SANGFOR NGFW Competition Brief

	SANGFOR	Fortinet	PaloAlto	Checkpoint	Sonicwall	Sophos	Mcafee	Cyberoam	Watchuard
Signature-based anti-malware	●	●	●	●	○	◎	◎	○	○
Heuristic based anti-malware	●	○	●	●	○	○	○	○	○
Sandboxing cloud	●	●	●	●	○	○	●	○	●
Intrusion Prevention System	●	●	●	●	●	●	●	●	●
MAPP & CVE	●	●	None CVE	None CVE	None CVE	None CVE	●	None CVE	None
Risk assessment	●	◎	○	○	○	○	○	○	○
Web Application Firewall	●	○	○	○	○	○	○	◎	○
Web Filter & App Control	●	●	●	●	●	●	●	●	●
Bandwidth management	●	◎	◎	○	◎	◎	◎	◎	○
Buil-in reporting	●	◎	●	●	◎	◎	◎	●	◎
Service-level threat report	●	○	○	○	○	○	○	○	○
Auto Link load balance	●	●	○	○	●	●	●	●	●
Solution Position *	**Affordable enterprise-grade security solution, threat-oriented**	**List of features, but suffering poor performance after enabling multiple functions.**	**Expensive enterprise-grade security solution, traffic & activity focused**	**Different blades are required to achieve different function. High cost**	**Provide average features for each function modules, SMB oriented solution**	**Provide average features for each function modules, SMB oriented solution**	**Legacy security vendor, SMB oriented solution**	**Listed in Gartner MQ for UTM, not for NGFW. Poor performance, none enterprise security features**	**Limited enterprise-grade security features: Failed in NSS Labs NGFW evasive testing**

●:Good, ◎: Not as good as, ○: Not Available

Standard NGFW function: FW, IPS, anti-virus, BM, Web fiter & application control, anti-virus, VPN, reporting

Key enterprise-grade solution criteria: Signature& heuristic based anti-malware, Sandboxing technology. IPS capability, Performance

Notes: SANGFOR NGFW provides anti-malware, cloud-based sandboxing, reporting capability for free, while other vendors normally require costly subscription.

SANGFOR NGFW Overview

Characteristics

Smart Firewall for Smart Protection

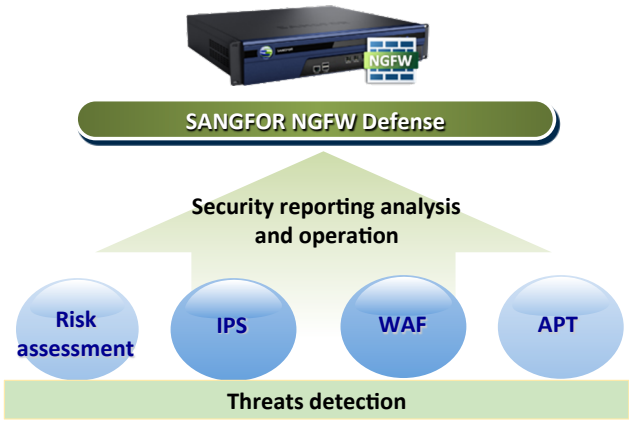
- **Proactive protection: Risk Visibility is Equally Important to Attack Prevention**
  - Sandboxing cloud, Anti-malware, Risk assessment
- **Streamline management: Keep it Simple: Consolidated and Simplified**
  - NGFW+WAF; Service-level security reporting
- **Efficient performance: No Compromise between Security and Performance**
  - One-pass & Multi-core; Sangfor Regex engine

Highlights

- **Listed in Gartner MQ for Enterprise Firewall 2015**
- **Earned "Recommended" rating from NSS Labs for WAF**
- **CVE compatibility & MAPP partner on IPS**
- **Equipped with industry-leading sandboxing technology for APT solution**
- **Exclusive features:** Exclusive service-level threat reporting, risk assessment, Reputation & heuristic anti-malware; Free cloud-based sandboxing, NGFW+ WAF design
- **Bring the core value:** Help to mitigate risks, streamline security operation, ensure performance
- **Lower TCO:** Low TCO for a enterprise-grade security solution

Solution Modules

- **Threats detection:** Advanced security threats identification
- **Risk assessment:** Identify security loopholes
- **IPS:** Prevention against vulnerability exploits
- **WAF:** Enhanced prevention to web-based attacks and protection to web applications
- **APT:** Pinpoint compromised endpoints& sandboxing for emerging threats
- **Security reporting analysis and operation:** streamline security management



DEPLOYMENT	SOLUTION & BENEFITS
Internet Gateway	• Next generation security to deal with emerging threats
DMZ (public-facing application)	• Protect public-facing applications from various attacks. Anti-defacement. Data breach prevention
Gateway+DMZ	• Protect both endpoints and public-facing applications in DMZ • Save a WAF(Web Application Firewall)
Data center	• High performance • FW+IPS+WAF+APT for threats prevention • Security reporting to facilitate security operation • Real-time risk assessment for identifying security loopholes • Unified threats detection& reporting. SANGFOR NGFW can act as 2nd tier FW as needed.
WAN Edge	• Clean up traffic traversing through WAN in case endpoints in branch networks get infected or compromised for facilitating intrusions to DC. • Manage both security and branch user behaviour and traffic through a single SANGFOR NGFW, support entrap management • Reporting for monitoring branch network security, traffic and activities
Mirror mode	• Monitor security events without interrupting the business • Generate security reports for security operation • Real-time vulnerability analysis to discover and help to repair system vulnerability timely
2nd tier of protection	• Asymmetrical protection to increase defense capability • Assess security loopholes and generate reports • Security reporting to streamline security operation
In front of core biz server (internal network, DC)	• APT threats prevention • Security reporting; • Risk assessment module, especially on real-time vulnerability assessment module • IPS +WAF+APT with cross-module intelligence