SANGFOR

NGAF FIREWALL PLATFORM

Best Value for Money

The World 1st Integrated NGFW + WAF

- Competitive TCO Through Technology Innovation
- Holistic & Self-Adaptive Security Solution
- Big Data Security Analytics
- Simplified Operation & Maintenance

Recommended By

NSS LABS RECOMMENDED
Recommended Rating for WAF

Recognized By

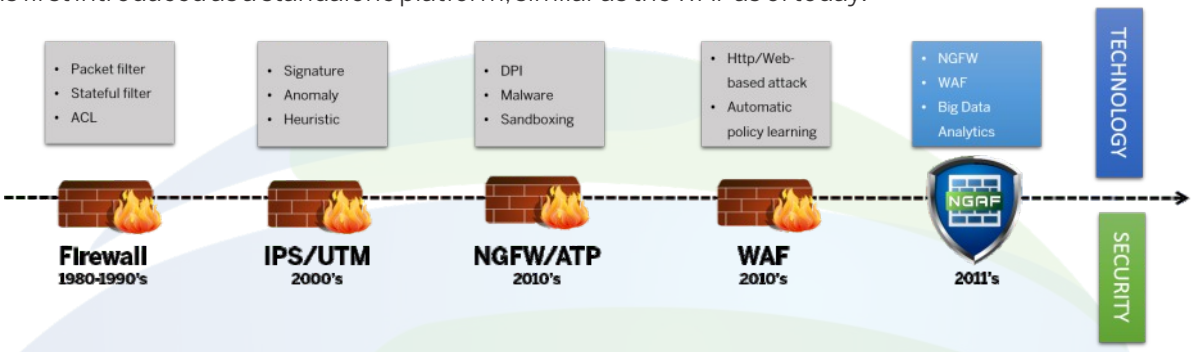
Magic Quadrant for Enterprise Network Firewalls

Gartner®

www.sangfor.com
sales@sangfor.com

Firewall Market Trend

Firewalls were first developed in the 1980's and were mainly performing basic security tasks such as packet-filtering & stateful-filtering. With the emergence of new type of attacks such as viruses, worms, malware and new hacking techniques targeting businesses, there was an increase need for a solution integrating a set of security features to provide a total protection. In 2010's, the first Next Generation Firewall (NGFW) & Web Application Firewall (WAF) models were released, providing better protection with focus on the Application & User Layers. IPS appeared later and was first introduced as a standalone platform, similar as the WAF as of today.



Nowadays there are many types of security solutions available on the market, however less than 40% of enterprises are protected using Next Generation Firewalls*[1]. 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*[2].

As indicated 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. For SANGFOR, the next natural step was to offer an affordable & integrated security solution with both NGFW + WAF , which is at the source of the NGAF Platform development.

* Source: Gartner Magic Quadrant for Enterprise Firewalls. 2015
* Source: Web Application Firewalls Are Worth the Investment for Enterprises (Gartner), 2014

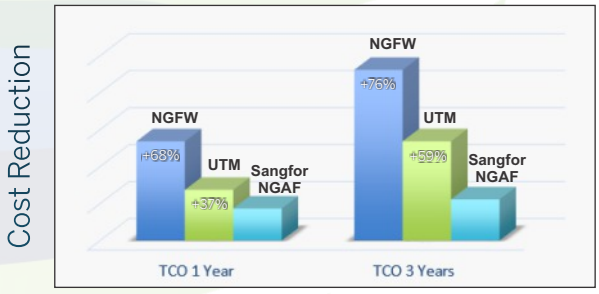
Best Value for Money

Not only SANGFOR NGAF is the World 1st integrated NGFW + WAF, but it is also one of the most affordable solution available on the market. Without sacrificing the quality & performance, SANGFOR is able to provide a total security solution for small & large businesses.

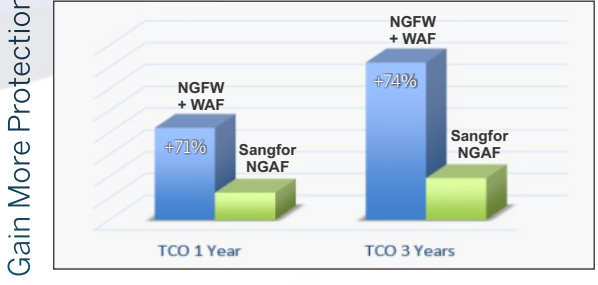
Before making your final decision and choose the right security protection, you cannot only take into account the initial cost of your purchase but you also have to take into account the overall TCO (Total Cost of Ownership) for a period from 3 to 5 years.

As shown in the graphs on the right, Sangfor NGAF can offer a better value for your money by making sure that it is the best suited Security Solution according to your needs (NGFW/UTM or NGFW+WAF) to provide a Safe, Secure and Managed network environment.

FW for Terminal Protection
Save up to 76% of your TCO !



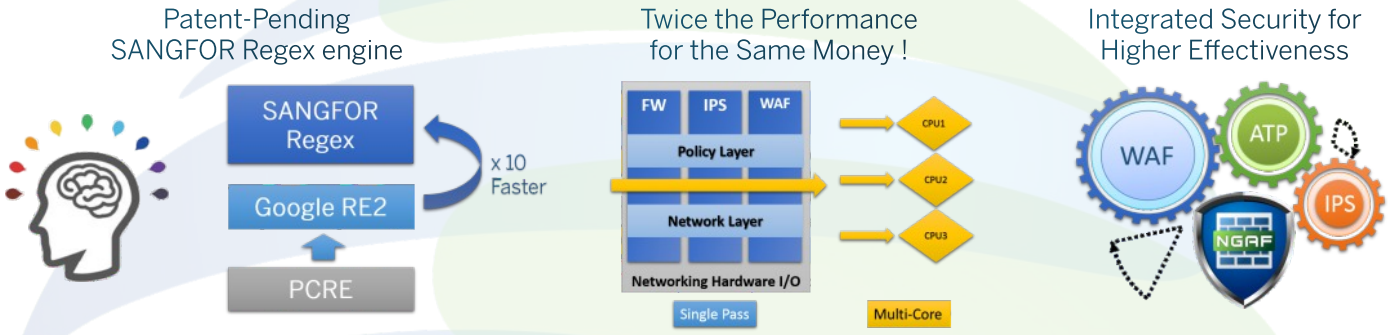
NGAF for Total Threat Prevention
Save up to 74% of your TCO !



Make the Impossible Possible with Technology Innovation

The World 1st Integrated NGFW+WAF

- In-house developed SANGFOR Regex (Regular Expression) engine accelerates regular expression matching at tens of Gbit/s, which has been proved to be 10 times faster than the current RE2 engine.
- NGAF Platform is designed with Single-Pass Analysis Algorithm and Multi-core Parallel Processing to improve efficiency.
- Cross-module intelligent correlation & cost increase for potential hacker intrusion



A Holistic Approach of Security

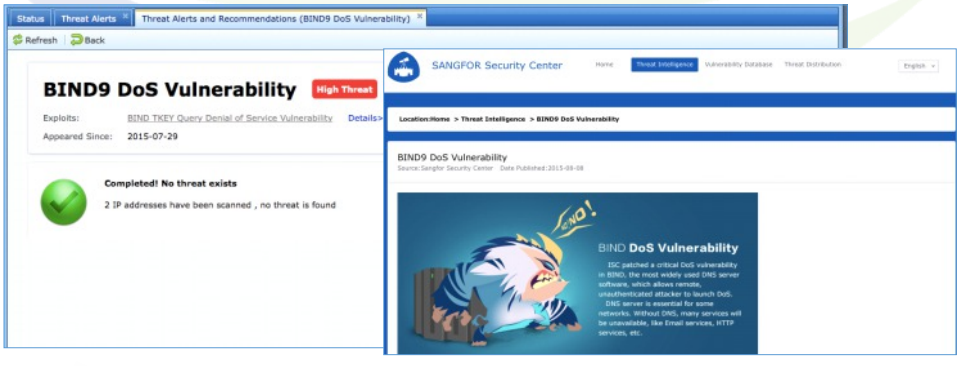
With the increasing number of new applications and online web-based applications we cannot see, there was an urgent need for a security device capable of Visualizing & Controlling Applications and Users. With Sangfor NGAF platform, we developed a new approach based on 4 key principles: Prediction, Defense, Remediation and Backtracking.

You can now **Predict** the threats before they even happen, **Defend** your Network against existing Threats and if any suspicious traffic went through, it will be **Remediated** and with its **Backtracking** capabilities, you can access to comprehensive logs & recommendations to timely and efficiently set up network security policies.

Prediction

Threat Intelligent Service

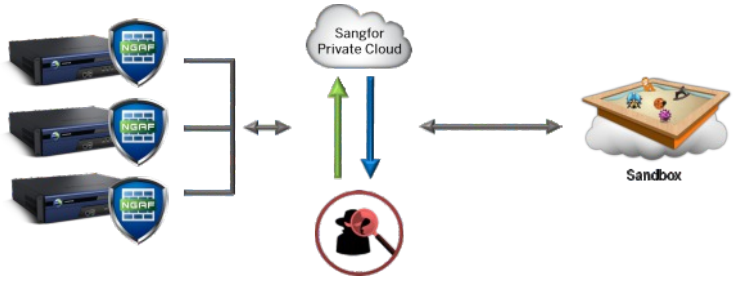
Sangfor NGAF provides real-time threat intelligence service to our customers and let you keep your IT team updated with up-to-date information such as latest vulnerabilities, malware & security incidents, and provides alerts & recommendations to create suitable network security policies to protect your enterprise against new & recent threats.



Sangfor Cloud-Sandboxing

Advanced and emerging threats can quickly adapt themselves to evade signature-based detections and traditional defenses.

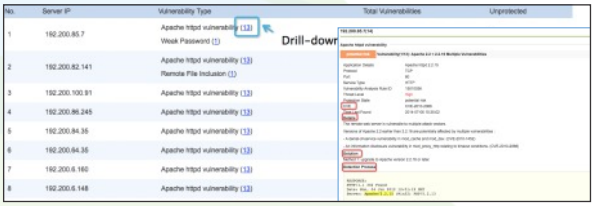
Nowadays attacks are using a new breed of threats to launch targeted & sophisticated attacks that can lead to serious damages of business networks.



Using the industry-leading Cloud-Sandboxing technology, suspicious traffic and files can be reported and executed in the Sangfor Private Cloud-Sandbox environment. By observing the actual behaviors of the reported suspicious traffic, SANGFOR NGAF is able to effectively and timely identify the evasive, unknown, 0-day and advanced threats.

Risk Assessment Module

The exclusive risk assessment module of SANGFOR NGAF assesses the security level of the current network & system and identifies security vulnerabilities. Furthermore, security assessment reports will be provided to assist IT people to quickly diagnose & repair security vulnerabilities before the attacks even happen.



Defense

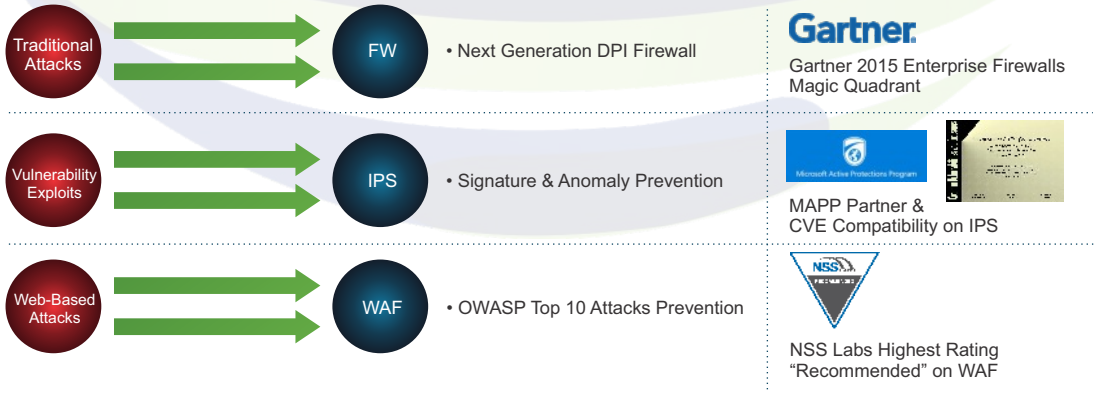
Traditional Firewall & Anti-Virus

Leading IPS - Intrusion Prevention System

SANGFOR NGAF provides various types of intrusion prevention protection. It performs inspection not only by signature matching, but also for its Gray-Scale Threat Correlation Analysis Engine which ensures suspicious traffic are analyzed and threats can be identified with higher accuracy for not known and anomaly threats.

NSS Labs Recommended WAF - Web Application Firewall

SANGFOR NGAF effectively defends against the 10 major types of web-based attacks identified by the Open Web Application Security Project (OWASP). It leverage built-in comprehensive web-based signatures for detecting popular web-based attacks, including SQL injection, XSS, CSRF, Buffer overflow, password cracking ,etc. SANGFOR NGAF is also the only vendor in the industry to have obtained the highest rating" Recommended" from NSS Labs on Web Application Firewall test.



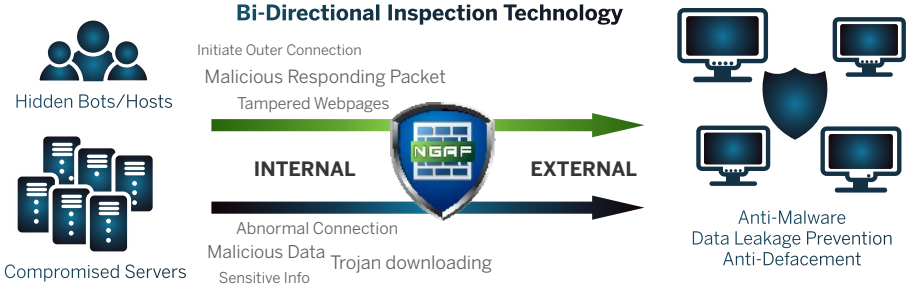
Remediation

Advanced Anti-Malware Protection & Anti-Virus

By inspecting the suspicious inside-out connections and behaviors from internal hosts, SANGFOR NGAF unveils hidden threats existing in the network and blocks the control connections to external attacker to avoid data leak and future intrusion. The NGAF is also equipped with a stream-based anti-virus for HTTP, FTP, SMTP & POP3, protocols, etc.

Botnet Detection, DLP (Data Leakage Prevention) & Anti-Defacement

Inside & Outside malicious behaviors and connections inspection is required to pinpoint the infected bots and endpoints. By inspecting the suspicious inside-outside connections and behaviors from internal hosts, SANGFOR NGAF unveils hidden threats existing in the network and blocks control connections to external attacker to avoid data leak and future intrusion. SANGFOR NGAF can also detect and send out an alarm when a website is tampered with, and can also detect any unsafe links to virus/ads.

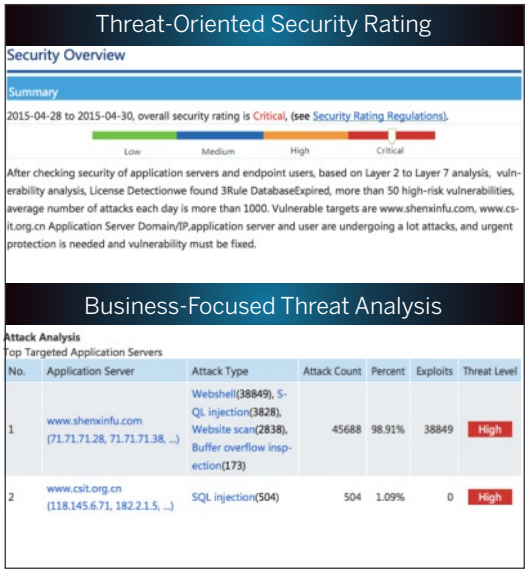


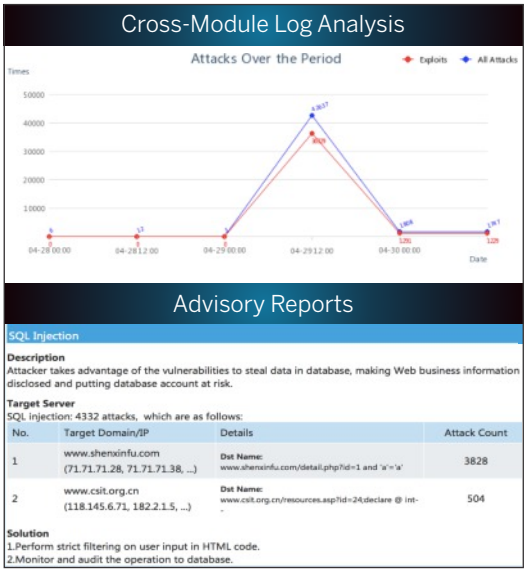
Backtracking

Comprehensive & Intelligent Reporting Tools

SANGFOR NGAF Platform provides the most comprehensive visibility reporting capability to allow IT managers gain full visibility of the network, endpoints and the business servers to facilitate the organization's security management. Unlike the other solutions available on the market,

SANGFOR Security Reports are simple & intuitive by telling you where the issues are located, what damages they could cause and how you can protect yourself against it. IT managers also have the possibility to choose whether they would like or not to receive daily, weekly or monthly report about the network status and create relevant security policies.





SANGFOR NGAF Platform

Best Value for Money

Designed with our customers' needs in mind, SANGFOR developed the NGAF as an affordable, high performance & complete threat protection solution for enterprises. With the new and advanced threats bypassing traditional defenses, a new approach to threat defense, visibility and response is needed.

Sangfor developed a holistic approach based on 4 key principles : Prediction, Defense, Remediation & Backtracking. You can now Predict the attacks & threats before they even happen, Defend your Network and if any suspicious is detected, it will be Remediated and with its Backtracking capabilities, you can analyze the reports to timely and efficiently set up network security policies.

Product Family

Model	M4500-F-I	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	Desktop	1U	1U	1U	1U	2U	2U	2U	2U	2U
RAM	2G	4G	4G	4G	4G	4G	8G	16G	24G	32G
HD Capacity	SSD 32GB	SSD 32GB	SSD 32GB	320GB	320GB	500GB	500GB	500GB +4G CF	500GB +4G CF	500GB +4G CF
Firewall Throughput*	1 .5 Gbps	2 Gbps	3 Gbps	6 Gbps	8 Gbps	12 Gbps	18 Gbps	20 Gbps	30 Gbps	80 Gbps
Threat Prevention Throughput*	480 Mbps	550 Mbps	850 Mbps	950 Mbps	1.7 Gbps	3 Gbps	8 Gbps	12 Gbps	20 Gbps	40 Gbps
IPsec VPN Throughput	200 Mbps	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	300	500	1000	1500	3000	4000	5000	10000	10000
Concurrent Connections (TCP)	250,000	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)	15,000	50,000	60,000	100,000	110,000	130,000	210,000	250,000	320,000	400,000
Power and Hardware Specifications										
Dual Power Supplies	N/A	N/A	N/A	N/A	N/A	√	√	√	√	√
Power [Watt] (Typical)	60W	60W	100W	100W	250W	300W	300W	500W	500W	500W
Temperature	0 ~40°C	0~ 40 °C	0~ 40 °C	0~ 40°C	0~ 40°C	0~ 40°C	0~ 40°C	0~ 40°C	0~ 40°C	0~ 40°C
Relative Humidity	5%~95% non-condensing	5%~95% non-condensing	5%~95% non-condensing	5%~95% non-condensing	5%~95% non-condensing	5%~95% non-condensing	5%~95% non-condensing	5%~95% non-condensing	5%~95% non-condensing	5%~95% non-condensing
System Dimensions (W×L×H mm³)	275 x 175 x 44.5	430 x 300 x 44.5	430 x 300 x 44.5	430 x 300 x 44.5	430 x 300 x 44.5	430 x 500 x 89	430 x 500 x 89	430 x 500 x 89	440 x 600 x 90	440 x 600 x 90
System Weight	1.5 Kg	3.85 Kg	3.85 Kg	6.65 Kg	6.65 Kg	20.0 Kg	20.0 Kg	20.0 Kg	20.0 Kg	20.0 Kg
Network Interfaces										
Bypass (Copper)	N/A	1 pair	1 pair	2 pairs	4 pairs	3 pairs	5 pairs	4 pairs	2 pairs	2 pairs
10/100/1000 Base-T	3	4	6	4	8	8	10	8	4	8
SFP	N/A	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	N/A	2	4
Optional Interface & 10G Fiber SFP *	N/A	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	RJ45×1
USB Port	2	2	2	2	2	2	2	1	2	2

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

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

SANGFOR NGAF Product Features

PREDICTION

Risk and Cloud Intelligence

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 system vulnerabilities
Real-time Vulnerability Scanner	- Discover vulnerabilities in real-time while guarantee zero infection to the protected system
SANGFOR Threat Intelligence Service	-Threat Intelligence to deliver the latest vulnerabilities, malware and security incidents information with advisory alerts for policies creation.
Cloud-based Sandbox Threats Analysis	- Identify in real-time emerging and new threats with Cloud Sandboxing technology

DEFENSE

Firewall

Firewall	- Intelligent DoS / DDoS prevention - SSL VPN & IPsec VPN - IPv6 & IPv4 supported
Link Load Balance	- Auto link load balance per traffic load and application type

Threats Prevention

Full SSL Inspection	-SSL inspection to all security modules including IPS, WAF, ATP, Access control, etc.
Cross-Module Intelligent Protection	- Policy association of IPS, WAF and APT prevention modules - Cross-module visibility reporting analysis
Advanced Threat Prevention	- APT (Advanced Persistent Threat), Remote Access Trojan, Botnet and Malware Detection
Anti-Virus	- Scan and kill viruses infecting HTTP, FTP, SMTP and POP3 traffic as well as viruses infecting compressed data packets.

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
Certificate & Partnership	- Common Vulnerabilities and Exposures (CVE) compatibility certified - Microsoft Active Protections Program (MAPP) partnership

Web Application Firewall

Web-based Attack Prevention	- Defend against the 10 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 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 restricted by file type according to blacklist - Specify access privilege of sensitive URL such as the admin login page for risk prevention
Buffer Overflow Detection	- Defend against buffer overflow attacks
Detection of HTTP anomalies	- Analyzes anomalies of the fields of the HTTP protocol via single parsing

REMEDIATION

Data Leakage Prevention

Data Leakage Prevention	- Control and detection over multiple types of sensitive information 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

Anti-Defacement

Gateway Anti-Defacement	- Options of page replacement/page redirection/mirror site and sending out alarm when website tampering is detected - Detect unsafe links to virus/ads on protected webpage

Anti-Malware

Anti-Malware	-Anti-Malware signature database, covering threats type of Trojan, AdWare, Malware, Spy, Backdoor, Worm, Exploit, Hacktool, Virus, etc.

BACKTRACKING

Visibility Reporting

Built-In Report Center	- Full visibility to network, endpoint and business servers with multi-dimensional analysis of risks, vulnerabilities, attacks, threats, traffic and behaviors - Threats analysis for specific attack separated in three parts : description, target and solution
Report Subscription	- Support XML, PDF format and automatically send to pre-defined mailbox on daily/weekly/monthly basis

OTHERS

Deployment

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

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

SANGFOR TECHNOLOGIES

SANGFOR is the leading vendor of Application Security, Optimization and Internet Access Management in Asia. Founded in 2000, SANGFOR set a clear goal to build high performance, reliable and secure network devices that increase the business growth of our clients and at the same time decrease their Total Cost of Ownership (TCO).

SANGFOR currently has 55 representative offices located in major cities of mainland China, Hong Kong, Singapore, Malaysia, Indonesia, Thailand, United Kingdom and United States of America, with over 2000 employees, which 40% of them are dedicated to R&D.

In 2014, SANGFOR has got a record-breaking income and has continuously invested 20% of the revenue into R&D each year. So far, SANGFOR has provided solutions to over 28,000 businesses partners in various industries, among which lists a number of Fortune 500 companies, as well as hundreds of local government departments and famous education institutions.

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.
- "Business Security Contribution" Award in 2010 by Communication World.
- Sangfor SSL VPN no. 1 in Network Security market in Mainland China, Hong Kong & Taiwan according to Frost & Sullivan.
- 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 Magic Quadrant for Secure Web Gateways (2011-2015).
- Sangfor WANO listed for 3 consecutive years in the Gartner Magic Quadrant for WAN Optimization (2013-2015).
- Sangfor NGFW listed in the Enterprise Network Firewalls Magic Quadrant by Gartner (2015).
- Reviewed by NSS Labs with a "Recommended" rating in 2014 for SANGFOR NGFW (WAF test).

Vision

Become the Global Leading Vendor of Advanced Network Solutions.

Mission

Provide Network Innovation, Focus on Network Security, Optimization and Virtualization.

Values

- Continuous Innovation
- Collective Commitment
- Customer & Result Oriented
- Caring for Employees

Our Notable Clients

SANGFOR
www.sangfor.com

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

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 , Boulevard Mid Valley City, Lingkaran Syed Putra,
Kuala Lumpur, Malaysia
Tel: (+60) 3 2201 0192
Fax: (+60) 3 2282 1206

SANGFOR THAILAND
29 Vanissa Building 4th Floor, Unit 4G, Soi Chidlom,
Ploenchit Road, Lumpini, Patumwan, Bangkok, Thailand
Tel: (+66) 2 254 5884
Fax: (+66) 2 254 5884

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 : Take Back Control of your Network
- WANO : LAN Speed on your WAN
- NGAF : Best Value for Money
- Easy Connect: Anywhere, Anytime and on Any Devices

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

NGAF_BR_P_NGAF-Brochure_20160309