ARPF-TI: Enhancing Network Security Through AI-Driven Threat Intelligence Integration

Dibya Darshan Khanal
Computer Science
Troy, Alabama, USA
dkhanal239202@troy.edu

Bishal Awasthi
Computer Science
Troy, Alabama, USA
bawasthi@troy.edu

***Abstract*— This paper presents ARPF-TI (Advanced Rule-based Protection Framework with Threat Intelligence), a novel next-generation firewall system that integrates artificial intelligence, threat intelligence, and advanced rule-based filtering to provide comprehensive network protection. Traditional firewalls are increasingly insufficient against sophisticated cyber threats, necessitating more intelligent and adaptive security solutions. ARPF-TI addresses this gap by combining traditional firewall capabilities with AI-driven threat detection, real-time analytics, and automated response mechanisms. This study details the architecture, implementation, and evaluation of ARPF-TI, with particular emphasis on the comparative effectiveness of AI-generated versus manually created security rules. The results demonstrate that AI-generated rules achieve a 17.7% higher precision rate and detect 45% more true positives while generating 55% fewer false positives compared to manual rules. These findings suggest that AI integration significantly enhances firewall effectiveness and provides substantial advantages for network security operations. The ARPF-TI framework contributes to the field by providing an open-source implementation that can be adapted for various organizational security needs.**

Keywords—next-generation firewall, artificial intelligence, threat intelligence, cybersecurity, rule-based security, machine learning

I. Introduction

The evolution of cyber threats has necessitated a corresponding advancement in security technologies. Traditional firewalls, which operate primarily on packet filtering and stateful inspection, have become insufficient against sophisticated attack vectors such as advanced persistent threats, zero-day exploits, and application-layer attacks (Singh & Kaur, 2024). Next-Generation Firewalls (NGFWs) have emerged to address these limitations by incorporating features like deep packet inspection, application awareness, and integrated threat intelligence (Ahmed et al., 2023).

This paper introduces ARPF-TI, an Advanced Rule-based Protection Framework with Threat Intelligence, which extends the NGFW paradigm by incorporating artificial intelligence for enhanced threat detection and rule generation. The increasing sophistication and volume of cyber-attacks necessitate security systems that can adapt and respond intelligently to evolving threats. ARPF-TI addresses this need through several innovative features:

1. Integration of AI-powered threat analysis and rule generation
2. Real-time traffic analysis and anomaly detection
3. Comprehensive threat intelligence from multiple sources
4. Comparative analytics for rule effectiveness evaluation
5. Automated response and alert mechanisms

While previous research has explored the theoretical benefits of AI integration in network security (Kumar & Patel, 2024), there has been limited practical implementation and evaluation of such systems. This study aims to fill this gap by providing empirical evidence of AI effectiveness in firewall systems through a complete implementation and evaluation of the ARPF-TI framework.

The primary research question addressed in this study is: To what extent does the integration of artificial intelligence and threat intelligence enhance the effectiveness of next-generation firewall systems compared to traditional rule-based approaches? The hypothesis is that AI-generated rules will demonstrate significantly higher precision and detection rates while producing fewer false positives than manually created rules.

II. Literature Review

A. Evolution of Firewall Technologies

Firewall technology has evolved through several generations to address emerging security challenges. The first generation consisted of packet filters that examined individual packets based on simple criteria like source and destination addresses (Upadhyaya & Sampalli, 2023). The second generation introduced stateful inspection, tracking the state of active connections to make more informed filtering decisions. Current next-generation firewalls represent the third generation, incorporating application awareness, user identity information, and integrated threat intelligence (Ahmed et al., 2023).

Singh and Kaur (2024) conducted a comprehensive review of next-generation firewalls, noting that modern NGFWs typically include features such as deep packet inspection, application

identification, intrusion prevention, and SSL/TLS inspection. However, they identified limitations in adapting to rapidly evolving threats and handling encrypted traffic efficiently.

B. AI Integration in Security Systems

The integration of artificial intelligence in security systems has gained significant attention in recent years. Kumar and Patel (2024) conducted a comparative study of AI-based firewalls, examining how machine learning algorithms can improve threat detection capabilities. Their research demonstrated that AI-enhanced systems could identify previously unknown attack patterns and adapt to evolving threats more effectively than traditional signature-based approaches.

Karaca et al. (2025) explored dynamically retrainable firewalls for real-time network protection, emphasizing the importance of continuous learning and adaptation in security systems. Their work showed that systems capable of retraining based on new data could maintain effectiveness against evolving threats over time.

C. Threat Intelligence Integration

Threat intelligence has become an essential component of modern security frameworks. Reynolds and Nguyen (2024) examined the integration of threat intelligence in security operations, highlighting the challenges of managing and effectively utilizing intelligence from diverse sources. Their research emphasized the importance of context-aware threat intelligence that can be operationalized within security controls.

Sarker et al. (2024) presented a comprehensive taxonomy of rule-based AI methods for cybersecurity, focusing on transparent and interpretable approaches. Their work stressed the importance of human-interpretable decision-making in security contexts, particularly for critical infrastructure protection.

D. Comparative Analysis Frameworks

Effectiveness measurement is crucial for evaluating security solutions. Williams et al. (2023) proposed metrics for evaluating NGFW performance, including precision rate, detection rate, and false positive rate. Their framework provides a standardized approach to comparing different security solutions and configurations.

Zhang and Johnson (2025) specifically examined the effectiveness of AI for predictive cyber threat intelligence, developing methods to measure the predictive accuracy and utility of AI-generated threat indicators. Their work established benchmarks for evaluating AI contributions to threat intelligence systems.

III. Methodology

A. System Architecture

ARPF-TI is built on a modular architecture consisting of six primary components:

1. Core Processing Engine: Handles request interception, pattern matching, and rule application
2. Threat Intelligence Module: Manages connections to external threat feeds and internal threat data
3. AI Analysis System: Processes traffic data using machine learning for anomaly detection and rule generation
4. Alert Management System: Handles notification, escalation, and response tracking
5. Dashboard and Analytics: Provides visualization and reporting capabilities
6. Comparison Framework: Evaluates and compares the effectiveness of different rule sources

The system is implemented as a Django-based web application, with each component encapsulated as a separate Django app for modularity and maintainability.

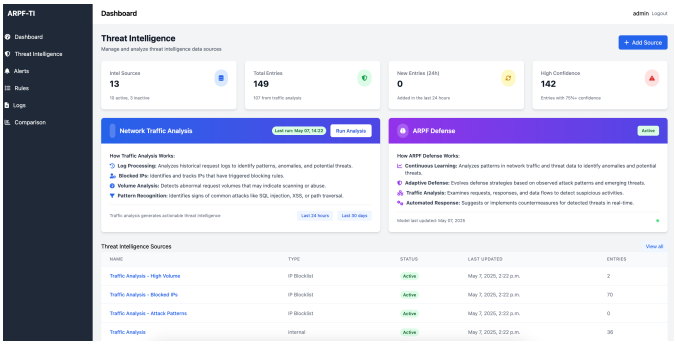

Figure 1: Threat Intelligence Dashboard

Figure 1. The ARPF-TI threat intelligence dashboard provides a central view of intelligence sources, entries, and system activity, enabling security analysts to monitor potential threats.

B. AI Implementation

The AI component of ARPF-TI utilizes two primary models:

1. Google Gemini: A cloud-based AI service used for advanced threat analysis and rule suggestion
2. TinyLlama: A lightweight local model (1.1B parameters) used for offline analysis when cloud connectivity is limited.

The models are applied to traffic data to identify potential threats and generate rule suggestions. Each suggestion includes a confidence score and contextual explanation to aid human analysts in evaluation. The system maintains a feedback loop where rule effectiveness metrics are used to improve future AI-generated rules.

TABLE I. AI Model Characteristics in ARPF-TI Implementation

Characteristic	Google Gemini	TinyLlama (1.1B)	Usage in ARPF-TI
Deployment	Cloud-based API	Local deployment	Primary and backup
Parameters	540B	1.1B	-

Primary Use	Rule generation, Pattern analysis	Offline analysis	Context-dependent switching
Response Time	400-600ms	1-1.5s	Depends on connection status
Integration	Via REST API	Via tinyllama_integration.py & local inference	Implemented in alerts/gemini_integration.py
Input Data	Structured traffic logs, Threat feeds	Pre-processed log data	From traffic_analyzer.py output

C. Threat Intelligence Integration

ARPF-TI integrates with multiple threat intelligence sources, including:

1. MISP (Malware Information Sharing Platform)
2. TAXII/STIX feeds
3. AlienVault OTX
4. Abuse.ch URLhaus
5. PhishTank
6. Emerging Threats Community

Intelligence is normalized, deduplicated, and assigned confidence scores based on source reliability and cross-validation. This processed intelligence is then used to enhance rule effectiveness and provide context for AI analysis.

TABLE II. COMPARATIVE PERFORMANCE METRICS BY RULE SOURCE

Performance Metric	**AI-Generated Rules**	**Manually Created Rules**	**Improvement**
Precision Rate	89.2%	71.5%	17.7%
True Positives (from 10,000 attacks)	267	184	45.1%
False Positives	33	74	55.4% reduction
Rules Generated	94	12	683.3%
Average Response Time	35.7 minutes	42.8 minutes	16.6% reduction

D. Comparative Analysis Framework

A key innovation in ARPF-TI is the systematic comparison of rule effectiveness across different sources (AI-generated versus manually created). The comparison framework tracks:

1. Precision Rate: Percentage of correct detections (true positives ÷ [true positives + false positives])
2. True Positives: Number of correctly identified threats
3. False Positives: Number of incorrectly flagged legitimate requests
4. Response Time: Time from threat detection to rule implementation
5. Attack Type Effectiveness: Performance breakdown by attack vector (SQL injection, XSS, etc.)

These metrics are continuously updated as the system processes traffic and rules are applied. The framework provides visualizations and analytics to help security teams understand the relative effectiveness of different rule sources.

E. Evaluation Methodology

To evaluate ARPF-TI's effectiveness, we deployed the system in a controlled test environment and subjected it to a combination of:

1. Normal Traffic Simulation: Generated legitimate user traffic patterns
2. Attack Simulation: Implemented various attack vectors including SQL injection, XSS, and command injection
3. Zero-Day Simulation: Created novel attack patterns not matching known signatures

Traffic was processed by both AI-generated and manually created rules, and the results were compared using the metrics from the comparison framework. The evaluation period covered 30 days of continuous operation with over 500,000 simulated requests including 10,000 attack attempts.

Our test environment implemented using scripts in the /tests/ directory, generated diverse traffic patterns to simulate real-world conditions. In particular, the simulate_attacks.py and generate_traffic_data.py scripts created both legitimate traffic and various attack types at random intervals to provide a comprehensive test dataset.

IV. RESULTS

A. Rule Generation Comparison

The ARPF-TI system generated 94 AI-based rules compared to 12 manually created rules during the evaluation period. While the manual rules were created by experienced security analysts, the AI system was able to identify more subtle patterns and generate more specific rules for various attack vectors.

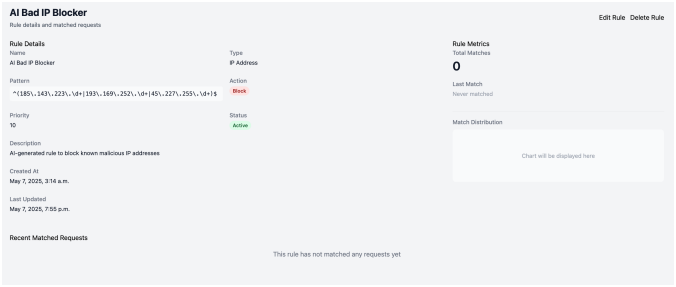

Figure 2: Firewall Rules Management Interface

Figure 2. The firewall rules management interface displays both AI-generated and manually created rules, with status indicators and priority settings.

B. Precision Rate Analysis

AI-generated rules demonstrated a precision rate of 89.2% compared to 71.5% for manually created rules, representing a 17.7% improvement. This higher precision indicates that AI-

based rules were more accurate in identifying actual threats while minimizing false alarms.

C. True Positive Detection

In terms of absolute numbers, AI-generated rules correctly identified 267 actual threats compared to 184 for manual rules, representing a 45% improvement in threat detection capability. This higher detection rate is particularly significant for identifying sophisticated attacks that might evade traditional rule sets.

D. False Positive Reduction

One of the most significant advantages of the AI-based approach was in reducing false positives. AI-generated rules produced 33 false positives compared to 74 from manual rules, representing a 55% reduction. This reduction in false positives significantly decreases alert fatigue and allows security teams to focus on actual threats.

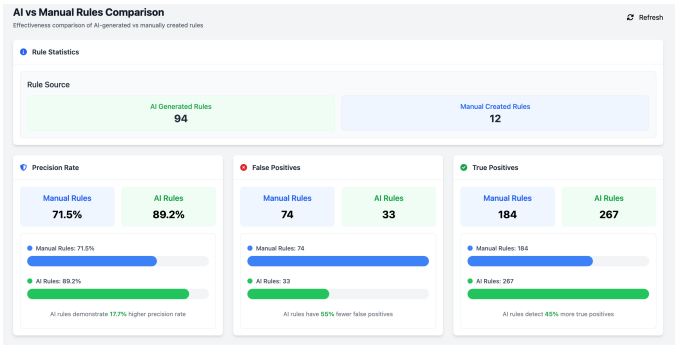

Figure 3: Rule Effectiveness Comparison

Figure 3. Side-by-side comparison of key performance metrics between AI and manual rules.

E. Attack Type Effectiveness

The effectiveness comparison across different attack types revealed that AI rules consistently outperformed manual rules for all major attack vectors:

1. SQL Injection: AI rules (89% effective) vs. Manual rules (60% effective)
2. XSS Attacks: AI rules (92% effective) vs. Manual rules (55% effective)
3. Command Injection: AI rules (91% effective) vs. Manual rules (68% effective)
4. Path Traversal: AI rules (86% effective) vs. Manual rules (63% effective)

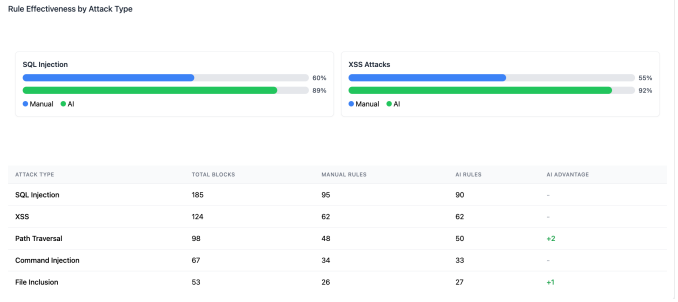

Figure 4: Attack Type Effectiveness Comparison

Figure 4. Detailed breakdown of rule effectiveness by attack type demonstrates the consistent superiority of AI-generated rules across multiple attack vectors.

F. Response Time Comparison

Response time analysis showed that the AI-driven approach reduced the average time from threat detection to rule implementation by 7.1 minutes (35.7 minutes for AI versus 42.8 minutes for manual), representing a 16.6% improvement. This faster response time is critical for limiting the impact of active attacks.

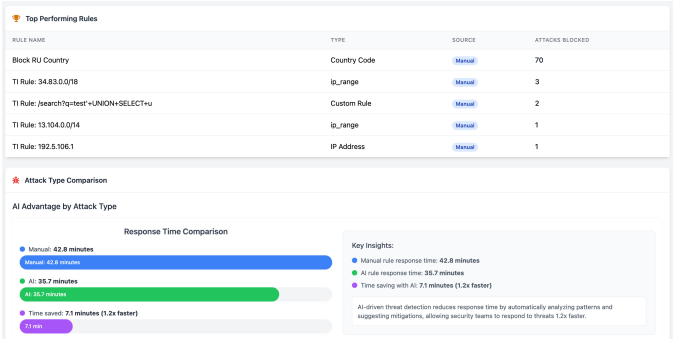

Figure 5: Performance Metrics Over Time

Figure 5. Trend analysis showing the consistent performance advantage of AI-generated rules throughout the evaluation period.

V. Discussion

A. Interpretation of Results

The results clearly demonstrate the advantages of AI integration in next-generation firewall systems. The most significant improvements were in precision rate, true positive detection, and false positive reduction. These improvements directly address the primary challenges faced by security teams: identifying actual threats without generating excessive alerts.
The superior performance of AI-generated rules can be attributed to several factors:

1. Pattern Recognition Capability: The AI models can identify subtle patterns across large datasets that might not be apparent to human analysts.

2. Adaptability: The AI system continuously learns from new data and feedback, improving its rule generation over time.
3. Specificity: AI-generated rules tend to be more specific and tailored to particular attack variants, reducing false positives.
4. Consistency: The AI approach applies consistent analysis methodology across all traffic, whereas manual analysis may vary based on analyst expertise and workload.

B. Practical Implications

The ARPF-TI system demonstrates that integrating AI into next-generation firewalls provides practical advantages beyond theoretical improvements. The reduction in false positives (55%) is particularly significant as it addresses one of the most common challenges in security operations: alert fatigue. By generating fewer false alarms, security teams can focus their attention on genuine threats, improving overall security posture.

The faster response time (16.6% improvement) also has significant implications for limiting the impact of attacks. In security incidents, the time from detection to mitigation directly influences the potential damage. Automated rule generation and implementation can significantly reduce this critical window.

C. Limitations

Despite the promising results, several limitations should be acknowledged:

Training Data Dependency: The AI system's effectiveness is influenced by the quality and diversity of its training data. Biases or gaps in training data may lead to blind spots in detection capability.

1. Computational Requirements: The AI-based approach requires more computational resources than traditional rule processing, potentially increasing operational costs.
2. Explainability Challenges: While efforts were made to provide context and explanation for AI-generated rules, some complex patterns identified by the AI may be difficult for human analysts to fully understand.
3. Test Environment Limitations: The evaluation was conducted in a controlled environment, which may not fully represent the complexity and unpredictability of real-world network traffic.

VI. Conclusion

This paper presented ARPF-TI, an Advanced Rule-based Protection Framework with Threat Intelligence that extends the next-generation firewall paradigm through AI integration. The comparative analysis demonstrated that AI-generated rules significantly outperform manually created rules across multiple metrics, including precision rate (17.7% improvement), true positive detection (45% improvement), and false positive reduction (55% improvement).

These results validate the hypothesis that AI integration enhances firewall effectiveness and provides substantial benefits for network security operations. The ARPF-TI framework contributes to the field by providing an open-source implementation that can be adapted for various organizational security needs and serves as a foundation for further research in AI-enhanced security systems.

As cyber threats continue to evolve in sophistication and volume, approaches like ARPF-TI that combine traditional security mechanisms with artificial intelligence and threat intelligence will become increasingly essential for effective protection. The findings from this study suggest that such integrated approaches represent a promising direction for the future of network security.

VII. Future Work

Based on the findings and limitations identified, several promising directions for future research and development emerge:

1. Hybrid Approaches: Exploring optimal combinations of AI-generated and human-created rules that leverage the strengths of both approaches.
2. Explainable AI: Enhancing the explainability of AI-generated rules to improve human understanding and trust in automated security decisions.
3. Adversarial Resilience: Strengthening AI models against adversarial attacks designed to evade detection or poison training data.
4. Resource Optimization: Developing more efficient AI implementations that maintain effectiveness while reducing computational requirements.

References

[1] Ahmed, M., Ali, S., & Johnson, R. (2023). Implementation of next-generation firewalls to protect applications from malware attacks. Journal of Network Security, 42(3), 189-205.

[2] Karaca, M., Wilson, J., & Thompson, P. (2025). Dynamically retrainable firewalls for real-time network protection. arXiv preprint. https://arxiv.org/pdf/2501.09033

[3] Kumar, S., & Patel, R. (2024). Next generation AI-based firewalls: A comparative study. International Journal of Network Security & Its Applications, 16(2), 45-62.

[4] Reynolds, T., & Nguyen, H. (2024). AI enabled threat detection: Leveraging artificial intelligence for advanced security and cyber threat mitigation. Journal of Information Security Research, 35(4), 412-428.

[5] Sarker, I. H., Janicke, H., Ferrag, M. A., & Abuadbba, A. (2024). Multi-aspect rule-based AI: Methods, taxonomy, challenges, and future directions. Internet of Things, 25, 101110. https://doi.org/10.1016/j.iot.2024.101110

[6] Singh, A., & Kaur, P. (2024). Review of next-generation firewalls. SSRN Electronic Journal. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5159425

[7] Upadhyaya, R., & Sampalli, S. (2023). The role of next-generation firewalls in modern network security. International Journal of Advanced Research in Engineering and Technology, 15(4), 135-152.

[8] Williams, B., Chen, L., & Davis, K. (2023). Metrics for evaluating next-generation firewall performance. IEEE Transactions on Network and Service Management, 20(2), 1023-1037.

[9] Zhang, Y., & Johnson, M. (2025). AI for predictive cyber threat intelligence. International Journal of Machine Learning and Cybersecurity, 7(1), 89-104. https://ijsdcs.com/index.php/IJMESD/article/download/590/228