NSFOCUS

NSFOCUS ADBOS

Active Defense Business Operation System

OVERVIEW

With the rapid development of the digital economy, Internet Service Providers (ISPs) are faced with greater challenges than ever:

» The growing data traffic with a phenomenal annual rate has not translated into a matching increased profit.

» More and more newly emerged Cloud Service Providers started to set strategy emphasis on cloud hosting and bandwidth lease services which are intended to carve up the market share of ISPs.

» Increasingly stringent regulatory challenges lead to the constant shrinking of ISPs' traditional service marketplace.

No doubt shifting the service mode and expanding into cloud services have become one of the best choices for ISPs to overcome these challenges. ISPs could do more to position themselves as leading the charge against DDoS attacks, as the DDoS (Distrusted Denial-of-Service) attack has been around for decades and is still the most worrisome threat to all organizations, both in terms of protecting their networks and offering security capabilities to their customers.

WHAT IS ADBOS?

NSFOCUS ADBOS is a breakthrough, smart traffic scrubbing scheduling platform for centralized management of all on-premises Anti-DDoS devices and cloud services. It can be operated either by a self-service portal that is easy to use for the management of many customers.

NSFOCUS ADBOS provides a unique user experience for each customer with customer-specific branding and corporate identity, per user/group/role permission for controlled access, and mass customization and configuration operation. Every customer is like using an independent system that enables traffic monitoring, scrubbing, and scalability as their demands.
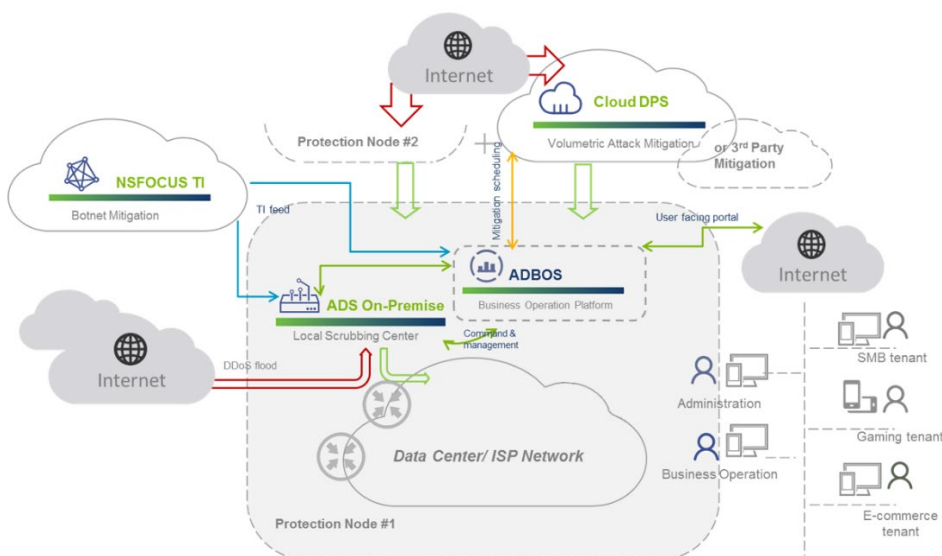
INTELLIGENT RESOURCE SCHEDULING

According to the various attacking traffic scales, NSFOCUS ADBOS has realized automatic schedule attack traffic mitigation from on-premises devices, ISP protection nodes, or even the cloud resource.
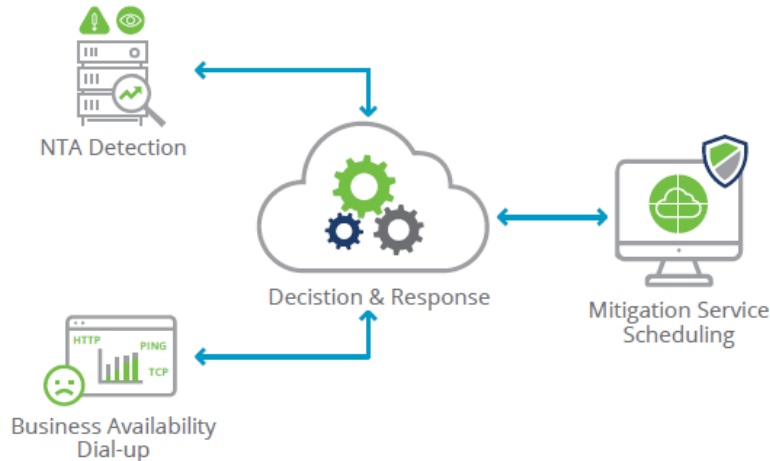

MULTI-TENANT SELF SERVICE PORTAL

NSFOCUS ADBOS is specifically for ISPs to cope with volumetric traffic with efficient use of resources, cost-effectiveness, time savings, scalability, and improved customer services. A single portal structure delivering services to multiple customers reduces the cost of operating a multi-tenant environment rather than multiple portals. The easy-to-use single dashboard also gives global administrators easy visibility for centralized control and management of many customers with sub-organizations by flexible access control.
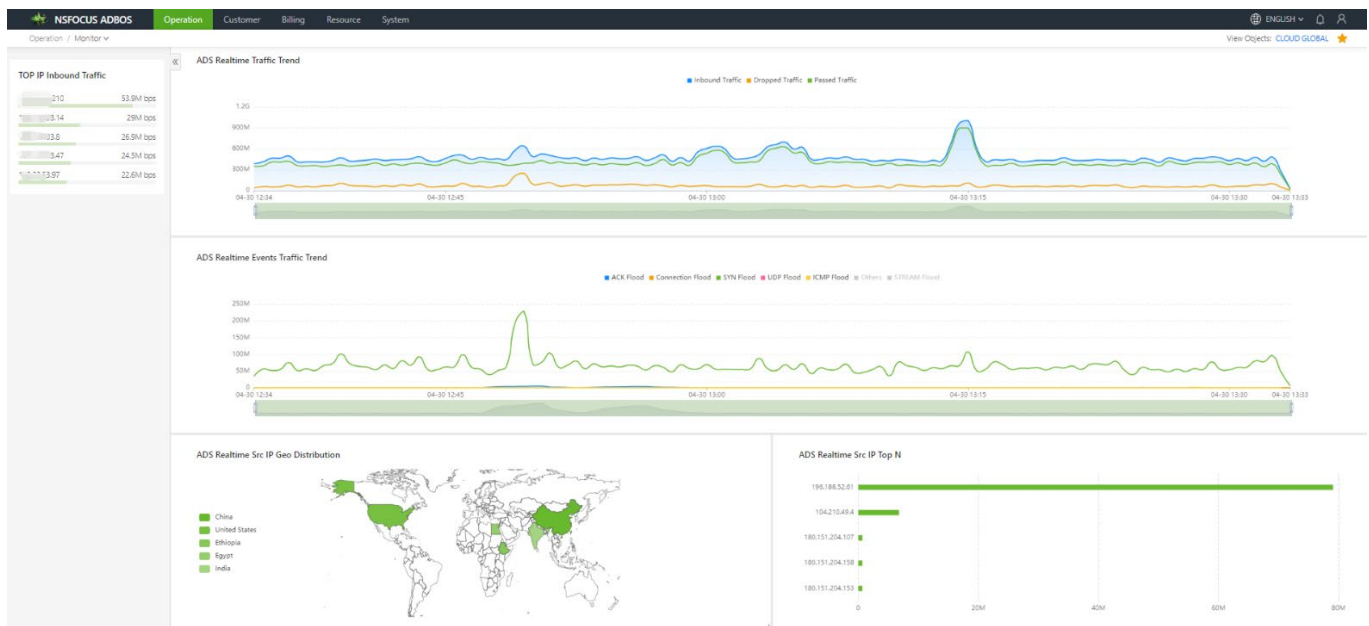
SCALABLE, OPERATIONAL, PROFITABLE

NSFOCUS ADBOS is a scalable virtualized product requiring minimal investment. It covers all ADS models and supports multi vendors by using plug-ins. ADBOS facilitates business growth and streamlines the operation process:

» Shorten the response time from hours to minutes

» Save labor costs by 50%

» Cut down mitigation escalation process and enable user self-service mitigation

» Businesses need high availability, reliability, and security scalability for their IT infrastructure, specifically Anti-DDoS service. NSFOCUS ADBOS offers what you need and help expand your product lines in the competitive market.

FEATURES AND FUNCTIONALITIES OF NSFOCUS ADBOS

Features and Functionalities	ADBOS
User Portal	Yes
Multi-tenancy	Yes
Tenant scrubbing capacity differentiation	Yes
Bill and account management	Yes
Mitigation scheduling between nodes	Yes
Cloud-based security solution	Yes
Real-time monitoring	Yes
Device health monitoring	Yes
Target user	ISP, IDC, MSSP and Business Operation team
Support 3rd-party DDoS systems by plug-in	Yes
API to 3rd parties Cloud DDoS platform for total mitigation, local and cloud	Yes
Flexibly allocate local Anti-DDoS resources for customer services	Yes

ADBOS HARDWARE REQUIREMENTS

1. Standalone

CPU	RAM	DISK	QTY	Managed ADS&NTA&WAF	Management Capability of Customer's IP Address	Limitation of scenario
24 cores	32G	1TB	1	≤5	≤5000	Normal number of alerts. The customer does not require the storage of traffic and alert data for more than six months.

2. Cluster (Minimum Configuration)

CPU	RAM	DISK	QTY	Managed ADS&NTA&WAF	Management Capability of Customer's IP Address	Limitation of scenario
24 cores	32G	2TB	2	≤20	≤20000	Normal number of alerts. The customer does not require the storage of traffic and alert data for more than six months. （minimum configuration is appropriate for POC test）
24 cores	32G	1TB	1			

3. Cluster (Recommended Configuration)

CPU	RAM	DISK	QTY	Managed ADS&NTA&WAF	Management Capability of Customer's IP Address	Limitation of Scenario
32 cores	64G	8TB	2	≤64	≤60000	Cloud scenario with long-term storage of traffic and alert data.
32 cores	64G	2TB	1			