DATASHEET

ADS

Anti-DDoS System

Service Providers all agree that DDoS attacks are more frequent, complex, and destructive than ever. Providers all report an increase in DDoS attacks against their customers, and have experience attacks that impacted their infrastructures as well. Providers of all sizes agree that DDoS defenses deployed in their networks are no longer an option — they're becoming a requirement to maintain consistent levels of service.

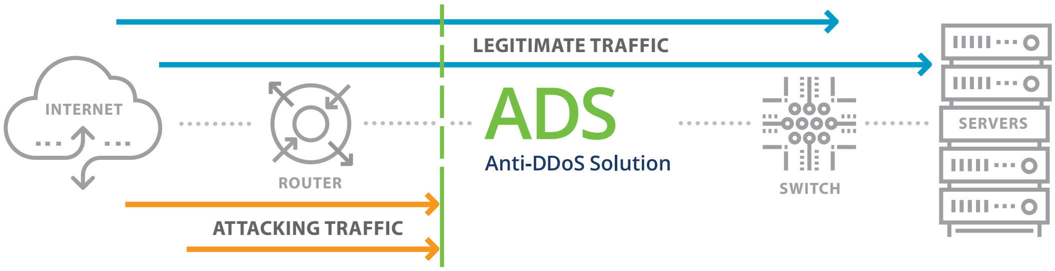
At the heart of the NSFOCUS On-Premises DDoS Defenses is the ADS. It provides comprehensive, multi-layered protection from today's advanced DDoS attacks. When deployed out-of-path, traffic streams for the IP addresses under attack are "diverted" to the ADS. It surgically mitigates DDoS attack traffic, while allowing all legitimate traffic to continue to pass downstream. When deployed in-line, the ADS detects attacks, and mitigates DDoS traffic. Both deployment modes provide extremely low latency and reliable detection and mitigation of attacks; while ensuring service provider's customers and services are protected from the impact of DDoS.

MONITOR

The ADS is easily deployed in any providers network and can scale to support hundreds of Gbps of inspected traffic. When deployed in-line, it monitors the incoming traffic for signs of DDoS. When deployed out-of-path, the NSFOCUS Network Traffic Analyzer (NTA) performs the monitoring and detection function by consuming xFlow data from border, core, or edge routers. Either method provides reliable monitoring and detection of DDoS.

DETECT

At the core of the ADS are innovative, multi-stage detection engines. All packets are subjected to a series of analyses, checks, and validations to accurately identify both legitimate and attack 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 all DDoS attacks. The detection engine is optimized frequently, so providers always have the most accurate protection available.



MITIGATE

Regardless of the deployment scenario, once attack traffic has been identified by the ADS, it immediately removes this traffic from the traffic streams it's inspecting. The ADS then forwards only legitimate traffic to its intended destination. The ADS supports DDoS attack reporting in real-time to provide valuable information such as attack types, source/destination IPs, protocols, and more. An integrated web services API can also be used to assist with automated configuration, post-incident reporting, and billing operations.

PERFORMANCE. QUALITY. VALUE.

The ADS is the ideal solution for service providers to mitigate DDoS attacks against their customers, and their services. Providers who deploy ADS no longer need to rely on null routes to defeat attacks. Available in a range of cost and performance optimized appliances, they ADS has been purpose-built to deliver high quality, scalable mitigation of DDoS attack traffic.

BENEFITS

Defeat DDoS attacks against your customers when deployed in your network

Reduces operating expenses for DDoS mitigation by providing increased levels of automation

KEY FEATURES

Multi-Tenant Design
Domain specific configurations, learning algorithms, automated mitigation responses, modular architectures, flexible licensing models, and the lowest total cost of ownership **(TCO)**

Reliable, Accurate
Algorithmic, multi-filter, rule-based approach provides automated and reliable DDoS mitigation with low false positives and high performance

Best-in-Class Performance
Provides advanced DDoS mitigation for any size service provider that is easy to integrate with your network

Scalable Architecture
Supports scalable clusters for both In-line and out-of-path deployment scenarios to meet the needs of any size network

SOFTWARE SPECIFICATIONS

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
- Integrated with NSFOCUS Cloud DDoS Defenses

DDoS Protection 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 unknown DDoS Attacks

Management

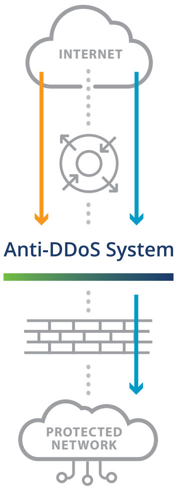
- Protocols: HTTP, SNMP, Email, Syslog
- Authentication: Local database, Radius, TACACS+
- API: web services for reporting and automated configuration
- IP Protocols
- Addressing: IPv4/v6
- Routing: BGP, OSPF, RIP, IS-IS, static routing and PBR
- Data link and network layer: MPLS, GRE, VLAN (802.1q)

Reporting

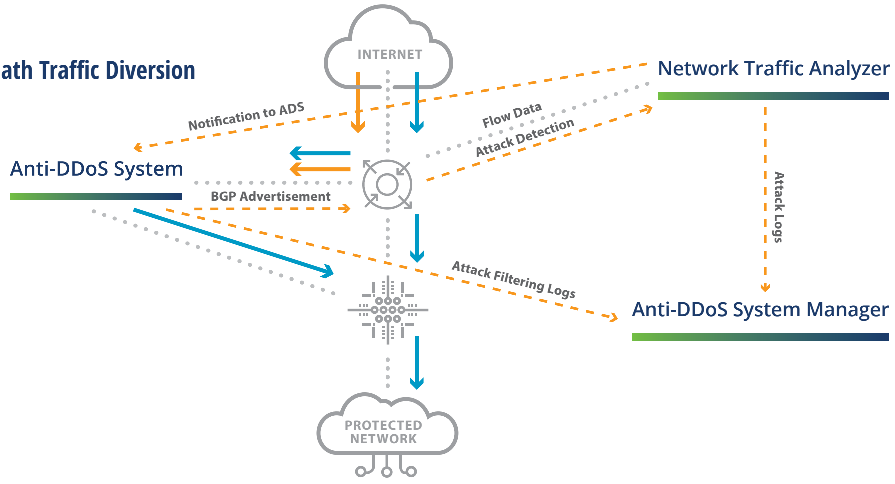
- Real-time and historical reporting of attack types, source/destination IP
- Formatting: XML, PDF, HTML, and Microsoft Word
- Web services API to support automated configuration and reporting functions

DEPLOYMENT OPTIONS

Inline Mode



Out-of-path Traffic Diversion



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	Up to: 8*10GE SFP+ Or 4*10GE SFP+ and 16*GE port (copper, SFP-GE-SX, and SFP-GE-LX available)	Up to: 8*10GE SFP+ Or 32*GE port (copper, SFP-GE-SX, SFP-GE-LX and bypass module available)	Up to: 8*10GE SFP+ Or 32*GE port (copper, SFP-GE-SX , SFP-GE-LX and bypass module available)	Up to: 4*GE +4*SFP Or 8*SFP (copper, SFP-GE-SX, SFP-GE-LX and bypass module available)
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 (450W total)		AC Dual Power Supply (350W total)	
MTBF	45,000 hours		60,000 hours	