DATASHEET

NSFOCUS

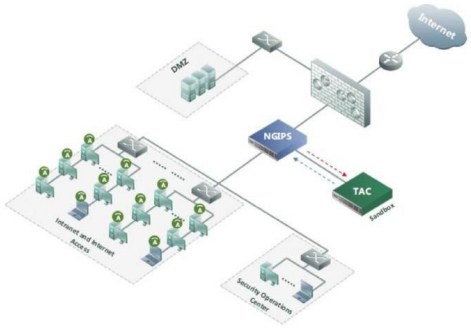
NGIPS

NEXT GENERATION INTRUSION PREVENTION SYSTEM

The NSFOCUS Next-Generation Intrusion Prevention System (NGIPS) provides comprehensive threat protection that blocks intrusions, prevents breaches, and safeguards your valuable assets.

NGIPS uses an innovative, multi-layer approach to identifying and addressing known, zero-day, and advanced persistent threats to protect you from malware, worms, spyware, back-door Trojans, data leakage, brute force cracking, protocol attacks, scanning/probing, web threats, and more. This approach combines signature and behavior-based detection, protocol and traffic anomaly detection, correlation analysis, deep packet inspection, and the latest threat intelligence to detect malicious sites and botnets.

An optional virtual sandboxing capability can be added to the NGIPS system using the NSFOCUS Threat Analysis Center (TAC) appliance. The TAC uses several detection engines to identify known and zero-day threats, including an IP reputation engine, anti-virus engine, static analysis engine, and virtual sandbox execution.



INTEGRATED THREAT INTELLIGENCE

The most dangerous cyber threats are the ones that can't be seen or detected until it is too late. In order to protect themselves, forward thinking companies are building threat intelligence directly into their network security infrastructure. The NGIPS integrates global threat intelligence from the NSFOCUS Threat Analysis to provide up-to-date protection from botnets, malicious sites, viruses and other discovered exploits.

ADVANCED PERSISTENT THREAT PROTECTION

The NGIPS can discover and block advanced threats by discerning anomalous network behaviors such as sensitive data leakage, file identification, and server illegal outreach. In addition, it prevents zero-day attacks through an optional TAC appliance that monitors CPU, network activity, memory utilization, system driver behavior and more in a virtual environment. This allows you to identify malicious activity and harmful executables before they reach your critical servers and desktops.

ACCURATE THREAT DETECTION

Legacy IPS products only analyzed data packets without considering the specific configuration of the end-systems. This caused many false positive alarms. For example, in some instances, a target system running an Apache web server would trigger events on Microsoft IIS related vulnerabilities or exploits. The NSFOCUS NGIPS provides accurate threat detection and event reporting through a combination of context data from the end-systems, IP reputation, user identity, geographical locations, and other user assets.

KEY BENEFITS

Comprehensive threat protection

Combines intrusion prevention, threat intelligence, and an optional virtual sandboxing capability to effectively address known, zero-day, and advanced persistent threats.

Networking and security features designed to keep you online

Integrates traffic prioritization, shaping, and DDoS protection to ensure bandwidth is available for your critical users, servers, and applications.

Scalable protection with industry leading price/performance

Designed for any size organization in a range of cost and performance-optimized virtual and hardware appliances that scale up to 20Gbps.

Simplified threat management

Can be deployed in a high availability configuration and provides advanced network management features, including threat visualization based on the attack chain, asset views, and more.

HIGHLIGHTS

Intrusion Prevention Threat Intelligence Threat Analysis Web Application Security Traffic Control

Context-aware User Identity Threat Visualization

ADAPTION TO COMPLEX ENVIRONMENTS

The NGIPS provides up to 20Gbps of application-layer data processing capacity and has flexible IPv4/IPv6 dual-stack adaptive capability to fully adapt to complex network environments.

HARDWARE SPECIFICATIONS
GIGABIT ETHERNET (GE) AND 10 GIGABIT ETHERNET (10GE)

		NIPS HD4200	NIPS HD4500	NIPS HD4700	NIPS HD6200	NIPS T9010	NIPS T9020
Interfaces	Onboard Interface	N/A	N/A	N/A	N/A	N/A	N/A
	Slot	4	4	8	8	4	4
	Extension Interface	Non-bypass NIC: 4*SFP/8*SFP/2*SFPP/4*SFPP; Bypass NIC：4*GE-B/8*GE-B/4*SFP-B/4*SFP-B-SM/4*SFP4GE-B/2*SFPP-B/2*SFPP-B-SM/4*SFPP-B/4*SFPP-B-SM	Non-bypass NIC: 4*SFP/8*SFP/2*SFPP/4*SFPP; Bypass NIC：4*GE-B/8*GE-B/4*SFP-B/4*SFP-B-SM/4*SFP4GE-B/2*SFPP-B/2*SFPP-B-SM/4*SFPP-B/4*SFPP-B-SM	Non-bypass NIC: 4*SFP/8*SFP/2*SFPP/4*SFPP; Bypass NIC：4*GE-B/8*GE-B/4*SFP-B/4*SFP-B-SM/4*SFP4GE-B/2*SFPP-B/2*SFPP-B-SM/4*SFPP-B/4*SFPP-B-SM	Non-bypass NIC: 4*SFP/8*SFP/2*SFPP/4*S FPP; Bypass NIC：4*GE-B/8*GE-B/4*SFP-B/4*SFP-B-SM/4*SFP4GE-B/2*SFPP-B/2*SFPP-B-SM/4*SFPP-B/4*SFPP-B-SM	Non-bypass NIC: 4*SFP/8*SFP/2*SFPP/4*SFPP; Bypass NIC: 4*GE-B/8*GE-B/4*SFP-B/4*SFP-B-SM/4*SFP4GE-B/2*SFPP-B/2*SFPP-B-SM/4*SFPP-B/4*SFPP-B-SM	Non-bypass NIC: 4*SFP/8*SFP/2*SFPP/4*SFPP; Bypass NIC: 4*GE-B/8*GE-B/4*SFP-B/4*SFP-B-SM/4*SFP4GE-B/2*SFPP-B/2*SFPP-B-SM/4*SFPP-B/4*SFPP-B-SM
	Max. Number of Business Interfaces	16*GE or 8*10GE interface	16*GE or 8*10GE interface	32*GE or 16*10GE interface	32*GE or 16*10GE interface	16*GE or 8*10GE interface	16*GE or 8*10GE interface
	Bypass	Optional	Optional	Optional	Optional	Optional	Optional
Management Interface	Management Interface	2GE	2GE	2GE	2GE	2GE	2GE
	Serial Port	1*RJ45	1*RJ45	1*RJ45	1*RJ45	1*RJ45	1*RJ45
	USB Interface	2	2	2	2	2	2
Storage	Hard Disk	1T	1T	1T	1T	1T	1T
Performance	Real-world Throughput	2 Gbps	4 Gbps	6 Gbps	8 Gbps	10 Gbps	20 Gbps
	HTTP Throughput	1 Gbps	2 Gbps	3 Gbps	4 Gbps	5 Gbps	10 Gbps
	Max. Concurrent TCP Connections	2 Million	4 Million	5 Million	6 Million	10 Million	15 Million
	TCP Connections Per Second	60,000	120,000	150,000	200,000	400,000	600,000
	Latency (μs)	<40 μs	<40 μs	<40 μs	<40 μs	<40 μs	<40 μs
Physical Features	Dimensions	435* 560* 44 mm (1U)	435* 560* 88 mm (2U)	435* 560* 88 mm (2U)	435* 560* 88 mm (2U)	443* 626* 88 mm (2U)	443* 626* 88 mm (2U)
	Power Supply	100-240V AC, (50-60HZ), 5-2.5A, 300W Redundant	100-240V AC, (50-60HZ), 4.5-2A, 300W Redundant	100-240V AC, (50-60HZ), 4.5-2A, 300W Redundant	100-240V AC, (50-60HZ), 4.5-2A, 300W Redundant	100-240V AC, (47-63HZ), 3-7A, 450W Redundant	100-240V AC, (47-63HZ), 3-7A, 450W Redundant
	Weight	9.6 Kg	20 Kg	20 Kg	20 Kg	19.7 Kg	19.7 Kg
	Mean Time Between Failure (MTBF)	> 100,000 hours	> 100,000 hours	> 100,000 hours	> 100,000 hours	> 100,000 hours	> 100,000 hours
	Operating Temperature	0-40°C	0-40°C	0-40°C	0-40°C	0-40°C	0-40°C

FEATURES*

Intrusion Prevention

- Over 9000 attack signature databases
- Detect and prevent attack events including overflow, worm, virus, backdoor program, Trojan, port scanning, spyware, etc.
- Protection IEC 61850 and IEC 60870-104 based SCADA systems
- Complex password configuration and customized weak password dictionary

150+ Application-layer Protocol Detection

DDoS Protection

- ICMP (Ping) flood
- UPD flood
- SYN flood
- ACK flood
- DNS reply flood
- DNS req flood
- TCP port scanning
- UDP port scanning
- ARP spoofing
- HTTP Get flood
- HTTP Post flood

Threat Intelligence

- On-line query (TI Portal)
- Cloud-based detection (C&C/ malicious file/malicious URL/IP blacklist)
- Threat analysis and traceback
- Off-line threat intelligence package

Support for IPv4/IPv6 Dual Stacks

Pre-defined Policy Templates and Zero Initial Configuration

- DMZ server protection template
- Intranet protection
- Template
- Web server protection template
- Windows server template
- UNIX server template
- Template derived from built-in policies

Web Security

- XSS
- SQL Injection
- Malicious URL
- Webshell

Data Leakage Prevention

- Sensitive data identification
- File identification

Malicious File

- Signature-based anti-virus
- Heuristics-based anti-virus

Sandboxing

High Availability

- Active/Standby mode
- Configuration synchronization

Global Blacklist & Whitelist

- Malicious IP database
- DNS blacklist
- IP blocking
- Blocking service
- Built-in whitelist

URL Filtering

Traffic Management

- NetFlow
- Bandwidth management
- Traffic analysis

Anti-Virus (AV)

- Combination of own AV database and third-party advanced AV database
- Over 100,000 stream AV
- Over 13 million heuristics AV
- Support HTTP, FTP, SMTP, POP3, IMAP, NFS, SMB2, ICS protocols (IEC 61850, IEC 60870)
- AV file storage and export for tracing analysis
- Real-time AV database update
- Response to spotlight incidents

Server Security

Traffic Integrity Analysis

Traffic Mirroring

Geolocation Database

Asset Identification

Link Status Synchronization

User Management

- User authentication
- Automated user correlation

Static Routing

IPMAC Binding

DNS Security

SNMP Security Syslog

Application Management

Response methods

- Block
- Pass through
- Alert
- Quarantine
- Capture packet

Open APIs

- Integration with external network and security management applications to share events and log data

© COPYRIGHT 2022, NSFOCUS. ALL RIGHTS RESERVED NGIPS | DS220930