NSFOCUS

DDoS Protection Solution for Larger Environments

Scaling Mitigation Capacity

It has never been easier and less expensive to launch massive DDoS attacks that result in loss of revenue, loss of customers, disruption of service availability, damage to brand, theft of vital data, and more. DDoS attacks that used to be measured in hundreds of Mbps are now observed in hundreds of Gbps, due to the proliferation of easy-to-rent botnets, and the continued development of sophisticated attack amplification techniques. As a result, it is more important than ever to deploy a DDoS mitigation solution that is optimized for today's DDoS attacks, but is capable of scaling to meet future performance demands. The NSFOCUS DDoS Protection Solution uses a scalable architecture that is performance-optimized to meet the current and future needs of large enterprise, hosting, cloud, and service provider environments.

The NSFOCUS DDoS Protection Solution consists of three components:

Network Traffic Analyzer (NTA)

A threat detection appliance that identifies malicious traffic.

Anti-DDoS System (ADS)

A mitigation appliance that removes unwanted, malicious traffic.

Anti-DDoS System Manager (ADS-M)

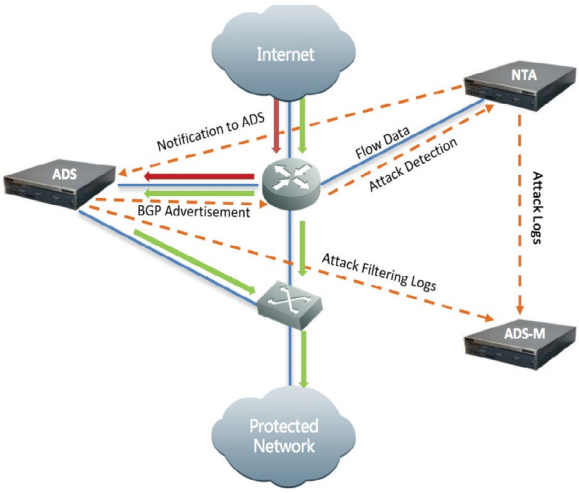
A multi-tenant management system designed for service providers, hosting providers, cloud, and large enterprise data centers. It provides centralized management of the ADS and NTA appliances as well as support for multiple, separate configuration and reporting domains for each customer. Together, these systems provide virtually unlimited DDoS mitigation capacity to withstand the most persistent threats, while under the most extreme network conditions.

Solution Architecture and Operation

The complete solution has been designed for network environments that require more than 10 Gbps of DDoS mitigation capacity.

It uses a distributed architecture that separates DDoS mitigation, threat detection, and centralized management, and scales in each of these areas.

It can also be clustered and deployed in an out-of-path mode to provide hundreds of Gbps and beyond of mitigation capacity.



Out-of-path Traffic Diversion

BENEFITS

Alleviate concerns over loss of revenue, loss of customers, damage to brand, service availability and theft of vital data

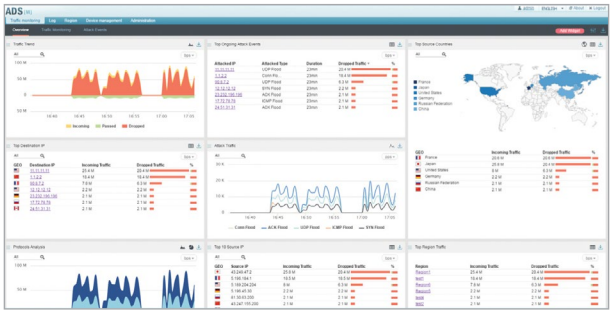
Scalable, advanced DDoS protection to withstand the most extreme attacks

KEY FEATURES

- **Industry-leading Accuracy**
  Filters malicious traffic to ensure only legitimate traffic reaches your infrastructure
- **Scalable Architecture**
  Out-of-path and clustering deployment options to meet the needs of the most demanding networks
- **Multi-tenant, Centralized Management**
  Domain-specific configuration, policy, logging and reporting to simplify managed DDoS services
- **Multi-Layered Security**
  Network, application and web application security designed to respond to modern-day DDoS attacks

At the heart of the solution, the NTA monitors network activity by receiving and analyzing xFlow statistics from border and core routers. It uses an innovative, multi-stage DDoS detection engine made up of several algorithms and other mechanisms to accurately identify malicious traffic. These include RFC Checks, Protocol Analysis, Access Control Lists, IP Reputation, Anti-spoofing, L4-L7 Algorithmic Analysis, User Behavior Analysis, Regular Expressions, and Connection/Rate Limiting. Together they provide industry-leading accuracy that protects against both known and zero-day threats. The detection engine is optimized frequently, so you always have the most accurate protection available.

The ADS system, under the direction of the NTA, works with border routers to divert traffic, filter malicious flows and then forward legitimate traffic back into your network. Multiple ADS systems can be clustered to increase the overall mitigation capacity of the solution.



ADS-M
The ADS-M real-time views are highly optimized for traffic monitoring, reporting, ease of use, and improved user experience.

The ADS-M is used for central configuration, management, and reporting. It can be configured in a multi-tenant mode of operation to provide separate administrative domains on a per-customer basis and includes a flexible, web services API to automate provisioning and reporting for your specific environment. Network operators can use the ADSM to direct and collect packet captures from co-resident ADS systems to shorten problem resolution and incident response times. Extensive reporting options include information on attack types, attack targets, protocols, alerts, network status, alert information, device logs, and more. The ADS-M also supports an optional DDoS detection software module to provide an integrated management and threat detection solution that supports environments up to 60,000 flows per second.

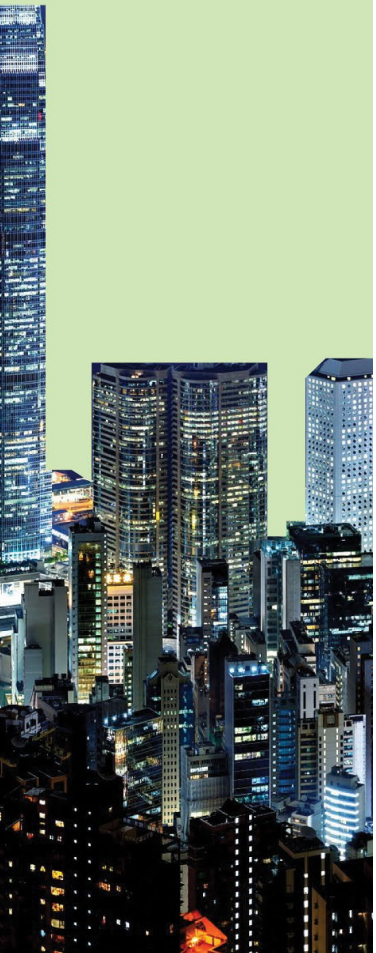
Industry-leading accuracy and rapid threat detection
The DDoS Protection Solution incorporates the latest intelligence from our internationally-recognized research labs and is developed with over 10 years of experience protecting the world's largest banks, telecommunications, gaming and social media companies. The NSFOCUS Research Institute (NSRI) is a cybersecurity research and threat response center at the forefront of vulnerability assessment, threat detection and mitigation research. Their work, combined with world-class engineering, has resulted in a solution with industry leading accuracy capable of detecting advanced, multi-layer DDoS attacks in as little as 20 seconds. This enables the solution to react quickly to new information from multiple sources during rapidly changing network conditions.

Scalability
The ADS series includes models that range from 1Gbps to 320Gbps of DDoS mitigation capacity. When deployed with an NTA or ADS-M appliance, these systems can be clustered to withstand the most extreme volumetric and application-layer DDoS attacks.

Multi-tenant, centralized management
The ADS-M provides a multi-tenant configuration interface that simplifies the administration and monitoring of managed DDoS services. It enables service providers to create and configure customer specific security policies and reports, including daily/weekly/monthly/yearly intervals with pie charts, bar graphs, line graphs, and more. It also provides real-time traffic monitoring, log information, and detailed attack history for post-incident forensic analysis.

Easy to deploy and integrate
The ADS is typically deployed at the ingress point to your network while the NTA and ADS-M appliances can be installed at any location in your network. The ADS uses industry standard routing protocols to communicate with other routers in order to redirect suspicious traffic and forward legitimate flows back into the network. A flexible web services API in the ADS-M further simplifies integration of the system into your network by providing a programmatic interface that can be used to automate labor intensive tasks.

The NSFOCUS DDoS Protection Solution is the ideal solution for today's advanced and evolving threats. It is highly scalable and is performance optimized to meet the current and future needs of large enterprise and service provider environments. It is also easy to deploy, flexible and provides a multi-tenant configuration interface to simplify the configuration and administration of large-scale, managed DDoS services.



NSFOCUS Hybrid DDoS Protection Solution

Many organizations utilize a hybrid approach to defeat the damaging effects of DDoS attacks. The approach combines NSFOCUS on-premises defenses with on-demand NSFOCUS Cloud DDoS Protection. Working in unison, the solution eliminates smaller/shorter attacks on-premises, while defending infrastructures against bandwidth saturating DDoS attacks using the cloud. Both defenses are fully integrated resulting in increased bandwidth visibility, reduced cloud redirect times for mitigation, and coverage for all L3-L7 DDoS attack vectors.

Software Specifications

NTA

• Flow Monitoring
- sFlow-v4/v5, Netflow-v5/v9, NetStream-v5, Flexible Netflow, IPFIX

• DDoS Attack Detection
- SYN/ACK/UDP/ICMP/IGMP/HTTP/HTTPS/DNS/Land/SIP floods, TCP flag misuse, flag null, Private IP, abnormal traffic, alert threshold self-learning, IP group inbound/outbound attack traffic, business domain and region inbound/outbound attack traffic

• ADS Traffic Diversion
- Diversion notice to routers based on traffic volume

• Management Interfaces and Reporting
- SNMP GET/Trap, syslog, Email, Flow data forwarding

• Virtual NTA
- Virtual NTA on VMware platform available

ADS Series

• DDoS Protection
- Comprehensive, multi-layered protection against volumetric, application, and web application attacks
- Multi-protocol support and advanced inspection including TCP, UDP, HTTP, ICMP, NTP, DNS, SIP, fragments, flooding, connection exhaustion, header manipulation, and more
- Fully Integrated with NSFOCUS Cloud Security Platform

• DDoS Detection and Mitigation Algorithms
- RFC Checks, Protocol Analysis, Access Control Lists, IP Reputation, Anti-spoofing, L4-L7 Algorithmic Analysis, User Behavior Analysis, Regular Expressions, Fragmentation Controls, Connection and Rate Limiting
- Protect against both known and zero-day threats

• Management
- Protocols: HTTP, SNMP, Email, Syslog
- Authentication: Local database, Radius, TACACS+
- API: web services for reporting and automated configuration

• IP Protocols
- Addressing: IPv4/v6
- Routing: BGP, OSPF, RIP, IS-IS, static routing, and PBR
- Data link and network layer: MPLS, GRE, VLAN (802.1q)

• Reporting
- Real-time and historical reporting of attack types, source/destination IP, and more
- Formatting: XML, PDF, HTML, and Microsoft Word
- Web services API for forensics and compliance initiatives

ADS-M

• Centralized Management and Configuration
- Devices: add, delete and configure
- Multi-tenant
- Security policies
- High availability
- ADS clustering

• Reporting
- Attack events, attack summaries, traffic trends
- Extensive logging: attack summary, traffic alerts, performance, link state, authentication activity

• Role-based Management Authentication
- Administrator, supervisor and user

NSFOCUS

2520 Mission College
Blvd, Suite 130
Santa Clara CA 95054
www.nsfocusglobal.com

Hardware Specifications

ADS-M

Hardware	ADS-M 1600
Interfaces	1xRJ45 serial 2x100/1000M (copper) 4x1000M SFP slots
Dimensions (WxDxH)	17.4"x20.2"x3.5" 2 RU
Weight	41.89 lbs (19 kg)
Environmental	Operating: 32-113° F (0-45° C) Storage: -4-149° F (-20-65° C)
Power	AC Dual Power Supply (350W total)
Flow Collection Capacity (optional NTA license)	60,000 flows/sec
Maximum managed devices	40 ADS, 20 NTA
Maximum concurrent users	50
Maximum number of regions	1024
Maximum number of policies	4000
Maximum IP addresses/region	65,535
MTBF	60,000 hours

NTA

Hardware	NTA 2000
Interfaces	2xRJ45 serial 2xUSB 2.0 4xGE (copper), 4xGE (SFP)
Dimensions (WxDxH)	17"x20.2"x3.5" 2 RU
Weight	36.6 lbs (16.6 kg)
Environmental	Operating: 32-113° F (0-45° C) Storage: -4-149° F (-20-65° C)
Power	AC Dual Power Supply (350W total)
Flow Collection Capacity	120,000 flows/sec
Maximum number of monitored routers	20
Maximum number of monitored router interfaces	1,000
MTBF	60,000 hours

Virtual NTA

Item	Recommended Configuration
CPU	Intel® Core™ i7-2600 CPU @ 3.40 GHz Four cores and eight threads
Memory	16 GB
Hard disk	1 TB + 2 GB
NIC	2

CPU + MEM	Flows/sec
1*2CPU+16G	30,000
1*4CPU+16G	120,000
1*8CPU+16G	200,000
1*16CPU+16G	240,000

ADS Series

Hardware	ADS 8000	ADS 6025	ADS 4020	ADS 2020
Mitigation Capacity	40 Gbps* 29,760,000 pps	20 Gbps* 14,880,000 pps	10 Gbps 8,928,000 pps	4 Gbps 2,976,000 pps
Interfaces	8x10GE (SFP+)	4x10GE (SFP+) or 4x10GE (SX fiber)	16xGE (copper) or 16xGE (SX fiber) or 12xGE (SFP) or 4x10GE (SFP+) or 4x10GE (SX fiber) or 2x10GE(SX fiber) and 8xGE(SX fiber) or 2x10GE (SFP+) and 8xGE(SFP)	4xGE (copper) or 4xGE (SX fiber) and 4xGE (copper)
Dimensions (WxDxH)	24.7"x17.4"x3.5" 2 RU	22.6"x17"x3.5" 2 RU		
Weight	36.49 lbs (16.55 kg)	24.25 lbs (11 kg)		
Environmental	Operating: 41-104° F (5-40° C) Storage: 14-158° F (10-70° C)	Operating: 32-104° F, (0-40° C) Storage: -4-176° F, (-20-80° C)		
Power	AC Dual Power Supply (500W total)	AC Dual Power Supply (350W total)		
MTBF	45,000 hours			

DOCUMENT NUMBER 10032016