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 defeated 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 begins 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

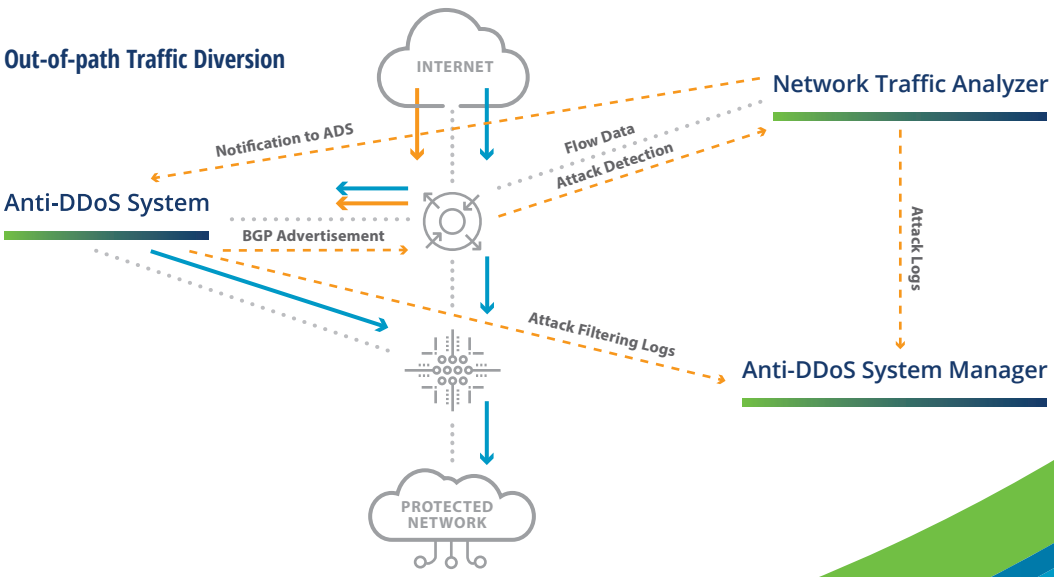
NTA is a DDoS detection appliance that identifies attacks via traffic flow monitoring

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.



NSFOCUS

BENEFITS

Complete service provider-ready solution

Defeats 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

Shortens 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

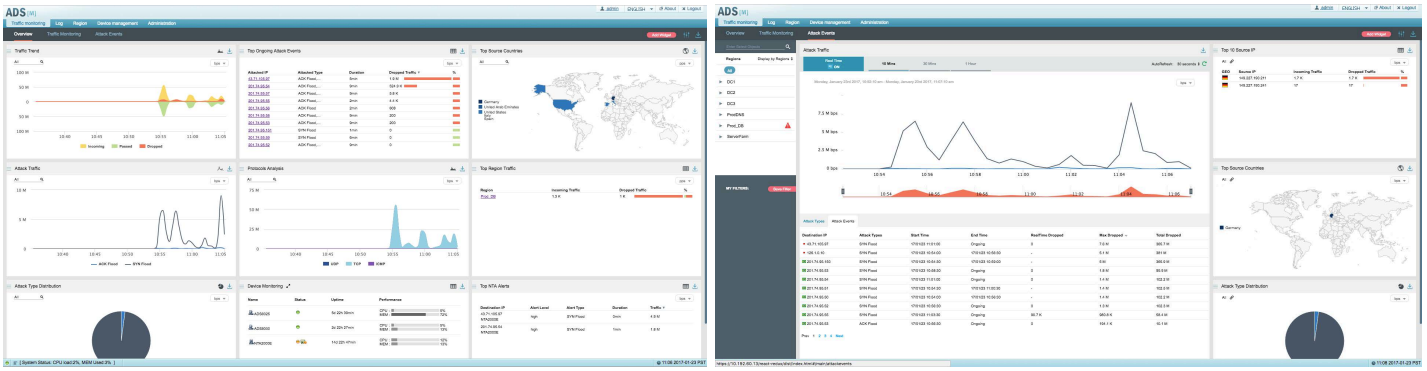
Easy to integrate and cohabitate

Automated and reliable DDoS mitigation

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. The NTA can be deployed as a stand-alone system that provides DDoS detection only and supports Remotely Triggered Black Hole (RTBH) functionality.

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 notifies 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



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 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

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 floods, TCP flag misuse, flag null, Private IP, abnormal traffic, alert threshold self-learning, IP group inbound/outbound attack traffic, business domain and region inbound/ outbound attack traffic

ADS Traffic Diversion

- Diversion notice to routers based on traffic volume

Management Interfaces and Reporting

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

Virtual NTA

- Virtual NTA on VMware platform available

ADS SERIES

DDoS Protection

- Comprehensive, multi-layered protection against volumetric, application, and web application attacks
- Multi-protocol support and advanced inspection including TCP, UDP, HTTP, ICMP, NTP, DNS, SIP, fragments, flooding, connection exhaustion, header manipulation, and more
- Integrated with NSFOCUS Cloud Security Platform

DDoS Protection and Mitigation Algorithms

- 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
- Protect against both known and unknown DDoS attacks

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

ADS-M

Centralized Management and Configuration

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

Reporting

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

Role-based Management Authentication

- Administrator, supervisor, and user

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-M

Hardware	ADS-M 1600
Interfaces	1xRJ45 serial 2x100/1000M (copper) 4x1000M SFP slots
Dimensions (WxDxH)	17.4"x20.2"x3.5" | 2 RU
Weight	41.89 lbs (19 kg)
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 (optional NTA license)	60,000 flows/sec
Maximum managed devices	40 ADS, 20 NTA
Maximum concurrent users	50
Maximum number of regions	1024
Maximum number of policies	4000
Maximum IP addresses/region	65,535
MTBF	60,000 hours

NTA

Hardware	NTA 2000
Interfaces	2xRJ45 serial 2xUSB 2.0 4xGE (copper), 4xGE (SFP)
Dimensions (WxDxH)	17"x20.2"x3.5" | 2 RU
Weight	36.6 lbs (16.6 kg)
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	20
Maximum number of monitored router interfaces	1,000
MTBF	60,000 hours

VIRTUAL NTA

Item	Recommended Configuration
CPU	Intel® Core™ i7-2600 CPU @ 3.40 GHz Four cores and eight threads
Memory	16 GB
Hard disk	1 TB + 2 GB
NIC	2

CPU + MEM	Flows/sec
1*2CPU+16G	30,000
1*4CPU+16G	120,000
1*8CPU+16G	200,000
1*16CPU+16G	240,000

ADS SERIES

Hardware	ADS 8000	ADS 6025	ADS 4020	ADS 2020
Mitigation Capacity	40 Gbps | 29,760,000 pps	20 Gbps | 14,880,000 pps	10 Gbps | 8,928,000 pps	4 Gbps | 2,976,000 pps
Interfaces	Up to: 8*10GE SFP+ Or 4*10GE SFP+ and 16*GE port (copper, SFP-GE-SX, and SFP-GE-LX available)	Up to: 8*10GE SFP+ Or 32*GE port (copper, SFP-GE-SX, SFP-GE-LX and bypass module available)	Up to: 8*10GE SFP+ Or 32*GE port (copper, SFP-GE-SX , SFP-GE-LX and bypass module available)	Up to: 4*GE +4*SFP Or 8*SFP (copper, SFP-GE-SX, SFP-GE-LX and bypass module available)
Dimensions (WxDxH)	24.7"x17.4"x3.5" 2 RU		22.6"x17"x3.5" 2 RU	
Weight	36.49 lbs (16.55 kg)		24.25 lbs (11 kg)	
Environmental	Operating: 41-104° F (5-40° C) Storage: 14-158° F (-10-70° C)		Operating: 32-104° F, (0-40° C) Storage: -4-176° F, (-20-80° C)	
Power	AC Dual Power Supply (450W total)		AC Dual Power Supply (350W total)	
MTBF	45,000 hours		60,000 hours	