International Journal of Sciences and Innovation Engineering
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
website: www.ijsci.com
Vol.02 No.10
E-ISSN : 3049-0251
DOI: https://doi.org/10.70849/ijsci

Next-Generation Firewall (NGFW) Technologies and Their Application in Enterprise Security

Kaneriya Smit. P[1], Prof. Devangi Paneri[2]
[*1,2] *Atmiya University's Computer Engineering Department, Rajkot, Gujarat, India*

Article Info

Article History:

Published:5 Oct 2025

Publication Issue:
Volume 2, Issue 10
October-2025

Page Number:
106-115

Corresponding Author:
Kaneriya Smit. P

Abstract:

This paper provides a comprehensive review of firewall technologies, focusing on the evolution from traditional firewalls to Next-Generation Firewalls (NGFWs). The study examines various firewall types, including packet filtering, stateful inspection, application-layer, and next-generation firewalls. It highlights their key features, advantages, and limitations. The paper compares Fortinet's FortiGate NGFW with Cisco's Adaptive Security Appliance (ASA), emphasizing the advanced capabilities of NGFWs in addressing modern cybersecurity challenges. Key aspects covered include virtualization, SSL/TLS inspection, and automation features. The research underscores the importance of NGFWs in protecting hybrid environments and handling increasing volumes of data-intensive traffic and cloud-based applications.

Keywords: Next-Generation Firewalls, Network Security, Deep Packet Inspection, Intrusion Prevention Systems, Application Awareness, SSL/TLS Inspection, Virtualization, Unified Threat Management, FortiGate, Cisco ASA, Firewall Evolution, Cybersecurity, Cloud Security, Hybrid Environments, Threat Intelligence

1. INTRODUCTION

Next-generation firewalls (NGFWs) represent a significant advancement in network security technology, offering comprehensive protection for modern hybrid environments. Unlike traditional firewalls, NGFWs incorporate advanced features such as deep packet inspection, intrusion prevention systems, and application awareness. They analyse traffic across multiple layers, combining traditional firewall functionalities with sophisticated threat detection and prevention tools. NGFWs leverage real-time threat intelligence to identify emerging threats, including zero-day vulnerabilities. Key features of NGFWs include application awareness and control, integrated intrusion prevention systems deep packet inspection, SSL/TLS traffic inspection, and user identity integration. These capabilities enable NGFWs to provide more robust security, better performance, and simplified management compared to traditional firewalls. For instance, FortiGate NGFWs, backed by Al-powered security services, offer consistent, real-time protection against advanced threats while efficiently handling high volumes of data-intensive traffic and cloud-based applications. In contrast, traditional firewalls like Cisco's Adaptive Security Appliance (ASA) provide basic perimeter security but lack the advanced features and integrated threat management capabilities of NGFWs

2. EVOLUTION OF FIREWALLS

A. Packet-Filtering Firewalls (First-Generation)

Packet-filtering firewalls represent the earliest form of firewall technology. They are designed to monitor both incoming and outgoing traffic based on established rules concerning IP addresses, protocols, and port numbers. Operating at the network (Layer 3) and transport (Layer 4) layers of the OSI model, these firewalls determine whether to permit or block packets based solely on header information, without examining the contents or payload of the packets.

B. Stateful Inspection Firewalls (Second-Generation)

Stateful inspection firewalls significantly improved upon first-generation firewalls by incorporating the ability to track the state of active connections. Unlike their predecessors, which only assessed individual packets, stateful firewalls maintain a state table that monitors entire sessions. For instance, they can identify the initiation, maintenance, and termination of TCP connections through recognizable packets, such as SYN, ACK, and FIN. This enhanced session awareness enables stateful firewalls to offer more robust protection against spoofed packets and unauthorized access.

C. Application-Layer Firewalls and Proxy Firewalls (Third-Generation)

Third-generation firewalls introduced

application-layer filtering, enabling inspection of traffic at the application level (Layer 7 of the OSI model). These application-layer firewalls, frequently implemented as proxy firewalls, function as intermediaries between users and destination servers. They can selectively block or allow traffic based on application-specific signatures, thereby offering enhanced control over the traffic that traverses the network.

D. Next-Generation Firewalls (NGFWs)

Next-generation firewalls (NGFWs) represent a notable advancement in firewall technology by incorporating advanced features such as deep packet inspection (DPI), intrusion prevention systems (IPS), and application awareness. These firewalls analyse traffic across multiple layers, merging the functionalities of traditional firewalls with more sophisticated tools designed for threat detection and prevention. Additionally, NGFWS leverage real-time threat intelligence, enabling them to identify emerging threats, including zero-day vulnerabilities

3. TYPES OF FIREWALLS

A. Packet filtering firewall

A packet-based firewall supervises incoming and outgoing network traffic, applying filters based on a predetermined set of rules that consider IP addresses, protocols, and ports. However, these firewalls do not analyse the payload for malicious content, which makes them vulnerable to threats at the application layer.

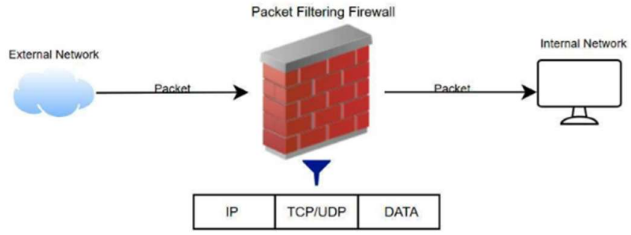

Figure 1

B. Stateful firewall

A Stateful firewall is an advanced version of a packet-filtering firewall. The term "stateful" signifies that it can monitor and maintain awareness of active sessions within the network. When a new connection is initiated, a SYN packet in the TCP flow establishes a session based on Layer 3 and Layer 4 information—namely, the IP address, protocol, and port number. The session is concluded either when a FIN packet is received or if the connection remains inactive for a specified duration.

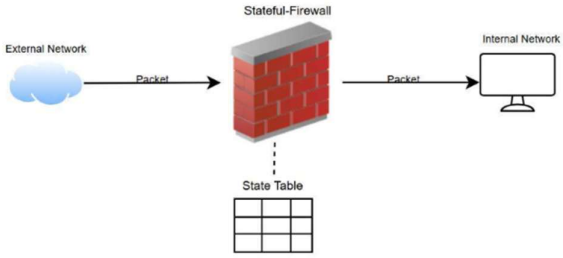

Figure 2

C. Application firewall (Proxy Firewalls)

An applicants firewall operates as an intermediary between users and the destination server, scrutinizing traffic at the application layer (Layer 7). Acting as a "gateway," it inspects incoming traffic at this specific level. When a client seeks to access the server's resources, the firewall functions as a reverse proxy. Although this added layer of security enhances protection, it can result in slower traffic speeds due to the additional processing requirements

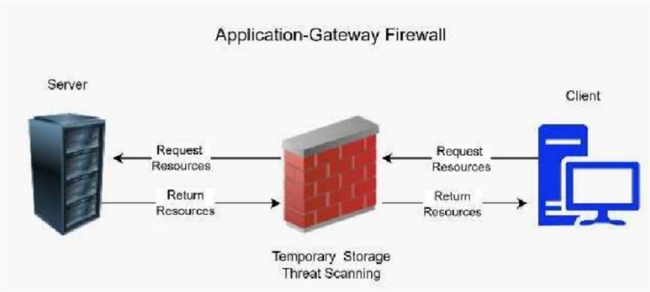

Figure 3

D. Circuit-Gateway firewall

A circuit gateway firewall operates similarly to an application gateway firewall, acting as a "gateway" between the client and the server. However, while an application gateway functions at layer 7, a circuit gateway firewall works at layer 5 (the session layer). It focuses on the connections established between the client and the server, rather than the server's network resources. It provides a proxy that creates a transparent connection, referred to as a virtual circuit, and relays TCP connections between the client and server. It ensures that the connections are valid and that the responses align with the requests, checking for mismatches that could indicate an attempt to exfiltrate data.

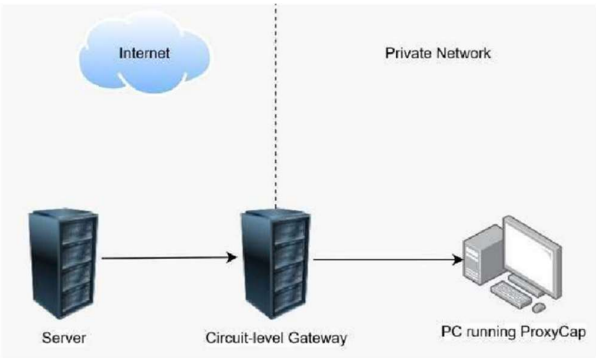

Figure 4

E. Web Application Firewall

A web application firewall (WAF) serves to protect web applications by acting as a security component within an application proxy device. It defends the back-end web server against various threats by meticulously inspecting HTTP and HTTPS request packets and analysing network traffic patterns. When a WAF identifies malicious packets or suspicious behaviours, it can block harmful HTTP requests or terminate the session. WAFs are particularly adept at countering well-documented web attacks, such as cross-site scripting (XSS), SQL injection, and distributed denial-of-service (DDoS)

attacks. However, they face challenges when it comes to unknown vulnerabilities commonly referred to as zero-day exploits, because their detection mechanism often depends on pattern recognition.

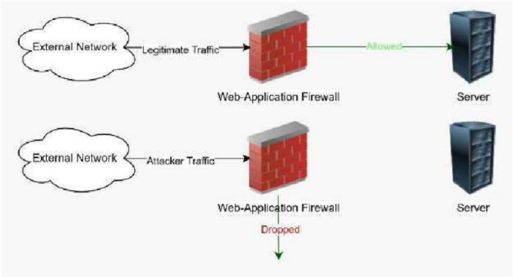

Figure 5

F. Unified Threat Management

Unified Threat Management (UTM) brings together various security features and services into a single device for a network. This approach makes it easier to manage IT security because it consolidates tools such as antivirus protection, content filtering, email and web filtering, and anti-spam capabilities. A single, user-friendly interface allows administrators to monitor all potential threats and security activities, simplifying management for the IT team.

G. SUMMARY

Each type of firewall offers distinct protection across various network layers. The selection of a firewall is contingent upon specific security requirements, necessitating a balance between the depth of inspection and performance demands. In contemporary networks, the deployment of multiple firewall types is often employed to establish a robust layered defence

4. NEXT-GENERATION FIREWALL

A. DEFINITION

Next-generation firewalls (NGFWs) and unified threat management (UTM) systems are advanced cybersecurity technologies that provide comprehensive protection by integrating multiple security tools into a single solution. This integration allows IT administrators to manage their networks more effectively, saving time and resources.

Though both serve comparable functions, NGFWs are more specialized in tackling specific threats, such as denial-of-service (DoS) attacks and insider threats. They typically offer advanced features, including robust intrusion prevention systems and enhanced visibility into application activities.

NGFWs address the shortcomings of traditional firewalls, which often allow threats to go undetected due to their reliance on basic packet inspection. In contrast, NGFWs employ deep packet inspection (DPI) and leverage machine learning algorithms to identify potential threats with greater efficacy.

B. Key Features

1. Application Awareness and Control

A defining feature of Next-Generation Firewalls (NGFWs) is their ability to identify and control applications with a high degree of granularity. Unlike traditional firewalls that operate based on ports and protocols, NGFWs use deep packet inspection and application-specific signatures to recognize applications regardless of their transmission method. This allows NGFWs to differentiate between casual web browsing and specific applications like social media platforms or video streaming services, thereby enhancing security and control over network usage. Organizations can enforce policies that permit business-critical applications while blocking or restricting recreational ones, enhancing productivity and security.

2. Integrated Intrusion Prevention System (IPS) NGFWs feature an advanced

Intrusion Prevention System (IPS) that continuously monitors network traffic for suspicious activities and known threats. The IPS uses techniques like signatured matching for recognized vernebilities and behaviour-based analysis to identify anomalous action. this function enables the firewall to detect and mitigate real time attack such as SQL injections, buffer overflow, and denial-of-services attempts. NGFWs offer seamless integration between firewall rules and threat detection mechanism, unlike standalone IPS system.

3. Deep Packet Inspection (DPI)

Traditional firewall typically examines only the header of data packets. In contrast, NGFWs use Deep Packet Inspection (DPI) to conduct a more thorough analysis of packet content. This enables them to detect and block malicious payloads, such as hidden malware, ransomware, or viruses, even within encrypted or compressed data streams. DPI provide robust protection against advanced threat disguised as legitimate traffic

4. SSL/TLS Traffic Inspection

Since most web traffic is now encrypted, NGFWs are crucial for inspecting temporarily decrypting the traffic, scanning it for malicious content, and then re-encrypting it before forwarding it to its destination. This process enforces security policies for encrypted communications, addressing blind spots traditional firewalls often overlook.

5. User Identity Integration

Next-Generation Firewalls (NGFWs) enhance policy enforcement by integrating with user identity services such as Active Directory, LDAP, and RADIUS. This capability allows administrators to establish access rules based on user identities rather than statics IP addressed. Permission can be allocated to employees according to their roles or departments, ensuring only authorized individual access sensitivity system or data. This identity-based approach improves both security and users accountability.

C. Benefits of Next-Generation Firewalls (NGFWs)

1. Performance

Next-Generation-Firewalls (NFGs) are designed to meet the demand of contemporary network without sacrificing speed or efficiency. Unlike traditional firewalls that may falter with advanced inspection, NGFWs use advanced hardware acceleration and optimized software algorithms to deliver high throughput, even during peak loads. While resource-intensive features like DPI and SSL/TLS decryption can be executed with minimal delay. They can also dynamically allocate bandwidth, prioritizing critical business applications, making them-suited for high speed, high-preformation network, especially in enterprises and cloud environments.

2. Security

Security is integral to NGFWs, offering more than basic protections. They incorporate advanced tools, such as In Intrusion Prevention Systems (IPS), malware detection, and real-time threat intelligence, to safeguard against a wide array of cyber threats. NGFWs are adept at countering sophisticated attacks, including Advanced Persistent Threats (APTs), ransomware, and zero-day exploits. Their ability to inspect encrypted traffic (SSL/TLS) is a standout feature, allowing them to decrypt, analyse, and re-encrypt packets to identify hidden threats and uphold privacy. Consolidating multiple layers of security within a single platform reduces vulnerabilities and helps organizations stay ahead of evolving threats.

3. Simplicity

Next-Generation-Firewalls (NFGs) make managing network security easier and more efficient through their comprehensive, all- in-one strategy. They integrate functions that historically required distinct solutions (firewalls, IPS, anti-malware, content filtering) into a single platform, reducing the complexity of managing multiple devices and software. They provide intuitive, centralized management interfaces for administrators to monitor network activity, configure policies, and update protocols from one dashboard. This centralization ensures policy consistency and lessens administrative burdens. NGFWs also enhance troubleshooting with extensive visibility into network traffic and user behaviour, aiding in swift issue resolution and minimizing downtime.

5. NEXT GENERATION FIREWALL VS TRADITIONAL FIREWALL

The distinctions between NGFWs and traditional firewalls are highlighted by comparing Fortinet's NGFW, FortiGate, with Cisco's traditional firewall, the Adaptive Security Appliance (ASA).

FortiGate: FortiGate NGFWs provide robust protection for data and users in hybrid environments. Equipped with patented Fortinet security processors, they enhance security and networking performance to manage increasing data demands. They are supported by FortiGuard AI-Powered Security Services, offering real-time defence against sophisticated cyber threats.

ASA: The Adaptive Security Appliance (ASA) is a traditional firewall solution that provides network security at the perimeter. Although Cisco has designated the Firepower Threat Défense (FTD) as the preferred security solution, ASAs remain available and supported.

A. Virtualization

Virtualization is a firewall feature that enables a single device to be partitioned into multiple independent firewalls, each with distinct zones, interfaces, policies, and access control lists

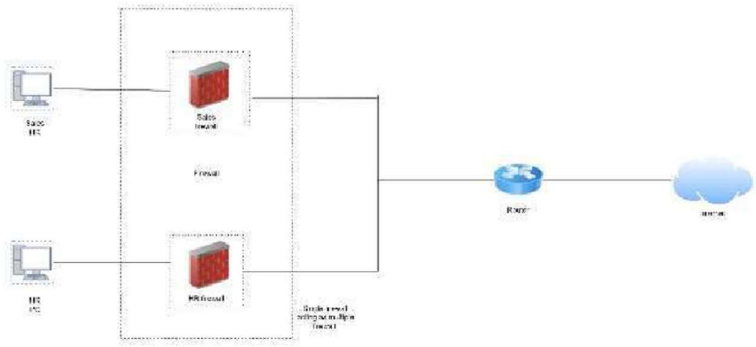

Figure 6

(ACLs). FortiGate: In FortiGate systems, Virtual Domains (VDOMs) partition a FortiGate device into two or more distinct virtual units that operate independently of one another.

ASA: In ASA technology, security contexts serve as a tool for partitioning a single ASA device into multiple independent virtual entities. This allows for distinct security policies and configurations tailored to different network segments, providing isolation and flexibility.

B. SSL/TLS inspection

SSL/TLS inspection involves intercepting connections secured by SSL/TLS that enter or leave an organization's network to analyse the traffic for malicious content.

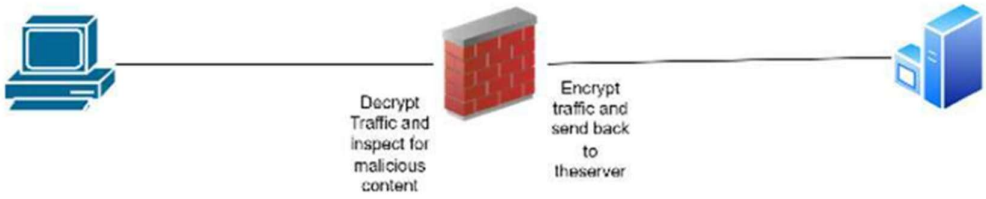

Figure 7

FortiGate: FortiGate offers native support for SSL/TLS inspection, which aids in identifying harmful traffic within secure communications (e.g., HTTPS). This feature can be used alongside other capabilities like Antivirus and IPS to detect malware and intrusion attempts.

ASA: The ASA itself does not support SSL/TLS inspection natively. It can be accomplished by installing the Firepower module, but this is not recommended due to the potential for up to90%

performance degradation. Additionally, the ASA does not support other Unified Threat Management (UTM) features such as antivirus and IPS.

C. Automation

Firewall automation uses software and tools to manage, configure, and monitor firewalls more effectively.

FortiGate: FortiGate supports RESTful APIs for system administration. APIs are increasingly popular for automating repetitive tasks and integrating FortiGate with other OEM products.

ASA: Newer ASA versions do not support APIs, and they are not available on higher-end hardware models.

6. CONCLUSION

Next-generation firewalls (NGFWs) represent a significant advancement in network security technology, delivering comprehensive protection for modern hybrid environments. This research paper provided a thorough examination of firewall technologies, tracing their evolution from traditional packet-filtering firewalls to the more advanced NGFWs.

The study explored various types of firewalls, including packet filtering, stateful inspection, application-layer firewalls, and next-generation firewalls, highlighting their key features, benefits, and limitations. Special attention was given to NGFWs, which integrate advanced capabilities such as deep packet inspection, intrusion prevention systems, and application awareness. These features enable NGFWs to analyse traffic across multiple layers, effectively merging traditional firewall functionalities with sophisticated threat detection and prevention tools.

Additionally, the paper presented a comparative analysis of Fortinet's FortiGate NGFW and Cisco's Adaptive Security Appliance (ASA), a traditional firewall solution. This comparison illustrates the enhanced capabilities of NGFWs in addressing contemporary cybersecurity challenges, particularly in areas such as virtualization, SSL/TLS inspection, and automation.

The research underscores the critical role of NGFWs in safeguarding hybrid environments and adeptly managing the growing volumes of data-intensive traffic and cloud-based applications. By harnessing real-time threat intelligence and AI-powered security services, NGFWs like FortiGate offer reliable, real-time protection against advanced threats, positioning them as vital components in modern network security strategies.

References

[1] J. Liang and Y. Kim, "Evolution of Firewalls: Toward Securer Network Using Next Generation Firewall," 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 2022, pp. 0752-0759, Doi: 10.1109/CCWC54503.2022.9720435.

[2] Beloin, Steven M., and William R. Cheswick. "Network firewalls." IEEE communications magazine 32, no. 9 (1994): 50-57. [3] Wack, John, Ken Cutler, and Jamie Pole. "Guidelines on firewalls and firewall policy." NIST special publication 800 (2002): 41.

[4] Alsaqour, Raed, Ahmed Motmi, and Maha Abdelhaq. "A systematic study of network firewall and its implementation." International Journal of Computer Science & Network Security 21, no. 4 (2021): 199 208.

[5] K. Salah, K. El Badawi and R. Bout Aba, "Performance Modelling and Analysis of Network Firewalls," in IEEE Transactions on Network and Service Management, vol. 9, no. 1, pp. 12-21, March 2012, Doi: 10.1109/TNSM.2011.122011.110151.

[6] Bringhenti, Daniele, Francesco Pizzato, Riccardo Sisto, and Fulvio Valenza. "Autonomous attack mitigation through firewall reconfiguration." INTERNATIONAL JOURNAL OF NETWORK MANAGEMENT (2024).A

[7] Patel, Udit. "THE ROLE OF NEXT-GENERATION FIREWALLS IN MODERN NETWORK SECURITY: COMPREHENSIVE ANALYSIS." INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN ENGINEERING AND TECHNOLOGY (IJARET) 15, no. 4 (2024): 135-154.

[8] BOUAZIZ, IMene. "Modern Firewall System and Al-Driven Intrusion Detection: Implementation and Evaluation." PhD diss., 2024.

[9] BOUAZIZ, IMene. "Next-Gen Cybersecurity: A Study on Al and Machine Learning for Enhanced Network Défense and Intrusion Detection." PhD diss., 2024.

[10] Cavusoglu, Huseyin, Srinivasan Raghunathan, and Hasan Cavusoglu. "Configuration of and interaction between information security technologies: The case of firewalls and intrusion detection systems." Information Systems Research 20, no. 2 (2009): 198-217.

[11] Bringhenti, Daniele, and Fulvio Valenza. "GreenShield: Optimizing Firewall Configuration for Sustainable Networks." IEEE Transactions on Network and Service Management (2024).

[12] Alicea, Michael, and Izzat Alsmadi. "Misconfiguration in firewalls and network

access controls: Literature review." Future Internet 13, no. 11 (2021): 283.

[13] Chopra, Aakanksha. "Security issues of firewall." Int. J. P2P Newt. Trends Techno 22, no. 1 (2016): 49.

[14] Gupta, Namit, Aakash Saikia, and D. Sanghi. "Web application firewall" Indian Institute of Technology, Kanpur 61 (2007): 62.

[15] Cruz, Luis. "What Is Unified Threat Management (UTM)?" Study.com https://study.com/academy/lesson/what-is-unified-threat-management utm.html

[16] Agham, Vinit. "Unified threat management" International Research Journal of Engineering and Technology 3, no. 4 (2016): 32-36.

[17] "The Evolution of Internet Security." Preferred IT Group, https://www.preferreditgroup.com/2018/05/11/the-evolution-of-internet security/LLC.

[18] Matt Keil September 8, Matt Keil, and Matt Keil. "Balancing the Risks and Benefits of Evasive Applications." Palo Alto Networks Blog, September 8, 2009. https://www.paloaltonetworks.com/blog/2009/09/controlling-evasive applications/

[19] "App-ID Technology Brief Palo Alto Networks." Accessed November 13, 2021. https://media.paloaltonetworks.com/docume nets/tech brief-app id.pdf

[20] Amos, Jesse Daniel. "7 Layers of Cybersecurity Threats in the ISO-OSI Model." Computer Learning Courses - Online & In Person Training. Accessed November 13, https://training.nhlearninggroup.com/blog/7-2021. layers-of-cybersecurity threats-in-the-iso-soy-model

[21] Koch, Robert. "Towards next-generation intrusion detection." In 2011 3rd International Conference on Cyber Conflict, pp. 1-18. IEEE, 2011.