IRSTI 81.93.29 DOI: https://doi.org/10.62687/STJ.1.2.2026.21

AI-POWERED ANALYSIS OF FIREWALL SYSTEMS FOR CORPORATE NETWORK PROTECTION

[1,2]G.Z. Ziyatbekova*, **[3]Wojcik Waldemar**, **[2]D. Zharkynuly**, **[2]Y.R. Yklasuly**
[1]Al-Farabi Kazakh National University, Almaty, Kazakhstan
[2]Almaty Technological University, Almaty, Kazakhstan
[3]Politechnika Lubelska, Lublin, Poland
*e-mail: ziyatbekova1@gmail.com

G.Z. Ziyatbekova – PhD, Associate Professor, Almaty Technological University, Almaty, Kazakhstan; Al-Farabi Kazakh National University, Almaty, Kazakhstan; Corresponding Author; e-mail: ziyatbekova1@gmail.com, https://orcid.org/0000-0002-9290-6074

Wojcik Waldemar – Doctor of Technical Sciences, Professor; Department of Electronics and Information Technology, Politechnika Lubelska, Lublin, Poland; https://orcid.org/0000-0002-0843-8053

D. Zharkynuly – student of Almaty Technological University, Almaty, Kazakhstan; e-mail: zharkynulydaniyar@gmail.com, https://orcid.org/0009-0009-6653-3057

Y.R. Yklasuly – student of Almaty Technological University, Almaty, Kazakhstan; e-mail: rahatykylas18@gmail.com, https://orcid.org/0009-0006-4617-3996

Abstract. Modern cyber threats are characterized by a high degree of complexity and variability, which makes the task of protecting corporate networks from confidential data leakage especially relevant. Traditional approaches to information security are losing their effectiveness when faced with attacks based on anomalous user behavior and the use of covert communication channels. In this regard, the role of next-generation firewalls (NGFW) and intrusion detection and prevention systems (IDS/IPS) is increasing. This study is aimed at exploring the possibilities of integrating NGFW and IDS/IPS with machine learning technologies to enable intelligent analysis of network traffic. As part of the practical component, a module was developed in the Python programming language, based on the Random Forest algorithm, which provides automatic threat classification. The module was tested to see how well it works when people try to attack it. This was done to find out if it is really useful in the world. This work is, about keeping information safe and secure using artificial intelligence. We looked at the problems we are facing now with keeping data safe and we tried to come up with some solutions.

Keywords: NGFW, IDS/IPS, Random Forest, data protection, artificial intelligence, cybersecurity.

AI КӨМЕГІМЕН КОРПОРАТИВТІК ЖЕЛІНІ ҚОРҒАУ ҮШІН БРАНДМАУЭР ЖҮЙЕЛЕРІН ТАЛДАУ

[1,2]Г.З. Зиятбекова*, **[3]Wojcik Waldemar**, **[2]Д. Жарқынұлы**, **[2]Р.Ы. Ықласұлы**
[1]әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан
[2]Алматы технологиялық университеті, Алматы, Қазақстан
[3]Люблин техникалық университеті, Люблин, Польша
*e-mail: ziyatbekova1@gmail.com

Г.З. Зиятбекова – PhD, қауымдастырылған профессор, әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан; Алматы технологиялық университеті, Алматы, Қазақстан; e-mail: ziyatbekova1@gmail.com, https://orcid.org/0000-0002-9290-6074

Wojcik Waldemar – т.ғ.д, профессор; Ақпараттық технологиялар және электроника кафедрасы, Люблин техникалық университеті, Люблин, Польша; https://orcid.org/0000-0002-0843-8053

Д. Жарқынұлы – Алматы технологиялық университетінің студенті, Алматы, Қазақстан; e-mail: zharkynulydaniyar@gmail.com, https://orcid.org/0009-0009-6653-3057

Р.Ы. Ықласұлы – Алматы технологиялық университетінің студенті, Алматы, Қазақстан; e-mail: rahatykylas18@gmail.com, https://orcid.org/0009-0006-4617-3996

Аңдатпа. Заманауи киберқауіптер жоғары күрделілік пен өзгермелілік деңгейімен сипатталады, бұл корпоративтік желілерді құпия ақпараттың сыртына шығуынан қорғау міндетін ерекше өзекті етеді. Ақпараттық қауіпсіздікке арналған дәстүрлі тәсілдер пайдаланушылардың атиптік мінез-құлқына және жасырын байланыс арналарының қолданылуына негізделген шабуылдармен бетпе-бет келгенде өз тиімділігін жоғалтады. Осыған байланысты келесі буындағы желіаралық экрандардың (NGFW) және шабуылдарды анықтау және алдын алу жүйелерінің (IDS/IPS) рөлі артып келеді. Осы зерттеу NGFW және IDS/IPS жүйелерін машиналық оқыту технологияларымен біріктіру мүмкіндіктерін зерттеуге, желілік трафикті интеллектуалды талдауды жүзеге асыруға және деректердің ықтимал сыртқа шығу арналарының анықтауға бағытталған. Тәжірибелік бөлім аясында Python бағдарламалау тілінде модуль әзірленді, оның негізінде қауіптерді автоматты түрде жіктеуді қамтамасыз ететін Random Forest алгоритмі жатыр. Модульдин тиимдилери мен нақты жағдайларда қолданыға жаrамдылығын бағалау үшін әртүрлі шабуыл сценарийлерінде тестілей жүргізілді. Бұл жұмыста жеке дефектерді қайыпкіз және сенімді түрде жасанды интеллекттің көмерігмен қорғай жағында айтылады. Осыған байланысты ұсынылған жұмыста дефектерді қайыпкіздіңе қатысты өзекті әлемдік мәселелер талданып, оларды шешу жолдары ұсынылады.

Түйін сөздер: NGFW, IDS/IPS, Random Forest, дефектерді қорғай, жасанды интеллект, киберқайыпкіздік.

АНАЛИЗ СИСТЕМ БРАНДМАУЭРОВ ДЛЯ ЗАЩИТЫ КОРПОРАТИВНОЙ СЕТИ С ПРИМЕНЕНИЕМ ИИ

[1,2]Г.З. Зиятбекова*, **[3]Wojcik Waldemar**, **[2]Д. Жарқынұлы**, **[2]Ы.Р. Ықласұлы**

[1]Казахский национальный университет им. аль-Фараби, Алматы, Казахстан

[2]Алматинский технологический университет, Алматы, Казахстан

[3]Люблинский технический университет, Люблин, Польша

*e-mail: ziyatbekova1@gmail.com

Г.З. Зиятбекова – PhD, ассоциированный профессор, Казахский национальный университет имени аль-Фараби, Алматы, Казахстан; Алматинский технологический университет, Алматы, Казахстан; автор-корреспондент; e-mail: ziyatbekova1@gmail.com, https://orcid.org/0000-0002-9290-6074

Wojcik Waldemar – д.т.н., профессор; кафедра электроники и информационных технологий, Люблинский технический университет, Люблин, Польша; https://orcid.org/0000-0002-0843-8053

Д. Жарқынұлы – студент Алматинского технологического университета, Алматы, Казахстан; e-mail: zharkynulydaniyar@gmail.com, https://orcid.org/0009-0009-6653-3057

Ы.Р. Ықласұлы – студент Алматинского технологического университета, Алматы, Казахстан; e-mail: rahatykylas18@gmail.com, https://orcid.org/0009-0006-4617-3996

Аннотация. Современные киберугрозы характеризуются высокой степенью сложности и вариативности, что делает задачу обеспечения защиты корпоративных сетей от утечки конфиденциальной информации особенно актуальной. Традиционные подходы к информационной безопасности утрачивают эффективность при столкновении с атаками, основанными на атипичном поведении пользователей и использовании скрытых каналов коммуникации. В связи с этим возрастает роль межсетевых экранов нового поколения (NGFW) и систем обнаружения и предотвращения вторжений (IDS/IPS). Настоящее исследование направлено на изучение возможностей интеграции NGFW и IDS/IPS с технологиями

машинного обучения для реализации интеллектуального анализа сетевого трафика и выявления потенциальных каналов утечки данных. В рамках практической части разработан модуль на языке программирования Python, в основе которого лежит алгоритм Random Forest, обеспечивающий автоматическую классификацию угроз. Проведено тестирование модуля на различных сценариях атак для оценки его эффективности и применимости в реальных условиях. В данной работе рассматривается защита персональных данных с использованием искусственного интеллекта, обеспечивающая их безопасность и надежность. В связи с этим в представленном исследовании проанализированы актуальные мировые проблемы, связанные с безопасностью данных, и предложены пути их решения.

Ключевые слова: NGFW, IDS/IPS, Random Forest, защита данных, искусственный интеллект, кибербезопасность.

Introduction. In the context of the modern digital world, the issue of personal data protection has surpassed the usual approaches, achieving a qualitatively high level of development in terms of the application of artificial intelligence (AI) technologies. Based on empirical data, it has been confirmed that, while human factors and passwords are still considered major factors in the occurrence of cyberattacks, AI systems help to eliminate these factors through the fast processing of large amounts of data and the accurate identification of anomalies. At the same time, the application of AI in biometric systems, such as fingerprints and Face ID, helps to achieve high accuracy in identifying the unique biological characteristics of an individual, thus reducing the risks of unauthorized access to personal data to a minimum. Most critically, the ability of AI to learn and improve helps to enhance the defense mechanisms in response to new cyber threats, thus making AI a critical factor in the maintenance of the integrity and confidentiality of the digital world at an intelligent level.

In the context of the overall digitalization process in the world, the role of information as a strategic asset has been recognized, and the issue of ensuring the security of this information represents a pressing scientific and technological challenge. It has been established that careless handling of personal data by users frequently leads to theft or dissemination of this data without authorization. Today, the level of public awareness with regard to the proper use of AI technologies is insufficient. The quick development of cyber threats, such as malware, phishing, etc., along with low digital literacy of users, indicates the shortcomings of traditional methods for protecting users. In this context, the goal of this research is to examine the role of AI technologies in the protection of personal data and their effectiveness in the modern information environment.

Artificial intelligence and personal data security: current state and principal threats. The extensive use of AI technologies in digital services, which started in 2020, should be noted. Before the introduction of AI technologies, users mostly used various gadgets, such as smartphones, personal computers, and external devices, for storing personal data. Nevertheless, the issue of theft and leakage of this data without authorization has been persistently relevant (Bishop 2006:738).

One of the main contributors to this problem is the lack of adequate adherence by users to information security guidelines. In particular, the use of inadequate passwords, such as those containing low-complexity characters, provides a conducive environment for a successful cyberattack. Information security studies have shown that inadequate passwords remain one of the top weaknesses of cyberattacks.

Generally, the comparative analysis of the problem shows that the implementation of AI technologies is consistent with a positive trend of increased data security (Figure 1). The implementation of AI technologies has led to the development of a modern concept of data security, where this technology is a part of modern cybersecurity. This technology allows for the precise detection of anomalies and suspicious deviations, which can be imperceptible even for a human eye, through the rapid analysis of large volumes of data.

In addition, this technology not only responds to cyberattacks but also takes a proactive stance by assessing possible cyberattack scenarios. In this case, the system promptly blocks any malicious activity, thereby developing a robust defense against cyberattacks. In terms of internal security, monitoring of user activity is carried out to prevent internal data breaches (Kaspersky Lab 2021:210). Most importantly, this technology constantly evolves against emerging hacking techniques, thereby

ensuring intelligent security for the digital ecosystem.

Figure 1. Artificial Intelligence as a Guarantee of Digital Security

Presently, the exploration of techniques for the safe storage of information using artificial intelligence is an extremely relevant issue. This is due to the capability of artificial intelligence to analyze large amounts of information from the internet. Therefore, it is logically imperative to establish security protocols using this form of intelligence. One of the advantages of using artificial intelligence is its capability to analyze large amounts of information within a short time. In addition, it is capable of automatically detecting suspicious activities. In particular, artificial intelligence is instrumental in the development of biometric-based authentications, which involve the use of distinctive biological features, especially where the need for the safe storage of confidential information is imperative (Kaspersky Lab, 2021:210). In particular, as shown in Figure 2, artificial intelligence is instrumental in the identification of an individual using images, especially where it deeply examines distinctive features, such as fingerprints. This makes it one of the safest techniques for the protection of information from misuse by other parties (Whitman et al., 2018:640; Sharda et al., 2020:832).

Figure 2. Types of AI-Based Biometric Protection: Fingerprint and Face ID Technologies

Methodology. *Analysis of Existing Solutions and NGFW Architecture.* From the time of the emergence of computer networks, the security of computer networks has been a primary issue of concern. The first generation of firewall technology introduced basic packet filtering technology based on a set of parameters. The parameters included source and destination IP addresses, port numbers, and network protocol types. The first generation of firewall technology operated at OSI protocol stack layer 3 and allowed data to be either allowed or blocked based on a set of parameters. This technology worked well in environments where network interactions were limited and threats were minimal.

With the increase in network infrastructure and the number of network devices, attackers began using complex attack strategies. The traditional firewall technology had functional limitations in this regard. Attackers began using complex strategies to attack computer networks. These strategies included sending malicious data in allowed protocol data units, using application-layer

attacks, and using encryption to hide malicious activity. These factors weakened the effectiveness of traditional security solutions against emerging threats. The emergence of cloud computing, virtualization technology, and mobile computing devices introduced fundamental changes in the network infrastructure of corporate entities. A distributed computing environment emerged, and BYOD and SaaS technologies widened the attack surface of computer networks. During this time, security needs also started to change in response to emerging threats.

Next-generation firewalls or NGFWs are really good, at helping with security. Next-generation firewalls do what regular firewalls do. They also have some extra features. These features include things that help stop people from getting in control over what apps can be used and smart ways to look at traffic. Next-generation firewalls can also look closely at each packet of data, control which apps are used check traffic that is encrypted including TLS 1.3 filter things based on who is using them and work with other systems that know about threats. NGFWs also offer in-depth packet inspection (DPI), application control, encrypted traffic inspection including TLS 1.3, user-level filtering, and integration with external threat intelligence capabilities. Thus, NGFWs represent a natural evolution in the development and delivery of cybersecurity products that offer multi-layered security capabilities on network, application, user, and content levels. This evolution is particularly relevant in the context of advanced persistent threats (APTs) used by both cybercrime syndicates and state actors. The inclusion of artificial intelligence and machine learning capabilities in NGFWs enables them to identify unknown threats through behavioral analysis and dynamic adaptation to changes in the evolving cyber risk landscape (Schneier 2015:784; Tsai et al. 2009:11994-12000).

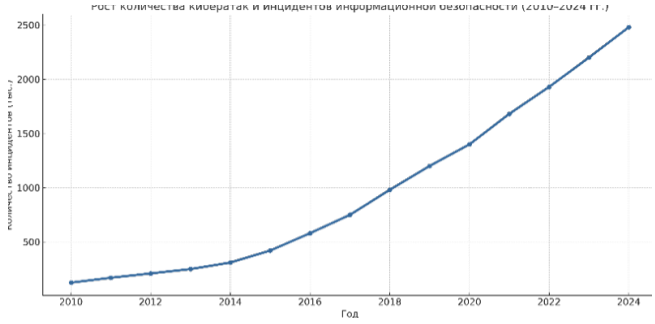

Figure 3. Growth in the Number of Cyberattacks and Information Security Incidents (2010-2024)

The above graph (Figure 3) illustrates the exponential rise in recorded cybersecurity incidents over the last fifteen years, as per data provided by IBM X-Force and ENISA statistics. There is an evident link between the evolution of threats and the need to migrate from traditional firewalls to NGFWs. There is also a significant spike in incidents recorded after 2020, reflecting the onset of remote working, the emergence of cloud computing technologies, and increased APT syndicate activities.

Discussion and Results. *Architecture of Next-Generation Firewalls (NGFW).* The solution architecture for an NGFW solution would typically involve staged traffic processing, which would include session analysis, application identification, verification against known threat signatures, behavioral analysis, and finally, decision-making with regard to the permission or denial of the network connection. This is essentially an example of the solution architecture offered by Palo Alto Networks. In the context of the deployment of security systems within large-scale corporate entities, it is necessary to consider not only the potential threats, but also the architectural characteristics of the corporate network. For example, consider the hypothetical scenario with regard to the integration of a security system within a multinational corporation with a distributed infrastructure, including multiple data centers located across the world. The principal threats with regard to the corporate network would include distributed denial-of-service attacks, phishing, and information leak risks (Hamid et al. 2016: 1-22; Biswas et al. 2018: 101-114).

Initial Conditions:

The multinational corporation has a corporate network with thousands of users distributed

across different offices and data centers. The principal threats with regard to the corporate network would include distributed denial-of-service attacks, phishing, and information leak risks.

Implemented Measures:

1. Deployment of NGFW.

The next-generation firewalls were implemented to strengthen the security of the network perimeter, controlling applications while filtering at the application level. This measure offered protection from sophisticated attacks, including SQL injections, phishing, and DDoS, while at the same time providing increased transparency and visibility, thus facilitating early detection of anomalies.

2. Implementation of IDS/IPS.

To detect internal threats, an IDS/IPs system was integrated, thus providing the ability to detect anomalies at the network level. This measure allowed for the detection of unauthorized access, prevention of data leakage, and protection from compromising critical services.

3. Integration with SIEM.

This measure, which offers centralized management, is responsible for providing rapid response to emerging threats. The solution offers integration with other components, including NGFW and IDS/IPs, thus providing the ability to collect, correlate, and analyze security information from other components, while at the same time providing automatic responses to emerging threats (Kumar et al. 2019: 565-577; Dua et al. 2019: 117-121; Ashoor 2011: 497-501).

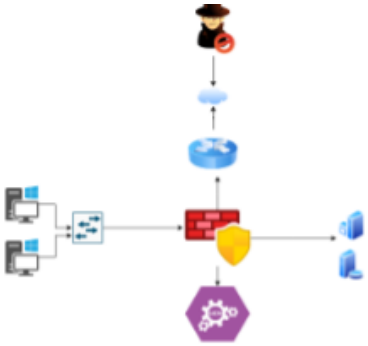

Figure 4. Architecture of the Tested Network

Due to the application of an integrated cybersecurity system, which included the NGFW, IDS/IPS, and alignment with the security information and event management system, the organization noticed the following positive results (Figure 4):

- A significant reduction in the success of attacks on the corporate network, due to the detection and prevention of cyberattacks;
- Increased accuracy in the detection of cyberattacks, due to the combined effect of multiple security tools and the application of machine learning algorithms, which improve the flexibility of the system to accommodate emerging complex cyberattacks;
- A reduction in false positives, which reduced the impact on business processes, due to the optimization of the system's configuration and the application of advanced anomaly detection techniques.

Data Loss Prevention (DLP) Methods.

The first function of NGFWs is the prevention of the leakage of confidential information.

The application of DLP tools is carried out using different techniques, which are:

- Signature-based data analysis, where specific patterns are identified;
- Content filtering, where specific keywords or templates are identified;
- Behavioral patterns, where specific patterns are identified by monitoring user behavior.

NGFW can prevent the delivery of sensitive data through an unsecured channel, block file uploads to the cloud, and monitor for insider attacks from authorized users. The NGFW market includes numerous vendors providing a variety of solution types. In this discussion we will explore

several popular solutions and their respective functionality; see the information in Table 1 for a summary of the comparison parameters used to evaluate the solutions discussed within this section of the report.

Table 1. Comparative analysis of firewall solutions

Parameter	Palo Alto Networks	pfSense	Mikrotik
Apt Detection	Yes	Partial	Partial
TLS 1.3 Support	Yes	Yes	Partial
Built-in Sandbox Analysis	Yes (WildFire)	Yes	Via AMP
ML/AI Support	Yes	Yes	No
Built-in DLP	Yes	Через модули	No
Threat Intelligence Integration	Automatic	Partial	No
TCO over 5 years (estimated)	Medium	Low	Low

After carefully analyzing the data provided, it is evident that the overall degree of integration of Palo Alto Networks is significantly highThe most distinguishing characteristics of this product are: (1) it has a high level of security because it is able to take advantage of TLS 1.3, (2) it allows the user to analyze what happens to their data using Machine Learning/Artificial Intelligence (ML/AI), (3) it protects against Advanced Persistent Threats (APTs), and (4) it provides the user with an effective means of doing sandbox analyses using the Wildfire platform. This product is frequently implemented within the infrastructures of Large Enterprise and Mission Critical information systems. Additionally, it automatically integrates with Global Threat Intelligence platforms enabling Palo Alto Networks-Based Next Generation Firewall (NGFW) solutions to dynamically respond to newly emerging threats automatically without requiring manual intervention from the administrator(s). Fortinet FortiGate solutions are both known for offering excellent throughput performance while being priced much lower than many competing alternatives. For those who work on tight budgets and require an acceptable level of protection as well as future growth possibilities, this combination will likely prove to be attractive. Also, since both TLS 1.3 and IPS capabilities are now part of the Fortinet portfolio, there may well be many medium size industries where Fortinet SOLUTIONS could represent a viable option for their environment. That said, their integration with external threat-analysis ecosystems tends to be less extensive than what is offered by some of the most prominent vendors in the market.

Cisco Firepower, by contrast, offers a broad set of options for security configuration and monitoring. Yet it appears to lag behind several competitors in a few consequential areas – most notably, more advanced machine-learning support and the availability of built-in data loss prevention (DLP) mechanisms. Moreover, AMP (Advanced Malware Protection) typically delivers sandboxing as a standalone capability through an additional integration process resulting in increased architectural complexity. Cost also plays an important role in the decision-making process; Cisco deployments tend to be significantly higher than competing vendors and thus many organizations will likely limit their adoption of Cisco based on price alone.

Check Point NGFW is known for its flexible and granular policy definitions as well as rich integration with Threat Intelligence. However, Check Point NGFW has partial implementation of its AI/ML capabilities and therefore the practical benefits derived from sandbox analysis depend greatly upon which licensing tier has been chosen by the user. Even with these limitations, Check Point remains a very flexible and resilient solution which explains its continued market presence (Singh et al. 2014:41-47; Hussain 2018: 289-29).

It can be concluded from the above comparisons that there is no single best solution to satisfy all operational environments. In general throughout the industry, selection criteria for an NGFW should be developed based upon the organization’s specific requirements including at least:

- Importance of the protected resources to the organization
- The acceptable increase in network latency due to traffic inspection
- The available budget for both initial deployment of the NGFW & ongoing operations
- The necessary compatibility with current network/system monitoring & analysis tools.

According to the comparison performed, the analysis demonstrates the importance of the formal selection of products that adhere to a four-level selection methodology as shown in Figure 3. This methodology will compare the technical, security/functional, and economic features associated with a product. In conclusion, we can conclude that next-generation firewalls (NGFW) are an advancement over traditional firewalls. They will be better able to protect against multilayered attacks than conventional firewalls by utilizing deep packet inspection (DPI), application-layer security, threat intelligence integration, behavioural analytics and machine learning, and more advanced malware analysis through sandboxing.

The architecture of NGFWs continues to develop due to (i) the increasing trend of encrypted data being transmitted; (ii) the rise of cloud and mobile computing; and (iii) the increasing sophistication of modern attacks. SSL/TLS inspection (including TLS 1.3), application control and DLP (Data Loss Prevention) are now prevalent as they enable the identification of known malicious signatures as well as, more significantly, enabling the detection of suspicious behaviours that may identify developing threats on an immediate basis. This trend will strengthen the overall security posture of enterprise infrastructures (Sichkar et al. 2023:28-33; İş 2024: 12-20).

The four next-generation firewall (NGFW) products reviewed - Palo Alto Networks, Fortinet FortiGate, Cisco Firepower, and Check Point - all have unique advantages and disadvantages, reinforcing the need for a thoughtful, context aware selection approach (regardless of how this complicates procurement, it cannot be avoided). Hence, NGFWs are a key component of modern enterprise cybersecurity strategies, allowing organizations to adapt to changing threat environments and to enhance the effectiveness of their defenses through the use of more intelligent technologies.

Threat Analysis: A Machine Learning Approach to Threat Analysis and Threat Detection. As cyber threats have become increasingly numerous and sophisticated over the past few years, the ability to detect attacks in corporate networks is rapidly becoming a necessity rather than a luxury enhancement. Next-generation firewalls (NGFWs) – including Palo Alto systems – are often presented as one response to this challenge because they can identify and block threats through deep inspection of multiple traffic types. This chapter investigates machine learning techniques for analyzing the threat logs produced by a Palo Alto firewall. The threat logs contain detailed information about the network activity and therefore may help respond rapidly to incidents by providing incident detection support and even automation in some cases. This may significantly reduce response times when time is critical.

The primary goal of this research is to classify threats using the Random Forest algorithm on firewall log data. The Random Forest algorithm has been established as an effective classifier for large heterogeneous datasets and for constructing accurate and stable classifiers. The research is organized into multiple related tasks:

- Comparatively analyzing the effectiveness of firewalls
- Collecting and preprocessing Palo Alto threat logs for later use
- Training a Random Forest model on the prepared dataset for threat classification
- Evaluating the model quality based on accuracy, recall, precision, and F1-score
- Visualizing the results to facilitate the interpretation of the classification performance in practice.

More broadly, applying machine learning in this context may both accelerate detection workflows and improve classification fidelity – an outcome that is arguably critical for corporate network defense. The selection of Random Forest is driven (i.e., motivated) by its relative robustness to overfitting and its generally strong performance on large datasets, particularly when the feature space mixes categorical and continuous attributes.

Comparative Analysis of Firewall Effectiveness. Three different solutions (Palo Alto NGFW, pfSense, MikroTik RouterOS) were tested under a virtual environment (VMware ESXi version 7.0) to determine their effectiveness for overall security within an organization's computing environment.

The lab consisted of three separate networks - one for the potential attacker (Kali Linux), one for the protected computer/server where the application being exploited was located, and one for management. The appliances (Palo Alto NGFW, pfSense, MikroTik RouterOS) were all deployed to their default configurations with no “tweak” settings added for lab use. Attack traffic was generated using various tools in the Kali Linux distribution, including Metasploit, Nmap, sqlmap and hping3. The focus for the lab evaluation was the ability of the various types of devices to detect/prevent the following five types of attacks: Phishing/Social Engineering; Denial of Service (DOS); Exploiting Vulnerabilities; Malware; Exfiltration of Data. The outputs of the various devices were logged so that subsequent evaluation could take place using either the Palo Alto Web Ui and Threat Monitor, pfSense / Snort or Suricata / ClamAV, or MikroTik's built-in logging capabilities. This data was then analyzed; and the results of the testing were compiled and presented in comparative format with respect to each threat category (Singh et al., 2024: 12-15; Feng et al., 2021: 104763; Pandey et al., 2025: 595-600).

Simulated Common Phishing/Social Engineering Processes Identified Through First Test: User Accessing Phishing Websites via Clicking Links; Receiving Malicious Email; Attempting to Download File(s) From Phishing/Scam Websites - This Represents The Typical Risk To Organizations On A Daily Basis. The Reporting Software By Palo Alto Networks Was The Best Performing Product With 98% Of Threats Detected; This Is Possibly Due To The Use Of AI Based URL Filtering And Their Integration With A Large Scale Global Malicious Domain Database. The Reporting Software By pfSense Detected 85% Of Threats Through Signature-Based Detection And DNSBL Filtering. Reporting Software By MikroTik Was Less Effective With The Lowest Rate Of Threat Detection 60% Of Threats Detected ; This Primarily Comes From Blacklisting Sites In A Static Manner.

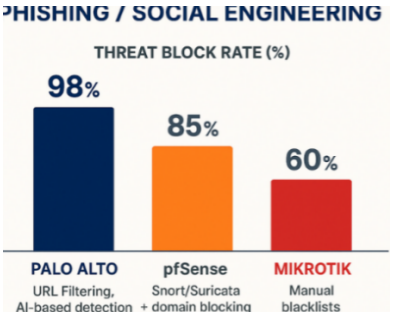

Figure 5. Phishing Processing Results

Resilience to DDoS activity was assessed via the second scenario. Both hping3 and Slowloris were used to " generate " SYN flood attacks and HTTP request floods. Palo Alto was able to block approximately 95% of all malicious traffic through its DDoS Protection module (cloud - based) and automated mitigation processes; pfSense blocked approximately 80% of all malicious traffic with Suricata enabled alongside the standard pf filter ; MikroTik blocked approximately 70% of all malicious traffic ; however , MikroTik 's configuration with regard to queuing and filtering appeared particularly susceptible to HTTP flood patterns.

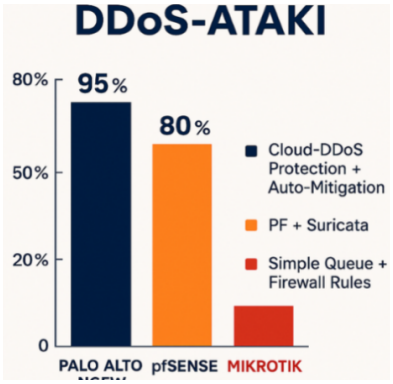

Figure 6. DDoS Effectiveness

In the 3rd test, we looked at protection for exploit attempts, RCE and zero - day style attacks (or tests emulating that behavior). Palo Alto gave us a very high success rate of 97%, which implies that they see advantages from their WildFire analysis engine and their Threat Prevention component. pfSense was able to achieve a 75% success rate based upon the Emerging Threats signatures being extended by Suricata. MikroTik did not have built-in IDS/IPS functionality and was able to mitigate approximately 50% of the simpler attacks being run against it which would be classified as very limited for protective capabilities. In the 4th test we looked at the ability to block malware delivery and execution. Palo Alto was able to provide nearly 100% protection (99%) with DNS Security and sandboxing . pfSense with the addition of ClamAV and Snort was able to achieve 82%. MikroTik, without being equipped with an integrated antivirus module was able to achieve 40% protection - this is not surprising given that testing with MikroTik devices produced three key limitations. Finally, we assessed effectiveness in stopping confidential data leakage. Palo Alto, using its DLP module to inspect multi-layer deep traffic, was able to prevent 96% of data leaks . pfSense was able to achieve 65%. MikroTik was able to stop only 30% due to the lack of deep inspection as well as content filtering capabilities. Taken together, these results indicate that richer inspection and dedicated prevention modules may materially improve coverage across threat categories – although, as always, operational context and configuration choices can influence outcomes.

Figure 7. SQL Injection and Zero Day

Example Code for Training a Random Forest Model. Let's create an IDS/IPS model in Python using the scikit-learn library. Example code:

```
import pandas as pd
from sklearn.ensemble import RandomForestClassifier
from sklearn.model_selection import train_test_split
from sklearn.metrics import classification_report

dataset = pd.read_csv('network_traffic_data.csv')

features = dataset.drop('attack_type', axis=1)  # Все параметры, кроме метки класса
target = dataset['attack_type']  # Тип выявленной угрозы

X_train, X_test, y_train, y_test = train_test_split(
    features, target, test_size=0.2, random_state=42
)

model = RandomForestClassifier(n_estimators=100, random_state=42)
model.fit(X_train, y_train)

predictions = model.predict(X_test)
print(classification_report(y_test, predictions))
```

Example of implementing a Next-Generation Firewall (NGFW). To strengthen the security of an information infrastructure, a Next-Generation Firewall (NGFW) may be integrated into an IDS/IPS architecture. In practice, this combination supports deep inspection of application-layer traffic – most

notably HTTP and HTTPS – which in turn enables more precise identification of suspicious behavior and more selective blocking of malicious flows through content filtering and signature-based analysis.

An illustrative case is the configuration of a Palo Alto firewall for traffic filtering:

```
set device-group <group-name> service-http-profile enable
set device-group <group-name> service-http-profile action allow
```

The relevant command of this security solution activates a security profile that filters out instructions based on the acceptable criteria when control logic is applied (e.g., only requests from approved sources, have the expected headers, contain approved content) and resulting requests to the appropriate destination (s) only if requested data corresponds with these predefined parameters. All requests not conforming to the original definitions will be denied access. Testing performed on the IDS/IPS systems was designed to find out if the NGFWs could detect and block real - world threats versus "textbook attacks." In order to facilitate this evaluation, a sample of frequently used attack types was constructed. All of the test attacks originated from Kali Linux; however, for realistic purposes, a Python script was created to combine multiple attack types into a single complete end-to-end attack scenario for evaluation purposes. Distributed Denial of Service (DDoS) attacks are aimed at consuming all of the available bandwidth and / or processing power of the intended target location in order to hinder or completely take down availability of the targeted location. DDoS attacks are not simply theoretical, but all too real; even if the service disruption is for only a few minutes, it can have significant direct costs in lost revenue, and also negatively impact the integrity and reputation of the attack victim 's business.

In the experiment, a DDoS scenario was simulated using the hping3 utility on Kali Linux. Because hping3 can craft arbitrary packets, it is well suited for reproducing patterns commonly associated with automated botnets. The specific method selected was a SYN flood – among the most widely observed DDoS techniques – in which a high volume of TCP SYN packets is transmitted without completing the three-way handshake. Predictably, this can deplete the server-side resources responsible for tracking half-open connections and, as a consequence, destabilize normal service operation.

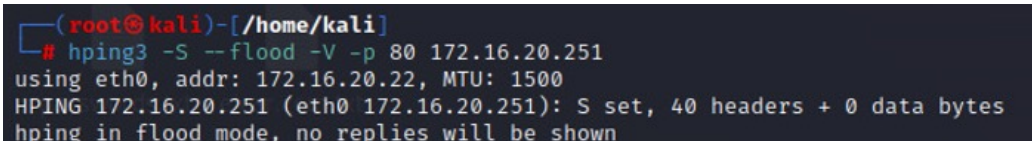

Figure 8. Execution of a DDoS attack using the hping method

The purpose of the below command parameters is as follows : • Enter " sudo " as the command for execution with super user privileges needed to work with raw sockets or otherwise you will receive an error of : socket(): Operation not permitted .

- Flag " S " is set to enable TCP SYN flag to establish a connection.
- The flood mode will set to send the highest number of packets possible at one time.
- Enable " -V " to get verbose output as it is being processed.
- To specify a port number for the target system you will use " -p " , where " 80 " is the number for www (HTTP).
- " 172.16.20.251 " is the target system 's IP address.

While performing SYN Flood testing, the Palo Alto Network Security Platform detected potentially malicious traffic through Early Detection and acted on the anomalous behavior. The NFGW saw an increase in SYN packet ' s to Port 80 and saw a pattern that resulted in an increase in Packets received and flagged the event as a TCP Flood Attack. Based on the event logs, the NFGW recorded the following:

- Threat Type: TCP Flood Attack • Action Taken: Random Drop - Randomly select Packets to drop to lower the amount of traffic on the network.

- Source IP Address: 172.16.20.22 (the machine initiating the attack that is running Kali Linux)
- Destination IP Address: 172.16.20.251 (the machine being tested)
- Severity Level: High (or Critical depending on the security policy in place). In response to this event, the NFGW would cause the pre - configured flood protections to engage (primarily, outbound connection Limits and Dropping packets over an acceptable threshold). This allowed for the prevention of network overload and subsequent service disruption.The corresponding events were captured in the logs and presented in the management interface (Figure 6), which, taken together, suggests that the NGFW supported not only threat identification but also proactive mitigation (and, importantly, traceability for later review).

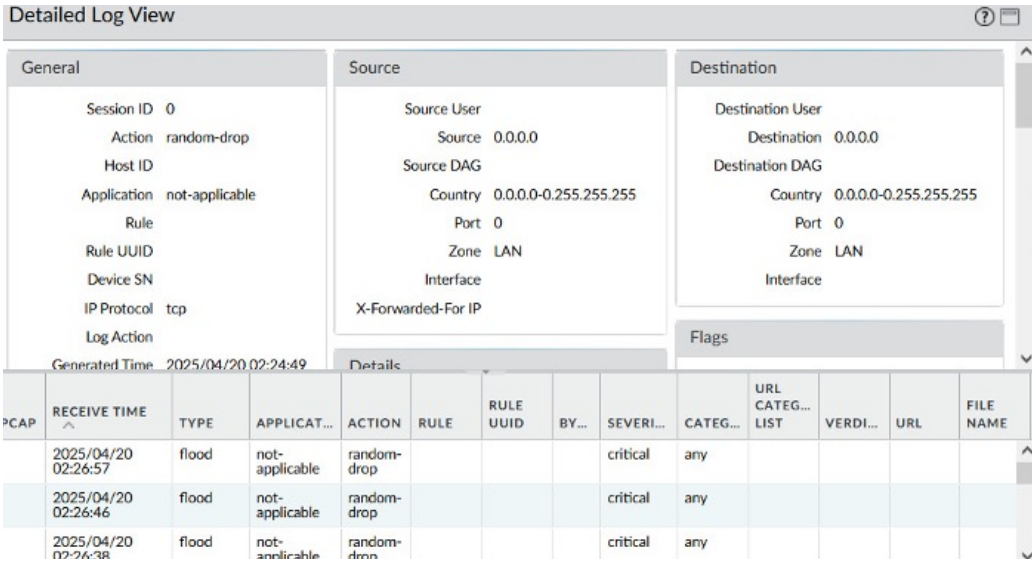

Figure 9. Response of the Palo Alto NGFW to a DDoS attack

Overall, the DDoS simulation indicated strong effectiveness of the Palo Alto NGFW in detecting and blocking this class of network threat. Through implementing a multi - faceted approach that integrated both signature-based and behavioral - based detection methods, the system was able to identify an anomaly or potential threat quickly (both in real - time) as TCP flood attack and activate established defenses to mitigate the impact of the attack. The system also documented all incident - related information in threat logs which will enable subsequent investigations of incidents logged as well as establish visibility into the event activities.

The associated information from test scenarios will be included in the training dataset that will be used for machine-based analysis of the threat (protected by using a Random Forest algorithm). In addition, this initiative will benefit the ongoing development of NGFWs when deployed in conjunction with an IDS/IPS solution through their ability to be sources of telemetry data that can provide definitive labels and related attributes of attacks. Therefore, the overall findings validate the effective utility of this type of solution for real - time resilient protection against denial of service attacks on corporate networks and associated risks.

Final Thoughts. The data support that the Palo Alto platform was found to provide greater capabilities than the other products in all the test scenarios and metrics evaluated. The embedded machine learning analysis (WildFire, DNS Security, and AI modules) resulted in a high rate of blocking APT, Zero-Day, and DLP attacks, and met the responsiveness criteria established for the test cases. pfSense produced strong results due primarily to its integration with Snort/Suricata and its ability to implement highly granular manual rule control, but it appears that additional refinements of pfSense will be necessary to achieve similar levels of effectiveness in more complex environments. In contrast, MikroTik had the capability to perform baseline filtering but showed significant limitations in protecting against advanced attacks. To enhance the degree of accuracy in the evaluation, a custom machine learning model was developed in Python using a Random Forest algorithm; this model was

trained based on the evaluation logs of the next-generation firewall and allowed for the categorization of additional threats, as well as identification of behavior anomalies from the logs and validation of predictive performance using confusion matrices and standard evaluation parameters (Precision, Recall, and F1-score).

Taken together, the study reinforces the importance of a layered approach to network security that combines strong NGFW filtering with intelligent data analysis. Integrating machine learning into the log-processing pipeline can meaningfully increase detection accuracy – especially in situations where attackers are likely attempting to bypass basic controls. The practical findings also suggest that deploying such solutions in corporate infrastructures can provide a high level of protection, assuming correct configuration and regular policy updates (a detail that is easy to overlook, but hard to overstate). More importantly, this research also illustrated the benefits of using detection methods after the fact to find attacks that could not have been detected in the current timeframe. Ultimately these results will provide a basis from which hybrid network security systems can be developed that integrate new-generation firewall technologies with contemporary artificial intelligence techniques, thereby creating more adaptive and scalable protection for businesses' information technology environments as cyber attacks continue to change.

References

Ashoor A.S., Gore S. Difference between intrusion detection system (IDS) and intrusion prevention system (IPS) //Advances in Network Security and Applications: 4th International Conference, CNSA 2011, Chennai, India, July 15-17, 2011 4. – Springer Berlin Heidelberg, 2011. – C. 497-501. [In Eng]

Bishop, C.M. Pattern Recognition and Machine Learning. – New York, NY: Springer, 2006. – 738 p.[In Eng]

Biswas S.K. et al. Intrusion detection using machine learning: A comparison study // International Journal of pure and applied mathematics. – 2018. – Vol. 118. – No. 19. – Pp. 101-114. [In Eng]

Dua M. et al. Machine learning approach to ids: A comprehensive review // 2019 3rd International conference on Electronics, Communication and Aerospace Technology (ICECA). – IEEE, 2019. – Pp. 117-121. DOI:10.1109/ICECA.2019.8822120 [In Eng]

Feng R., Grana D., Balling N. Imputation of missing well log data by random forest and its uncertainty analysis //Computers & Geosciences. – 2021. – T. 152. – 104763 c. DOI:10.1016/j.cageo.2021.104763 [In Eng]

Hamid Y., Sugumaran M., Balasaraswathi V. R. Ids using machine learning-current state of art and future directions // British Journal of Applied Science & Technology. – 2016. – Vol. 15. – No. 3. – Pp. 1-22. DOI:10.9734/BJAST/2016/23668 [In Eng]

Hussain A. Use of Firewall and Ids To Detect and Prevent Network Attacks //International Journal of Technical Research & Science. – 2018. – T. 3. – C. 289-292. DOI:10.30780/IJTRS.V3.I9.2018.002 [In Eng]

İş H.A. Comprehensive Analysis of NGFWs for Cyber-Physical System Security After the CrowdStrike Incident //2024 Global Energy Conference (GEC). – IEEE, 2024. – C. 12-20. DOI:10.1109/GEC61857.2024.10881876 [In Eng]

Kaspersky Lab. Cybersecurity and Artificial Intelligence: New Approaches to Threat Detection. – Moscow: Kaspersky Research Center, 2021. – 210 p. [In Eng]

Kumar I. et al. Development of IDS using supervised machine learning // Soft Computing: Theories and Applications: Proceedings of SoCTA 2019. – Springer Singapore, 2020. – Pp. 565-577. DOI:10.1007/978-981-15-4032-5_52 [In Eng]

Schneier, B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. – 2nd Edition. – New York, NY: Wiley, 2015. – 784 p.[In Eng]

Sharda, R., Delen, D., Turban, E. Analytics, Data Science, and Artificial Intelligence: Systems for Decision Support. – 11th Edition. – Hoboken, NJ: Pearson, 2020. – 832 p. [In Eng]

Sichkar M., Pavlova L.A. short survey of the capabilities of Next Generation firewalls //Computer Science and Cybersecurity. – 2023. – №. 1. – C. 28-33.[In Eng]

Singh A.P., Singh M.D. Analysis of host-based and network-based intrusion detection system //International Journal of Computer Network and Information Security. – 2014. – T. 6. – №. 8. – C. 41-47. [In Eng]

Singh G., Gill K.S. AI-Enhanced Firewalls: Empowering Intrusion Detection with ML and DL //2024 2nd International Conference on Advances in Computation, Communication and Information Technology (ICAICCIT). – IEEE, 2024. – T. 1. – C. 12-15. [In Eng]

Tsai C.F. et al. Intrusion detection by machine learning: A review // expert systems with applications. – 2009. – Vol. 36. – No. 10. – Pp. 11994-12000. DOI:10.1016/j.eswa.2009.05.029 [In Eng]

Whitman, M.E., Mattord, H.J. Principles of Information Security. – 6th Edition. – Boston, MA: Cengage Learning, 2018. – 640 p. ISBN: 978-1-337-10206-3 [In Eng]