

SANGFOR NGAF

M5250-F-I

Sangfor Next Generation Application Firewall is the world first fully integrated NGFW + WAF with pre-event, during-event and post-event defense for all business assets.

A truly integrated firewall solution, providing holistic overview of the entire organization security network, with ease of management for administration, operation and maintenance.

NGAF-5250 is the ideal Converged Security solution for Small & Medium Enterprises. It is also ideal for Branch Deployment.

Gartner

ICSA labs
CERTIFIED FIREWALL-CORPORATE



Performance & Capacity	NGAF M5250-F-I
Dimension	1U
Firewall Throughput	3.5Gbps
NGFW Throughput ¹	2.45Gbps
WAF Throughput	2.45Gbps
IPS & WAF Throughput	2.1Gbps
Threat Protection Throughput ²	1.75Gbps
IPSec VPN Throughput	375Mbps
Max IPSec VPN Tunnels	500
Concurrent Connections (TCP)	1,000,000
New Connections (TCP)	60,000
Dual Power Supply	N/A

Compliance	NGAF M5250-F-I
Certifications	CE, FCC

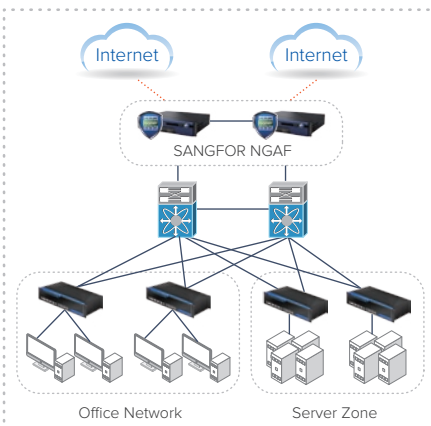
Hardware Specifications	NGAF M5250-F-I
RAM	4Gb
Storage HD Capacity	64G SSD (Customizable up to 2T)
Power [Watt] Max	100W
Operating Temperature	0°C~40°C
Humidity	5%~95% non-condensing
System Weight	3.85 Kg
System Dimensions	300x430x44.5 mm (W x L x H)

Network Interfaces	NGAF M5250-F-I
Bypass (Copper)	1 pair
10/100/1000 Base-T	6
SFP	2
10G Fiber SFP	N/A
Optional Interface & 10G Fiber SFP*	N/A
Serial Port	1 x RJ45
USB Port	2

¹ NGFW is measured with Firewall, Bandwidth Management, IPS, Application Control

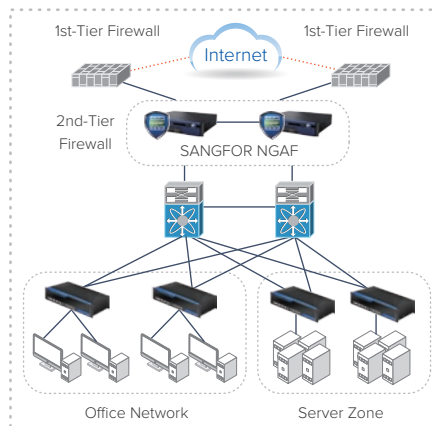
² Threat Prevention is measured with Firewall, Bandwidth Management IPS, Application Control, Anti Virus

Deployment Modes



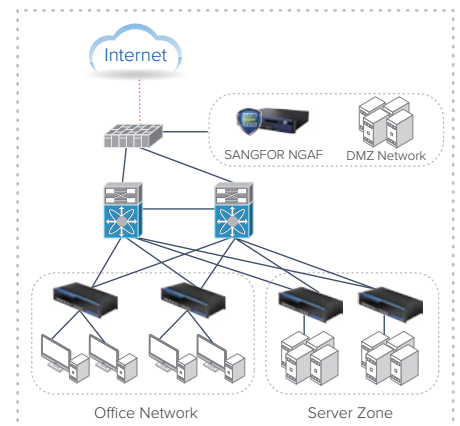
End-to-End Protection

- End-to-end protection from endpoint to business system
- Total visibility of the entire organization security status
- Provides High Availability features with Multi-line HA and Load Balancing
- Proactive early detection and prevention at the gateway to prevent attacks from reaching the network



Double Security (2nd-Tier Firewall)

- Double protection which complement existing firewall security policies to ensure full protection
- Providing regulatory compliance
- Simplified deployment, reducing downtime
- Provides flexibility of security design and security policies for different business requirements



DMZ Protection

- Dedicated business system protection for advance protection, without impacting other networks
- Providing regulatory compliance
- Simplified deployment, reducing downtime
- Minimize operation and maintenance works to monitor and troubleshoot security incidents

Key Features

① Lower TCO Converged Security Solutions

Fully converged security solution from endpoint to business systems, without the needs of manual integration & consolidation of each feature, as well as additional hardware, which results in lower operational and maintenance costs.

② Comprehensive Business Systems Protection

Comprehensive business systems protection with built-in Web Application Firewall and Vulnerability Scanners, which is critical for internal systems as well as "internet-facing" systems. Business systems protection is easily enabled via advanced license, without any integration or additional appliance required.

③ User Friendly

A single simplified operation & maintenance with interactive GUI, which provides ease of configuration, maintenance, troubleshooting and reporting for IT managers, administrators and operations team.

Security Features

① Converged Security

Integrated L2–L7 Security features:

- DoS/DDoS: Inbound, Outbound, Attack Protection
- Content Security
- IPS
- Anti-virus
- Engine Zero: AI based anti-malware, anti-virus
- APT
- WAF
- Data Leakage Prevention
- Bandwidth Management
- Web Scanner
- Real-Time Vulnerability Scanner
- Security Reporter
- Neural-X: Cloud threat intelligence and analytics

② Comprehensive WAF

- Web Application Firewall (WAF).
- Semantic Engine
- Support OWASP Top 10 WAF requirements.
- Recommended by NSS.

Software Features

01 Networking

Interface: Physical Interface, Sub Interface, VLAN Interface, Aggregated Interface

Routing: Static, Policy-based, RIP, OSPF, BGP

Network Functions: ARP, DNS, DHCP, SNMP, NAT, High Availability

02 Access Control

User: Import / export from external server

Authentication: SSO/LDAP/RADIUS

Application: ACL and application rules

URL Filter: Supported

03 VPN

SANGFOR VPN, IPSEC VPN and SSL VPN supported
SDWAN auto path selection

04 Management

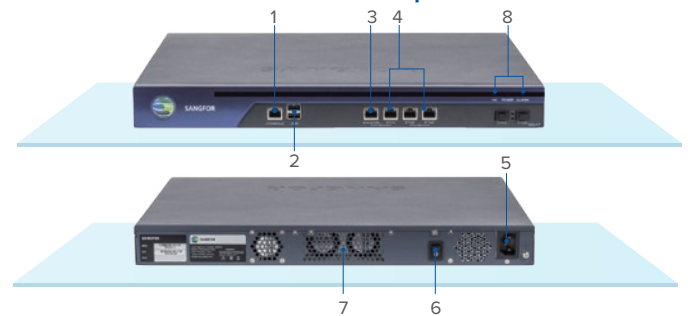
SNMP v1, v2c, v3

Syslog

Real-Time Vulnerability Scanner

Central management

Hardware Description



1. Default Interface

2. USB ports

3. Management Console

4. Line Interface

5. Power outlet

6. Switch

7. Fan Trays

8. LED Indicators

NGAF M5250-F-I Ordering Guide

DESCRIPTION

NGAF Hardware & Base Software (Mandatory)

M5250-F-I, Hardware, SSL VPN for 30 concurrent users, Site-to-site IPsec VPN with 10 IPsec Clients included.

NGAF Hardware & Base Software (Mandatory)

M5250-F-I, NGFW license suite, FW, BM, IPS, URL&APP, Email Security, Sandboxing, Risk Assessment, Security Visibility, Basic security reporter: 1 year, 3 years or 5 years options.

NGAF-Add Advanced Business System Total Protection License (Optional)

M5250-F-I, Add Anti-Defacement Module, Web Application FW, Application Hiding, HTTP Anomalies Detection, Data Leak Protection, Web Scanner, Vulnerability Scanner, Advanced Security Reporter : 1 year, 3 years or 5 years options.

NGAF Software Module, Service Subscription (Optional)

Engine Zero, Neural-X, Security Butler, 1 year, 3 years or 5 years options.

IPSec VPN Remote Client, IPSec VPN Remote Client , 1 User

NGAF-NGFW Software Upgrade, 24*7 Technical Support, NGAF RTF (Return to Factory), Hardware Service (Mandatory)

M5250-F-I, NGFW software upgrade, 24*7 technical support, NGAF RTF hardware service : 1 year, 3 years or 5 years options.

For more information on Sangfor' full range of support & services, please contact your local representative.

NGAF_DS_P_NGAF5250-Datasheet_20190410