DATASHEET

NSFOCUS

# On-Premises DDoS Defenses

## COMPREHENSIVE, MULTI-LAYERED DDOS PROTECTION

## OVERVIEW

The flourishing development of Internet has brought convenience to people's lives, but at the same time it has also become a hotbed for nourishing DDoS attacks. The direct economic losses caused by DDoS attacks continue to rise every year, seriously impacting enterprise revenue and reputation.

Rapidly growing compromised IoT devices promote DDoS attacks to show characteristics of high frequency, sophistication and variation. Meanwhile, DDoS attacks have been industrialized and weaponized. Attackers can easily subscribe to SaaS services to initiate DDoS attacks at a very low cost.

To effectively defend against modern DDoS threats and ensure continuous service availability, a comprehensive, multi-layered DDoS protection architecture is essential.

## NSFOCUS' ON-PREMISES DEFENSES COMPONENTS

### NETWORK TRAFFIC ANALYZER (NTA) - DETECTS DDOS ATTACKS

NTA is a DDoS detection appliance that identifies attacks via Deep Flow Inspection (DFI) and Deep Packet Inspection (DPI)

### ANTI-DDOS SYSTEM (ADS) - MITIGATES DDOS ATTACKS

ADS is a stateless DDoS mitigation appliance that scrubs and eliminates malicious traffic

### ANTI-DDOS BUSSINESS OPERATION SYSTEM (ADBOS-L) - MANAGES COMPLETE SOLUTION

ADBOS-L is a multi-tenant management system providing centralized management and reporting for the entire Anti-DDoS solution. A web-based customer portal is also included.

## CONCORDANT AND CLOSED LOOP DEFENSES

The NTA monitors network activity by receiving and analyzing xFlow data or packets data from border, core and/or edge routers, providing scalable, flow-based detection for **high-volume DDoS attacks**. For more complex and DDoS attack scenarios, NTA also supports packet-level traffic inspection to enable more precise and accurate detection. It uses an innovative, multi-stage DDoS detection engine with more than 30 vectors to accurately identify DDoS traffic from other traffic streams. Users can customize NTA alert plugins with specific signatures, to extend NTA detection capability. Also, the NTA can rely on machine learning to generate dynamic threshold baseline automatically. Multiple response actions are available, including BGP diversion, DDoS traffic diversion, BGP Flowspec, and Remotely Triggered Black Hole (RTBH).

When an ADS is added to the deployment, the ADS then comes under the direction of the NTA. Upon detecting an attack, NTA automatically communicates the targeted IP address(es) to ADS. The ADS next announces the border routers to divert traffic via BGP to the ADS where malicious traffic is discarded. It then re-injects legitimate traffic back into your network with extremely low latency and high accuracy. The entire process is highly efficient and typically completed within 1-3 seconds.

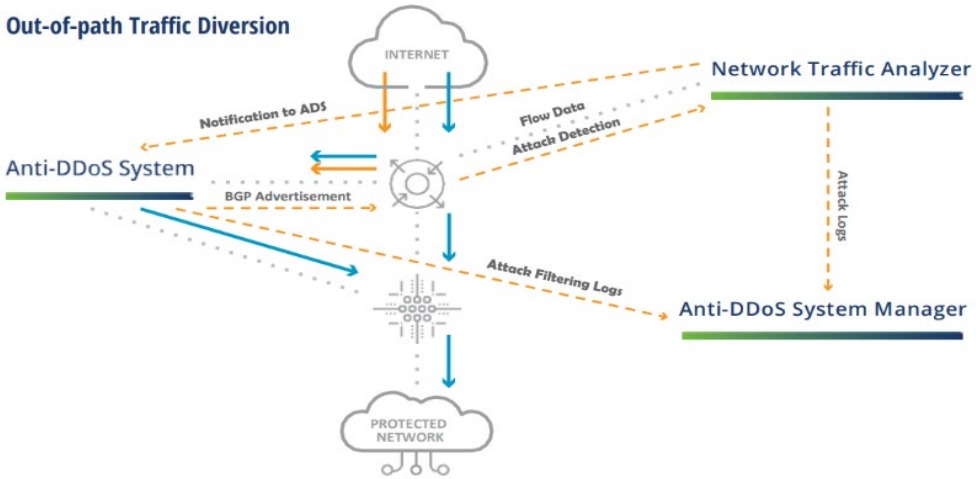
## KEY BENEFITS

- Quick and easy deployment
- Flexible, on-demand licensing model
- Designed for statelessness
- Automatic hand-off with NSFOCUS Cloud Centers
- Low latency from diversion to cloud mitigation
- Increased visibility and traffic threshold monitoring
- Versatile deployment options
- Complete service provider ready solution
- Lowest total cost of ownership (TCO)

## KEY FEATURES

- Automated or manual BGP redirection
- GRE, VLAN, MPLS, PBR traffic re-injection
- All-in-one solution, multi-tenancy enabled
- SOAR-based automatic response
- Low false positives, high performance
- Easy to integrate and cohabitate
- Automated and reliable DDoS mitigation
- Efficient and intelligent protection from the botnet-based attacks with NTI

ADBOS-L provides optimized real-time dashboards for traffic visibility, monitoring, and reporting, with a strong focus on usability and operational efficiency. It provides centralized management of the ADS and NTA appliances as well as support for multiple, separate configuration and reporting domains for each customer.




## INDUSTRY-LEADING ACCURACY AND PRECISE MITIGATION

With more than 20 years of internationally recognized forefront protection research and combat experience, NSFOCUS On-Premises DDoS Defenses provide protection against volumetric, application and web application attacks in seconds, including DNS, carpet-bombing attacks, HTTP/S floods, UDP/TCP amplification attacks, low and slow attacks, etc. Unlike products from other vendors, NSFOCUS On-Premises DDoS Defenses don't require additional WAF modules to mitigate web-application attacks, simplifying the overall security architecture while reducing deployment cost and operational complexity. Plus, ADS supports fine-grained protection, such as URL-based protection and differentiated PC and APP traffic protection, ensuring customer service availability macro to micro. Built on stateless mitigation architecture, ADS requires no limitation on the number of concurrent DDoS attack traffic sessions, enabling it to effectively handle large-scale and highly concurrent attack scenarios. Also, both ADS and NTA can integrate with NSFOCUS Threat Intelligence (NTI) to defend botnet-based attacks.

## SCALABILITY PERFORMANCE AND EASY TO DEPLOY

The ADS is typically deployed at the ingress of your network, while the NTA and ADBOS-L appliances can be flexibly deployed at any location in your network. The ADS series offer models that range from 200Mbps to 1Tbps of DDoS mitigation capacity that support flexible licensing, allowing customers to scale mitigation capacity according to their specific needs. ADS can also be deployed as a cluster to protect the largest and most demanding network environment against the most extreme volumetric and application-layer DDoS attacks. Virtualization of ADS, NTA and ADBOS-L is available, which is easy to implement and save CAPAX. In addition, the solution provides open and well-documented APIs, allowing seamless integration with existing network and security systems and enabling automation of operational and management tasks.

## MULTI-TENANT, CENTRALIZED MANAGEMENT WITH HIGH VISIBILITY

The centralized management system ADBOS-L supports not only central configuration of ADS and NTA but also provides comprehensive reports and monitoring dashboards. Based on the multi-tenant design concept, ADBOS-L enables administrators to monitor traffic and attack conditions from perspective of each tenant as well as global with multi-dimensional graphical visualizations for enhanced situational awareness.

Extensive reporting options include information on attack types, attack targets, protocols, ports, network status, alert information, device logs, and more. The ADBOS-L also supports a customizable "customer portal" designed for providers who desire to offer Managed DDoS Services. This portal allows providers to offer web-based access to their customers for traffic analysis, reporting, and analytics.

## NSFOCUS HYBRID DDOS DEFENSES

Nearly all industry experts recognize the fact that defeating the broad spectrum of DDoS attacks requires more than just cloud DDoS defenses, and more than just on-premises defenses. It requires both. From massive volumetric DDoS attacks to sophisticated low-and-slow DDoS attacks, the best approach to defeat all DDoS attacks requires a combination of on-

premises defenses and cloud defenses – called Hybrid DDoS Defenses. NSFOCUS Hybrid DDoS Defenses support fully automated traffic diversion, enabling seamless coordination between on-premises and cloud POPs without any manual intervention.

## SOFTWARE SPECIFICATIONS – ADS

### DDoS Protection

- Comprehensive, stateless, 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/CHARGEN/ Memcached), fragments floods, connection exhaustion, header manipulation, carpet-bombing attacks and more
- Integrated with NSFOCUS Threat Intelligence
- DNS Rate-Limiting, DNS TCP-BIT Check, DNS CNAME Check, DNS Retransmission, DNS Keyword Checking, Random Subdomain Attacks
- HTTP Keyword Checking, HTTP Authentication, HTTP Dynamic Script, HTTP FCS Check, HTTP Pattern Matching Check, HTTP Slow Attack Check, SSL/TLS Keyword Checking with JA3/JA3S/JA4/JA4S Fingerprint
- Botnet & IP Behavior Analysis, Trusted Source IP Control, Empty Connection Check
- HTTPS SSL Connection Control, HTTPS Authentication, HTTPS Renegotiation Protection, Fingerprint Protection, Decrypted Traffic Protection, Non-decrypted Traffic Protection
- SIP Authentication

### DDoS Mitigation Algorithms

- RFC Checks, Blacklists, NTI Blacklists, Whitelists, GEOIP Filter Lists, Access Control Lists, DNS Subdomain Whitelists
- TCP Regular Expression Filtering, TCP SYN Source IP Rate Limit, TCP SYN Source Bandwidth Limit, TCP SYN Time Sequence Check, TCP Fragment Control, TCP Watermark Check, TCP Pattern Matching
- SYN Check, ACK Check, Port Check, Connection Exhaustion, URL-ACK Filter Lists, Anti- spoofing, Protocol ID Check
- ICMP Fragment Control, ICMP Traffic Control
- UDP Regular Expression Filtering, UDP Payload Check, UDP Fragment Control, UDP Packet Length Check, UDP Traffic Control, UDP Watermark Check, UDP Pattern Matching, Reflection Amplification Rules
- Programmable Protection Rules

### Virtual ADS

- Virtual ADS on VMware and KVM platform available

## SOFTWARE SPECIFICATIONS – NTA

### Management

- Protocols: HTTP, SNMP, Email, Syslog
- Authentication: Local database, Radius, TACACS+, LDAP
- 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)

### Flow Monitoring

- sFlow-v4/v5, Netflow-v5/v9, NetStream-v5, Flexible Netflow, IPFIX, Cflow, Jflow

### DDoS Mitigation Algorithms

- SYN/ACK/UDP/ICMP/IGMP/HTTP/HTTPS/DNS/LAND/SIP/Protocol null/Tcpflag null/Tcpflag misuse/DNS query/DNS response/NTP amplification/SSDP amplification/SNMP amplification /CHARGEN amplification floods, private IP abnormal, traffic abnormal, auto-learning baseline, region/IP group inbound/outbound traffic abnormal
- False source IP detection
- Integrate with NSFOCUS Threat Intelligence

### Traffic Diversion

- ADS Diversion
- BGP Diversion
- Null-Route Diversion
- FlowSpec BGP

### Management Interfaces and Reporting

- Formatting: XML, PDF, CSV
- SNMP GET/Trap, syslog, Email, Flow data forwarding
- Scheduled Email report
- Traffic Report, DDoS Attack Report, Bogus Source IP Report, Traffic Comparison Report

### Virtual NTA

- Virtual NTA on VMware and KVM platform available

## SOFTWARE SPECIFICATIONS – ADBOS-L

### DDoS Monitoring & Analytics

- Real-time DDoS traffic monitoring and visualization.
- Attack trend analysis, source distribution, protocol analysis, and event statistics.
- Mitigation policy monitoring and protection status overview.
- Customizable monitoring dashboards.

### Reporting & Log Management

- Predefined and customized report generation.
- Flexible report templates, scheduled delivery, and multi-format export.
- Centralized collection, query, and export of security and operation logs.
- Platform audit log management.

### Security Policy Management

- Centralized ADS/NTA policy management.
- Traffic diversion scheduling and policy template configuration.
- Advanced protection rule configuration.
- Multi-level service domain and scrubbing resource management.

### Multi-Tenant Service Management

- Multi-tenant customer portal and self-service management.
- Customer group and service order management.
- Customizable service offerings and billing reports.
- Role-based access control (RBAC).

### Intelligent Protection & Automation

- AI-based traffic learning, threshold optimization, and policy tuning.
- Attack-defense lifecycle visualization.
- SOAR-based automated response with customizable playbooks.
- Automated response execution tracking.

### Platform Management & Security

- Configuration backup and storage policy management.
- System health monitoring and runtime alarms.
- Customizable platform branding and SSL certificate management.
- HA deployment, diagnosis, packet capture, and security configuration.

### Integration & Notification

- Email/SMS notification and customizable templates.
- SNMP, Syslog, Kafka, HTTP, and Web API integration.
- Third-party security platform integration support.

## PERFORMANCE – HARDWARE ADS

| Model | ADSNX5-HD20000 | ADSNX5-HD8500 | ADSNX5-8000 |
|---|---|---|---|
| **Mitigation Capacity** | 100Gbps to 1Tbps<br>74,400,000pps - 744,000,000pps | 100Gbps<br>74,400,000pps | 40Gbps<br>29,760,000pps |
| **Interfaces** | 1*RJ45 Serial<br>1*GE Copper<br>1*USB<br>1*Extension Slot | 1*RJ45 Serial<br>2*GE Copper<br>2*USB<br>4*Extension Slot | 1*RJ45 Serial<br>2*GE Copper<br>2*USB<br>4*Extension Slot |
| **Optional Network Interface Modules for Extension Slot** | 6*100GE QSFP28<br>4*40GE QSFP<br>16*10GE SFP+ | 4*GE Copper<br>8*GE Copper<br>4*GE SFP<br>8*GE SFP<br>2*10GE SFP+<br>4*10GE SFP+<br>2*40GE QSFP+<br>2*100GE QSFP28 | 8*GE Copper<br>8*GE SFP<br>2*10GE SFP+ |
| **Dimensions (W*D*H)** | 19”x27”x10.5”<br>6 RU | 17.4”x24.6”x3.5”<br>2 RU | 17.4”x24.6”x3.5”<br>2 RU |
| **Weight** | 121.25 lbs (55 kg) | 46.29 lbs (21 kg) | 36.38 lbs (16.5 kg) |
| **Environmental** | Operating:<br>32-113° F (0-45° C)<br>Storage:<br>-40-158° F (-40-70° C) | Operating:<br>32-104° F (0-40° C)<br>Storage:<br>-4-176° F (-20-80° C) | Operating:<br>41-104° F (5-40° C)<br>Storage:<br>14-176° F (-10-80° C) |
| **Power** | AC/DC 4* Power Supply (AC-8000W total / DC-6400W 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 |
| **Latency** | 5µs | 5µs | 5µs |

| Model | ADSNX5-HD6500 | ADSNX5-HD4500 | ADSNX3-HD2500 |
|---|---|---|---|
| **Mitigation Capacity** | 40Gbps<br>29,760,000pps | 20Gbps<br>14,880,000pps | 4Gbps<br>2,976,000pps |
| **Interfaces** | 1*RJ45 Serial<br>2*GE Copper<br>2*USB<br>4*Extension Slot | 1*RJ45 Serial<br>2*GE Copper<br>2*USB<br>4*Extension Slot | 1*RJ45 Serial<br>2*GE Copper<br>2*USB<br>4*Extension Slot |
| **Optional Network Interface Modules for Extension Slot** | 4*GE Copper<br>8*GE Copper<br>4*GE SFP<br>8*GE SFP<br>2*10GE SFP+<br>4*10GE SFP+ | 4*GE Copper<br>8*GE Copper<br>4*GE SFP<br>8*GE SFP<br>2*10GE SFP+<br>4*10GE SFP+ | 4*GE Copper<br>8*GE Copper<br>4*GE SFP<br>8*GE SFP<br>2*10GE SFP+<br>4*10GE SFP+ |
| **Dimensions (W*D*H)** | 17.4”x20.7”x3.5”<br>2RU | 17.13”x22”x1.7”<br>1RU | 17.13”x22”x1.7”<br>1RU |
| **Weight** | 44 lbs (20 kg) | 21.2 lbs (9.6 kg) | 21.2 lbs (9.6 kg) |
| **Environmental** | Operating:<br>32-104° F (0-40° C)<br>Storage:<br>-4-176° F (-20-80° C) | Operating:<br>32-104° F (0-40° C)<br>Storage:<br>14-158° F (-10-70° C) | Operating:<br>32-104° F (0-40° C)<br>Storage:<br>14-158° F (-10-70° C) |
| **Power** | AC/DC Dual Power Supply (300W total) | AC Dual Power<br>Supply (300W total) | AC Dual Power<br>Supply (300W total) |
| **MTBF** | 60,000 hours | 86,046 hours | 86,046 hours |

## PERFORMANCE –VIRTUAL ADS

| Host | |
|---|---|
| **Item** | **Recommended Configuration** |
| **CPU** | Intel(R) Xeon(R) CPU E5-2687W v4 @ 3.00GHz |
| **Memory** | 128G (at least 32GB free space) |
| **Hard Disk** | 1TB (at least 10GB free space) |
| **Operation System** | CentOS |
| **1000M NIC Support** | I210, I350, 82571, 82576, 82580 (up to 8) |
| **10Gb NIC Support** | 82599, X710/XL710 (up to 4) |
| **Virtual NIC Support** | NIC other than those above (cannot guarantee the capacity) |

| Virtual ADS for VMware | | | | | |
|---|---|---|---|---|---|
| **Item** | **Recommended Configuration** | | | | |
| **Hypervisor Support** | VMware ESXi 6.5 or above | | | | |
| **Mitigation Capacity** | (@128bytes) | 200M-2Gbps | 10Gbps | 20Gbps | 40Gbps |
| **Minimal Requirement** | **vCPU Cores** | 4 | 6 | 10 | 22 |
| | **Memory** | 16G | 16G | 16G | 32G |
| | **Storage** | 10GB at least | | | |
| **License Options** | 200M, 500M, 1G, 2G, 10G, 20G, 40G | | | | |

| Virtual ADS for KVM | | | | | |
|---|---|---|---|---|---|
| **Item** | **Recommended Configuration** | | | | |
| **Hypervisor Support** | QEMU KVM 1.5.3 or above | | | | |
| **Mitigation Capacity** | (@128bytes) | 200M-2Gbps | 10Gbps | 20Gbps | 40Gbps |
| **Minimal Requirement** | **vCPU Cores** | 4 | 6 | 10 | 22 |
| | **Memory** | 16G | 16G | 16G | 32G |
| | **Storage** | 10GB at least | | | |
| **License Options** | 200M, 500M, 1G, 2G, 10G, 20G, 40G | | | | |

## PERFORMANCE –HARDWARE NTA & ADBOS-L

| NTA | | ADBOS-L | |
|---|---|---|---|
| **Hardware** | **NTA NX3- HD2200** | **Hardware** | **ADBOS NX5-HD6000** |
| **Interfaces** | 2*GE Copper, 1*RJ45 Serial, 2*USB<br>Up to: 8*10GE SFP+<br>Or 32*GE port (copper, SFP-GE-SX, SFP-GE-LX) | **Interfaces** | 2*GE Copper (1*Management, 1*HA), 1*RJ45 Serial, 2*USB<br>6*GE Copper (3 bypass pairs), 4*1 GE SFP Ports<br>2* NIC Expansion Slots |
| **Dimensions (W*D*H)** | 17''*22''*3.5'' \| 2RU | **Dimensions (W*D*H)** | 17.1''*22''*3.5'' \| 2RU |
| **Weight** | 44 lbs (20kg) | **Weight** | 44 lbs (20kg) |
| **Environmental** | Operating: 32-113°F (0-45°C) Storage: -4-149°F(-20-65°C) | **Environmental** | Operating: 32-113°F (0-45°C) Storage: -4-149°F(-20-65°C) |
| **Hard Disk** | 2T | **Hard Disk** | 4T |
| **Power** | AC/DC Dual Power Supply (300W total) | **Power** | AC Dual Power Supply (350W total) |
| **Flow Collection Capacity** | 240,000 flows/sec (DFI)<br>10 Gbps (DPI) | **Maximal Managed Devices** | 16 Devices/ 200G Mitigation Throughput |
| **Maximal Number of Monitored Routers** | 80 | | |
| **MTBF** | 60,000 hours | **MTBF** | 60,000 hours |

## PERFORMANCE –VIRTUAL NTA

| Host | |
|---|---|
| **Item** | **Recommended Configuration** |
| **CPU** | Intel(R) Xeon(R) CPU E5-2670 v3 @ 2.60GHz, 24 threads |
| **Memory** | 32G, DDR4 |
| **Hard Disk** | ≥2TB (at least 7200 rpm) |
| **Hard Disk Number** | 2 (One of the hard disks must be at least 2T) |
| **NIC** | 2 |

| Virtual NTA for VMware | | | | | |
|---|---|---|---|---|---|
| **Item** | **Recommended Configuration** | | | | |
| **Hypervisor Support** | VMware ESXi 6.0 and above | | | | |
| **Detection Capacity** | **Flow** | 60,000/sec | 120,000/sec | 240,000/sec | 300,000/sec |
| **Minimal Requirement** | **vCPU Cores** | 10 | 12 | 16 | 24 |
| | **Memory** | 32G | | | |
| | **Storage** | 2TB | | | |

| Virtual NTA for KVM | | | | | |
|---|---|---|---|---|---|
| **Item** | **Recommended Configuration** | | | | |
| **Hypervisor Support** | QEMU KVM 1.5.3 or above | | | | |
| **Detection Capacity** | **Flow** | 60,000/sec | 120,000/sec | 240,000/sec | 300,000/sec |
| **Minimal Requirement** | **vCPU Cores** | 10 | 12 | 16 | 24 |
| | **Memory** | 32G | | | |
| | **Storage** | 2TB | | | |

## PERFORMANCE –VIRTUAL ADBOS-L

| Host | |
|---|---|
| **Item** | **Recommended Configuration** |
| **CPU** | Intel(R) Xeon(R) CPU E5-2680V2@2.80GHz |
| **Memory** | 128G, DDR4 (at least 64GB) |
| **Hard Disk** | 4TB |
| **NIC** | at least 1 |

| Virtual ADBOS-L for VMware | | | Virtual ADBOS-L for KVM | | |
|---|---|---|---|---|---|
| **Item** | **Minimum Configuration** | **Recommended Configuration** | **Item** | **Minimum Configuration** | **Recommended Configuration** |
| **Hypervisor Support** | VMWare ESXI 7.0 | | **Hypervisor Support** | QEMU KVM 1.5.3 and above | |
| **vCPU Cores** | 24 | **32** | **vCPU Cores** | 24 | **32** |
| **Memory** | 64G | **64G** | **Memory** | 64G | **64G** |
| **Storage** | 2TB | **4TB** | **Storage** | 2TB | **4TB** |