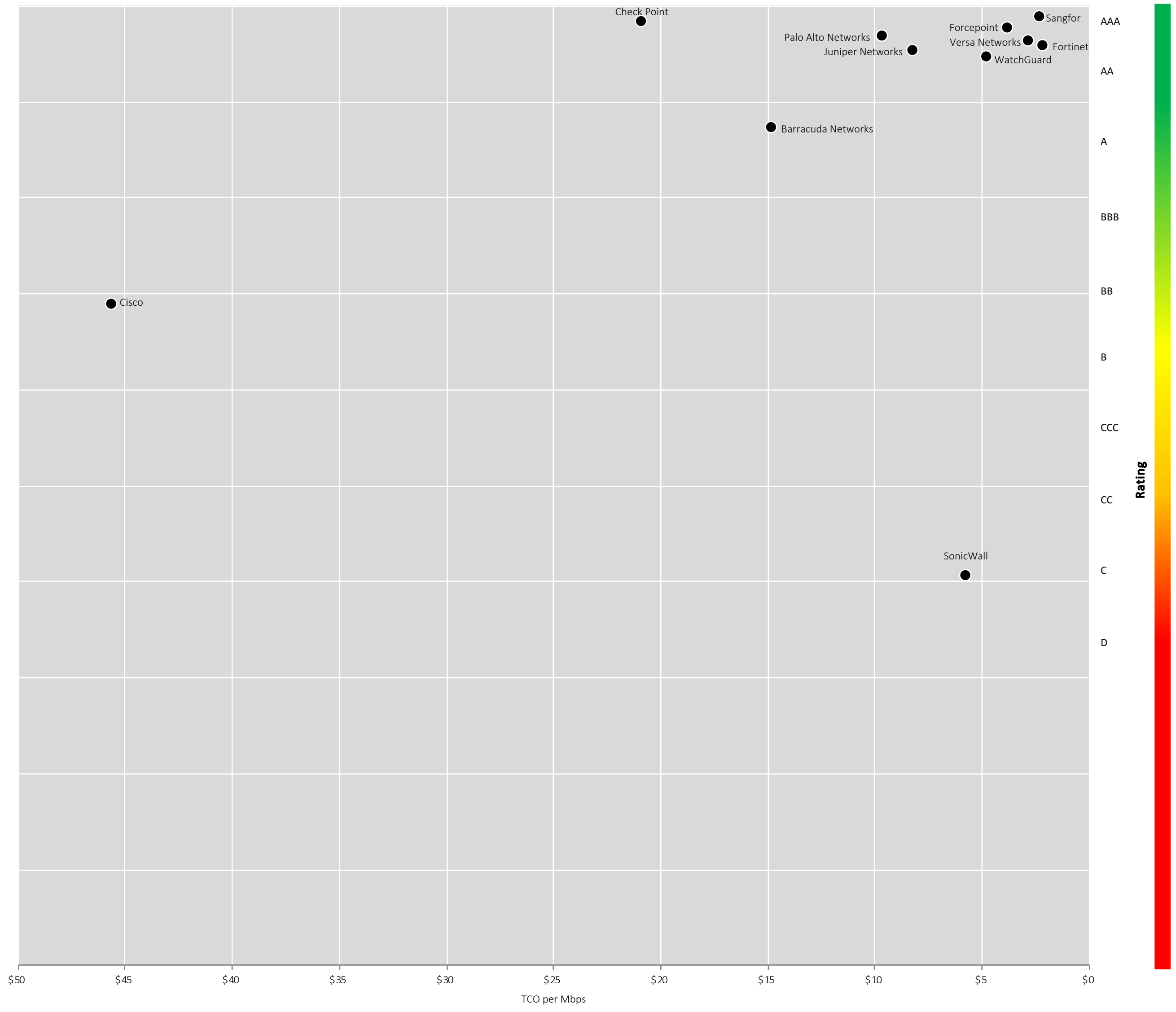
2021 Enterprise Firewall Ratings Chart™



Summary of Results

Enterprise Firewall	Rating	Management	Security Effectiveness	SSL/TLS Functionality	Customer Feedback
Barracuda Networks	A	A	AA	AAA	A
Check Point	AAA	AAA	AAA	AAA	AA
Cisco	BB	A	BBB	-	B
Forcepoint	AAA	AAA	AAA	AAA	AA
Fortinet	AA	AA	AAA	AAA	AA
Juniper Networks	AA	AA	AAA	AA	A
Palo Alto Networks	AAA	AAA	AAA	AA	AA
Sangfor	AAA	AA	AAA	AA	AAA
SonicWALL	C	N/A	N/A	N/A	A
Versa Networks	AA	AA	AA	AAA	AAA
WatchGuard	AA	AA	AA	AA	AA

Key Findings

- Most products did well. Security Effectiveness has improved for most products over the last few years.
- Encryption matters. Roughly 75% of web traffic is encrypted.
- Firewalls cannot see / will not block attacks that are delivered via (encrypted) HTTPS unless they are configured to do so.
- TLS / HTTPS performance was on average 46.9% of clear text performance; best was 74.7% and lowest was 21.2%.
- Most products offered support for all the top/emerging cipher suites; however, some have opted not to provide support ciphers with known vulnerabilities, albeit used/popular. Individual Product Rating reports offer a breakdown of supported ciphers.
- Supply Chain attacks are on the rise; APIs, code reuse, open-source libraries, not maintained code, and other shared resources introduce unknown risk if they are not proactively identified. Software Bill of Materials (SBOM) has been introduced as a solution.

Recommendations

- Plan deployments using rated *encrypted* throughput, not just clear text.
- Existing firewall deployments should enable TLS/HTTPS decryption features whenever possible; and prioritize upgrading equipment when not.
- Update firewall software and signatures regularly. New versions of software often have code/capabilities that signatures rely on.
- Keep an eye on vendor/product performance (security, throughput, etc.) after purchasing. Most products slip at some point, but you don't want to find out the hard way.
- Focus on value-added use cases that support your priorities; don't let vendors drive your agenda.
- Select a vendor that maintains an SBOM. That way, you know they can supply it if the need should arise.

Introduction

Consumers no longer buy a security offering (such as a firewall or an antivirus) as a static product. Most modern cybersecurity products rely on some form of cloud services that provide ongoing protection. As a result, consumers are purchasing a product, plus a vendor's commitment of continuing protection in the future.

CyberRatings.org is a member organization dedicated to quantifying cyber risk and providing transparency on cybersecurity product efficacy through testing and ratings programs.

Ratings are expert opinions: forward looking guidance on a product’s ability to meet future commitments to customers and is based on multiple factors including technology and business leadership, employee turnover, customer satisfaction, financial strength, test results, and market conditions. Test results included security effectiveness, performance, SSL/TLS functionality, management, and customer feedback.

> *Please see the Ratings Matrix at the end of this document for details of what each rating means. Detailed findings for each product can be found in the Product Rating reports within the CyberRatings.org Library.*

Enterprise Firewall Ratings

The rating is calculated using a scale that ranges from 0 to 800, based upon: *Security Effectiveness, Performance, SSL/TLS functionality, Management, Customer Feedback,* and *Cost.*

Rating	Min	Max
AAA	775	800
AA	720	774
A	660	719
BBB	590	659
BB	540	589
B	480	539
CCC	420	479
CC	360	419
C	300	359
D	0	299

CyberRatings.org’s sole objective is to provide accurate information to the market. To that end, prior to publication, CyberRatings shared test results with all vendors, including SonicWALL; SonicWALL did not dispute the findings. However, after publication, SonicWALL’s general counsel demanded test results to be removed, claiming NSS Labs did not have the right to sell the test data to CyberRatings. From our perspective this is a legal technicality, which may or may not be true. Regardless, we do not want to be in the middle of a dispute between NSS Labs and SonicWALL. We have therefore removed the NSS Labs data and any findings that were based upon the NSS Labs data regarding SonicWALL.

SonicWALL’s attempt to suppress independent test results are surprising and troubling. Consumers will have to decide for themselves whether or not SonicWALL’s behavior is acceptable. CyberRatings.org has decided out of an abundance of caution, to issue SonicWALL a ‘C’ rating.

Security Effectiveness

Security Effectiveness tests verified how effectively the firewall protected control network access, applications, and users while preventing threats (exploits, malware, phishing, evasions, etc.) and remained resistant to false positives.

Security Effectiveness = Exploits x Evasions x Stability & Reliability

Product	Rating	Security Effectiveness
Barracuda Networks	AA	90.4%
Check Point	AAA	99.0%
Cisco	BBB	70.4%
Forcepoint	AAA	99.1%
Fortinet	AAA	97.6%
Juniper Networks	AAA	99.5%
Palo Alto Networks	AAA	97.6%
Sangfor	AAA	99.7%
SonicWALL	N/A	N/A
Versa Networks	AA	96.7%
WatchGuard	AA	96.4%

Exploit Block Rate

A total of 2,331 exploits were tested. All of the live exploits and payloads in the exploit test were validated in our lab such that one or more of the following was true: a reverse shell was returned; a bind shell was opened on the target allowing the attacker to execute arbitrary commands; arbitrary code was executed; a malicious payload was installed, or a system was rendered unresponsive.

Resistance to Evasion Techniques

A total of 264 evasions were tested. Evasions are a means of disguising and modifying attacks at the point of delivery to avoid detection and blocking by security products. Failure of a security device to correctly identify a specific type of evasion potentially allows an attacker to use an entire class of exploits for which the device is assumed to have protection. This can render the device virtually useless. Many of the techniques used in this test have been widely known for years and should be considered minimum requirements for the enterprise firewall product category.

Product	Exploits	Evasions
Barracuda Networks	90.7%	99.6%
Check Point	99.0%	100.0%
Cisco	88.9%	79.2%
Forcepoint	99.1%	100.0%
Fortinet	97.6%	100.0%
Juniper Networks	99.5%	100.0%
Palo Alto Networks	97.6%	100.0%
Sangfor	99.7%	100.0%
SonicWALL	N/A	N/A
Versa Networks	96.7%	100.0%
WatchGuard	96.4%	100.0%

Stability and Reliability

All the products passed the stability and reliability tests. Long-term stability is essential for an inline device, where failure can produce a network outage; we verified that the devices could block malicious traffic while under extended load. A product unable to sustain legitimate traffic while under load would have failed the test.

All the devices remained operational and stable throughout all these tests and blocked 100% of previously known malicious attacks, raising an alert for each. If any non-allowed traffic had passed successfully, caused either by the volume of traffic or by the device failing open for any reason, it would have failed the test.

For additional details, please see the individual Product Rating reports.

SSL/TLS Functionality

Product	SSL/TLS Functionality
Barracuda Networks	AAA
Check Point	AAA
Cisco	N/A
Forcepoint	AAA
Fortinet	AAA
Juniper Networks	AA
Palo Alto Networks	AA
Sangfor	AA
SonicWALL	N/A
Versa Networks	AAA
WatchGuard	AA

The Internet Security Research Group's *Let's Encrypt* project has been wildly successful, providing digital (server) certificates required to encrypt via SSL/TLS to more than 225 million websites. Over 75% of web traffic is currently encrypted using SSL/TLS, and that number is increasing every day. Unfortunately, attackers started delivering cyber-attacks via those encrypted channels.

Firewalls must decrypt this encrypted traffic to inspect for threats; devices that cannot decrypt traffic are largely useless, limited to inspecting clear-text traffic.

Performance

Product	Plain Text	HTTPS (SSL/TLS)	Rated Mbps
Barracuda Networks	4,738	2,509	3,178
Check Point	8,214	2,611	4,292
Cisco	2,657	-	2,657
Forcepoint	7,943	5,936	6,538
Fortinet	10,548	5,834	7,248
Juniper Networks	11,483	5,159	7,056
Palo Alto Networks	11,425	2,424	5,124
Sangfor	7,486	3,091	4,409
SonicWALL	N/A	N/A	N/A
Versa Networks	9,527	5,367	6,615
WatchGuard	1,908	837	1,158

We performed 24 discrete performance tests with 36 measurements to see if the firewalls performed as expected. While a letter grade is not given for performance, each product has achieved a rated throughput, including encrypted and unencrypted traffic. Details for each product's maximum concurrency, connection rates, transaction rates, throughput, and latency can be found in the individual reports.

Management

We evaluated each centralized management solution across 38 features that highlighted how difficult it was to configure, maintain, and operate (i.e., find information).

The highest-rated products offered robust and standardized logging and reporting formats along with several pre-defined and customizable dashboards and report generators, enabling administrators to create custom reports for outputs in a range of standard formats. Support for role-based access control (RBAC) and comprehensive third-party authentication, two-factor authentication, and token/time-based authentication were also included in the highest rated products. Furthermore, top products provided the administrator the ability to define and save multiple policies. Features such as Inheritance (nested rules), version control, and revision history were fully supported.

Product	Management
Barracuda Networks	A
Check Point	AAA
Cisco	A
Forcepoint	AAA
Fortinet	AA
Juniper Networks	AA
Palo Alto Networks	AAA
Sangfor	AA
SonicWALL	N/A
Versa Networks	AA
WatchGuard	AA

Value

While security effectiveness, SSL/TLS functionality, management, and customer feedback are top of mind, there is almost always a budget to consider. Sophisticated consumers consider not only the price of the product but the total cost of ownership (TCO).

Product	Rated Mbps	TCO (5 Devices + 1 CMS)	TCO / Mbps
Barracuda Networks	3,178	$235,385	$14.82
Check Point	4,292	$448,006	$20.88
Cisco	2,657	$606,043	$45.62
Forcepoint	6,538	$123,796	$3.79
Fortinet	7,248	$77,463	$2.14
Juniper Networks	7,056	$290,739	$8.24
Palo Alto Networks	5,124	$248,250	$9.69
Sangfor	4,409	$51,535	$2.34
SonicWALL	N/A	N/A	N/A
Versa Networks	6,615	$92,715	$2.80
WatchGuard	1,158	$27,765	$4.79

One way to look at value is to think of it within the context of price/performance, or in this case, TCO/Mbps. Using this formula, we can normalize data and account for wide-ranging TCO differences and performance among products.

Value = (TCO / Performance) / Security Effectiveness
= TCO / (Security Effectiveness x Performance)
= TCO / Protected Mbps

Given that this is a security device, a low cost must be viewed within the context of security effectiveness. After all, an inexpensive device that only blocks 10 percent of attacks is not serving the purpose for which it was purchased; there is no value—similarly, performance matters, but not at the expense of security. Therefore, calculating a security device's value requires considering the relationship between price, performance, manageability, and security; we take the TCO/Mbps and divide it by security effectiveness. Using our formula, a device that provides less security, i.e., 50%, will be twice as expensive as a device that offers 100% security.

Product	Security Effectiveness	TCO / Mbps	TCO / Protected Mbps
Barracuda Networks	90.4%	$14.82	$16.39
Check Point	99.0%	$20.88	$21.09
Cisco	70.4%	$45.62	$64.80
Forcepoint	99.1%	$3.79	$3.82
Fortinet	97.6%	$2.14	$2.19
Juniper Networks	99.5%	$8.24	$8.28
Palo Alto Networks	97.6%	$9.69	$9.92
Sangfor	99.7%	$2.34	$2.34
SonicWALL	N/A	N/A	N/A
Versa Networks	96.7%	$2.80	$2.90
WatchGuard	96.4%	$4.79	$4.97

Ratings Matrix

RATING	DEFINITION
AAA	A product rated 'AAA' has the highest rating assigned by CyberRatings.org. The product's capacity to meet its commitments to consumers is extremely strong.
AA	A product rated 'AA' differs from the highest-rated products only to a small degree. The product's capacity to meet its commitments to consumers is very strong.
A	A product rated 'A' is somewhat less capable than higher-rated categories. However, the product's capacity to meet its commitments to consumers is still strong.
BBB	A product rated 'BBB' exhibits adequate stability and reliability. However, previously unseen events and use cases are more likely to negatively impact the product's capacity to meet its commitments to consumers.
	A product rated 'BB,' 'B,' 'CCC,' 'CC,' and 'C' is regarded as having significant risk characteristics. 'BB' indicates the least degree of risk and 'C' the highest. While such products will likely have some specialized capability and features, these may be outweighed by large uncertainties or major exposure to adverse conditions.
BB	A product rated 'BB' is more susceptible to failures than products that have received higher ratings. The product has the capacity to meet its commitments to consumers. However, it faces minor technical limitations that have a potential to be exposed to risks.
B	A product rated 'B' is more susceptible to failures than products rated 'BB'; however, it has the minimum capacity. Adverse conditions will likely expose the product's technical limitations that lead to an inability to meet its commitments to consumers.
CCC	A product rated 'CCC' is susceptible to failures and is dependent upon favorable conditions to perform expected functions. In the event of adverse conditions, the product is not likely to have the capacity to meet its commitments to consumers.
CC	A product rated 'CC' is highly susceptible to failures. The 'CC' rating is used when a failure has not yet occurred, but CyberRatings considers it a virtual certainty.
C	A product rated 'C' is highly susceptible to failures. The product is expected to fail under any abnormal operating conditions and does not offer a useful management systems and logging information compared with products that are rated higher.
D	A product rated 'D' is actively underperforming and failing and does not meet the use-case. The 'D' rating is used when the product is not operational without a major technical overhaul. Unless CyberRatings believes that such technical fixes will be made within a stated grace period (typically 30-90 calendar days), the 'D' rating also is an indicator that existing customers using the product have already experienced a failure and should take immediate action.

Products

Barracuda CloudGen Firewall F800.CCE v8.0.2
Check Point Software Quantum 16000 Security Gateway R80.30
Cisco Firepower 4110 v6.4.0.9
Forcepoint NGFW 2105 V6.8.0
Fortinet FortiGate 600E v6.2.3GA build1066
Juniper Networks SRX4600 v18.4X3.12
Palo Alto Networks PA-5220 PANOS 9.0.6
Sangfor Technologies, Inc. NGAF M5300-F-I AF8.0.8R1
SonicWALL NSA 5650 SonicOS 6.5.4.6
Versa Networks V2000 VOS 21.1.1
WatchGuard Technologies Firebox M670 V12.5.3

Methodology

Enterprise Firewall v1.0

Authors

Thomas Skybakmoen, Vikram Phatak, Ahmed Basheer

Contact Information

CyberRatings.org
2303 Ranch Road 620 South
Suite 160, #501
Austin, TX 78734
info@cyberratings.org
www.cyberratings.org

Please read the disclaimer in this box because it contains important information that binds you. If you do not agree to these conditions, you should not read the rest of this report but should instead return the report immediately to us. “You” or “your” means the person who accesses this report and any entity on whose behalf he/she has obtained this report.

1. The information in this report is subject to change by us without notice, and we disclaim any obligation to update it.
2. The information in this report is believed by us to be accurate and reliable at the time of publication, but is not guaranteed. All use of and reliance on this report are at your sole risk. We are not liable or responsible for any damages, losses, or expenses of any nature whatsoever arising from any error or omission in this report.
3. NO WARRANTIES, EXPRESS OR IMPLIED ARE GIVEN BY US. ALL IMPLIED WARRANTIES, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT, ARE HEREBY DISCLAIMED AND EXCLUDED BY US. IN NO EVENT SHALL WE BE LIABLE FOR ANY DIRECT, CONSEQUENTIAL, INCIDENTAL, PUNITIVE, EXEMPLARY, OR INDIRECT DAMAGES, OR FOR ANY LOSS OF PROFIT, REVENUE, DATA, COMPUTER PROGRAMS, OR OTHER ASSETS, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.
4. This report does not constitute an endorsement, recommendation, or guarantee of any of the products (hardware or software) tested or the hardware and/or software used in testing the products. The testing does not guarantee that there are no errors or defects in the products or that the products will meet your expectations, requirements, needs, or specifications, or that they will operate without interruption.
5. This report does not imply any endorsement, sponsorship, affiliation, or verification by or with any organizations mentioned in this report.
6. All trademarks, service marks, and trade names used in this report are the trademarks, service marks, and trade names of their respective owners.