceedings of the 10th ACM SIGCOMM conference on Internet measurement, (2010), pp. 206-217.

2. L. Deri and F. Fusco, “Exploiting commodity multi-core systems for network traffic analysis”, (2009).