CanDis
Canadian Journal of Discovery

Open Access

Performance Evaluation of Firewall Technologies

Dr.Eng. Jouma Ali Al-Mohamad✉

Faculty member at Al-Shahbaa Private University, Aleppo, Syria

✉*Corresponding author:*
Email: jalmohamad@su.edu.sy

Article History
Received: 22 December 2024; Revised: 23 December 2024; Accepted: 24 december 2024; E-publication: 26 December 2024
Academic Editor: Nambukara Wasam Wakwella Gamage Kumesh

Abstract

The document evaluates both traditional firewalls and next-generation firewalls (NGFWs), highlighting NGFWs' advanced capabilities, such as application awareness, intrusion prevention, deep packet inspection, and real-time threat intelligence. It also provides an in-depth comparison between specific products, such as Check Point and Palo Alto NGFWs, based on their performance, deployment options, and cost.

Keywords:
Firewall Technologies, Next-Generation Firewalls (NGFWs), Traditional Firewalls, Cybersecurity, Deep Packet Inspection, Intrusion Prevention, Check Point, Palo Alto, Network Security, Performance Comparison.

Introduction

Firewalls are essential for safeguarding network security by acting as barriers between trusted internal networks and potentially untrusted external networks, such as the internet. Their primary function is to control and monitor incoming and outgoing network traffic based on established security rules, ensuring that only legitimate traffic is permitted. This study explores traditional firewalls and next-generation firewalls (NGFWs), comparing their functionalities, strengths, and limitations in meeting modern cybersecurity demands.

1.Introduction and Purpose of Firewalls

The primary purpose of a firewall is to act as a barrier between a trusted internal network and potentially untrusted external networks, such as the internet, to protect systems and data from unauthorized access and cyber threats. Firewalls monitor and control incoming and outgoing network traffic based on predetermined security rules, ensuring that only legitimate traffic is allowed through.

While all firewalls share the same fundamental objective of protecting networks and systems, their features, capabilities, and levels of sophistication can differ greatly. Some firewalls offer basic filtering based on IP addresses or ports, while others provide more advanced functionalities, such as deep packet inspection, intrusion detection, and real-time traffic analysis. Additionally, modern firewalls may incorporate machine learning algorithms to detect and adapt to emerging threats, thereby enhancing security measures. The complexity and deployment strategy of a firewall often depend on the specific needs and security posture of the organization.

Firewalls also play a crucial role in maintaining compliance with regulatory requirements, such as data protection laws, by preventing unauthorized access to sensitive data. Furthermore, firewalls can provide visibility into network activities, enabling administrators to track and log access attempts, which aids in both real-time security monitoring and forensic analysis.

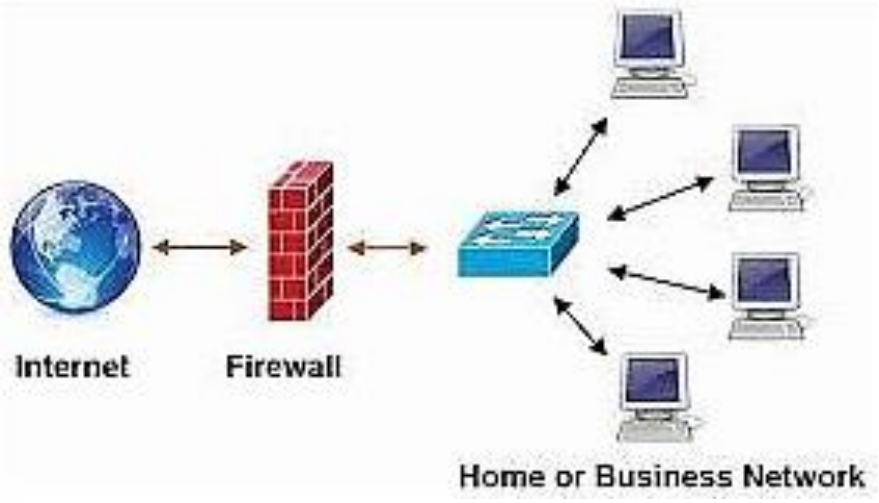

Figure 1

2. Literature Review

The evolution of firewall technologies reflects an ongoing need to address the increasing sophistication of cyber threats. Early studies focused on traditional firewalls, which operated primarily at the network and transport layers of the OSI model, with limited capabilities such as packet filtering based on IP addresses and port numbers. However, as applications became more complex and attackers began to exploit vulnerabilities at the application layer, traditional firewalls were deemed insufficient for comprehensive network security (Stallings, 2018; Gollmann, 2011).

To bridge this security gap, Next-Generation Firewalls (NGFWs) emerged, integrating traditional firewall capabilities with additional features such as Deep Packet Inspection (DPI), Intrusion Prevention Systems (IPS), and application-level awareness (Shackleford, 2013). NGFWs aim to provide a more comprehensive defense by examining data packets beyond the header, allowing for the detection and blocking of advanced threats embedded in the payload (Easttom, 2019).

Numerous comparative studies have analyzed the effectiveness of NGFWs versus traditional firewalls, with particular emphasis on security performance, adaptability, and cost-effectiveness. For instance, Check Point and Palo Alto NGFWs have been evaluated in terms of their security features, with findings indicating that Palo Alto offers high throughput and extensive application tracking, while Check Point excels in policy flexibility and granular control (NSS Labs, 2021; Cisco, 2021). These studies

OPEN ACCESS I Canadian Journal of Discovery I August 2024, 5(12), 1-22, doi: https://doi.org/10.5281/zenodo.14674409

highlight the adaptability of NGFWs to enterprise environments, particularly in handling high data flows and securing cloud-based architectures (Fortinet, 2021).

Overall, the literature underscores the critical role NGFWs play in modern cybersecurity, emphasizing the need for continuous updates, integrated threat intelligence, and adaptable policy management to combat evolving threats in diverse network environments.

3. Methodology and Comparative Analysis

This study employs a comparative analysis approach using carefully selected criteria to evaluate NGFWs, specifically Check Point and Palo Alto products. These criteria include security performance, deployment flexibility across multiple environments, and cost efficiency. Data was collected from empirical test results, independent reports, and user reviews from enterprises that have adopted these security solutions. This methodology enables a better understanding of product performance in practical environments.

4. Categories of Firewalls

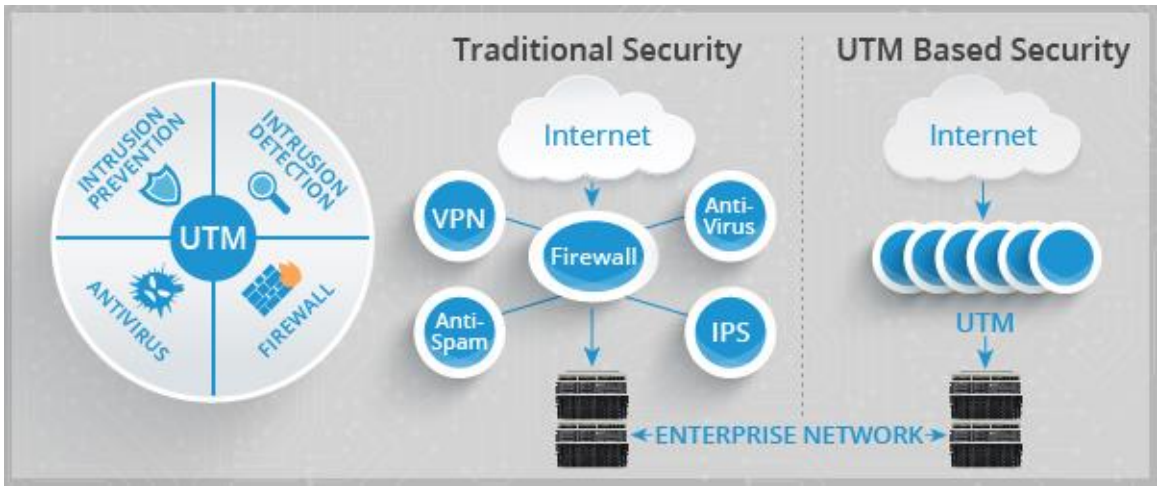

Figure 2

Firewalls can be broadly categorized based on their functionalities, sophistication, and the types of threats they are designed to handle. Here, we explore two primary categories: Traditional Firewalls and Next-Generation Firewalls (NGFWs).

4.1 Traditional Firewalls

Traditional firewalls, also known as first-generation or packet-filtering firewalls, are the earliest type of network defense. They function primarily at the **network layer** of the OSI model and are designed to control data flow between networks based on specific criteria, such as IP addresses, protocols, and ports.

4.1.1 Key Features and Functions:

- **Packet Filtering:** Traditional firewalls inspect packet headers and apply filtering rules to allow or deny packets based on criteria such as source and destination IP addresses, protocols, and port numbers.

OPEN ACCESS I Canadian Journal of Discovery I August 2024, 5(12), 1-22, doi: https://doi.org/10.5281/zenodo.14674409

- **Stateless and Stateful Inspection:** Some traditional firewalls use **stateless inspection**, where each packet is analyzed independently of any previous network activity. In contrast, **stateful firewalls** track active connections and can make more context-aware decisions about packet handling.
- **Basic Access Control Lists (ACLs):** Traditional firewalls typically use simple access control lists (ACLs) to set network rules, which helps limit access to network resources based on IP addresses and port numbers.

Limitations of Traditional Firewalls: While effective for basic traffic filtering, traditional firewalls struggle to handle complex, modern threats such as **malware** or **zero-day attacks**. They are also less effective against **application-layer threats**, as they lack the ability to inspect data within application packets or monitor encrypted traffic [1][2].

Traditional Firewall (Layer 3/4)

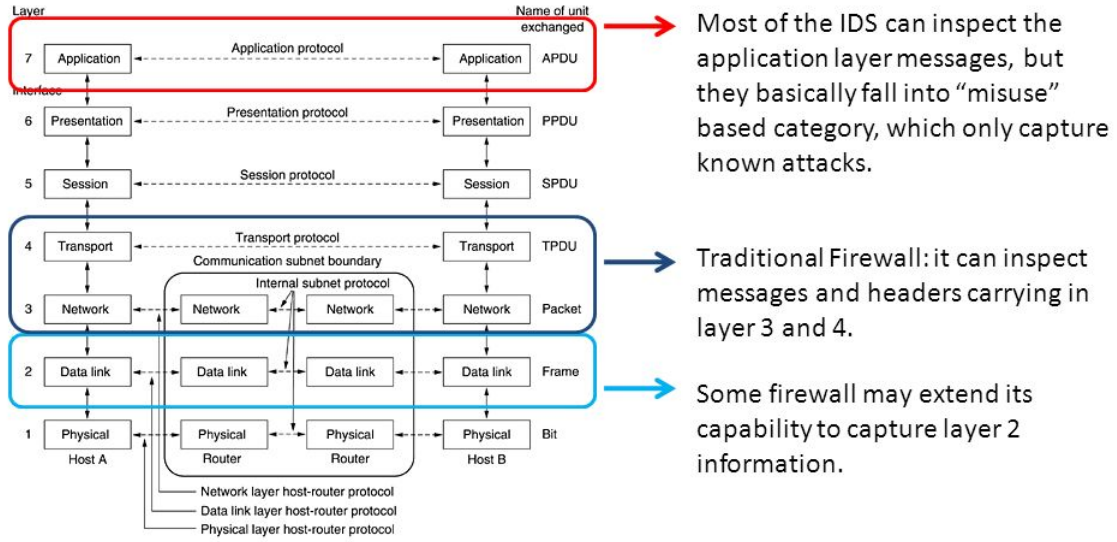

Figure 3

A traditional firewall is primarily designed to regulate the flow of network traffic based on parameters such as port numbers, protocols, source IP addresses, and destination IP addresses. Acting as a gatekeeper, the traditional firewall examines data packet headers to decide whether to permit or deny traffic, thus enforcing basic security policies at the network perimeter.

When we refer to "traditional" firewall features, we are discussing the foundational functionalities that emerged prior to the development of **Next-Generation Firewalls (NGFWs)**. Traditional firewalls focus on basic traffic filtering and are limited to operating at the **network** and **transport layers** of the OSI model. These firewalls are effective for straightforward network security tasks but lack advanced capabilities like deep packet inspection or application awareness, which are hallmarks of NGFWs.

4.1.2 Core Features of Traditional Firewalls

1. **Packet Filtering**: Traditional firewalls analyze packet headers to apply simple allow-or-deny rules based on specific attributes, such as IP addresses, protocol types, and port numbers. This packet filtering ensures that only permitted types of traffic enter or leave the network.

OPEN ACCESS I Canadian Journal of Discovery I August 2024, 5(12), 1-22, doi: https://doi.org/10.5281/zenodo.14674409

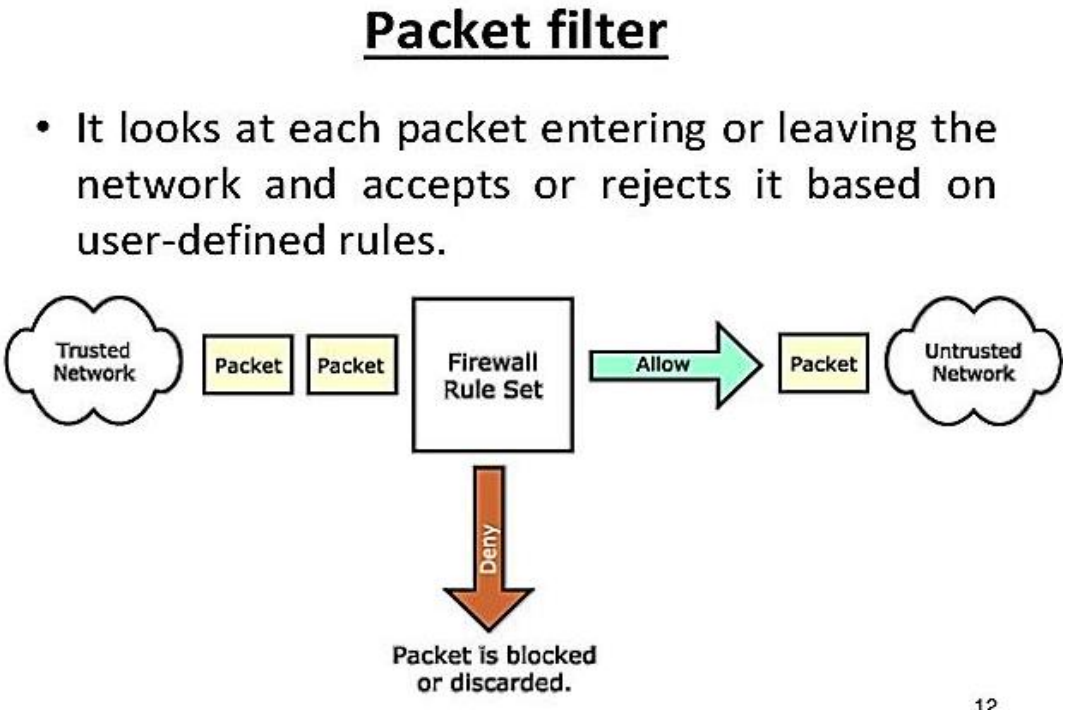

Figure 4

2. **Stateful Inspection**: Many traditional firewalls utilize **stateful inspection**, which allows them to monitor the state of active connections. By tracking sessions and retaining data about each connection, stateful firewalls can make more informed decisions and identify potentially unauthorized traffic that may not align with ongoing sessions.
3. **Access Control Lists (ACLs)**: Traditional firewalls rely heavily on **Access Control Lists (ACLs)**, which are predefined rules that determine which traffic is allowed or blocked. ACLs enable administrators to manage access to network resources by defining which IP addresses, ports, and protocols are acceptable.
4. **Network Address Translation (NAT)**: Traditional firewalls often include **NAT capabilities** that help to mask internal IP addresses. NAT not only conserves public IP addresses but also adds a layer of security by hiding the internal network structure from external entities.

4.1.3 Limitations of Traditional Firewalls

While traditional firewalls provide essential perimeter defense, they are less effective against modern threats, such as advanced malware, application-layer attacks, or encrypted traffic. They lack the application-layer visibility and sophisticated threat detection capabilities found in Next-Generation Firewalls [5][6].

Next-Generation Firewalls (NGFWs)

4.2 Next-Generation Firewalls (NGFWs)

OPEN ACCESS I Canadian Journal of Discovery I August 2024, 5(12), 1-22, doi: https://doi.org/10.5281/zenodo.14674409

Figure 5

Next-Generation Firewalls (NGFWs) represent a more advanced approach to network security, integrating traditional firewall functions with additional, sophisticated features to protect against modern and complex threats. Unlike traditional firewalls, NGFWs operate at multiple layers of the OSI model, offering not only network-layer protection but also visibility and control over **application-layer traffic**.

Key Features and Functions:

- **Deep Packet Inspection (DPI):** NGFWs analyze packet payloads as well as headers, allowing for better detection of malicious content embedded within data packets, even if they bypass traditional filtering rules.
- **Intrusion Prevention System (IPS):** Many NGFWs include an integrated **Intrusion Prevention System (IPS)**, which actively monitors network traffic to detect and block attacks like SQL injection, cross-site scripting, and buffer overflows.
- **Application Awareness and Control:** NGFWs can recognize and manage traffic from specific applications (e.g., Facebook, Dropbox) rather than just network ports. This allows for more granular security policies based on application type, enabling organizations to block high-risk applications or limit their functionality.
- **Threat Intelligence and Sandboxing:** Many NGFWs utilize threat intelligence services to identify and block known threats and employ **sandboxing** techniques to analyze potentially harmful files in a secure, isolated environment before they are allowed onto the network.
- **SSL/TLS Decryption:** NGFWs can decrypt SSL/TLS traffic, enabling security checks on encrypted data flows, which are increasingly common in today's networks.

Benefits of NGFWs: Next-Generation Firewalls provide a comprehensive defense mechanism by combining network security with real-time monitoring and threat intelligence. This hybrid approach allows organizations to respond quickly to evolving cyber threats, making NGFWs an essential tool for any modern cybersecurity strategy [3][4].

OPEN ACCESS I Canadian Journal of Discovery I August 2024, 5(12), 1-22, doi: https://doi.org/10.5281/zenodo.14674409

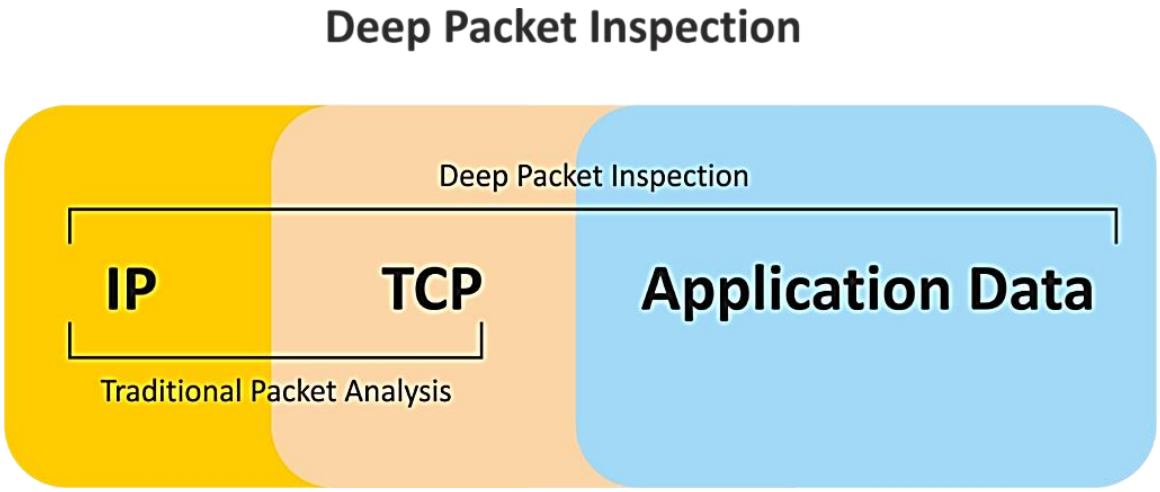

Figure 6

4.2.1 Key Features of Next-Generation Firewalls (NGFWs):

- **Application Awareness**: NGFWs can identify and monitor specific applications within network traffic, allowing for precise control and enhanced security at the application level.
- **Intrusion Prevention System (IPS)**: Integrated IPS capabilities enable NGFWs to detect and prevent malicious activities, including attacks like SQL injection, cross-site scripting, and other threats targeting vulnerabilities.
- **Deep Packet Inspection (DPI)**: DPI allows NGFWs to analyze the content of data packets, rather than just the headers, to detect and block threats embedded within packet payloads.
- **Enhanced Visibility and Control**: NGFWs provide administrators with detailed insights into network activity, enabling more effective monitoring, policy enforcement, and traffic management.
- **Simplified Management**: NGFWs consolidate multiple security functions into a single platform, reducing administrative complexity and streamlining security management.
- **Real-Time Traffic Inspection**: NGFWs can inspect traffic in real-time, allowing them to block suspicious or harmful data flows as they occur, enhancing overall network security.
- **Lower Total Cost of Ownership (TCO)**: By integrating multiple security features into one device, NGFWs reduce the need for separate security solutions, which can lower both operational and maintenance costs [7][8].

5. Similarities Between Traditional Firewalls and Next-Generation Firewalls (NGFWs)

Despite their differences, both **Traditional Firewalls** and **Next-Generation Firewalls (NGFWs)** share several core features that provide foundational network security capabilities:

- **Static Packet Filtering**: Both types of firewalls can perform static packet filtering, which blocks or allows packets at network interfaces based on protocols, ports, or IP addresses. This feature forms the basis of traffic control in both firewall types.
- **Stateful Inspection (Dynamic Packet Filtering)**: Both firewalls support stateful inspection, which monitors and validates active connections across each firewall interface. This feature enables both traditional and NGFWs to track session states and prevent unauthorized traffic from gaining access.

OPEN ACCESS I Canadian Journal of Discovery I August 2024, 5(12), 1-22, doi: https://doi.org/10.5281/zenodo.14674409

- **Network Address Translation (NAT)**: Both firewalls offer NAT capabilities, which re-map IP addresses within packet headers. This process not only conserves IP addresses but also provides a layer of protection by masking internal network structures.
- **Port Address Translation (PAT)**: Both traditional firewalls and NGFWs support PAT, allowing multiple devices on a Local Area Network (LAN) to share a single public IP address, simplifying network management and enhancing security.
- **Virtual Private Network (VPN) Support**: Both types of firewalls can support VPNs, enabling secure remote access to networks through encrypted connections. This is essential for remote work and secure data transmission over public networks[9][10][11].

Figure 7

6. Differences Between Traditional Firewalls and Next-Generation Firewalls (NGFWs)

While Traditional Firewalls and Next-Generation Firewalls (NGFWs) share basic functionality, NGFWs offer several advanced features that make them better suited for addressing today's complex security challenges:

- **Integrated Signature-Based Intrusion Prevention System (IPS)**: NGFWs include an IPS that detects and blocks known threats using signature-based detection. Traditional firewalls typically lack this feature, limiting their ability to protect against sophisticated attacks.
- **Application Identification**: NGFWs are capable of identifying applications by using pre-defined signatures, payload analysis, and header inspection. This application awareness enables NGFWs to monitor and control traffic based on specific applications rather than simply by IP address or port.
- **Full-Stack Visibility**: Unlike traditional firewalls, which operate mainly at the network and transport layers, NGFWs provide full-stack visibility, allowing them to inspect traffic at the application layer and beyond. This in-depth analysis offers greater insight into network activity and enables more precise traffic management.
- **Granular Control of Applications**: NGFWs allow administrators to set detailed controls for specific applications, providing extremely fine-tuned management over how applications are used within

OPEN ACCESS I Canadian Journal of Discovery I August 2024, 5(12), 1-22, doi: https://doi.org/10.5281/zenodo.14674409

the network. Traditional firewalls lack this level of granularity, as they operate with broader, less flexible rules.

- **SSL/TLS Decryption**: NGFWs can decrypt SSL/TLS-encrypted traffic, which allows them to inspect and identify potentially harmful applications or data within encrypted streams. This capability is crucial for detecting threats in encrypted traffic, which traditional firewalls cannot analyze.
- **Upgrade Path for Emerging Threats**: NGFWs are designed to be updated with new security features and information feeds, allowing them to adapt to emerging threats. Traditional firewalls, in contrast, lack the ability to dynamically integrate new threat intelligence, making them less adaptable to evolving cyber risks. [12][13][14]

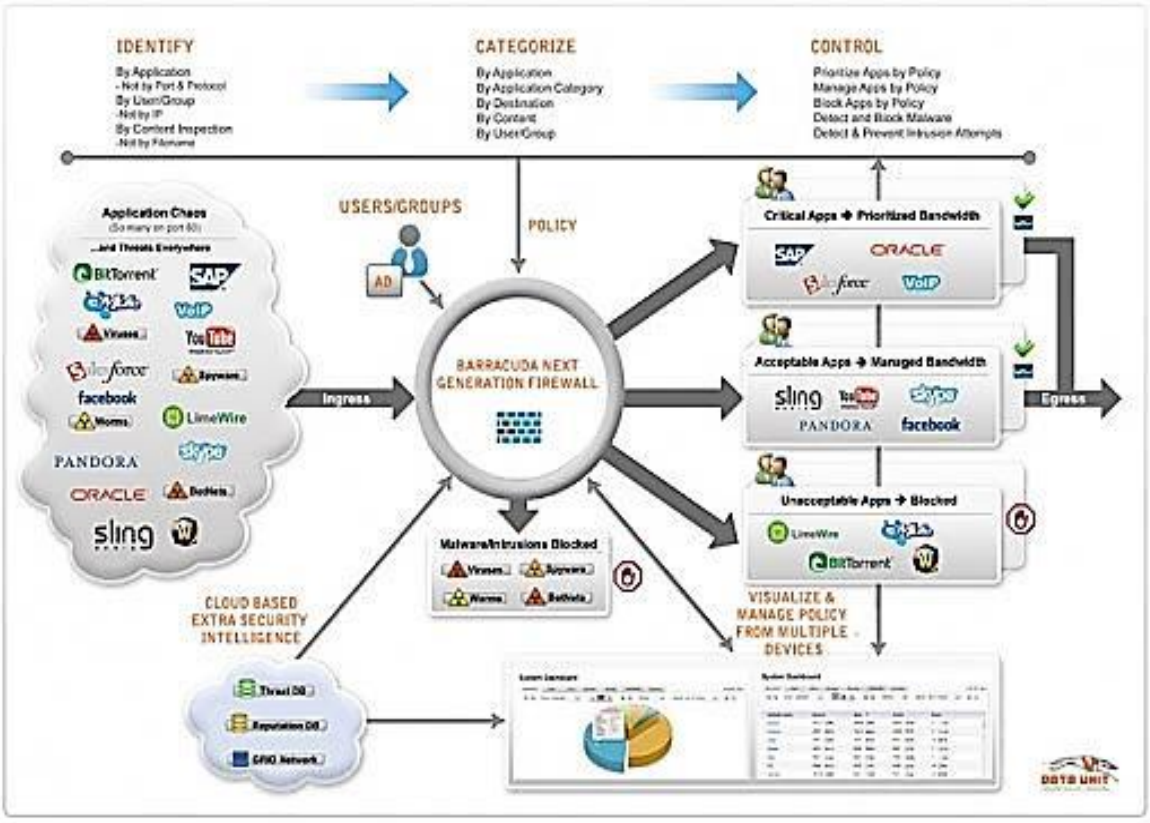

Figure 8

Side By Side Comparison Different Vendors:

OPEN ACCESS I Canadian Journal of Discovery I August 2024, 5(12), 1-22, doi: https://doi.org/10.5281/zenodo.14674409

	Cisco FirePOWER 8350	CheckPoint 13500	Fortinet FortiGate-3600C	WatchGuard XTM1525	Dell SonicWALL SuperMassive E10800
Server Application Attacks (Blocked %)	99.50%	97.10%	97.00%	96.70%	96.40%
Client Application Attacks (Blocked %)	99%	95.90%	91.80%	98.70%	99.10%
IPS Throughput (Specification)	15 Gbps	5.7 Gbps	15 Gbps	13 Gbps	28 Gbps
IPS Throughput (Tested)	18.7 Gbps	6.7 Gbps	9.6 Gbps	3.4 Gbps	16.4 Gbps
Total Throughput	30 Gbps	23.6 Gbps	60 Gbps	25 Gbps	40 Gbps
Cost per Protected Mbps	$20.03	$21.45	$8.30	$11.87	$15.46
Max Power Consumption	635-1000 Watts	431 Watts	615 Watts	130 Watts	750 Watts
Stackable	Yes (Up to 4)	No	No	No	No
Rack Space Used per unit	2U	2U	3U	1U	4U

Figure 9

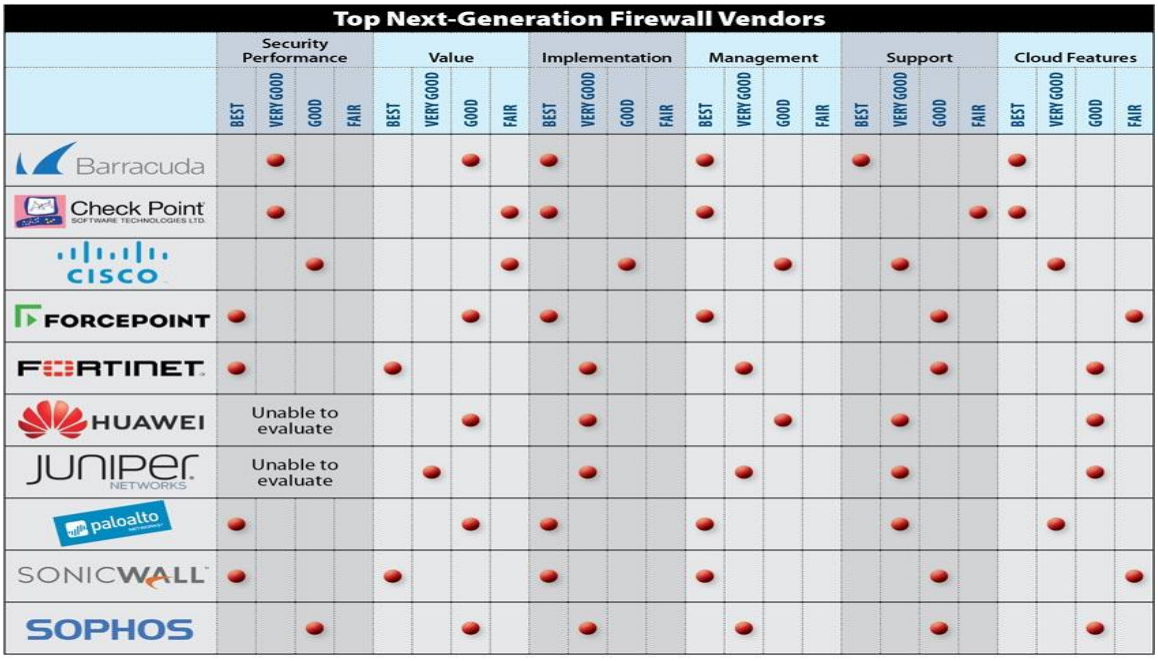

Figure 10

7. Check Point Firewall vs. Palo Alto Firewall

7.1 Check Point Product Highlights

OPEN ACCESS I Canadian Journal of Discovery I August 2024, 5(12), 1-22, doi: https://doi.org/10.5281/zenodo.14674409

Overview: Check Point's Next-Generation Firewalls (NGFWs) use an extensive application library with over 6,600 web applications. This enables them to identify, permit, restrict, or block applications and specific application features, ensuring safe internet usage while defending against threats and malware. Check Point's **SmartLog** analyzer offers real-time visibility into billions of log records across different time periods and domains, providing administrators with detailed insights for improved security management.

Recent Developments: Check Point recently expanded its NGFW lineup by introducing new high-end platforms and launched the **Check Point Infinity** security architecture. This comprehensive framework is designed to secure a company's entire IT infrastructure, from the data center to remote endpoints, delivering a unified solution for threat prevention, visibility, and policy enforcement.

7.2 Palo Alto Product Highlights

Overview: Palo Alto Networks' NGFWs offer advanced monitoring of applications, threats, and content, linking activity to specific users, regardless of location or device type. Their NGFWs are available as hardware appliances (from the PA-200 to the high-performance PA-7000 Series, which can achieve threat prevention throughput of up to 100 Gbps) and as virtual appliances, supporting cloud environments like AWS and Azure, thus providing a flexible deployment model for a wide range of use cases.

Recent Developments: Palo Alto recently released version 8.1 of its **PAN-OS** operating system, adding more than 60 new features. Key improvements include enhanced **SSL decryption capabilities**, allowing deeper inspection of encrypted traffic, and more detailed controls for **SaaS applications**. These updates reflect Palo Alto's commitment to providing more granular application control and stronger data protection in cloud-based environments.

Summary of Key Differences

- **Application Library**: Check Point leverages a library with over 6,600 applications, while Palo Alto focuses on deep user-based tracking for applications and threats across devices and locations.
- **Architecture**: Check Point's Infinity architecture offers end-to-end security for enterprise IT environments, while Palo Alto's PAN-OS provides extensive support for SaaS applications and advanced SSL decryption.
- **Deployment Options**: Both companies offer flexible deployment options, but Palo Alto is particularly known for its high-throughput hardware appliances and robust support for virtualized and cloud environments[15][16].

8. NGFW Product Ratings: Palo Alto vs. Check Point

- **Security Performance**

Both Palo Alto and Check Point excel in security performance. In recent **NSS Labs** tests, **Palo Alto's PA-5220** received a security effectiveness rating of 98.7%, while the **Check Point 15600** achieved a higher rating, blocking 99.6% of attacks. Both products provide robust protection against known and emerging threats, making them leaders in the NGFW market for security performance.

- **Performance**

In terms of throughput, Palo Alto's PA-5220 was rated the top performer among tested firewalls, with an impressive speed of **7,888 Mbps**. Check Point's 15600 model followed closely with a solid **6,034**

OPEN ACCESS I Canadian Journal of Discovery I August 2024, 5(12), 1-22, doi: https://doi.org/10.5281/zenodo.14674409

Mbps. These high throughput ratings make both products suitable for enterprises with high-speed requirements.

- **Value**

Both Check Point and Palo Alto firewalls are premium options with higher price points than most NGFWs. Organizations considering these firewalls typically prioritize advanced security features and performance over cost, given the added value both systems bring to enterprise environments.

- **Implementation and Management**

Users report that both firewalls require more technical expertise and planning during setup than many other NGFW solutions. Once operational, **Check Point's management interface** is often praised for its usability and effectiveness in policy management. **Palo Alto's management features** are also highly rated, though some users note that **Panorama**, its centralized management solution, may experience performance issues when handling a large fleet of appliances.

- **Support**

Check Point has received some customer complaints regarding the responsiveness of its support services. Both vendors face feedback from customers about their infrequent firmware updates, which, though generally beneficial, can introduce stability issues.

- **Cloud Features**

Both Check Point and Palo Alto offer strong cloud support, providing **virtual appliances** and a comprehensive set of features for cloud environments. These capabilities make them well-suited for businesses migrating to or operating within cloud infrastructures, including hybrid and multi-cloud setups.[17]

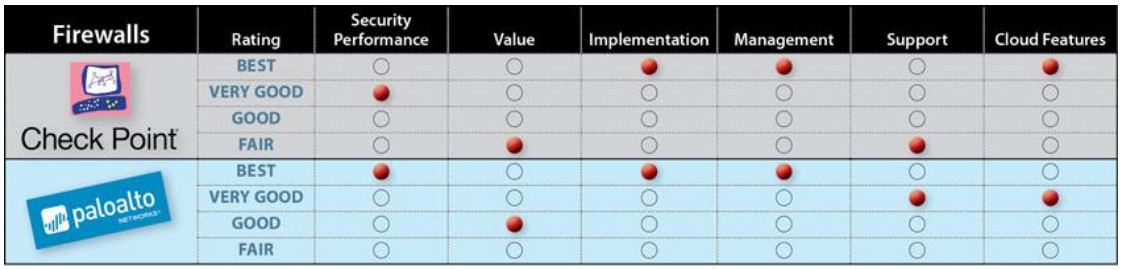

Figure 11

9. Deployment Options: Check Point vs. Palo Alto

Check Point

Deployment Flexibility: Check Point offers its NGFW products in several forms to accommodate diverse deployment needs:

- **Hardware Appliances**: Check Point provides physical NGFW devices designed for various enterprise requirements, ensuring high performance and reliability.
- **Software-Only Solutions**: For organizations seeking more customization, Check Point offers software-only solutions that can be deployed on compatible hardware.
- **Cloud Services**: Check Point's cloud-based NGFWs are available as part of its robust cloud security portfolio, suitable for securing hybrid and multi-cloud environments.

OPEN ACCESS I Canadian Journal of Discovery I August 2024, 5(12), 1-22, doi: https://doi.org/10.5281/zenodo.14674409

- **Managed Services**: For enterprises seeking to outsource security management, Check Point provides managed services that oversee firewall operations, updates, and incident response.

Palo Alto

Deployment Flexibility: Palo Alto's NGFWs are available across multiple environments to support a wide range of enterprise infrastructures:

- **Hardware Appliances (PA Series)**: The PA Series offers physical devices with high throughput, designed to support various deployment scales, from branch offices to data centers.
- **Virtual Appliances (VM Series)**: Palo Alto's VM Series is built for deployment in virtualized environments and is compatible with major cloud platforms. These virtual firewalls support seamless integration into cloud and hybrid infrastructures, making them ideal for organizations with flexible or distributed environments.

10. Pricing: Check Point vs. Palo Alto

Check Point

Pricing Structure: Check Point's pricing depends on the configuration of servers and security gateways required.

- **Entry-Level Options**: Check Point's NGFW pricing starts around **$799** for a single gateway, making it accessible for smaller deployments.
- **Management Appliances**: For larger deployments, the **Smart-1 405** management appliance starts at **$7,500**, offering centralized management capabilities.
- **High-End Models**: The Check Point 15600 model, tested by NSS Labs, is priced at approximately **$70,000**, reflecting its performance capabilities for larger enterprise environments.

Palo Alto

Pricing Structure: Palo Alto Networks provides a broad range of NGFW options tailored to different organizational needs.

- **Entry-Level and Ruggedized Models**: The **PA-220** starts at around **$1,000**, suitable for small offices or branch locations, with 100 Mbps VPN throughput and capacity for 64,000 sessions. The ruggedized **PA-220R** offers enhanced durability for industrial environments.
- **Mid- to High-End Models**: The PA-3200 Series and PA-5280 range in price from **$2,900** to **$200,000**, with features suitable for more intensive environments. The PA-5280 provides up to 24 Gbps VPN throughput and supports 64 million sessions.
- **Enterprise Models**: The PA-5220, tested by NSS Labs, is available at around **$70,000**, plus additional costs for support packages, offering a balance of price and high performance.

OPEN ACCESS I Canadian Journal of Discovery I August 2024, 5(12), 1-22, doi: https://doi.org/10.5281/zenodo.14674409

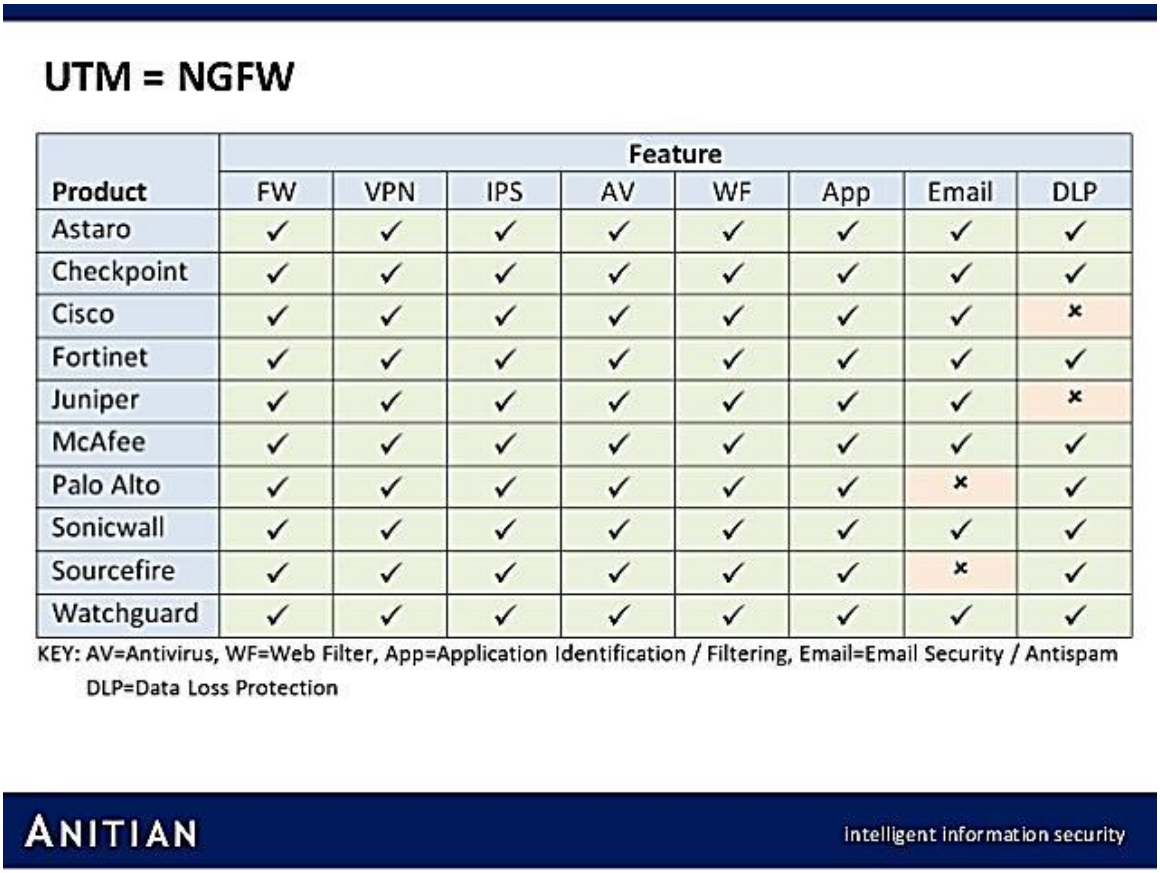

Figure 12

11. Comparison of Next-Generation Firewalls (NGFWs)

- **Cisco FirePOWER 8350**

The **Cisco FirePOWER 8350** is part of Cisco's portfolio after its acquisition of Sourcefire. It represents an entry-level model in the FirePOWER 8300 series, with other higher-tier models including the 8360, 8370, and 8390. Additionally, Cisco offers other lower-end series such as the 8100 and 8200 appliances, as well as its legacy Adaptive Security Appliance (ASA) line. Although Cisco has yet to fully integrate the FirePOWER line into its broader security offerings, both FirePOWER and ASA lines remain available as separate solutions for now.

The **FirePOWER 8350** is a versatile device capable of operating as a Next-Generation Firewall (NGFW), a Next-Generation Intrusion Prevention System (NGIPS), or an Advanced Malware Protection (AMP) solution. These functions can be deployed individually or concurrently, depending on the specific security requirements of the organization [18][19].

Key Specifications:

- **Server Application Attacks Blocked:** 99.5%
- **Client Application Attacks Blocked:** 99%
- **Evasion Resistance:** The 8350 model is highly resistant to evasion techniques, making it robust against sophisticated attacks.
- **Stability and Reliability:** The 8350 is known for its stability and reliability in operational environments.

OPEN ACCESS I Canadian Journal of Discovery I August 2024, 5(12), 1-22, doi: https://doi.org/10.5281/zenodo.14674409

- **Enforcement of Application Policies:** Successful enforcement of application policies, ensuring secure and controlled application traffic.
- **Enforcement of Identity Policies:** Efficient enforcement of identity-based policies, which is critical for managing access controls.
- **IPS Throughput (Specification):** 15 Gbps
- **IPS Throughput (Tested):** 18.7 Gbps, indicating strong performance under real-world conditions.
- **Total Throughput:** 30 Gbps, demonstrating a high capacity for processing network traffic.
- **Cost per Protected Mbps:** $20.03, offering competitive value for each unit of throughput protection.
- **Dual Power Supplies:** Yes, ensuring redundancy for improved system uptime.
- **Maximum Power Consumption:** Ranges between 635-1000 Watts, though the exact value is not specified in the datasheet.
- **Stackable Configuration:** Yes, allowing up to four units to be stacked for scalability.
- **Rack Space Usage:** 2U, meaning it occupies two rack units of space in a standard server rack.

➢ **Check Point 13500: A Next-Generation Firewall Solution**

The **Check Point 13500** is part of Check Point's **13000 series** of appliances, renowned for its advanced security features and deployment versatility. Check Point has established itself as a leading provider of security solutions, and its firewalls are among the most widely deployed in global enterprise networks today.

The **13000 series** can be configured for various roles, including a Next-Generation Firewall (NGFW), Next Generation Threat Prevention (NGTP), Next Generation Secure Web Gateway (NGSWG), and Next Generation Data Protection (NGDP). The series includes models such as the **13500** and **13800**, with the option to use specific blade packages to tailor the device's functionality. For even larger scale deployments, Check Point offers the **41000** and **61000** series, which are designed for high-capacity data centers and service provider environments.

Key Specifications:

- **Server Application Attacks Blocked:** 97.1%
- **Client Application Attacks Blocked:** 95.9%
- **Evasion Resistance:** The 13500 model is designed to be highly resistant to evasion techniques, ensuring that it can effectively block sophisticated attacks.
- **Stability and Reliability:** Known for robust and dependable performance, making it suitable for large-scale enterprise deployments.
- **Enforcement of Application Policies:** Successfully enforces application policies, ensuring security across network applications.
- **Enforcement of Identity Policies:** Efficiently enforces identity-based access controls, which is critical for securing access to network resources.
- **IPS Throughput (Specification):** 5.7 Gbps

OPEN ACCESS I Canadian Journal of Discovery I August 2024, 5(12), 1-22, doi: https://doi.org/10.5281/zenodo.14674409

- **IPS Throughput (Tested):** 6.7 Gbps, which demonstrates strong real-world performance under varying network loads.
- **Total Throughput:** 23.6 Gbps, offering significant capacity for handling enterprise-level network traffic.
- **Cost per Protected Mbps:** $21.45, providing a cost-effective solution for high levels of throughput protection.
- **Dual Power Supplies:** Yes, ensuring redundancy and reducing the risk of downtime.
- **Maximum Power Consumption:** 431 Watts, providing an efficient power profile.
- **Stackable Configuration:** No, the 13500 model does not support stacking, which may limit scalability in some environments.
- **Rack Space Usage:** 2U, meaning it occupies two rack units in a server rack.

➢ **Fortinet FortiGate-3600C: A High-Performance Next-Generation Firewall**

The **Fortinet FortiGate-3600C** is part of Fortinet's **3000 series** of appliances, designed to provide flexible deployment options for various network security needs. This model can function as a Next-Generation Firewall (NGFW), a traditional firewall, a Virtual Private Network (VPN) terminator, and a Next-Generation Intrusion Protection System (NGIPS). The FortiGate-3600C, along with other devices in the 3000 series (such as FortiGate-3040B, FortiGate-3140B, FortiGate-3240C, FortiGate-3700D, FortiGate-3810A, and FortiGate-3950B), offers comprehensive protection against evolving cyber threats.

This firewall is designed to deliver high throughput and low latency, making it suitable for medium to large enterprises and service provider environments. Fortinet is known for integrating their security fabric across devices, enhancing the overall network security posture with advanced features like secure SD-WAN, application control, and integrated threat intelligence[20][21].

Key Specifications:

- **Server Application Attacks Blocked:** 97%
- **Client Application Attacks Blocked:** 91.8%
- **Evasion Resistance:** The FortiGate-3600C is highly resistant to evasion tactics, ensuring comprehensive threat blocking.
- **Stability and Reliability:** Known for its consistent performance and uptime, making it suitable for demanding environments.
- **Enforcement of Application Policies:** Effectively enforces application security policies to ensure that only trusted applications are allowed to run.
- **Enforcement of Identity Policies:** Successfully enforces identity-based policies for secure access control.
- **IPS Throughput (Specification):** 15 Gbps
- **IPS Throughput (Tested):** 9.6 Gbps, which demonstrates reliable performance under real-world conditions.
- **Total Throughput:** 60 Gbps, offering ample throughput for high-traffic environments.

OPEN ACCESS I Canadian Journal of Discovery I August 2024, 5(12), 1-22, doi: https://doi.org/10.5281/zenodo.14674409

- **Cost per Protected Mbps:** $8.30, providing competitive pricing for its protection capabilities.
- **Dual Power Supplies:** Yes, ensuring high availability and resilience.
- **Maximum Power Consumption:** 615 Watts, balancing performance and energy efficiency.
- **Stackable Configuration:** No, unlike some models, this device cannot be stacked for greater scalability.
- **Rack Space Usage:** 3U, meaning it requires three rack units of space in a server rack.

Comparison Table:

Feature	Cisco FirePOWER 8350	CheckPoint 13500	Fortinet FortiGate-3600C	WatchGuard XTM1525	Dell SonicWALL SuperMassive E10800
Server Application Attacks Blocked (%)	99.5%	97.1%	97%	96.7%	96.4%
Client Application Attacks Blocked (%)	99%	95.9%	91.8%	98.7%	99.1%
IPS Throughput (Specification)	15 Gbps	5.7 Gbps	15 Gbps	13 Gbps	28 Gbps
IPS Throughput (Tested)	18.7 Gbps	6.7 Gbps	9.6 Gbps	3.4 Gbps	16.4 Gbps
Total Throughput	30 Gbps	23.6 Gbps	60 Gbps	25 Gbps	40 Gbps
Cost per Protected Mbps	$20.03	$21.45	$8.30	$11.87	$15.46
Max Power Consumption	635-1000 Watts	431 Watts	615 Watts	130 Watts	750 Watts
Stackable	Yes (Up to 4)	No	No	No	No
Rack Space Used per unit	2U	2U	3U	1U	4U

Figure 13

Compare Industry Next-Generation Firewalls (NGFWs)

Data Valid as of October 2018

	Cisco	Palo Alto Networks	Fortinet	Check Point Software Technologies
Security Features				

OPEN ACCESS I Canadian Journal of Discovery I August 2024, 5(12), 1-22, doi: https://doi.org/10.5281/zenodo.14674409

Continuous analysis and retrospective detection	✓ Cisco Firepower employs continuous analysis, beyond the event horizon (point-in-time) and can retrospectively detect, alert, track, analyze, and remediate advanced malware that may at first appear clean or that evades initial defenses and is later identified as malicious.	Limited Point-in-time only. (Point-in-time analysis indicates that a verdict is made on the disposition of a file at the moment it is first seen. If a file morphs or begins acting maliciously later, there are no controls in place to keep track of what happened or where the malware ended up.)	Limited Point-in-time only. (Point-in-time analysis indicates that a verdict is made on the disposition of a file at the moment it is first seen. If a file morphs or begins acting maliciously later, there are no controls in place to keep track of what happened or where the malware ended up.)	Limited Point-in-time only. (Point-in-time analysis indicates that a verdict is made on the disposition of a file at the moment it is first seen. If a file morphs or begins acting maliciously later, there are no controls in place to keep track of what happened or where the malware ended up.)
Network file trajectory	Continuous Cisco maps how hosts transfer files, including malware files, across your network. It can see if a file transfer was blocked or the file was quarantined. This provides a means to scope, provide outbreak controls, and identify patient zero.	✗ Trajectory dependent on continuous analysis.	✗ Trajectory dependent on continuous analysis.	✗ Trajectory dependent on continuous analysis.
Impact assessment	✓ Cisco Firepower correlates all intrusion events to an impact of the attack, telling the operator what needs immediate attention.	Limited Impact is measured only against threat severity. No host profile information to determine if host is actually vulnerable to threat.	Limited Impact is measured only against threat severity. No host profile information to determine if host is actually vulnerable to threat.	Limited Impact is measured only against threat severity. No host profile information to determine if host is actually vulnerable to threat.

OPEN ACCESS I Canadian Journal of Discovery I August 2024, 5(12), 1-22, doi: https://doi.org/10.5281/zenodo.14674409

	The assessment relies on information from passive device discovery, including OS, client and server applications, vulnerabilites, file processing, and connection events, etc.			
Security automation and adaptive threat management	✓ Cisco automatically adapts defenses to dynamic changes in the network, in files, or with hosts. The automation covers key defense elements such as NGIPS rule tuning and network firewall policy.	Limited All policies require administrator interaction. Policies are limited to basic tuning. False positives are manually identified and mitigated.	Limited All policies require administrator interaction. Policies are limited to basic tuning. False positives are manually identified and mitigated.	Limited Policies require administrator interaction.

- **The Next Great Thing in Cybersecurity**

As the landscape of computing continues to evolve, so too do the methods and techniques employed by cyber attackers. With this constant change, the tools and technologies used to defend against these threats must also progress. **Next-Generation Firewalls (NGFWs)** have significantly advanced the field of network security, but their evolution is far from over. As computing capabilities expand and cyber threats become increasingly sophisticated, it's inevitable that NGFWs will eventually be surpassed by newer, more advanced security solutions.

The future of cybersecurity is likely to bring new technologies that go beyond traditional firewalls, addressing emerging challenges like artificial intelligence (AI)-driven attacks, deep packet inspection, and zero-trust security models. Innovations such as quantum computing, blockchain-based security solutions, and AI-powered threat detection could usher in the next generation of defense mechanisms, rendering NGFWs as the stepping stones toward even more secure and adaptive network infrastructures.

Ultimately, the dynamic nature of both computing and cyber threats ensures that we are on the verge of discovering the next "great thing" in cybersecurity. It will be exciting to witness the development and deployment of the next wave of solutions that will redefine how we protect our networks and digital assets.

12. Findings

OPEN ACCESS I Canadian Journal of Discovery I August 2024, 5(12), 1-22, doi: https://doi.org/10.5281/zenodo.14674409

1. **Traditional Firewalls**: Effective in basic traffic filtering but lack the advanced threat-detection capabilities required to manage complex, modern threats, particularly at the application layer.
2. **Next-Generation Firewalls (NGFWs)**: Offer comprehensive protection by integrating additional security features like deep packet inspection, intrusion prevention, and encrypted traffic analysis, thus addressing sophisticated attack vectors.
3. **Product Comparison (Check Point vs. Palo Alto)**: Both vendors offer strong NGFW options, each with unique deployment models, advanced feature sets, and varying performance metrics. Check Point offers extensive application control, while Palo Alto is noted for its high throughput and superior application monitoring capabilities.
4. **Performance Metrics**: Both Check Point and Palo Alto received high security effectiveness ratings. Check Point's firewalls scored higher in blocking specific attacks, while Palo Alto's devices led in throughput performance.

13. Recommendations

Adopt NGFWs: Organizations should consider NGFWs for their capability to detect and mitigate modern cyber threats, especially those requiring application-level visibility and control.

Select NGFWs Based on Use-Case Needs: Organizations with complex infrastructures, particularly those with high traffic, may benefit more from Palo Alto's offerings, whereas Check Point is ideal for environments prioritizing granular application control.

Continuous Upgrading and Threat Intelligence: Regular updates and access to real-time threat intelligence services are essential to maintain firewall efficacy against emerging threats.

14. Conclusion

This study concludes that while traditional firewalls are still useful for basic network protection, NGFWs are more equipped to handle today's security landscape, with advanced functionalities that mitigate complex threats effectively. Organizations should assess their specific security needs and choose firewall solutions that offer the best balance between performance, control, and cost-effectiveness.

OPEN ACCESS I Canadian Journal of Discovery I August 2024, 5(12), 1-22, doi: https://doi.org/10.5281/zenodo.14674409

15. References:

1. Stallings, W. (2018). *Network Security Essentials: Applications and Standards*.
2. Gollmann, D. (2011). *Computer Security*.
3. Antonopoulos, A., & Gillam, L. (2010). *Cloud Computing: Principles, Systems and Applications*.
4. Harwood, S. (2016). *Business Data Communications and Networking*.
5. Stallings, W. (2019). *Network Security Essentials: Applications and Standards*.
6. Kizza, J. M. (2020). *Guide to Computer Network Security*.
7. Shackleford, D. (2013). *Next-Generation Firewalls: Security That Meets Today's Complex Threat Landscape*. SANS Institute.
8. Easttom, C. (2019). *Computer Security Fundamentals*.
9. Kizza, J. M. (2020). *Guide to Computer Network Security*.
10. Harwood, S. (2016). *Business Data Communications and Networking*.
11. Easttom, C. (2019). *Computer Security Fundamentals*.
12. Harwood, S. (2016). *Business Data Communications and Networking*.
13. Shackleford, D. (2013). *Next-Generation Firewalls: Security That Meets Today's Complex Threat Landscape*. SANS Institute.
14. Easttom, C. (2019). *Computer Security Fundamentals*.
15. Palo Alto Networks. (2021). *PAN-OS 8.1 Release Notes*.
16. Check Point Software Technologies. (2021). *Check Point Infinity Security Architecture Overview*.
17. NSS Labs, Inc. (2021). *Next-Generation Firewall Comparative Analysis Report*.
18. Cisco. (n.d.). Cisco Firepower 8300 Series Data Sheets. Cisco. Retrieved from https://www.cisco.com/
19. Cisco. (n.d.). Adaptive Security Appliances (ASA) and Firepower Overview. Cisco. Retrieved from https://www.cisco.com/
20. Fortinet. (n.d.). FortiGate 3000 Series Data Sheets. Fortinet. Retrieved from https://www.fortinet.com/
21. Fortinet. (n.d.). FortiGate NGFW Overview. Fortinet. Retrieved from https://www.fortinet.com/.

OPEN ACCESS I Canadian Journal of Discovery I August 2024, 5(12), 1-22, doi: https://doi.org/10.5281/zenodo.14674409

CanDis Canadian Journal of Discovery

Citation

Dr.Eng. Jouma Ali Al-Mohamad, Performance Evaluation of Firewall Technologies

Canadian Journal of Discovery, 2024, 5(12), 1-22, doi: https://doi.org/10.5281/zenodo.14674409