



Visionary in 2022 Gartner® Magic Quadrant™ for Network Firewalls

# SANGFOR NETWORK SECURE NSF-1200A-I

Sangfor Network Secure (previously known as Sangfor NGAF) is the world's first next-generation firewall that combines the latest AI Technology, Cloud Threat Intelligence, NG-WAF, IoT Security, and SOC Lite.

Experience unrivaled protection, simplified management, and effortless operation with Sangfor Network Secure.



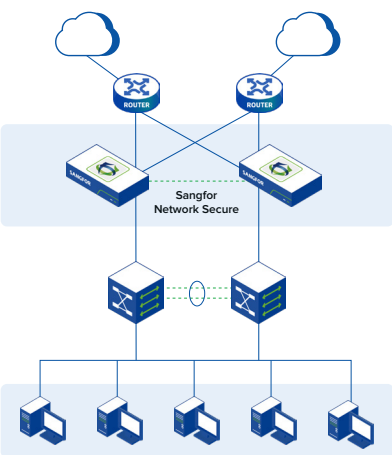
Performance	NSF-1200A-I	Hardware Specifications	NSF-1200A-I
Firewall Throughput <sup>1,2</sup>	20Gbps	Form Factor	1U
Application Control Throughput (64K HTTP/Enterprise Mix) <sup>1,3</sup>	14Gbps/12.5Gbps	RAM	8GB
IPS Throughput (64K HTTP/Enterprise Mix) <sup>1</sup>	3.5Gbps/3Gbps	Storage	128GB SSD
NGFW Throughput (64K HTTP/Enterprise Mix) <sup>1,4</sup>	3.5Gbps/3Gbps	Power Supply Type	Dual AC, Hot-Swapping
Threat Prevention Throughput (64K HTTP/Enterprise Mix) <sup>1,5</sup>	2Gbps/1.5Gbps	Power Input	100-240V, 50/60Hz
Web Application Protection Throughput (64K HTTP/Enterprise Mix) <sup>1,6</sup>	2.5Gbps/1.2Gbps	Power Consumption (Average)	28W
IPsec VPN Throughput <sup>1,7</sup>	1.8Gbps	Power Consumption (Max)	40W
Max IPsec VPN Tunnels	1000	Operating Temperature	0°C – 45°C
Recommended Maximum SSL VPN Users	200	Humidity	5% - 90% non-condensing
Concurrent Connections	2,000,000	System Weight	7.96kg
New Connections	90,000	Length x Width x Height (mm)	400 x 430 x 44.5
Virtual Domains (Recommended/Max)	3/6	Certificates	CE, FCC, ROHS
Interface & IO	NSF-1200A-I	Interface & IO	NSF-1200A-I
Hardware Bypass (Copper)	2 Pairs	Optional Interface Card	• 2 x GE RJ45
10/100/1000 Base-T	8 (Fixed onboard)		• 2 x GE SFP
1G SFP	N/A		• 4 x GE RJ45
10G SFP+	2 (Fixed onboard)		• 4 x GE SFP
40G QSFP+	N/A		• 8 x GE RJ45
Network Slots (In Use/Total)	0/1		• 8 x GE SFP
Dedicated Management Interface	1 (Fixed onboard)		• 2 x GE RJ45 & 2 x GE SFP
		• 4 x GE RJ45 & 4 x GE SFP	
		• 2 x 10GE SFP+	
		• 4 x 10GE SFP+	
		Serial Port	1 x RJ45
		USB Port	2

## Remarks

- All throughput performance data is measured under laboratory conditions. Actual performance may vary based on configuration and network environment.
- Firewall Throughput is measured with 1518 Bytes UDP packets.
- Application Control throughput is measured with Firewall and Application Control enabled.
- NGFW Throughput is measured with Firewall, Application Control, Bandwidth Management, and IPS enabled.

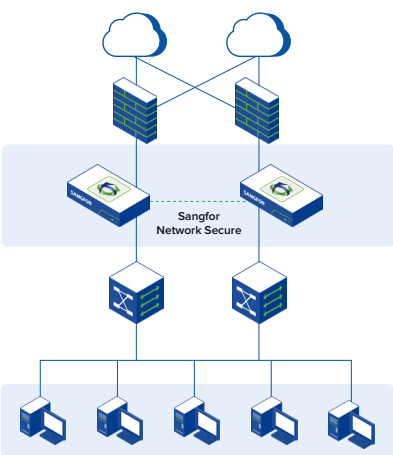
- Threat Prevention Throughput is measured with Firewall, Application Control, Bandwidth Management, IPS, and Anti-Virus enabled.
- Web Application Protection Throughput is measured with Firewall, Application Control, Bandwidth Management, IPS, and WAF enabled.
- IPsec VPN Throughput includes Sangfor-to-Sangfor device connection and Sangfor-to-3rd party device connection scenarios.
- All Pictures shown are for illustration purpose only. Actual Product may vary.

## Key Scenarios



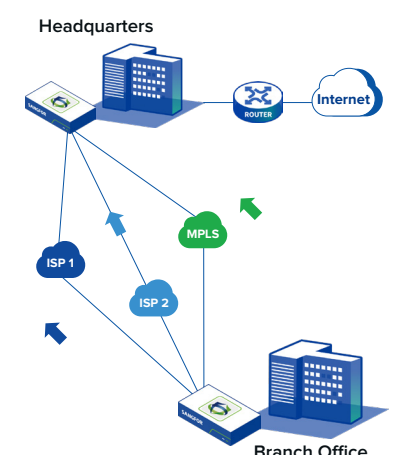
### Network Protection

- ✓ AI, Threat Intelligence & WAF
- ✓ Complete asset & threats visibility
- ✓ Auto threat mitigation
- ✓ Avoid misconfigurations



### 2<sup>nd</sup>-Tier Firewall

- ✓ Extra layer of protection
- ✓ Effortless deployment
- ✓ No configuration changes
- ✓ Built-in hardware bypass



### Secure SD-WAN

- ✓ Boost network agility
- ✓ Guarantee business continuity
- ✓ Strengthen security control
- ✓ Reduce TCO

## Feature List

### Networking & Deployment

- Deployment Modes: Routed Mode (Layer 3), Transparent/Bridge Mode (Layer 2), Virtual Wire Mode, Bypass Mode, Hybrid Mode
- IPv6-Ready: IPv4, IPv6, or IPv4/IPv6 dual-stack deployment
- Interfaces: Physical, VLAN (802.1Q tagging & trunking), Sub-interface, Loopback
- PPPoE Support: Physical interfaces and sub-interfaces
- Interface Definition: Define interfaces as WAN, LAN, DMZ without hardware constraints
- Supports GRE and GRE tunneling
- Interface Aggregation: LACP Mode and Static Mode (Round Robin, Hash, and Active-Standby)
- Link Health Detection: ARP, DNS, Ping, BFD
- Jumbo Frame: Supported on physical interfaces
- Customizable network and security zones
- DHCP Features: DHCP, DHCPv6, DHCP & DHCPv6 relay, IP reservation (IPv4 & IPv6)
- DNS Capabilities: DNS proxy, DNS transparent proxy, DNS64, DDNS
- ARP Proxy
- Static routing, policy-based routing, multicast routes, reverse path forwarding, ECMP
- Policy Routing: By source/destination IP, ISP, country/region service, application type
- Link Load Balancing: Round robin, bandwidth ratio, weighted least traffic, priority link
- Protocols: RIPv1/v2, RIPNG, OSPFv2/v3, BGP/BGP4+
- Supports Route redistribution
- OSPF supports access list and route maps, graceful restart
- Supports route testing to verify the routing result
- Displays routing table on GUI
- NAT Features: SNAT, DNAT, Bidirectional NAT/PAT (Modes 1:1, 1:N, N:1, M:N), NAT64, NAT46, NAT66, DNS-mapping
- Application Layer Gateways (ALG): FTP, RTSP, SQLNET, PPTP, TFTP, H.323, SIP
- Availability Features: Active-Active, Active-Standby, Hardware Bypass

### IPsec VPN

- Supports: Sangfor VPN, IPsec VPN
- Site-to-site IPsec VPN (static IP, dynamic IP, dynamic domain)
- IKEv1 and IKEv2
- Works in tunnel mode
- IPsec protocols: AH and ESP
- Supports main mode and aggressive mode
- Authentication methods: pre-shared key and certificate
- Local & peer ID: IP address, Domain String(FQDN), User String(USER\_FQDN)
- DH Group & Perfect Forward Secrecy: group1(MODP1024), group2(-MODP768), group5(MODP1536), group14(MODP2048), group15(MODP3072), group16(MODP4096), group17(MODP6144), group18(MODP8192), group19(ECP256), group20(ECP384), group21(ECP512), group22(-MODP1024\_160), group23(MODP2048\_224), group24(MODP2048\_256), group25(ECP192), group26(ECP224), group27(ECP224\_BP), group28(ECP256\_BP), group29(ECP384\_BP), group30(ECP512\_BP).
- IPsec encryption algorithms: DES, 3DES, AES/AES128, AES192, AES256, Sangfor\_DES
- IPsec authentication algorithms: MD5, SHA1, SHA256, SHA384, SHA512
- NAT-T, DPD
- Supports setup expiration time of IPsec VPN tunnels
- Supports VPN tunnel auto rebuild during heartbeat failure or HA failover
- VPN tunnel status monitoring, including traffic, latency, packet loss, etc.
- Configuration wizard for Sangfor VPN or IPsec VPN

### SSL Decryption

- SSL/TLS inspection: Outbound traffic to the Internet and inbound traffic to application servers
- TLS 1.3 decryption

## Feature List

### SSL VPN

- Supports SSL VPN in CS (client-server) mode
- Hash Algorithms: MD5, SHA1, SHA256, SHA384, SHA512
- Encryption algorithms: DES, 3DES, AES/AES128, AES192, AES256, Sangfor\_DES.
- Protocols: TCP, UDP, ICMP
- Browser Compatibility: IE, Edge, Firefox, Chrome, etc.
- OS Compatibility: Windows, Android, iOS, macOS, etc.
- Authentication: Primary authentication (local/LDAP), secondary authentication (hardware ID, TOTP with Google/Microsoft authenticators)

### SD-WAN & Central Management

- Dynamic Path Selection: Based on custom SLAs (jitter, latency, packet loss), bandwidth, application type
- Application categorization by type to meet different SLA requirements
- SOFAST Engine: Link optimization in high packet loss environments
- SD-WAN tunnel failover and link failover
- Zero-touch provisioning via email template
- Map view of device location
- Centralized management with Sangfor Central Manager
- Centralized monitoring of device status, CPU/RAM/disk usage, traffic
- Centralized remote control of devices
- Centralized security policy distribution
- Centralized VPN deployment and configuration

### Bandwidth Management

- Manage bandwidth by application, user/group, IP address, schedule, country/region, sub-interface, VLAN interface, VPN tunnel
- Bandwidth Control: Bandwidth guarantee, bandwidth limit, upload & download speed, speed for single IPs

### Access Control & Authentication

- Stateful Packet Inspection (Stateful Firewall)
- Deep Packet Inspection (DPI): Identifies applications to allow/deny access
- Built-in Application Signature Database: Over 9,000 signatures, including P2P, IM, gaming, video streaming, email, proxy apps
- "From top to bottom, first match basis" method
- Access control based on source/destination IP, source/destination zone, source port, FQDN, MAC, User, service, applications, schedule, etc.
- Supports persistent connections
- Supports matching count for access control policies
- Policy optimizer: One-click to identify abnormalities in access control policies, including redundancy, duplication, and conflicts
- Automatically records the access control policy lifecycle
- Geolocation blocking: Allow/deny access from certain countries/regions
- Connection control based on source IP, destination IP, bidirectional IP
- User authentication: Captive portal, MAC/IP address binding, or Single Sign-On (SSO)
- Authentication with LDAP, RADIUS, POP3. Supports user imports via CSV file
- Single-Sign-On (SSO) with Microsoft AD, RADIUS, Web, etc.
- HTML-based customizable captive portal

### ARP, DoS/DDoS Attack Protection

- DoS/DDoS attack protection for both the network and the device itself
- SYN flood, ICMP flood, ICMPv6 flood, UDP flood, DNS flood, ARP flood prevention
- IP scan and port scan prevention
- Packet-based attack prevention, e.g., TearDrop Attack, IP fragment, LAND attack, WinNuke attack, Smurf attack, Ping of Death, Unknown protocol
- Bad IP option, Bad TCP option prevention
- ARP Spoofing Protection

### Content Security

- URL filtering with a built-in URL signature database
- Supports customized URL signatures
- File filtering in both upload and download directions. Supported file types include pictures, text files, compressed files, and executables
- Gateway malware inspection: Cloud-based Sangfor Neural-X (threat intelligence, sandbox) and on-premises Sangfor Engine Zero (AI malware inspection engine). Able to prevent known and unknown threats
- Malware inspection supports protocols like HTTP, HTTPS, FTP, SMB, SMTP, POP3, IMAP
- Malware inspection supports file types including movies, music, image, text, compressed files (up to 16 layers), executables, documents, scripts
- Remove malware from detected malicious files
- Whitelist based on MD5 and URL
- In-depth inspection of email body and attachments
- Inserts warning messages into email subjects to caution users against opening malicious emails

### Web Application Firewall (WAF)

- Dedicated web application protection with a semantic detection engine, not with IPS
- Supports custom WAF rules
- Detects and protects against 13 major types of attacks, including SQL injection, XSS, web shells, CSRF, system command injection
- Protection against the OWASP Top 10 web application security risks
- Defense against buffer overflow attacks, including URL length overflow, HTTP header overflow, POST entity overflow
- CC (Challenge Collapsar) attack prevention
- XXE (XML External Entity) attack prevention
- Detect HTTP request anomalies
- Prevent cookie-based attacks
- Cloud Intelligence: for the latest IP reputation and IP blacklist data
- Real-time Web Vulnerability Scanner: Analyzes web application vulnerabilities in passive mode and generates reports in HTML format
- Application Hiding: Prevent targeted attacks with the feedback information from the applications
- Weak password detection and brute-force attack prevention
- Restrict upload of blacklisted file types
- Specify access privileges for sensitive URLs such as the admin page

## Feature List

### APT Protection & Intrusion Prevention System (IPS)

- Malicious Domain & URL Detection
- Remote Access Trojan (RAT) Detection
- Suspicious Traffic Detection: Discover abnormal behavior on standard ports
- Vulnerability Exploit Protection: Protect against vulnerability exploits targeting systems, applications, middleware, databases, explorer, Telnet, DNS, and more
- Brute-Force Attacks: Protection profiles for SSH, Telnet, RDP, NTLM, FTP, etc.
- Botnet Detection: Detect botnet client communication, include DNS tunneling, ICMP tunneling, HTTP tunneling etc.
- Correlate with Sangfor Endpoint Secure to detect hidden botnet activity
- Cloud-based analysis engine for enhanced detect
- Dedicated protection profiles for client & server scenarios
- Supports custom IPS rules

### IoT Security

- Detect IoT devices across the network through proactive scans and traffic learning
- Detected IoT devices are presented as an asset list
- Support Spoofed Access detection & control via IP, MAC, and Device Type
- Dedicate IoT IPS signature database

### SOC Lite

- Proactive asset detection and guidance for fixing potential risks
- Business System & Client Threats Dashboard: Monitor and manage threats to business systems and clients, including severity levels, threat types, kill-chain steps, top security events
- Ransomware Protection Dashboard: Detect and manage ransomware-related risks such as weak passwords, risky ports, etc. Helps administrators create ransomware protection policies
- Account Security Dashboard: Detect account-related threats, including weak passwords, abnormal login activity, brute-force attacks, compromised accounts
- Whitelist & Blacklist
- Cloud Deception: Utilize cloud resources to deploy decoys to confuse attackers, track malicious behaviors, locate and block the source of the threat

### Certifications

- CE, FCC, RoHS
- ICSA Firewall, Gartner Magic Quadrant, CyberRatings

### Logging & Reporting

- Built-in log and report center available by default for all hardware models
- Records logs to local disk including access control logs, session logs, traffic audit logs, user authentication logs admin operation logs, SSL VPN logs, local ACL logs.
- Traffic/session monitoring by device, application, IP, interface
- Displays traffic rankings by user/IP, group, application type & application category.
- Options for daily, weekly, or monthly security report subscriptions
- Supports security reports in PDF format
- Supports syslog in Common Event Format
- Supports sending syslog to multiple target servers

### Management

- Support manage via WebUI, SSH, CLI, serial port etc.
- WebUI supports TLS1.0, TLS1.1, TLS1.2, TLS1.3
- Supports role-based authorization for admin users. Default roles include security admin, system admin, and audit admin
- Admin user supports local password, TACACS server, and RADIUS server
- Automatic or manual configurations backup
- Backup configuration file to FTP, TFTP & SFTP by schedule
- Out-of-Band Management (OOBM)
- Time setting supports synchronization with local PC and NTP servers
- Firmware version rollback
- SNMP v1/v2c/v3, SNMP trap
- Email alerts for hardware abnormality, resource usage, security event, HA status, etc.
- Troubleshooting via WebUI; Identify packet drop reasons by policy, interface, etc.

### Integration

- Sangfor Neural-X: Latest threat intelligence, cloud-based URL/App classifications, etc.
- Sangfor Endpoint Secure: Share intelligence and locate and mitigate malicious processes with quick/full scan and one-click kill
- Sangfor Cyber Command: Security log analysis
- Sangfor Platform-X: Centralized management
- Restful APIs available to integrate with third-party SIEM, SOC, etc.

#### Remarks

\* All the feature above is based on Network Secure firmware version 8.0.85 and higher

## • Ordering Guide •

### Sangfor Network Secure Hardware

SKU	Description
NSF-1200A-I	NSF-1200A-I, hardware appliance. 1U, 8 x GE RJ45, 2 x 10G SFP+, 1 x available NIC slot. 128GB SSD. Dual AC power supply.

### Sangfor Network Secure Bundle Subscription

SKU	Description
ESS-1200A-1Y/2Y/3Y/5Y	NSF-1200A-I, Essential Bundle (SSL VPN, Site-to-Site IPsec VPN, Stateful Firewall, Bandwidth Management, URL Filtering, Application Control, IPS, Botnet Prevention, Email Security, SOC Lite, Basic Security Reporter).
PM-1200A-1Y/2Y/3Y/5Y	NSF-1200A-I, Premium Bundle(SSL VPN, Site-to-Site IPsec VPN, Stateful Firewall, Bandwidth Management, URL Filtering, Application Control, IPS, Botnet Prevention, Email Security, SOC Lite, Basic Security Reporter, Engine Zero, Neural-X).
ULT-1200A-1Y/2Y/3Y/5Y	NSF-1200A-I, Ultimate Bundle including Premium Bundle(SSL VPN, Site-to-Site IPsec VPN, Stateful Firewall, Bandwidth Management, URL Filtering, Application Control, IPS, Botnet Prevention, Email Security, SOC Lite, Basic Security Reporter, Engine Zero, Neural-X) & Basic device management & Complimentary 30 units of Endpoint Secure Protect Agents with one Endpoint Secure manager.
SDWE-1200A-1Y/2Y/3Y/5Y	NSF-1200A-I, Secure SD-WAN Essential bundle (SSL VPN, Site-to-Site IPsec VPN, Stateful Firewall, Bandwidth Management, URL Filtering, Application Control, IPS, Botnet Prevention, Email Security, SOC Lite, Basic Security Reporter, SD-WAN, 1 * Central management branch access license).
SDWP-1200A-1Y/2Y/3Y/5Y	NSF-1200A-I, Secure SD-WAN Premium bundle (SSL VPN, Site-to-Site IPsec VPN, Stateful Firewall, Bandwidth Management, URL Filtering, Application Control, IPS, Botnet Prevention, Email Security, SOC Lite, Basic Security Reporter, Engine Zero, Neural-X, SD-WAN, 1 * Central management branch access license).

### Sangfor Network Secure A-La-Carte Subscription

SKU	Description
FNX-1200A-1Y/2Y/3Y/5Y	NSF-1200A-I, Neural-X License, Threat Intelligence & Analytics, Unknown Threat & Advanced Threat Defense, Value-Added Cloud Service.
FEZ-1200A-1Y/2Y/3Y/5Y	NSF-1200A-I, Engine Zero License, AI-Powered Malware Detection, Anti-Malware, Anti-Virus.
WAF-1200A-1Y/2Y/3Y/5Y	NSF-1200A-I, Web Application Firewall Module, support Signature-based protection, Semantic Engine, Application Hiding, HTTP Anomalies Detection, Vulnerability Scanner, Advanced Security Reporter.
SDWL-1200A-1Y/2Y/3Y/5Y	NSF-1200A-I, Secure SD-WAN License, support SD-WAN path Selection, Sangfor SOFAST packet loss optimization engine and 1 * central management branch access(BBCAL-ID).
IOTL-1200A-1Y/2Y/3Y/5Y	NSF-1200A-I, IoT Security license, support IoT/OT device discovery, access control & security protection.
CDEP-1200A-1Y/2Y/3Y/5Y <sup>1</sup>	NSF-1200A-I, Cloud Deception License, supporting cloud integration to simulate business systems, helping to discover internal malicious behavior and mitigate lateral movement.

### Sangfor Network Secure Hardware & Software Service

SKU	Description
SUS-1200A-1Y/2Y/3Y/5Y	NSF-1200A-I, Software Upgrade Services.
TSS-1200A-1Y/2Y/3Y/5Y	NSF-1200A-I, 24*7 Technical Support Services.
HRTF-1200A-1Y/2Y/3Y/5Y	NSF-1200A-I, Return to Factory (5 Business Days Shipment after Receipt) Hardware Service.
HSDS-1200A-1Y/2Y/3Y/5Y	NSF-1200A-I, Network Secure, Same Day Shipment Hardware Service.
HNBD-1200A-1Y/2Y/3Y/5Y	NSF-1200A-I, Network Secure, Next Business Day Delivery Hardware Service.
H244G-1200A-1Y/2Y/3Y/5Y	NSF-1200A-I, 24x7x4 Delivery Hardware Service.

#### Remarks

1. Cloud Deception availability varies across regions. Please check with Sangfor local representatives for details.

Network Secure Datasheet\_DS\_P\_NSF-1200A-I\_20240709