7th International Scientific Conference ITEMA 2023 – Conference Proceedings
DOI: https://doi.org/10.31410/ITEMA.2023.19

Implementation of Next-Generation Firewalls in Modern Networks

Milan Pavlović[1]
Marija Zajeganović[2]
Milan Milivojević[3]

Received: December 22, 2023
Accepted: February 12, 2024
Published: May 28, 2024

Keywords:
Next-generation firewall;
Network security;
IoT

Abstract: *The primary function of any firewall is to assist in protecting against unwanted or malicious traffic entering or leaving a network. However, as threats evolve and become increasingly challenging to detect, network security must remain equally sophisticated. In addition to access control, Next-Generation Firewalls can block modern threats such as advanced malware and application-layer attacks. This paper will present the fundamental characteristics of Next-Generation Firewalls and their implementation in modern networks, particularly their use in IoT. First, the concept of Next-Generation Firewalls will be explained, highlighting significant improvements they have over previous generations of firewalls, and the reasons for implementing them. Next, the authors will provide an overview of Next-Generation Firewall architectures. Special attention will be given to the use of Next-Generation Firewalls in the context of IoT.*

1. INTRODUCTION

Without a doubt, a notable challenge in the realm of network security involves guaranteeing access to data, secure transactions, data integrity, and privacy, among several other considerations. An essential protective measure in the modern Internet network is the firewall. In the computing network, a firewall serves as a device that segregates a potentially dangerous external network from the local network. However, it must possess a level of sophistication to regulate both incoming and outgoing network traffic based on specific rules, ensuring security against undesired and perilous network activities. So, network security is one of the important things that need to be implemented in computer networks. The primary function of any firewall is to assist in protecting against unwanted or malicious traffic entering or leaving a network. Firewalls are divided into hardware and software firewalls.

A hardware firewall is a physical device that is typically placed between your internal network and the Internet. It acts as a barrier, inspecting all incoming and outgoing network traffic to protect your network from unauthorized access, malware, and other threats. Hardware firewalls are more expensive and somewhat more challenging to use, but they offer better protection. Compared to software firewalls, hardware firewalls have a higher data throughput and processing power, depending on the quality and performance of the firewall hardware. They are suitable for larger organizations, allowing the installation of multiple devices in the same network to increase data processing speed, flow, and protect various servers. Different departments within a company can be separated, and distinct rules can be created for each. The main advantage lies in speed and enhanced security. Since hardware firewalls have their operating system, they are

[1] The Academy of Technical and Art Applied Studies Belgrade, Department School of Information and Communication Technologies, Zdravka Čelara 16, Belgrade, 11000, Republic of Serbia

[2] The Academy of Technical and Art Applied Studies Belgrade, Department School of Information and Communication Technologies, Zdravka Čelara 16, Belgrade, 11000, Republic of Serbia

[3] The Academy of Technical and Art Applied Studies Belgrade, Department School of Information and Communication Technologies, Zdravka Čelara 16, Belgrade, 11000, Republic of Serbia

less susceptible to attacks, offer advanced security features, and various configuration options. With proper centralized management and maintenance by a qualified individual, the security level is significantly higher compared to software firewalls. The main drawback remains the high purchase cost and the need for proper configuration.

A software firewall, on the other hand, is a program or application that runs on an individual computer or device. It monitors and controls network traffic on that specific device, allowing or blocking data based on predefined security rules. Its job is to control every entry point through which network traffic passes on a computer. Software firewalls maintain a list of all applications with network access and control entry points through which communication occurs. If the firewall detects malicious traffic, it blocks it and alerts the user to unauthorized activity. Software firewalls are affordable and cheaper than physical or hardware firewalls. They are easy to use, and suitable even for individuals with general computer knowledge. Settings of the software firewall can be quickly and easily changed to adapt to our needs. The firewall automatically monitors active applications on the computer and adjusts filtering settings accordingly.

A drawback of software firewalls is vulnerability at the physical level of the OSI reference model. All network traffic from external networks reaches the computer before the firewall thoroughly scans it. It is more efficient in filtering outbound traffic, blocking any unauthorized traffic immediately. Software firewalls are susceptible to DoS attacks as they overload the firewall and, consequently, the computer on which it is installed. Another drawback is that they protect only the computers on which they are installed, not other devices in the local network. With an informed user and an updated application version, a software firewall is a relatively powerful means of protecting personal computers.

However, as threats evolve and become increasingly challenging to detect, network security must remain equally sophisticated. In addition to access control, Next-Generation Firewalls can block modern threats such as advanced malware and application-layer attacks. There are numerous manufacturers and various versions of next-generation firewalls. To make the right choice for the implementation of a next-generation firewall, it is necessary to accurately define the requirements based on the organization's needs.

In this paper, it will be explained the various implementations of firewall devices in modern networks. After a brief review of the main Next-Generation firewall characteristics given in Chapter 2, Chapter 3 will provide an overview of the Next-Generation firewall architecture. The use of Next-Generation Firewalls in the context of IoT will be emphasized in Chapter 4, while the specific case studies analyzed are described in Chapter 5.

2. FIREWALL TECHNOLOGY GENERATIONS

Since the first attacks on computer networks, firewall technologies have been continuously developed and improved. Historically, there have been multiple generations of firewall devices. Specifically, they are classified into three generations based on their characteristics and capabilities, as well as the latest fourth generation – a new generation of firewall technology (Liang & Kim, 2022).

Packet filtering was the first method by which firewalls checked incoming and outgoing traffic. It operates at the network layer. This is an extremely simple and accessible form of firewall protection. With this protection, each incoming and outgoing packet of information is examined. The firewall can allow the packet to pass or reject it based on pre-defined rules set by the user. The firewall examines each packet based on the following criteria: Source IP address, Destination IP address, TCP/UDP source port, TCP/UDP destination port.

Such a simple system has its drawbacks. Packet filtering is susceptible to many attacks, including IP spoofing, where an attacker attempts to gain unauthorized access to a computer by sending messages to the computer with an IP address that indicates the message is coming from a trusted host. Packet filtering firewalls do not put data into context, analyze each one individually, and therefore are quite slow, also not providing a high level of security. They are very susceptible to IP spoofing attacks.

The second generation of firewalls has introduced packet filtering based not only on the source but also on content (Mukkamala & Rajendran, 2020). These firewalls incorporate stateful packet inspection, known as dynamic packet filtering, operating at the network layer. They constantly monitor the network's state, allowing decisions to be made not just according to user-defined rules but also based on the context of packets established during the successful passage of previous packets. This method enables the inspection of packet content rather than just their filtering. A key advantage of stateful inspection is dynamic filtering, facilitating faster data processing and the ability to track packets throughout a network session. However, while this type of firewall establishes a direct connection between two points in the network, configuring it and establishing effective security policies present challenges.

An application firewall is the third generation which can detect malicious traffic that packet filtering cannot. This is achieved through detailed packet inspection (DPI). A more in-depth understanding of data flow allows better monitoring and control of applications, improved traffic optimization, and enhanced security. To achieve this, it's necessary to look beyond just the layer 4 OSI model of the packet. Packets are examined at a specific moment, from level 2 up to level 7.

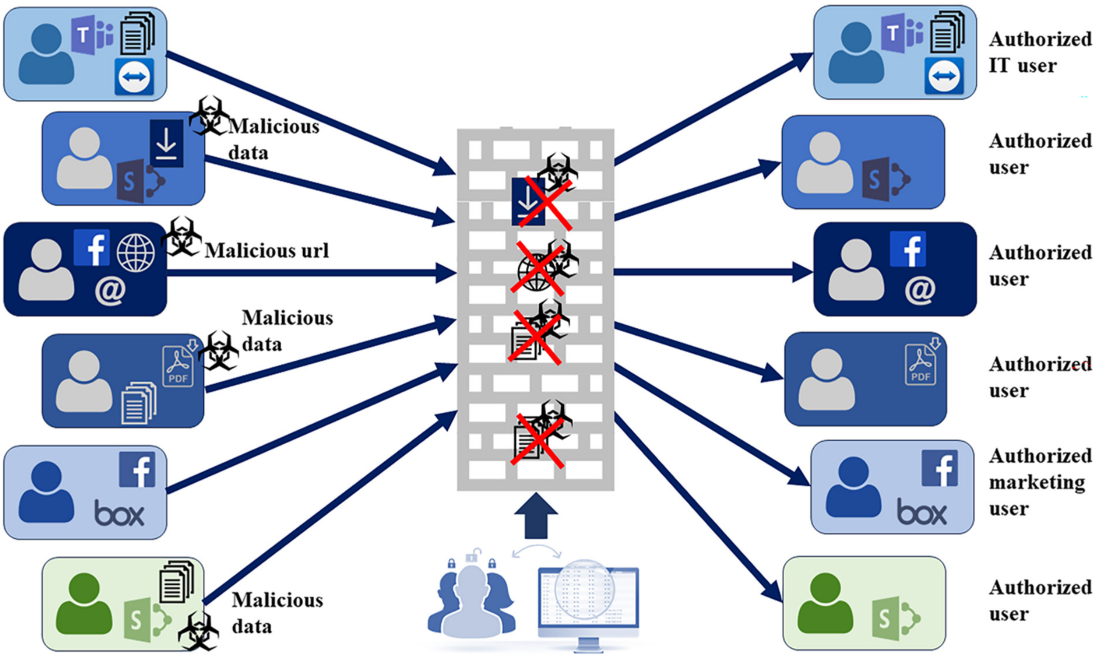

Figure 1. Packet inspection and filtering on application level 7 OSI model

Source: Own research

Based on packet inspection, the firewall classifies the packet, allowing it to enforce a specific security policy in the event of an attack. Such devices offer a wide range of functions. In addition to traditional analysis, they must identify applications without relying on basic criteria (Freet & Agrawal, 2016). They filter connections not only based on the port used but also based on the processes through which an application wants to connect to the web, see Figure 1. They provide much greater security than their predecessors, but as a result, they are more complex and require more than basic firewall knowledge to manage them. However, they are unable to create advanced security rules or perform traffic classification based on application, content, or user, which led to the development of a new generation of firewalls. These shortcomings are implemented in the fourth-generation firewall technology, i.e. next-generation firewalls.

3. NEXT-GENERATION FIREWALLS

Next-generation firewalls (NGFWs) are security walls with deep scanning of network packets, going beyond scanning only at the port and protocol levels. They can examine packets at the application layer of the OSI model and are capable of preventing intrusions. NGFWs are, therefore, independent devices whose main purpose is comprehensive protection between the local network and the external network, along with controlling local network traffic. The essence of the NGFWs is to have all the capabilities of previous versions of firewalls, as well as incorporate new technologies such as packet control, application control, and user control. The basic functional requirements for effective NGFWs include numerous capabilities like:

1. application identification regardless of port, protocol, operation technique, or use of SSL encryption;
2. support for traffic prioritization using traffic shaping and traffic policing mechanisms;
3. providing better visibility and granular control of applications;
4. accurate identification of users and using user identity as an attribute for security control;
5. ensuring traditional system protection against various threats, including application layer threats;
6. integration instead of combining traditional firewalls with IPS systems, antivirus solutions, and web filters;
7. support for processing large traffic volumes on the order of several gigabits per second without compromising system performance.

In addition to these requirements, support for traditional firewall functions is needed, including support for packet filtering, state inspection, NAT, deep packet inspection, VPN, IPS and IDS capabilities (Santos, 2020).

A key characteristic of next-generation firewalls is that they can do everything a traditional firewall can do, but with additional advanced capabilities that include new technologies, high performance, and additional functionalities depending on system requirements. NGFWs are adaptable, available in different setups, and can scale from small branch offices to carrier-grade data centers. They include centralized management that facilitates the easy administration of events and policies for network security solutions, dynamic protection, ensuring continuous visibility and policy enforcement for applications across networks and workloads. They offer administrators to monitor hosts, users, mobile devices, applications, virtual environments, threats, and vulnerabilities in the network. It is possible threat management in real-time, to control network access, monitor application usage, and defend against known attacks. NGFWs implement scalable log management combined with behavioral analysis for real-time threat detection and response. This type of traffic analysis will later help in more detailed preparation of defense against future attacks. Furthermore, NGFWs automatically correlate security events with vulnerabilities in the network, prioritize attacks and suggest security policies for implementation.

NGFWs come in various types, each with specific features and capabilities to meet different security needs (Santos, 2020). Here are some common types of NGFWs along with their definitions.

First, there are Hardware-based NGFWs, physical devices that combine traditional firewall features with advanced security functionalities like intrusion prevention, application control, and content filtering. These appliances are deployed at the network perimeter to protect an organization's internal network from external threats. Then, NGFW software-based applications or software packages can be installed on standard servers or virtual machines. They offer NGFW capabilities on existing hardware and are often used for virtualized or cloud environments.

In cloud environments, cloud-based NGFW are delivered as a service and are hosted in the cloud. They protect traffic to and from cloud-based resources, making them well-suited for organizations that rely heavily on cloud services and need to secure their connections. Integrated NGFWs are part of a broader security appliance or platform, such as Unified Threat Management (UTM) devices. These devices incorporate multiple security features, including NGFW capabilities, in a single hardware appliance.

NGFW can be offered as a managed NGFW service which are outsourced NGFW solution where a third-party provider manages and maintains the NGFW on behalf of an organization. This is often used by companies looking to offload the responsibility of firewall management.

There are also virtual NGFWs, designed to run within virtualized environments. They offer the same NGFW capabilities as hardware-based appliances but are optimized for use in virtual machines or cloud environments. Then, container-based NGFWs, are designed to provide security for containerized applications and microservices. They are specifically built to secure containerized workloads and orchestration platforms.

Each type of NGFW has its advantages and may be better suited for specific use cases, depending on an organization's requirements, infrastructure, and security goals. The common thread among these types is their focus on providing advanced security features and capabilities beyond basic firewall functions.

4. NEXT-GENERATION FIREWALL ARCHITECTURE

There are several different firewall architectures in terms of their positions in a computer network where their implementation is possible. One architecture is known as the dual-homed architecture, where the firewall device has two network interfaces. One interface accepts traffic from the external network, and the other interface connects to the internal network. All traffic into the network enters through one interface, and necessary traffic control is then performed. When implementing this architecture, hosts from the internal network can communicate with the firewall device just like hosts from the external network, but a direct connection between the external and internal networks is disabled, providing a high level of control. The advantage of this architecture is a single entry point into the network, which allows excellent control. The disadvantage of this architecture is the high-performance load on the firewall and the issue of a single point of failure because, in the event of a firewall device failure, an attacker gains direct access to the internal network.

The screened host architecture offers some additional options for providing new, unreliable, or inbound services. A screened host represents a type of firewall located at the edge of the network behind the edge router. Traffic coming from the Internet is first filtered at the router, and then the traffic is forwarded to the firewall device that performs additional traffic control. After the control, the traffic is forwarded to the internal network. This model represents the basic architecture of multi-layered network protection, the so-called defense in depth because if the firewall fails, a large part of the traffic will be filtered at the edge router. In this architecture, primary security is ensured by packet filtering. Packet filtering configuration in the screening router can do one of the following:

1. Allow other internal hosts to open connections to hosts on the Internet for certain services (allowing access to these services through packet filtering).
2. Disallow all connections from internal hosts (forcing those hosts to use proxy services through a bastion host).

The screened subnet architecture adds a layer of security to the screened host architecture by adding a perimeter network that further isolates the internal network from the Internet. With the simplest type of screened subnet architecture, there are two screening routers, each connected to the perimeter network. One is located between the perimeter network and the internal network, and the other is between the perimeter network and the external network (usually the Internet). To break into the internal network with this type of architecture, an attacker would have to pass both routers. Even if the attacker somehow breaks through to the bastion, they would still have to pass the internal router. This architecture is a true example of multi-layered protection because, for an attacker to gain access to the internal network, they must hack three devices.

There are more complex implementations of this architecture that use several different demilitarized zones, as well as multiple firewalls, including proxy firewalls for controlling access to a specific application, as shown in the image below. Placing a next-generation firewall in the right location within the system is a key factor in system design.

Designing systems that implement next-generation firewalls is based on the concept of segmentation. There are many ways to segment networks. Next-generation firewalls use a unique combination of hardware and software segmentation capabilities to allow an organization to isolate key parts of the network. Next-generation firewalls use the concept of security zones for network segmentation and isolation of key parts of information and communication systems. A security zone is a logical container for physical interfaces, VLANs, a set of IP addresses, or a combination of the above. Interfaces assigned to a specific security zone can be configured in layer 2, layer 3, or mixed mode. Interfaces operating in Layer 2 mode classify traffic based on MAC address or assigned VLAN tag. Layer 3 interfaces classify traffic based on IP address. Interfaces in mixed mode use a combination of Layer 2 and Layer 3 modes. Figure 2 shows the mentioned types of firewall architectures.

The placement of NGFWs in a network architecture depends on the specific security requirements and the desired level of control over network traffic.

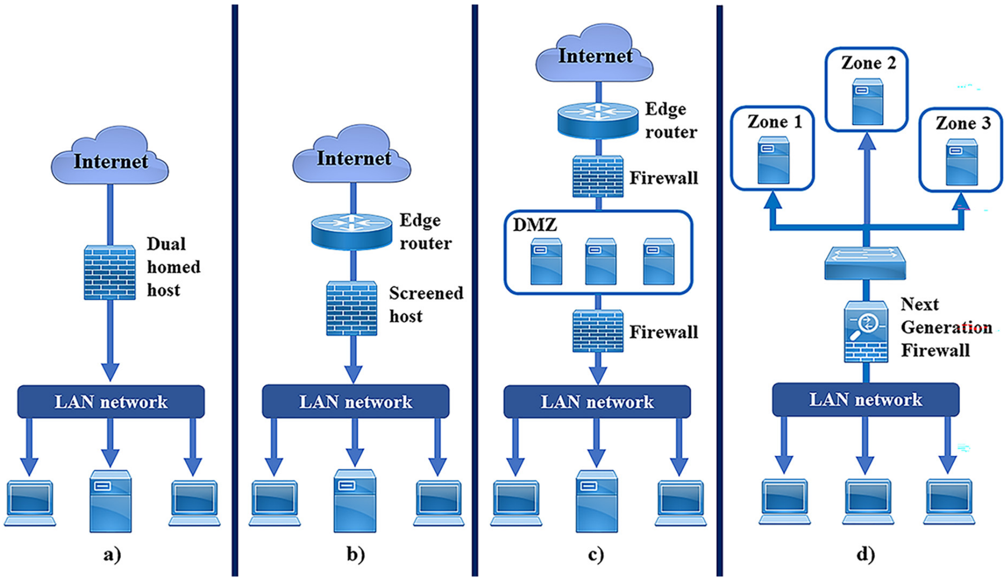

Figure 2. The various types of firewall architectures: A) dual-homed; b) Screened host; c) screened subnets; d) zone implementation

Source: Own research

One of the most common positions for an NGFW is at the network perimeter, acting as the first line of defense between the internal network and external networks (e.g., the internet). In this position, the NGFW monitors and filters incoming and outgoing traffic to prevent unauthorized access, block malicious content, and enforce security policies. NGFWs can be deployed between different segments of the internal network to control and monitor traffic between departments, business units, or other network segments. This helps in implementing and enforcing security policies for internal communications.

When organizations use VPNs for secure communication between remote offices or remote users, an NGFW can serve as the termination point for VPN connections. This allows the NGFW to inspect and secure VPN traffic, ensuring that encrypted communications are not used as a vector for threats. As organizations move services and applications to the cloud, NGFWs can be deployed at the edge of the cloud network or integrated with cloud security services. This ensures consistent security policies across on-premises and cloud environments.

NGFWs can be placed at the perimeter of the data center to protect critical servers and applications from external threats. They help in enforcing security policies and preventing unauthorized access to sensitive data. In distributed network environments with branch offices, NGFWs can be deployed to protect each branch's local network. This allows for consistent security policies and threat prevention across the entire organization.

Some organizations choose to deploy NGFWs inline within the network to inspect traffic between internal devices. This approach is used to add an extra layer of security and control over the lateral movement of threats within the network. NGFWs may be placed at internet egress points within the network to control and monitor outgoing traffic. This helps in preventing data exfiltration and enforcing security policies on outbound communications.

It is possible to implement failover for NGFW devices, organize them into clusters (Rajib, 2022), and thereby ensure a high level of availability. In this case, it is important to have two identical firewall devices that are interconnected with a dedicated failover link. Simultaneously, a state link is configured for the exchange of stateful firewall information between the devices.

In Active-Standby failover mode, one firewall device is active and processes all traffic. The standby device in this mode does not process active traffic but synchronizes with the configuration and other information of the active device via the state link. When a failover occurs and the active firewall device goes down, the standby device is activated at that moment and takes over all traffic (Santos, 2020). The architecture of NGFW devices in Active-Standby failover mode is illustrated in Figure 3. In Active-Active failover mode, both devices monitor and filter traffic simultaneously.

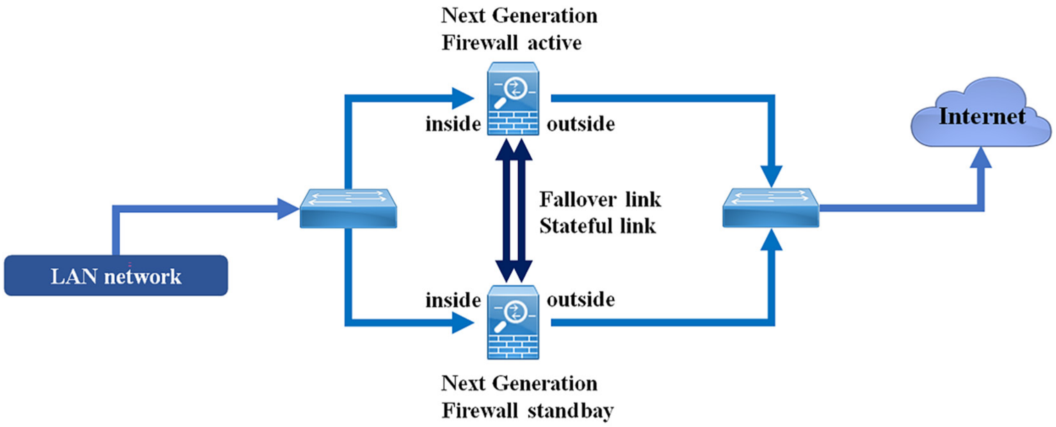

Figure 3. NGFW devices in Active-Standby failover mode

Source: Own research

The optimal placement of an NGFW depends on factors such as the organization's network architecture, security policies, and the specific use case. In many cases, a combination of these deployment scenarios is used to create a layered and comprehensive security strategy.

5. NEXT-GENERATION FIREWALLS IN IOT

IoT devices find applications across diverse industries, each employing unique architectures. Industrial and consumer IoT often adopt distinct structures, with manufacturers commonly utilizing the Purdue model to segment their Industrial Control Systems (ICS) networks. IoT network firewalls play a crucial role in reviewing and controlling traffic at network borders. This model divides the IoT architecture into several layers, each serving specific purposes. Level 4/5 is the Enterprise layer represents the corporate IT network, where Enterprise Resource Planning (ERP) systems oversee high-level manufacturing operations. Level 3.5 presents the Demilitarized Zone (DMZ) acts as a buffer separating IT and OT environments, incorporating security systems designed to safeguard OT environments from potential attacks via IT networks. Level 3 is Production Operations Systems manage workflows on the factory floor. Within the process network, operators use a Human Machine Interface (HMI) to access Supervisory Control and Data Acquisition (SCADA) software for monitoring and controlling physical processes and that would be Level 2. In the control network, intelligent devices such as Programmable Logic Controllers (PLC) and Remote Terminal Units (RTU) monitor and manipulate physical devices, defined in Level 1. The network field involves physical devices and sensors performing production operations and that would be Level 0.

Firewalls, which restrict incoming and outgoing network traffic based on predefined rules, are fundamental elements of network security. Firewalls are crucial to secure IoT devices, too. By utilizing an IoT firewall, administrators can narrow down their potential points of vulnerability, thereby minimizing the risk of an attack culminating in a security breach (Arefin et al., 2021). An IoT firewall is a security system that protects IoT devices and networks from cyber threats. Its primary purpose is to prevent unauthorized access to the Internet of Things behind the firewall and networks. The IoT firewall checks traffic from your devices and allows passage only to authorized traffic. Your devices are protected from network threats and illegal access by the firewall standing between them and the Internet. The IoT firewall analyzes network traffic and applies rules to decide whether to allow or stop it (Maheshwari & Dagale, 2018). For example, the firewall will determine if an attempt by a device to connect to the Internet is authorized. If so, the connection is valid; if not, the connection is blocked. IoT firewalls protect devices from exploitation and can be applied as IoT networks or IoT embedded firewalls. IoT network firewalls are deployed as part of network gateways and enable both macro and micro-segmentation of an organization's specific IoT implementation. IoT network firewalls can use VPNs to encrypt traffic between the network gateway and remote servers processing data collected by IoT devices.

On the other hand, IoT embedded firewalls are embedded in the operating system of IoT devices. They are installed by the manufacturer of IoT devices and can filter traffic to devices and potentially act as a VPN endpoint. These firewalls come in various types, each with unique features and capabilities. For example, some may encrypt communication to protect your data, while others may identify and prevent malicious traffic. IoT devices differ from traditional network firewalls. IoT security is crucial because of protecting personal data. IoT devices collect and store personal data that hackers can use to steal your identity, conduct illegal transactions, or even extort you. Securing your IoT devices prevents them from doing so. Furthermore, IoT devices are vulnerable to malware attacks, data leaks, and hacking. Installing reliable firewalls and antivirus software can prevent such attacks. To guarantee the efficiency of IoT networks and applications, users are encouraged to perform end-to-end testing. The network system must undergo several tests to ensure that all parts function together seamlessly, from end devices to cloud infrastructure such as Azure. Developers take necessary precautions to protect IoT applications from cross-site scripting (XSS). This script is a security flaw in which hackers access your network and other devices and data. Avoid such attacks by using the latest IoT security solutions. As more homes and businesses adopt IoT devices in their daily operations, they are increasingly used in critical resources and infrastructure. Breaching security in these systems can have catastrophic consequences, and it's best to stay ahead of attackers.

6. CONCLUSION

In today's world, there is no possibility of normal business operations without a developed information and communication system. A key aspect of protecting access to information systems is a well-configured and customized firewall. Traditional firewalls identified applications in a way that applied the rule IP address + port = application. Traditional security mechanisms performed their job well until the emergence of Web 2.0 applications. With the emergence and widespread use of Web 2.0 applications, user behavior changed, and concurrently, with the development and expansion of the Web, there is an increasing number of attack techniques and attempts. The operation of the next-generation firewall is based on three components: application identification, user identification, and content identification. By combining these three components, advanced security policies and controls can be created. There are many manufacturers and options for NGFW, and the choice depends on the user's needs.

The NGFW plays a pivotal role in enhancing the security posture of IoT environments by providing advanced threat protection, visibility, user identification, segmentation, and integration with broader security measures. It enables organizations to address the unique challenges posed by the diverse and dynamic nature of IoT ecosystems.

The implementation of NGFW is an evolving field, and future research may focus on several key areas to address emerging challenges and improve the effectiveness of NGFW technologies. It could be the development of specialized NGFW solutions for IoT environments, considering the unique challenges associated with securing a diverse range of IoT devices or investigation into the scalability and performance of NGFWs in large-scale IoT deployments.

References

Arefin, M. T., Uddin, M. R., Evan, N. A., & Alam, M. R. (2021). Enterprise network: Security enhancement and policy management using next-generation firewall (NGFW). In *Computer Networks, Big Data and IoT: Proceedings of ICCBI 2020* (pp. 753-769). Springer Singapore.

Freet, D., & Agrawal, R. (2016). Network security and next-generation firewalls. In *Proceedings of International Conference on Technology Management (ICTM 2016)* (p. 23).

Liang, J., & Kim, Y. (2022, January). Evolution of firewalls: Toward securer network using next generation firewall. In *2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 0752-0759). IEEE.

Maheshwari, N., & Dagale, H. (2018, January). Secure communication and firewall architecture for IoT applications. In *2018 10th International Conference on Communication Systems & Networks (COMSNETS)* (pp. 328-335). IEEE.

Mukkamala, P. P., & Rajendran, S. (2020). A survey on the different firewall technologies. *International Journal of Engineering Applied Sciences and Technology*, *5*(1), 363-365.

Rajib, N. (2022). *CCNP Security Cisco Secure Firewall and Intrusion Prevention System Official Cert Guide*. Cisco Press.

Santos, O. (2020). *CCNP and CCIE Security Core SCOR 350-701 Official Cert Guide*. Cisco Press.