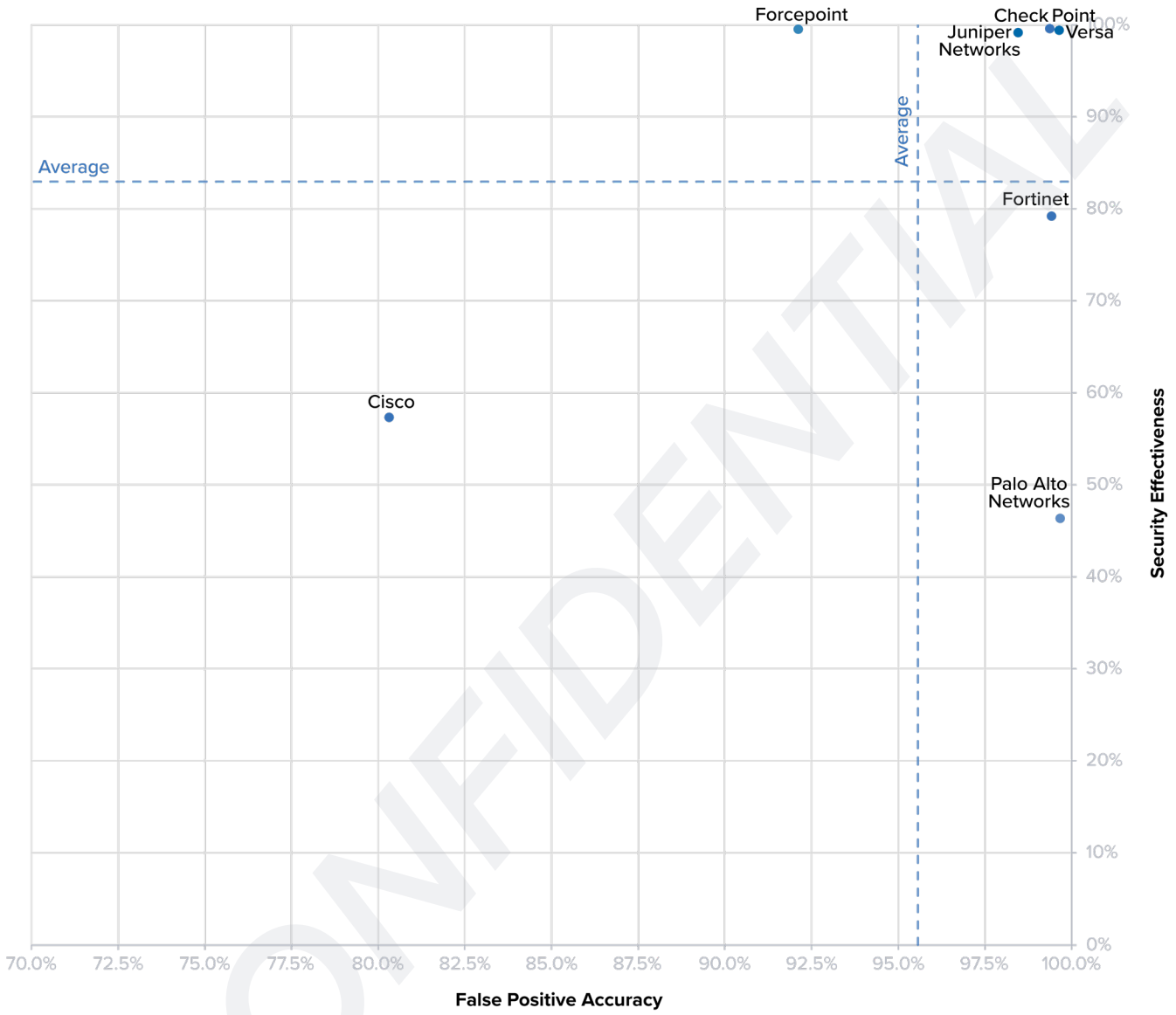
COMPARATIVE TEST REPORT

Enterprise Firewall

In Q3 2025, NSS Labs conducted independent evaluations of seven leading Enterprise Firewall offerings using the Enterprise Firewall Test Methodology v3.0. The evaluation covered key performance metrics, including how effectively the firewall protected customers from exploits and malware over encrypted traffic, while also avoiding evasions and triggering false positives, all while remaining stable under enterprise workloads. The firewalls were tested using real-world attack scenarios, enterprise-grade workloads, and adversarial evasion techniques to measure their resilience, reliability, and performance.

Table of Contents

Comparative Security Map (CSM)



Enterprise Firewall (EFW)	Rating	Security Effectiveness	False Positive Accuracy
Check Point CP-CGS-9300	Recommended	99.59%	99.36%
Cisco Firepower 2130	Caution	57.34%	80.31%
Forcepoint 2210	Neutral	99.53%	92.11%
Fortinet FortiGate-200G	Caution	79.19%	99.42%
Juniper Networks SRX4300	Recommended	99.16%	98.46%
Palo Alto Networks PA-1410	Caution	46.37%	99.67%
Versa Networks CSG5200	Recommended	99.43%	99.64%

Ratings

The NSS Labs Comparative Security Map (CSM) provides a high-level analysis of empirical data gathered during testing. It conveys the relative capabilities of product offerings by mapping a tested product's security effectiveness on one axis and false positive accuracy as a measurable proxy for operational overhead on the other.

Every enterprise has unique requirements, and the CSM should only be a starting point. In addition to this comparative report, individual test reports for each product tested, along with comprehensive documentation on the methodology employed, are available at https://nsslabs.com

The Recommended, Neutral, or Caution ratings are determined by the product's position on the Comparative Security Map. For more information, see the end of this report.

SVM vs. CSM: Price, Operational Overhead, and False Positive Accuracy

Historically, the NSS Labs Comparative Report included the Security Value Map (SVM). The SVM sought to answer, "How good is it?" and "How expensive is it?" by mapping a product's price per protected megabit and its security effectiveness on a chart. Over the past few years, we have found "How expensive is it?" has become less relevant as the business impact of security breaches and longer-term total cost of ownership far exceeded the purchase price of security products. Additionally, vendors price their products using differing licensing and consumption models making a standardized comparison across vendors impractical.

We found that in addition to security effectiveness, "What is the business impact of using this product?" is what buyers care about. Rather than price, we determined that false positive accuracy was objective, measurable and could be standardized across vendors. False positives are when a product mistakenly classifies legitimate activity or content as malicious, causing security operations teams to waste resources on false alarms, impacting end-user productivity by blocking necessary content or applications, and increasing load on IT support to service those end-users impacted. The most effective solutions provide both comprehensive threat detection with minimal disruption to legitimate operations.

Executive Summary

Key Findings

- **Test Results point to how attackers are bypassing defenses.** While average exploit and malware block rates exceeded 98%, three widely deployed vendors failed critical evasion tests that significantly reduced their effectiveness. Only four of seven products earned a Recommended rating.
- **Evasion test results are alarming.** The fact that well-known transport and network layer evasions (that can be applied to nearly every attack) were able to bypass some of the most widely held security products in the world should be concerning to everyone. Attackers use evasion techniques to bypass security defenses. It is critical that products properly handle evasions, especially high-impact transport and network-layer evasions.
- **Encrypted traffic contains attacks.** Protecting against attacks within encrypted traffic is the true test of firewall performance. Industry research and data indicate that more than 95% of global web traffic is now encrypted.[1] Most products handle TLS/SSL effectively, but some showed greater performance drops than others.
- **High accuracy is essential** to avoid wasted resources, user disruption, and reduced trust in security. One product recorded a below-average 81% false positive accuracy rate; their customers are likely experiencing high operational costs and/or reduced security effectiveness as protections are disabled to reduce false positive noise.

Recommendations

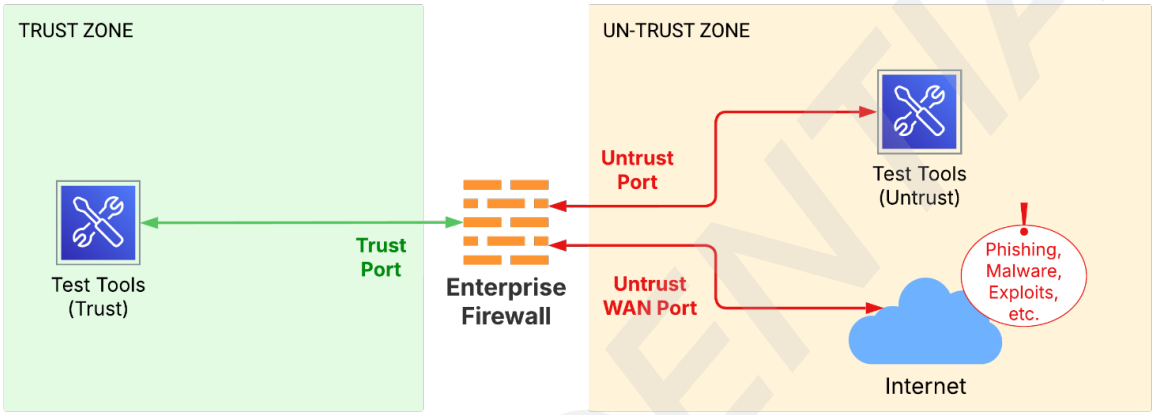
- **Regularly test your security products.** Agile development and modern CI/CD pipelines enable rapid development and deployment, but those rapid product improvements may also introduce bugs that can impact the effectiveness of your security product. Regular testing provides ongoing assurance that security technologies are performing as promised. If you lack the resources to perform regular in-depth testing, ask NSS Labs about its Minion by NSS Labs managed testing offering.
- **Re-evaluate your network firewall requirements.** Local AI models, agentic workflows, and third-party AI models from Anthropic, Google, Microsoft, OpenAI, etc. will consume increasing amounts of network resources as applications are tooled with AI capabilities (e.g., Microsoft Office Copilot, Salesforce Agentforce, Perplexity Assistant). Will there be more east-west agent-to-agent traffic? Will your firewall be expected to enforce larger and more complex policies? Evaluate emerging requirements and independently test results before committing to a product.
- **Hold Vendors accountable.** Ask Firewall Vendors about their test results and pay attention to their response. No product is perfect. Every cybersecurity product will have a bug on occasion. How did the vendor respond? Did they make excuses? Were they dismissive? Or were they responsive in a positive manner and did they put your interests first?
- **Demand transparency.** Favor vendors willing to undergo independent third-party testing. Lack of transparency should be a red flag.

1 https://comparecheapssl.com/data-privacy-encryption-statistics/

Overview

The test focused on real-world attack techniques and enterprise workloads to evaluate both security, potential operational impact, and performance thoroughly. By applying consistent and repeatable benchmarks, this report gives enterprises clear, objective data to assess the effectiveness, reliability, and efficiency of leading enterprise firewall offerings.

Test Topology



.

Figure 1 — Enterprise Firewall Test Topology

The firewalls for this round of testing were deployed in-line between trusted and untrusted networks. Traffic flows included both legitimate business traffic and malicious activity, ensuring a comprehensive assessment of each firewall's ability to enforce security policies while maintaining operational stability.

Inclusion Criteria

This test was conducted at the request of CyberRatings.org and was not sponsored by any vendor. Vendors could not pay to be included or excluded from this test. Decisions regarding the inclusion of a product were based on:

- Market presence
- Identification by industry analysts covering the specific technology area
- Consumer requests
- Innovative technology/offering or marketing claims that receive significant market attention (requires internal vetting for emerging vendors)

How We Tested

To ensure realistic and rigorous evaluation, the following datasets and workloads were used:

- **False Positives:** 6,603 samples from business-critical files and applications, validating that security measures did not disrupt legitimate traffic.
- **Exploits:** 3,326 attack samples from widely exploited vulnerabilities in enterprise environments.
- **Malware:** 11,311 samples sourced from active malware campaigns across multiple operating systems.
- **Evasion Techniques:** 5,752 attack variations spanning 53 evasion categories, crafted to bypass firewall defenses.
- **Performance:** 55 tests across diverse workloads to measure throughput, stability, and reliability under stress.

These comprehensive tests determined the Enterprise Firewall's ability to deliver reliable threat prevention, operational stability, and minimal disruption to legitimate traffic. Organizations can use these results to make informed decisions when selecting a firewall for modern enterprise environments.

Security Effectiveness

Implementing a firewall can be complex, with multiple factors affecting security effectiveness. The following should be considered over the life of the device:

- What operating systems and applications are to be protected?
- What defensive capabilities are necessary (malware and exploit block rate)?
- What is the product's ability to protect against common evasion techniques?
- How well does the firewall handle false positives?
- What TLS/SSL cipher support is required?
- How much throughput is needed?
- Is the device stable and reliable?

To assess security effectiveness and accurate product comparisons, we applied the following formula:

$$\textbf{Security Effectiveness} = \text{Routing \& Access Control} \times \text{TLS/SSL Support} \times \text{Stability \& Reliability} \times \frac{(\text{Malware Block Rate} \times \text{Malware Evasions Resistance}) + (\text{Exploit Block Rate} \times \text{Exploit Evasions Resistance})}{2}$$

Figure 2 — Security Effectiveness Formula

By using the formula above, we calculated the overall security effectiveness of a product by incorporating evasion resistance, rather than just the exploit and malware block rate alone. This formula not only considers detection accuracy but also assesses how effectively a product can counter advanced evasion tactics, providing a thorough understanding of an Enterprise Firewall product's capacity to mitigate tactics, techniques, and procedures used in the current real-world threat landscape. For more details, see the Evasions section.

Malware typically acts as the payload, while exploits can act as a stand-alone threat and a delivery method. Both malware and exploits are vital elements in real-world attacks—overemphasizing one aspect could result in overlooking essential protection gaps. Furthermore, certain evasion techniques are specific to exploits, while others apply only to malware, meaning not all evasions are relevant to both threat types.

Enterprise Firewall	Routing & Policy Enforcement	TLS/SSL Support	Stability & Reliability	Malware Block Rate	Malware Evasions Resistance	Exploit Block Rate	Exploit Evasions Resistance	**Security Effectiveness**
Check Point	100.00%	100.00%	100.00%	99.28%	100.00%	99.91%	100.00%	**99.59%**
Cisco	100.00%	100.00%	100.00%	77.49%	100.00%	92.99%	40.00%	**57.34%**
Forcepoint	100.00%	100.00%	100.00%	99.94%	100.00%	99.13%	100.00%	**99.53%**
Fortinet	100.00%	100.00%	100.00%	98.48%	100.00%	99.82%	60.00%	**79.19%**
Juniper Networks	100.00%	100.00%	100.00%	98.71%	100.00%	99.61%	100.00%	**99.16%**
Palo Alto Networks	100.00%	100.00%	100.00%	92.74%	100.00%	99.37%	0.00%	**46.37%**
Versa Networks	100.00%	100.00%	100.00%	99.01%	100.00%	99.85%	100.00%	**99.43%**

Figure 3 — Security Effectiveness

Routing & Access Control

Access control is a firewall's primary responsibility. Throughout its history, the goal of a firewall has been to enforce an access control policy between two networks. Rules are configured to permit or deny traffic from one network resource to another based on identifying criteria such as source IP, destination IP, source port, destination port, and protocols.

This test validated that the firewalls enforced security policies over various policy environments, from simple to complex. The tests were incrementally built on a baseline consisting of a simple configuration with no policy restrictions and no content inspection, to a complex multiple-zone configuration that supports many users, networks, policies, and applications. Traffic was tested at each level of complexity to ensure specified policies were enforced.

Enterprise Firewall	Network Segmentation Results		Access Control Results	
	Unrestricted Traffic Test	Segmented Traffic Test	Simple Policies	Complex Multi-Zone Policies
Check Point	Supported	Supported	Supported	Supported
Cisco	Supported	Supported	Supported	Supported
Forcepoint	Supported	Supported	Supported	Supported
Fortinet	Supported	Supported	Supported	Supported
Juniper Networks	Supported	Supported	Supported	Supported
Palo Alto Networks	Supported	Supported	Supported	Supported
Versa Networks	Supported	Supported	Supported	Supported

Figure 4 — Routing & Access Control Results

These tests also assess resilience against lateral movement, a common tactic used by attackers after compromising an endpoint. By enforcing strong segmentation, firewalls prevent attackers from pivoting to sensitive systems.

TLS/SSL Support

Industry-wide research and data indicate that encryption now dominates web traffic, with more than 95% of global traffic using HTTPS due to browser mandates, security expectations, and regulations.[2] TLS/SSL is the default protocol for most websites, protecting user data and transactions. The tested cipher suites represent ~97% of TLS sessions observed globally,[3] with TLS 1.3 as the default standard.

Encryption, while beneficial, creates security challenges. Attackers increasingly hide exploits and malware within encrypted sessions, targeting the handshake, record, application data, and PKI layers. To address these threats, we tested the Firewall for its ability to detect both attacks hidden in encrypted traffic and attacks against the encryption protocols themselves:

- Tested handling of insecure cipher suites, including null and anonymous ciphers.
- Verified correct decryption and inspection of TLS/SSL traffic, ensuring previously blocked content remained blocked once encrypted.
- Tested conditional decryption bypass for regulatory or privacy requirements.
- Validated TLS session reuse (session tickets and IDs) to confirm the firewall reduced overhead and improved efficiency.

Top 5 Cipher Suite Support

The firewalls were expected to support a wide range of commonly used cipher suites to provide visibility into potential threats encrypted using TLS/SSL. Cipher suites were selected based on current industry data on usage frequency[4] and security status.[5]

Cipher Version	Cipher Suite Description	Frequency of Use
TLS 1.3	TLS_AES_256_GCM_SHA384 (0x13, 0x02)	~72%
TLS 1.3	TLS_AES_128_GCM_SHA256 (0x13, 0x01)	~13%
TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xC0, 0x30)	~7%
TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xC0, 0x2F)	~5%
TLS 1.3	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xCC, 0xA8)	~1%

Figure 5 — Top 5 Cipher Suite Support

2 https://comparecheapssl.com/data-privacy-encryption-statistics/

3 https://www.sci-tech-today.com/stats/ssl-statistics-updated/

4 https://crawler.ninja/files/ciphers.txt

5 https://ciphersuite.info/cs/

Enterprise Firewall	Top 5 Cipher Support	Prevention of Weak Ciphers	Decryption Bypass Supported
Check Point	5/5	Yes	Yes
Cisco	4/5	Yes	Yes
Forcepoint	5/5	Yes	Yes
Fortinet	5/5	Yes	Yes
Juniper Networks	5/5	Yes	Yes
Palo Alto Networks	4/5	Yes	Yes
Versa Networks	5/5	Yes	Yes

Figure 6 — TLS/SSL Support (I)

*Palo Alto Networks and Cisco do not support the CHACHA20 cipher suites and do not claim to support them. We determined this lack of support to be immaterial since CHACHA20 cipher suites account for only ~1% of TLS/SSL traffic. As a result, no penalty was assessed.

Session reuse is one of the mechanisms used to improve TLS/SSL performance; the table below lists which products have either functionality as an option.

Enterprise Firewall	TLS Session Reuse - Session Tickets	TLS Session Reuse - Session IDs
Check Point	Supported	Supported
Cisco	Supported	Supported
Forcepoint	Supported	Supported
Fortinet	Supported	Not Supported
Juniper Networks	Not Supported	Supported
Palo Alto Networks	Not Supported	Supported
Versa Networks	Not Supported	Not Supported

Figure 7 — TLS/SSL Support (II)

Malware

Malware is malicious software designed to disrupt, damage, or gain unauthorized access to computer systems or data. It can appear in many forms—including viruses, worms, trojans, ransomware, and spyware—but its primary goal is to compromise the confidentiality, integrity, or availability of data and systems.

While malware can be delivered through various vectors such as phishing emails, social media, or compromised websites, all these methods rely on successfully downloading or executing a malicious payload. In evaluating malware protection efficacy, we specifically examined the firewall's ability to block malware at the point of download, where it acts as a crucial line of defense.

To evaluate effectiveness in protecting diverse platforms, we tested the product's ability to block malicious files and URLs across both Linux and Microsoft Windows operating systems.

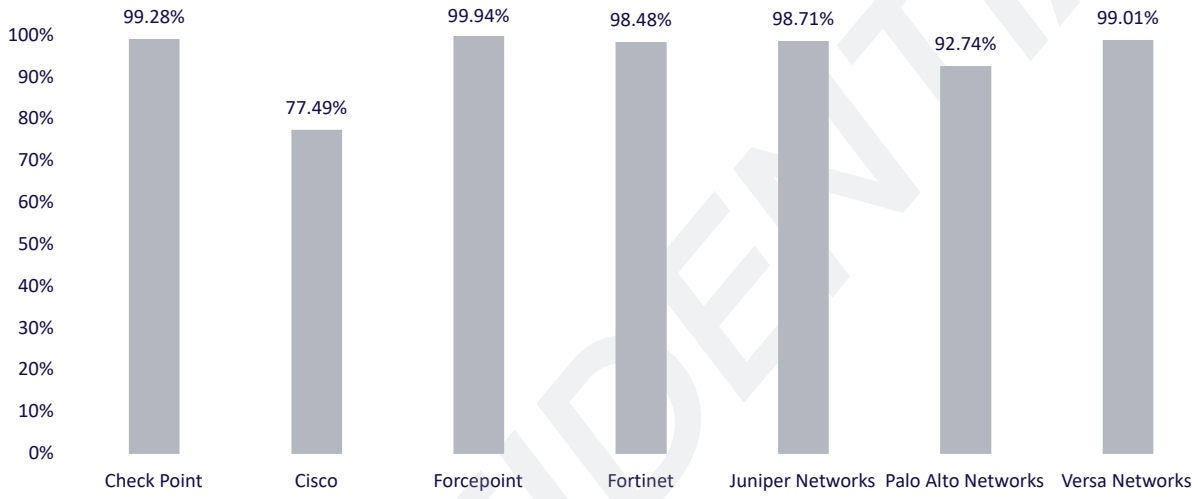


Figure 8 — Malware Blocked

Exploits

An exploit is an attack that takes advantage of a vulnerability in a protocol, product, operating system, or server application. This test verified the firewall's ability to detect and block exploits targeting known vulnerabilities.

Exploits used in this test are a collection of internal, third-party, in-the-wild, and public exploits encompassing a wide range of protocols and applications. It is based on the Common Vulnerabilities and Exposures (CVEs) publicly listed in the MITRE CVE and NIST NVD databases.[6]

The subset of exploits selected for this test includes, but is not limited to:

- Recent vulnerabilities (last 6 years)
- CISA's Known Exploited Vulnerabilities
- Vulnerabilities with a high Common Vulnerability Scoring System (CVSS) score (version 3.x)

Coverage by CVE

Exploit protection was categorized by CVEs rated critical, high, medium and low.

Enterprise Firewall	Critical	High	Medium	Low	**Overall**
Check Point	100.00%	99.86%	99.91%	100.00%	**99.91%**
Cisco	94.75%	94.37%	90.52%	86.00%	**92.99%**
Forcepoint	99.57%	99.16%	98.78%	100.00%	**99.13%**
Fortinet	99.86%	99.72%	99.91%	100.00%	**99.82%**
Juniper Networks	99.43%	99.51%	99.83%	100.00%	**99.61%**
Palo Alto Networks	100.00%	99.37%	98.96%	100.00%	**99.37%**
Versa Networks	99.72%	99.86%	99.91%	100.00%	**99.85%**

Figure 9 — Exploit Coverage by CVE

6 cve.org: https://www.cve.org/; NIST NVD: https://nvd.nist.gov/vuln/search

Coverage by Attack Vector

Because a failure to block attacks could result in significant compromise, severely impacting critical business systems and data, firewalls should be evaluated against a broad set of exploits. Exploits can be categorized as client-initiated or server-initiated. Server-initiated exploits are threats executed remotely against a vulnerable application and/or operating system by an individual, while client-initiated exploits are initiated by the vulnerable target. Client-initiated exploits are the most common type of attack experienced by the end user, and the attacker has little or no control over when the threat is executed.

Enterprise Firewall	Server-Side Exploits	Client-Side Exploits	**Total Blocked**
Check Point	99.91%	99.90%	**99.91%**
Cisco	94.89%	88.68%	**92.99%**
Forcepoint	99.18%	99.02%	**99.13%**
Fortinet	99.78%	99.90%	**99.82%**
Juniper Networks	99.48%	99.90%	**99.61%**
Palo Alto Networks	99.31%	99.51%	**99.37%**
Versa Networks	99.91%	99.70%	**99.85%**

Figure 10 — Exploit Coverage by Attack Vector

Coverage by Year

Our research indicates that the most significant risks are not always driven by the latest "Patch Tuesday" disclosures. Studies reveal that many older applications, operating systems, and attacks are still circulating and relevant.

Vendors may retire older signatures to alleviate product performance limitations, which may result in poor coverage for older vulnerabilities and inconsistent protection across products. Exploits for the past ten years, classified by disclosure date and tracked by CVE numbers are shown below.

Enterprise Firewall	<=2016	2017	2018	2019	2020	2021	2022	2023	2024	2025
Check Point	100.00%	100.00%	100.00%	100.00%	99.38%	99.63%	100.00%	100.00%	100.00%	100.00%
Cisco	95.78%	96.93%	95.71%	88.71%	94.15%	94.05%	94.53%	92.98%	70.49%	50.00%
Forcepoint	98.11%	98.85%	99.24%	99.88%	98.77%	99.26%	100.00%	98.76%	100.00%	100.00%
Fortinet	100.00%	100.00%	100.00%	99.88%	100.00%	100.00%	99.61%	98.35%	100.00%	100.00%
Juniper Networks	99.85%	100.00%	98.23%	99.88%	99.38%	99.63%	99.61%	100.00%	100.00%	100.00%
Palo Alto Networks	98.69%	98.85%	99.24%	100.00%	99.08%	99.26%	99.61%	100.00%	100.00%	100.00%
Versa Networks	99.56%	100.00%	99.75%	100.00%	100.00%	100.00%	99.61%	100.00%	100.00%	100.00%

Figure 11 — Exploit Coverage by Year

Vendors take different approaches to adding coverage once a vulnerability is disclosed. Attempts to provide rapid coverage for vulnerabilities that are not fully understood can result in multiple exploit-specific signatures that may be inaccurate, ineffective, or prone to false positives. Vendors that have the resources to research a vulnerability fully should be able to produce vulnerability-oriented signatures that provide coverage for all exploits written to take advantage of that flaw. This approach provides more effective coverage with fewer false positives.

Coverage by Target Vendor

Exploits within the NSS Labs exploit library target many protocols and applications.

Enterprise Firewall	Adobe	Microsoft	Apache	Oracle	Google	Atlassian	Nagios	Cisco	WordPress	VMware
Check Point	100.00%	100.00%	99.18%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%
Cisco	94.07%	90.67%	97.12%	90.96%	95.38%	96.23%	100.00%	97.92%	97.67%	92.86%
Forcepoint	100.00%	99.25%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%
Fortinet	100.00%	99.81%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%
Juniper Networks	100.00%	100.00%	99.59%	100.00%	100.00%	100.00%	100.00%	100.00%	97.67%	100.00%
Palo Alto Networks	100.00%	99.44%	99.59%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	97.62%
Versa Networks	99.26%	99.63%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%

Figure 12 — Exploit Coverage for Top Vendors

Please refer to the NSS Labs individual Enterprise Firewall product test report for additional details of what was missed by each product.

Evasions

This test aimed to determine whether an evasion technique could bypass the firewall. Attackers use evasions to conceal malicious activity at the point of delivery, attempting to bypass inspection and defenses. A single successful evasion can enable adversaries to reuse entire categories of exploits or malware through the same vulnerability, making proper evasion handling critical to dependable security.

We tested 53 evasion categories across 5,752 unique variations. The majority were handled correctly; only three products failed to block certain categories. To keep the comparative report concise, the table below highlights only those categories where failures occurred, along with their assigned impact (e.g., 40% for TCP segmentation).

Each product starts with a baseline of 100% evasion resistance, and the assigned impact for any missed evasion is subtracted. The resulting value is then factored into the security effectiveness.

Enterprise Firewall	OSI Level 3	OSI Level 4	OSI Level 7	Total Impact	**Malware Evasions Resistance**
Check Point	Pass	Pass	Pass	0%	**100%**
Cisco	Pass	Pass	Pass	0%	**100%**
Forcepoint	Pass	Pass	Pass	0%	**100%**
Fortinet	Pass	Pass	Pass	0%	**100%**
Juniper Networks	Pass	Pass	Pass	0%	**100%**
Palo Alto Networks	Pass	Pass	Pass	0%	**100%**
Versa Networks	Pass	Pass	Pass	0%	**100%**

Figure 13 — Malware Evasions Resistance

Enterprise Firewall	OSI Level 3	OSI Level 4	OSI Level 7	Total Impact	**Exploit Evasions Resistance**
Check Point	Pass	Pass	Pass	0%	**100%**
Cisco	Pass	Fail	Pass	60%	**40%**
Forcepoint	Pass	Pass	Pass	0%	**100%**
Fortinet	Pass	Fail	Pass	40%	**60%**
Juniper Networks	Pass	Pass	Pass	0%	**100%**
Palo Alto Networks	Fail	Fail	Pass	100%	**0%**
Versa Networks	Pass	Pass	Pass	0%	**100%**

Figure 14 — Exploit Evasions Resistance

Evasion Impact

Weightings based on the characteristics of the evasion technique were used to determine impact.

Evasion Technique Commonality

- **Common-use techniques** – Techniques based on normal protocol behaviors that can be found present in legitimate traffic such as retransmissions, compression, or segmentation. These are techniques easy for attackers to leverage because defensive systems must allow these behaviors as a part of normal operations – making the malicious nature of the evasion harder to determine.
- **Less-common techniques** – Based on less common and abnormal behavior such as malformed headers, overlapping fragments, or bogus HTTP headers. These have a limited real-world effectiveness because they should, under normal circumstances, be rejected by applications and network stacks.

Layer-based Impact

Network based evasions using lower level OSI layers have a wider scope of impact and a cascading effect that can provide evasion from detection for a greater range of exploits and malware. Wide ranging application or content level evasions, such as compression or packers, provide a similar wide scope of impact or cascading effect for malware.

Note: Full details of all 53 categories and test outcomes are available in the individual product reports.

False Positive Accuracy

False positives can have serious operational consequences, forcing teams to disable security features and reduce overall protection. They also create extra work for security staff, leading to “alert fatigue” and increasing the likelihood that real threats will be missed. This test measured the enterprise firewall’s ability to discern between legitimate and malicious traffic effectively.

The NSS Labs false positive repository contains approximately 100,000 legitimate samples, including URLs, file transfers, and application flows relevant to enterprise use cases. To prevent skewed results, items such as software cracks, game cheats, crypto wallets, mining software, and adware-filled freeware are excluded from the dataset.

We tested initially with both inbound and outbound traffic to determine if the firewall was applying blanket restrictions. We then assessed connections using standard ports (80, 443) and alternative ports (30080, 30443) to ensure that legitimate connections, including those required for software and system updates, were not blocked unnecessarily. Blocking these types of connections would be an unacceptable practice for enterprises.

We then moved on to file-based testing, beginning with system files and executables before expanding to productivity-related formats, compressed files, and media.

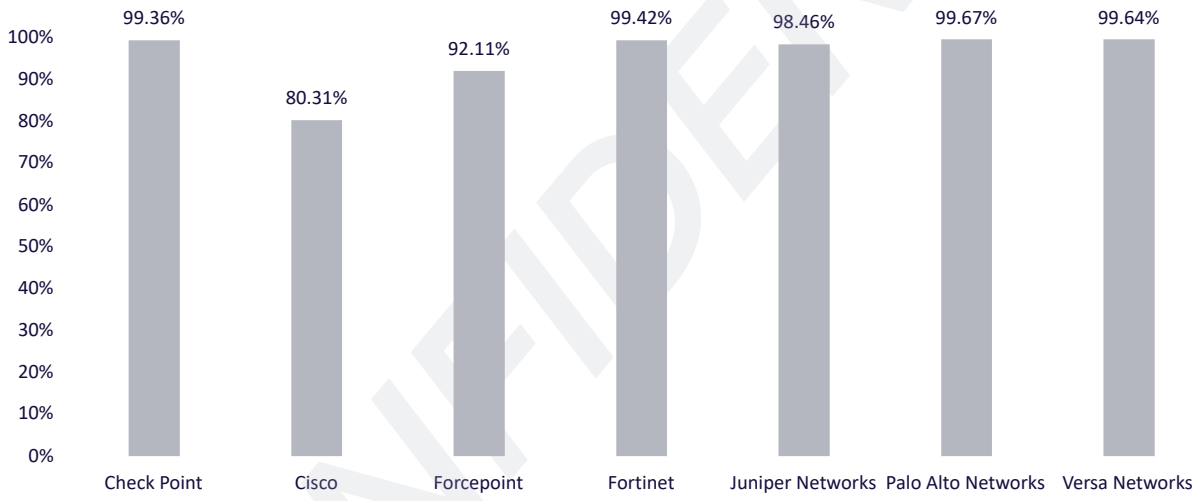


Figure 15 — False Positive Accuracy

False Positives Impact

Understanding the impact of false positives is crucial for assessing enterprise firewalls beyond just detection accuracy. While blocking malicious attacks is vital, blocking legitimate traffic or files can disrupt business operations, impact user productivity, and undermine trust in security measures. By analyzing both web page and file-based detections, this section addresses how even a small share of false positives can lead to significant operational costs, system inefficiencies, and user frustration.

Web pages: All web page blocks are classified as low impact. This accounts for the possibility that a site may actively be hosting malware during testing, making it impossible to prove or disprove definitively. The websites tested were standard websites that host content and are not representative of SaaS applications.

Files: File blocks are also initially classified as low impact. However, as the number of blocked files exceeds a threshold of 90%, the impact is increased to high, reflecting the operational effects of regularly blocking legitimate files.

Since firewalls can dynamically adjust their security settings using machine learning or heuristic updates, false positives were checked before, during, and after security effectiveness testing. A sample was considered a false positive if it was blocked at any time during the test.

This evaluation method ensures that false positives are considered not only by type, but also by frequency to account for the extent to which they affect enterprise operations. High false positive accuracy represents a maturity in a product's ability to distinguish legitimate activity from malicious traffic without causing unnecessary disruptions.

Performance

We tested 55 performance use cases for each product to capture their performance curves. This included maximum connections and transactions per second, concurrency, throughput, and latency to see how the firewall performed under various adverse conditions. As a result, each product has achieved a rated throughput. For more tests and details, please see the individual test reports.

Rated Throughput

To establish a consistent and meaningful rated throughput across enterprise firewalls, NSS Labs measured sustained throughput over time across a range of packet sizes and connection rates per second.

Note: This year, we've updated our test methodology calculation for rated throughput to better reflect real-world conditions. The main change is a higher weighting for encrypted (TLS) traffic, which may result in lower NSS Labs Rated Throughput compared to previous years for the same product. This does not necessarily indicate decreased product performance; rather, it reflects a more realistic traffic mix. The NSS Labs Rated Throughput provides a useful comparison based on defined use cases and industry experience, but we recommend enterprises review specific test cases to see how closely the traffic patterns match their own environments.

Testing captured the firewall's performance curves for both clear-text (HTTP) and encrypted (HTTPS/TLS) traffic. Since approximately 95%[7] of real-world enterprise traffic is encrypted, the NSS Labs Rated Throughput is calculated with a 95% weighting for TLS/SSL encrypted traffic and 5% weighting for plain-text traffic, reflecting the real-world mix observed in enterprise networks. Please see the individual test report for details on the calculation.

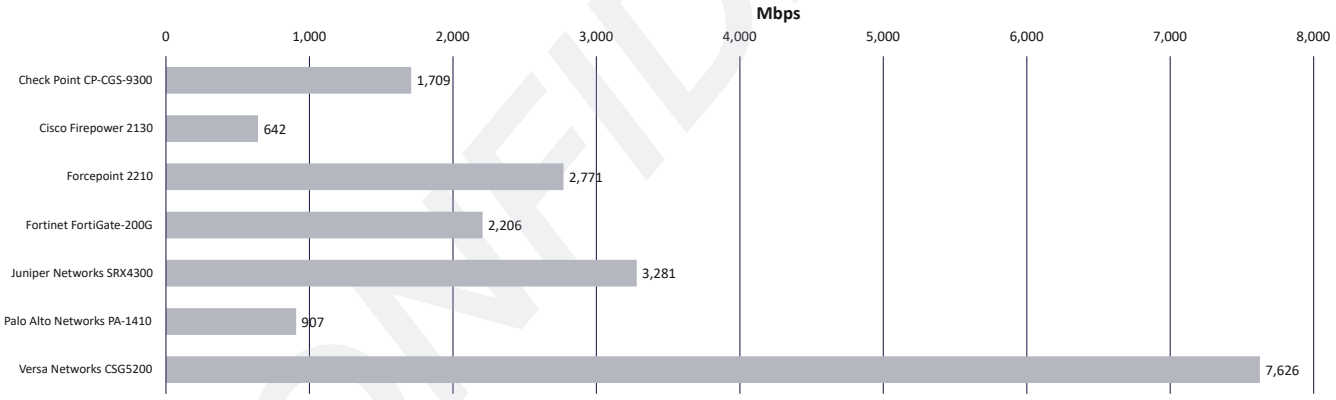


Figure 16 — NSS Labs Rated Throughput

These results are not best-case scenarios. Firewall performance was measured using the same security configurations as those in the security tests and was verified to be maintained over extended periods of time. Our tests are designed to uncover what an organization can expect from its firewall under (reasonably) adverse conditions, not best-case scenarios. Performance testing was conducted with the firewall configured according to vendor-recommended best practices, including security features such as intrusion prevention, TLS/SSL decryption, and logging enabled.

The Rated Throughput results are what an enterprise can expect the firewall to deliver consistently in production environments while providing full protection capabilities. This benchmark provides organizations with practical data on each product's ability to support encrypted workloads, maintain stability under load, and enforce security policies without degrading user experience.

7 https://comparecheapssl.com/data-privacy-encryption-statistics/

Theoretical Maximum Capacity

These tests aimed to stress the inspection engine and determine how it copes with high volumes of TCP connections per second, application-layer transactions per second, and concurrent open connections. All packets contained valid payload and address data. In all tests, final measurements were taken at the following critical "breaking points:"

- **Excessive concurrent TCP connections** – Latency within the firewall is causing an increase in open connections.
- **Excessive concurrent HTTP connections** – Latency within the firewall is causing delays and increased response time.
- **Unsuccessful HTTP transactions** – Normally, there should be zero unsuccessful transactions. Once these appear, it indicates that firewall latency is causing connections to time out.

Theoretical Maximum Concurrent TCP Connections

This test determined the device's maximum concurrent TCP connections with no data passing across the connections. This type of traffic would not typically be found on a normal network, but it provides the means to determine the maximum possible concurrent connections.

Maximum TCP Connections per Second

This test is designed to determine the maximum TCP connection rate of the device with one byte of data passing across the connections. This type of traffic would not typically be found on a normal network, but it provides the means to determine the maximum possible TCP connection rate.

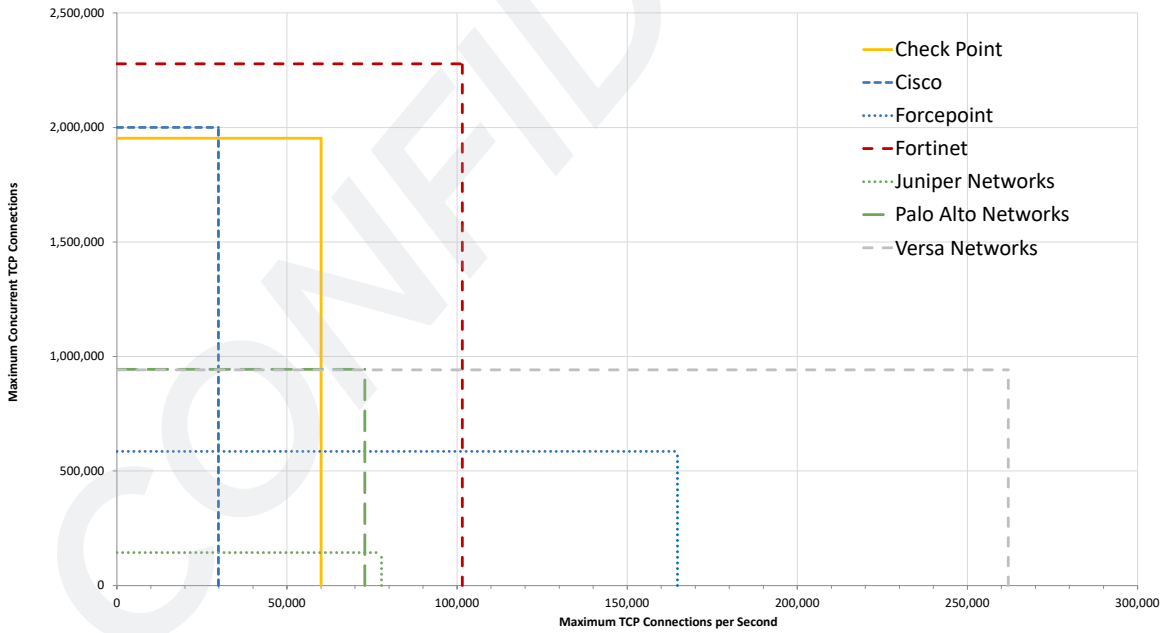


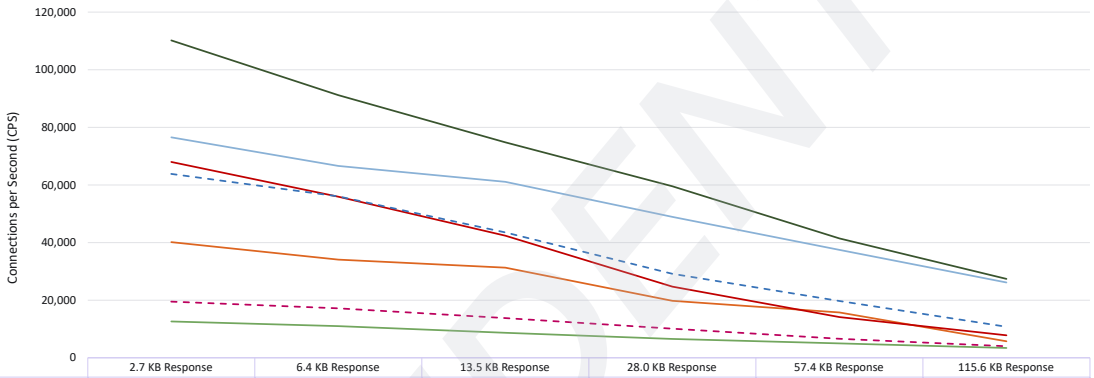
Figure 17 — Maximum Capacity

The rate of maximum TCP CPS increases toward the right side of the x axis. The rate of concurrent/simultaneous connections increases toward the top of the y axis.

HTTP Capacity

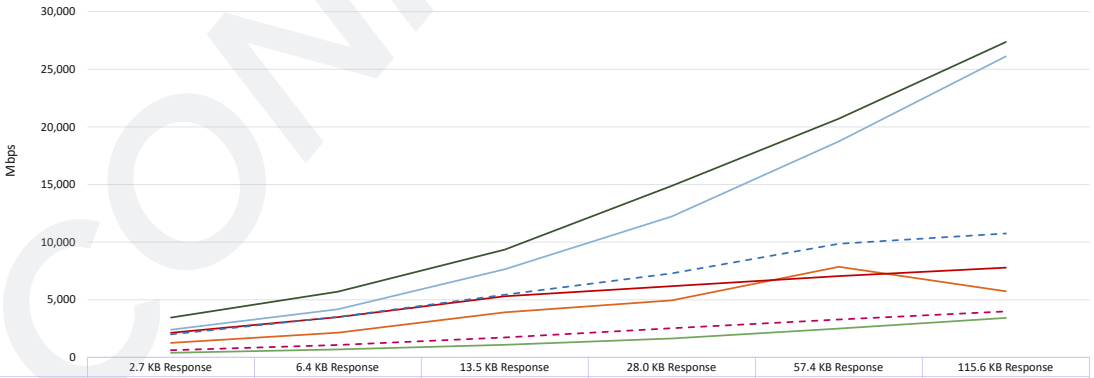
The goal of the HTTP Capacity test was to stress the HTTP detection engine and determine how the device copes with network loads of varying average packet sizes and varying connections per second. By creating genuine session-based traffic with varying session lengths, the device was forced to track valid TCP sessions, thus ensuring a higher workload than simple packet-based background traffic. This provided a test environment as close to real-world conditions as possible in a lab while ensuring accuracy and repeatability.

Each transaction consisted of a single HTTP GET request, and there were no transaction delays (i.e., the web server responded immediately to all requests). All packets contained valid payload (a mix of binary and ASCII objects) and address data. This test provided an excellent representation of a live network (albeit one biased towards HTTP traffic) at various network loads. For the application average response time, test traffic was passed across the infrastructure switches and through all inline port pairs of the device simultaneously (the basic infrastructure latency was known and constant throughout the tests). The figures below show how each product performed in Connections per Second (CPS) and Megabits per second (Mbps), respectively.



	2.7 KB Response	6.4 KB Response	13.5 KB Response	28.0 KB Response	57.4 KB Response	115.6 KB Response
Check Point	40,132	34,076	31,272	19,751	15,702	5,735
Cisco	19,510	17,151	13,774	10,063	6,568	3,981
Forcepoint	76,520	66,613	61,107	48,888	37,485	26,123
Fortinet	67,986	55,890	42,400	24,695	14,100	7,780
Juniper Networks	63,850	56,010	43,511	29,123	19,709	10,741
Palo Alto Networks	12,591	10,971	8,670	6,552	4,980	3,415
Versa Networks	110,185	91,146	74,802	59,555	41,418	27,368

Figure 18 — HTTP Capacity (CPS)



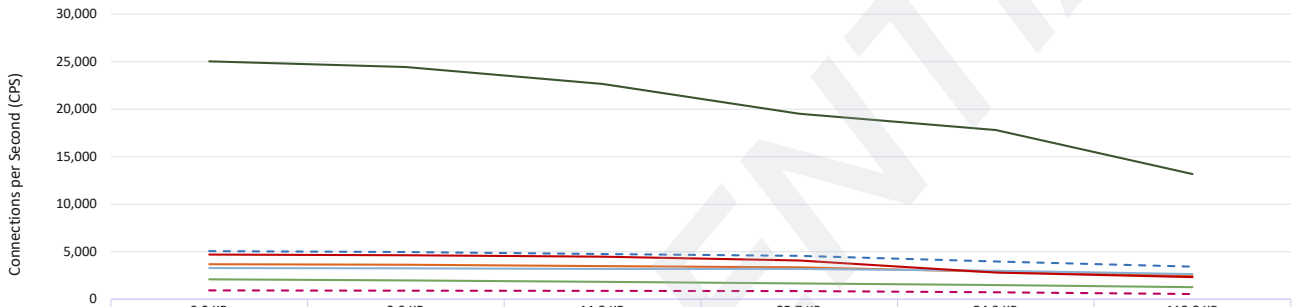
	2.7 KB Response	6.4 KB Response	13.5 KB Response	28.0 KB Response	57.4 KB Response	115.6 KB Response
Check Point	1,254	2,130	3,909	4,938	7,851	5,735
Cisco	610	1,072	1,722	2,516	3,284	3,981
Forcepoint	2,391	4,163	7,638	12,222	18,743	26,123
Fortinet	2,125	3,493	5,300	6,174	7,050	7,780
Juniper Networks	1,995	3,501	5,439	7,281	9,855	10,741
Palo Alto Networks	393	686	1,084	1,638	2,490	3,415
Versa Networks	3,443	5,697	9,350	14,889	20,709	27,368

Figure 19 — HTTP Capacity (Mbps)

HTTPS Capacity

The goal of the HTTPS Capacity test was to stress the HTTPS engine and determine how the device coped with network loads of varying average packet sizes and connections per second.

By creating session-based traffic with varying session lengths, the device was forced to track valid TCP sessions, ensuring a higher workload than simple packet-based background traffic. Encrypting the traffic using TLS/SSL with different algorithms forced the device to decrypt traffic before inspection, increasing the workload further. Tests were performed similarly to HTTP with one HTTPS transaction per connection. Testing determined the maximum rate the firewall was able to process HTTPS traffic of various sizes and its efficiency at forwarding packets quickly to provide the highest level of network performance with the lowest latency. The results were recorded at each response size at a load level of 95% of the maximum throughput, just before latency increased (indicating that the throughput was not sustainable).

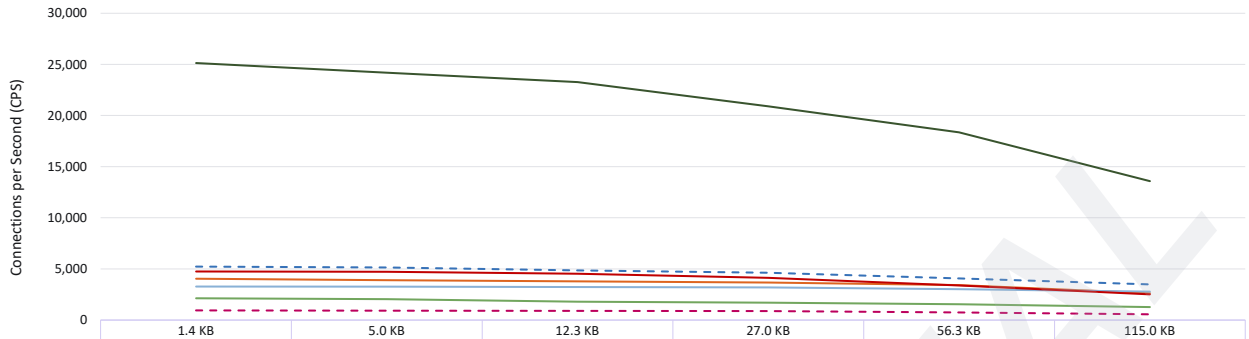


	0.2 KB Response	3.9 KB Response	11.2 KB Response	25.7 KB Response	54.9 KB Response	113.8 KB Response
Check Point	3,671	3,625	3,478	3,354	2,880	2,445
Cisco	920	883	869	847	718	535
Forcepoint	3,267	3,246	3,190	3,179	2,986	2,631
Fortinet	4,703	4,630	4,475	4,073	2,795	2,320
Juniper Networks	5,055	4,969	4,744	4,550	3,960	3,423
Palo Alto Networks	2,094	1,983	1,816	1,666	1,483	1,255
Versa Networks	25,024	24,442	22,650	19,524	17,805	13,173

Figure 20 — HTTPS Capacity [TLS_AES_256_GCM_SHA384 (0x13, 0x02)] (CPS)

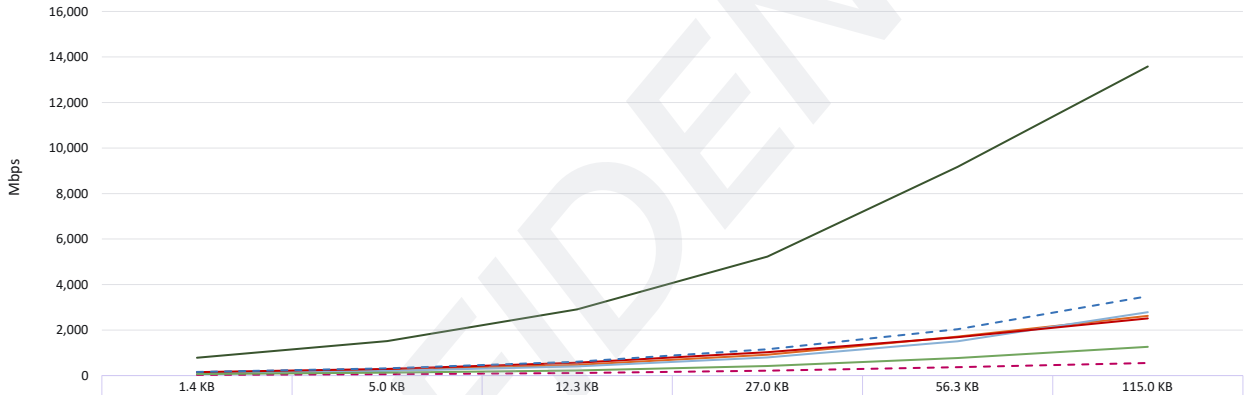
	0.2 KB Response	3.9 KB Response	11.2 KB Response	25.7 KB Response	54.9 KB Response	113.8 KB Response
Check Point	115	227	435	838	1,440	2,445
Cisco	29	55	109	212	359	535
Forcepoint	102	203	399	795	1,493	2,631
Fortinet	147	289	559	1,018	1,398	2,320
Juniper Networks	158	311	593	1,138	1,980	3,423
Palo Alto Networks	65	124	227	417	742	1,255
Versa Networks	782	1,528	2,831	4,881	8,903	13,173

Figure 21 — HTTPS Capacity [TLS_AES_256_GCM_SHA384 (0x13, 0x02)] (Mbps)



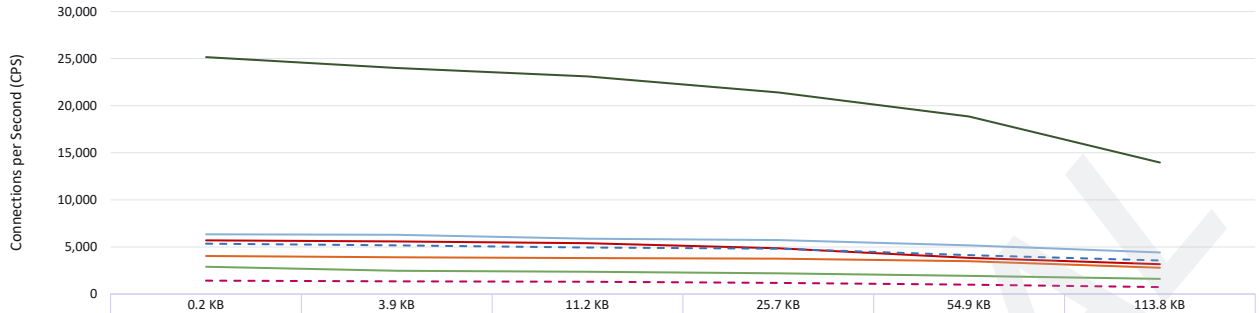
	1.4 KB Response	5.0 KB Response	12.3 KB Response	27.0 KB Response	56.3 KB Response	115.0 KB Response
Check Point	4,036	3,898	3,790	3,667	3,417	2,625
Cisco	938	918	886	866	734	554
Forcepoint	3,283	3,262	3,222	3,194	3,009	2,784
Fortinet	4,754	4,711	4,522	4,124	3,376	2,512
Juniper Networks	5,227	5,137	4,852	4,622	4,078	3,491
Palo Alto Networks	2,128	2,034	1,800	1,695	1,542	1,265
Versa Networks	25,137	24,186	23,267	20,899	18,351	13,586

Figure 22 — HTTPS Capacity for TLS 1.3 (TLS_AES_128_GCM_SHA256 [0x13, 0x01]) (CPS)



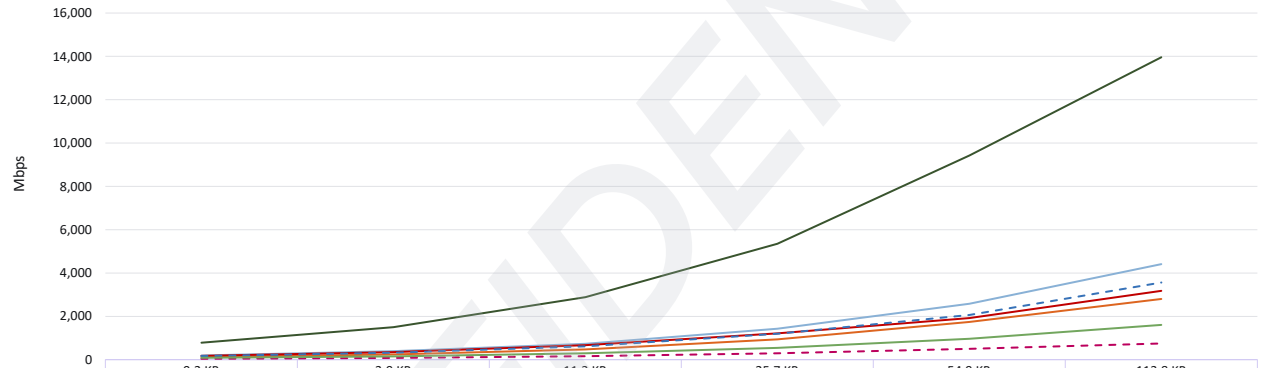
	1.4 KB Response	5.0 KB Response	12.3 KB Response	27.0 KB Response	56.3 KB Response	115.0 KB Response
Check Point	126	244	474	917	1,709	2,625
Cisco	29	57	111	217	367	554
Forcepoint	103	204	403	798	1,504	2,784
Fortinet	149	294	565	1,031	1,688	2,512
Juniper Networks	163	321	607	1,156	2,039	3,491
Palo Alto Networks	67	127	225	424	771	1,265
Versa Networks	786	1,512	2,908	5,225	9,176	13,586

Figure 23 — HTTPS Capacity for TLS 1.3 (TLS_AES_128_GCM_SHA256 [0x13, 0x01]) (Mbps)



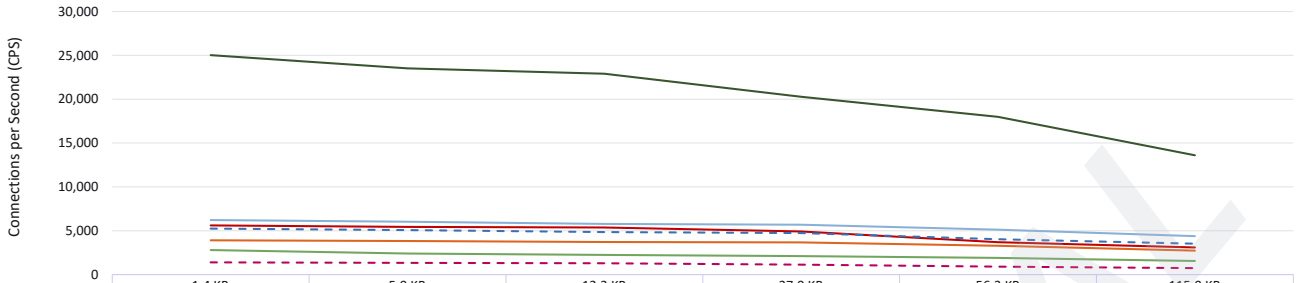
	0.2 KB Response	3.9 KB Response	11.2 KB Response	25.7 KB Response	54.9 KB Response	113.8 KB Response
Check Point	4,050	3,910	3,824	3,760	3,490	2,800
Cisco	1,434	1,354	1,313	1,191	998	747
Forcepoint	6,338	6,292	5,869	5,735	5,163	4,407
Fortinet	5,694	5,581	5,398	4,850	3,847	3,175
Juniper Networks	5,338	5,171	4,942	4,810	4,133	3,559
Palo Alto Networks	2,900	2,470	2,365	2,200	1,935	1,607
Versa Networks	25,145	23,984	23,093	21,393	18,849	13,960

Figure 24 — HTTPS Capacity for TLS 1.2 (TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 [0xC0, 0x2F]) (CPS)



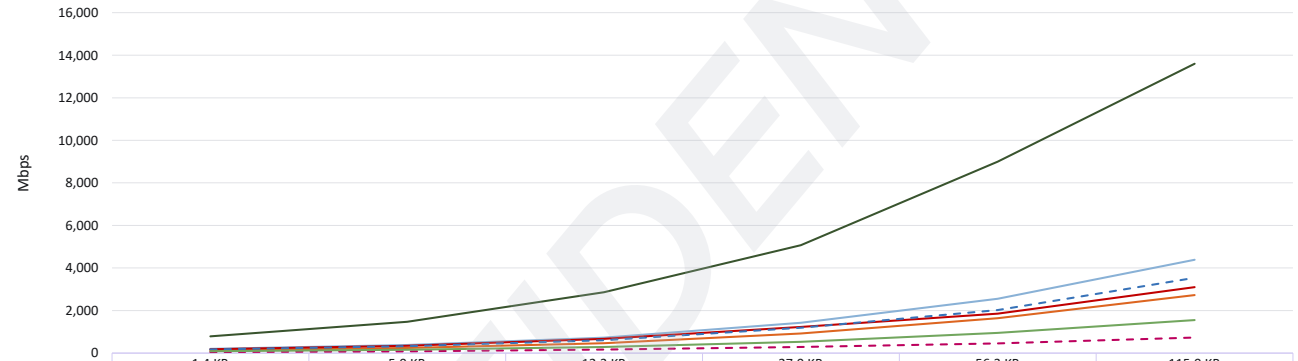
	0.2 KB Response	3.9 KB Response	11.2 KB Response	25.7 KB Response	54.9 KB Response	113.8 KB Response
Check Point	127	244	478	940	1,745	2,800
Cisco	45	85	164	298	499	747
Forcepoint	198	393	734	1,434	2,582	4,407
Fortinet	178	349	675	1,213	1,924	3,175
Juniper Networks	167	323	618	1,203	2,067	3,559
Palo Alto Networks	91	154	296	550	968	1,607
Versa Networks	786	1,499	2,887	5,348	9,425	13,960

Figure 25 — HTTPS Capacity for TLS 1.2 (TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 [0xC0, 0x2F]) (Mbps)



	1.4 KB Response	5.0 KB Response	12.3 KB Response	27.0 KB Response	56.3 KB Response	115.0 KB Response
Check Point	3,914	3,826	3,721	3,674	3,277	2,722
Cisco	1,398	1,325	1,280	1,139	903	730
Forcepoint	6,206	6,015	5,782	5,694	5,109	4,383
Fortinet	5,610	5,445	5,358	4,906	3,700	3,098
Juniper Networks	5,246	5,080	4,841	4,743	4,031	3,532
Palo Alto Networks	2,800	2,400	2,238	2,100	1,900	1,552
Versa Networks	25,017	23,517	22,906	20,265	17,994	13,600

Figure 26 — HTTPS Capacity for TLS 1.2 (TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 [0xC0, 0x30]) (CPS)



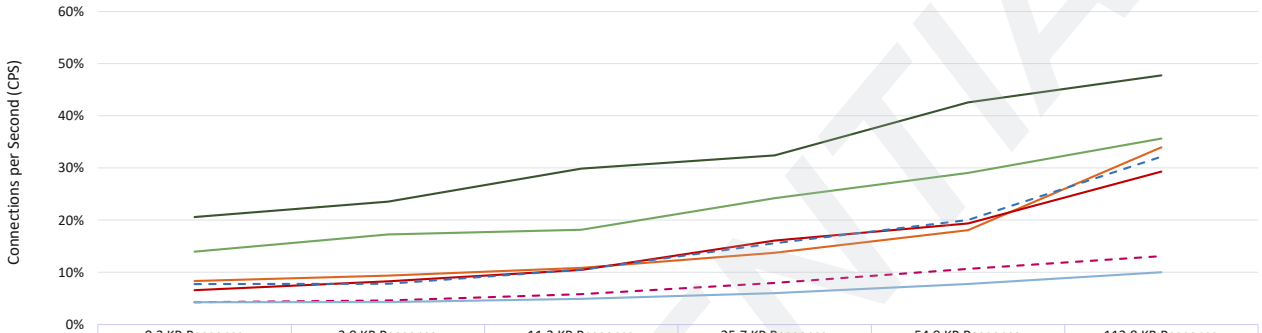
	1.4 KB Response	5.0 KB Response	12.3 KB Response	27.0 KB Response	56.3 KB Response	115.0 KB Response
Check Point	122	239	465	918	1,638	2,722
Cisco	44	83	160	285	452	730
Forcepoint	194	376	723	1,424	2,555	4,383
Fortinet	175	340	670	1,226	1,850	3,098
Juniper Networks	164	318	605	1,186	2,016	3,532
Palo Alto Networks	88	150	280	525	950	1,552
Versa Networks	782	1,470	2,863	5,066	8,997	13,600

Figure 27 — HTTPS Capacity for TLS 1.2 (TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 [0xC0, 0x30]) (Mbps)

Efficiency of HTTPS vs. HTTP Capacity and Throughput

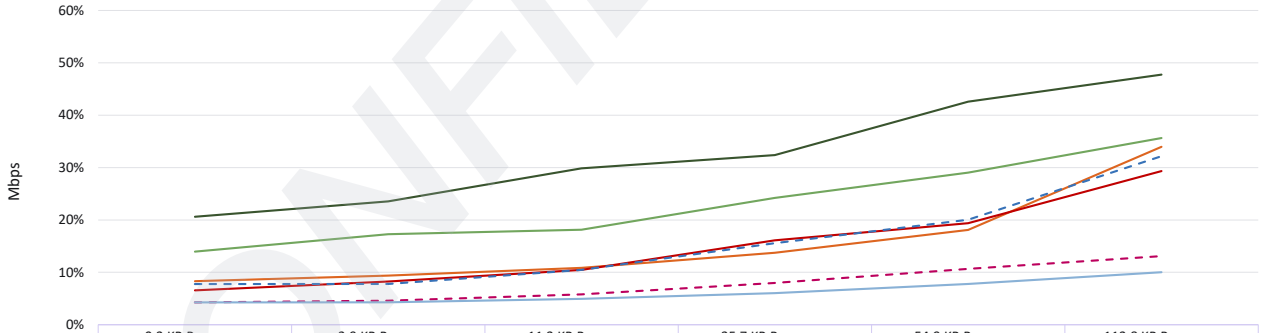
These tests examined the impact of encryption overhead on network performance. Specifically, we measured how TLS/SSL encryption affected bandwidth for different payload sizes and how payload size influenced overall efficiency.

These tests compared unencrypted HTTP traffic against encrypted HTTPS traffic using TLS 1.3 (TLS_AES_256_GCM_SHA384 [0x13, 0x02]). Each test transaction consisted of a single HTTPS GET request with no delays—the web server responded immediately to every request. All traffic carried valid payloads, ensuring that results reflected realistic network conditions.



	0.2 KB Response	3.9 KB Response	11.2 KB Response	25.7 KB Response	54.9 KB Response	113.8 KB Response
Check Point	8%	9%	11%	14%	18%	34%
Cisco	4%	5%	6%	8%	11%	13%
Forcepoint	4%	4%	5%	6%	8%	10%
Fortinet	7%	8%	10%	16%	19%	29%
Juniper Networks	8%	8%	10%	16%	20%	32%
Palo Alto Networks	14%	17%	18%	24%	29%	36%
Versa Networks	21%	24%	30%	32%	43%	48%

Figure 28 — Efficiency of HTTPS vs HTTP Capacity & Throughput (CPS)



	0.2 KB Response	3.9 KB Response	11.2 KB Response	25.7 KB Response	54.9 KB Response	113.8 KB Response
Check Point	8%	9%	11%	14%	18%	34%
Cisco	4%	5%	6%	8%	11%	13%
Forcepoint	4%	4%	5%	6%	8%	10%
Fortinet	7%	8%	10%	16%	19%	29%
Juniper Networks	8%	8%	10%	16%	20%	32%
Palo Alto Networks	14%	17%	18%	24%	29%	36%
Versa Networks	21%	24%	30%	32%	43%	48%

Figure 29 — Efficiency of HTTPS vs HTTP Capacity & Throughput (Mbps)

To calculate efficiency, we compared the throughput or connection rates achieved with HTTPS to those achieved with HTTP. Efficiency is defined as the ratio of HTTPS performance to HTTP performance. For example, if HTTP throughput measured 20,000 Mbps and HTTPS throughput using TLS 1.3 measured 16,400 Mbps, efficiency would be 16,400 ÷ 20,000 = 82%. Similarly, if HTTP handled 1,000,000 connections per second and HTTPS handled 780,000 under the same conditions, efficiency would be 78%. These calculations were repeated across different payload sizes, where smaller payloads typically showed higher overhead due to fixed TLS processing costs being distributed over fewer bytes.

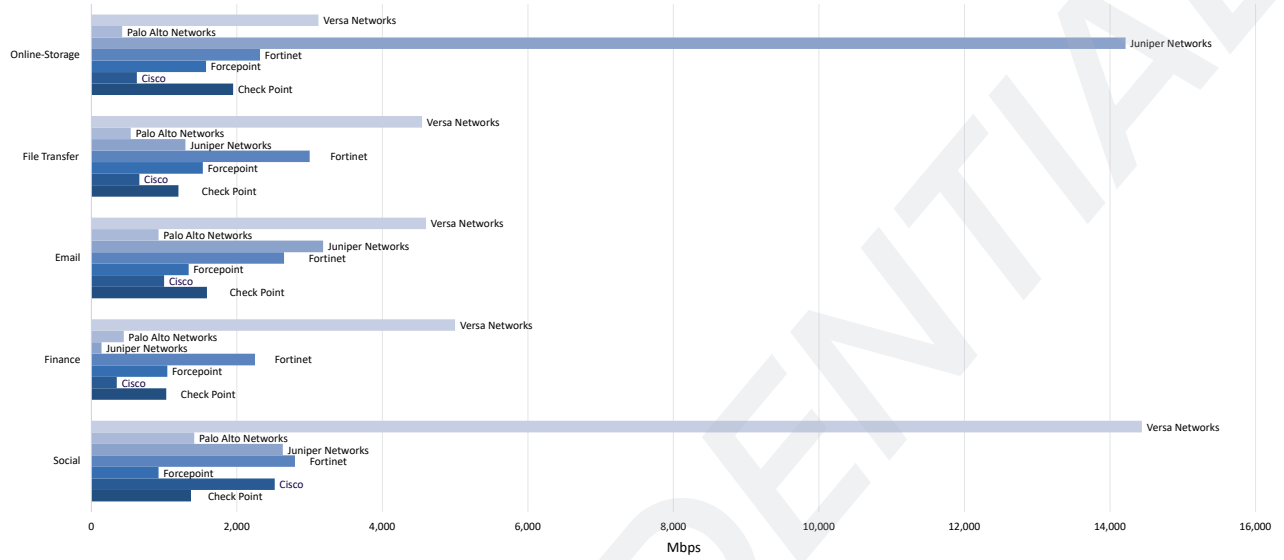


Figure 30 — Real–World Single Application Flows (I)

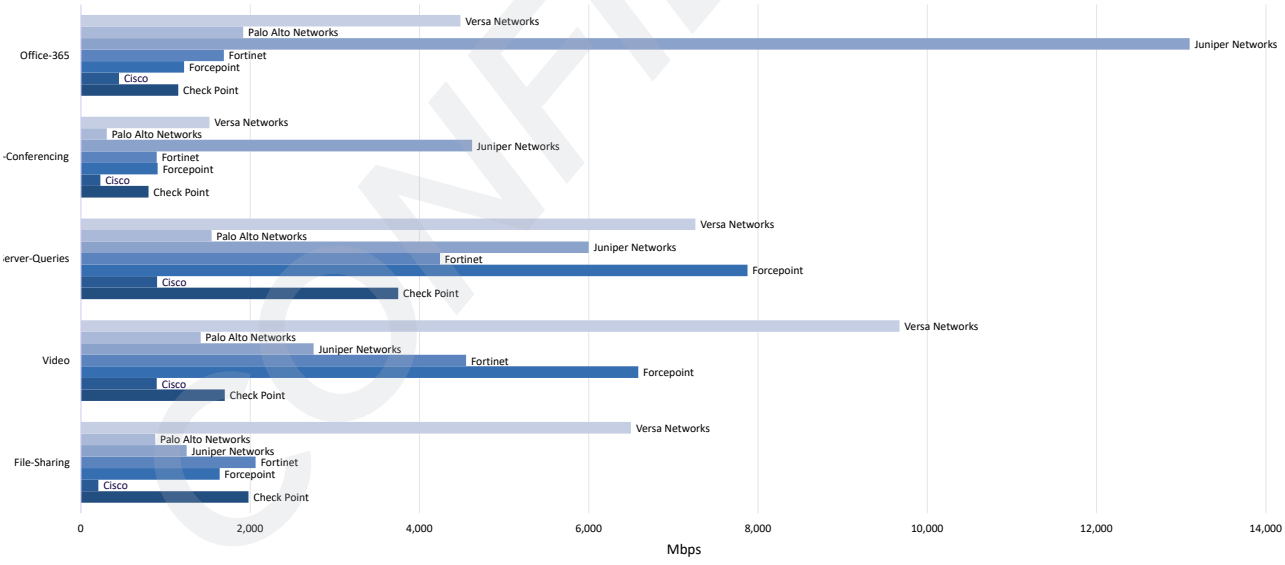
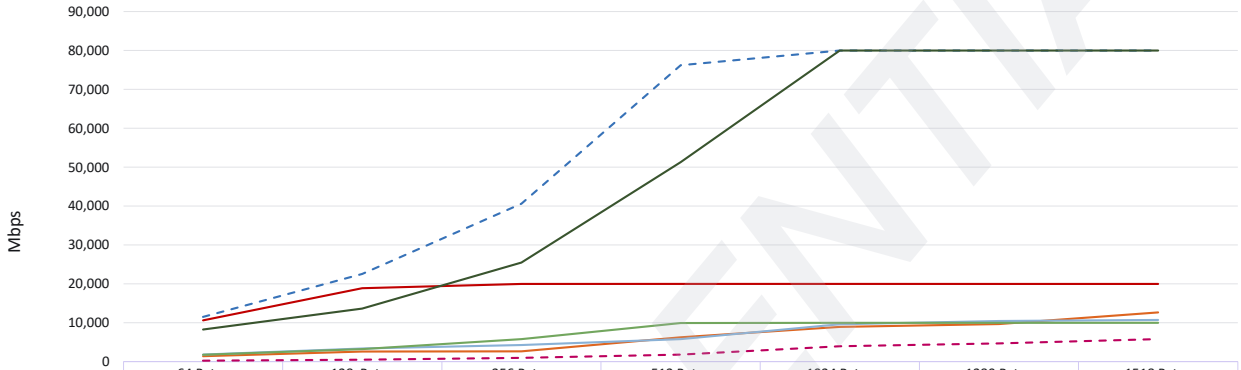


Figure 31 — Real–World Single Application Flows (II)

Raw Packet Processing Performance (UDP Throughput)

This test used UDP packets of varying sizes generated by traffic generation appliances. A constant stream of the appropriate packet size — with variable source and destination IP addresses transmitting from a fixed source port to a fixed destination port — was transmitted bidirectionally through each port pair. Each packet contained dummy data and was targeted at a valid port on a valid IP address on the target subnet. The percentage load and frames per second (fps) figures across each inline port pair were verified by network monitoring tools before each test began. Multiple tests were run, and averages were taken where necessary.

This traffic was not designed to replicate real-world network conditions. The test adheres to RFC 2544 specifications and does not aim to emulate typical network traffic patterns.



	64 Bytes	128 Bytes	256 Bytes	512 Bytes	1024 Bytes	1280 Bytes	1518 Bytes
Check Point	1,423	2,595	2,667	6,244	8,937	9,655	12,637
Cisco	277	520	988	1,788	3,952	4,691	5,822
Forcepoint	1,804	3,381	4,268	5,808	9,606	10,460	10,715
Fortinet	10,620	18,855	20,000	20,000	20,000	20,000	20,000
Juniper Networks	11,496	22,534	40,613	76,212	80,000	80,000	80,000
Palo Alto Networks	1,776	3,217	5,800	9,925	9,961	9,969	9,973
Versa Networks	8,235	13,654	25,477	51,294	80,000	80,000	80,000

Figure 32 — Real–World Single Application Flows (II)

Stability & Reliability

Long-term stability is essential for a firewall, where failure can produce network outages. These tests verified the firewall's stability while maintaining security effectiveness under normal load passing malicious traffic. A firewall that could not sustain legitimate traffic (or that crashed) while under hostile attack would not pass. The product was required to remain operational and stable throughout these tests and to block 100% of previously blocked traffic, raising an alert for each. If any policy-forbidden traffic was passed, due to either the volume of traffic or the product failing open for any reason, this resulted in a failure.

All devices we tested remained operational and stable throughout all these tests and blocked 100% of previously known malicious attacks, raising an alert for each.

Enterprise Firewall	Pass Legitimate Traffic – Normal Load	Drop Traffic – Maximum Exceeded	Blocking with Minimal Load	Blocking Under Load (75% load)
Check Point	Pass	Pass	Pass	Pass
Cisco	Pass	Pass	Pass	Pass
Forcepoint	Pass	Pass	Pass	Pass
Fortinet	Pass	Pass	Pass	Pass
Juniper Networks	Pass	Pass	Pass	Pass
Palo Alto Networks	Pass	Pass	Pass	Pass
Versa Networks	Pass	Pass	Pass	Pass

Figure 33 — Stability & Reliability (I)

Enterprise Firewall	Attack Detection/Blocking – Normal Load (50% load)	State Preservation – Normal Load (50% load)	State Preservation – Maximum Exceeded
Check Point	Pass	Pass	Pass
Cisco	Pass	Pass	Pass
Forcepoint	Pass	Pass	Pass
Fortinet	Pass	Pass	Pass
Juniper Networks	Pass	Pass	Pass
Palo Alto Networks	Pass	Pass	Pass
Versa Networks	Pass	Pass	Pass

Figure 34 — Stability & Reliability (II)

Price

Security, performance, and cost must be considered to understand the true total cost of ownership. Prices may vary due to several factors, including vendor promotions, enterprise renewal agreements, multi-year discounts, and competitive bids.

Enterprise Firewall	Purchase Price	24/7 Support	1-Year	Total Cost (3-Years)
Check Point*	$32,176.90	$3,045.34	$35,222.24	$41,312.93
Cisco[8]	$16,066.29	$6,285.66	$22,351.95	$34,923.27
Forcepoint*	$18,670.50	$6,967.35	$25,637.85	$39,572.55
Fortinet*	$8,184 (3 Year Bundle)	Included	$8,184.00	$8,184.00
Juniper Networks*	$160,000.00	$22,400.00	$76,320.00	$114,742.00
Palo Alto Networks*	$7,496.25	$5,625.00	$13,121.25	$24,371.25
Versa Networks*	$25,000.00	$11,348.00	$36,348.00	$59,044.00

Figure 35 — Price

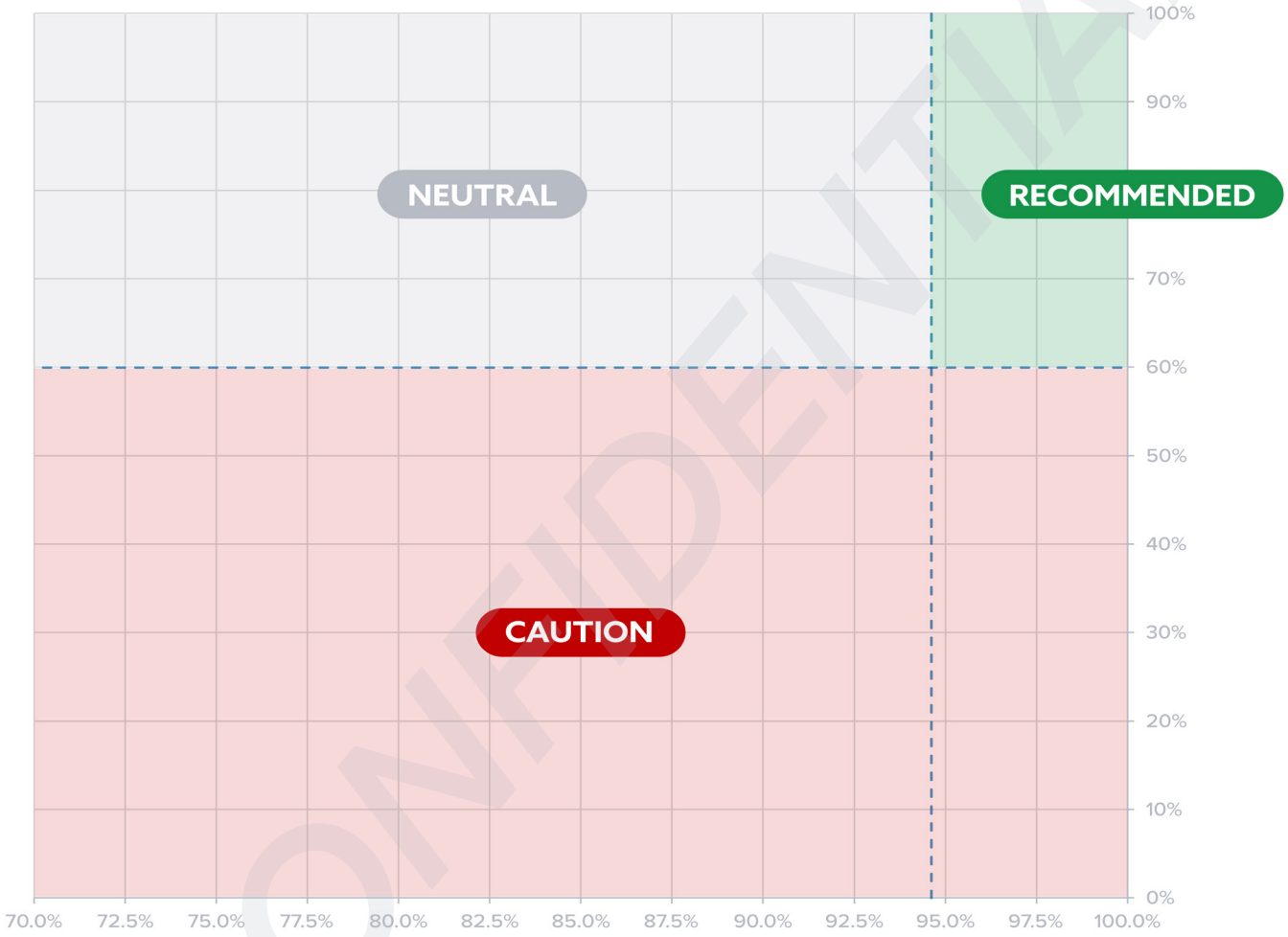
This pricing data (*) was verified by the vendor.

8 Cisco's price was collected from the following sources: https://www.secureitstore.com/firepower-2130.asp, https://www.cdw.com/product/cisco-threat-defense-threat-protection-subscription-license-3-years-1/4565414, https://www.zones.com/site/product/index.html?id=109390457

How We Rate Firewall Products

The Comparative Security Map (CSM) captures the value of the Enterprise Firewall products using Security Effectiveness and False Positive Accuracy.

The Comparative Security Map (CSM) assesses Enterprise Firewall products based on Security Effectiveness and False Positive Accuracy.



The x-axis of the CSM shows False Positive Accuracy as a percentage, increasing from left to right. Products with higher false positive rates are positioned towards the left. The y-axis displays Security Effectiveness, increasing from bottom to top. Products lacking in critical security capabilities are placed lower on this axis. The two dashed lines on the CSM represent the average Security Effectiveness and False Positive Accuracy across all evaluated products.

Products' positions on the CSM determine their ratings:

Recommended: Products with high Security Effectiveness and False Positive Accuracy, exceeding the group averages, are positioned in the upper right section of the CSM. These products offer an excellent level of detection, earning the highest rating assigned by NSS Labs. This rating is an affirmation of the product's strong capacity to meet its commitments to consumers.

Neutral: Products in this category are less capable than Recommended ones but can still be suitable for organizations that can tolerate a slightly higher level of false positives. They remain acceptable for some use cases.

Caution: Products with below-average Security Effectiveness should be reviewed for potential alternatives. End users of these products should consider seeking other solutions.

NSS Labs provides independent, objective ratings of security product efficacy through our research and testing programs. NSS Labs is not pay-to-play. No vendor provided payment or compensation for inclusion or to influence the outcome of this test.

Special Thanks

We want to issue a special thank you to Keysight for providing their CyPerf tool for us to test the security, performance, TLS functionality, and stability of Enterprise Firewall.

Authors

Thomas Skybakmoen, Ahmed Basheer, Tim Otto, Edsel Valle

Contact Information

CyberRatings.org

515 South Capital of Texas Highway

Suite 225

Austin, TX 78746

info@cyberratings.org

www.cyberratings.org