ISSN: 2754-6659

Journal of Artificial Intelligence & Cloud Computing

SCIENTIFIC Research and Community

Review Article

Open Access

Next-Gen Firewalls: Enhancing Cloud Security with Generative AI

Seshagirirao Lekkala[1]*, Raghavaiah Avula[2] and Priyanka Gurijala[3]

[1]Senior Software Engineer, Cisco Systems Inc, USA

[2]Sr. Principal Engineer, Palo Alto Networks Inc, USA

[3]Software Engineer, Microsoft Corporation, USA

ABSTRACT

Next-generation firewalls are available and use machine learning and generative modeling to enhance the detection of hard-to-detect cyber threats. These systems incorporate advanced security controls, policies, and protocols with Layer 7 of the OSI model. This chapter updates these steep AI-based protection systems and applications. We present a taxonomy of machine learning solutions for cybersecurity and outline a family of next-gen firewalls that incorporate intelligent AI-based technologies, including deep learning, generative adversarial networks, and convolutional neural networks. We present extensive experimental results that show how deep generative Gaussian models effectively identify hard-to-detect threats of particular interest. Then we conclude with recommendations and further R&D directions within the next-generation firewall ecosystem that benefits significantly from AI and machine learning.

Next-generation (next-gen) firewalls are already in the cybersecurity market, delivering crucial advancements previously not seen in traditional firewalls, in addition to incorporating the advanced security controls, policies, and protocols with Layer 7 of the OSI model. In general, next-gen firewalls leverage Artificial Intelligence (AI) and machine learning resources to keep up with the ongoing evolution of cyber threats as the systems develop and learn from accurate and incident data conditions. However, a shortcoming of some of the most expensive and advanced next-gen firewalls available is their reliance on supervised learning, which may require shared sensitive information from industries and extra difficulties.

***Corresponding author**

Seshagirirao Lekkala, Senior Software Engineer, Cisco Systems Inc, USA.

Received: August 14, 2024; **Accepted:** August 20, 2024; **Published:** August 28, 2024

Keywords: Next-Generation Firewalls, Machine Learning, Generative Modeling, Cybersecurity, Layer 7 OSI Model, Deep Learning, Generative Adversarial Networks, Convolutional Neural Networks, Deep Generative Gaussian Models, AI-Based Protection, Generative AI, Defensive Classification Model, Improving NGFW, Network Traffic Log, Next-Generation Firewalls, Security Threat Response

Introduction

From state-sponsored attacks against critical infrastructures to malicious ransomware campaigns, ensuring the security, integrity, and confidentiality of an organization's information and systems has never been more challenging. To combat the myriad attack vectors and adversaries intent on doing harm, network and computer security technologies must continue to evolve, improving our cyber defense capabilities. The Next-Generation Firewall (NGFW) represents one of the premier defensive systems that network security practitioners can utilize to ensure the confidentiality, integrity, and availability of the entity's resources, as well as visibility and control over their apps and services, both on-premises and in the cloud. However, like other security technologies, restrictions prevent current NGFW from further improving threat detection and enhanced security automation.

This paper outlines how the integration of state-of-the-art Generative Artificial Intelligence (AI) and Machine Learning (ML) technologies represent the future for vastly improving the defensive capabilities of NGFW, significantly enhancing active cybersecurity threat responsiveness and cooperation. The integration of state-of-the-art Generative Artificial Intelligence (AI) and Machine Learning (ML) technologies into Next-Generation Firewalls (NGFW) promises to revolutionize cybersecurity defenses by enhancing threat detection and response capabilities. By leveraging AI and ML, NGFW can analyze vast amounts of data in real-time, identifying patterns and anomalies that traditional security measures might overlook. This proactive approach allows for the automation of threat identification and mitigation processes, enabling organizations to respond to emerging threats more swiftly and effectively. Furthermore, these advanced technologies can facilitate improved visibility into applications and services across both on-premises and cloud environments, fostering a more robust security posture. As adversaries become increasingly sophisticated, the adaptive capabilities of AI and ML will be essential in ensuring the confidentiality, integrity, and availability of critical systems, transforming NGFW from reactive tools into proactive defenders in the cybersecurity landscape.

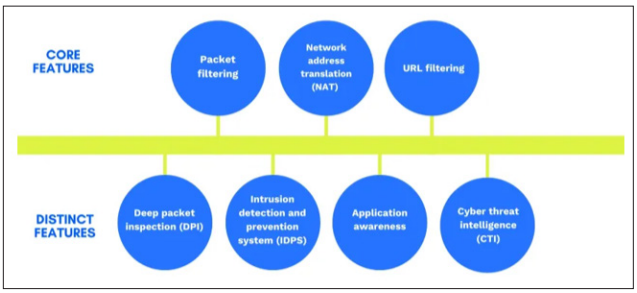

Figure 1: Next-Generation Firewall

Background and Significance

In this technology-driven information age, when cyberattacks are increasing in quantity and sophistication, artificial intelligence (AI) and machine learning are revolutionizing the field of cybersecurity. Experts agree that the highly sophisticated and mutating cyberattacks that happen in cyberspace require a proactive solution that effectively eliminates the seed of cyberattacks. With artificial intelligence and machine learning, next-generation firewalls (NGFW) cross the traditional physical barriers and leverage network traffic log data to understand and safeguard enterprise information assets and resources.

This chapter reveals related work from knowledge of the network security triangle, and upon this foundation, provides extensive research discussion relative to improving the security threat responses with data analytics and defensive learning models using generative AI and unsupervised classification methods. This research contributes to the NGFW commercialized product and industry knowledge.

Next-generation firewalls (NGFW) combine the capabilities of firewalls with intrusion detection and prevention and integrate security services such as those offered by antivirus, intrusion prevention, application identification and filtering, and advanced persistent threat protection. An important distinction of NGFW is the ability to inspect and learn the application status through the packaging layers, which enables detailed decisions to be made for protecting enterprise information assets and ensuring good governance about network usage.

Existing observation research has determined that NGFW can handle cyberattacks based on the virtual reassembly and modeling of application payload content. However, researchers also argue that, in cyberspace, the rapid and mutating cyberattacks generate false positives that present a significant concern to network security. These concerns emerge from the considerable impact on the performance of NGFW without involving the engagement of verification methods. Because of this, extensive research has emerged and extended prior suggestions that look to machine learning, optimization methods, and complex pattern recognition methods to resolve the false positive concern and effectively validate NGFW's decision-making capability.

Research Objectives

Since both targeted attacks and cybercrime represent ever-increasing threats that can have very serious financial and even human consequences, there is a growing need for improving intrusion detection systems. With both targeted attacks and cybercrime having the common property that the respective attackers are highly motivated, intelligent, and adaptive entities, creating increasingly more efficient, more accurate, more adaptable, and scalable systems should be an important research goal. These are the four main objectives of the research presented in this thesis paper: to investigate how to infuse features from standard and next-gen firewall technology to create a conceptually similar platform for intrusion detection, continuously improve security by using training and/or adapting generative AI and machine learning models, explore if record-level training shadows Pac-Man-type evolutionary exploration behavior, and test if filtering known attacks can both promote significant energy saving and speed up attack detection.

Scope and Limitations

The present work focuses on the efficient implementation of generative AI, particularly DCGAN, as a component of next-generation firewalls for payload visualization and analysis. We make use of the generated images to identify the feasibility of implementing conditional GANs to detect application-specific attacks. We present a general architecture for a next-generation firewall and evaluate the feasibility of integrating a generative AI technique to defend network systems. We also discuss the key techniques to couple a modified GAN with DPI engines. We present a hypothetical phased development process; however, we provide only a partial set of data with the GAN outputs and visualize only some of the expected virus and attack payloads through the generative model following the payload preprocessing to pixel formats.

We consider further that the training and performance data of the AI is not generalized and will require extensive fine-tuning to adapt to the dynamic real-world network data in various scenarios. The performance assessment of the AI-assisted next-generation firewall should incorporate the computational efficiency, delay, and false-positive/false-negative performance, and we only provide a few outputs of the testbed scenarios under continuous adversarial perturbations without fine-tuning. We outline some of the deep learning optimization algorithms currently available, such as actor-critic, Few Shotguns and recent work on RLSR and Mask GAN. These could provide guidance on the specialized designs or should be considered for the future development of next-generation AI-driven network security systems; the performance and further directions will depend on the implementation and fine-tuning of real-world network traffic data. This work explores the integration of generative AI, specifically DCGANs, into next-generation firewalls for enhanced payload visualization and analysis. By leveraging generated images, we investigate the potential of conditional GANs to detect application-specific attacks, proposing a general architecture for such firewalls that incorporates this innovative approach. Our analysis highlights key methodologies for coupling modified GANs with Deep Packet Inspection (DPI) engines, alongside a hypothetical phased development process. While we present preliminary data from GAN outputs that visualize certain virus and attack payloads post-preprocessing, we acknowledge that the training and performance metrics are not yet generalized, necessitating extensive fine-tuning to adapt to diverse real-world network scenarios. The assessment of our AI-assisted firewall encompasses critical factors like computational efficiency, latency, and the balance of false positives and negatives. Furthermore, we touch on advanced deep learning optimization algorithms such as actor-critic, Few Shotgun, and recent developments like RLSR and Mask GAN, suggesting these could inform future enhancements of AI-driven network security systems, contingent upon further implementation and real-world data fine-tuning.

Equation 1: Logistic Regression

$$Y = \ln\left(\frac{p}{1-p}\right) = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \ldots + \beta_n X_n$$

$$\ln\left(\frac{p}{1-p}\right) = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \ldots + \beta_n X_n$$

Evolution of Firewalls

While UTM (Unified Threat Management) has been the traditional defense in place against malware and advanced threats, well beyond the above-mentioned NGFW features, these systems are becoming less and less effective. Therefore, there has been a renewed interest in maximizing the utilization of firewalls in detecting adverse traffic and raising alerts. Traffic monitoring alone is not effective in finding indicators of compromise; added intelligence enhanced with AI and generative machine learning provides the necessary solution capability. With AI-based approaches and advanced deep learning techniques, algorithms are being trained to ingest the content of network traffic, regardless of whether it is in clear or encrypted form. This content is then processed and analyzed to find various indicators of compromise.

Generative AI machines learn the structure of the input data traffic. They then generate multiple variations of such data that share the same underlying structure. In this process, AI analyzes and learns the structure to synthesize data that looks similar to the original input data type. Deep learning models are designed to recognize threat indicators in heavily encrypted traffic. In this model, the deep learning neural network is trained on clear traffic data. After exposure, the network can identify malware, command and control communication, and lateral movement; results are generated on secure or encrypted traffic. The gathered security analytics through this AI-enabled Deep Learning system help evolve the signature-based traditional methods to the next level.As traditional Unified Threat Management (UTM) systems increasingly fall short in effectively combating malware and advanced threats, there is a growing focus on enhancing firewalls' capabilities to detect adverse traffic and trigger alerts. Relying solely on traffic monitoring is insufficient for identifying indicators of compromise; thus, integrating AI and generative machine learning provides a vital solution. AI-driven approaches utilize advanced deep learning techniques to analyze both clear and encrypted network traffic, enabling algorithms to detect potential threats more effectively. Generative AI models learn the underlying structure of input traffic and can produce variations that mirror this structure, enhancing the ability to recognize patterns associated with malicious activities. By training deep learning neural networks on clear traffic data, these models become adept at identifying malware, command-and-control communications, and lateral movement within networks, even in encrypted environments. This AI-enabled analytics framework advances traditional signature-based methods, evolving them into a more proactive and adaptive security paradigm capable of addressing the complexities of modern network threats.

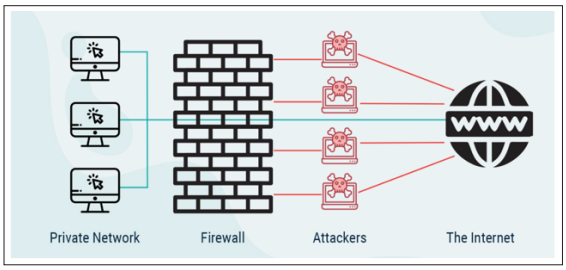

Figure 2: Evolution of Firewalls

Traditional Firewalls

The demand for Next-Generation (NG) firewalls is growing, and it's significant for the cybersecurity landscape. As of 2021, we have learned about traditional firewalls and their capabilities. In this section, we start by introducing traditional firewalls and discussing their capabilities, including the problems they solve and the architecture they deploy. Next, we conclude this section by summarizing the shortcomings of traditional firewalls that need to be overcome.

Firewall technology has become one of the best tools for ensuring network security. When a network is operated under closed management, it can be used to block malicious behaviors effectively. As a kind of economic and efficient network security mechanism, the rapid growth of the Internet has brought about higher performance and reliability requirements for firewalls. A traditional firewall is a boundary defense device that inspects data packets passing through it and can only decide whether or not to pass the packet based on the network layer and so-called transport layer network headers, essentially monitoring application traffic, ports, and connected devices by ignoring the inside of the packet. It can use User Datagram Protocol (UDP) or Transmission Control Protocol (TCP) to filter packet contents, but only part of it can filter deeper protocol stack contents based on filtering HTTP, File Transfer Protocol (FTP), and Simple Mail Transfer Protocol (SMTP) popular applications' string information.

Next-Generation Firewalls (NGFWs)

Following the introduction of APTs, the focus of the cyber world shifted from the established trend to creating the next-gen firewall. Security applications, such as antivirus software, have always relied on detection signatures for every entity that should be protected. Once those signatures become known to bad actors, they adapt new ones to penetrate security barriers without notice during their breaches. Moreover, the process of incorporating signatures is lengthy and expensive. Threats have developed rapidly in recent years, which has led to a modern security landscape in which AI and ML have made substantial inroads due to their ability to avoid the traditional limitations of signature and rule-based approaches.

The mantra of the next-gen firewall, which leads current defensive cybersecurity thinking, is namely 'assume breach'. In standard practice, most cyber-attacks utilize malware in the form of APTs, with the attribution of events squarely aligned as targeting malicious activity being operated by bad actors. Complex pieces of armed software are designed based on a custom malign objective to avoid detection by security applications, modify sophisticated censorship filters, breach conviction standards to secure a strategic position with the radial firewall or raise global geopolitical stimuli intended by the global KPI. The rise of Advanced Persistent Threats (APTs) has fundamentally reshaped the cybersecurity landscape, pushing the focus from traditional security measures to more sophisticated defenses, particularly next-gen firewalls. These firewalls embody the 'assume breach' mentality, acknowledging that threats can bypass conventional defenses. Traditional security applications, reliant on detection signatures, face challenges as attackers quickly adapt and innovate to evade detection. The lengthy and costly process of signature updates further exacerbates vulnerabilities. In response, artificial intelligence and machine learning have emerged as critical tools, enabling proactive threat detection and response that transcends the limitations of rule-based approaches. As cyber-attacks increasingly leverage custom-designed malware aimed at evading traditional security measures and achieving strategic objectives, the need for adaptive, intelligent security

solutions has never been more pressing. This dynamic environment demands continuous evolution in cybersecurity strategies to outpace malicious actors and safeguard sensitive information.

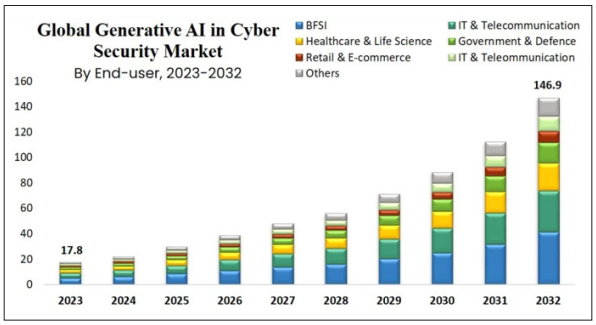

Figure 3: Generative AI in Cyber Security

Role of Generative AI and Machine Learning in Cybersecurity

Generative AI models assist in various tasks like generating conversational text, creating robust Generative Adversarial Networks (GANs), and supporting the development of data anonymization tools such as Differential Privacy. In computer security, GANs can be used to generate adversarial examples to support the development and detection of evasion attacks on AI systems. Besides, they can also help generate robust malware variants to keep pace with the evolving threat landscape.

At a high level, machine learning algorithms learn to perform specific tasks from sample data by identifying patterns within the data. Machine learning has independently gained a significant foothold in the realm of cybersecurity. Specifically, supervised learning and unsupervised learning models help detect variations in malware and network traffic flows, identify abnormalities in system logs and trajectories, and classify web traffic.

Given the emerging thrust on AI and ML within cybersecurity, the questions are: what roles do these futuristic technologies play in the evolution of the next-gen firewalls and how do they ensure improved capabilities for business entities in safeguarding the multi-cloud environments? In fact, instead of being a mere keyword in attacks, businesses use ML to be one step ahead in threat identification and defense. When used correctly, ML performs complex pattern recognition and task assistance more effectively than traditional handcrafted rule-based systems. However, our modeling also shows that without careful implementation, devices and software with less complex ML models are more vulnerable to attacks. This implies that rather than a full stop, organizations should view this as a stepping stone in ML development with better models and sensor devices for cybersecurity.

Equation 2: Value at Risk

$$\mathrm{VaR}_{1-\alpha}(X) := \inf_{t\in\mathbf{R}}\{t : \Pr(X \le t) \ge 1-\alpha\},$$

$$\mathrm{CVaR}_{1-\alpha}(X) := \frac{1}{\alpha}\int_0^{\alpha} \mathrm{VaR}_{1-\gamma}(X)d\gamma,$$

$$\mathrm{RVaR}_{\alpha,\beta}(X) := \frac{1}{\beta-\alpha}\int_{\alpha}^{\beta} \mathrm{VaR}_{1-\gamma}(X)d\gamma,$$

$$\mathrm{EVaR}_{1-\alpha}(X) := \inf_{z>0}\{z^{-1}\ln(M_X(z)/\alpha)\},$$

Overview of Generative AI

There are several approaches to generative AI. These include variational autoencoders, generative adversarial networks, and reinforcement learning. Generative AI differs from discriminative algorithms that are used heavily in machine learning. Generative models are conceptually pretty simple: they just generate new data instances and are fundamental for unsupervised learning applications. Our two real-life superheroes of deep learning (convolutional neural networks for images and (recurrent) neural networks for sequences) can also perform generative tasks. Variational autoencoders are a generative model that learns a posterior distribution over the input space. This idea is useful to produce new digit images never seen before. Variational autoencoders can be used to learn efficient representations of tokens from corpora of documents, where the model learns word statistics.

Deep generative models or generative models are poorly researched compared to discriminative models. This is probably because it is hard to generate new data instances, let alone interpretable multimodal models. Research in this field has been emerging continuously, along with new approaches to improve their performance in highly diverse and subjective problem domains. There are many possible criteria to evaluate generative models—accuracy, sample quality, diversity, novelty vs familiarity, information disentanglement, interpretable and controllable factors of variation, efficient optimization, and scalable inference. According to a recent review, generative models have come a long way, tackling high-dimensional unstructured distributions, and have become essential for many AI applications when facing data generation and unsupervised learning problems. In particular, deep learning has benefited significantly from generative models with methods such as neural Wavetable synthesizers for audio generation, style GANs for unconditioned image generation or face Style GANs, and UDTMs and UDTSMs for extremely unsupervised discrete data, just to name a few. Generative AI encompasses several innovative approaches, including variational autoencoders (VAEs), generative adversarial networks (GANs), and reinforcement learning, distinguishing itself from the more commonly utilized discriminative algorithms in machine learning. At its core, generative models aim to produce new data instances, making them essential for unsupervised learning applications. Notably, convolutional neural networks (CNNs) and recurrent neural networks (RNNs) the cornerstones of deep learning for images and sequences—can also engage in generative tasks. VAEs, for instance, effectively learn a posterior distribution over input data, enabling the generation of entirely new digit images and efficient representation of word statistics in text corpora. Despite their potential, deep generative models remain less explored than their discriminative counterparts, partly due to the inherent challenges of generating new, interpretable multimodal data. However, ongoing research is progressively enhancing their performance across diverse and subjective domains. Evaluating generative models involves various criteria such as accuracy, sample quality, and the balance between novelty and familiarity. As advancements continue, generative models have become vital for numerous AI applications, exemplified by techniques like neural Wavetable synthesizers for audio, style GANs for image generation, and unsupervised discrete data models, significantly enriching the field of deep learning.

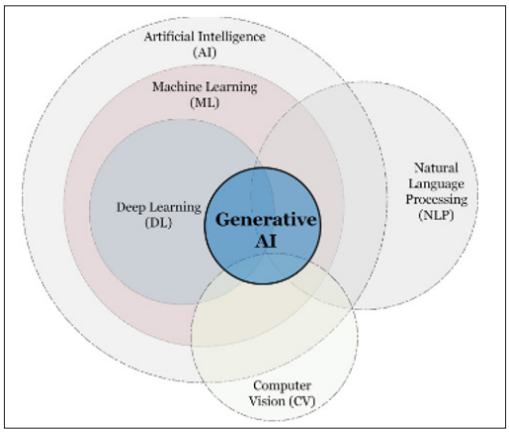

Figure 4: Overview of Generative AI

Machine Learning in Cybersecurity

Machine learning is involved in cybersecurity in many aspects. One of the main uses of machine learning is that it can be introduced in intrusion detection systems to allow them to learn what kind of traffic is normal and what kind can be potentially harmful. This way, intrusion detection systems can be constantly learning and adapting their response to new threats that may appear. This is important since cybersecurity is a never-ending race: hackers are constantly creating new threats, and cybersecurity systems need to constantly adapt themselves to keep up with the latest dangers. Another application of machine learning is in malware detection. Random forests (a type of ensemble machine learning method) can be used to detect new computer viruses, even when they have not been included in the databases of traditional antivirus software. Furthermore, as cloud computing continues to become more popular and we deal with large databases of information every day, machine learning can be used to assess and control who has access to the databases. This is important to avoid any possible data breaches that might occur. One way in which machine learning can be used for access control is to create intelligent systems that can learn from the behavior patterns of your users.

Integration of Generative AI and Machine Learning in Next-Gen Firewalls

With the increasing rate of sophisticated attacks such as advanced persistent threats (APTs), the existing state-of-the-art next-generation firewalls (Next-Gen FWs) are insufficient as they offer signature-based attack detection only. To enhance cybersecurity, standard Next-Gen FWs should be complemented with generative AI, especially the VAE which can generate features for better attack detection. This work proposes REMGEN as a proof of concept. The complementary generative adversarial networks (GANs) for better attack generation to fool the VALUE of REMGEN will be future work.

To enhance cybersecurity, enabling Next-Gen FWs for attack detection with generative AI can significantly close the auto-generated traffic data in our use case. A standard Next-Gen FW is limited to the use of classic machine learning such as support vector machines (SVMs) on variance features to detect APTs. The main limitation of this method is that the attack traffic can easily be modified to bypass the detection system. Meanwhile, generative machine learning, like VAE, holds promise by training a model to learn the distribution of the entire feature set mapping to its original traffic. Thus, the ones mapped distant from the modeled distribution are the ones with the tasting feature that can fool the VAE for better attack detection.

Benefits and Challenges

So, what benefits do decision evaluators bring to automated decision-making? They bring the ability to be context-sensitive, to an abductive reasoning system that does not make sub-goal-contribution or intended contributions. It is not that the decision evaluator promised so much and delivered so little. On the contrary, the Decisions Evaluator sits astride the discussion of the other insights and limitations as an Archon. It decides on the importance of the insights at different levels of the world model. If a query is put to the classifier, these must be swept up and the answers synthesized to provide an unambiguous response.

The Decisions Evaluator's multiple flavors of knowledge representation supersede the logical and symbolic representation method and the VPN of Chapter 3. Those tools pertain to the earlier, logical, operations of finding, framing, formalizing, and supporting questions in the classifier. The Decisions Evaluator's abductive reasoning system also uses arithmetic, numerical, uncertainty, inexpert, or fuzzy representations. It can apply knowledge to trace and coordinate information whatever is needed to carry out the full evaluation in the decision loop.Decision evaluators play a crucial role in automated decision-making by providing context-sensitive analysis within an abductive reasoning framework, distinguishing themselves from systems that merely focus on sub-goal contributions. Rather than underperforming against expectations, decision evaluators act as an Archon, guiding the synthesis of insights and limitations across various levels of a world model. When a query is directed to the classifier, these evaluators effectively aggregate relevant information to generate clear, unambiguous responses. This versatility enables decision evaluators to comprehensively trace and coordinate information, ensuring that all necessary evaluations are integrated into the decision loop, thereby enhancing the overall effectiveness and reliability of automated decision-making processes.

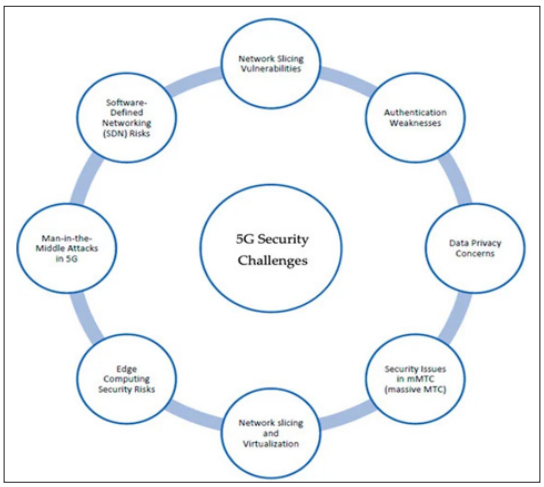

Figure 5: Challenges of Generative AI

Use Cases

There are a wide range of use cases for AI in next-gen firewalls. All involve making the firewall smarter and more capable of performing a more contextual inspection of traffic and content to improve security detection and increase the identification, containment, and neutralization of malware; reduce false positives; and respond to security events in real-time.

Given the ongoing escalation of attacks and data breaches, there can never be too much focus on security. Indeed, the number one-use case for AI-driven next-gen firewalls is enhancing

overall enterprise cybersecurity. With real-time traffic and content scanning at enforced speeds, these firewalls can enhance security risk aversion by identifying, containing, and neutralizing potential information security threats.

Many organizations conduct threat detection in an offline, incubated environment, and then often need to conduct remediation through systems separate from the firewall. The use of AI techniques in the firewall to detect then appropriately respond to or remediate security events, when used in conjunction with other AI use cases in security, can lead to real-time, single-pass detection and response.AI applications in next-gen firewalls offer a multitude of use cases, primarily aimed at enhancing the firewall's ability to perform contextual inspection of traffic and content. This capability significantly improves security detection, enabling more effective identification, containment, and neutralization of malware while also minimizing false positives and facilitating real-time responses to security events. In light of the rising frequency of attacks and data breaches, prioritizing security has never been more critical; indeed, the foremost objective of AI-driven next-gen firewalls is to bolster overall enterprise cybersecurity. By leveraging real-time traffic and content scanning at high speeds, these firewalls enhance security risk aversion, swiftly identifying and mitigating potential threats. Many organizations currently conduct threat detection in isolated environments and address remediation through separate systems, which can introduce delays and inefficiencies. Integrating AI techniques within firewalls allows for immediate detection and response to security incidents, promoting a streamlined, real-time approach to cybersecurity that significantly improves the efficacy of threat management.

Case Studies and Practical Applications

In this section, we describe Deep Instinct's Asymmetric Risk Score (ARS), which was designed to classify an incoming unknown executable file, and how the ARS reduces false positives and minimizes the risks associated with good files set to quarantine. We describe our overall design process and Walk the Tree (WTT), a new model we developed to analyze model outputs. And, we present a series of tests and case studies to illustrate key elements of ARS and how it can help a business reduce the number of false positives and assess the risks associated with quarantining some files.

AI offers major gains for next-gen firewalls by enabling better risk mitigation and categorization of threats. In the past, next-gen firewalls (NGFW) merely blocked network traffic they marked as malicious. However, identifying unknown executables has helped with the creation of the asymmetric risk and Track Guard, a major part of how we communicate the potential risk of a file to help reduce the number of false positives and the risks associated with quarantining good files. As we developed our platform, we recognized the benefits that AI — specifically deep learning — could bring to the table to identify unknown executables in more ways than static analysis did. The advantages that deep learning could bring to the development of a neural network were the primary reasons why NGFW embraced AI.

Industry Examples

One of the most notable uses of generative AI in the field of cybersecurity is in the development of next-gen firewalls. For example, in 2019, Sophos moved on from using supervised machine learning and embraced generative technology as the key mechanism in their software, which identifies previously unseen viruses. The company describes the implementation of deep neural networks which use untampered files to create new examples that the network is not yet capable of generating. These examples are then put through the company's existing supervised machine-learning systems to identify new viruses. The company has gone further by hiring what it calls "neural network zookeepers", who act as specialized ML researchers.

Deep Instinct uses a deep learning approach that leverages a proprietary GPU-based algorithm for their next-gen endpoint protection. The company's sophisticated deep learning models and classification algorithms evaluate the whitelist while simultaneously reducing false positives and negatives, resulting in accuracy during the detection phase. Their training architecture is based on an ensemble of various deep neural network models, such as feedforward DNN, Convolutional Neural Network (CNN), and Recurrent Neural Network (RNN) layers that leverage a diversity of neurons. The trained architecture is then used in the online testing phase during inference.

Byte Defender's approach to next-gen endpoint protection is based on an artificial intelligence optimizer. They use an Artificial Gene Regulator (AGR) algorithm as the basis of their AI approach.

Equation 3: Anomaly Detection

$$p(x;\mu,\Sigma) = \frac{1}{(2\pi)^{\frac{n}{2}}|\Sigma|^{\frac{1}{2}}} \exp\left(-\frac{1}{2}(x-\mu)^T\Sigma^{-1}(x-\mu)\right)$$

Whereas:

$$\mu = \frac{1}{m}\sum_{i=1}^{m} x^{(i)}$$

$$\Sigma = \frac{1}{m}\sum_{i=1}^{m}(x^{(i)}-\mu)(x^{(i)}-\mu)^T$$

Academic Research

The area of AI-based security research is vast, and this paper aims to provide a snapshot of the current weaknesses in AI models that affect the selection and performance of AI-based Next-Gen firewalls, which guard today's IT environments. These general weaknesses lie in supporting sufficiently diverse low-level data for AI model training and validation. All relevant cybersecurity data comes from the fields of security and network professionals, national security and intelligence, and the recent operational use of security software and hardware. These areas already have existing data collection processes that can be practically automated at multidisciplinary academic research centers.

Cybersecurity requires experts with multidisciplinary education to design, select, configure, troubleshoot, and adapt AI model reverse-engineered features to IT systems. Once these findings are in place, we need even greater use of multidisciplinary research to understand and model the interaction of these AI system features on AI model performance. Potential topic areas include the number of required training data, the use of additional symptom and root cause data to meet pre-established implementation goals, the transfer into new environments, the population of features with adversary data, business strategy, and system security investment, defensive strategy and adversary intelligence source reputability, adversarial attack identification, and adversarial attack effectiveness. If performance could be improved by using adversarial contamination to address common vulnerabilities in 10 years, then let us start sharing, exploring, and systematically answering these and other AI Next-Gen firewall high-performance AI model questions today.

Future Trends and Directions

This chapter discusses ongoing developments and future research on AI-ML-based next-generation firewalls (AI-NGFWs). The dream of the AI-NGFW is an intelligent, self-righting system capable of real-time adaptation to a rapidly changing adversary. AI-ML tools hold the promise of pioneering firewalls at the dawn of the AI era. ML models can be trained to detect novel cybersecurity threats. Our survey suggests that feature learning architectures, such as deep learning models for C2 detection, performed well in practice. We also pointed out a few emergent trends: the rise of GANs, LSTMs, and autoencoders in the next-gen cybersecurity domain.

However, the AI breakthroughs in the NGFW space also incite fresh thinking in cybersecurity practices using the very power of generative AI models. Imagine malware-fighting malware. Where do we draw the line? While the arms race continues, the benefits of using AI-NGFW models to better understand, learn from, and deal with adversaries are truly transforming. These AI techniques also come at a high price of performance and energy consumption and make AI-NGFWs very susceptible to adversarial attacks. These AI models are also just as susceptible to adversarial examples. That is why, in anticipation of adware exploiting adware, we proposed 10 well-posed research problems. Furthermore, we also propose the implementation of an AI-NGFW research framework using a combination of data storage and ML training models. To compensate for the limitations, we discuss the use of multimodal learning architectures, such as CLIP, to circumvent Rule A.

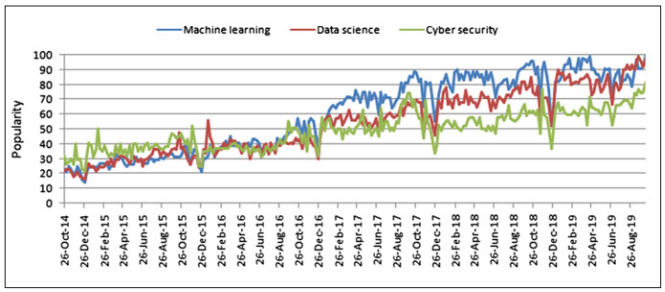

Figure 6: Machine Learning and Cybersecurity

Ethical Considerations

In terms of ethical considerations, this work is generally aligned with a vast amount of research literature focused on enhancing cybersecurity through the application of AI and ML technologies. However, a detailed exploration of ethical considerations is not directly addressed in the paper, as the emphasis has mainly been on our technical model advancements. While some of the other work more directly describes discussion on their ethical understanding or outlines some concern (e.g., questionable labeling patterns in training data), this particular Another Look effort can directly help protect existing and future research in this sector. It provides an approach that aligns with several recommendations of ethical guidelines for AI development and application.

For example, as outlined at the start of the Introduction, Next-Gen Firewall solutions are a fundamental technology that helps to protect against a vast array of types of threats to networks. Such technology is already employed by many large companies and institutions and is an area of significant AI/ML research interest. However, if Next-Gen Firewalls can be rendered less effective, this could directly result in a substantial range of negative consequences. Such potential negative consequences directly work against the "do no harm" (Principle I) and "promote the betterment of humanity" (Requirement 1.4) suggestions given in the Organization for Economic Co-operation and Development (OECD) AI Principles policy report.

Emerging Technologies

Emerging technologies. Next-gen firewalls are also being infused with a variety of emerging technologies and techniques to enhance their ability to find and respond to advanced cyber espionage tactics more effectively. SOC experts can also now directly deploy network detection and response and other network security monitoring solutions on their next-gen firewalls for further protection. These enhanced firewalls should be key components of a zero-trust architecture that focuses on thwarting and responding to breach attempts in real time.

Generative AI and machine learning. Next-gen firewalls are undergoing upgrades today to combine advanced research with AI and machine learning algorithms. These newer technologies enable expertly designed AI agents to generate humanly understandable good and bad example data for teaching the next-gen firewalls. When trained by security and privacy experts to recognize risk signs, the firewalls can more quickly and reliably verify whether a real or suspected incident with advanced cyber-espionage associates or uses any ideal form of data. Firewalls armed with this targeted type of generative AI and machine learning will improve the security posture of the organization.

Conclusion and Recommendations

Conclusion

This article has introduced the ongoing Fourth Industrial Revolution that will bring unparalleled levels of change to the traditional business landscape of many organizational functions, not the least of which is that of private sector and public sector information security professionals. Progressive cybersecurity organizations are currently exploring the potential of next-generation firewalls to enhance the traditional, and yet still poorly defended, boundary protection mechanism.

There are currently more 'good guys' who are looking to protect their sensitive data than there are the 'bad guys' whose aim is to exploit those defenses for financial gain or malfeasance. As a generalization, those who currently defend in both private and public sectors deploy many who work long hours using yesterday's technology to ensure who and what is behind the logical and physical boundaries are not the wrong people with nefarious intent. Deploying intelligent perimeter defense – in terms of the next-generation firewall – is making considerable inroads into making those dedicated individuals whose task is to defend a business or regulatory infrastructure more effective, efficient, and timely [1-33].

Recommendations

This article outlines the reasons why the traditional boundary protection, enterprise defense method was no longer regarded as being as effective when next-generation firewall technology was compared. With all of the multiple security features that many of these hardware and software packages are currently being adopted, the need for careful policy creation and control management of what and how the NGFW function is implemented is a critical issue. When senior managers are assessing the resilience of an organization to both technical and non-technical attacks, the latest innovations in both software and artificial intelligence, and machine learning capabilities that can be programmed into the next-gen firewall need to be assessed and – where possible - integrated into the existing IT protection strategy.

Key Findings

The practice of using high-speed deterministic AI and machine learning algorithms, collectively known as generative AI, to complement the fundamental objective of a next-gen firewall, has created an apparatus that can be described as a "smart," "sophisticated," and "fast-learning" next-gen firewall.

Chapter 5 briefly describes new interpretations and understandings of the traditional roles and functions of a next-gen firewall. Through the practice of high-speed generative AI, the virtual embodiment of these new understandings has now become real and available to better serve its operational role as the defensive central management and processing point for future "defense-in-depth" cybersecurity architectures. A desirable characteristic of deploying a next-gen firewall is its multiplicative effect. The deployment of a multi-layer next-gen firewall addresses deficiencies, redundancy, and inefficiencies that are known to be present in the existing cybersecurity technologies and applications that it replaces.

Implications for Cybersecurity Practices

Drawing upon this analysis, the lessons for cybersecurity practices are the following. We have found that generative AI and machine learning make potential contributions to the cyber defense functions of situational awareness (systematically collecting valid data to detect and assess security breaches, identify the breach characteristics, and prioritize the response) and hostile action resistance (combining intrusion, IM, and resilience functions to address security breaches). While we are focused on generative AI and machine learning in next-generation firewalls used for network security, we suspect that IT operations teams may find them useful for broader network and system management purposes. We suggest managers plan for and monitor the increasing use of machine learning in the existing ANNs and the emerging use of generative AI to stimulate stronger specifications and metrics and deployment permutations based on expected probabilities.

We suggest that analysts monitor progress in applying AI for functions in all CND categories to define whether or not the unknowns, difficulties, and lagging implications of cybersecurity for AI will generally be resolved in any reasonable amount of time. Managers, reviewers, and audit teams might question the attack defense designers to determine whether this capability brings more robustness along with the promise of fewer false positives on the important issue of evidence for security incident reports. We support consideration of legal, ethical, and information disclosure impact factors, even as we notice the current range of generative AI and machine learning research in the tangent of being entertaining, producing novel content, or augmenting human creativity in disciplines like visual arts, graphics, semantic analysis, natural language processing, speech synthesis and recognition, cancer clinic transcription, and biotechnology.

References

1. Laxminarayana Korada, Vijay Kartik Sikha (2022) Enterprises Are Challenged by Industry-Specific Cloud Adaptation - Microsoft Industry Cloud Custom-Fits, Outpaces Competition and Eases Integration. Journal of Scientific and Engineering Research 9: 182-187.
2. Mandala V, Premkumar CD, Nivitha K, Kumar RS (2022) Machine Learning Techniques and Big Data Tools in Design and Manufacturing. Big Data Analytics in Smart Manufacturing Chapman and Hall/CRC https://www.taylorfrancis.com/chapters/edit/10.1201/9781003202776-9/machine-learning-techniques-big-data-tools-design-manufacturing-vishwanadham-mandala-premkumar-nivitha-satheesh-kumar.
3. Shah C, Sabbella VRR, Buvvaji HV (2022) From Deterministic to Data-Driven: AI and Machine Learning for Next-Generation Production Line Optimization. Journal of Artificial Intelligence and Big Data 2: 21-31.
4. Pamulaparthyvenkata S, Avacharmal R (2023) Leveraging Interpretable Machine Learning for Granular Risk Stratification in Hospital Readmission: Unveiling Actionable Insights from Electronic Health Records. Hong Kong Journal of AI and Medicine 3: 58-84.
5. Bansal A (2022) Establishing a Framework for a Successful Center of Excellence in Advanced Analytics. ESP Journal of Engineering and Technology Advancements 2: 76-84.
6. Avacharmal R, Pamulaparthyvenkata S, Gudala L (2023) Unveiling the Pandora's Box: A Multifaceted Exploration of Ethical Considerations in Generative AI for Financial Services and Healthcare. Hong Kong Journal of AI and Medicine 3: 84-99.
7. Yadav PS (2023) Enhancing Software Testing with AI: Integrating JUnit and Machine Learning Techniques. North American Journal of Engineering Research 4: 1-6.
8. Perumal AP, Deshmukh H, Chintale P, Molleti R, Najana M, et al. (2023) Leveraging machine learning in the analytics of cyber security threat intelligence in Microsoft azure. International Journal of Communication and Information Technology 4: 28-32.
9. Kommisetty PDNK, Valiki Dileep (2022) Leading the Future: Big Data Solutions, Cloud Migration, and AI-Driven Decision-Making in Modern Enterprises. Educational Administration: Theory and Practice 28: 352-364.
10. Aravind R (2023) Implementing Ethernet Diagnostics Over IP For Enhanced Vehicle Telemetry-AI-Enabled. Educational Administration: Theory and Practice 29: 796-809.
11. Sikha VK, Siramgari D, Korada L (2023) Mastering Prompt Engineering: Optimizing Interaction with Generative AI Agents. Journal of Engineering and Applied Sciences Technology 5: 2-8.
12. Aravind R, Shah CV (2023) Physics Model-Based Design for Predictive Maintenance in Autonomous Vehicles Using AI. International Journal of Scientific Research and Management 11: 932-946.
13. Mandala V (2022) Revolutionizing Asynchronous Shipments: Integrating AI Predictive Analytics in Automotive Supply Chains. International Journal of Artificial Intelligence & Machine Learning 1: 47-59.
14. Chirag Vinalbhai Shah (2022) Vehicle Control Systems: Integrating Edge AI and ML for Enhanced Safety and Performance. International Journal of Scientific Research and Management 10: 871-886.
15. Pamulaparthyvenkata S (2023) Optimizing Resource Allocation for Value-Based Care (VBC) Implementation: A Multifaceted Approach to Mitigate Staffing and Technological Impediments Towards Delivering High-Quality, Cost-Effective Healthcare. Australian Journal of Machine Learning Research & Applications 3: 304-330.
16. Bansal A (2022) Advanced Approaches to Estimating and Utilizing Customer Lifetime Value in Business Strategy. International Journal of Science and Research 11: 2045-2048.
17. Avacharmal R, Sadhu AKR, Bojja SGR (2023) Forging Interdisciplinary Pathways: A Comprehensive Exploration of Cross-Disciplinary Approaches to Bolstering Artificial Intelligence Robustness and Reliability. Journal of AI-Assisted Scientific Discovery 3: 364-370.
18. Perumal AP, Deshmukh H, Chintale P, Desaboyina G, Najana M (2022) Implementing zero trust architecture in financial

services cloud environments in Microsoft azure security framework. International Journal of Circuit, Computing and Networking 3: 75-80.

19. Korada L (2023) AIOps and MLOps: Redefining Software Engineering Lifecycles and Professional Skills for the Modern Era. Journal of Engineering and Applied Sciences Technology 5: 1-7.
20. Pamulaparthy venkata S, Reddy SG, Singh S (2023) Leveraging Technological Advancements to Optimize Healthcare Delivery: A Comprehensive Analysis of Value-Based Care, Patient-Centered Engagement, and Personalized Medicine Strategies. Journal of AI-Assisted Scientific Discovery 3: 371-378.
21. Bansal A (2023) Power BI Semantic Models to enhance Data Analytics and Decision-Making. International Journal of Management 14: 136-142.
22. Avacharmal R, Gudala L, Venkataramanan S (2023) Navigating the Labyrinth: A Comprehensive Review of Emerging Artificial Intelligence Technologies, Ethical Considerations, And Global Governance Models in The Pursuit of Trustworthy AI. Australian Journal of Machine Learning Research and Applications 3: 331-347.
23. Perumal AP, Chintale P (2022) Improving operational efficiency and productivity through the fusion of DevOps and SRE practices in multi-cloud operations. International Journal of Cloud Computing and Database Management 3: 49-53.
24. Ravi Aravind, Srinivas Naveen D Surabhi, Chirag Vinalbhai Shah (2023) Remote Vehicle Access: Leveraging Cloud Infrastructure for Secure and Efficient OTA Updates with Advanced AI. European Economic Letters 13: 1308-1319.
25. Korada L (2023) Leverage Azure Purview and Accelerate Co-Pilot Adoption. International Journal of Science and Research 12: 1852-1954.
26. Pamulaparthyvenkata S (2022) Unlocking the Adherence Imperative: A Unified Data Engineering Framework Leveraging Patient-Centric Ontologies for Personalized Healthcare Delivery and Enhanced Provider-Patient Loyalty. Distributed Learning and Broad Applications in Scientific Research 8: 46-73.
27. Bansal A (2024) Enhancing Customer Acquisition Strategies Through Look-Alike Modelling with Machine Learning Using the Customer Segmentation Dataset. International Journal of Computer Science and Engineering Research and Development 14: 30-43.
28. Avacharmal R (2022) Advances in Unsupervised Learning Techniques for Anomaly Detectiona and Fraud Identification in Financial Transactions. Neuro Quantology 20: 5570-5581.
29. Chintale P (2020) Designing a secure self-onboarding system for internet customers using Google cloud SaaS framework. International Journal of Applied Research 6: 482-487.
30. Aravind R, Surabhi SNRD (2023) Harnessing Artificial Intelligence for Enhanced Vehicle Control and Diagnostics. Journal of Basic Science and Engineering 20: 79-95.
31. Korada L, Somepalli S (2023) Security is the Best Enabler and Blocker of AI Adoption. International Journal of Science and Research 12: 1759-1765.
32. Pamulaparthyvenkata S, Avacharmal R (2021) Leveraging Machine Learning for Proactive Financial Risk Mitigation and Revenue Stream Optimization in the Transition Towards Value-Based Care Delivery Models. African Journal of Artificial Intelligence and Sustainable Development 1: 86-126.
33. Bansal A (2024) Enhancing Business User Experience: By Leveraging SQL Automation through Snowflake Tasks for BI Tools and Dashboards. ESP Journal of Engineering and Technology Advancements 4: 1-6.