NETWORK TRAFFIC FILTERING METHODS FOR ENSURING INFORMATION SECURITY

Anvarjon Abdujabborovich Mahkamov*; Ilhomjon Rustamjon O'g'li Boqiyev**

*Senior Teacher,
"Department Of Modern Ict",
International Islamic Academy Of Uzbekistan,
Tashkent, UZBEKISTAN
Email id: Mahkamovanvar2020@Gmail.Com

**Graduate Student,
"Department Of Modern Ict",
International Islamic Academy Of Uzbekistan,
Tashkent, UZBEKISTAN
Email id: ilhomjonboqiyev2020@Gmail.Com

DOI: 10.5958/2249-7137.2023.00031.9

ABSTRACT

This article provides a brief overview of network traffic filtering methods. These methods help us closely manage the processes in the network. These methods mainly control the ingress and egress of traffic. It identifies illegal activities, harmful situations and certain types of dangers and eliminates them.

KEYWORDS: Network, Filter, Methods, Illegal Activities, Malicious Programs, Internet, Traffic, Firewall.

INTRODUCTION

Today, new technology is introduced in the world almost every day. The development of technologies, in turn, opens the way to various illegal activities in network traffic. In information security, network technologies are developing, and the methods of detecting illegal activities in it are also increasing. Due to this, the types of attacks are increasing. In order to eliminate such attacks, each port is scanned and the information in it is filtered, the necessary information is received, the information that is unfamiliar to us is checked and then it is performed. In order to preserve the integrity of information, first of all, it is necessary to protect the paths leading to this information. These paths can go through the network, through employees and from different parties. In order to protect against attacks coming from the network, it is necessary to pass incoming data through filters. If we receive an unknown package, it is advisable to check this file and eliminate its dangerous aspects and use it.

Main Part

Network traffic filtering is the process of monitoring and restricting the flow of data through a network. This is usually done to protect the network from malicious activity, but it can also be used to control the flow of certain types of traffic. It is an important component of a comprehensive security strategy. Network traffic filtering is usually done through a combination of hardware and software. A hardware component is usually a device or router configured to inspect and block traffic based on predefined criteria. For example, a firewall can be configured to block traffic from certain malicious or suspicious sources, or to block traffic that contains certain keywords. A software component is usually a set of rules or policies that specify which traffic should be allowed through and which should be blocked.

There are several different ways to filter network traffic:

1. Packet Filtering: In this method, packets are filtered based on predefined criteria such as source IP address, destination IP address, port numbers and protocol type. Packet filtering is relatively simple and effective, but can be difficult to manage on larger networks. Filtering is a network security technology that examines incoming and outgoing network packets and allows or denies them based on a user-defined set of rules. Packet filtering is designed to help protect your network from malicious traffic, such as malware and other malware. Packet filtering is typically used to protect internal networks from external attacks and external networks from internal threats. Packet filtering is usually done by firewalls, but it can also be done by routers, Layer 2 switches, and other network equipment.

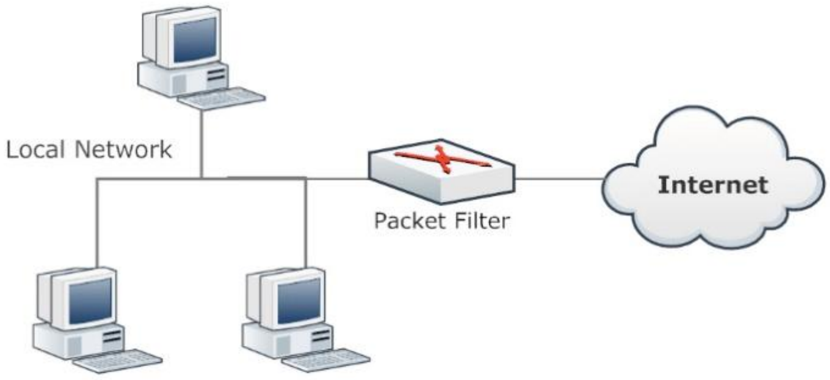


Figure 1. Packet filtering

2. Stateful Inspection: This method adds an extra layer of security to filter packets by examining the packet context (connection state) and determining the appropriate action. This makes it harder for malicious actors to bypass the packet filter. Stateful inspection is a type of packet filtering used in firewalls. It is also known as dynamic packet filtering, dynamic state inspection, dynamic packet state inspection, or dynamic state inspection. State inspection is the process of analyzing packets sent over a network. It examines each packet based on its characteristics, including source and destination addresses, port numbers, sequence numbers, and TCP flags, as well as its content. The firewall compares the packet data to an internal database of connection states. Based on this comparison, the firewall can decide whether or not to allow the packet. The advantage of stateful inspection is that it allows firewalls to be more flexible and efficient than traditional firewalls. In traditional firewalls, all packets, regardless of their content or origin, must be inspected against a predefined list of rules. With stateful inspection, the firewall can recognize already established connections and automatically allow packets by matching source and destination addresses, ports, and other connection information. This allows the firewall to be more selective and effective because it can distinguish between legitimate and malicious connections.

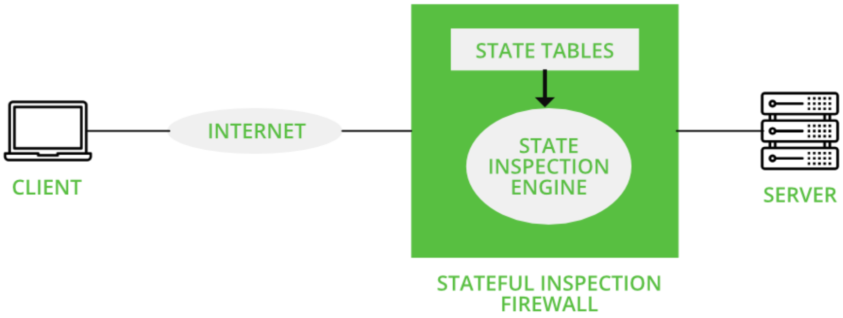


Figure 2. Stateful Inspection

3. Application Layer Filtering: This technique examines the application layer of network traffic to determine if the content is malicious or not. It is more advanced than packet filtering and can be used to detect and block malicious traffic such as viruses and malware. Application layer filtering is a technique used to regulate network traffic by restricting access to certain applications based on a set of rules. It is used to enforce security policies between hosts on a network and is typically used to block or allow traffic to or from certain applications or protocols. Application layer filtering can be used to prevent malicious or illegal activity, such as blocking malicious applications, monitoring network traffic for suspicious activity, and preventing users from accessing certain websites.

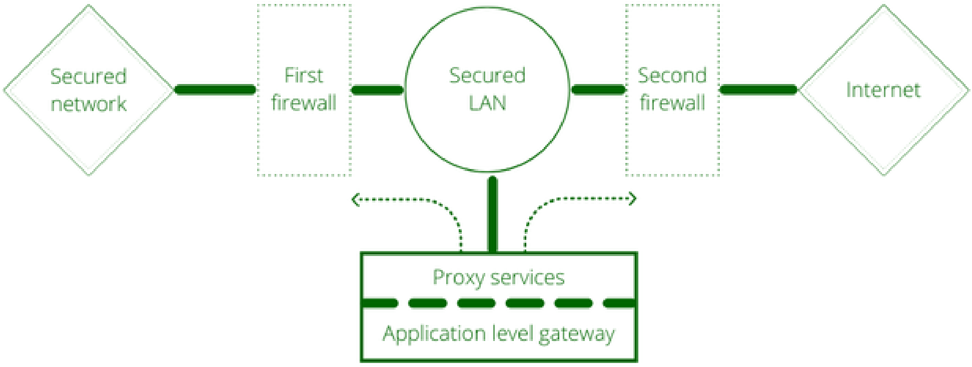


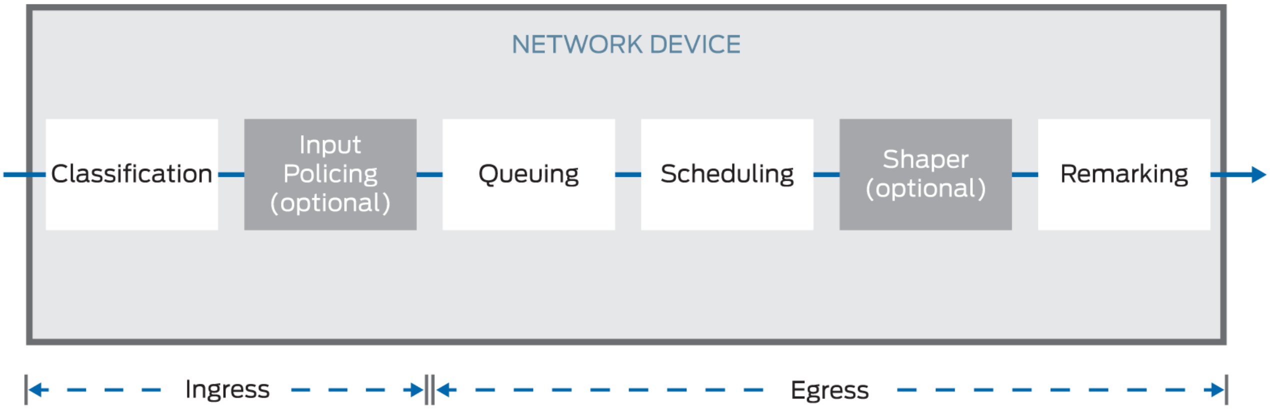
Figure 3. Application layer filtering

4. QoS Filtering: Quality of Service (QoS) filtering is used to ensure that certain types of traffic, such as voice and video, are prioritized over others. This helps deliver high-priority traffic quickly and reliably. QoS filtering is a type of network filtering technology used to allocate resources to different types of network traffic in order to improve user experience and prevent congestion. This type of filtering is used to prioritize certain types of traffic, such as real-time traffic, or to limit less important traffic. QoS filtering can be implemented by network operators in their routers and other network devices.

By applying specific rules and parameters to their networks, operators can ensure that important traffic is prioritized, while less important traffic is throttled or blocked. This type of filtering can also be used to block or limit the rate of malicious traffic.

Figure 4. QoS filtering

No one method is perfect for all scenarios, and the most effective network security solution usually involves a combination of several methods. For example, packet filtering and stateful inspection can be used together to provide a comprehensive and robust defense.



CONCLUSION

In conclusion, the above methods will help us to control the processes in the network, to analyze suspicious files and to neutralize the files that are placed by various filters. Especially if these filters are used together, the effect will be very high.

BIBLIOGRAPHY:

1. Zhumaev, T.S., Mirzaev, N.S., & Makhkamov, A.S. (2015). Algorithms for segmentation of color images based on the selection of strongly coupled elements. Studies of Technical Sciences,(4), 22(27),
2. Маҳкамов, А. А., & Инадуллаев, Х.Ў.Ў. (2021). Сравнительный анализ биометрических систем в обеспечении информационной безопасности. Universum: технические науки, (12-1 (93)), 32-37.
3. Махкамов А. А. Алгоритмы идентификации личности человека по изображению ушных раковин //Исследования технических наук. – 2015. – №. 4. – С. 28-32.
4. https://www.apnic.net
5. https://patterns.arcitura.com
6. https://www.plixer.com
7. https://d3fend.mitre.org