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.

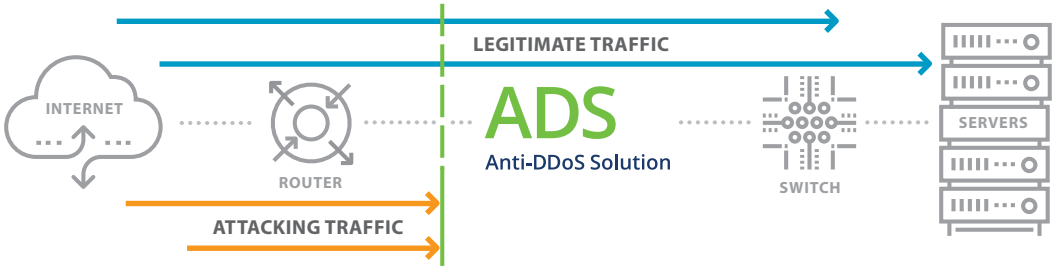
At the heart of the NSFOCUS On-Premises DDoS Defenses is the ADS. It provides comprehensive, multi-layered protection from today's advanced DDoS attacks. When deployed out-of-path, traffic streams for the IP addresses under attack are "diverted" to the ADS. It surgically mitigates DDoS attack traffic, 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 provider's 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, Fragmentation Controls, Connection and 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. Also, the ADS can integrate with NSFOCUS Threat Intelligence (NTI) to remove the traffic from known botnets immediately, and query the newest threat intelligence regarding the attackers. 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, the ADS has been purpose-built to deliver high quality, scalable mitigation of DDoS attack traffic.

NSFOCUS

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, efficient and intelligent protection from the botnet-based attacks with NTI

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

Optional Product Form
Capable to provide both hardware appliance and virtual product.

SOFTWARE SPECIFICATIONS

DDoS Protection	• Comprehensive, multi-layered protection against volumetric, application, and web application attacks • Multi-protocol support and advanced inspection including TCP/UDP/ICMP/HTTP/HTTPS/DNS/SIP floods, Amplification attacks (NTP/SSDP/SNMP/DNS/CHARGEN/Memcached/NetBIOS), fragments floods, connection exhaustion, header manipulation and more • Integrated with NSFOCUS Cloud Security Platform • Integrated with NSFOCUS Threat Intelligence	
DDoS Mitigation Algorithms	• RFC Checks • Black Filter Lists • NTI Black Filter Lists • White Filter Lists • GEOIP Filter Lists • Access Control Lists Filtering • TCP Regular Expression Filtering • UDP Regular Expression Filtering • SYN Check • ACK Check • Reflection Amplification Rules • Port Check • Connection Exhaustion • URL-ACK Filter Lists • Anti-spoofing • TCP SYN Source IP Rate Limit • TCP SYN Source Bandwidth Limit • TCP SYN Time Sequence Check • TCP Fragment Control • ICMP Fragment Control • ICMP Traffic Control	• DNS Keyword Checking • DNS Rate-Limiting • DNS TCP-BIT Check • DNS CNAME Check • DNS Retransmission • HTTP Keyword Checking • HTTP Authentication • HTTP Dynamic Script • HTTP FCS Check • HTTP Pattern Matching Check • HTTP Slow Attack Check • IP Behavior Analysis • Trusted Source IP Control • Empty Connection Check • HTTPS SSL Connection Control • HTTPS Authentication • SIP Authentication • UDP Payload Check • UDP Fragment Control • UDP Packet Length Check • UDP Traffic Control • TCP Watermark Check • UDP Watermark Check • TCP Pattern Matching • UDP Pattern Matching • Protocol ID Check
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 Service API to support automated configuration and reporting functions	

NSFOCUS SECURITY REPORT

DDoS and Web Application Attack Landscape Report

Annual Cybersecurity Insights Report

Botnet Trend Report

Fintech Security Analysis Report

DDOS ATTACK TREND

167,400 DDoS attacks had been detected in 2019, an increase of 30.2% compared with 2018.

Nearly 3000 super-sized attacks (> 300 Gbps) had been spotted in 2019, increasing by around 200 compared with 2018.

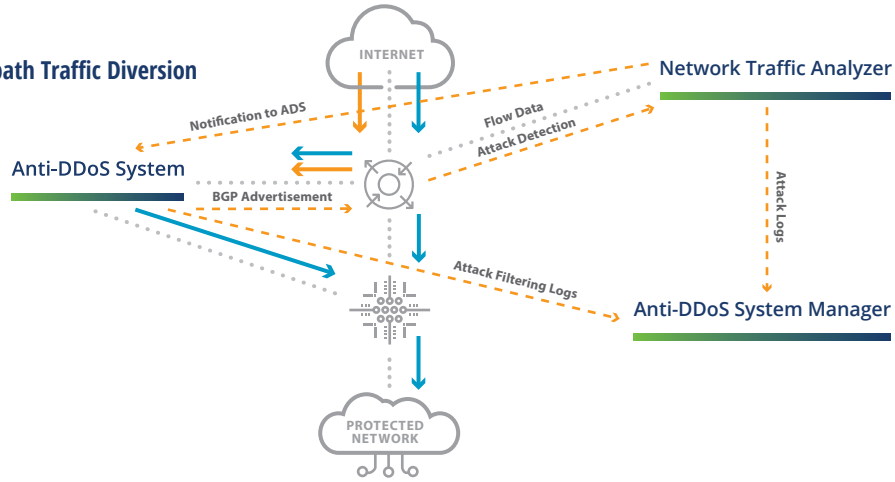
The max peak size stood at 885 Gbps in 2019, lower than the max peak size of 1.41 Tbps in 2018.

To download the latest report, go to: https://nsfocusglobal.com/company-overview/resources

DEPLOYMENT OPTIONS

Inline Mode

Out-of-path Traffic Diversion



Hardware	ADSNX5-10000	ADSNX5-8000	ADSNX5-6025E	ADSNX5-4020E	ADSNX3-2020E
Mitigation Capacity	240Gbps 149,942,000pps	40Gbps 29,760,000pps	20Gbps 14,880,000pps	12Gbps 8,928,000pps	4Gbps 2,976,000pps
Interfaces	1*IPMI, 1*RJ45 Serial, 1*USB Optional Interface Card: 2*100GE CXP and 20*10GE SFP+ Or 6*100GE QSFP28 and 4*40GE QSFP+ and 16*10GE SFP+ Or 16*10GE SFP+ and 4*GE Copper	1*IPMI, 2*GE Copper, 1*RJ45 Serial, 2*USB Up to: 8*10GE SFP+ Or 4*10GE SFP+ (bypass module available) and 16*GE port (copper, SFP-GE-SX, and SFP-GE-LX available)	2*GE Copper, 1*RJ45 Serial, 2*USB Up to: 8*10GE SFP+ Or 32*GE port (copper, SFP-GE-SX, SFP-GE-LX and bypass module available)	2*GE Copper, 1*RJ45 Serial, 2*USB Up to: 8*10GE SFP+ Or 32*GE port (copper, SFP-GE-SX, SFP-GE-LX and bypass module available)	2*GE Copper, 1*RJ45 Serial, 2*USB Up to: 4*GE and 4*SFP Or 8*SFP (copper, SFP-GE-SX, SFP-GE-LX and bypass module available)
Dimensions (WxDxH)	19"x27"x10.5" 6 RU	17.4"x24.6"x3.5" 2 RU	17.3"x22.2"x3.5" 2RU		
Weight	121.25 lbs (55 kg)	36.38 lbs (16.5 kg)	26.46 lbs (12 kg)		
Environmental	Operating: 32-113° F (0-45° C) Storage: -40-158° F (-40-70° C)	Operating: 41-104° F (5-40° C) Storage: -4-176° F (-20-80° C)	Operating: 32-113° F (0-45° C) Storage: -4-158° F (-20-70° C)		
Power	AC/DC Five Power Supply (1200W total)	AC/DC Dual Power Supply (500W total)	AC/DC Dual Power Supply (450W total)		
MTBF	52,879 hours	45,000 hours	60,000 hours		

Host		Virtual ADS	
Item	**Recommended Configuration**	**Item**	**Recommended Configuration**
CPU	Intel® Xeon® CPU E5-2687W v4 @ 3.00GHz	**vCPU (processor cores)**	An even number ranging from 4 to 32
Memory	128G (at least 32GB free space)	**Memory**	32GB at least
Hard Disk	1TB (at least 10GB free space)	**Storage**	10GB at least
Operation System	CentOS	**Hypervisor Support**	QEMU KVM version 1.5.3 or later
1000M NIC Support	I210, I350, 82571, 82576, 82580 (up to 8)	**Mitigation Capacity**	Up to 20G
10Gb NIC Support	82599, X710/XL710 (up to 4)	**License Options**	200M, 400M, 2G, 12G, 20G
Virtual NIC Support	NIC other than those above (cannot guarantee the capacity)		