SANGFOR NGAF FIREWALL PLATFORM

Secured. Converged. Simplified.

The World First Fully Integrated NGFW + WAF

- Reduce Security Hardware Footprint Up to 70%
- One Management Panel for All Security Operations
- Security Expertise Enablement Through Visualization
- Do More With Less. Minimum 50% of TCO Reduction

Recommended by

NSS LABS RECOMMENDED — Recommended Rating for WAF

Listed In

Gartner

Magic Quadrant for Enterprise Network Firewalls

Certified by

ICSA labs CERTIFIED FIREWALL - CORPORATE

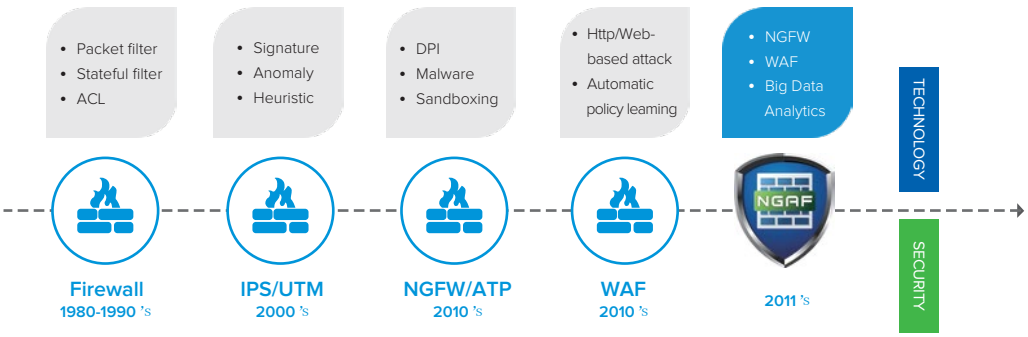
SANGFOR

A New World, New IT, New Security

With the fast evolution in the IT Industry, business applications and IT services will be accessed through the internet, hosted locally or through the new emerging cloud trends. The rise of BYOD and IoT would allow easier and convenience access to these systems, however these new trends will be a great concern on Network Security.

Sensitive data such as financial information and confidential corporate information, will be the target of unethical activities. Cyber Threats such as Defacement Attacks, Ransomware and Information Theft are growing at alarming rate and more & more new threats are emerging.

Nowadays there are many types of security solutions available on the market to protect your against these threats, however less than 40% of enterprises are protected using Next Generation Firewalls (according to Gartner). For these enterprises already protected by a Firewall or IPS, they often neglect to use a Web Application Firewall as it is only considered as an additional investment with few benefits. Protections offered by NGFW & IPS are too general against the increasing number of web vulnerabilities, which often can only protect against the known vulnerabilities.



As mentioned in Gartner's report, 75% of attacks are against Web Applications, but only 10% of investment in security solutions are spent on it. There is a large gap between the real needs and offers on the market, which need to be filled. However cost issue & risk awareness are important factors delaying this convergence.

Sangfor Security Concept

Network Security is a vast subject with many different definitions and opinions according to each security expert. For many, Network Security could be defined as a protection to unauthorized access to files and directories on a computer and often referred to an Anti-Virus. Traditional security solutions will not give you any visibility of users, traffic and IT assets. There won't be any real-time or post-event detection of network threats. Lower performance for Application Layer Security (also known as L7) will also allow more attacks to happen.

For Sangfor, our concept of Network Security is going much more further to provide a complete & comprehensive solution to protect our users against all type of threats, no matter if its internal or external, existing or future threats. As your Security Guard to the Future, Sangfor' s concept of Network Security is following four fundamentals points that are at the core of our market strategy:

Security Visibility

- Holistic End-to-End Visibility
- Intelligent Analyzing
- Management Visibility

Rapid Response

Real-time Detection

- Pre & Post-Event Detection
- Business Risks Detection

Rapid Response

- Automatic Policy Enforcement
- Solution Synergy and Correlation
- Security Expertise as a Service

Simplified Security

Easy Deployment

- Configuration Wizard
- Simplified Business Based Policy Layout

Simple O&M

- Intuitive Security Reporting
- Presented as Security Event
- Convergence

L7 High-Performance — Hardware and Software Architecture — Efficient Algorithm

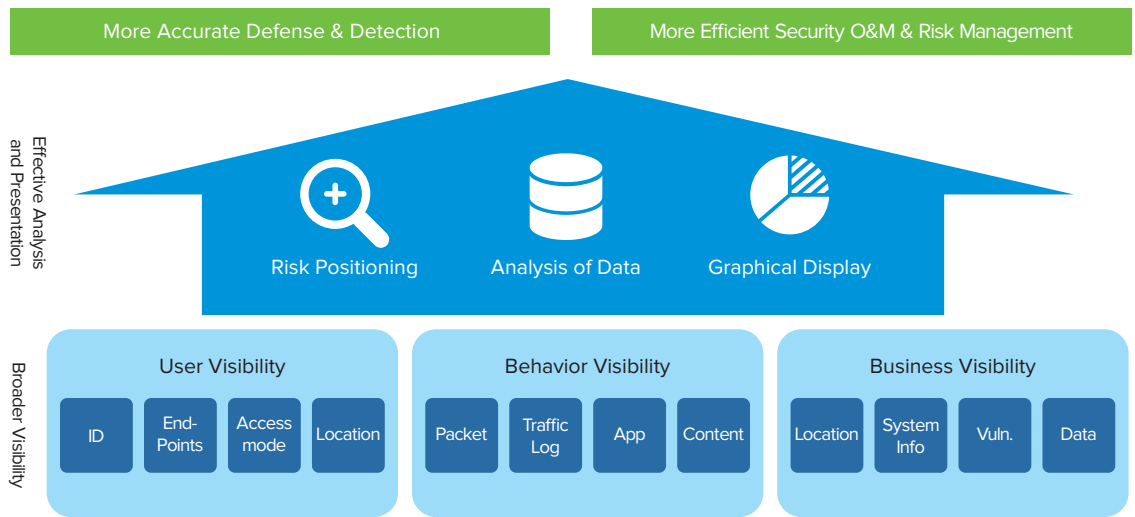
Security Visibility

Security is becoming more and more complex with illegal traffic mixed with legitimate traffic. Even in trusted domains, legitimate users cannot be trusted as they might be a potential attacker. Therefore we believe that the visibility of the whole network is the foundation of network management. We need to see the risk of information assets, people and behaviors, so that we can recognize security threats and timely dispose of them.

However Security Visibility is not just gathering data and statistics, you also need to make further analysis by making correlation between the users, behaviors and business systems to understand where the attack is coming from, how it happened, how to solve it and trace it back to the attacker.

With Sangfor NGAF Reporting Tools included in the product itself (Free-of-Charge), users are able to have an extensive overview of their network with just a few clicks. You can choose whether you want to see information such as who the online users are, servers, abnormal traffics, attack status, attack source, etc.

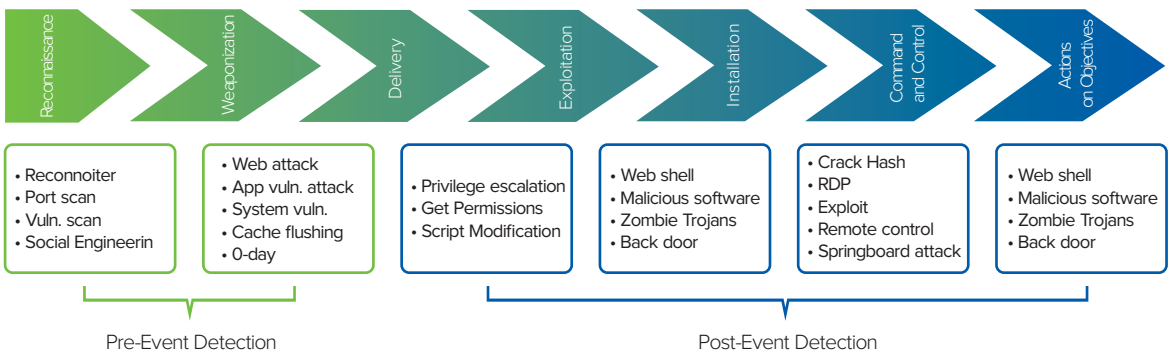
Sangfor provides a Holistic View, which provides end-to-end visibility, from endpoints to business systems.

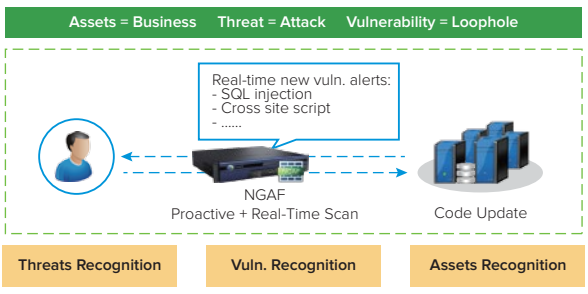


Real-Time Detection, Rapid Response

For many users, real-time detection is only limited for attacks that happened before it entered the network. However real-time detection should also take into account all attacks that have already succeeded and bypassed security protection.

Traditional security devices are limited in terms of capability and are only able to detect pre-event attacks, which are making them vulnerable against new and evolving threats. Created by renowned security defense Lockheed Martin, the term Cyber Kill Chain® has been widely used to describe the different stages of cyber-attacks. This can help users have a better visibility of an attack and help them understand the tactics, techniques and procedures of an attack.

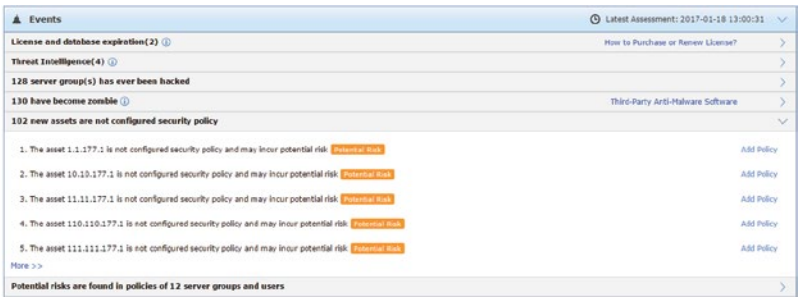




Provide Active & Passive Vulnerability Detection, 7*24-hour Vulnerability Monitoring Service

Based on this Chart, Sangfor NGAF is capable of detecting in real-time threats at every step and provide a rapid response on how to deal with them. In order to meet the challenges of escalating attacks, it's not enough to provide the detection of static elements. We need a total security collaboration between each module to continuously detect unknown & new threats to quickly issue policy based on detection results to refine the scope of the threats.

Alert Notification



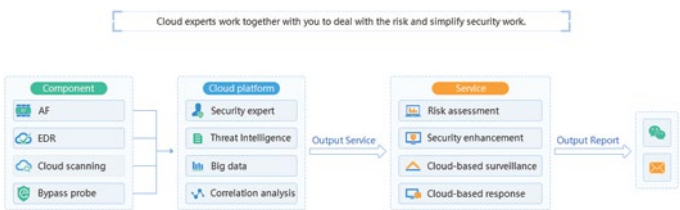
Threat Alerts List

No.	Appeared Since	Description	Threat Level	Protection	Operation
1	2016-05-03	ImageMagick Exposed High-risk Vulnerability	High Threat	Unprotected	Protect
2	2016-04-21	Struts2 Exposed High-risk Vulnerability	High Threat	Unprotected	Protect
3	2016-03-25	Be Careful Of Locky Virus	High Threat	Unprotected	Protect
4	2016-03-15	Apache Struts2 Remote Command Execution Vulnerability	High Threat	Unprotected	Protect
5	2015-07-29	BIND9 DoS Vulnerability	High Threat	In protection	Details
6	2015-07-21	PHPCMS critical 0day vulnerability is exposed	High Threat	In protection	Details
7	2015-05-14	PHP remote DoS vulnerability is exposed	High Threat	In protection	Details
8	2015-04-14	Microsoft IIS critical vulnerability is exposed	High Threat	In protection	Details
9	2014-09-24	Bash shellshock vulnerability	High Threat	Unprotected	Protect
10	2014-04-08	OpenSSL Heartbleed Vulnerability	High Threat	In protection	Details

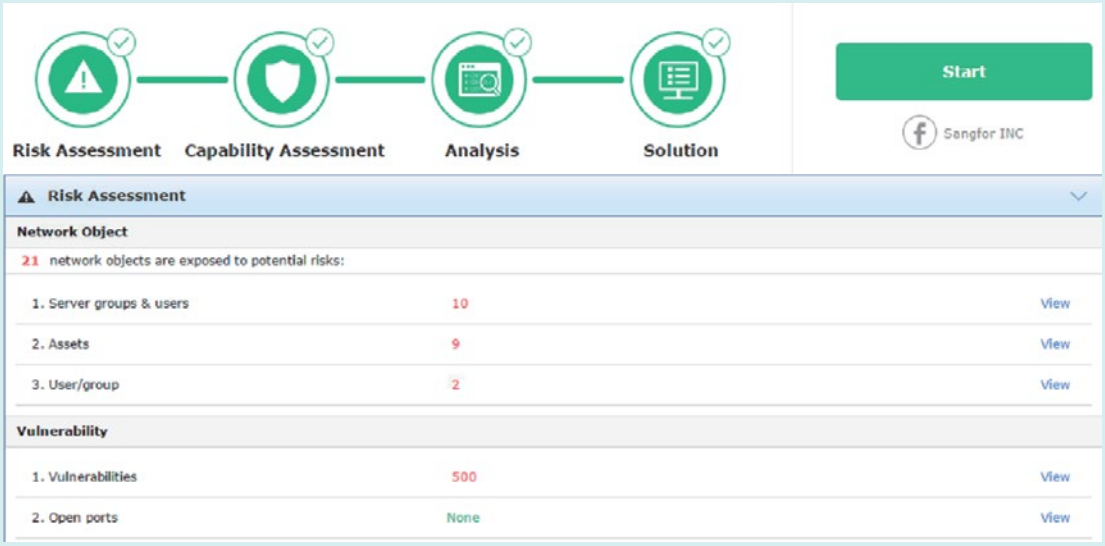
Sangfor Cloud Security Services For Web Servers

Sangfor, as a Security Expert, provides Cloud Security Services for Web Servers. Services offered includes:

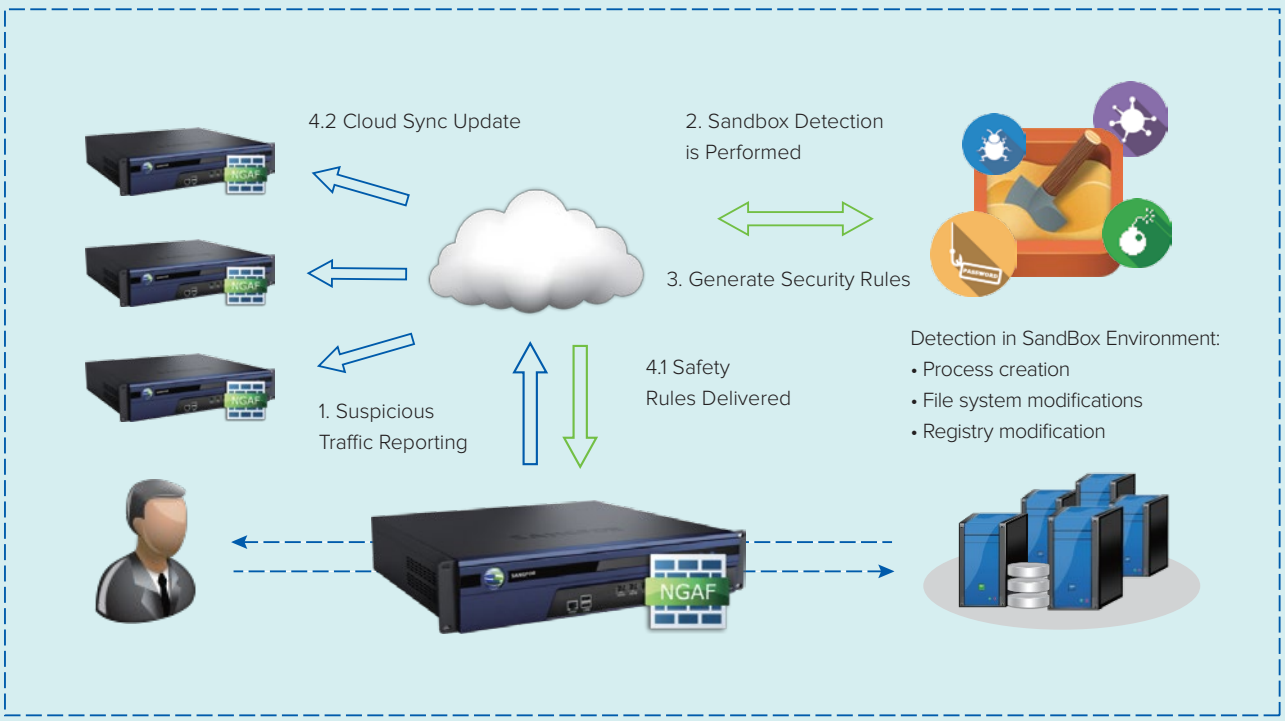
- Vulnerability Assessment
- Countermeasure Implementation
- Risk & Threat Intelligence Analysis & Surveillance
- Cyber-Security Incident Response



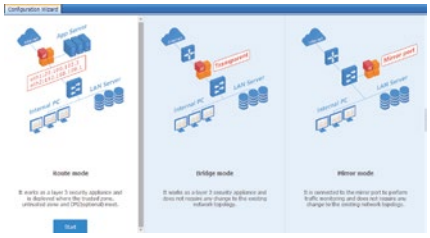
Risk Assessment Module



Against unknown threats, Sangfor NGAF also includes its own Cloud Sandbox tool to help our users isolate possible emerging new threats that haven' t been included in any security database. This is especially useful against 0-day attacks. When any suspicious traffic is reported, it will be put in the Cloud Sandbox for analysis and if it is indeed a threat, security rules will be generated and delivered to all Sangfor NGAFs worldwide.



Simplified Security Operation & Maintenance



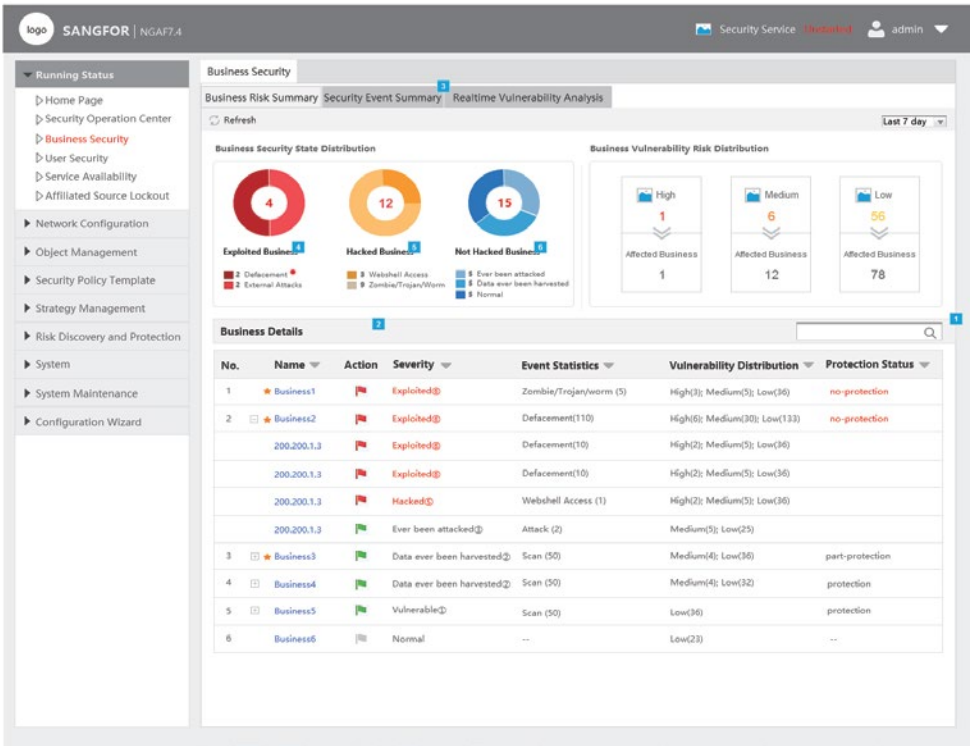
An organization can receive thousands of alerts per week, which increase its operation costs. The IT department have to spent a lot of time & effort investigating these alerts to recognize genuine threats and identify the root-cause. This can be the beginning of a nightmare for the IT department !

This also increase the risk on longer downtime due to difficulty in finding root-cause and difficulty to take actions as they lack visibility and evidence.

With Sangfor, *Security Operation* is reliable and simple. Our *Easy Deployment* and *Simple Operation & Maintenance* features provides simplicity for effective and productive IT environment.

Sangfor NFAF provides a configuration wizard, which makes security policy deployments easy. Furthermore, Sangfor provides an integrated intuitive reporting tools which provides a total end-to-end visibility of overall security in an organization, from business aystems to the endpoints. With these visibility components in-placed, together with real-time detection feature, the IT department and business owners can execute a proactive check of their systems before it goes online, thus providing a secured environment for the business systems.

Simplified Business Based Layout

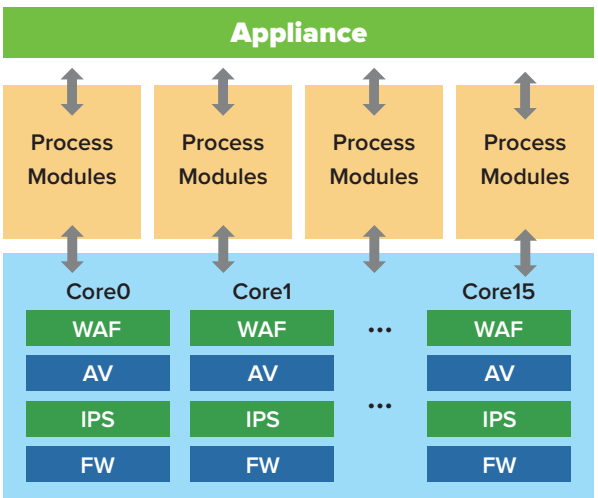


High-Performance for Application Layer Security

With around 75% of the attacks happening at the Application Layer, it is important for organizations to ensure that they have the right tools to protect them. Unfortunately, many vendors will sacrifice some critical features for better performance. This will often lead to attacks bypassing the existing security solutions.

For a successful Application Layer Security, it must be focus on the Detection Methods, Software Architecture, Engine Performance and Computing Power. This is where Sangfor NGAF excels at, with superior technologies overcoming common performance issues.

From a hardware point of view, the architecture used in Sangfor NGAF is optimized for performance with all included security features such as WAF (Web Application Firewall), AV (Anti-Virus), IPS (Intrusion Prevention System) and FW (Firewall) able to use all computing power to run at the same time.



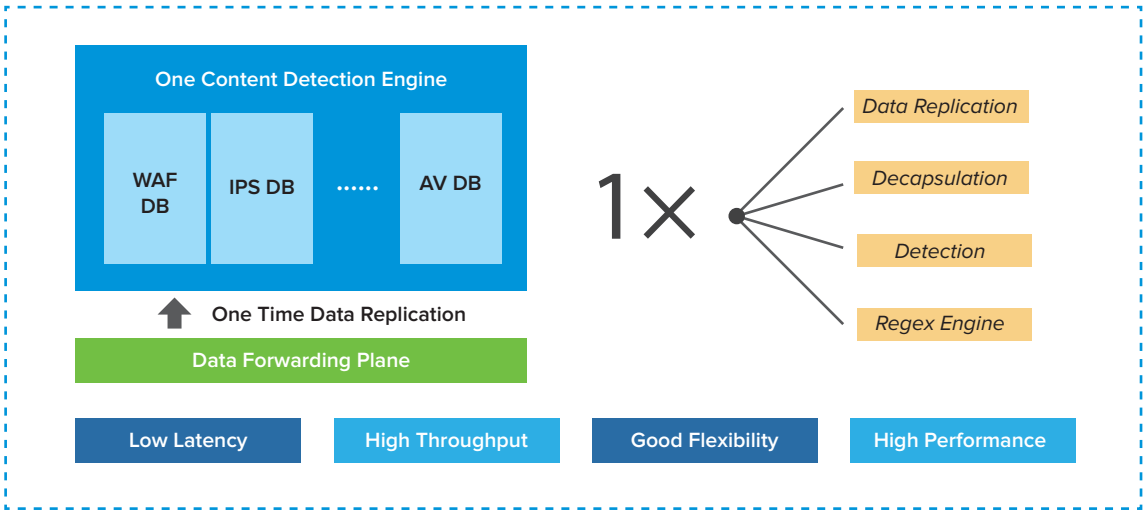
Core Strengths of NGAF' s Hardware Architecture

Intel Quick Path Interconnect
- Wide bus bandwidth
- High computing capacity

Multi-Core Level Processing
- Up to 2.5GHz
- Maximum up to 126 cores

Hybrid Processing Model
- Fragmented processing
- One module can use all power

From a software point of view, resources are not wasted with our "1X" technology that performs all action such as data replication, decapsulation and detection only once. With also one content detection engine and Sangfor patented REGEX engine, users can enjoy a fast & flexible security.



New Business Environment Drives New Security Model !

- Real Time Security Visibility is the foundation of modern security.
- Fast response to security events is crucial.
- Security operation simplification becomes part of security requirements.
- Application layer Security capability is what new security cares about.

SANGFOR NGAF
Product Family

Model	M5100-F-I	M5200-F-I	M5300-F-I	M5400-F-I	M5500-F-I	M5600-F-I	M5800-F-I	M5900-F-I	M6000-F-I
Profile	1U	1U	1U	1U	2U	2U	2U	2U	2U
RAM	4G	4G	4G	4G	4G	8G	16G	24G	32G
HD Capacity	SSD 32GB	SSD 32GB	SSD 64 GB	SSD 128 GB	1 TB	1 TB	1 TB +4G CF	1 TB +4G CF	1 TB +4G CF
Firewall Throughput*	2 Gbps	3 Gbps	6 Gbps	8 Gbps	12 Gbps	18 Gbps	20 Gbps	40 Gbps	80 Gbps
IPS + WAF Throughput (HTTP)	550 Mbps	850 Mbps	950 Mbps	1.7 Gbps	3 Gbps	8 Gbps	12 Gbps	20 Gbps	40 Gbps
IPS or WAF Throughput (HTTP)	1 Gbps	2 Gbps	3.6 Gbps	5.4 Gbps	8 Gbps	12 Gbps	15 Gbps	20 Gbps	40 Gbps
IPsec VPN Throughput	250 Mbps	375 Mbps	1 Gbps	1.25 Gbps	2 Gbps	3 Gbps	3.75 Gbps	5 Gbps	5 Gbps
Max IPsec VPN Tunnels	300	500	1000	1500	3000	4000	5000	10000	10000
Concurrent Connections (TCP)	250,000	1,000,000	1,000,000	1,000,000	1,000,000	2,000,000	4,000,000	8,000,000	16,000,000
New Connections (TCP)	50,000	60,000	100,000	110,000	220,000	300,000	330,000	450,000	600,000
Power and Hardware Specifications									
Support Dual Power Supplies	N/A	N/A	N/A	N/A	√	√	√	√	√
Power [Watt] (Max)	60W	100W	100W	250W	300W	300W	500W	500W	500W
Temperature	0~40°C								
System Weight	3.85Kg	3.85Kg	6.65Kg	6.65Kg	20.0Kg	20.0Kg	20.0Kg	20.0Kg	20.0Kg
System Dimensions (mm^3)	300x430x44.5	300x430x44.5	300x430x44.5	375x430x44.5	440x500x89	440x600x90	440x600x90	440x600x90	440x600x90
Relative Humidity	5%~95% non-condensing								
Compliance & Certificates	CE, FCC								
Network Interfaces									
Bypass (Copper)	1 pair	1 pair	2 pairs	4 pairs	3 pairs	5 pairs	4 pairs	2 pairs	4 pairs
10/100/1000 Base-T	4	6	4	8	8	10	8	4	8
SFP	N/A	N/A	2	N/A	2	4	4	4	8
10G Fiber SFP	N/A	N/A	N/A	N/A	N/A	N/A	N/A	2	4
Optional Interface & 10G Fiber SFP*	N/A	N/A	N/A	N/A	√	√	√	√	√
Serial Port	RJ45×1	RJ45×1	RJ45×1	RJ45×1	RJ45×1	RJ45×1	RJ45×1	RJ45×1	RJ45×1
USB Port	2	2	2	2	2	2	2	2	2

* "Optional Interface & 10G Fiber SFP" allows upgrading interfaces according to your requirement.

** M5100-F-I are available with 6 interfaces platforms with corresponding cost.

All performance values are "up to" and vary depending on the system configuration.

SANGFOR NGAF Product Features

Firewall

• Networking
- Policy routing, static routing, RIP v1/2, OSPF, BGP, and GRE.
- Application policy-based forwarding, NAT (1-1 NAT, many-to-one NAT, and many-to-few NAT), VLAN tagging
- IPv6 & IPv4 supported
- Support multi cast traffic, SNMP v3, and Syslog server with UTF-8 format
- Intelligent Dos/ DDos prevention
- ARP spoofing prevention
- HA fail-over time less than 1 second
- Support at least 10000 security policies
- Policies basis with "first come first match"
- Provide management via SSH, HTTPS, CLI, and Web-based GUI

• SSL VPN

• IPsec VPN
- IPSec Protocol: AH, ESP
- D-H Group: MODP768 Group(1), MODP1024 Group(2), MODP1536 Group(5)
- IPSec Authentication Algorithm: MD5, SHA-1. SHA-2, SM3
- IPSec Encryption Algorithm: DES, 3DES, AES-128, AES-256. SANGFOR_DES, SCB2, SM4

Threats Prevention

• Full SSL inspection
- SSL inspection to all security modules including IPS, WAF, ATP, Access control, etc.

• Cross-module intelligent correction
- Policy association of IPS, WAF and APT prevention modules.
- Cross-module visibility reporting analysis

• Threats prevention
- APT (Advanced Persistent Threat), Remote Access Trojan, Botnet, malware detection
- Cloud-based Sandbox threats analysis
- Anti-Malware signature database, covering threats type of Trojan, AdWare, Malware, Spy, Backdoor, Worm, Exploit, Hacktool, Virus, etc.

• Anti-virus
- Scan and kill viruses infecting HTTP, FTP, SMTP and POP3 traffic as well as viruses infecting compressed data packets
- Support remove virus from detected malicious files

• Email security
- Categorize and filter various forms of malicious emails.
- Support detection deep into email body and attachments.
- Support place warning messages into email title to avoid users from opening malicious emails

IPS

• IPS signature database
- Prevention against vulnerability exploits towards various system, application, middleware, database, explorer, telnet, DNS, etc.
- Employ cloud-based analysis engine
- Allow custom IPS rules
- Database update once a week

• Certificate and partnership
- Common Vulnerabilities and Exposures (CVE) compatibility certificated
- Microsoft Active Protections Program (MAPP) partnership

Risk Assessment and Security Service

• Risk assessment
- Scan and identify security loopholes such as open port, system vulnerabilities, weak passwords, etc.

• Web scanner
- On-demand scanning of targeted website/URL to discover the system vulnerabilities.

• Real-time vulnerability scanner
- Discover vulnerabilities in real-time and protection against 0-days attacks

• SANGFOR threat intelligence service
- Threat intelligence to deliver the latest vulnerabilities, malware and security incidents information with advisory alerts for policy creation

• Web-based attack prevention
- Defend against the 10 top major web-based attacks identified by the Open Web Application Security Project (OWASP)
- Web-based attack rules database
- Support custom WAF rules

• Parameters protection
- Proactive protection of automatic parameter learning

• Application hiding
- Hide the sensitive application information to prevent hackers from mounting targeted attacks with the feedback information from the applications

• Password protection
- Weak password detection and brute-force attack prevention

• Privilege control
- File upload restriction of file type blacklist
- Specify access privilege of sensitive URL such as the admin page for risk prevention

• Buffer overflow detection
- Defend against buffer overflow attacks

• Detection of HTTP anomalies
- Analyze anomalies of the fields of the HTTP protocol via single parsing

• Secondary authentication for server access
- Server access verification by IP address restriction and mail authentication

Data Leakage Prevention

• Data leakage detection and prevention
- Control and detection over multiple types of sensitive information (customizable)including user information, email account information, MD5 encrypted passwords, bank card numbers, identity card numbers, social insurance accounts, credit card numbers, and mobile phone numbers

• File downloading control
- Restrict suspicious file downloading

User Access Management

• User identity:
- Mapping by IP, MAC, IP/MAC binding, hostname and USB-Key. User account import from CSV file and LDAP Server.
- SSO integration with AD domain, proxy, POP3 and WEB

• Internet content classification
- Cloud-based URL/APP classification engine

• Access control
- Policy configuration oriented toward users and applications for web filter, application control and bandwidth management

Visibility Reporting

• Built-in report center
- Full visibility to network, endpoint and business servers with multi-dimensional analysis of risks, vulnerabilities, attacks, threats and behaviours
- Threats analysis for specific attack by Description, Target, Solution
- Support visualization into cyber kill chain
- Business Systems based reporting

• Report subscription
- Support PDF format and automatically send to pre-defined mailbox on daily/weekly/monthly basis

Deployment

• Configuration Wizard
- Guideline for deployment and policy configuration

• Deployment
- Gateway (Route mode) | Bridge mode | Bypass mode | Multiple Bridge mode (2- 4 bridges)

• High Availability
- Active-Active | Active-Passive

• Bypass
- Hardware bypass in the event of hardware failure

• Central Management
- Support central management of multiple NGAFs

Sangfor Technologies

Sangfor Technologies is the global leading vendor of IT infrastructure solutions. It is specialized in Cloud Computing, Network Security & Optimization with products including but not limited to: Hyper-Converged Infrastructure, Virtual Desktop Infrastructure, Next Generation Application Firewall, Internet Access Management, WAN Optimization, SSL & IPSec VPN and so on.

Through constant innovation, Sangfor always strives to create value for our customers by helping them achieve sustainable growth. We take customers' business needs and user experience very seriously, placing them at the heart of our corporate strategy.

Established in 2000, Sangfor now has more than 55 branch offices in the world (Hong Kong, Malaysia, Thailand, Indonesia, Singapore, US, UK, etc.). Sangfor currently has 3,000+ employees, with 40% of them dedicated to R&D. Furthermore, each year at least 20% of Sangfor's revenue will be put into R&D to improve current products as well as develop new solutions for our customers.

Awards & Achievements

- "Technology Fast 500 Asia Pacific Region" Award for 8 consecutive years from 2005 to 2012 by Deloitte.
- "Best Companies to Work for in China" Award from 2009 to 2011 by the Fortune Magazine.
- "Best Practice Award in Asia-Pacific Region" in 2010 by Frost & Sullivan.
- "Management Action Award" in 2012 by Harvard Business Review.
- Sangfor SSL VPN no. 1 in Network Security market in China, Hong Kong & Taiwan according to F&S.
- No. 1 for Secure Content Management Hardware and VPN Hardware segment in China according to IDC.
- Sangfor IAM listed for 5 consecutive years in the Gartner MQ for Secure Web Gateways (2011-2016).
- Sangfor WANO listed for 3 consecutive years in the Gartner MQ for WAN Optimization (2013-2016).
- Sangfor NGAF listed in the Enterprise Network Firewalls MQ by Gartner (2015-2016).
- Sangfor HCI listed in the x86 Server Virtualization Infrastructure MQ by Gartner (2016).
- Reviewed by NSS Labs with a "Recommended" rating in 2014 for SANGFOR NGAF (WAF test).
- ICSA Labs certification for SANGFOR Next Generation Firewall in April 2016.
- "Most Promising Network Security Solution" in June 2016 by Singapore NetworkWorld Asia.
- "Readers Choice Awards for Enterprise Security" in October 2016 by Computerworld Malaysia.

Our Notable Clients

SANGFOR NGAF FIREWALL PLATFORM

SANGFOR HONG KONG
Unit 1109, 11/F, Tower A, Mandarin Plaza, 14 Science Museum Road, Tsim Sha Tsui East, Kowloon, Hong Kong
Tel: (+852) 3427 9160
Fax: (+852) 3427 9910

SANGFOR SINGAPORE
8 Burn Road # 04-09, Trivex,
Singapore (369977)
Tel: (+65) 6276 9133

SANGFOR INDONESIA
World Trade Centre, WTC 5, 6th Floor,
Jl.Jend .Sudirman Kav.29
Jakarta 12920, Indonesia.
Tel: (+62) 21 2933 2643
Fax: (+62) 21 2933 2643

SANGFOR MALAYSIA
No. 47-10 The Boulevard Offices, Mid Valley City, Lingkaran Syed Putra, 59200 Kuala Lumpur, Malaysia
Tel: (+60) 3 2201 0192
Fax: (+60) 3 2282 1206

SANGFOR THAILAND
6th Floor, 518/5 Maneeya Center Building, Ploenchit Road, Lumpini, Patumwan, Bangkok, 10330 Thailand
Tel: (+66) 22517700
Fax: (+66) 22517700

SANGFOR USA
2901 Tasman Drive, Suite 107, Santa Clara, California, USA
Tel: (+1) 408 520 7898
Fax: (+1) 408 520 7898

SANGFOR EMEA
Unit 1, The Antler Complex, 1 Bruntcliffe Way, Morley, Leeds LS27 0JG, United Kingdom
Tel: (+44) 0845 533 2371
Fax: (+44) 0845 533 2059

AVAILABLE SOLUTIONS

IAM	Advanced Bandwidth Management with Valuable Big Data Analytics
WANO	Enjoy a LAN Speed on your WAN
NGAF	Secured. Converged. Simplified.
HCI	Driving Hyperconvergence to Fully Converged
aBOS	The World First NFV Converged Gateway
VDI	Ultimate User Experience that Beats PC

SANGFOR

www.sangfor.com

Sales : sales@sangfor.com
Marketing : marketing@sangfor.com
Global Service Center : +60 12711 7129 (or 7511)

Our Social Networks :

https://twitter.com/SANGFOR
https://www.linkedin.com/company/sangfor-technologies
https://www.facebook.com/Sangfor
https://plus.google.com/+SangforTechnologies
http://www.youtube.com/user/SangforTechnologies

NGAF_BR_P_NGAF-Brochure_20170603