Next-Generation Firewall Effectiveness Against Encrypted and Evasive Threats

Favour Anene

Old Dominion University
November 10/2025

Introduction

Coded traffic is emerging as a foundation of security and confidentiality in business networks. Google Transparency Report has a report showing that more than 95 percent of traffic over the internet is encrypted using Hypertext Transfer Protocol secure (HTTPS), Transport Layer Security (TLS) 1.3 and Quick UDP Internet Connections (QUIC). Even though encryption ensures confidentiality and integrity, there are new blind spots to the traditional security solutions because of this feature. The command-and-control (C2) traffic is concealed in encrypted channels; malware and the extraction of sensitive information are issued without their awareness.

To complicate the matter further, those to whom it opposes have advanced avoidance techniques such as fragmentation of traffic, tunneling, and polymorphic malware. Such plans are tailor made to avoid systems of inspections. It is impossible to deal with such threats using traditional firewalls and intrusion detection systems (IDS).

Next-Generation Firewalls (NGFWs) emerged to address these inadequacies. They constitute a combination of deep packet inspection (DPI), intrusion prevention systems (IPS), application knowledge and user identity tracking. However, their ability to balance between good threat detection and network performance particularly in the encrypted traffic, malware that evades are still doubtful.

The purpose of this paper is to examine the performance of NGFW under such a state. It will compare solutions of vendors, investigate detection features and propose an augmentation framework based on AI. The following questions will be used as research questions:

Research Questions

1. How effective are NGFWs in detecting threats within encrypted traffic?
2. How resilient are NGFWs to advanced evasion techniques?
3. What trade offs exist between security effectiveness and network performance?
4. How might AI based enhancements improve NGFW effectiveness?

Thesis Statement: While NGFWs offer enhanced protection compared to traditional firewalls they face measurable limitations when dealing with encrypted and evasive threats. Through empirical testing and proposed AI driven enhancements, this study aims to strengthen NGFW effectiveness in enterprise networks.

Literature Review

How Effective Are NGFWs in Detecting Threats Within Encrypted Traffic?

Coded traffic is emerging as a foundation of security and confidentiality in business networks. Google Transparency Report has a report showing that more than 95 percent of traffic over the internet is encrypted using Hypertext Transfer Protocol secure (HTTPS), Transport Layer Security (TLS) 1.3 and Quick UDP Internet Connections (QUIC). Even though encryption ensures confidentiality and integrity, there are new blind spots to the traditional security solutions because of this feature. The command-and-control (C2) traffic is concealed in encrypted channels; malware and the extraction of sensitive information are issued without their awareness.

To complicate the matter further, those to whom it opposes have advanced avoidance techniques such as fragmentation of traffic, tunneling, and polymorphic malware. Such plans are tailor made to avoid

systems of inspections. It is impossible to deal with such threats using traditional firewalls and intrusion detection systems (IDS).

Next-Generation Firewalls (NGFWs) emerged to address these inadequacies. They constitute a combination of deep packet inspection (DPI), intrusion prevention systems (IPS), application knowledge and user identity tracking. However, their ability to balance between good threat detection and network performance particularly in the encrypted traffic, malware that evades are still doubtful.

The purpose of this paper is to examine the performance of NGFW under such a state. It will compare solutions of vendors, investigate detection features and propose an augmentation framework based on AI. The following questions will be used as research questions:

How Resilient Are NGFWs to Advanced Evasion Techniques?

Traffic coding is becoming the source of security and confidentiality in business networks. A report provided in Google Transparency Report reveals that over 95 percent of the traffic traversing the internet is encrypted using Hypertext Transfer Protocol secure (HTTPS), Transport Layer Security (TLS) 1.3 and Quick UDP Internet Connections (QUIC). Although the traditional security solutions are assured by encryption, which guarantees confidentiality and integrity, there are emerging blind spots due to this feature. The command and control (C2) traffic will be hidden on the encrypted channels; virus and retrieval of their sensitive data will be given without their knowledge.

To make the issues more complicated, the methods of avoiding it have been developed by its opponents, including traffic fragmentation, tunneling, and polymorphic malware. These plans are specifically designed so as to shun systems of checks. Such threats cannot be addressed by the use of conventional firewalls and intrusion detection systems (IDS).

Next-Generation Firewalls (NGFWs) came up to fill in these shortcomings. They are a conglomerate of deep packet inspection (DPI), intrusion prevention systems (IPS), application knowledge and user identity tracking. Nevertheless, they are still questionable in terms of balancing between good threat detection and network performance, specifically in the encrypted traffic, malware that avoids detection.

This paper is aimed at discussing the performance of NGFW in such a state. It will create comparisons of the solutions of vendors, examine the features of detection and suggest an augmentation framework grounded in AI. Research questions will be the following.

What Trade-Offs Exist Between Effectiveness and Network Performance?

One of the typical issues with NGFW implementation is the balancing of security depth against operational performance. DPI, SSL/TLS decryption, and behavior analysis are operations that require a lot of CPU and memory, and therefore, they can cause slowdown or drop-in throughput. The Sherry et al. (2015) paper shows that in high-volume scenarios, performance can be lowered by up to 70% due to the inspection based on full decryption, and hence, the administrators are forced to choose between a high level of visibility and a tolerable latency or performance at a reduced level of their acceptability.

Most of the enterprises decide to deactivate such resource-intensive functions as SSD decryption to improve the performance of the firewall, as stated in the Gartner 2023 Magic Quadrant for Network Firewalls report. Nevertheless, this leads to fewer protections. Hence, the administrators NGFW should be changed cautiously as well as deciding on the highest priority of the inspections, which captures rules, and even if some analyses are done by a cloud-based threat intelligence service.

Giving up these concessions to the trade-off problem proves that there is always a trade-off, the more thorough the inspection, the bigger the overhead. The optimal trade-off would consist in some kind

of intelligent selectivity according to which an inspection should be performed on a high-risk flow or a suspicious flow, while traffic that is benign should be allowed to proceed without any interruption.

How Might AI-Based Enhancements Improve NGFW Effectiveness?

Artificial intelligence (AI) can be used together with machine learning (ML) to transform the approach of NGFWs to scan traffic and adapt to emerging threats. According to Buczak and Guven (2016), intrusion detection systems (IDS) with the requirement of using a ML can identify an anomaly in encrypted traffic along the statistical and flow-based characteristics rather than packet content. This will allow discovery of threats without disrupting encryption.

AI-enhanced NGFWs leverage several techniques, including:

- Network behavior learning models that identified network behavior abnormalities.
- Automated optimization of the rules, i.e., with varying threat intelligence fees, the security system policies are also modified.
- Predictive threat modeling that uses pattern recognition to infer any attempt to get around prior to signature versions updating.

Vendors including Fortinet and Palo Alto have already integrated AI-based engines on their NGFW engines to prevent false positives and improve adaptive filtering. The effectiveness of such systems, however, heavily relies on the quality and diversity of the training information, and the ability to extrapolate complex network behavior in real-time.

Besides increasing the detection level, AI enables the performance-security trade-off since fewer resources are needed to perform exhaustive decryption and inspection to process the traffic to make quicker and smarter filtering decisions by the security system.

Technical Overview of Next-Generation Firewalls (NGFWs)

Handling Encrypted Communication

Modern NGFWs employ complementary methods to preserve visibility while processing encrypted traffic:

1. **SSL/TLS Interception (Decryption and Inspection).** The firewall is a temporary MITM proxy that will decrypt, examine and re-encrypt data to make DPI and IPS functions possible. Although detailed, this approach adds to the latency and introduces privacy and compliance challenges (Papadogiannaki et al., 2021; Sherry et al., 2015).
2. **Certificate and Handshake Analysis.** Deciphlation of TLS metadata, such as certificates, cipher suites, and session parameters, can be used to identify the anomaly when it is impossible to decrypt TLS. JA3/JA3S fingerprinting are techniques that divide encrypted sessions and distinguish spoofed or malicious traffic (Dusi et al., 2017).
3. **Encrypted Traffic Analytics (ETA).** The machine-learning-based flow statistic-based ETA EDT identifies malicious traffic without decryption based on packet size, timing and direction. These solutions are Cisco ETA and Palo Alto App-ID. They work, though, when the data that undergoes the training is of good quality, and the context is diverse (Buczak and Guven, 2016).

Methods Used to Filter Adversarial Communication

NGFWs integrate multiple detection layers to identify adversarial traffic:

- Signature-Based Detection quickly stops familiar attacks - yet struggles when facing changing malware designed to dodge detection (Cazorla et al., 2019).

- Behavioral plus heuristic analysis spots odd traffic behavior - like strange DNS queries or weird data movement - to find never-before-seen threats (Buczak & Guven, 2016).
- App-aware filtering shows what's happening at level seven, using tight rules while stopping dangerous apps - per Gartner's 2023 report.
- Threat intelligence links up with worldwide data streams to refresh signs of breaches along with trust ratings (Papadogiannaki et al., 2021).

Sandboxing along with deep learning sets apart shady code to study how it acts when running, which boosts spotting sneaky or changing malware forms (Dusi et al., 2017).

Main Flaws and Limitations

However, the sophisticated technologies of NGFWs are not enough to solve their persistent limitations.

- When the data is being decrypted, speed problems are occurring - the operation consumes more power, which slows down the whole system and limits further development (Sherry et al., 2015).
- When decryption is off, a limited view is available - the analysis is performed based on metadata, so it may not detect that kind of threats. The inspection may be less safe since it only minimally checks the surface when decoding is not active (source).
- By-passing vulnerabilities. Dividing or concealing operations are escaping from the most recent methods of checking - the studies confirm this beyond doubt (Cazorla et al., 2019).
- The dependence on external data sources can slow the process down - when the threat information is delayed or some pieces are missing, the instant protection can be weakened (Dusi et al., 2017).
- There might be privacy concerns when using SSL inspection - it may conflict with regulations like HIPAA or GDPR.
- Mixing up configurations most of the time results in a low level of security - a common problem, as Gartner states (2023).

Such limits push toward smart systems that mix precision with speed while keeping data safe in scrambled settings.

Methodology

Research Design

Some Practical experiments, and a follow-up analysis, to examine the performance and endurance of next-generation firewalls when confronted with a real network environment specially constructed for testing purposes. Various NGFW instruments are tested through the same complex and mixed-up data streams - the same rules each time - to keep the results accurate and reproducible.

Experimental Testbed

An artificially created network layout comprises core components, intermediate spaces, and external areas that are supposed to represent malicious entities. The equipment used comprises Palo Alto firewalls along with FortiGate units, Cisco Firepower devices, or pfSense boxes; also incorporates VMware ESXi platforms; testing apps like Ixia in conjunction with Metasploit and Scapy; and finally, monitoring tools like Wireshark along with Zeek.

Traffic and Data Collection

Three kinds of traffic data will be exposed:

- Real encrypted traffic - for example, TLS 1.3 or QUIC - for common scenarios.
- Stealthy data travels through morphing code, fragments - deep down in encrypted routes.
- Hybrid traffic consists of good network usage together with malicious data streams.

Evaluation Metrics

1. Detection: were the hits real or missed, how often did it find things, also precision.

2. Speed: how much work gets done, waiting times for the task, usage of the computer power and memory.
3. Being able to keep on going without losing is basically being able to avoid problems and being able to keep your composure under long-term pressure.

Statistical operations in Python - with the help of pandas or NumPy - can find not only the averages and the spreads but also the relative standings of different things.

AI-Enhanced Analytical Framework

Once the results are inspected, we will recommend an AI-powered instrument that comprises:

1. Locating unusual patterns through monitoring data movement, identifying unusual behavior by intelligent algorithms that derive learning from the details of network traffic.
2. Automatically updating rules with reinforcement learning by way of trial and error.
3. Real-time threat intelligence is integrated into the system - hence, security can change dynamically.

Limitations

Vendor opacity, simulation constraints, and dataset bias may affect generalizability; results will therefore be contextualized using industry benchmarks.

Expected Results and Discussion

Detection Performance

Next-generation firewalls (NGFWs) are capable of detecting more than 95% of straightforward threats but their detection rate drops to only 70-80% when they need to handle concealed or encrypted data. Machine

learning-based tools are often more effective in such cases as they do not depend on traditional pattern-matching methods, which is supported by the research of Papadogiannaki and the team in 2021 and Cazorla's group in 2019.

Performance Trade-Offs

Complete SSL/TLS decryption combined with deep packet inspection usually results in a reduction of operating speeds by approximately 40–60% and the slowing of response times as well - thus, the current findings are in line with the previous ones (Sherry et al., 2015). Choosing certain traffic for verification along with a more efficient set of rules supports the alleviation of the performance decline.

Evasion Resistance

Hybrid firewalls using pattern checks, behavior analysis, or isolated testing should block typical bypass tricks - yet still struggle against hidden data paths and disguised traffic formats (Dusi et al., 2017).

Implications

Up Buddh to this point it has only been a theoretical concept. The findings may serve as evidence for a different approach to managing secure systems that utilize AI for data privacy, which would be a development of the idea that Buczak and Guven presented in 2016.

Quite practical. Results empower decision makers to decide the extent of SSL verification, incorporate traffic analysis through flow techniques - at the same time fine-tuning rules for keeping operations swift without putting user data at risk.

Future Directions

Scientists should dig deeper and try new ways or check different angles before concluding.

- AI-powered intelligent firewalls, deployed either at the cloud or at the edge.

- Federated learning systems that develop intelligent networks while no private data is shared.
- Long-term studies monitoring the changes in behavior of intelligent firewalls.

Conclusion

The study indicates that Next-Generation Firewalls (NGFWs) represent a significant advancement in a company's cyber defense arsenal. However, they still have difficulties with unmonitored encrypted traffic, sophisticated attacks, and sometimes causing the system to slow down. The results emphasize that security, speed, and privacy are the main factors influencing the network defenses of today.

One of the findings is that SSL inspection is effective but may conflict with the privacy of users. Instead of having set rules, detecting abnormal behavior is more effective in finding more threats. Besides that, intelligent AI-powered analysis might make systems more efficient in responding and using fewer resources.

The greater impact of this is the transition to smart, adaptable security measures that are ethically guided and capable of protecting data in complex, encrypted systems. Meanwhile, law enforcement officials should put in place oversight regulations to ensure that AI-powered security measures operate transparently and comply with privacy laws.

Ultimately, the development of NGFWs will be a matter of combining new technologies with established security principles - thus, future safeguards will not only protect companies but also ensure integrity and trust in the current digital world.

References

- Buczak, A. L., & Guven, E. (2016). *A survey of data mining and machine learning methods for cyber security intrusion detection.* IEEE Communications Surveys & Tutorials, 18(2), 1153–1176. A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection | IEEE Journals & Magazine | IEEE Xplore
- Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials, 18*(2), 1153–1176. https://ieeexplore.ieee.org/abstract/document/7307098
- Cazorla, C., Díaz, R., Sánchez, P., & Berrocal, J. (2019). Polymorphic malware detection: Taxonomy, challenges and open issues. *Journal of Information Security and Applications, 48*, 102–110.
- Dusi, M., Gringoli, F., & Hock, D. (2017). Detection of evasive traffic in encrypted environments. *IEEE Transactions on Network and Service Management, 14*(3), 705–718.
- Papadogiannaki, E., Ioannidis, S., & Markatos, E. P. (2021). Deep packet inspection of TLS encrypted traffic: A survey. *IEEE Communications Surveys & Tutorials, 23*(1), 1–33.
- Sherry, J., Lan, C., Popa, L., & Ratnasamy, S. (2015). BlindBox: Deep packet inspection over encrypted traffic. In *Proceedings of the ACM SIGCOMM Conference* (pp. 213–226). ACM. https://dl.acm.org/doi/abs/10.1145/2785956.2787502
- Zscaler ThreatLabz. (2025, April 1). Over 85% of attacks are encrypted: ThreatLabz Report. Retrieved from https://www.zscaler.com/blogs/security-research/2022-encrypted-attacks-report
- Google Transparency Report. (n.d.). HTTPS encryption on the web. Retrieved November 19, 2025, from https://transparencyreport.google.com/https?hl=en
- Skyone. (2025, August 7). NGFW: visibility and protection in encrypted traffic. Retrieved from https://skyone.solutions/en/blog/cybersegunca/role_of_ngfw/

- Corelight. (2024, November 12). What Is a Next-Generation Firewall (NGFW)? Retrieved from https://corelight.com/resources/glossary/ngfw-next-generation-firewall
- Checkpoint. (2025, August 27). AI-Powered Firewall. Retrieved from https://www.checkpoint.com/cyber-hub/network-security/what-is-firewall/ai-powered-firewall/
- SageNet. (2022, January 20). Can Your Firewall Detect Encrypted Threats? Retrieved from https://www.sagenet.com/insights/can-your-firewall-detect-encrypted-threats/
- SecureITConsult. (2024, September 23). Leveraging AIOps To Enhance Next-Generation Firewall. Retrieved from https://secureitconsult.com/aiops-for-ngfw/
- Sherry, J., Lan, C., Popa, L., & Ratnasamy, S. (2015). *BlindBox: Deep packet inspection over encrypted traffic.* In *Proceedings of the ACM SIGCOMM Conference* (pp. 213–226). ACM. BlindBox | Proceedings of the 2015 ACM Conference on Special Interest Group on Data Communication