NEXT-GENERATION FIREWALL AND ARTIFICIAL INTELLIGENCE

Aleksandar Jokić*,
Marko Šarac,
Saša Adamović

Singidunum University,
Belgrade, Serbia

Abstract:

As cyber threats evolve and become more sophisticated, the need for advanced network security solutions continues to grow. Next-Generation Firewalls (NGFWs) have emerged as a practical solution, utilizing Artificial Intelligence (AI) and Machine Learning (ML) algorithms to provide adaptive and intelligent protection against advanced cyber-attacks. This paper explores the development of NGFWs, their integration with AI and ML, and their impact on network security.

Keywords:

Evolution of Firewalls, Ngfws, Deep Packet Inspection, Intrusion Prevention Systems.

INTRODUCTION

Organizations have become more vulnerable to cyber threats due to increased dependence on digital technology. Traditional firewalls are no longer sufficient to counteract the rapidly changing landscape of cyber threats, and this has led to the development of Next Generation Firewalls (NGFWs), which incorporate advanced features such as deep packet inspection, intrusion prevention systems, and application awareness. Integrating Artificial Intelligence (AI) and Machine Learning (ML) in NGFWs has further enhanced their ability to detect and mitigate cyber threats. This paper discusses the development of NGFWs, their integration with AI and ML, and their impact on network security.

Correspondence:
Aleksandar Jokić

e-mail:
aleksandar.jokic.22@singimail.rs

DOI: 10.15308/Sinteza-2023-36-43

2. NEXT-GENERATION FIREWALLS AN OVERVIEW

2.1. EVOLUTION OF FIREWALLS

Traditional or packet-filtering firewalls rely on static rules to filter traffic based on the source and destination IP addresses, protocol, and port numbers. However, as cyber threats grew more sophisticated, these firewalls became less effective, prompting the development of stateful firewalls. The emergence of web applications and the increasing use of encrypted traffic called for a more advanced firewall solution; this led to the development of NGFWs, which incorporated additional features such as application awareness, deep packet inspection, and intrusion prevention systems [1].

2.2. INTEGRATION OF AI AND ML IN NGFWS

AI and ML algorithms enable NGFWs to analyze and learn from network traffic patterns, identify anomalous behaviour, and adapt their security measures accordingly. This technology has significantly improved our ability to detect, prevent, and respond to cyber-attacks. As cyber threats evolve and become more sophisticated, we will likely see even more innovative applications of AI and machine learning in cybersecurity [2].

2.3. APPLICATIONS OF AI AND MACHINE LEARNING IN CYBERSECURITY

AI and machine learning are in various applications, such as tackling huge volumes of malware, detecting spam and business email compromises, analyzing network traffic, using facial recognition, and more. However, little evidence supports the belief that criminal cyber gangs are already using AI to help generate new malware strains. Evidence shows that artificial intelligence and machine learning are being used in other areas to circumvent protective security measures [3].

2.3.1. Generating deep fake videos and images to phish users and bypass security measures

Deep fakes can create fake identities on social media sites, making it more difficult for security measures to detect malicious activity. For example, an attacker could create a deep fake video of a CEO requesting sensitive information from an employee, tricking the employee into handing over the data [4].

2.3.2. Solving CAPTCHAs to bypass authentication protections

Attackers can use AI to solve CAPTCHAs, making it easier to carry out automated attacks against vulnerable targets.

They were gathering open-source intelligence on organizations to target attackers. AI and ML can collect information on organizations from public sources such as social media, news articles, and company websites. This information can craft targeted attacks against specific individuals or organizations [5].

2.3.3. Network traffic analysis

AI and machine learning can also analyze network traffic and identify patterns indicating a potential attack.

Zero-day attacks. AI and machine learning algorithms can detect anomalous behaviour within an application, which may indicate a zero-day attack [6].

2.3.4. Fraud detection

AI and machine learning algorithms can identify patterns and anomalies that may suggest fraudulent behaviour, such as credit card fraud, identity theft, and account takeover attacks [7].

2.3.5. Vulnerability assessment

AI and machine learning algorithms can identify potential weaknesses attackers may exploit by analyzing data from vulnerability scans and penetration tests [7].

2.3.6. Insider threat detection

AI and machine learning algorithms can identify behaviour indicative of an insider threat by analyzing data from various sources, including employee activity logs, network traffic, and social media activity [7].

2.3.7. Behavioural biometrics

AI and machine learning algorithms can create a unique behavioural profile for each individual based on data such as keystroke patterns, mouse movements, and mobile device usage, making it more difficult for attackers to impersonate legitimate users [8].

2.3.8. Threat intelligence

AI and machine learning algorithms can analyze large amounts of threat intelligence data to identify emerging threats and trends [2].

2.3.9. Cybersecurity risk assessment

AI and machine learning algorithms can help organizations identify potential weaknesses and prioritize their security efforts by analyzing data from various sources, including vulnerability scans, penetration tests, and employee activity logs [1].

2.3.10. Threat hunting

AI and machine learning algorithms can proactively search for threats within an organization's network.

2.3.11. Predictive analytics

AI and machine learning algorithms can predict future cyber-attacks by analyzing historical data and identifying patterns and trends.

2.3.12. Fraud prevention

AI and machine learning algorithms can prevent fraudulent activity before it occurs by analyzing data from various sources, including transaction logs, user activity logs, and social media activity [4].

2.3.13. Network anomaly detection

AI and machine learning algorithms can detect network anomalies that may indicate a potential attack.

2.3.14. Cloud Security

AI and machine learning algorithms can secure cloud-based applications and infrastructure.

2.3.15. Cybersecurity training

AI and machine learning algorithms can provide personalized cybersecurity training to employees.

3. EXPLORING THE KEY AI AND ML TECHNIQUES AND FEATURES OF NEXT-GENERATION FIREWALLS (NGFWS)

Integrating AI and ML algorithms in NGFWs has significantly enhanced their ability to detect and mitigate cyber threats. AI and ML techniques enable NGFWs to analyze large volumes of network traffic data, identify patterns and anomalies, and adapt their security measures accordingly.

3.1. SOME OF THE ESSENTIAL AI AND ML TECHNIQUES USED IN NGFWS INCLUDE:

3.1.1. Deep Packet Inspection

Deep packet inspection is a fundamental technique in NGFWs that enables them to inspect traffic beyond the traditional network and transport layer headers. This technique involves analyzing the content of packets at a granular level to identify threats, malicious payloads, and other security risks, and this allows NGFWs to detect and block various security threats, including malware, viruses, and intrusion attempts [2].

3.1.2. Behavioural Analysis

Behavioural analysis involves analyzing network traffic for patterns, trends, and anomalies that indicate potential security threats. This technique consists of monitoring network traffic and researching ways to identify anomalous behaviour indicative of an attack or security breach. NGFWs use machine learning algorithms to detect and analyze network traffic behaviour and identify potential security threats based on patterns that deviate from the norm [7].

3.1.3. Machine Learning

NGFWs use machine learning to detect and prevent security threats in real-time, such as identifying and blocking malicious traffic before it can reach its target. NGFWs use machine learning algorithms to analyze large datasets and identify patterns and anomalies that may indicate potential security threats. Machine learning algorithms can analyze large volumes of data and detect difficult or impossible patterns for humans [2].

3.1.4. Natural Language Processing

Natural language processing involves analyzing the content of network traffic to identify potential threats based on the language used, sentiment, and context. This technique analyses and understands network traffic's context and meaning to identify potential threats. This technique can identify social engineering attacks, such as phishing emails or spear phishing attacks [9].

3.1.5. Predictive Analytics

NGFWs use predictive analytics to anticipate potential security threats and take proactive measures to prevent them from occurring. Predictive analytics involves analyzing historical data to identify patterns and trends that may indicate potential security threats. NGFWs can use this information to predict future threats and take appropriate action to prevent them from occurring [6].

3.1.6. Threat Intelligence

Threat intelligence involves gathering information about potential security threats from various sources, such as security vendors, government agencies, and industry groups. NGFWs can use this information to identify and block known threats in real-time, improving their ability to detect and prevent security breaches. This technique involves using external sources of threat intelligence, such as threat feeds, to identify and block known threats [6].

3.1.7. User and Entity Behavior Analytics (UEBA)

UEBA analyzes user and entity behaviour to identify potential insider threats and security risks. UEBA involves analyzing user and entity behaviour to identify anomalies that may indicate potential security threats. NGFWs can use UEBA to identify potential insider threats, such as employees accessing sensitive data outside of regular business hours or attempting to access data they are not authorized to access [10].

3.1.8. Heuristics

NGFWs use heuristics to detect and block new and unknown threats based on their behaviour and characteristics. Heuristics involves analyzing the behaviour and characteristics of network traffic to identify potential threats based on patterns or signatures. NGFWs use heuristic analysis to detect threats not previously identified, such as new malware or zero-day attacks [6].

3.1.9. Anomaly Detection

This technique identifies network traffic that deviates significantly from normal behaviour, indicating a potential security threat. Anomaly detection uses statistical analysis to compare current network behaviour against historical data and predefined thresholds. An alert is triggered when network behaviour deviates significantly from the regular pattern, indicating a potential security threat [4].

3.1.10. Contextual Awareness

NGFWs use contextual awareness to understand the context in which network traffic occurs, such as the location of the user or device, to identify potential threats better. Contextual awareness involves analyzing the metadata associated with network traffic, such as the user's location, device type, and application. This information helps NGFWs identify potential security threats more accurately, as some behaviours may be considered normal in one context but abnormal in another [3].

3.1.11. Multi-Factor Authentication

Multi-factor authentication involves using two or more authentication factors to verify a user's identity. NGFWs use machine learning algorithms to identify patterns in user behaviour and determine if a login attempt is legitimate or fraudulent, helping to prevent unauthorized access. NGFWs use machine learning algorithms to detect anomalous login attempts, such as multiple failed attempts or attempts from unfamiliar devices, and take appropriate action, such as blocking the user or notifying an administrator [8].

3.1.12. Data Loss Prevention (DLP)

DLP techniques prevent the unauthorized transfer or exfiltration of sensitive data by analyzing network traffic for patterns that indicate potential data breaches. DLP involves scanning network traffic for sensitive data, such as credit card numbers, social security numbers, or intellectual property, and blocking or encrypting the data to prevent unauthorized transfer. NGFWs use AI and ML techniques to detect and classify sensitive data, even when it is obfuscated or disguised within other data [11].

3.1.13.Reputation Analysis

This technique involves analyzing the reputation of network traffic sources, such as IP addresses or domains, to identify potential threats based on their historical behaviour. Reputation analysis consists of gathering data on the historical behaviour of network traffic sources, such as the number of malicious or spam-related activities associated with an IP address or domain. NGFWs use this information to evaluate the risk associated with network traffic and take appropriate action, such as blocking traffic from high-risk sources [3].

3.1.14. Application Awareness

NGFWs provide deep application visibility and control, allowing administrators to identify and manage specific applications running on the network. Application-aware firewalls can recognize the application protocol and enforce policies based on application type, behaviour, or user identity. This feature allows organizations to identify and mitigate security risks associated with specific applications and prevent unauthorized access to sensitive data [3].

3.1.15. SSL Inspection

NGFWs can inspect SSL-encrypted traffic to identify and block potential threats hidden within the traffic. SSL inspection involves decrypting SSL traffic, analyzing it for potential hazards, and re-encrypting it before sending it to the destination. This feature is essential for preventing attacks that use SSL encryption to hide their activities, such as malware or phishing attacks [7].

3.1.16. Virtual Private Networks (VPN)

NGFWs often include VPN functionality, providing secure remote network access. VPNs allow remote users to connect to the network using an encrypted tunnel, providing a safe and private connection. VPNs are essential for remote workers, branch offices, and business partners to access network resources securely [7].

3.1.17. Intrusion Prevention System (IPS)

IPS systems are essential for protecting against various threats, including viruses, malware, and zero-day exploits. IPS functionality is often integrated into NGFWs to detect and block known and unknown attacks. IPS systems analyze network traffic in real-time, comparing it against available attack signatures and behavioural anomalies. If an attack is detected, the IPS can block the traffic, preventing the attack from reaching its target [6].

3.1.18. Web Filtering

NGFWs can filter web traffic based on categories such as productivity, social media, gambling, and others to prevent employees from accessing sites that are not work-related. Web filtering enables organizations to control web access and reduce the risk of security threats arising from unsecured websites or inappropriate content. It also helps to maintain productivity by reducing distractions and improper use of resources [6].

3.1.19. Centralized Management

NGFWs often include centralized management consoles, which enable administrators to configure, monitor, and manage firewall policies across multiple locations or devices from a single interface. Centralized management provides a holistic view of network traffic, simplifying the management of security policies and reducing the risk of errors or inconsistencies in the policy application [6].

3.1.20. Advanced Threat Protection

NGFWs often include advanced threat protection features such as sandboxing, threat emulation, and threat extraction to detect and prevent sophisticated attacks. These features use advanced AI and ML techniques to identify and analyze potential threats, providing a more comprehensive level of protection. Sandboxing, for example, isolates unknown files in a virtual environment to test their behaviour and identify any malicious activity [10].

In summary, these features are critical to the effectiveness of NGFWs in detecting and preventing a wide range of known and unknown security threats. AI and ML techniques in NGFWs enable organizations to detect and respond to security threats more quickly and effectively, improving their overall security posture.

Furthermore, as cyber threats evolve, organizations must adopt and utilize NGFWs with advanced AI and ML capabilities; this will not only improve their ability to detect and prevent cyber attacks but also help them stay ahead of the latest threats. Ultimately, investing in

NGFWs with advanced AI and ML techniques is an investment in the security and resilience of an organization's network infrastructure.

4. CHALLENGES AND FUTURE PROSPECTS OF AI-ENABLED NGFWS

Implementing AI and machine learning algorithms in Next Generation Firewalls (NGFWs) has significantly enhanced their ability to detect and mitigate cyber threats. However, several challenges must maximize the benefits of these technologies.

Data privacy and legal concerns are among the primary challenges of implementing AI and ML algorithms in NGFWs. These algorithms require access to vast network traffic data, which may include sensitive information. This raises concerns about data privacy and potential violations of data protection laws.

The computational complexity of AI-enabled NGFWs is another significant challenge. Implementing machine learning algorithms can increase computational complexity and resource consumption, impacting network performance. Adversarial attacks are also a significant challenge for AI-enabled NGFWs. Cybercriminals may use malicious machine learning techniques to evade NGFWs, creating new network security challenges.

The need for the explainability of AI-enabled NGFWs is another challenge. Machine learning algorithms can make decisions based on complex models that are difficult to understand or interpret. This lack of explainability can make troubleshooting or identifying the cause of security issues challenging.

Training data is also a significant challenge for AI-enabled NGFWs. The accuracy and effectiveness of machine learning algorithms depend on the quality of the training data used. However, training data may need to be completed, leading to accurate or complete security decisions.

Integrating AI-enabled NGFWs with legacy systems can also be a challenge. Legacy systems may need to be compatible with the latest AI and machine learning technologies, making it challenging to implement NGFWs effectively.

High cost is another challenge for AI-enabled NGFWs. They may require significant hardware, software, and professional personnel investment, making them cost-prohibitive for some organizations.

Finally, using AI and ML in NGFWs raises ethical concerns, such as potential discrimination or bias against certain groups or individuals. Organizations must ensure that their AI-enabled NGFWs are designed and implemented ethically and responsibly.

5. PROSPECTS OF AI-ENABLED NGFWS

Despite the challenges, AI-enabled NGFWs hold great promise for the future of network security. These technologies offer several benefits, including [12]:

- Enhanced threat intelligence sharing: With AI and ML algorithms, NGFWs can analyze vast amounts of threat data from various sources, identify commonalities and patterns, and share this information with other NGFWs and security vendors. This can lead to more effective collective security, helping organizations to stay one step ahead of cyber attackers.
- Improved network visibility: AI-enabled NGFWs can analyze encrypted traffic to identify anomalies and detect threats that may be hidden within encrypted communication. This can lead to more effective threat detection and prevention measures and help organizations protect their sensitive data better.
- Autonomous security solutions: Developing AI and ML algorithms may pave the way for fully autonomous network security solutions. These autonomous security systems would detect and respond to threats in real time without human intervention, potentially reducing the risk of human error and improving overall security posture.
- More accurate threat detection and prevention: AI and ML-enabled NGFWs offer more accurate threat detection and prevention, adaptive security that can adjust to changing threat landscapes, cost savings through reduced reliance on human intervention, and improved compliance with regulatory requirements.
- Advanced Behavioral Analysis: AI and ML algorithms have the potential to provide advanced behavioural analysis of network traffic, allowing NGFWs to detect and prevent threats based on anomalous behaviour.
- Predictive Analytics: NGFWs can analyze vast amounts of data to identify patterns and predict future threats, allowing them to take proactive measures to prevent attacks before they occur.

- Quantum Computing: NGFWs can harness the power of quantum computing to improve their threat detection and prevention capabilities, allowing them to analyze vast amounts of data quickly and accurately.
- Cybersecurity Ecosystems: AI and ML technologies can help NGFWs collaborate and share threat intelligence with other security systems, developing interconnected cybersecurity ecosystems.
- Immersive Technologies: Immersive technologies such as virtual and augmented reality can provide real-time visualization and network traffic analysis, allowing security professionals to quickly identify threats and take appropriate action.
- Explainable AI: Explainable AI refers to the development of transparent AI algorithms that can explain their decision-making process, making it easier to refine the NGFW's rules and policies for more effective threat detection and prevention.
- Edge Computing: NGFWs could be deployed on edge devices such as routers and switches, allowing real-time threat detection and prevention at the network's edge.
- Cybersecurity as a Service: AI and ML technologies in NGFWs could enable the development of cybersecurity as a service (CSaaS) offerings, providing NGFWs with AI and ML capabilities to detect and prevent threats.
- Privacy-Preserving Technologies: Privacy-preserving technologies such as homomorphic encryption could ensure that sensitive data remains encrypted even when AI and ML algorithms are processed in NGFWs.
- Biometric Security: NGFWs could incorporate biometric authentication methods such as fingerprint or facial recognition to improve access control and prevent unauthorized access to the network.
- Adversarial Machine Learning: Adversarial machine learning involves designing AI and ML algorithms to be robust against attacks that aim to manipulate their decision-making process.
- GANs for Network Security: GANs could generate synthetic network traffic that mimics real traffic, allowing NGFWs to test and refine their threat detection and prevention capabilities more effectively.
- Swarm Intelligence: AI algorithms inspired by the behaviour of natural swarms could design AI algorithms that are more adaptive and flexible, allowing NGFWs to respond quickly to new and emerging threats.
- Memory-Augmented Neural Networks: Memory -augmented neural networks (MANNs) could enable NGFWs to learn from past threats and use this knowledge to detect and prevent future threats more effectively.
- Hybrid AI Algorithms: Hybrid AI algorithms could enable NGFWs to detect and prevent threats by leveraging the strengths of different AI algorithms more accurately.

6. CONCLUSION

Integrating AI and ML algorithms in NGFWs has significantly enhanced their ability to detect and mitigate cyber threats. Despite the challenges associated with data privacy, legal concerns, computational complexity, and adversarial attacks, AI-enabled NGFWs hold great promise for the future of network security. Improved threat intelligence sharing, enhanced network visibility, and the potential for autonomous security solutions are just some of the exciting prospects that lie ahead. As cyber threats evolve, AI and ML's ongoing development and integration in NGFWs will ensure robust protection for organizations worldwide.

7. REFERENCES

[1] R. W. Anwar, T. Abdullah and F. Pastore, "Firewall Best Practices for Securing Smart Healthcare Environment: A Review," *Applied Sciences*, vol. 11, no. 19, pp. 1-9, 2020.

[2] T. T. Nguyen and V. J. Reddi, "Deep Reinforcement Learning for Cyber Security," *IEEE Transactions on Neural Networks and Learning Systems*, pp. 1-17, 2021.

[3] Coulter, R. &. Han, Q.-L. &. Pan, L. &. Zhang, J. &. Xiang and Yang, "Data-Driven Cyber Security in Perspective--Intelligent Traffic Analysis," *IEEE Transactions on Cybernetics*, vol. 1, pp. 1-13, 2019.

[4] M. Westerlund, "The Emergence of Deepfake Technology: A Review," *Technology Innovation Management Review*, pp. 1-52, 2019.

[5] G. Hidalgo, J. &. Alvarez and Gonzalo, "CAPTCH-As. An Artificial Intelligence Application to Web Security," *Advances in Computers*, vol. 83, pp. 100-190, 2011.

[6] Ali, Rehman, Imran, Adeem, Iqbal and Kim, "Comparative Evaluation of AI-Based Techniques for Zero-Day Attacks Detection," *Electronics*, vol. 23, no. 3934, p. 11, 2022.

[7] Eberle, W. &. Holder, L. &. Graves and Jeffrey, "Insider Threat Detection Using a Graph-Based Approach," *Journal of Applied Security Research*, vol. 6, p. 10, 2010.

[8] Krishnamoorthy, S. &. Rueda, L. &. Saad, S. &. Elmiligi and Haytham, "Identification of User Behavioral Biometrics for Authentication Using Keystroke Dynamics and Machine Learning," *Conference: the 2018 2nd International*, pp. 1-7, 2018.

[9] Oliveira, N. &. Pisa, P. &. Andreoni, M. &. Medeiros, D. &. Menezes and Diogo, "Identifying Fake News on Social Networks Based on Natural Language Processing: Trends and Challenges.," *Information*, vol. 12, p. 38, 2021.

[10] Salitin, M. &. Zolait and Ali, "The role of User Entity Behavior Analytics to detect network attacks in real time," *Conference: 2018 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*, pp. 1-5, 2018.

[11] Ali, Jalal, Ahmed and Ibrahem, "Data loss prevention (DLP) by using MRSH-v2 algorithm," *International Journal of Electrical and Computer Engineering (IJECE)*, pp. 3615-3622, 2020.

[12] Chan and Jack, "AI (Artificial Intelligence) and Machine Learning in the Cybersecurity Battle," 5 4 2022. [Online]. Available: https://www.fortinet.com/blog/business-and-technology/battle-ai-ml-cybersecurity-world. [Accessed 23 4 2023].