2017 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM)

Functional Model of Firewall Application Layer Protection for WEB-Based Information Systems

Ozhiganova M., Kostyukov A., Maslova M.
Sevastopol State University
Sevastopol, Russia
mashechka-81@mail.ru

***Abstract*—The purpose of this article is to develop a functional model of an effective application layer firewall to protect the Web-based information systems. For successful achievement of this goal, analysis of the vulnerability of the application layer protocols and the existing means of solving these problems is performed in the paper. The technology and methods of implementation of protection means of the Web-oriented information systems at the application level are examined. The functional model of the application layer firewall for the Web-based information systems protection is designed. In the process of the research, the methods for implementation of protective means of the Web-oriented information systems at the application level were used.**

Keywords—functional model; information system; information security; application layer; firewall; protocol; server

I. INTRODUCTION

Modern trends in the development of web-based information systems show a lack of common secure coding standards that leads to errors in the software development and the emergence of serious vulnerabilities in Web services of the information systems, which use these applications. The situation is complicated by the fact that the vulnerable web application can easily be compromised without the use of special means, but using just a browser. Cybercrime is now becoming developed as never before because almost every company has a website on the Internet, and an attacker on the network could easily remain completely anonymous, if desired [1-3].

However, web-based information systems allow companies to provide more interaction with the real potential clients and improve internal corporate activities forcoworkers. It should be noted that over the past few years the number of Internet threats for organizations of different sizes and sectors of activity has increased dramatically. Architecture construction and operation of web applications is a complex process, which may include individual components that can be combined in a variety of chains for the implementation and application of the functional capacity. As components can act database management systems, XML-storage, Lightweight Directory Access Protocol system (LDAP) and the server file system, in the environment of which applicationsoperate. On the strength of these components, there are vulnerabilities on the servers and on the client side [4-6].

Firewalls provide security in the implementation of the electronic exchange of information with other interacting information systems and external networks, access network between the corporate segment, as well as protection against penetration and interference in the work of the information system of violators from external systems [7-9].

II. RESULTS OF THE STUDY

Web-based information systems are a special type of software, built on the "client-server" architecture. Their peculiarity lies in the fact that the system itself is and is executed on the server;a client thus only receives the results. The system is based on the receipt of requests from the user, their processing and issuing of results. Transfer of requests and results of processing occurs over the internet (Fig. 1).

A significant advantage of Web-based information systems construction for standard browser features support is that the functions to be performed independently of the operating system of the client. Instead of having to write different versions for MicrosoftWindows, Linux, Mac and other operating systems, the system is created once for an arbitrary platform and develops on itsbasis [10]. However, various implementations of HTML, CSS, DOM and other browser specifications can cause problems in the development of the system and follow-up support. In addition, the user's ability to configure many browser options may prevent proper operation of the system [11].

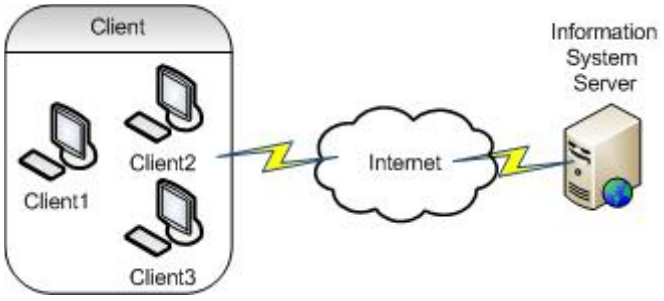

Рис. 1. The architecture of web-based information system.

The Web-based information system consists of client and server parts, thereby realizing the "client-server" technology. The server part receives a request from a client, performs the calculations, then creates a web page and sends it to the client over a network using HTTP protocol. The client part realizes a

978-1-5090-5648-417$31.00 ©2017 IEEE

user interface, generates requests to the server and processes the responses from it.

To create web-based information systems on the server side a variety of technologies and any programming languages, which are capable of outputting to the standard console, are used.

The query resultsdisplay, as well as data receiving from a client and its transfer to the server is usually handled by a special application called browser. As is well known, one of the functions of a browser is to display the data received from the Internet as a page described in the HTML language.

The firewall is a local (single component) or functionally distributed tool (complex), which accomplishes the control of input and/or output information, and secures the information system by filtering information, i.e. analysis on the set of criteria and the decision making on its spreading within (from) the information system [12-14].

A firewall is a set of hardware and software means in a computer network, which, in accordance with prescribed rules, shall control and filter the network packets passing through it. The exact implementation depends on the network size, the amount of traffic and the necessary tasks. The most common type is a software firewall. In this case, it is realized as a program running on the target computer or edge network device, such as a router. In case of a hardware performance,a firewall is a separate network element that usually has more performance capabilities but performs similar tasks.

The main task of the gateway firewall isprotection of network or its individual components against unauthorized access. In addition, firewalls are often called filters, as their main task is not to pass (filter) packets that do not fit the criteria defined in the configuration [15-16].

A firewall allows you to configure filters responsible for the transmission of traffic on the following criteria:

- IP-address;
- domain name;
- port;
- protocol.

Any target device that runs over IP must have a unique address. By setting a certain address or a certain range, you can prevent them from receiving packets, or, vice versa, allow access only from the given IP-address.

Firewalls are used to distinguish between networks with different security requirements. Firewalls should be usedeach time, when the internal networks and systems interact with external networks and systems, and when the security requirements differ in several internal networks. Let us consider, where firewalls should be located and how should be located other networks and systems with respect to firewalls [17-20].

Since the original function of a firewall is to prevent unwanted traffic entering the network, firewalls should be placed at the entry points on the logical borders of the network. This usually means that the firewall is a node, inwhich the network traffic is divided into several paths, or ingather in one way. When routing, firewall is usually located directly in front of the router and is sometimes combined with a router. The situation when the firewall is located after the separation of traffic on several routes is much rarer, because in this case, the firewall will need to watch out for each of these routes. Often, the firewall hardware devices also have routing capabilities, and in the networks built with switches, a firewall is often a part of the switch, which provides the ability to protect all switched segments.

The firewall receives traffic, checks it in accordance with its policy and takes the appropriate action (e.g., gates the traffic, blocks it,performs a conversion).

Principles of a firewall construction:

- simplicity;
- suitable application of the devices;
- build defense in depth;
- focus on internal threats.

The principle of “simplicity” suggests the first and foremost what should be kept in mind when designing the network, in which firewall operates – safer is something that is easier to manage. It is important to make the simplest solutions. Difficultly understood functionalities often lead to errors in configuration.

The use of network devices for the purpose for which they were originally intended, in this context, means that you should not do firewalls from equipment that is not intended for use as a firewall. For example, routers are designed to perform routing; packet filtering capabilities are not their original purpose, and it should always be considered in the development environment of the firewall. Dependence solely on the router’s ability to provide the functionality of a firewall is dangerous: it can be easily reconfigured. Another example is the network switches: when they are used to provide firewall functionality beyond the firewall environment, they are sensitive to attacks,which can disrupt the switch functioning. In many cases, hybrid firewalls andfirewall hardware devices are the best choice because they are optimized primarily to operate as a firewall.

Defense in depth means compulsory creationof several levels of protection as opposed to having a single level. You should not ensurethe whole protection with a firewall only. Where multiple firewalls can be used, they should be used. Where routers can be configured to provide some access control and filtering, it should be done. If the server operating system may provide some firewall capabilities, it should be applied.

Finally, if attention is paid only to external threats, this leads to the network turning open to attacks from within. Although it is unlikely, but should be considered the possibility that an intruder can somehow bypass the firewall and havecarte blanche for internal or external systems attacks.

Operation of all firewalls is based on the use of information of different levels of OSI model (Table 1). The OSI model, developed by the International Organization for Standardization, defines seven levels at which computer systems communicate with each other – from the level of the physical mediaof data transfer to application programs level, which are used for communications. In general, the higher OSI model level, on which firewall filters packets, the higher the level of protection provided by it.

At the network level, it filters incoming packets based on IP addresses. At the session level, filtering is legal also on TCP port numbers and flags contained in the packets. At the application layer theapplication protocols analysiscan be carried out as well as monitoring of the content of data streams.

To minimize threats to information security it is necessary to introduce firewalls in different layers of the OSI model, as shown in the table.

Supported level of the OSI model is the main characteristic of firewalls classification. The following types of firewalls are distinguished:

- manageableswitches (data link layer);
- network filters of network layer (static filtering is carried out by analyzing the IP-addresses of the source and the receiver, protocol, source and destination ports);
- circuit-level proxy.

Table 1. FIREWALLS AND THE OSI MODELS

The layer of the OSI model	Internet Protocols	Firewall Category
Application layer	telnet, ftp, dns, nfs, ping, smtp, hhtp	Application Layer Gateway Expert-level firewall
Data presentation layer		
Session layer	TCP	Circuit-level proxy
Transport layer	TCP	
Network layer	IP	Packet filtering firewall
Data Link layer		
Physical layer		

The protocols used in networks (TCP/IP, SPX/IPX) do not fully comply with the OSI reference model, so these types of firewalls in the performance of its functionscan cover the adjacent levels of the reference model. For example, an application screen can perform automatic encryption of messages when they are sent to the external network, as well as automatic decryption of the cryptographically sealed data received. In this case, such a screen not only operates at the application layer of the OSI model, but also on the layer of presentation.

Protective functions of an application gateway, as well as a circuit-level gateway, refer to the functions of mediation. However, the application gateway, unlike the circuit-level gateway, can perform significantly more protection functions, which include the following:

- identification and authentication of users when trying to establish connections through the firewall;
- authentication of information transmitted through the gateway;
- access control to resources of internal and external networks;
- filtering and message flow conversion, e.g., dynamic search of viruses and transparent encryption of information;
- check of events, responding to preset events, as well as the analysis of the recorded information and reports generation;
- datacaching requested from the external network.

Specialized security facilities WAF (WebApplication Firewall)are firewalls that work at the application layer and perform filtering traffic of web applications. WebApplicationFirewall is a special mechanism, which has a certain set of rules on the server and client interaction, processing HTTP packages. The basis is the same principle as that of the conventional custom firewalls– monitoring of all data coming from the outside. WebApplicationFirewall is based on sets of rules by which the fact of signature attack is revealed –evidence of user activity that implies an attack. These facilities do not demand changes to the source web application code and provide much better protection for web services of conventional firewalls and intrusion detection tools.

The following standard protection mechanismsare usually regulated by the set of Web Application Firewall functions, such as:

- validation of the protocol;
- signature analysis;
- protection from injection and XSS;
- the ability to create own rules of protection;
- integration with reputational and fraud-services;
- integrationwith other devices in the company's information security landscape.

When using an application layer firewall all connections pass through it (Fig. 2). As shown in the figure, the connection starts at the client system, and is supplied to the internal firewall interface. The firewall accepts the connection, analyzes the contents of the packet and the protocol used, and determines whether the traffic complies with the rules of the security policy. If so, the firewall initiates a new connection between its external interface and the system server.

The advantages of application-level proxies:

- Owing to the ability to authenticate a user, application proxies are considered less vulnerable to fake address attacks;

- Application layer firewalls tend to have more opportunities to analyze the entire network packet, not just the network addresses and port numbers;
- As a rule, the application layer proxies provide more detailed logs;
- Proxy is in a position to request authentication.

Application Layer Firewalls use access modules for incoming connections. Access module in the firewall receives an incoming connection and processes the commands before sending traffic to the recipient. Thus, the firewall protects the systems against attacks carried out by the applications.

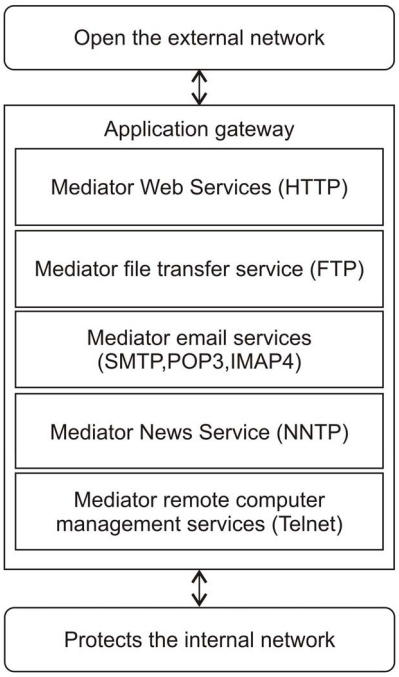

Рис. 2. Functional model of the firewall

At the moment, there is no methodology that focuses specifically on specialized testing of firewalls. To assess the quality of firewalls one has to use more general techniques.

Firewall policy specifies how the firewall will process network traffic for certain IP-addresses and address ranges, protocols, applications, and content types. Before designing a firewall policy, one should conduct a risk analysis and determine the types of traffic essentialfor the organization. Risk analysis is based on an assessment of threats and vulnerabilities.

Typically, the firewall should block all incoming and outgoing traffic that is not explicitly allowed by the firewall policy. This practice is called“deny by default”. It reduces the risk of attacks and can reduce the amount of traffic in the local network. Due to the dynamic nature of the hosts, networks, protocols, and applications it is a much safer approach to ban everythingthan to allow the whole traffic that is not explicitly forbidden.

The criteria for analysis are:

- Command windows of communication control packages that contain network addresses, IDs, interface addresses, port numbers, etc.;
- The external characteristics of the flow of information, e.g., time, frequency characteristics, volume of data, etc.;
- Direct content of communication control packages, which is checked, for instance, for the presence of computer viruses.

Assessment of the firewall can be done by calculating the probability of unauthorized access through the firewall. This index is available at the stage of operation as the ratio of the weight of the area of the input values of the fields of IP packets of filtered digital stream in which the firewall during operation may be considered overcome (the area of realization of threats of unauthorized access of the firewall), to the weight of the entire area of the input values of IP packets fields.Weight of the area of input values of IP addresses fields, in which the firewall during operation is considered to be overcome depends on the quality of the firewall work and on the firewall administrator firewall responsiveness to unauthorized access events, i.e., depends on how many typical scenarios of threats of unauthorized access was taken into account in the filtering rules in its development and on what area of the input values of the fields of the IP address of the filtered digital stream corresponding to these threats, as well as how much of the realized threat of unauthorized access could detect using intrusion detection systems or digital stream analysts within the protected segment with a firewall operation, and what value area of the IP packet fields corresponds to the identified threats.

III. CONCLUSIONS

1. Based on the research of existing data protection technologies in web-based information systems, principles of the firewall construction for this class of systemshave been formulated.

2. In the result of the analysis of information security features in the web-based information systems at various levels of the OSImodel,required functions of information protection at the application layerhave been defined.

3. By analyzing the most vulnerable areas in the organization of web-based information system for data exchangea functional diagram of an application layer firewall consisting of a filtering massage flow module at the application level, intermediaries of Web services, file transfer services, email services, news services, remote computer management services have been proposed.

4. On the basis of the experiments with the developed firewallthe methodology of assessing the effectiveness of the firewall application in the form of calculation of the probability of unauthorized access through the defender has been developed.

REFERENCES

[1] D. Melnikov, Information processes in computer networks, Moscow, 2012.

[2] M. Borisov, I. Zavodtsev, I. Chizhov, Basics of software and hardware protection of information, Moscow, 2012.

[3] V. Gafner, Information security, Rostov-on-Don, 2010.

[4] V. Gerasimenko, Information protection in automated data processing systems, Moscow, 2014.

[5] K. Brenton, Development and Diagnostics multiprotocol networks, Moscow, 1999.

[6] V. Olifer, N. Olifer, Networks. Principles, technologies, protocols, St. Petersburg, 2010.

[7] Y. Dymarsky, N. Krutyakova, G. Yanovsky, Network Management Communication: Principles, protocols, application tasks, Moscow, 2003.

[8] M. Kulginov, Corporate networks technology, St. Petersburg, 1999.

[9] D. Melnikov, Information processes in computer networks, Moscow, 1999.

[10] E. Wilson, Monitoring and network analysis. Methods for detection of faults, Moscow, 2002.

[11] Y. Tulyakov, V. Abdal, E. Sorokin, "Generalized data evaluation in mobile communication systems," Telecommunications, no. 1, pp. 37-43, 2009.

[12] V. Vishnevsky, S. Taylor, I. Shakhnovich, Encyclopedia WiMAX. Path to 4G, Moscow, 2009.

[13] V. Syuvatkin, I. Kovalev, V. Suhorebrov, V. Yesipenko, WiMAX - wireless technology: Basic theory, standards, applications, St. Petersburg, 2005.

[14] A. Maluk, S. Pazizin, N. Pogozhin, Introduction to the protection of information in automated systems, Moscow, 2011.

[15] G. Buzov, Protection against leakage of information through technical channels: Training, Benefit, Moscow, 2005.

[16] A. Maluk, Introduction to information security in the Automation of systems, Moscow, 2004.

[17] A. Snytnikov, Licensing and certification in the field of information security, Moscow, 2003.

[18] A. Petrakov, Essentials practical information protection. Tutorial, Moscow, 2005.

[19] P. Devyanin, A. Saderdinov, B. Traynev, Enterprise IT security, Moscow, 2006.

[20] V. Romanets, P. Timofeev, V. Shangin, Information protection in computer systems and networks, Moscow, 2011.