Шутова Елена Юрьевна
Тюменский государственный университет
Кафедра иностранных языков и международных профессиональных коммуникаций
Старший преподаватель
eushutova@mail.ru

Стукун Кристина Сергеевна
Тюменский государственный университет
Кафедра информационной безопасности
Студент группы КБ167
krisstukun@mail.ru

БРАНДМАУЭРЫ

Elena Yurievna Shutova
University of Tyumen
Department of foreign languages and intercultural professional communication
Senior lecturer
eushutova@mail.ru

Stukun Kristina Sergeevna
University of Tyumen
Department of information security
Student of CS167

FIREWALLS

АННОТАЦИЯ. *Статья называется «Брандмауэры». Статья посвящена одной из многих потенциальных тем в области инфраструктуры IT-безопасности. Брандмауэры приложений пытаются использовать специальные знания приложений для повышения безопасности. В этой статье представлен обзор технологий брандмауэра. Обеспечение безопасной операционной среды для критически важного приложения является*

окончательным и, возможно, самым важным шагом в процессе сборки и интеграции. В статье содержится информация о типах брандмауэра, таких как межсетевые экраны фильтрации пакетов, прокси-серверы, брандмауэры с обратным прокси-сервером. Автор статьи дает информацию об использовании инспекции пакетов, схемы пакетного контроля, повторного использования IP-адресов, NAT и PAT.

КЛЮЧЕВЫЕ СЛОВА: *технологии брандмауэра, сетевая безопасность, фильтрация пакетов, NAT, PAT, проверка пакетов, IP-адресация.*

ABSTRACT. *The article is named "Firewalls". The article is devoted to the one of the many potential topics in the field of IT security infrastructure. Application firewalls attempt to use application-specific knowledge to improve the security. This article provides an overview of firewall technologies. Providing a safe operating environment for a business-critical application is among the final—and arguably most crucial—steps in the assembly and integration process. The article contains information about firewall types such as Packet-Filtering Firewalls, Proxy Firewalls, Reverse-Proxy Firewalls. The author of the article provides information about Utilizing Packet Inspection, Packet-Inspection Flow Diagram, Reusing IP Addresses, NAT and PAT.*

KEY WORDS: *Firewall technologies, network security, packet filtering, NAT, PAT, Packet Inspection, IP addressing.*

The definition "firewall" was used in the late 1980s to network technology that appeared when the Internet was rather new in terms of its global use and exploitation. The predecessors to firewalls for network security were the routers used in the 1980s.

A Firewall is a computer, router or other communication device that filters access to the protected network.

Cheswick and Bellovin define a firewall as a collection of elements or a system that is placed between two networks and have criteria such as:

· All traffic from inside to outside, and outside to inside, must pass through it.

· Only authorized traffic, as defined by the local security policy, can pass through it.

· The firewall itself is protected from attacks.

The firewall goes as built-in software on computers with modern operating systems. A firewall can also be part of paid antivirus systems. On phones, by default, there is no network screen and it should be installed by standard means

There are several types of firewalls, each has its own advantages and disadvantages.

Firewalls with packet filters decide whether to skip a packet or drop it by looking at IP addresses, flags, or TCP port numbers in the header of that packet. The IP address and port number are network and transport layer information, but packet filters also use application layer information because all standard services in TCP/IP are associated with a specific port number.

Firewalls having this function execute only very simple operations, such as examining the packet header, verifying the IP address, the ports, and granting and denying access without making any changes.

The positive qualities of packet filters include the following:

- relatively low cost
- flexibility in defining filtering rules
- a small delay at passage of packets

Due to this simplicity of operation, they have the benefits of both speed and efficiency.

In computer networks, a proxy server is a server that acts as an intermediary for requests from clients seeking resources from other servers. Because proxy firewalls act on behalf of a client, they provide an additional buffer from port scans, application attacks and other function.

Proxy firewalls are very effective devices to control traffic flow and secure clients from malicious malware and outside attacks. Firewalls with reverse proxy work similarly to firewalls with a proxy server, with the exception that they are used for security of the servers but not the clients.

Utilizing Packet Inspection involves checking contents of packets as well as their headers. Packet-inspection firewalls look at the session information between networks. For example, session information is usually a protocol, new or existing connection, source and destination IP address and port numbers, IP checksum, sequence numbers, and application information.

Packet-inspection firewalls are generally much faster and better than application firewalls because they are not required to host client applications.

A feature that is common among all firewalls is Network Address Translation and Port Address Translation. NAT obfuscates the IP address scheme you are using internally, and the PAT function helps minimize the use of public address space. NAT gives you the capability to change the source or destination IP address. PAT provides superior scalability from an IP usage standpoint, consequently reducing the number of public IP- addresses required on the Internet.

Another key component of the firewall is the system for collecting statistics and warning about the attack. Information about all events such as incoming and outgoing connection failures, number of bytes transferred, services used, connection time is stored in the statistics files. Many firewalls give you the flexibility to determine to be logging the events, describe the actions of the firewall when attacks or unauthorized access. An immediate message about the attempt to break into the console or administrator can help if the attempt was successful and the attacker has already entered the system. Many firewalls include a reporting tool used for statistics processing. They allow you to collect statistics on the use of resources by specific users, on the use of services, failures, sources from which unauthorized access attempts were made, etc.

Authentication is one of the most important components of firewalls. Before the user is granted the right to use a particular service, it is necessary to make sure

that he is really the one for whom he claims to be. The process of determining which services are allowed is called authorization. Authorization is usually considered in the context of authentication - once a user is authenticated, the services that can him are determined. When a service request is received on behalf of a user, the firewall checks which authentication method is defined for that user and passes control to the authentication server. After receiving a positive response from the authentication server, the firewall forms the connection that the user requests.

As a rule, the principle is used, called "what he knows". It means that the user knows a secret word that he sends to the authentication server in response to his request.

One of the authentication schemes is the use of standard UNIX passwords. This scheme is the most vulnerable from the security point of view because the password can be intercepted and used by another person.

The most commonly used schemes are one-time passwords. If these passwords become intercepted, they're will be useless at the next registration, and getting the next password from the previous one is extremely difficult. Both software and hardware generators are used to generate one - time passwords. Knowing the secret word is necessary for the user to bring this device into action. Several firewalls support Kerberos, one of the most common authentication methods. Some schemes require changing the client software, but this step that is not always acceptable. Typically, all commercial firewalls support several different schemes, allowing the administrator to make the most appropriate choice for their conditions.

BIBLIOGRAPHY

1. Firewalls [Electronic resource]. – Access mode: https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html
2. Application Firewalls and Proxies [Electronic resource]. Access mode: https://www.us-cert.gov/bsi/articles/best-practices/assembly-integration-

and-evolution/application-firewalls-and-proxies---introduction-and-concept-of-operations

3. Types of Firewalls [Electronic resource]. Access mode: https://www.networkworld.com/article/2255950/lan-wan/chapter-1--types-of-firewalls.html?page=2