

NSFOCUS NIPS Datasheet



© 2000-2009 NSFOCUS INFORMATION TECHNOLOGY CO., LTD.

Product Overview

NSFOCUS Network Intrusion Protection System (NIPS) is the core of the NSFOCUS intrusion protection solution. As a new generation of security products that has independent intellectual property, NSFOCUS NIPS adopts the advanced intrusion detection technique, detects network traffic in real time, controls different traffic types based on the security policy, and blocks malicious traffic, such as hack attack, worms and viruses, Trojan and backdoors, spyware, and Botnet. At the same time, NSFOCUS NIPS prevents misused traffic such as P2P download, instant messaging, online video, stream media, and online games, keeps attacks outside the enterprise network, and ensures the security of enterprise information assets. For the application of intrusion protection, appropriate NSFOCUS NIPS products are chosen and deployed based on the actual network environment and traffic information to actively prevent attack traffic in real time.

Product Features

- **Highly converged integration platform**

NSFOCUS NIPS is an innovative and highly integrated IPS/IDS/Firewall platform. Its unique design enables NSFOCUS NIPS to provide the user with in-depth prevention from network layer to application layer. NSFOCUS NIPS addresses the problem of convergence between static defense of the firewall and dynamic defense of the IPS and provides users with a comprehensive prevention solution.

NSFOCUS NIPS integrates the powerful firewall function, and utilizes dynamic packets filtering technique based on the status detection to implement static defense; NSFOCUS NIPS provides dynamic defense with comprehensive and in-depth protocol analysis technique as the base and the protocol discover, protocol anomaly detection, and association analysis as the core.

NSFOCUS NIPS runs on a secure, reliable and effective hardware platform. The hardware platform is built with strict design and craftwork standard to guarantee high reliability; its unique hardware architecture improves the processing capacity and throughput greatly; the operating system is optimized and the security is reinforced to guarantee the system security and invulnerability.

- **Virtual system based on object**

NSFOCUS NIPS offers virtual intrusion protection system (VIPS) based on objects. Aiming at different net environments and security needs, it sets various rules and responding methods based on objects such as

security zone, IP address (group or segment), rule (group or set), time, and action. Every virtual system carries on different rule sets, detecting intellectually with different strategies against different objects.

Comprehensive rule database contains over 2000 detection signatures that have been carefully extracted and thoroughly tested by NSFOCUS Security Team. At the same time, NSFOCUS gets the top-level CVE Compatible certification by the compatible standard examination of the most famous international security disclosure organization CVE.

- **Comprehensive and elaborate attack prevention**

NSFOCUS NIPS provides virtual patches, prevents known and unknown attacks actively, and intercepts all hack attacks such as buffer overflow, SQL injection, brute force, denial of service, scan and reconnaissance, unauthorized access, worms and viruses, backdoors and Trojan, and spyware. Besides, NSFOCUS NIPS offers automated prevention against botnet so that the comprehensive and elaborate prevention helps users avoid security loss.

- **Complete and practical context management**

NSFOCUS NIPS can provide a powerful traffic sanitization function. Via the comprehensive and practical management of the content, NSFOCUS NIPS can monitor and control misused traffic, including IM, P2P download, online video, stream media and online games, to improve the efficiency of the enterprise.

NSFOCUS NIPS supports powerful traffic management function, using traffic controlling of quadruple, that is, overall dimension (protocol/port), part dimension (source/target IP address, net segment), time dimension (time) and traffic dimension (bandwidth), to realize the easy control of network traffic for users based on the policy configuration of the object.

- **Powerful and rich management capacity**

NSFOCUS NIPS supports zones, three working modes, that is, route, transparent and hybrid, and five zone modes including transparent (Layer 2), route (Layer 3), Monitor, Direct, and Mgt, which can be quickly deployed in various net environments. NSFOCUS NIPS also supports the fail-open mechanism and HA to avoid single point of failure.

NSFOCUS NIPS provides many responding methods, including active response (dropping packets and session) and passive response (firewall interaction, TCP Killer, email notification, console display, logs, printer output, customized command, XML files export, and snmp trap). Users can customize responding methods to meet their demands.

From system updates to report system, from attack alert to log backup, NSFOCUS NIPS can be totally run by the system backend periodically and automatically. This is called “zero management”. NSFOCUS NIPS supports both B/S and C/S management modes. The complete Chinese interface and report fit Chinese users’ operating habit. The Chinese rule database provides detailed description of all vulnerabilities, with solutions and patch download addresses.

Function List

Intrusion Prevention Technologies	
IP Fragments Reassembling	√
TCP Flow Convergence	√
TCP Status Tracing	√
Protocol Recognition	Over 100 Protocols
Protocol Analysis	√
Signature Detection	√
Associated Analysis	√
Protocol Abnormity Detection	√
Traffic Abnormity Detection	√
DoS Detection	√
Intrusion Detection and Block / Application Types	
Buffer Overflow	√
SQL Injection	√
Brute Force	√

Firewall Functions	
Stateful Firewall	√
Access Control	Granular Security Access Control Based on Source/Destination IP, Protocols, Time, VLAN and Security Zone
NAT	Support Bidirectional NAT, Static NAT, Dynamic NAT, and PAT
Policy Routing	Source/Destination IP, Port, Application Based Policy-Routing
Dynamic Routing	OSPF
VLAN Routing	√
VLAN Trunk	√
802.1Q	√
MPLS	√
Traffic Management	
Traffic Control Management	Application and Object-Oriented Traffic Control
Min. bandwidth	√

DoS Attacks	√
Scanning	√
Unauthorized Access	√
Worms & Virus	√
Trojan & Backdoors	√
Spyware	√
Bot Net	√
Zero-Day Attacks	√
P2P Downloading	√
IM	√
Online Game	√
Online Video	√
Steam Media	√
Intrusion Prevention Signature Database	
Signatures	2000+
Customized Signatures(Rules)	√
NSFocus ID Support	√
CVE ID Support	√
Bugtraq ID Support	√
Signatures Update	
Update Period	Per Week
Emergencies Real-time Update	√
Real-time Online Update	√
Scheduled Online Update	√

assurance	
Max. bandwidth assurance	√
Max. Session Limitation	√
Priority Setting	√
Active Response Mode	
Packets Dropping	√
Session Blocking	√
Console Display	√
Event Log	XML and DB
Protocol Replay	HTTP, FTP, SMTP, Telnet, POP3
Alarm via Email	√
User Customized Command	√
SNMP Trap(V1、V2、V3)	√
Syslog	√
Log & Report	
Log Classification	√
Log Record	> 50000 Entries per Second
Log Storage	MSDE, SQL Server, MySQL, Oracle
Log Backup	√
Log Cleanup	√
Log Recovery	√
Offline Analysis	Log Associated Analysis and Merger
Report Template	30+ Templates
Customized Report	√
Report Output	MS Word、HTML、JPG

Offline Update	√
Virtual IPS (VIPS)	
Virtual IPS System	Object-Oriented Virtual IPS(VIPS), Centralized & Unified Security Policy Management
High Availability	
Failure Open (BYPASS)	Internal Bypass External Bypass
Redundancy	Active-Active & Active-Standby Redundancy support
Redundancy Power Supply	√
Out-of-Band Management	√
Device Malfunction Self-Detection	√
Appliance Self-Security	
Security Kernel OS	√
Management Communication	Enhanced SSL Encryption
User Privilege Classification	√
Password Authentication	√
Certificate Authentication	√
Standard Radius & LDAP Authentication	√

Scheduled Report Delivery	√
Deployment	
Security Zone Mode	Transparent(Layer2), Routing(Layer3), Monitoring, Direct and Management Mode
Working Mode	Routing, Transparent, Hybrid Mode
Single Mgt.	√
Master-Slave Mgt.	√
Multi-level Mgt.	√
Management	
B/S Mgt.	Web Based, Support IE, Firefox, Netscape , Opera
Centralized Mgt.	NSFOCUS Security Center
SSH	Remote Assistance
CLI	√
Console Experience Mode	√
Language	English, Chinese
Traffic Analysis	√
Timer Synchronized	√

NSFOCUS NIPS 200, 600, 1200, 2000 Series Specifications

Specification \ Type		NIPS 200 Series	NIPS 600 Series	NIPS 1000 Series	NIPS 1200 Series	NIPS 2000 Series
Interfaces	Operating Interfaces	4*100M copper	8 *100M copper	10*1000M interface (SFM, MMF, and copper ports optional)	8*1000M interface (SFM, MMF, and copper ports optional)	8*1000M interface (SFM, MMF, and copper ports optional)
	Mgt. Interfaces	1* 100M copper	1*100M copper	N/A copper	1*100M copper	2*1000M copper
	Serial Port	1* RS232	1*RS232	1*RJ45	1*RJ45	1*RJ45
Performance	Throughput(bi-directional)	≤ 200Mbps	≤ 600Mbps	≤ 800Mbps	≤ 1.2Gbps	≤ 3Gbps
	Max concurrent TCP sessions	≤ 150,000	≤200,000	≤500,000	≤1,000,000	≤1,500,000
	New TCP sessions per second	≤ 100,000	≤ 150,000	≤ 200,000	≤ 300,000	≤ 500,000
	Max packet processing capacity(UDP 64bit)	≤200,000 pps	≤320,000 pps	≤600,000 pps	≤1,000,000	≤3,000,000 pps
	Latency (us)	<100 μs	<100 μs	<100μs	<100 μs	<100 μs

	Max. number of Policies	500	1,000	2,000	4,000	6,000
Physical characteristics	Dimension	320*428*44.5mm(1U)	320*428*44.5mm(1U)	440*392*88mm(2U)	528*426*88mm(2U)	512*430*88mm(2U)
	Weight	5.4 kg	5.4 kg	12 kg	14 kg	14 kg
	Power Supply	100-240V, AC, (50-60HZ), 4A, 180W	100-240V, AC, (50-60HZ), 4A, 180W	100-240V, AC, (50~60HZ), 5-8A,350W	100-240V, AC, (50~60HZ), 5-8A, 350W	100-240V, AC, (50~60HZ), 5-8A, 400W
				-36- -72V, DC, 25A, 350W	-36- -72V, DC, 25A, 350W	
	MTBF	≥100,000	≥100,000 hrs	≥100,000 hrs	≥100,000 hrs	≥100,000 hrs
	Operating Temperature	0-40°C	0-40°C	0-40°C	0-40°C	0-40°C
	Non-operating Temperature	-20-70°C	-20-70°C	-20-70°C	-20-70°C	-20-70°C
	Relative humidity	5%-95%, non-condensing	5%-95%, non-condensing	5%-95%, non-condensing	5%-95%, non-condensing	5%-95%, non-condensing
	Altitude	0-5,000m	0-5,000m	0-5,000m	0-5,000m	0-5,000m
Radiation standard	Class A, EN55022, FCC Part15	Class A, EN55022, FCC Part15	Class A, EN55022, FCC Part15	Class A, EN55022, FCC Part15	Class A, EN55022, FCC Part15	