DEVELOPMENT OF THE MODEL AND ARCHITECTURE OF A BLOCKCHAIN-BASED DATA PROTECTION SYSTEM

FIREWALL AND ITS ROLE IN CYBERSECURITY AND OSI MODEL

Erkinov Shohjahon Sherali o‘g‘li
Axmatov Bekzod Nurali ogli
Ramazonova Marjona Ikrom kizi
Ergasheva Farida Yunus kizi
Baliyev Firdavs Azimjonovich
Students of the Muhammad al-Khwarizmi Technical University

Annotation: This paper examines the concept of firewall technology and its critical role in ensuring cybersecurity within modern computer networks. With the rapid expansion of information technologies and the increasing volume of data exchange across various sectors such as banking, healthcare, education, and e-commerce, the need for robust network security mechanisms has become essential. The study highlights the main functions of firewalls, including traffic filtering, prevention of unauthorized access, detection of malicious activities, and network monitoring.

Keywords: Firewall, Cybersecurity, Network Security, OSI Model, Packet Filtering, Stateful Inspection, Application Layer Security, Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Deep Packet Inspection, Network Traffic Control, Data Protection

Nowadays, thanks to the rapid development of information technologies, computer networks are becoming an integral part of the life of society. Thanks to the expansion of Internet networks, development of various information systems and digital services there is a large amount of information exchange between users. In modern society, information technology is widely used in banking systems, e-commerce, public services, education systems, health care and many other areas. As a result, the volume of data transferred in computer networks increases dramatically.

However, along with such development of information technologies, the issue of information security is becoming one of the pressing problems. Threats such as unauthorized access to computer networks, attacks on systems with the help of malware, data theft, data alteration, denial-of-service attacks (DoS and DDoS attacks) pose a great threat to modern information systems. As a result of such attacks, important data of organizations can be lost or stolen, causing significant economic damage [3].

Therefore, ensuring information security in computer networks is one of the most important tasks. Various technologies are used to ensure information security. Authentication systems, encryption technologies, antivirus programs, network monitoring systems, and firewall technologies play an important role among them. All these tools work together to ensure network security.

A firewall is a piece of hardware or software designed to protect computer networks against external and internal threats, and it controls the flow of information transmitted over the network. Firewall system scans incoming and outgoing traffic and allows or blocks data packets based on predefined security rules. A firewall can be used to block unauthorized connections, detect malicious traffic, and secure your network.

The emergence of firewall technology is directly related to the development of computer networks. As a result of the spread of the Internet, internal networks of various organizations began to connect with the global Internet. As a result, the risks from external networks have also increased. In this regard, there is a need for special systems to protect the internal network from the outside environment. One such system is a firewall.

A firewall system is usually hosted on a network edge. It settles between internal and external network and controls the traffic between them. Every packet that passes through the firewall is inspected and allowed to roam the network only if it complies with security regulations. Otherwise, the package will be blocked [4].

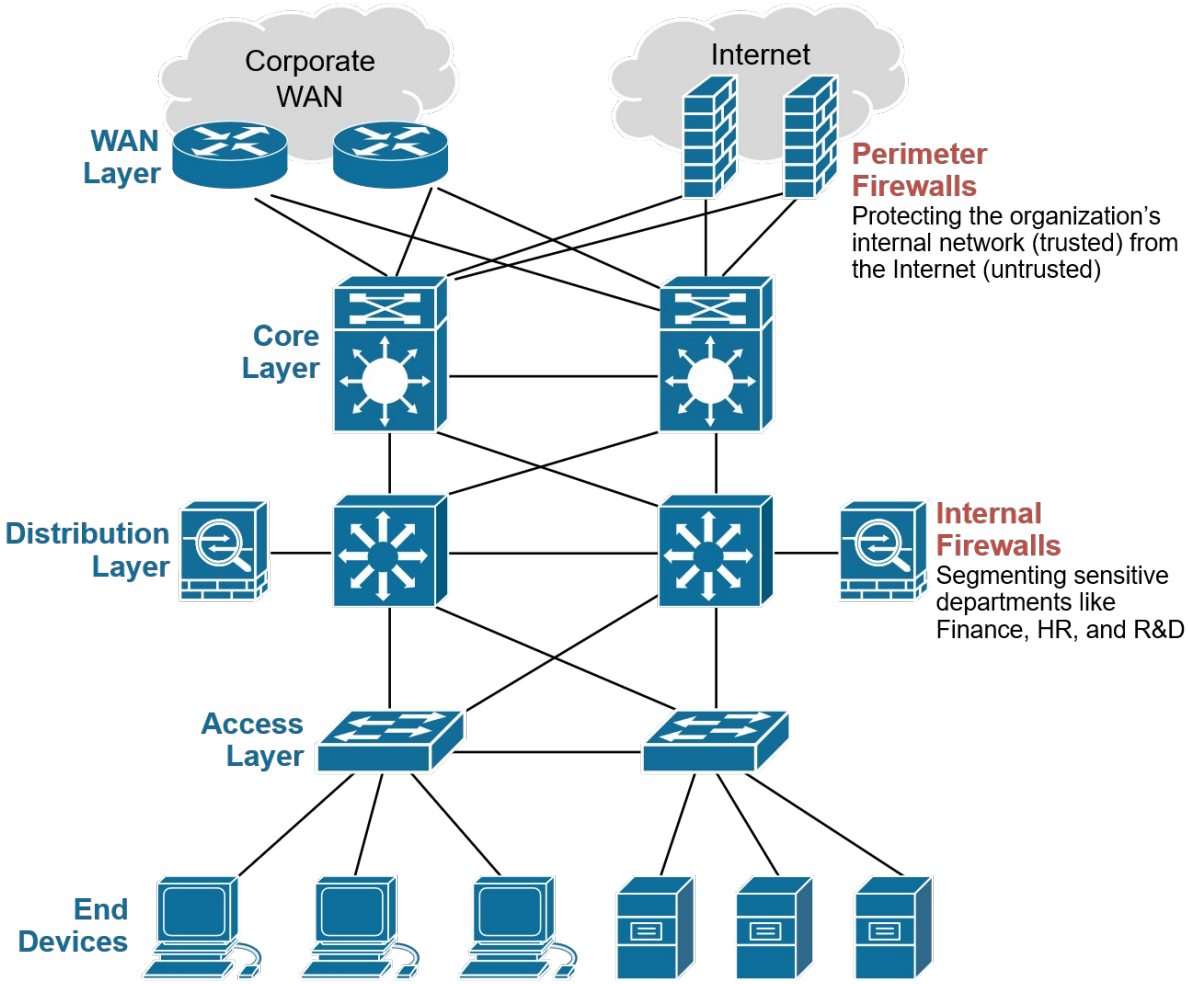

Figure 1.1. Firewall performance

The process of operation of the firewall system is based on special rules. These rules are set by the network administrators.

Table 1.1.

Main functions of firewall systems

No	Job	Description
1	Traffic control	Checks incoming and outgoing packets
2	Block Unauthorized Access	Stop Illegal Connections
3	Identifying Malicious Traffic	Blocks suspicious packets
4	Service management	Controls the port and services
5	Monitoring	Monitors network activity

Modern firewall systems are not limited to blocking traffic. They also perform additional functions such as network activity monitoring, attack detection, traffic analysis, and security policy management. Some firewall systems use Deep Packet Inspection technology to detect malicious traffic [3].

Firewall technology often works in conjunction with other security systems. For example, when applied in conjunction with IDS (Intrusion Detection System) and IPS (Intrusion Prevention System) systems, the network security is further strengthened. If the IDS system detects suspicious activity occurring on the network, the IPS system can automatically block such activity.

Firewalls matter a lot for protecting networks in companies and for regular users too. Many places rely on hardware versions to block outside threats while software ones show up more in smaller setups or home computers. It seems like they help stop malicious connections from reaching personal machines and that part stands out when you think about daily use [2].

Back in the late eighties the first packet filters came around as the internet grew from ARPANET and threats became more common. Engineers at one company started using rules to sort traffic. Over time the systems added state tracking for active connections then moved to checking content at higher levels and now newer ones pull in threat data along with other tools. The changes happened because needs kept shifting but not everything feels fully settled yet.

Some setups place a single firewall at one entry point while others put it between internal networks and the outside so everything flows through. A screened area keeps public servers apart which adds another layer if something goes wrong. The choice seems to depend on how sensitive the information is and what the group actually needs for speed.

Hardware appliances handle heavy traffic well since they run on special equipment with less delay and fewer weak points from regular systems. Software options work on normal machines and update easier without buying new gear. Many people suggest using both at different spots to build extra protection though it can get complicated to manage all at once.

The main job is deciding which packets move through by looking at addresses ports and protocols. Packet filtering is the basic method but other approaches check connection states or work at the application side. The OSI model gets mentioned to break down how networks exchange data across layers and that framework helps explain why firewalls sit where they do. It feels like some details on the layers still mix together when you try to map them out [4].

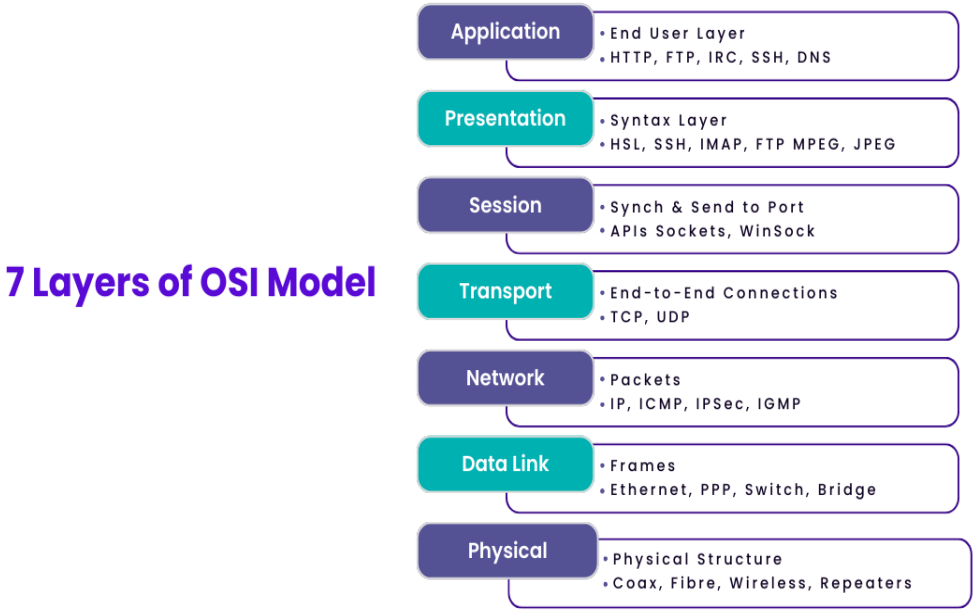

Figure 1.2. Layers of the OSI model

Firewall systems are actively operational in some of these layers. Most commonly used firewalls run on the Network, Transport, and Application layers of the OSI model.

Table 1.2.

Firewall operation across OSI model Layers

Layer	**What it does**	**Firewall role**	**OSI Layer**
Network	IP Address	Filters by IP	Layer 3
Transport	Ports	Manages Ports	Layer 4
Application	Data Contents	In-depth Traffic Analysis	Layer 7

Firewalls at the network layer just check ip addresses to filter traffic. They look at the source and where its going then drop packets that break the rules like blocking everything from one address. That seems like one of the easier ways to keep things secure at least at a basic level.

Transport layer firewalls go by tcp and udp ports instead. Each service uses its own port so if you block a port the connection gets stopped which does increase security quite a bit. Application layer ones go further and look inside the packets for bad content or sites and filter unwanted stuff. I think those are more common now in web setups.

Stateful inspection adds checking the connection status not just the header itself. If a user starts talking to an outside server the firewall keeps track and only lets related packets through and that part gets a bit messy when you try to explain all the states. Modern ones often combine these into next generation firewalls that do deeper analysis and policy management all together [4].

The rules really matter though. If they are set up wrong security gets weaker so admins have to be careful when making changes. Logging helps because a good firewall keeps records of attempts and that lets you spot problems later or meet rules in places like finance. Some also pull in threat feeds for known bad addresses so new risks get blocked without manual updates which seems useful but I might be oversimplifying how fast those feeds actually update [3].

Conclusion

In conclusion, firewall technology plays a vital role in maintaining the security and integrity of modern computer networks. As cyber threats continue to evolve, the importance of implementing effective security mechanisms becomes increasingly significant. Firewalls serve as the first line of defense by monitoring and controlling incoming and outgoing network traffic based on predefined security rules.

The analysis of firewall operations within the OSI model demonstrates that different types of firewalls operate at various layers, providing multiple levels of protection. Network layer firewalls offer basic filtering based on IP addresses, while transport layer firewalls enhance security through port control. Application layer firewalls provide advanced protection by inspecting the contents of data packets.

Modern firewall systems, including next-generation firewalls, integrate advanced features such as deep packet inspection, intrusion detection, and real-time threat intelligence. When combined with other security tools like IDS and IPS, firewalls contribute to a comprehensive and layered defense strategy.

However, the effectiveness of a firewall largely depends on proper configuration and continuous monitoring. Incorrect rules or poor management can weaken network security. Therefore, skilled administration and regular updates are essential to ensure optimal performance.

Ultimately, firewalls remain a fundamental component of cybersecurity, helping organizations and individuals safeguard their data and systems against a wide range of cyber threats.

References

1. Stallings, W. (2017). *Network Security Essentials: Applications and Standards*. Pearson Education.
2. Kurose, J. F., & Ross, K. W. (2021). *Computer Networking: A Top-Down Approach*. Pearson.
3. Scarfone, K., & Hoffman, P. (2009). *Guidelines on Firewalls and Firewall Policy*. NIST Special Publication 800-41.
4. Comer, D. E. (2018). *Internetworking with TCP/IP: Principles, Protocols, and Architecture*. Pearson.
5. Cisco Systems. (2022). *Firewall Technologies and Security Solutions Documentation*.