Competitive Analysis:
Sangfor NGAF VS WatchGuard

www.sangfor.com

SANGFOR

WatchGuard Introduction

01

WatchGuard is a network security vendor with headquarters in Seattle, Washington. Its firewalls have a large SMB client base. The vendor focuses on simplified firewall administration and management and offers mature malware detection features, compared to other SMB-focused vendors.

According to Gartner, “WatchGuard’s firewall product line (Firebox) includes physical and virtual appliances. Firewall models are also available on AWS and Microsoft Azure. Its management suite includes three components: the recently released WatchGuard Cloud, WatchGuard Dimension and WatchGuard System Manager (WSM). WatchGuard Dimension and WatchGuard Cloud are primarily focused on monitoring and reporting. WatchGuard Dimension is available as a virtual instance on-premises or deployed as IaaS, whereas WatchGuard Cloud is delivered as a service. WSM is centralized management software for Firebox appliances and is available only installed on a Windows server. WatchGuard's portfolio also includes wireless access points with integrated security features such as DNS protection and MFA.

WatchGuard offers a range of appliances, from a low-end Firebox T15 model (400 Mbps maximum throughput) up to the Firebox M5600 model (60 Gbps maximum throughput).

In 2019, in addition to WatchGuard Cloud, WatchGuard launched a zero-touch SD-WAN offering and DNSWatch, a recursive DNS service aimed at adding additional web protection to its product lines. The vendor launched IntelligentAV, which adds Cylance as AI-based antivirus protection to supplement the existing Bitdefender antivirus engine. The vendor also released the 12.4 version of its Fireware firmware, adding native TLS 1.3 decryption suppor.t”

WatchGuard Disadvantages

02

Marketing Execution: WatchGuard is not frequently cited on customer evaluation shortlists compared to competitors, and has become much less visible in Gartner client inquiries. WatchGuard is not visible on Asia/Pacific region’s client firewall shortlists.

Market Segmentation: WatchGuard has a full line of appliances supporting very small to medium-high throughput needs, as well as support for virtual and IaaS environments. The vendor has a major presence among SMBs, but lacks a presence in enterprise and data center firewall and public IaaS deployment use cases.

Product: At present, the WatchGuard cloud-based manager only offers reporting and visibility features. It also has a second management interface, the WatchGuard Dimension, with similar limited functionality. WSM, which is available on-premises only, offers mature management capabilities. Customers surveyed for this research expressed concerns about having multiple management consoles.

WatchGuard provides some lightweight DLP capabilities, but does not support ICAP for integration with enterprise DLP solutions. The product also lacks support for some key features desired by enterprise-grade customers, like open API and integration with NAC and SDN support.

Features: The WatchGuard firewall IDPS offering uses a single OEM partner for a signature set with no in-house team focused on writing signatures. In addition, it has no ability to add or customize signatures, does not include the ability to fail open, and lacks behavior analysis.

Offering: WatchGuard does not have a FWaaS offering for extending branch and mobile worker protections, and only offers a partnership with a single CASB vendor, instead of owning or integrating with additional third-party CASB vendors.

Watchguard Missing Critical Capabilities:

- Activity monitoring
- Purpose-built hardware
- Advanced malware capabilities

Performance Rating: The device is rated by NSS at 1,589 Mbps, which is lower than the vendor claimed performance. WatchGuard claims this device runs at 2,400 Mbps.
Low security effectiveness, at 89.1% according to NSS Labs

Sangfor NGAF VS WatchGuard

Sangfor Strengths

1. change to powerful ransomware killing - Effective Ransomware Protection

Ransomware-exposed surface inspection through business asset open port. Ransomware commonly uses vulnerabilities and weak password inspection, leading to surfaces being exposed to ransomware, and requiring specific optimization suggestions.

2. Powerful Ransomware Killing Engine - Sangfor Engine Zero Performance:

IPS

Equipment	Policy	Vulnerability Attack	Vulnerability Blocked	Block Rate
NGAF	Default	34	29	85%
Watchguard	Default	34	27	79%

WAF

Equipment	Policy	Vulnerability Attack	Vulnerability Blocked	Block Rate
NGAF	Default	379	379	100%
Watchguard	Default	379	245	65%

Known Malware

Equipment	Policy	Malware Sample	Malware Blocked	Block Rate
NGAF	Default	300	299	99.67%
Watchguard	Default	300	190	63%

Unknown Malware

Equipment	Policy	Malware Sample	Malware Blocked	Block Rate
NGAF	Default	43	43	100.00%
Watchguard	Default	43	25	58%

3. Sangfor RDP/SMB/SSH slow and distributed brute force protection

4. Ransomware C2 process evidence display

5. Data Center Security:

Least privileged access provides better visibility of production traffic, and reduces the attack surface of critical assets.

6. Strategy Optimization Module:

Policy clean-up, asset discovery and network mapping and policy tracking

7. Cloud-based management:

Platform-X supports device monitoring, unified upgrade, remote password-free login, cloud policy template editing, unified policy issuance, intelligent alarms, report analysis, and serial number unified viewing.

8. Centralized management:

CENTRAL MANAGER

9. Zero-touch deployment & centralized monitoring and management

10. Advanced threat detection relying on cloud, behavior and AI technologies

- Advanced Threat Intelligence
- C&C identification with DGA
- Engine Zero: Advanced malware inspection engine
- Cloud-based sandboxing

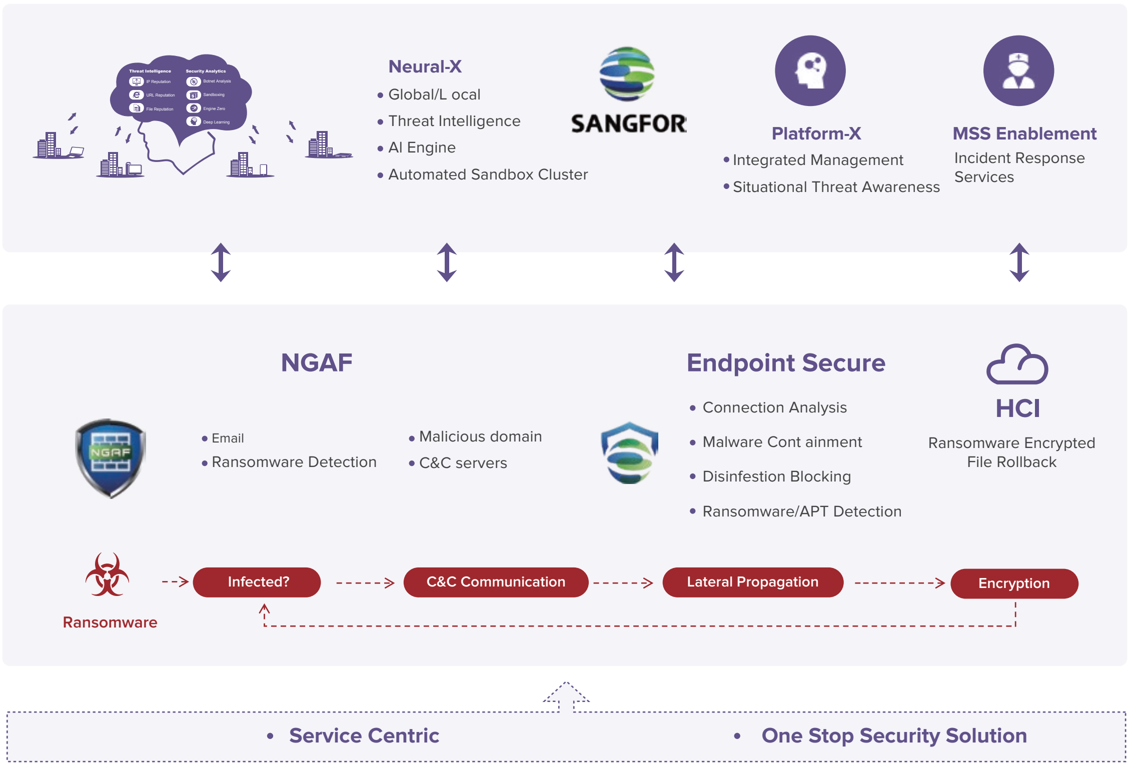
11. Real-time threat detection provides an easy to understand risk score and visibility for enterprises, significantly improving the time to detect and respond.

12. Sangfor NGAF cluster analysis of threat events based on asset perspective

13. Full integration ability covering cloud, network and endpoint

14. For scenarios with multiple zones and firewalls, Sangfor NGAF provides global threat management and visualization through Cyber Command

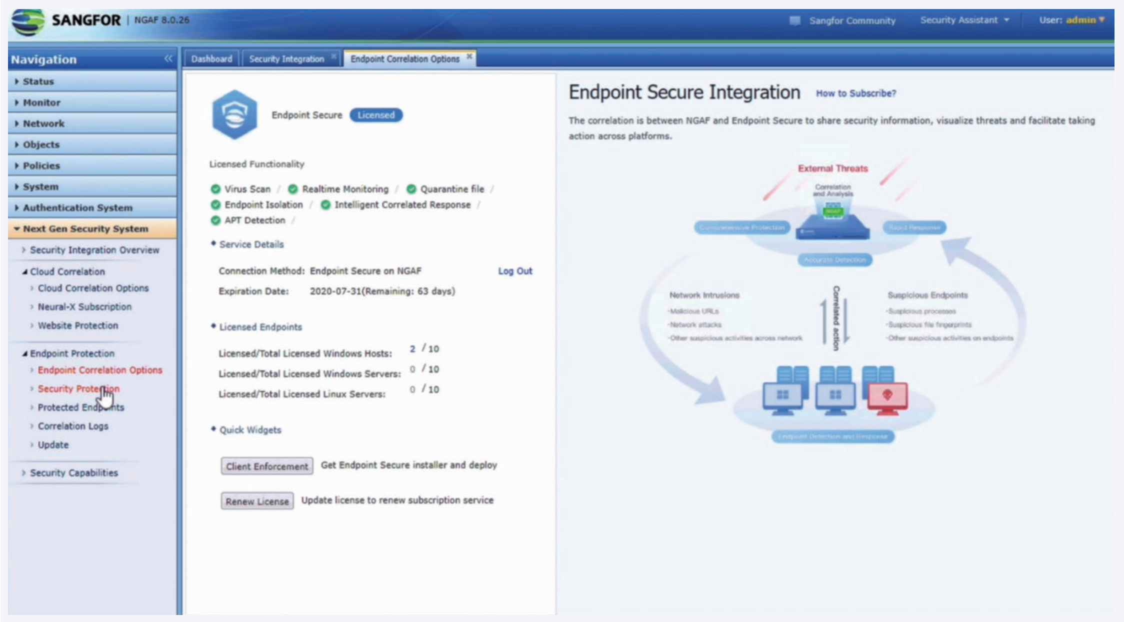
15. Multi-product integration solution



16. Automation between NGAF and ES/Cyber Command

17. Centralized threat correlation between NGAF and ES

Sangfor is the only vendor with comprehensive integrated EDR with firewall, extremely suited to the mid-market, while large enterprises deploy EDR hosted on Platform-X.



Endpoint Secure Licensed

Licensed Functionality

✓ Virus Scan / ✓ Realtime Monitoring / ✓ Quarantine file / ✓ Endpoint Isolation / ✓ Intelligent Correlated Response / ✓ APT Detection /

- Service Details

Connection Method: Endpoint Secure on NGAF Log Out

Expiration Date: 2020-07-31(Remaining: 63 days)

- Licensed Endpoints

Licensed/Total Licensed Windows Hosts: 2 / 10

Licensed/Total Licensed Windows Servers: 0 / 10

Licensed/Total Licensed Linux Servers: 0 / 10

- Quick Widgets

Client Enforcement Get Endpoint Secure installer and deploy

Renew License Update license to renew subscription service

Endpoint Secure Integration How to Subscribe?

The correlation is between NGAF and Endpoint Secure to share security information, visualize threats and facilitate taking action across platforms.

Competitive Comparison 04

● Strong ● Weak

Features	Sangfor	WatchGuard	Sangfor advantages
Security Visibility	●	●	Integrated Security Reporter providing a holistic, end-to-end security overview, from business system to endpoint users and their correlation, detailed visibility.
Total Business System Protection	●	●	Support Application Firewall which includes: Top 10 OWASP Certified, Support web application threat signatures, HTTP Anomalies Detection, Application Hiding, Integrated Web Scanner & Vulnerability Scanner and Integrated Security Reporter
Real Time Detection & Rapid Response	●	●	Automatic protection for pre-attack, mid-attack and post-attack.

● Strong 🟠 Weak

Features	Sangfor	WatchGuard	Sangfor advantages
Known & Unknown Threat Protection	●	●	Sangfor Engine Zero: 1. Supports Machine Learning method to recognize new variants of malware, viruses and ransomware 2. Supports behavior detection methods for new file-based threat 3. Uploads suspicious files to cloud to detect, not including files with private information Sangfor Neural-X: 1. Supports the use of cloud threat intelligence to do Unknown Threat Discovery and Advanced Threat Analytics 2. Suspicious URL/DNS will be detected by Neural-X 3. Professional support 4. Updates Calendar to show upgrade capabilities and trends 5. Shows hot events
Traditional FW	●	●	Sangfor NGAF is compatible with all traditional firewall features, including switching/routing, access control, AA/AS dual-system hot backup, software and hardware bypass, system management, log reporting, session management, anti-DDoS attacks, application proxy, DHCP/ DNS, etc.
IPS	●	●	1. Sangfor supports vulnerability attack protection for server and client, protecting clients from worms, Trojans, spyware, scanning, DoS, DDoS, vulnerability exploits, buffer overflow attacks, abnormal protocol and attacks with evasive tactic employed. 2. Sangfor supports brute-force attack for FTP, IMAP Auth, IMAP Login, IMAP Standard, IMAP Tls, MS Sql2000, MS Sql2008, Mysql, Ntlm, Oracle, POP3 Apop, POP3 Tls, POP3 User, RDP Win8, RDP Winxp, Rlogin, SMB, SMB2, SMTP Auth, SSH, Telnet, VNC Encrypt, VNC Unencrypt, Weblogic; 3. Sangfor supports automatically blocking, logging and upload of gray threat to the "cloud" 4. Detects more than 4000+ signatures 5. The policy can be configured based on src/dst zone, src/dst IP group 6. Sangfor supports TCP evasion detection
Application Control	●	●	Sangfor supports ACL based on source IP/zone, users/groups, dst IP/zone, application, protocol, src/dst port, and schedule; Supports more than 1000 applications, more than 2500 application rules and custom rules It is not recommended to enable log record and persistent connection Supports up to 4096 entries
URL Filter	●	●	Sangfor supports URL filter based on source IP/zone, users/groups, dst IP/zone, URL category and schedule. Support HTTP(get), HTTP(post), HTTPS filter Supports HTTP(S) upload/download file type filter URL and file types can be customized

🟣 Strong 🟠 Weak

Features	Sangfor	WatchGuard	Sangfor advantages
E-mail Security	🟠	🟣	Sangfor mail protection supports detection of mail attachments with viruses, malicious links, XSS attacks, file filters, and collision attacks. Mail whitelist can be added with IP address and email address, with a sender and receiver. Mail protection default detects port 25,110,143, it can support other ports using custom settings.
Anti-ransomware	🟣	🟠	Sangfor Ransomware Protection: Pre-attack: Sangfor provides vulnerability assessment Mid-Attack: Sangfor provides AI-based malware inspection and RDP password brute force inspection Post-Attack - Sangfor provides quick response
Centralized management	🟣	🟠	Sangfor supports joining NGAF device to Central Management platform Sangfor BBC2.5.3 (Central Manager) and being managed through the platform. (a) Push down configurations from Sangfor CENTRAL MANAGER to NGAF devices and management of those configurations on Sangfor CENTRAL MANAGER. (b) NGAF devices can be upgraded via Sangfor CENTRAL MANAGER by importing upgrade package manually or by obtaining upgrade package online. (c) 12 databases on NGAF device can be updated via Sangfor CENTRAL MANAGER, including Sangfor Engine Zero file verification model database, URL database, IPS vulnerability signature database, software update, application signature database, WAF signature database, sensitive keyword database, vulnerability database for RT analytics, IP address database, threat intelligence database, hot threat database and security events database. (d) Support pushing down predefined and custom signature database from Sangfor CENTRAL MANAGER. (e) Security overview, business system and user/group security information can be reported to and displayed on Sangfor CENTRAL MANAGER. (f) Support configuring alarm settings centrally on Sangfor CENTRAL MANAGER platform and reporting alarm configuration from branch devices. (g) Support connecting NGAF device deployed in high availability or cluster environment to Sangfor CENTRAL MANAGER platform for central management. (h) Support 15 predefined zones in Network > Interfaces > Zone.

🟣 Strong 🟠 Weak

Features	Sangfor	WatchGuard	Sangfor advantages
Neural-X (Cloud based TI)	🟣	🟠	Neural-X is a security center with threat intelligence and unknown threat detection capabilities. The threat intelligence center, also a security capability center, gathers masses of intelligence data, including that from Sangfor's on-line security devices, third-party security vendor (such as Virustotal purchase and Google open inquiry) and security communities. The center carries out user granularity analysis for accumulated security intelligence data through big data and cloud computing technology by utilizing various data analysis and artificial intelligence algorithms, and sends real-time intelligence to security devices (such as NGAF, Cyber Command, IAM, ES, and WAF, that have access to Neural-X) by subscription. Security devices load intelligence as required, and carry out detection, analysis and disposition based on intelligence according to their own functions.
Wifi integration protection	🟠	🟣	Sangfor does not support this function at the moment
Product integration	🟣	🟠	Sangfor provides many product integration solutions for different customers. For instance, Firewall + Sangfor Endpoint Secure + Central Manager + Cyber Command + Neural-X, Firewall + Platform-X + Sangfor Endpoint Secure.
Web Application	🟣	🟠	Sangfor Web Application function: 1.Use next generation WAF engine, including traditional SNORT based engine and Semantic engine, defends against the 10 major web-based attacks identified by the Open Web Application Security Project (OWASP) , including SQL injection, XSS and CSRF. 2. Supports restricting suspicious file uploading with asp, asa, exe, jsp, php, aspx, php3, php4, phtml, and vbs file types. 3. Supports application hiding of HTTP error page replacement, HTTP (S) response headers hidden, and FTP server and software version information hidden, etc. 4. Supports CC attack prevention 5. Supports FTP Weak Password Protection, web-access weak password, web-access cleartext request inspection and defense against brute-force attacks 6. Supports performing inspection of content at the perimeter for incoming traffic. Only allow input parameters that conform to the application functionalities required of the web application and no malicious input parameters; 7. Supports HTTP protocol abnormal detection and sHTTP request method filter 8. Supports protect for HTTP attack based on session and cookies 9. Supports more than 3000+ signatures 10. Supports machine learning to learn the business model and reduce false positive for webshell, SQL injection, etc.

● Strong 🟠 Weak

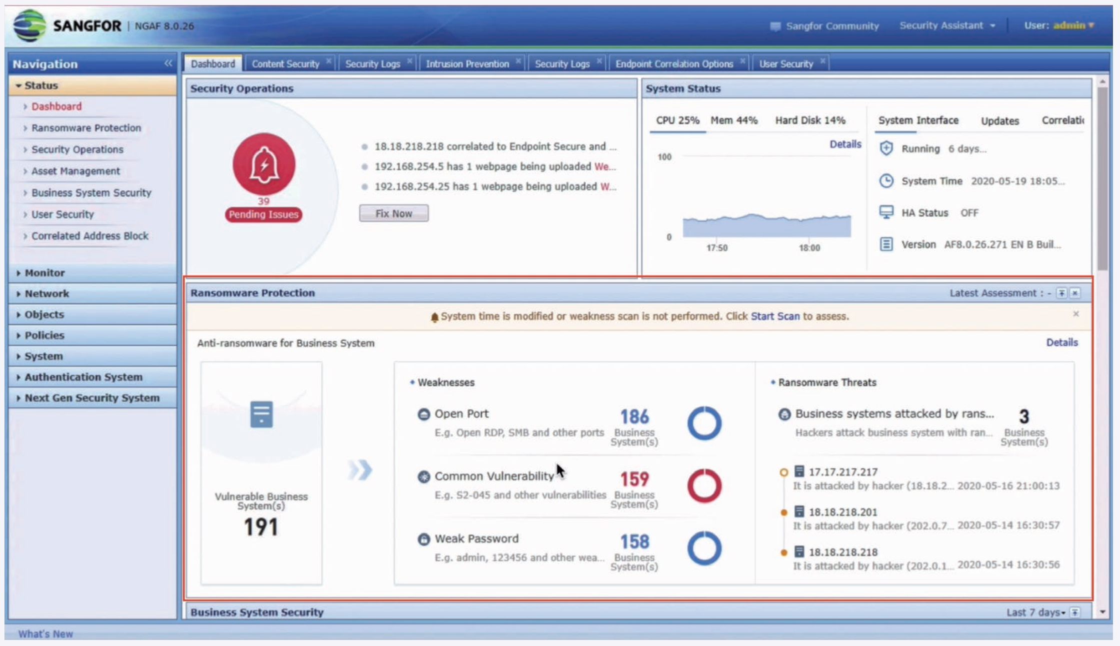
Features	Sangfor	WatchGuard	Sangfor advantages
Reporting & analytics	●	🟠	WatchGuard requires additional reporting tools.
Simplified Security Operation	●	●	User friendly interface minimizes the challenge of misconfiguration of security policies. Intuitive reporting which provides detailed information for management, incident response, as well as daily operations.

Model Comparison 05

NGAF	Threat Prevention Throughput	WatchGuard	Threat Prevention Throughput
M4500	1Gbps	Firebox T35R	325Mbps
M5100	1.2Gbps	Firebox T40	623Mbps
M5200	1.75Gbps	Firebox T80	1.15Gbps
M5300	3.5Gbps	Firebox M370	3.0Gbps
M5400	4.2Gbps	Firebox M470	3.5Gbps
M5500	8.4Gbps	Firebox M570	5.6Gbps
M5500	8.4Gbps	Firebox M670	6.2Gbps
M5600	16.8Gbps	Firebox M4600	9Gbps
M5600	16.8Gbps	Firebox M5600	12Gbps

Sangfor Defeats WatchGuard - Sangfor NGAF Selling Points 06

1. Independent Anti-Ransomware Module



Security Operations

39 Pending Issues

- 18.18.218.218 correlated to Endpoint Secure and ...
- 192.168.254.5 has 1 webpage being uploaded We...
- 192.168.254.25 has 1 webpage being uploaded W...

System Status

Running 6 days...

System Time 2020-05-19 18:05...

HA Status OFF

Version AF8.0.26.271 EN B Buil...

Ransomware Protection

Latest Assessment : -

System time is modified or weakness scan is not performed. Click Start Scan to assess.

Anti-ransomware for Business System

Vulnerable Business System(s) 191

Weaknesses

Open Port 186 Business System(s)
E.g. Open RDP, SMB and other ports

Common Vulnerability 159 Business System(s)
E.g. S2-045 and other vulnerabilities

Weak Password 158 Business System(s)
E.g. admin, 123456 and other wea...

Ransomware Threats

Business systems attacked by rans... 3 Business System(s)
Hackers attack business system with ran...

17.17.217.217
It is attacked by hacker (18.18.2... 2020-05-16 21:00:13

18.18.218.201
It is attacked by hacker (202.0.7... 2020-05-14 16:30:57

18.18.218.218
It is attacked by hacker (202.0.1... 2020-05-14 16:30:56

Business System Security

2. SDN is a function which WatchGuard doesn’t have. As of today, Sangfor doesn’t support VMware NSX. Instead, Sangfor has strong SDN support through Sangfor HCI, and our NGAF has a native integration.

3. Sangfor WAF is a pay-as-you-go licensing model which is much more cost effective than WatchGuard

4. WatchGuard integration is not real integration, with no automation disposition

5. WatchGuard has been accused of providing a less detailed view of data

6. WatchGuard only has a cloud sandbox and no local sandbox, and is not suitable for enterprises that do not want data to leave the local area

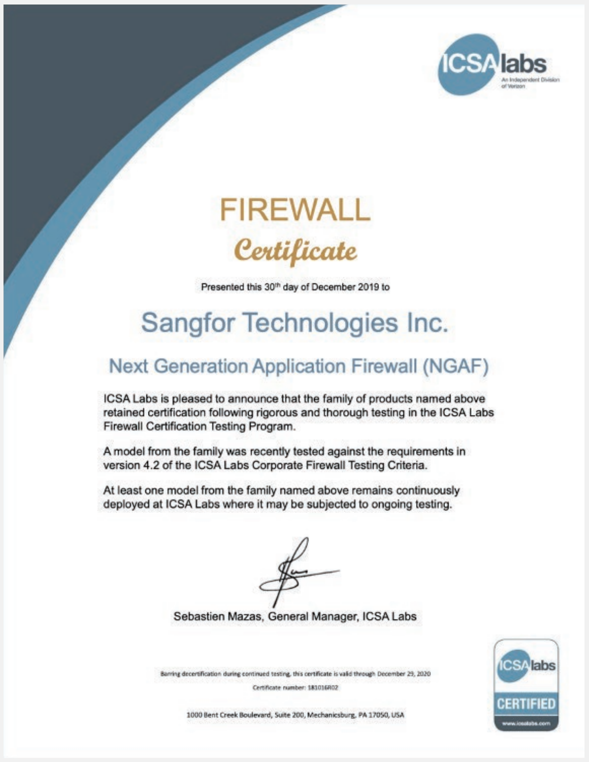
7. Sangfor can provide incident response service, which many vendors cannot provide.

Certifications & Achievements 07

Gartner

Sangfor Technologies has been listed in the Gartner Magic Quadrant for Network Firewalls since 2014.

ICSA Labs



ICSAlabs
An Independent Division of Verizon

FIREWALL
Certificate

Presented this 30th day of December 2019 to

Sangfor Technologies Inc.

Next Generation Application Firewall (NGAF)

ICSA Labs is pleased to announce that the family of products named above retained certification following rigorous and thorough testing in the ICSA Labs Firewall Certification Testing Program.

A model from the family was recently tested against the requirements in version 4.2 of the ICSA Labs Corporate Firewall Testing Criteria.

At least one model from the family named above remains continuously deployed at ICSA Labs where it may be subjected to ongoing testing.

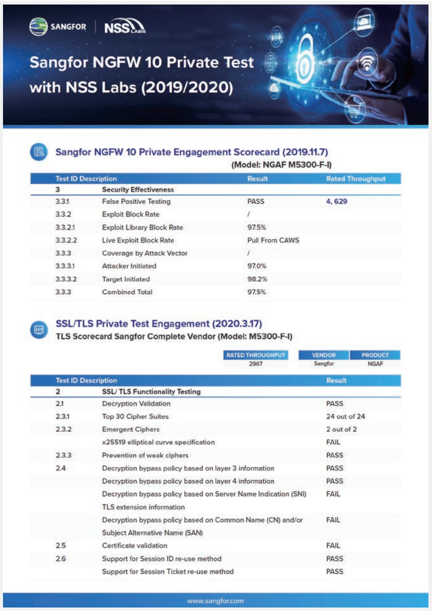
Sebastien Mazas, General Manager, ICSA Labs

Barring decertification during continued testing, this certificate is valid through December 29, 2020
Certificate number: 181016R02

1000 Bent Creek Boulevard, Suite 200, Mechanicsburg, PA 17050, USA

ICSAlabs CERTIFIED www.icsalabs.com

NSS LABS Private Test Result



SANGFOR | NSS LABS

Sangfor NGFW 10 Private Test with NSS Labs (2019/2020)

Sangfor NGFW 10 Private Engagement Scorecard (2019.11.7)
(Model: NGAF M5300-F-I)

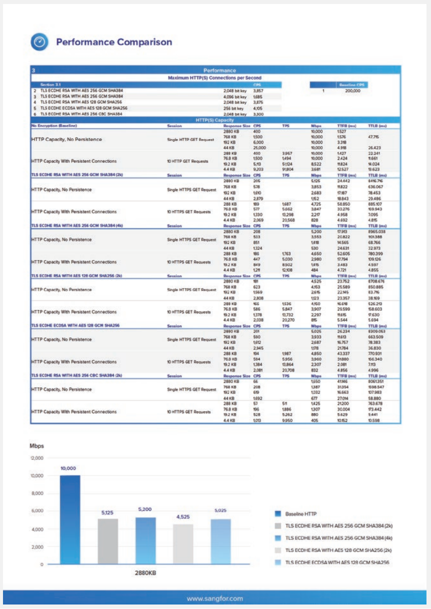
Test ID	Description	Result	Rated Throughput
3	Security Effectiveness		
3.3.1	False Positive Testing	PASS	4, 629
3.3.2	Exploit Block Rate	/	
3.3.2.1	Exploit Library Block Rate	97.5%	
3.3.2.2	Live Exploit Block Rate	Pull From CAWS	
3.3.3	Coverage by Attack Vector	/	
3.3.3.1	Attacker Initiated	97.0%	
3.3.3.2	Target Initiated	98.2%	
3.3.3	Combined Total	97.5%	

SSL/TLS Private Test Engagement (2020.3.17)
TLS Scorecard Sangfor Complete Vendor (Model: M5300-F-I)

RATED THROUGHPUT	VENDOR	PRODUCT
2907	Sangfor	NGAF

Test ID	Description	Result
2	SSL/ TLS Functionality Testing	
2.1	Decryption Validation	PASS
2.3.1	Top 30 Cipher Suites	24 out of 24
2.3.2	Emergent Ciphers	2 out of 2
	x25519 elliptical curve specification	FAIL
2.3.3	Prevention of weak ciphers	PASS
2.4	Decryption bypass policy based on layer 3 information	PASS
	Decryption bypass policy based on layer 4 information	PASS
	Decryption bypass policy based on Server Name Indication (SNI) TLS extension information	FAIL
	Decryption bypass policy based on Common Name (CN) and/or Subject Alternative Name (SAN)	FAIL
2.5	Certificate validation	FAIL
2.6	Support for Session ID re-use method	PASS
	Support for Session Ticket re-use method	PASS

www.sangfor.com



Performance Comparison

3 Performance

Maximum HTTP(S) Connections per Second

	Section 3.1		CPS
2	TLS ECDHE RSA WITH AES 256 GCM SHA384	2,048 bit key	3,857
3	TLS ECDHE RSA WITH AES 256 GCM SHA384	4,096 bit key	1,685
4	TLS ECDHE RSA WITH AES 128 GCM SHA256	2,048 bit key	3,875
5	TLS ECDHE ECDSA WITH AES 128 GCM SHA256	256 bit key	4,105
6	TLS ECDHE RSA WITH AES 256 CBC SHA384	2,048 bit key	3,300

	Baseline CPS
1	200,000

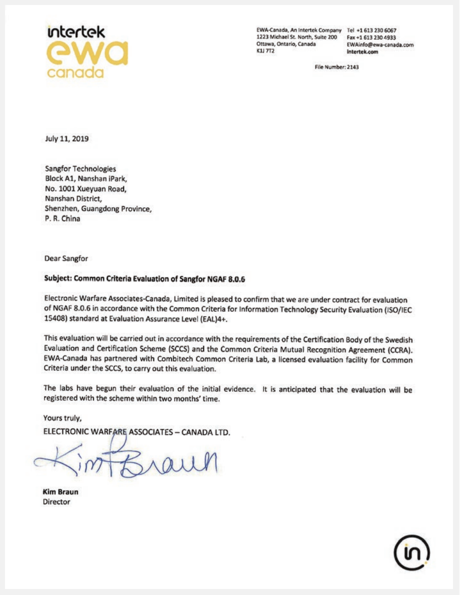
HTTP(S) Capacity

No Encryption (Baseline)	Session	Response Size	CPS	TPS	Mbps	TTFB (ms)	TTLB (ms)
HTTP Capacity, No Persistence	Single HTTP GET Request	2880 KB	400		10,000	1.527	
		768 KB	1,500		10,000	1.576	47.715
		192 KB	6,000		10,000	3.318	
		44 KB	25,000		10,000	4.918	26.423
HTTP Capacity With Persistent Connections	10 HTTP GET Requests	288 KB	400	3,957	10,000	1.427	22.241
		76.8 KB	1,500	1,494	10,000	2.424	11.661
		19.2 KB	5,113	51,124	8,522	11.824	14.024
		4.4 KB	9,203	91,804	3,681	12.527	13.623
TLS ECDHE RSA WITH AES 256 GCM SHA384 (2k)	**Session**	**Response Size**	**CPS**	**TPS**	**Mbps**	**TTFB (ms)**	**TTLB (ms)**
HTTP Capacity, No Persistence	Single HTTPS GET Request	2880 KB	205		5,125	24.442	8416.716
		768 KB	578		3,853	11.822	636.067
		192 KB	1,610		2,683	17.187	78.453
		44 KB	2,879		1,152	18.843	29.486
HTTP Capacity With Persistent Connections	10 HTTPS GET Requests	288 KB	189	1,687	4,725	58.850	885.107
		76.8 KB	577	5,662	3,847	33.276	169.943
		19.2 KB	1,330	13,298	2,217	4.958	7.095
		4.4 KB	2,069	20,568	828	4.692	4.815
TLS ECDHE RSA WITH AES 256 GCM SHA384 (4k)	**Session**	**Response Size**	**CPS**	**TPS**	**Mbps**	**TTFB (ms)**	**TTLB (ms)**
HTTP Capacity, No Persistence	Single HTTPS GET Request	2880 KB	208		5,200	17.913	8965.038
		768 KB	533		3,553	20.822	1101.388
		192 KB	851		1,418	14.565	68.766
		44 KB	1,324		530	24.631	32.973
HTTP Capacity With Persistent Connections	10 HTTPS GET Requests	288 KB	186	1,763	4,650	52.605	780.399
		76.8 KB	447	5,030	2,980	17.794	109.126
		19.2 KB	849	8,502	1,415	3.483	4.597
		4.4 KB	1,211	12,108	484	4.721	4.855
TLS ECDHE RSA WITH AES 128 GCM SHA256 (2k)	**Session**	**Response Size**	**CPS**	**TPS**	**Mbps**	**TTFB (ms)**	**TTLB (ms)**
HTTP Capacity, No Persistence	Single HTTPS GET Request	2880 KB	181		4,525	23.752	8708.676
		768 KB	623		4,153	25.589	850.885
		192 KB	1,569		2,615	22.145	83.716
		44 KB	2,808		1,123	23.357	38.169
HTTP Capacity With Persistent Connections	10 HTTPS GET Requests	288 KB	166	1,536	4,150	16.618	526.213
		76.8 KB	586	5,847	3,907	29.599	158.603
		19.2 KB	1,378	13,732	2,297	11.615	17.630
		4.4 KB	2,038	20,270	815	5.544	5.694
TLS ECDHE ECDSA WITH AES 128 GCM SHA256	**Session**	**Response Size**	**CPS**	**TPS**	**Mbps**	**TTFB (ms)**	**TTLB (ms)**
HTTP Capacity, No Persistence	Single HTTPS GET Request	2880 KB	201		5,026	26.234	8309.053
		768 KB	590		3,933	11.613	663.509
		192 KB	1,612		2,687	16.757	78.383
		44 KB	2,945		1,178	21.784	36.830
HTTP Capacity With Persistent Connections	10 HTTPS GET Requests	288 KB	194	1,987	4,850	43.337	770.931
		76.8 KB	594	5,956	3,960	31.880	156.340
		19.2 KB	1,384	13,864	2,307	2.081	7.113
		4.4 KB	2,081	20,708	832	4.856	4.996
TLS ECDHE RSA WITH AES 256 CBC SHA384 (2k)	**Session**	**Response Size**	**CPS**	**TPS**	**Mbps**	**TTFB (ms)**	**TTLB (ms)**
HTTP Capacity, No Persistence	Single HTTPS GET Request	2880 KB	66		1,650	41.146	8061.351
		768 KB	208		1,387	31.354	1598.547
		192 KB	619		1,032	16.663	107.983
		44 KB	1,092		677	27.014	58.880
HTTP Capacity With Persistent Connections	10 HTTPS GET Requests	288 KB	57	511	1,425	21.200	763.678
		76.8 KB	196	1,886	1,307	30.004	173.442
		19.2 KB	528	5,262	880	5.629	9.441
		4.4 KB	1,013	9,950	405	10.152	10.598

Mbps
12,000
10,000
8,000
6,000
4,000
2,000
0
10,000
5,125
5,200
4,525
5,025
2880KB
Baseline HTTP
TLS ECDHE RSA WITH AES 256 GCM SHA384 (2k)
TLS ECDHE RSA WITH AES 256 GCM SHA384 (4k)
TLS ECDHE RSA WITH AES 128 GCM SHA256 (2k)
TLS ECDHE ECDSA WITH AES 128 GCM SHA256

www.sangfor.com

EAL4+ (In Progress)



intertek
ewa
canada

EWA-Canada, An Intertek Company
1223 Michael St. North, Suite 200
Ottawa, Ontario, Canada
K1J 7T2

Tel +1 613 230 6067
Fax +1 613 230 4933
EWAinfo@ewa-canada.com
intertek.com

File Number: 2143

July 11, 2019

Sangfor Technologies
Block A1, Nanshan iPark,
No. 1001 Xueyuan Road,
Nanshan District,
Shenzhen, Guangdong Province,
P. R. China

Dear Sangfor

Subject: Common Criteria Evaluation of Sangfor NGAF 8.0.6

Electronic Warfare Associates-Canada, Limited is pleased to confirm that we are under contract for evaluation of NGAF 8.0.6 in accordance with the Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408) standard at Evaluation Assurance Level (EAL)4+.

This evaluation will be carried out in accordance with the requirements of the Certification Body of the Swedish Evaluation and Certification Scheme (SCCS) and the Common Criteria Mutual Recognition Agreement (CCRA). EWA-Canada has partnered with Combitech Common Criteria Lab, a licensed evaluation facility for Common Criteria under the SCCS, to carry out this evaluation.

The labs have begun their evaluation of the initial evidence. It is anticipated that the evaluation will be registered with the scheme within two months' time.

Yours truly,
ELECTRONIC WARFARE ASSOCIATES – CANADA LTD.

Kim Braun

Kim Braun
Director

This comparison and information document is based on the Sangfor interpretation of publicly available data as of the date of preparing this comparison. This document has been prepared by Sangfor and not the other vendors listed herein. The features or characteristics of the products under comparison, which may have direct impact on the accuracy and/or validity of this comparison, are subject to change. The information contained in this comparison is intended to provide broad understanding and knowledge of factual information of various products and may not be exhaustive. Anyone using the document should make their own decision based on their requirements and should also research original sources of information and not rely only upon this comparison while selecting any product.

Sangfor makes no warranty as to the reliability, accuracy, usefulness, or completeness of this document. The information in this document is provided "as is" and without warranties of any kind either expressed or implied. Sangfor retains the right to modify or withdraw this document at any time. This document is confidential and intended for private circulation to Sangfor internal personnel and authorized partners only, and may not be disclosed to unauthorized third parties. Partners-may use this comparison only if it is permitted in their jurisdiction and must use the most up- to-date version.