DATASHEET

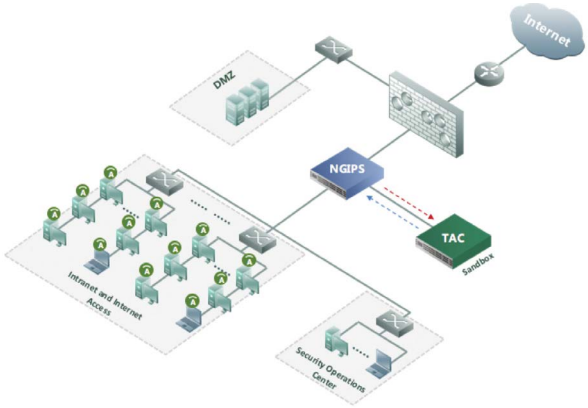
NGIPS

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 (TA) appliance. The TA 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.

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.

BENEFITS AND KEY FEATURES

Comprehensive threat protection
The NSFOCUS NGIPS 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
The NGIPS 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
The NGIPS is 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
The NGIPS 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.

ATTACK DETECTION CAPABILITIES

Intrusion Detection and Advanced Threat Prevention	• Flow-based detection: Supports IP fragment reassembly and TCP flow reassembly. • CVE-compatible signature library: Detect and blocks malware, worms, spyware, backdoor Trojans, scanning/probing, brute force cracking and other malicious traffic. Custom-coded signatures are supported. • Server exception detection: Inspects illegal outreach behaviors of a server through automated learning of the server's legitimate outreach behaviors. • Sensitive data protection: Detects and protects against leakage of sensitive data (ID number, bank card number, phone number, etc.) and special files. • Botnet protection: Executes appropriate protection actions based on malicious host and C&C server address reputation, which is updated in real-time. • Client-side vulnerability detection: Add application-specific vulnerability rules, such as Adobe, IE, and Office to address increasing attacks exploiting client-side application vulnerabilities. • Granular application management and traffic controls. • Supports SCADA-based vulnerability detection and protection • Online malware detection and blocking.
DoS/DDoS Protection	• Provides DoS/DDoS attack mitigations, and supports TCP/UDP/ICMP/ACK Flooding, UDP/ICMP Smurfing, and other common DoS/DDoS attacks.

DEPLOYMENT AND MANAGEMENT CAPABILITIES

Protection Configuration	• Supports configuration templates, and assigns the same protection policies to various asset clusters. • Can be used out-of-box.
High Availability	• Supports Active/Standby and Active/Active (asymmetric routing) deployment. • Supports automated failover and fail-back: If a hardware or software failure is detected, the NGIPS can automatically switch to the bypass channel, with no impact to traffic.
Protocol Encapsulation	• Supports IPv6. • Supports IPv6 and IPv4 hybrid network deployment. • Supports encapsulation protocol like VLAN 802.1Q, BGP, MPLS, QinQ, PPPOE, and can adapt to diversified network environments.
Management Capabilities	• Provides Web-based remote GUI management. • Provides centralized management. • Provides hierarchical management functions to meet requirements for tiered deployments in large-scale networks.
Alert Response Methods	• Supports multiple alert responses, such as session blocking, IP segregation, email notification, and SNMP/Syslog.

HIGHLIGHTS

Intrusion Prevention

Threat Intelligence

Threat Analysis

Web Application Security

Traffic Control

Context-aware User Identity

Threat Visualization

Physical and Virtual Appliances

TA KEY FEATURES

Flexible configuration interface
- Comprehensive object library
- Custom service and policy definition

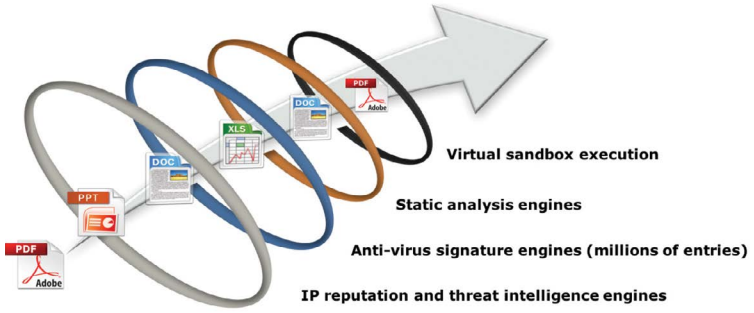
Threat visualization
- Statistics based on the attack chain
- Multiple views for threat information: locations, users, and assets

Flexible configuration interface
- Top 5 high-level threats
- Latest threat events
- 24-hour threat trends
- Daily, weekly, monthly, or annual reporting options

THREAT ANALYSIS (TA)

The NSFOCUS TA is an optional virtual sandboxing appliance that is capable of detecting, analyzing, and mitigating known, zero-day, and advanced persistent threats. The technology is often deployed as an additional line of defense that operates in unison with the NSFOCUS NGIPS.

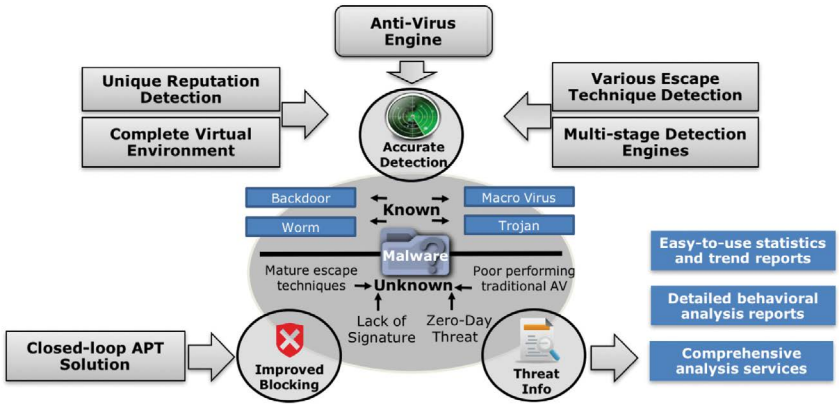
The TA utilizes a multi-stage detection engine to identify malicious activity. This approach combines signature detection, heuristic analysis, threat intelligence and virtual execution techniques to protect any network against today's cyber threats.



TA FUNDAMENTALS

The functions provided by the TA are highlighted in the diagram below. The various engines, detection techniques, malware databases, and reputation detection capabilities work in unison to address known and unknown threats. Easy -to-use statistics and trend reports, behavioral analysis reports, and comprehensive analysis services are also available.

Accurate detection of unknown malware helps reduce the risk of Advanced Persistent Threats.



TA PROTOCOL, APPLICATION, CODE, AND OS SUPPORT

The TA has broad protocol support, supports multiple file types, performs extensive static code analysis, and virtual OS support. t today's cyber threats.

Protocols | File Types | Static Code Analysis | OS

MULTIPLE TA FORM FACTORS

The TA has broad protocol support, supports multiple file types, performs extensive static code analysis, and virtual OS support.

D Series – malware detection for web or email

Hardware appliance form factor

2RU, 4 network card slots

Model	D Series (Online Detection)
1000M	Processing speed 1,000 Mbps
2000M	Processing speed 2,000 Mbps

MULTIPLE FORM FACTORS

The NSFOCUS NGIPS solution is cost and performance optimized to meet the needs of any size organization. Suitable for small to medium environments, NGIPS virtual appliances are deployed on virtual machines and with the appropriate hardware support can scale up to 2 Gbps. Demanding Enterprise and Service Provider Data Centers can choose from a range of scalable hardware appliances that can provide up to 40 Gbps of throughput.

HARDWARE SPECIFICATIONS

GIGABIT ETHERNET (GE) AND 10 GIGABIT ETHERNET (10GE)

		N2000-2	N4000	N6000	N8000	T9010	T9020
Interfaces	Onboard Interface	6GE+2SFP	N/A	N/A	N/A	N/A	N/A
	Slot	X	4	4	4	4	4
	Extension Interface	X	4*GE / 4*SFP / 8*GE / 8*SFP / 2*SFP+	4*GE / 4*SFP / 8*GE / 8*SFP / 2*SFP+	4*GE / 4*SFP / 8*GE / 8*SFP / 2*SFP+	4*GE / 4*SFP / 8*GE / 8*SFP / 2*SFP+ / 4*SFP+	4*GE / 4*SFP / 8*GE / 8*SFP / 2*SFP+ / 4*SFP+
	Max. Number of Business Interfaces	6*GE interface +2*10GE interface	32*GE interface or 8*10GE	32*GE interface or 8*10GE	32*GE interface or 8*10GE	32*GE interface or 8*10GE	32*GE interface or 8*10GE
	Whether Support 10GE Interface	Yes, 2*10 GE fiber interface	Yes	Yes	Yes	Yes	Yes
	Bypass (Default)	3 pairs of bypass copper ports	N/A	N/A	N/A	N/A	N/A
Management Interface	Management Interface	1 GE	2 GE	2 GE	2 GE	2 GE	2 GE
	Serial Port	1*RJ45	1*RJ45	1*RJ45	1*RJ45	1*RJ45	1*RJ45
	USB Interface	2	2	2	2	2	2
Performance	Real-world Throughput	2.5 Gbps	4 Gbps	6 Gbps	8 Gbps	10 Gbps	20 Gbps
	HTTP Throughput	1.5 Gbps	2 Gbps	3 Gbps	4 Gbps	5 Gbps	10 Gbps
	Max. Concurrent TCP Connections	2.5 million	4 million	5 million	6 million	8 million	10 million
	TCP Connections Per Second	100,000	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	432* 575* 88 mm (2U)	432* 575* 88 mm (2U)	432* 575* 88 mm (2U)	432* 575* 88 mm (2U)	443* 626* 88 mm (2U)	443* 626* 88 mm (2U)
	Power Supply	100-240V AC, (50-60HZ), 5-8A, 350W	100-240V AC, (50-60HZ), 5-8A, 350W	100-240V AC, (50-60HZ), 5-8A, 350W	100-240V AC, (50-60HZ), 5-8A, 350W	100-240V AC, (47-63HZ), 3-7A, 450W	100-240V AC, (47-63HZ), 3-7A, 450W
	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
	Certifications	Class A, EN55022, FCC Part 15	Class A, EN55022, FCC Part 15	Class A, EN55022, FCC Part 15	Class A, EN55022, FCC Part 15	Class A, EN55022, FCC Part 15	Class A, EN55022, FCC Part 15