SOLUTION BRIEF - PROTECT YOUR CUSTOMERS

ON-PREMISES **DDoS DEFENSES**

COMPREHENSIVE, MULTI-LAYERED DDOS PROTECTION

Today, Service Providers understand that a significant percentage of DDoS attacks targeting their customers can be defeated by anti-DDoS technology deployed within the providers network itself. Statistics demonstrate that nearly 50 percent of DDoS attacks observed are under 10Gbps in size, and last less than 30 minutes in duration. These attacks can easily be defended or mitigated by NSFOCUS On-Premises DDoS Defenses.

In order to defeat a DDoS attack against their customers, providers of all sizes must "detect" a DDoS attack first. Time-and-time again providers have been notified of DDoS attacks against their customers; however, without the proper detection technology in place, they had no ability to see the attack while in progress. DDoS defenses always begin with detection first. The most economical and effective way to detect DDoS attack traffic is to monitor xFlow data coming from the provider's border, core, and/or edge routers.

Once a DDoS attack is detected by the provider, the most economical and effective way to protect customers is to divert both good and bad traffic for the IP address(s) under attack to out-of-path mitigation technology. This technology is located "within" the providers' network itself. Once mitigation of the DDoS traffic is performed, legitimate traffic is re-injected back into the network for the entity under attack. This ensures that attack traffic is blocked and legitimate traffic continues to flow, without the use of null routes.

Once DDoS detection and mitigation have been addressed, a centralized management system is needed to control the overall solution. This system must allow service providers to implement multi-tenant configurations that control customer policies and rule sets, while providing real-time alerting, reporting, and analytics to the provider.

NSFOCUS provides a complete, on-premises anti-DDoS solution that provides detection, mitigation, and management as follows:

NETWORK TRAFFIC ANALYZER (NTA) - DETECTS DDOS ATTACKS

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

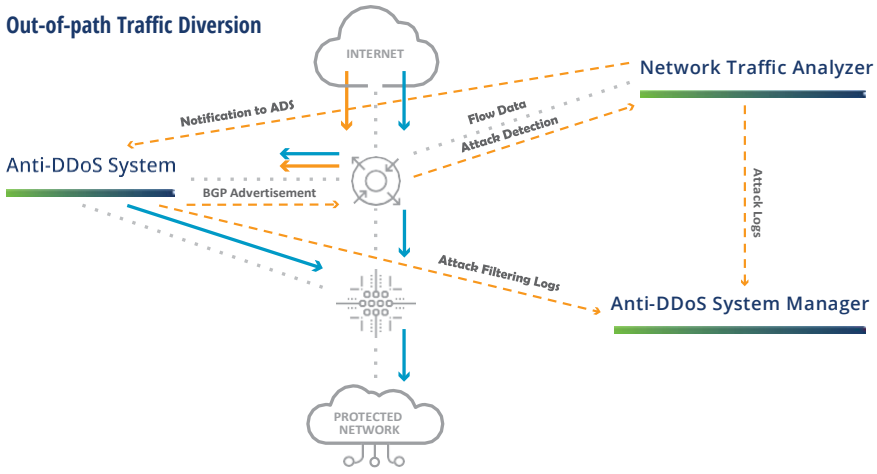
ANTI-DDOS SYSTEM (ADS) - MITIGATES DDOS ATTACKS

ADS is a 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 designed for providers. It provides centralized management of the ADS and NTA appliances as well as support for multiple, separate configuration and reporting domains for each customer. A web-based customer portal is also included.

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 made up of several algorithms and other mechanisms to accurately identify DDoS traffic from other traffic streams. User can customize NTA alert plugins with specific signatures, in order to extend NTA detection capability. Also, NTA auto-learning feature provides machine learning threshold baseline, which can be adopted in different scenarios. In addition, the NTA can integrate with NSFOCUS Threat Intelligence (NTI) to query the reputation of the suspicious source IP. On the deployment, the NTA can be deployed as a stand-alone system that provides DDoS detection only and supports Remotely Triggered Black Hole (RTBH) functionality. Under large network traffic scenarios, NTA-FLB can manage and collect flow data from multiple detect points, thus implement high performance detection and flow reuse.



NSFOCUS

BENEFITS

Complete service provider ready solution

Defend attacks against your customers

Lowest total cost of ownership (TCO)

Quick and easy install into your network

Deploy as much mitigation capacity as needed

Automatic hand-off with NSFOCUS Cloud Centers

Shorten time to redirection and cloud mitigation

Increased visibility and traffic threshold monitoring

Versatility of deployment options

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

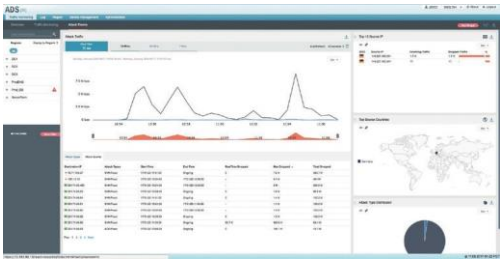
Easy to integrate and cohabitate

Automated and reliable DDoS mitigation

Efficient and intelligent protection from the botnet-based attacks with NTI

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(s) that are under DDoS attack. 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. Also, the ADS can integrate with NSFOCUS Threat Intelligence (NTI) to discard the traffic from known botnets immediately, and uploads the attack data to NTI for contributing to intelligence.

The ADS-M real-time views are highly optimized for traffic monitoring, reporting, ease of use, and improved user experience



The ADS-M is used for central configuration, management, and reporting. It can be configured in a multi-tenant mode of operation to provide separate administrative domains on a per-customer basis. The ADS-M includes a flexible, web services API to automate provisioning and reporting for your specific environment. Network operators can use the ADS-M to direct and collect packet captures from co-resident ADS systems to shorten problem resolution and incident response times. 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 on a case-by-case basis.

INDUSTRY-LEADING ACCURACY AND FASTEST TIME TO MITIGATION

NSFOCUS On-Premises DDoS Defenses incorporate the latest from our internationally-recognized research labs and is developed with over 16 years of experience protecting the world's largest banks, telecommunications, gaming, and streaming media companies. The NSFOCUS Security Labs is a cyber security threat research lab at the forefront of vulnerability assessment, threat detection, and mitigation research. Their work, combined with world-class engineering, has resulted in a solution with industry leading accuracy capable of automatically defeating advanced, multi-layer DDoS attacks in as little as 20 seconds.

SCALABILITY

The ADS series of appliances includes models that range from 1Gbps to 40Gbps of DDoS mitigation capacity that support flexible licensing, so providers can deploy as much mitigation capacity as needed. When deployed with an ADS-M appliance, the ADS systems can be clustered to withstand the most extreme volumetric and application-layer DDoS attacks.

MULTI-TENANT, CENTRALIZED MANAGEMENT

The ADS-M provides a multi-tenant configuration interface that simplifies the administration and monitoring of Managed DDoS Services. It enables service providers to create and configure customer specific security policies and reports, including daily/weekly/monthly/yearly intervals with pie charts, bar graphs, line graphs, and more. It also provides real-time traffic monitoring, log information, and detailed attack history for post-incident forensic analysis.

EASY TO DEPLOY AND INTEGRATE

The ADS is typically deployed at the ingress points to your network, while the NTA and ADS-M appliances can be installed at any location in your network. The ADS uses industry standard routing protocols to communicate with other routers in order to redirect suspicious traffic and forward legitimate traffic back into your network. A flexible web services API in the ADS-M further simplifies integration of the system into your network by providing a programmatic interface that can be used to automate labor intensive tasks.

NSFOCUS

NSFOCUS SECURITY REPORT

DDoS and Web Application Attack Landscape Report

Annual Cybersecurity Insights Report

Botnet Trend Report

Fintech Security Analysis Report

DDOS ATTACK TREND

640,000 TBytes of attack traffic in total, 79.4% increase over 2016

14.1 Gbps of average peak traffic of individual attacks, 39.1% increase over 2016

1.4 Tbps of maximum peak traffic among individual attacks, nearly 100% over 2016

DDOS ATTACK TREND

Linux/UNIX hosts and servers constituted a strong base (55%) of DDoS attack sources. IoT devices were more frequently seen in small attacks (29.8% in small attacks and 10.3% in large attacks). Windows servers were often present in large attacks.

The trend of traditional reflection attacks, such as those based on the Network Time Protocol (NTP), slowed down, while modern ones that abused Memcached servers surged and related peak traffic hit a new record high of 1.35 Tbps

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

NSFOCUS HYBRID DDoS DEFENSES

Many service providers utilize a hybrid approach to defeat the damaging effects of DDoS attacks. The approach combines NSFOCUS On-Premises Defenses (designed to defeat attacks against your customers) with NSFOCUS Cloud DDoS Protection Service (designed to defeat attacks that impact your infrastructure).

Working in unison, this Complete Service Provider DDoS Mitigation Solution eliminates smaller attacks on-premises, while defending infrastructures from larger attacks using the NSFOCUS Cloud. Both defenses are integrated, resulting in increased bandwidth visibility, reduced cloud redirect times for mitigation, and coverage for all L3-L7 DDoS attacks.

SOFTWARE SPECIFICATIONS

ADS SERIES

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/CHARGEN/ Memcached), 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, 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
- 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

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

NTA

Flow Monitoring

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

DDoS Attack Detection

- 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

- SNMP GET/Trap, syslog, Email, Flow data forwarding
- Email report regularly

Virtual NTA

- Virtual NTA on VMware platform available

ADS-M

Centralized Management and Configuration

- Devices: add, delete and configure
- Multi-tenant
- Security policies
- High availability
- ADS clustering
- NTA Clustering

Reporting

- Attack events, attack summaries, traffic trends
- Extensive logging: attack summary, traffic alerts, performance, link state, authentication activity
- Email report regularly

Role-based Management Authentication

- Administrator, supervisor and user

Virtual ADSM

- Virtual ADSM on VMware platform available

FOR SERVICE PROVIDERS OF ALL SIZES

NSFOCUS On-Premises Defenses is the ideal solution for today's service providers to defeat DDoS attacks against their customers. It is highly scalable and is performance optimized to meet the current and future needs of service provider environments. It is also easy to deploy, flexible, and provides a multi-tenant configuration interface to simplify the configuration and administration of large-scale Managed DDoS Services.

HARDWARE SPECIFICATIONS

ADS SERIES

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+ 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 (W*D*H)	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		

NTA

Hardware	NTA 2000E
Interfaces	2*GE Copper, 1*RJ45 Serial, 2*USB Up to: 8*10GE SFP+ Or 32*GE port (copper, SFP-GE-SX, SFP-GE-LX)
Dimensions (W*D*H)	17"*20.2"*3.5" | 2RU
Weight	36.6 lbs (16.6kg)
Environmental	Operating: 32-113°F (0-45°C) Storage: -4-149°F(-20-65°C)
Power	AC Dual Power Supply (350W total)
Flow Collection Capacity	120,000 flows/sec
Maximum number of monitored routers	80
Maximum number of monitored router interfaces	2000
MTBF	60,000 hours

ADS-M

Hardware	ADS-M 1600E
Interfaces	2*GE Copper, 1*RJ45 Serial, 2*USB Up to: 8*10GE SFP+ Or 32*GE port (copper, SFP-GE-SX, SFP-GE-LX)
Dimensions (W*D*H)	17.4"*20.2"*3.5" | 2RU
Weight	41.89 lbs (19kg)
Environmental	Operating: 32-113°F (0-45°C) Storage: -4-149°F(-20-65°C)
Power	AC Dual Power Supply (350W total)
Maximum managed devices	10*ADS or 10*NTA or 10*ADS+5*NTA
Maximum concurrent users	50
Maximum number of regions	1024
Maximum IP addresses/region	65,535
MTBF	60,000 hours

VIRTUAL ADS

Host		Virtual ADS	
Item	Recommended Configuration	Item	Recommended Configuration
CPU	Intel(R) Xeon(R) 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 1.5.3
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)		

VIRTUAL NTA

Item	Recommended Configuration	CPU	Flows/sec
CPU	Intel® CoreTM i7-2600 CPU @ 3.40GHz 4 cores and 8 threads	1*2CPU	30,000
Memory	16GB	1*4CPU	120,000

Hard disk	1TB + 2GB	1*8CPU	200,000
NIC	2	1*16CPU	240,000

VIRTUAL ADS-M

Item	Recommended Configuration	Performance Specification	Data Volume
CPU	Intel® Xeon® CPU E5-2650 v3 @ 2.30GHz 10 cores and 20 threads Assign 2 cores to virtual machine.	Support to manage 10 devices of ADS.	Each ADS upload the traffic data of 100 destination IP*10 source IP.
Memory	32GB Assign 8G to virtual machine.	Support to manage 10 devices of NTA.	Each NTA uploads the traffic data of 200 regions, and each region includes 4 IP groups.
Hard disk	1TB + 2GB	Support to manage 10*ADS and 5*NTA simultaneously.	Each ADS upload the traffic data of 100 destination IP*10 source IP.
NIC	6		Each NTA uploads the traffic data of 200 regions, and each region includes 4 IP groups.