SANGFOR NGAF Product Features

Firewall

• Networking

- Policy routing, static routing, dynamic routing: RIPv1/v2, OSPFv2/v3, BGP4, and GRE.
- Application policy-based forwarding, NAT (1-1 NAT, many-to-one NAT, NAT46, NAT64, and many-to-few NAT), VLAN tagging
- IPv6 & IPv4 supported
- Support multi cast traffic, SNMP v1,v2,v3, and Syslog server with UTF-8 format
- Intelligent Dos/ DDos prevention
- ARP spoofing prevention
- 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

- Support user authentication with LDAP Server, local user database
- Support 2FA authentication with Google Authenticator and Microsoft Authenticator

• IPsec VPN

- IKE Version: IKEv1, IKEv2
- IPSec Protocol: AH, ESP
- D-H Group: Support group 1,2,5,14,15,16,17,18
- IPSec Authentication Algorithm: MD5, SHA1, SHA256, SHA384, SHA512
- IPSec Encryption Algorithm: DES, 3DES, AES-192, AES-256. SANGFOR_DES
- Auto VPN, support creating and manage VPN connection from Central Management Console Support SDWAN path selection policy

• SD-WAN

- Intelligent Routing: Specific application routing, support routing based on remaining bandwidth, and best quality routing based on QOE detection
- Dynamic Routing: RIP, OSPF, BGP
- Tunnel Failover: Supports failure second-level switchover
- Easy to deploy with step by step email instructions
- Visualization of equipment operating status and geographic location distribution
- Visualization of VPN link status and delay
- Configuration batch management-support
- Support for GRE
- Support access to the centralized management platform (Central Manager), for unification management of branch appliances
- Support for SD-WAN networking solution, rapid deployment of VPN through Sangfor Central Manager
- Support for IPv6 services to meet the needs of user networks with IPv6 requirements

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
- AI based malware detection engine, covering threats type of Trojan, AdWare, Malware, Spy, Backdoor, Worm, Exploit, Hacktool, Virus, etc.
- Use cloud intelligence to prevent unknown and advanced threat.

• 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.

• 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

SANGFOR NGAF Product Features

Web Application Firewall

• Web-based attack prevention
- Support SNORT based and semantic detection engine to defend against the 10 top major web-based attacks identified by the OpenWeb Application Security Project (OWASP)
- Provide dedicated(not mix with IPS) Web-based attack signature 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. 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, Log & 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

• Logging
- Support local log storage for security logs, access logs, admin operation logs, SSL VPN logs
- Support centralized security logs from multiple devices to Sangfor Platform-X

• Configuration Wizard
- Guideline for deployment and policy configuration

• Deployment
- Gateway (Route mode) | Bridge mode | Span/Mirror mode | Multiple Bridge mode (2- 4 bridges) | Virtual Wire

• High Availability
- HA Fail-over time less than 1 second
- Active-Active | Active-Passive

• Bypass
- Hardware bypass in the event of hardware failure

• Central Management
- Support central management of multiple NGAFs
- Support quick deployment from Central Management Console
- Support Restful API to integrate with third-party devices