

# 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 are increasing every year, seriously damaging 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.

A comprehensive and multi-layered DDoS protection must in place to ensure the service availability.

## NSFOCUS' ON-PREMISES DEFENSES COMPONENTS

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

NTA is a DDoS detection appliance that identifies attacks via traffic flow monitoring

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

ADS is a stateless DDoS mitigation appliance that removes unwanted, malicious traffic

### ANTI-DDOS SYSTEM MANAGER (ADS-M) - MANAGES COMPLETE SOLUTION

ADS-M is a multi-tenant management system providing centralized management and reporting. A web-based customer portal is also included.

## CONCORDANT AND CLOSED LOOP DEFENSES

The NTA monitors network activity by receiving and analyzing xFlow data from border, core and/or edge routers. 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, Flowspec BGP, and Remotely Triggered Black Hole (RTBH).

When an ADS is added to the deployment, the ADS then comes under the direction of the NTA. The NTA communicates with the ADS, alerting it to the IP address(es) that are under DDoS attacks. 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.

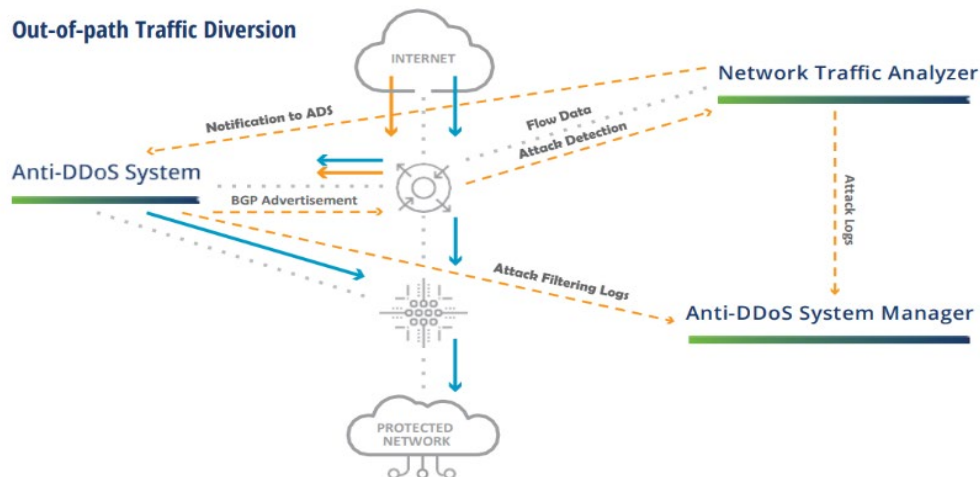
The ADS-M real-time views are highly optimized for traffic monitoring, reporting, ease of use, and improved user experience. It provides centralized management of the ADS and NTA appliances as well as support for multiple, separate configuration and reporting domains for each customer.

## 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
- 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



## 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 are able to protect against volumetric, application and web application attacks in seconds, including DNS, HTTP/S floods, UDP/TCP amplification attacks, low and slow attacks and etc. Unlike products from other vendors, NSFOCUS On-Premises DDoS Defenses don't require place any additional WAF modules to mitigate web-application attacks, making the security simple and reducing the cost and complexity of management. 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. Also, both ADS and NTA can integrate with NSFOCUS Threat Intelligence (NTI) to protect from botnet-based attacks.

## SCALABILITY PERFORMANCE AND EASY TO DEPLOY

The ADS is typically deployed at the ingress of your network, while the NTA and ADS-M appliances can be installed at any location in your network. The ADS series include models that range from 200Mbps to 400Gbps of DDoS mitigation capacity that support flexible licensing, so customers can subscribe as much mitigation capacity as needed. 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 ADS-M is available, which is easy to implement and save CAPAX. The open and documented API further simplifies integration of the system into your network by providing a programmatic interface that can be used to automate labor intensive tasks.

## MULTI-TENANT, CENTRALIZED MANAGEMENT WITH HIGH VISIBILITY

The centralized management system ADS-M supports not only central configuration of ADS and NTA, but also provides comprehensive reports and monitoring dashboards. Based on the multi-tenant design concept, administrators can monitor traffic and attack conditions from perspective of each tenant as well as global with multi-dimensional graphical displaying. Extensive reporting options include information on attack types, attack targets, protocols, ports, network status, alert information, device logs, and more. The ADS-M 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 volumetric DDoS attacks to 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 supports fully automatic diversion 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 and more
- » Integrated with NSFOCUS Threat Intelligence
- » DNS Rate-Limiting, DNS TCP-BIT Check, DNS CNAME Check, DNS Retransmission, DNS Keyword Checking
- » 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

### DDoS Mitigation Algorithms

- » RFC Checks, Black Filter Lists, NTI Black Filter Lists, White Filter Lists, GEOIP Filter Lists, Access Control Lists
- » 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

## SOFTWARE SPECIFICATIONS – NTA

### Management

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

### Virtual ADS

- » Virtual ADS KVM platform available

### 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/LAN D/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

### Virtual NTA

- » Virtual NTA on VMware and KVM platform available

### 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)

### 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

## SOFTWARE SPECIFICATIONS – ADS-M

### Centralized Management and Configuration

- » Devices: add, delete and configure
- » Monitoring: Overview, DDoS Traffic Monitoring, Net Traffic Monitoring, Attack Events, Countermeasures
- » Security Policy Configuration

### Reporting

- » Attack events, attack summaries, traffic trends
- » Extensive logging: attack summary, traffic alerts, performance, link state, authentication activity
- » Real-time and historical reporting
- » Scheduled reports by Email

### Role-Based Management Authentication

- » System Administrator
- » Device Config Administrator
- » Region Administrator
- » Audit User
- » Custom Access User
- » Region User

### Virtual ADS-M

- » Virtual ADS-M on VMware and KVM platform available

## PERFORMANCE – HARDWARE ADS

Model	ADSNX5-20000	ADSNX5-HD8500	ADSNX5-8000
<b>Mitigation Capacity</b>	100Gbps to 1Tbps 74,400,000pps - 744,000,000pps	100Gbps 74,400,000pps	40Gbps 29,760,000pps
<b>Interfaces</b>	1*RJ45 Serial 1*GE Copper 1*USB 1*Extension Slot	1*RJ45 Serial 2*GE Copper 2*USB 4*Extension Slot	1*RJ45 Serial 2*GE Copper 2*USB 4*Extension Slot
<b>Optional Network Interface Modules for Extension Slot</b>	6-ports 100GE QSFP28 4-ports 40GE QSFP 16*10GE SFP+	4-ports GE Copper 8-ports GE Copper 4-ports GE SFP 8-ports GE SFP 2-ports 10GE SFP+ 4-ports 10GE SFP+ 2-ports 40GE QSFP+ 2-ports 100GE QSFP28	8-ports GE Copper 8-ports GE SFP 2-ports 10GE SFP+
<b>Dimensions (W*D*H)</b>	19"x27"x10.5" 6 RU	17.4"x24.6"x3.5" 2 RU	17.4"x24.6"x3.5" 2 RU
<b>Weight</b>	121.25 lbs (55 kg)	46.29 lbs (21 kg)	36.38 lbs (16.5 kg)
<b>Environmental</b>	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)
<b>Power</b>	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)
<b>MTBF</b>	52,879 hours	60,000 hours	45,000 hours

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

## PERFORMANCE –VIRTUAL ADS

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

Virtual ADS for VMware

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

Virtual ADS for KVM

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

PERFORMANCE –HARDWARE NTA & ADS-M

NTA		ADS-M	
Hardware	NTA NX3- HD2200	Hardware	ADS-M HD2700
<b>Interfaces</b>	2*GE Copper, 1*RJ45 Serial, 2*USB  Up to: 8*10GE SFP+ Or 32*GE port (copper, SFP-GE-SX, SFP-GE-LX)	<b>Interfaces</b>	2*GE Copper, 1*RJ45 Serial, 2*USB  Up to: 8*10GE SFP+ Or 32*GE port (copper, SFP-GE-SX, SFP-GE-LX)
<b>Dimensions (W*D*H)</b>	17''*22''*3.5''   2RU	<b>Dimensions (W*D*H)</b>	17.1''*22''*3.5''   2RU
<b>Weight</b>	44 lbs (20kg)	<b>Weight</b>	44 lbs (20kg)
<b>Environmental</b>	Operating: 32-113°F (0-45°C) Storage: -4-149°F(-20-65°C)	<b>Environmental</b>	Operating: 32-113°F (0-45°C) Storage: -4-149°F(-20-65°C)
<b>Hard Disk</b>	2T	<b>Hard Disk</b>	2T
<b>Power</b>	AC/DC Dual Power Supply (300W total)	<b>Power</b>	AC/DC Dual Power Supply (350W total)
<b>Flow Collection Capacity</b>	280,000 flows/sec	<b>Maximal Managed Devices</b>	10*ADS, 5*NTA
<b>Maximal Number of Monitored Routers</b>	80	<b>Maximal Concurrent Users</b>	50
		<b>Maximal Number of Regions</b>	1024
<b>MTBF</b>	60,000 hours	<b>MTBF</b>	60,000 hours

PERFORMANCE –VIRTUAL NTA

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

Virtual NTA for VMware

Item	Recommended Configuration				
<b>Hypervisor Support</b>	VMware ESXi 5.5/6.0				
<b>Detection Capacity</b>	<b>Flow</b>	60,000/S	120,000/S	240,000/S	300,000/S
<b>Minimal Requirement</b>	<b>CPU Cores</b>	10	12	16	24
	<b>Memory</b>	16G			
	<b>Storage</b>	1.2TB			

Virtual NTA for KVM

Item	Recommended Configuration			
<b>Hypervisor Support</b>	QEMU KVM 1.5.3 or above			
<b>Detection Capacity</b>	<b>Flow</b>	60,000/S	120,000/S	180,000/S
<b>Minimal Requirement</b>	<b>CPU Cores</b>	24	24	24
	<b>Memory</b>	16G		
	<b>Storage</b>	1.2TB		

PERFORMANCE –VIRTUAL ADS-M

Host

Item	Recommended Configuration
<b>CPU</b>	Intel(R) Xeon(R) CPU E5-2680V2@2.8.0GHz
<b>Memory</b>	32G, DDR4 (at least 16GB)
<b>Hard Disk</b>	2TB
<b>NIC</b>	at least 1

Virtual ADS-M for VMware

Virtual ADS-M for KVM

Item	Recommended Configuration	Item	Recommended Configuration
<b>Hypervisor Support</b>	VMWare ESXI 6.7	<b>Hypervisor Support</b>	QEMU KVM 1.5.3 and above
<b>CPU Cores</b>	8	<b>CPU Cores</b>	8
<b>Memory</b>	16G	<b>Memory</b>	16G
<b>Storage</b>	2TB	<b>Storage</b>	2TB