DATASHEET

NSFOCUS

Anti-DDoS System (ADS)

COMPLETE DDoS MITIGATION APPLIANCE

OVERVIEW

Distributed denial-of-service (DDoS) attacks are increasing in complexity, volume, and frequency. There is no doubt that DDoS attacks threatening to overwhelm the bandwidth and application resources of enterprises globally in today's info-security threat landscape.

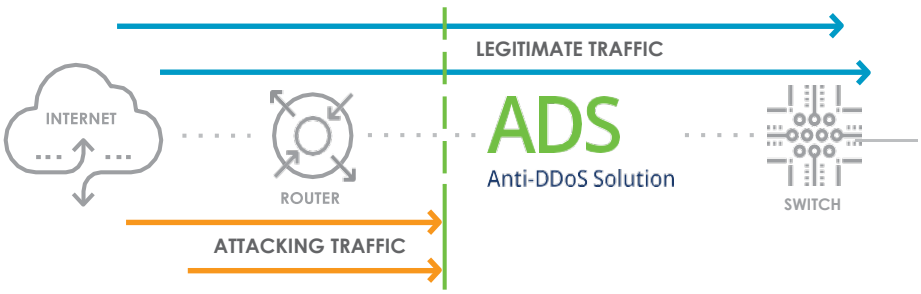
The NSFOCUS Anti-DDoS System (ADS) is the ideal solution for today's advanced and evolving DDoS attacks, which can provide comprehensive, multi-layered DDoS attacks protection. It surgically mitigates DDoS attack traffic, while allowing legitimate traffic to pass downstream. Both inline and out-of-path deployment modes provide extremely low latency and reliable detection and mitigation of attacks while ensuring customers and services are protected from the impact of DDoS.

MONITOR

The NSFOCUS WAF technology is powered by an internationally-recognized research lab and developed with over 10 years of experience protecting the world's largest banks, telecommunications, gaming, and social media companies. The WAF uses Intelligent Detection™ advanced machine learning technology that is far superior for identifying web attacks and minimizing false positives/negatives than traditional positive and negative security models to deliver next-gen real-time web security.

DETECT

The ADS provides a multi-stage detection engine with an innovative approach to ensure the full-spectrum DDoS defense. 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 DDoS protection.



KEY 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 engine

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

MITIGATE

Regardless of the deployment scenario, the ADS can remove DDoS attacks immediately before they reach the enterprise network and affect internet services with the industry-leading DDoS attack mitigation. By utilizing the NSFOCUS Threat Intelligence (NTI), the ADS also can remove the traffic from known botnets immediately and uploads the attack data to NTI for contributing to intelligence. The ADS also provides advanced visibility and reporting of attack mitigation which including attack types, source/ destination IPs, protocols, and more detailed information. An integrated web services API of the ADS can provide additional flexibility to assist with automated configuration, post-incident reporting, and billing operations for customer's unique business needs.

SOFTWARE SPECIFICATIONS

DDoS Protection

- Comprehensive, multi-layered protection against the 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
- API: web services for reporting and automated configuration

IP Protocols

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

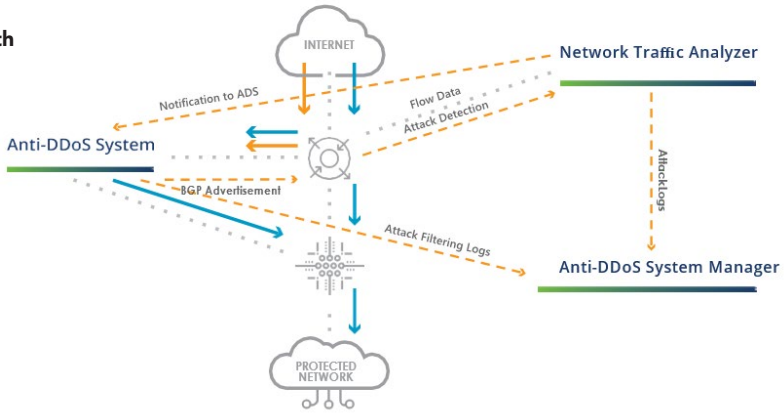
Virtualization

- Virtual ADS KVM platform available

DEPLOYMENT OPTIONS

Inline Mode Diversion

Out-of-path Traffic



PERFORMANCE – ADS-SERIES

Model	ADSNX5-HD12000/10000	ADSNX5-HD8500	ADSNX5-8000
Mitigation Capacity	240Gbps/400Gbps 149,942,000pps/297,600,000pps	80Gbps 59,520,000pps	40Gbps 29,760,000pps
Interfaces	1*RJ45 Serial, 1*GE Copper, 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	2*GE MGMT, 1*RJ45 Serial, 2*USB, 4*Extension Slot	2*GE Copper, 1*RJ45 Serial, 2*USB
Dimensions (W*D*H)	19”x27”x10.5” 6 RU	17.4”x24.6”x3.5” 2 RU	17.4”x24.6”x3.5” 2 RU
Weight	121.25 lbs (55 kg)	46.29 lbs (21 kg)	36.38 lbs (16.5 kg)
Environmental	Operating: 32-113° F (0-45° C) Storage: -40-158° F (-40-70° C)	Operating: 32-104° F (0-40° C) Storage: -4-176° F (-20-80° C)	Operating: 41-104° F (5-40° C) Storage: 14-176° F (-10-80° C)
Power	AC/DC Five Power Supply (6000W total)	AC/DC Dual Power Supply (300W total)	AC/DC Dual Power Supply (500W total)
MTBF	52,879 hours	60,000 hours	45,000 hours

Model	ADSNX5-HD6500	ADSNX5-HD4500	ADSNX5-2500
Mitigation Capacity	40Gbps 29,760,000pps	20Gbps 14,880,000pps	4Gbps 2,976,000pps
Interfaces	2*GE MGMT, 1*RJ45 Serial, 2*USB, 4*Extension Slot	2*GE Copper Intel I210 (1*MGMT, 1*Hot Standby) 1*RJ45 Serial, 2*USB	2*GE Copper Intel I210 (1*MGMT, 1*Hot Standby) 1*RJ45 Serial, 2*USB
Dimensions (W*D*H)	17.4”x20.7”x3.5” 2RU	17.13”x22”x1.7” 1RU	17.13”x22”x1.7” 1RU
Weight	44 lbs (20 kg)	21.2 lbs (9.6 kg)	21.2 lbs (9.6 kg)

Environmental	Operating: 32-104° F (0-40° C) Storage: -4-176° F (-20-80° C)	Operating: 32-104° F (0-40° C) Storage: 14-158° F (-10-70° C)	Operating: 32-104° F (0-40° C) Storage: 14-158° F (-10-70° C)
Power	AC Dual Power Supply (300W total)	AC Dual Power Supply (300W total)	AC Dual Power Supply (300W total)
MTBF	60,000 hours	86,046 hours	86,046 hours

PERFORMANCE – VIRTUAL ADS

<table>
<tr><th colspan="2">Host</th><th colspan="6">Virtual ADS</th></tr>
<tr><th>Item</th><th>Recommended Configuration</th><th>Item</th><th colspan="5">Recommended Configuration</th></tr>
<tr><td>CPU</td><td>Intel(R) Xeon(R) CPU E5-2687W v4 @ 3.00GHz</td><td>Hypervisor support</td><td colspan="5">QEMU KVM 1.5.3</td></tr>
<tr><td>Memory</td><td>128G (at least 32GB free space)</td><td>Mitigation capacity</td><td>(@128bytes)</td><td>200M-2Gbps</td><td>10Gbps</td><td>20Gbps</td><td>40Gbps</td></tr>
<tr><td>Hard disk</td><td>1TB (at least 10GB free space)</td><td rowspan="3">Minimum Requirement</td><td>CPU Cores</td><td>4</td><td>6</td><td>14</td><td>32</td></tr>
<tr><td>Operation system</td><td>CentOS</td><td>Memory</td><td>16G</td><td>16G</td><td>16G</td><td>32G</td></tr>
<tr><td>1000M NIC support</td><td>I210, I350, 82571, 82576, 82580 (up to 8)</td><td>Storage</td><td colspan="4">10GB at least</td></tr>
<tr><td>10Gb NIC support</td><td>82599, X710/XL710 (up to 4)</td><td>license options</td><td colspan="5">200M, 500M, 1G, 2G, 10G, 20G, 40G</td></tr>
<tr><td>Virtual NIC support</td><td>NIC other than those above (cannot guarantee the capacity)</td><td></td><td colspan="5"></td></tr>
</table>