DATASHEET

NSFOCUS

Next-Generation Firewall

Multi-Layered Comprehensive Security Solution

OVERVIEW

As the digital attack surface grows, both the volume and sophistication of cyberattacks increase. The resulting data theft and network disruptions can both threaten your reputation and business, a comprehensive security solution is an absolute necessity in every IT infrastructure.

NFNX3-HDB1080

NSFOCUS delivers fully integrated Next Generation Firewall (NGFW) to combat these emerging threats while reducing complexities and increasing operational efficiencies, which includes powerful security features such as firewall, IPS, DLP, Antivirus, Application Control, VPN service, and URL Filtering to combat cyber-attacks and threats.

With the new hardware and software architecture, NSFOCUS NGFW uses intelligent technologies in security solutions to block known and unknown cyber attacks accurately. It tracks the real-time state of network sessions, maintains deep subscriber and application awareness, and uniquely mitigates attacks based on more granular details than traditional firewalls. Leveraging the enhanced performance provided by its dedicated product architecture, NSFOCUS NGFW delivers a high-performance engine carrying out strong capabilities of IPS, and Antivirus without impacting the network traffic.

FEATURES

High-performance software and hardware platforms

» The firewall series uses advanced 64-bit (MIPS) multi-core processors and caches.

Attack protection

» Detects and prevents various attacks, including Land, Smurf, Fraggle, ping of death, Tear Drop, IP spoofing, IP fragment, ARP spoofing, reverse ARP lookup, invalid TCP flag, large ICMP packet, IP/port scanning, and common DDoS attacks such as SYN flood, UDP flood, DNS flood, and ICMP flood.

SOP 1:N virtualization

» Uses container-based virtualization technology. An NSFOUCS firewall can be virtualized into multiple logical firewalls, which have the same features as the physical firewall. Each virtual firewall can have its own security policy and can be managed independently.

Security zone

» Allows you to configure security zones based on interfaces and VLANs.

Packet filtering

» Allows you to apply standard or advanced ACLs between security zones to filter packets based on information contained in the packets, such as UDP and TCP port numbers. You can also configure time ranges during which packet filtering will be performed.

KEY FEATURES

Data leakage prevention (DLP)

Supports email filtering by SMTP mail address, subject, attachment, and content, HTTP URL and content filtering, FTP file filtering, and application layer filtering (including Java/ActiveX blocking and SQL injection attack prevention).

Intrusion prevention system (IPS)

Supports real-time active interception of DDoS, brute force disassembly, port scanning, sniffing, worms and other network attacks or malicious traffic, and protects internal network information from infringement.

Anti-virus (AV)

Uses a high-performance virus detection engine and a daily updated virus signature database to prevent attacks from over 5 million viruses.

Deep Visibility

Get insight into applications, users, and devices across the attack surface.

Access control

» Supports access control based on users and applications and integrates deep intrusion prevention with access control.

ASFP

» Dynamically determines whether to forward or drop a packet by checking its application layer protocol information and state. ASPF supports inspecting FTP, HTTP, SMTP, RTSP, and other TCP/UDP based application layer protocols

AAA

» Supports authentication based on RADIUS/HWTACACS+, CHAP, and PAP.

Blacklist

» Supports static blacklist and dynamic blacklist.

NAT and VRF-aware NAT

VPN

» Supports L2TP, IPsec/IKE, GRE, and SSL VPNs. Allows smart devices to connect to the VPNs.

Routing

» Supports static routing, RIP, OSPF, BGP, routing policies, and application- and URL-based policy-based routing.

Security logs

» Supports operation logs, zone pair policy matching logs, attack protection logs, DS-LITE logs, and NAT444 logs.

Traffic monitoring, statistics, and management

» Supports static routing, RIP, OSPF, BGP, routing policies, and application- and URL-based policy-based routing

Integrated security service processing platform

» Highly integrates the basic and advanced security protection measures to a security platform.

Application layer traffic identification and management.

» Uses the state machine and traffic exchange inspection technologies to detect traffic of P2P, IM, network game, stock, network video, and network multi-media applications.

» Uses the deep inspection technology to identify P2P traffic precisely and provides multiple policies to control and manage the P2P traffic flexibly.

Highly precise and effective intrusion inspection engine

» Uses the Full Inspection with Rigorous State Test (FIRST) engine and various intrusion inspection technologies to implement highly precise inspection of intrusions based on application states. The FIRST engine also supports software and hardware concurrent inspections to improve inspection efficiency.

NFNX3-HDB3080

Realtime virus protection

» Uses the stream-based antivirus engine to prevent, detect, and remove malicious code from network traffic.

Categorized filtering of massive URLs

» Uses the local & cloud mode to provide 139 categorized and 130 million URL libraries, and supports over 20 million URL filtering rules. Provides basic URL filtering blacklist and whitelist and allows you to query the URL category filtering server online.

Complete and updated security signature database

» NSFOCUS has a senior signature database team and world-class security labs that can provide a precise and up-to-date signature database.

Integrated link load balancing feature

» Uses link state inspection and link busy detection technologies, and applies to a network egress to balance traffic among links.

Integrated SSL VPN feature

» Uses USB-Key and the enterprise's existing authentication system to authenticate users, providing secure access to the enterprise network.

Intelligent management

» Intelligent security policy management—Detects duplicate policies, optimizes policy matching rules, and detects and proposes security policies dynamically generated in the internal network.

» SNMPv3—Compatible with SNMPv1 and SNMPv2.

» CLI-based configuration and management.

» Web-based management, with simple, user-friendly GUI

» Centralized log management based on advanced data drill-down and analysis technology—Requests and receives information to generate logs, compiles different types of logs (such as syslog and binary stream logs) in the same format, and compresses and stores large amounts of logs. You can encrypt and export saved logs to external storage devices such as DAS, NAS, and SAN to avoid the loss of important security logs.

» Abundant reports—Include application-based reports and stream-based analysis reports.

» Various exported report formats—Include PDF, HTML, word, and txt.

» Report customization through the Web interface—Customizable contents include time range, data source device, generation period, and export format.

Hardware Specification

Model	NFNX3-HDB680	NFNX3-HDB1080	NFNX3-HDB1180
Dimensions (W*D*H)	330mm*230mm*43.6mm Desktop	435mm*440mm*44.2mm 1RU	435mm*440mm*44.2mm 1RU
Interfaces	1 × Console 10 × GE Copper 2 × SFP	1 × Console 8 × GE Copper 2 × GE Combo 2 × GE Bypass	1 × Console 2 × MGMT 18 × GE Copper 8 × GE Combo 4 × GE Bypass 2 × SFP+
Expansion slots	N/A	N/A	N/A
Network interface modules (Optional)	N/A	N/A	N/A
Storage	1*64G SD CARD(Optional)	1*480G SSD (Optional)	1*480G SSD (Optional)
Flash	512M	512M	4G
SDRAM	2G	2G	4G
USB	2	2	2

Weight	1.6Kg	3.7Kg	3.7Kg
Power supply	AC	Dual AC	Dual AC
Power consumption	150W	150W	150W
MTBF	100,000 hours	100,000 hours	100,000 hours
Temperature	Operating: 0°C to 45°C (32°F to 113°F) Storage: –40°C to +70°C (–40°F to +158°F)	Operating: 0°C to 45°C (32°F to 113°F) Storage: –40°C to +70°C (–40°F to +158°F)	Operating: 0°C to 45°C (32°F to 113°F) Storage: –40°C to +70°C (–40°F to +158°F)
Operation modes	Route, transparent, and hybrid		

Model	NFNX3-HDB1480	NFNX3-HDB1780	NFNX3-HDB3080	NFNX3-HDB3280
Dimensions (W*D*H)	435mm*440mm*44.2mm 1RU	435mm*440mm*44.2mm 1RU	435mm*440mm*44.2mm 1RU	435mm*440mm*44.2mm 1RU
Interfaces	1 × Console 2 × MGMT 18 × GE Copper 8 × GE Combo 4 × GE Bypass 2 × SFP+	1 × Console 1 × MGMT 16 × GE Copper 4 × GE Combo 6 × SFP 2 × SFP+	1 × Console 1 × MGMT 16 × GE Copper 4 × GE Combo 6 × SFP 2 × SFP+	1 × Console 1 × MGMT 16 × GE Copper 4 × GE Combo 4 × SFP 6 × SFP+
Expansion slots	N/A	2	2	2
Network interface modules (Optional)	N/A	4-port SFP	4-port SFP	4-port SFP 6-port SFP+
Storage	1*480G SSD (Optional)	1*480G SSD (Optional)	1*480G SSD (Optional)	2*480G SSD (Optional)
Flash	4G	4G	4G	4G
SDRAM	4G	4G	4G	8G
USB	2	2	2	2
Weight	3.7Kg	5.4Kg	5.4Kg	5.6Kg
Power supply	Dual AC	Dual AC or DC	Hot-swappable, AC or DC	Hot-swappable, AC or DC
Power consumption	150W	150W	150W	150W
MTBF	100,000 hours	100,000 hours	100,000 hours	100,000 hours

Temperature	Operating: 0°C to 45°C (32°F to 113°F) Storage: –40°C to +70°C (–40°F to +158°F)	Operating: 0°C to 45°C (32°F to 113°F) Storage: –40°C to +70°C (–40°F to +158°F)	Operating: 0°C to 45°C (32°F to 113°F) Storage: –40°C to +70°C (–40°F to +158°F)	Operating: 0°C to 45°C (32°F to 113°F) Storage: –40°C to +70°C (–40°F to +158°F)
Operation modes	Route, transparent, and hybrid			

Model	**NFNX5-HD5280**	**NFNX5-HD6480**	**NFNX5-T6280**
Dimensions (W*D*H)	435mm*440mm*44.2mm 1RU	435mm*440mm*44.2mm 1RU	660mm*440mm*88.1mm 2RU
Interfaces	1 × Console 1 × MGMT 16 × GE Copper 4 × GE Combo 4 × SFP 6 × SFP+	1 × Console 2 × MGMT 14 × GE copper 8 × SFP 8 × SFP+	1 × Console 4 × GE Combo
Expansion slots	2	4	8
Network interface modules (Optional)	4-port SFP 6-port SFP+	4-port SFP 6-port SFP+	8-port GE Copper (Slot 4-8) 8-port SFP+ (Slot 1-3)
Storage	2*480G SSD (optional)	2*480G SSD (optional)	2*480G SSD (optional)
Flash	4G	8G	4G
SDRAM	8G	16G	16G
USB	2	2	2
Weight	5.6Kg	10Kg	20.1Kg
Power supply	Hot-swappable, AC or DC	Dual hot-swappable, AC or DC	Dual hot-swappable, AC or DC
Power consumption	250W(AC) 450W(DC)	650W	650W
MTBF	100,000 hours	100,000 hours	100,000 hours
Temperature	Operating: 0°C to 45°C (32°F to 113°F) Storage: –40°C to +70°C (–40°F to +158°F)	Operating: 0°C to 45°C (32°F to 113°F) Storage: –40°C to +70°C (–40°F to +158°F)	Operating: 0°C to 45°C (32°F to 113°F) Storage: –40°C to +70°C (–40°F to +158°F)
Operation modes	Route, transparent, and hybrid		

AAA	Portal authentication RADIUS authentication HWTACACS authentication PKI/CA (X.509 format) authentication Domain authentication CHAP authentication PAP authentication
Firewall	SOP virtual firewall technology, which supports full virtualization of hardware resources, including CPU, memories, and storage Security zone allocation Protection against malicious attacks, such as land, smurf, fraggle, ping of death, teardrop, IP spoofing, IP fragmentation, ARP spoofing, reverse ARP lookup, invalid TCP flag, large ICMP packet, address/port scanning, SYN flood, ICMP flood, UDP flood, and DNS query flood Basic and advanced ACLs Time range-based ACL User-based and application-based access control ASPF application layer packet filtering Static and dynamic blacklist function MAC-IP binding MAC-based ACL MAC-Limitation 802.1Q VLAN transparent transmission Bandwidth control
Antivirus	Signature-based virus detection Manual and automatic upgrade for the signature database Stream-based processing Virus detection based on HTTP, FTP, SMTP, and POP3 Virus types include Backdoor, Email-Worm, IM-Worm, P2P-Worm, Trojan, Adware, and Virus Virus logs and reports
Deep intrusion prevention	Prevention against common attacks such as worm/virus, Trojan, malicious code, spyware/adware, DoS/DDoS, buffer overflow, SQL injection, and IDS/IPS bypass Attack signature categories (based on attack types and target systems) and severity levels (including high, medium, low, and notification) Manual and automatic upgrade for the attack signature database (TFTP and HTTP). P2P/IM traffic identification and control
Email/webpage/application layer filtering	Email filtering SMTP email address filtering Email subject/content/attachment filtering Webpage filtering HTTP URL/content filtering Java blocking ActiveX blocking SQL injection attack prevention
NAT	Many-to-one NAT, which maps multiple internal addresses to one public address Many-to-many NAT, which maps multiple internal addresses to multiple public addresses One-to-one NAT, which maps one internal address to one public address NAT of both source address and destination address External hosts access to internal servers Internal address to public interface address mapping NAT support for DNS Setting effective period for NAT NAT ALGs for NAT ALG, including DNS, FTP, H.323, ILS, MSN, NBT, PPTP, and SIP
VPN	L2TP VPN IPSec VPN GRE VPN SSL VPN
IPSEC VPN	ESP-DES-CBC/ESP-3DES-CBC/ESP-AES-128-CBC/ESP-AES-192-CBC/ESP-AES-256-CBC/ ESPAES-128-GCM/ESP-NULL/SM1-cbc-128/SM4-cbc
IPSEC VPN authentication algorithm	MD5/SHA1/SM3

IPV6	IPv6 status firewall IPv6 attack protection IPv6 forwarding IPv6 protocols such as ICMPv6, PMTU, Ping6, DNS6, TraceRT6, Telnet6, DHCPv6 Client, and DHCPv6 Relay IPv6 routing: RIPng, OSPFv3, BGP4+, static routing, policy-based routing IPv6 multicast: PIM-SM, and PIM-DM IPv6 transition techniques: NAT-PT, IPv6 tunneling, NAT64 (DNS64), and DS-LITE IPv6 security: NAT-PT, IPv6 tunnel, IPv6 packet filter, RADIUS, IPv6 zone pair policies, IPv6 connection limit
IEEE	IEEE 802.1X
High availability	SCF 2:1 virtualization Active/active and active/standby stateful failover Configuration synchronization of two firewalls IKE state synchronization in IPsec VPN VRRP
Configuration management	Configuration management at the CLI Remote management through Web SNMPv3, compatible with SNMPv2 and SNMPv1 Intelligent security policy

PERFORMANCE

Model	NFNX3-HDB680	NFNX3-HDB1080	NFNX3-HDB1180
Firewall throughput (1518/IMIX/64 Bytes)	600Mbps/400Mbps/200Mbps	1Gbps/800Mbps/220Mbps	2Gbps/1Gbps/400Mbps
NGFW+APP	500Mbps	600Mbps	1.2Gbps
NGFW+APP+IPS	400Mbps	600Mbps	1.2Gbps
Threat protection throughput (NGFW+APP+IPS+AV)	400Mbps	500Mbps	1Gbps
Maximum concurrent sessions	500k	900k	1.5M
Maximum new connections per second	10K	15K	20K
Maximum number of SSL VPN concurrent users	500	750	1000
SSL VPN throughput	100Mbps	100Mbps	150Mbps

Model	NFNX3-HDB1480	NFNX3-HDB1780	NFNX3-HDB3080	NFNX3-HDB3280
Firewall throughput (1518/IMIX/64 Bytes)	4Gbps/1.5Gbps/500Mbps	6Gbps/2Gbps/600Mbps	8Gbps/2.5Gbps/700Mbps	10Gbps/6Gbps/2Gbps
NGFW+APP	2.5Gbps	2.5Gbps	3.5Gbps	5Gbps
NGFW+APP+IPS	2.5Gbps	2.5Gbps	3.5Gbps	5Gbps
Threat protection throughput (NGFW+APP+IPS+AV)	2Gbps	2Gbps	2.5Gbps	4.5Gbps
Maximum concurrent sessions	2M	2.5M	2.5M	5M
Maximum new connections per second	20K	30K	50K	100K

Maximum number of SSL VPN concurrent users	1500	3000	4000	6000
SSL VPN throughput	200Mbps	220Mbps	220Mbps	800Mbps

Model	NFNX3-HD5280	NFNX5-HD6480	NFNX5-T6280
Firewall throughput (1518/IMIX/64 Bytes)	15Gbps/10Gbps/2.5Gbps	20Gbps/15Gbps/6Gbps	40Gbps/18Gbps/8Gbps
NGFW+APP	5.5Gbps	15Gbps	20bps
NGFW+APP+IPS	5.5Gbps	14Gbps	18Gbps
Threat protection throughput (NGFW+APP+IPS+AV)	5Gbps	14Gbps	18Gbps
Maximum concurrent sessions	5M	10M	16M
Maximum new connections per second	120K	240K	500K
Maximum number of SSL VPN concurrent users	6000	10000	30000
SSL VPN throughput	800Mbps	1.8Gbps	2.5Gbps