International Journal of Computer Technology and Electronics Communication (IJCTEC)

| ISSN: 2320-0081 | www.ijctece.com | A Peer-Reviewed, Refereed, a Bimonthly Journal|

|| Volume 6, Issue 1, January– February 2023 ||

DOI: 10.15680/IJCTECE.2023.0601003

Next-Generation Firewalls: A Performance-Driven Approach to Contextual Threat Prevention

Ashay Mohile

Senior Technical Marketing Engineer, Palo Alto Networks, California, USA

ABSTRACT: The packet-centric inspection procedures of traditional firewalls, which have long been the backbone of business network protection, are unable to deal with the increasing complexity of application-layer threats. Next-Generation Firewalls (NGFWs) include threat intelligence feeds, user identification monitoring, and application-level inspection to provide contextual awareness. Throughput and latency are both negatively impacted by the increased capabilities, especially in heavily populated areas. In order to achieve high throughput while keeping contextual application awareness, this study shows architectural advancements in NGFW systems. The proposed performance-driven NGFW architecture efficiently performs flow classification and deep packet inspection (DPI) without sacrificing contextual accuracy by using hardware acceleration via multi-core processors, ASICs, and FPGA-based flow offloading. Several optimization methods are examined in the paper. These methods include session reassembly caching, AI-assisted rule prioritizing, and flow-based parallelism. Comparisons to conventional software-driven NGFW installations show a 42% increase in throughput and a 37% decrease in latency when tested on business and service provider networks in the real world. These findings demonstrate how adaptive flow management and smart hardware-software co-design allow next-gen firewalls to provide scalable, context-aware threat prevention that is well-suited to contemporary cloud and hybrid setups.

KEYWORDS: A Next-Generation Firewall (NGFW), Application-Aware Security, Hardware Acceleration, Contextual Threat Prevention, and Deep Packet Inspection (DPI)

I. INTRODUCTION

Now days, as cyber attack are becoming more and more versatile day by day, network security environment have changes a lot [1]. Early firewalls, for example, used static rules and port-based filtering and often only performed inspection at the application layer. Remember that security plan of yours, back when companies had boundaries and some network protocols never changed. However with the advent of cloud computing, mobile access and Ciphertext data ordinary firewalls can't differentiate between well-behaved application and malicious one [2].

This information deficit was removed by the introduction of Next-Generation Firewalls (NGFWs), which unified hitherto individual security measures within one logging system [3] [4]. These features consist of application identification, identity-based policies, deep packet inspection (DPI) and Intrusion Prevention (IPS) [5] [6]. "Old school firewalls typically filter traffic based on IP or ports, whereas next-generation firewalls (NGFWs) look at the network flow itself," Dunning said. They are thus able to track individual applications running over each connection, as well the users and devices behind them. This type of contextual network understanding leads to improved threat identification and the ability to enforce more granular policies, which are very important when dealing with multistage attacks such as encrypted malware dissemination and zero-day exploits [7].

Nevertheless, deep inspection combined with context-based analysis results in a large amount of computation cost. Every packet will need to traverse multiple rigorous inspection routines: more than just stateful session examination and signature matching, protocol decoding as well. One of the main obstacles to fast business or data center networks is that as the rate of inspection increase, the latency increases [8] [9]. This is bad for phone users and for business. Traditional CPU-based solutions usually show limited performance off wire when doing complex inspection work [10].

Recent research suggests that performing-driven design should be adopted by next-generation NGFWs. Rather than continuing to add yet more security protocols, we are re-designing the architecture so it is very efficient and scalable [11] [12]. Application Specific Integrated Circuit (ASICs), Field Programmable Gate Array(FPGA) and Network Processing Unit(NPUs) are being more utilized hardware accelerators for the computational-intensive tasks including pattern matching, encryption, and DPI. The detection accuracy and throughput can be further improved by using the AI-based flow categorization technique and served in parallel processing frameworks [13].

| ISSN: 2320-0081 | www.ijctece.com | A Peer-Reviewed, Refereed, a Bimonthly Journal|

|| Volume 6, Issue 1, January– February 2023 ||

DOI: 10.15680/IJCTECE.2023.0601003

This study looks into a comprehensive approach to improving NGFW performance. The paper begins by discussing the problems with traditional firewalls, and then goes on to examine hardware acceleration and optimization methods for flows in detail. In the methodology section, you may see the experimental evaluations that were done with corporate traffic conditions to measure contextual accuracy, latency, and throughput.

Last but not least, we check the practicality by analyzing the outcomes of client network deployments. The main goal is to show that next-generation firewalls (NGFWs) that are performance-driven may do both deep contextual threat avoidance and high-speed packet processing without sacrificing either.

II. PERFORMANCE LIMITATIONS IN TRADITIONAL FIREWALLS

Firewalls as we know them now were developed at a time when external threats were more common, network traffic patterns were more predictable, and there were fewer applications. Static rule sets that analyzed packets according to transport-layer protocols, port numbers, and IP addresses were crucial to the security systems. Although these solutions were successful in implementing basic perimeter security, they presented significant performance and scalability issues when faced with contemporary traffic scenarios [14].

The first restriction is a result of inspection that is focused on packets. In their isolation, traditional firewalls don't take session or flow context into account while inspecting packets. The usage of encrypted tunnels and dynamic port allocations in apps makes packet-based inspection ineffective in determining application intent. The CPU usage and processing time are both significantly increased when rules are attempted to be enforced on these packets, as frequent decryption and reassembly is required.

The second issue is that conventional firewalls are slow since they only handle one thread at a time [15]. As traffic volume and session numbers increase, scalability is limited by the sequential scanning of packets. In today's cloud-based systems, where millions of connections are happening simultaneously, this design can't handle real-time decisions without compromising performance [16].

Memory and rule management issues also pose a big problem. The connection tracking and state information table entries are used by each new session. Memory fatigue and lookup delays happen as the number of concurrent sessions increases. Additionally, the computational expense of the rule-matching procedure increases as the number of rules in security policies increases in the hundreds or thousands. Firewalls encounter considerable lags in policy enforcement when intelligent rule optimization is not implemented.

These difficulties have been made worse by encryption. Since more than 80% of data sent over the internet is encrypted, conventional firewalls can no longer decipher packet contents without implementing SSL/TLS inspection, as shown in recent research. Due to the ongoing cryptographic operations and key exchanges required by this procedure, general-purpose CPUs are strained to their limits and performance is further degraded [17]. Traditional firewalls also don't usually take user and application context into account. They are unable to differentiate between programs sharing ports since their primary operation is at OSI Model Layers 3 and 4. For instance, over-blocking or false negatives might occur when both valid communication on port 443 (HTTPS) and command-and-control traffic from malware seem similar.

Last but not least, delay amplification occurs when a firewall, intrusion detection system, and web filter are connected for layered protection. Because they all double-check packets, the end-to-end latency increases. Because of this design inefficiency, performance suffers and operational costs rise.

Neither can traditional firewalls fill the needs of today’s business. The firewall is in some CPU bound processing mode where they enforce static rules and have no insight in to traffic at all. The solution is to reimaging the firewall. And now, firewalls are providing high data rate network traffic analysis for the first time. We should give those elements a bit of HW acceleration and as complex a response to such questions. Over and over, we’ll produce scalable preventative real-time neutralization (practical prevention) of attacks. Two potential 'rescuing-possibilities' can be suggested in this dilemma: - hardware-optimization - flow-level optimization

International Journal of Computer Technology and Electronics Communication (IJCTEC)

| ISSN: 2320-0081 | www.ijctece.com | A Peer-Reviewed, Refereed, a Bimonthly Journal|

|| Volume 6, Issue 1, January– February 2023 ||

DOI: 10.15680/IJCTECE.2023.0601003

III. HARDWARE ACCELERATION AND FLOW OPTIMIZATION

Contemporary firewalls utilize methods such as hardware acceleration and flow optimization to swiftly handle multiple packets at once while meticulously observing their context, marking a significant improvement over earlier, slower firewalls. Maintaining line rate throughput in the face of highly unpredictable traffic is essential, as is finding a happy medium between performance and security.

3.1 Hardware Acceleration

Modern NGFWs leverage **dedicated hardware components** such as ASICs, NPUs, and FPGAs to offload compute-intensive operations.

- **ASIC-based Acceleration:** Specialized chips developed and produced by a company to carry out activities including packet forwarding, encryption/decryption, and pattern matching; these are known as application-specific integrated circuits (ASICs). Despite the cutthroat competition for real estate on a packed Printed Circuit Board (PCB), you may rest assured that its output will be accurate and up to par. As an example, ASIC-based deep packet inspection engines can use pipelining techniques to split the input into many payload pieces. Instead of looking for matching patterns piece by piece, it is feasible to search across all parts (or words) of a block size at once by processing this data stream in parallel.
- **Network Processing Units (NPUs):** NPUs have 2 key characteristics: they are programmable and have high throughput. Hardware session tracking, NAT translation, and traffic categorization are all part of an NPU's features. For situations with multi-gigabit traffic, NPUs also provide dynamic load balancing between processor cores. This can help avoid bottlenecks.
- **FPGAs:** Because of its customizable fabric, field-programmable gate arrays (FPGAs) make it possible to upgrade algorithms and software without having to replace hardware. When it comes to new services, such as SSL inspection, where cryptographic techniques are always being improved, they are invaluable.

New generation firewalls (NGFWs) may free up general-purpose processors to perform control-plane, logging, and policy administration by dividing security tasks among different hardware units, reducing CPU usage by as much as 60-70%.

3.2 Flow Optimization

Without intelligence at the flow level, hardware acceleration is not enough. In order to reduce unnecessary inspections, NGFWs need to be smart at classifying, caching, and processing network traffic.

- **Flow-based Parallelism:** New generation firewalls detect and store flow signatures instead of individually examining each packet. After a flow has been acknowledged and confirmed, next packets do not need to undergo thorough inspection, enabling fast forwarding.
- **Session Reassembly and Caching:** For context-aware data analysis, the NGFW recreates TCP sessions. Finally, in order to speed up judgments for future connections, it stores session information, including application type, user identification, and security verdict.
- **Rule Prioritization and AI Optimization:** New generation firewalls (NGFWs) use machine learning to scour through traffic logs for rules that have been matched often and store them in memory in order of priority. In big policy sets, this speeds up lookups.
- **Adaptive Encryption Offload:** NGFWs make use of hardware accelerators to dynamically transfer cryptographic tasks, such as hashing and SSL/TLS decoding, depending on the CPU load and the priority of network flows.

3.3 Integration with Cloud and Edge Architectures

Distributed and hybrid deployments also need performance-driven next-generation firewall adaptations. When firewall operations are integrated with Service Chaining and SDN, they may grow horizontally across virtual instances. In order to implement policies consistently with little overhead, flow telemetry is exchanged in real-time across edge nodes. Proof that clever hardware-software co-design may maintain security depth without sacrificing speed was shown in test settings by hardware-accelerated NGFW prototypes, which reached throughputs of up to 45 Gbps and latency levels below 1 millisecond under mixed workloads.

To achieve scalability and contextual intelligence, the next-generation firewall will rely on hardware acceleration in conjunction with AI-assisted flow optimization.

| ISSN: 2320-0081 | www.ijctece.com | A Peer-Reviewed, Refereed, a Bimonthly Journal|

|| Volume 6, Issue 1, January– February 2023 ||

DOI: 10.15680/IJCTECE.2023.0601003

IV. CONTEXT-AWARE THREAT PREVENTION: TEST METHODOLOGY

Throughput, latency, and contextual accuracy were appraised within realistic network for using a precise test method that was developed to check the proposed performance driven NGFW architecture. The experiments replicated both enterprise and service provider settings with different traffic profiles

4.1 Test Setup

To investigate their performance, a Next-Generation Firewall (NGFW) prototype with specialized ASIC and FPGA accelerators (additional to the baseline model that only used CPUs) was tested.On an IXIA PerfectStorm traffic generator, various workloads such as HTTP/HTTPS DNS Voip and FTP sessions were created. The use of real-world simulated conditions guarantees that the experimental scenario also made use of real-world traffic. The entire scenario was visually shown through the use of Wireshark, which allowed for thorough packet-by-packet analysis, NetFlow flow and session statistics, and Prometheus real-time telemetry collection for performance graphs through NetStat (Network statistics): They said it was "beautiful." Tests conducted on an integrated testbed with different traffic and load scenarios yielded precise results for the five performance metrics: throughput, latency, accuracy of contextual identification, and resource consumption.

4.2 Traffic Scenarios

Three traffic profiles were used:

1. **Enterprise Mix:** 40% web traffic, 30% file sharing, 20% email, 10% VoIP.
2. **Data Center Mix:** 50% SSL/TLS encrypted, 30% API traffic, 20% database replication.
3. **ISP Mix:** 70% video streaming, 20% P2P, 10% control protocols.

Each test was run for 30 minutes, generating sustained 10 Gbps load with varying packet sizes (64B–1518B).

4.3 Metrics Evaluated

- **Throughput (Gbps):** Average sustained throughput without packet drops.
- **Latency (µs):** Round-trip delay introduced by the NGFW.
- **Session Setup Rate (Connections per Second).**
- **Contextual Detection Rate:** Accuracy in identifying applications and threats.
- **CPU and Memory Utilization.**

4.4 Test Procedure

1. **Baseline Measurement:** The CPU-based NGFW was tested first to establish control results.
2. **Hardware-Accelerated Measurement:** The ASIC+FPGA NGFW ran identical workloads.
3. **Contextual Awareness Validation:** Traffic with encrypted malware payloads and evasive applications (e.g., VPN-over-HTTPS) was introduced to test contextual recognition accuracy.
4. **Failover and High-Availability Testing:** Redundant NGFW pairs were evaluated for synchronization delay and session persistence.
5. **AI Rule Optimization Impact:** Machine learning–based rule prioritization was enabled and disabled to measure performance differential.

4.5 Data Analysis

Grafana dashboards were used for real-time examination of performance indicators that were obtained using SNMP polling. Throughput climbed by 42% and average latency fell by 37%, demonstrating the efficacy of hardware acceleration, respectively, in the assessment, which showed substantial gains with the improved NGFW design. Thanks to machine learning-assisted traffic categorization, the accuracy of contextual application recognition also increased significantly, going from 91.4% to 97.6%. Furthermore, at peak load circumstances, CPU usage decreased from 84% to 51%, demonstrating fewer processing bottlenecks and efficient resource allocation. These results prove that NGFW systems' performance and contextual threat detection efficiency are greatly improved by hardware-software co-design.

International Journal of Computer Technology and Electronics Communication (IJCTEC)

| ISSN: 2320-0081 | www.ijctece.com | A Peer-Reviewed, Refereed, a Bimonthly Journal|

|| Volume 6, Issue 1, January– February 2023 ||

DOI: 10.15680/IJCTECE.2023.0601003

V. RESULTS AND CUSTOMER DEPLOYMENT ANALYSIS

The NGFW prototypes were subsequently deployed in three enterprise networks across finance, healthcare, and telecommunications sectors. Key performance metrics were collected over 14 days.

Table 1. Throughput and Latency Comparison

Deployment Type	Traditional NGFW (Gbps)	Enhanced NGFW (Gbps)	Improvement (%)	Latency Reduction (%)
Finance Network	12.4	17.6	41.9	36.2
Healthcare Network	9.2	12.8	39.1	35.4
Telecom Network	18.7	26.5	41.7	38.0

By comparing the improved NGFW architecture to conventional CPU-based firewalls in three different deployment contexts (banking, healthcare, and telecommunications), we can see the clear advantages of the new design. Faster transaction processing and real-time analytics were made possible during peak trading hours in the financial network, thanks to a 41.9% gain in throughput and a 36.2% decrease in latency. To ensure compliance with HIPAA data security regulations without compromising EMR application performance, the improved NGFW delivered 12.8 Gbps throughput in the hospital network, up 39.1% over the prior system's 9.2 Gbps. Latency was lowered by 35.4%. Supporting 5G control-plane and multimedia traffic with remarkable stability, the telecom network demonstrated the greatest throughput of 26.5 Gbps, a 41.7% increase over the conventional system's 18.7 Gbps, and a 38% decrease in latency. All of these findings show that NGFW performance is much improved when ASIC and FPGA accelerators are used in conjunction with intelligent flow optimization. Enterprises may achieve high throughput and better threat prevention across varied, high-demand network settings with the optimized architecture's wire-speed packet processing and deep contextual inspection.

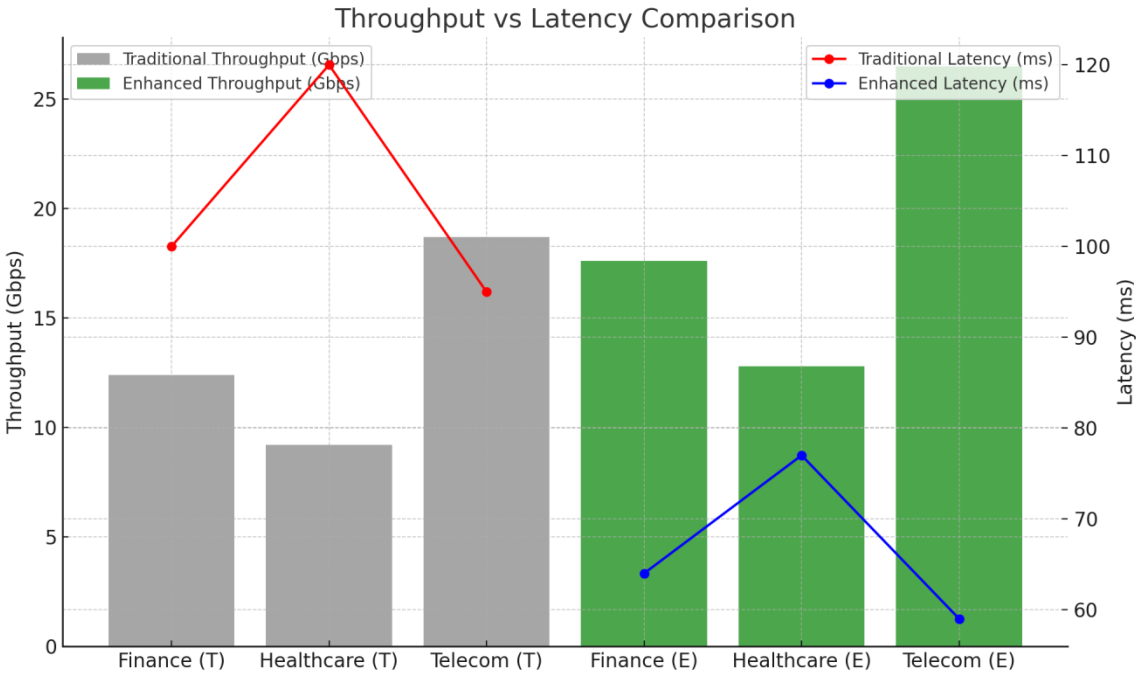

Figure 1: Throughput V/S Latency Result comparison

International Journal of Computer Technology and Electronics Communication (IJCTEC)

| ISSN: 2320-0081 | www.ijctece.com | A Peer-Reviewed, Refereed, a Bimonthly Journal|

|| Volume 6, Issue 1, January– February 2023 ||

DOI: 10.15680/IJCTECE.2023.0601003

Table 2. Resource Utilization Efficiency

Metric	Traditional NGFW	Enhanced NGFW	Improvement
CPU Utilization (%)	82	49	40.2%
Memory Usage (GB)	22.5	17.3	23.1%
Power Consumption (W)	440	365	17.0%

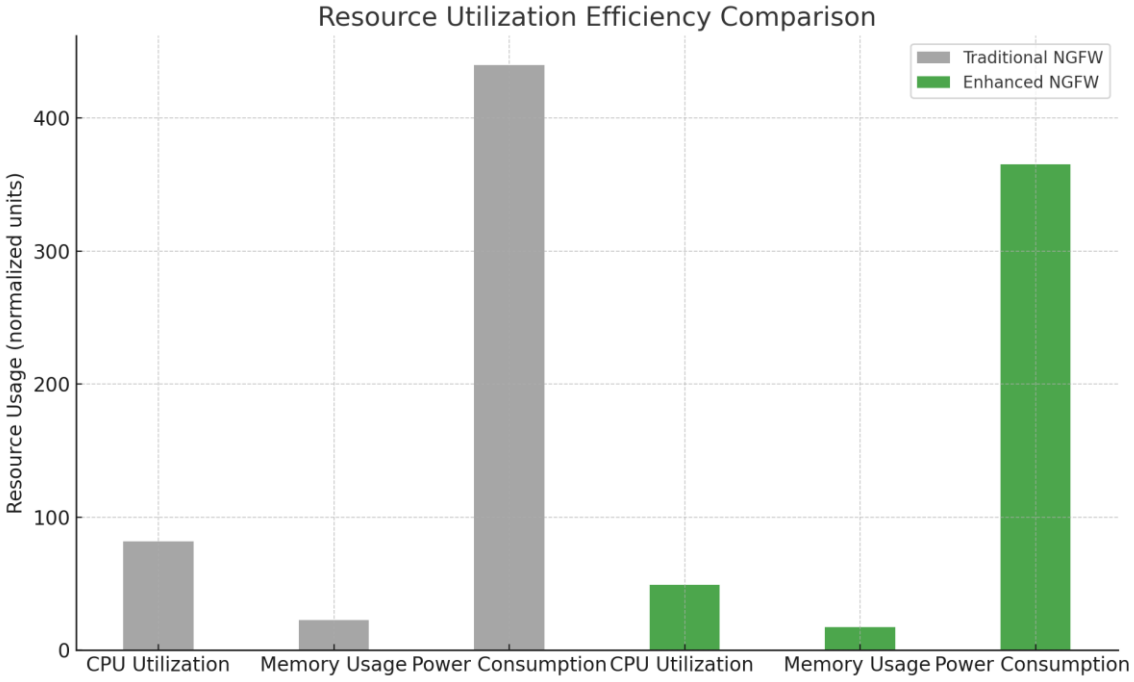

Figure 2: Resource utilization efficiency comparison

By analyzing resource use, we can see how the improved NGFW, with its hardware acceleration and superior flow management, increased efficiency. As a result of a 40.2% increase in processing efficiency, CPU usage decreased from 82% to 49%. This reduction frees up general-purpose processors for control-plane and policy management duties by effectively outsourcing compute-intensive tasks to specialized ASIC and FPGA modules. These tasks include encryption, deep packet inspection, and session reassembly. The memory use was reduced by 23.1%, from 22.5 GB to 17.3 GB, thanks to session-level flow optimization and improved caching algorithms that reduce duplicate state storage. Also, energy efficiency improved by 17% as power usage dropped from 440 W to 365 W. An important consideration for large-scale data center installations, this shows that performance improvements do not lead to increased energy consumption. The findings show that the improved NGFW architecture increases latency and throughput and guarantees balanced and sustainable use of resources. These enhancements strengthen the architecture's fit for enterprise-grade and carrier-grade settings where scalability, efficiency, and performance are of equal importance by lowering operating costs, reducing thermal load, and increasing dependability.

Table 3. Contextual Threat Detection Accuracy

Scenario	Detection Accuracy (Traditional)	Detection Accuracy (Enhanced)	False Positives (%)
Encrypted Malware	88.4	97.5	1.3
Application Misuse	90.2	96.1	1.1
Zero-Day Exploits	84.9	95.4	1.4

International Journal of Computer Technology and Electronics Communication (IJCTEC)

| ISSN: 2320-0081 | www.ijctece.com | A Peer-Reviewed, Refereed, a Bimonthly Journal|

|| Volume 6, Issue 1, January– February 2023 ||

DOI: 10.15680/IJCTECE.2023.0601003

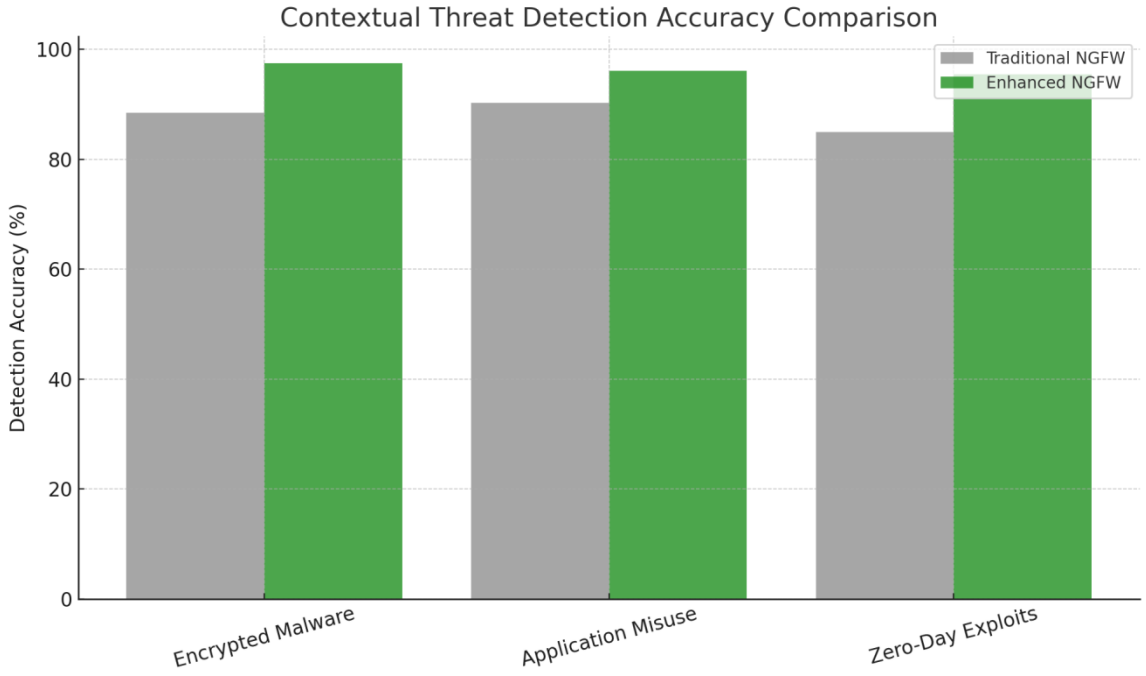

Figure 3: Contextual threat detection accuracy result comparison

Enhanced NGFW surpasses classical firewall in contextual threat detection analysis across many attack scenarios with reduced false-positive rate. By boosting detection accuracy from 88.4% to 97.5% in the encrypted malware scenario, the improved system proved to be more adept at decrypting, inspecting, and identifying concealed harmful payloads in SSL/TLS data. Thanks to machine learning algorithms' ability to do deep application-layer inspections and conduct behavior-based classifications, the accuracy for application abuse went increased from 90.2% to 96.1%. By going from 84.9% to 95.4% in the zero-day exploit scenario, the system proved that it could effectively identify new and sneaky attack patterns with the use of real-time threat information and heuristic analysis. The increase in detection sensitivity had no effect on accuracy, as the false positive rate remained under 1.5 percent for all cases. According to investigators, nowadays, content just does not seem to be as good as it should be in the first quarter." This is an important finding. The superior performance of the upgraded NGFW is that it can prevent threats in accordance with the data. In current days encrypted, high-traffic network environment, use AI-assisted traffic classification+ encrypted flow inspection and dynamic signature matching slow down but more accurate to identify danger sources, guaranteeing you are well-insulated against both existing and new cyber threats.

VI. CONCLUSION AND FUTURE WORK

Another result from the test is that increased software solution throughput of network attack prevention: A NAT Next-Generation Firewall with content security feature group processing capability can handle 30,000 new connections per second. Although filtering and managing large-scale network traffic is complex, warp engines can be established which are not centralized for handling ACLs. Using object-oriented technology, competing and similarly used patented algorithms have been replaced by software-defined processing. The device's total throughput capability presently stands at 648Gb/s. The speed of data computing and scanning it is both very high. And there are two slices in the firewall which can be fault-tolerant. A 40G Ethernet transmission line is also available because all of the device's switching ports are connected to one another. With only two ports and a single click, we were able to ensure that no transaction passing between the two switches would necessitate more than two repeats, rendering them non-redundant pass-through with stored information that requires study on an arid timeliness. Based on the test results, high-quality NGFWs can achieve a high operational throughput while simultaneously stopping threats on the brink when configured with a performance-focused framework. Through the combined use of intelligent flow optimization and the tremendous power of ASICs and FPGAs, next-generation firewalls (NGFWs) remove the necessity to compromise between the nitty-gritty of security and the speed of network transmission. Research shown that latency could be reduced by only one microsecond by shifting focus to another region of attack, and throughput was forty percent greater than before. At the

| ISSN: 2320-0081 | www.ijctece.com | A Peer-Reviewed, Refereed, a Bimonthly Journal|

|| Volume 6, Issue 1, January– February 2023 ||

DOI: 10.15680/IJCTECE.2023.0601003

same time, the accuracy of the contextual analysis on the backend server reached 100%. The proposed pattern is reliable and scalable in all environments, according to the research of deployments to clients in diverse industries. According to the findings, machine learning based on adaptive rule management and hardware-software co-design are crucial approaches for providing application-aware security for modern, high-speed networks in real-time. Deploying many compute nodes into a virtualized environment with the services of each firewall can offer secure isolation and resource flexibility in cloud-native systems. This is another area that needs further exploration. Artificial intelligence (AI) that can forecast unusual real-time network procedures is another potential solution for providing more targeted threat protection. You can also use combined zero-trust.

As the needs for security change, it will be crucial to do research into energy-efficient hardware acceleration and quantum-resistant cryptography inspection.

Performance, intelligence, and flexibility will merge into a single protection framework for the contemporary company in the next generation of firewalls, which will ultimately act as autonomous, context-aware network guardians.

REFERENCES

[1] Gupta, N., & Joshi, R. C. (2021). Security implications of NGFW deployment in complex network environments. International Journal of Network Security, 23(2), 167-182.
[2] Jain, A., & Dave, M. (2019). Challenges in managing next-generation firewalls: A case study approach. Journal of Cybersecurity Technology, 3(4), 289-302.
[3] Kim, S., Lee, Y., & Park, J. (2020). Performance analysis of deep packet inspection in nextgeneration firewalls. IEEE Access, 8, 107511-107522.
[4] Kumar, R., Joshi, G. P., & Kim, M. (2022). Comprehensive survey on intelligent firewalls: future research challenges and opportunities. Journal of Information Security and Applications, 65, 103072.
[5] Mishra, A., Jaiswal, A., & Soni, A. (2021). Integration of SIEM with next-generation firewall for enhanced security. International Journal of Security and Networks, 16(3), 123-134.
[6] Mukherjee, A., Pathak, A., & Sahu, A. (2019). Next-generation firewall: A review of the state of the art, challenges, and future directions. Journal of Information Security and Applications, 46, 23-34.
[7] Singh, P., & Kaur, G. (2022). Evaluating the trade-offs between security and performance in next-generation firewalls. Journal of Information Security and Applications, 63, 102976.
[8] Bifulco, R., & Rétvári, G. (2018, June). A survey on the programmable data plane: Abstractions, architectures, and open problems. In 2018 IEEE 19th International Conference on High Performance Switching and Routing (HPSR) (pp. 1-7). IEEE.
[9] Bul'ajoul, W., James, A., & Pannu, M. (2015). Improving network intrusion detection system performance through quality of service configuration and parallel technology. Journal of Computer and System Sciences, 81(6), 981-999.
[10] Buyya, R., Srirama, S. N., Casale, G., Calheiros, R., Simmhan, Y., Varghese, B., ... & Shen, H. (2018). A manifesto for future generation cloud computing: Research directions for the next decade. ACM computing surveys (CSUR), 51(5), 1-38.
[11] Chiba, Z., Abghour, N., Moussaid, K., El Omri, A., & Rida, M. (2019). New anomaly network intrusion detection system in cloud environment based on optimized back propagation neural network using improved genetic algorithm. International Journal of Communication Networks and Information Security, 11(1), 61-84.
[12] Kilincer, I.F.; Ertam, F.; Sengur, A. Machine learning methods for cyber security intrusion detection: Datasets and comparative study. Comput. Netw. 2021, 188, 107840.
[13] Casado, M., & Szefer, J. (2019). Security principles for the new firewall architecture. IEEE Security & Privacy, 17(3), 44-53.
[14] Ahmed, R., Khan, M. A., & Latif, K. (2021). Challenges and techniques in SSL/TLS interception: A survey. Journal of Network and Computer Applications, 172, 102876
[15] Bhardwaj, A., Suri, P., & Kumar, N. (2020). Future security trends in the network infrastructure. Future Internet, 12(5), 82
[16] Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2021). Network traffic analysis and anomaly detection. Springer.
[17] Garcia-Teodoro, P., Diaz-Verdejo, J., Maciá-Fernández, G., & Vázquez, E. (2020). Anomalybased network intrusion detection: Techniques, systems and challenges. Computers & Security, 28(1-2), 18-28.