NETWORK FIREWALL AND ITS CAPABILITIES

Abdusamatova Shahodat Khojiakbar's daughter
Informatics and information technology teacher of the academic lyceum under the Almalik branch of TDTU named after Islam Karimov
phone: +998(93) 375 – 42 - 15 e-mail: abdusamatovashahodat@gmail.com
Mannonov Asliddin Akbar's son
Student of cyber security faculty of TATU named after Al Khorazimi
phone: +998(97) 960-03-02, e-mail: asliddinmannonov0980@gmail.com

Abstract: *This article provides an analysis of the concept of security devoir and its possibilities in order to ensure the security of information in the network.*

Keywords: *security devoir, internet protocol, packet filtering, network address, proxy filtering.*

Users always want their data to be delivered securely, regardless of whether it is transmitted over a wireless or wired network. To achieve this goal, both the service provider and the user use various methods and tools, one of such methods is the creation of a security wall.

A firewall is a combination of hardware and software that controls the flow of incoming and outgoing network traffic and prevents unauthorized access to and from the network. A firewall detects names, Internet Protocol (IP) addresses, applications, and other characteristics of incoming traffic. It checks this information in accordance with the rules of access programmed into the system by the network administrator, thereby preventing or warning about various failures in the network. Today, there are a number of firewall screening technologies that differ in their network capabilities and attack resilience. Security devoir has many possibilities, we can take the following as an example:

 Packet filtering examines the fields in the headers of data packets flowing between the network and the Internet on an individual packet basis.

 Current inspection determines whether packets are part of an ongoing communication between sender and receiver.

 Network Address Translation (NAT) hides the IP addresses of an organization's internal host computer(s) to protect against sniffer programs outside the firewall.

 Application proxy filtering inspects the application content of packets. The proxy server intercepts data packets originating outside the organization, inspects them, and forwards them to the other side of the proxy server. If a user outside the company wants to communicate with a user inside the organization, the external user first talks to the proxy application, and the proxy application communicates with the firm's internal computer.

– A firewall is placed between the firm's private network and the public Internet or other untrusted network to protect against unauthorized traffic.

– Intrusion detection systems have full-time monitoring tools deployed at the weakest points of corporate networks to continuously detect and prevent intruders. The scanning software looks for patterns that indicate certain methods of computer attacks, such as incorrect passwords, checks whether important files have been deleted or changed, and sends alerts about vandalism or system management errors.

– Antivirus programs are designed to check computer systems and drivers for computer viruses. However, to remain effective, antivirus software must be updated regularly.

– Vendors of Wi-Fi equipment have developed stronger security standards. The Wi-Fi Alliance industry trade group's 802.11i specification enhances security for wireless LAN products.

– Many organizations use encryption to protect sensitive information transmitted over networks. Encryption is the coding and encryption of messages to prevent access by unauthorized persons.

– When the firewall is used to its full potential, it constantly monitors all incoming and outgoing traffic. Unlike just a traffic analyzer, a firewall can also be set to block certain things.

– A firewall can block certain applications from connecting to the network, stop URLs from loading, and block traffic through certain network ports.

– Some firewalls can also be used in a mode where you can block everything up to a specific permission. It's a way to block everything on your network so you can manually install protections against network-related threats.

– Most home network routers include support for built-in firewalls. The administrative interface of these routers includes configuration options for the firewall. Router firewalls can be disabled (disabled) or they can be configured to filter specific types of network traffic, called firewall rules.

– Most software is properly installed by firewall programs directly onto the computer's hard drive. However, these firewalls only protect the computer running it; Network firewalls protect the entire network. Many computer firewalls can be disabled, such as network firewalls.

– In addition to dedicated firewall programs, antivirus programs often include a built-in firewall.

Another common form of network firewall is a proxy server. Proxy servers act as an intermediary between internal networks and external networks and do this by selecting and blocking packets of information in a network packet. These network firewalls also provide additional security measures by hiding internal LAN addresses from the outside Internet. In a proxy security environment, network requests from multiple clients appear to an outsider as originating from the same proxy server address.

REFERENCES:

1. Bradley Mitchell "Definition and Purpose of Network Firewall" 2023
2. Stanford Encyclopedia of Philosophy "Privacy and Information Technology" November 20, 2014.
3. "6 Emerging Trends in Physical Security" by Jay Palter March 8, 2021 in Emerging Trends in Physical Security.
4. "Security Technology Guide and Trends to 2022" 2023 Openpath