DATASHEET

Cloud DPS

Cloud DDoS Protection Service

As the security threat landscape continues to evolve, threat actors and their methods are evolving as well. New motivations for DDoS attacks and network breaches are being discovered regularly and extortionists targeting organizations with threats of DDoS attacks are becoming more common. These attackers are suspected to have enough capacity at their disposal to take almost anyone offline. In addition, DDoS attacks are now being used as a distraction for other malicious behavior, including APT attacks and the exfiltration of valuable data.

It has never been easier and less expensive to launch massive DDoS attacks that result in loss of revenue, loss of customers, disruption of service availability, damage to brand, theft of vital data, and more. DDoS attacks that used to be measured in hundreds of Mbps are now observed in hundreds of Gbps, due to the proliferation of easy-to-rent botnets, and the continued development of sophisticated attack amplification techniques. Without the proper defenses in place, organizations today are faced with substantial risk to their business.

The NSFOCUS Cloud DDoS Protection Service protects organizations against debilitating and costly DDoS attacks. NSFOCUS' anti-DDoS detection and mitigation technologies have prevented millions of DDoS attacks and are used by some of the world's largest banks, telecommunications companies, technology companies, and other organizations. This technology powers the NSFOCUS Cloud Centers and is the perfect complement to our on-premises DDoS Protection Solution by protecting your organization from volumetric attacks that would otherwise completely saturate your bandwidth and take you offline.

WORLD-WIDE COVERAGE

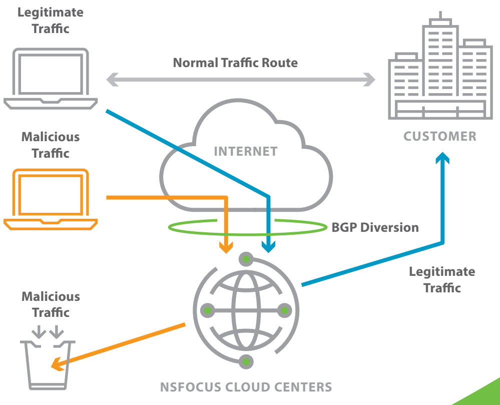
The NSFOCUS Cloud is made up of five NSFOCUS Cloud Centers strategically located where vast amounts of internet traffic originates and terminates with the largest Internet exchanges.*

Ashburn
Frankfurt
Singapore
Silicon Valley
London

SEAMLESS INTEGRATION WITH YOUR NETWORK

The NSFOCUS Cloud DDoS Protection Service utilizes BGP diversion for incoming traffic redirection to the Cloud Centers for attack traffic removal. Legitimate traffic is returned using either GRE tunneling or a direct connection to your network.

- A BGP announcement will divert customer traffic when under attack
- The solution will pull traffic into multiple Cloud Centers for cleaning
- Malicious traffic will be discarded by the Cloud Center closest to the source of attack
- Legitimate traffic will be forwarded to customer via GRE or direct connection
- Operates within acceptable latency for all regions within the global footprint



*Contact NSFOCUS sales for the latest coverage map

BENEFITS

Alleviate concerns over loss of revenue, loss of customers, damage to brand, service availability, and theft of vital data

Reduce operating expenses and free up valuable IT security personnel

Eliminate costly bandwidth charges

KEY FEATURES

Strategically located, global Cloud Centers

Seamless integration with your network

Direct access to popular cloud services, including Amazon, Dropbox, Azure, and more

Automatic handoff with NSFOCUS on-premises DDoS defenses

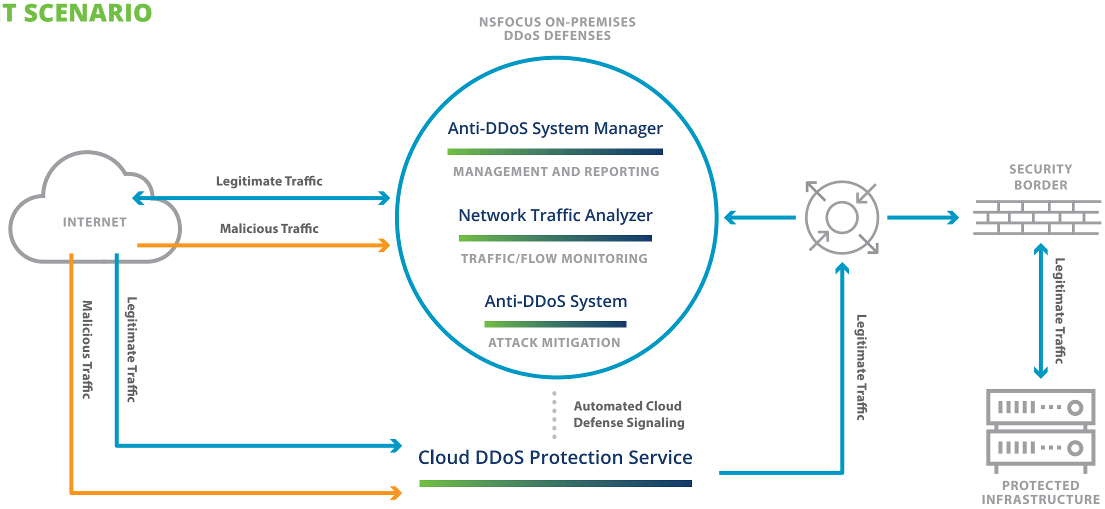
Regular and user configurable data feed update intervals

Easy to use, feature rich web portal

NSFOCUS HYBRID DDOS DEFENSES

Many service providers and enterprises utilize a *hybrid approach* to defeat the damaging effects of DDoS attacks. This approach combines NSFOCUS On-Premises Defenses with the on-demand NSFOCUS Cloud DDoS Protection Service. Working in unison, the solution eliminates smaller attacks on-premises; while defending infrastructures against bandwidth saturating DDoS attacks using the NSFOCUS Cloud. Both defenses are fully integrated; resulting in increased bandwidth visibility, reduced cloud redirect times for mitigation, and coverage for all L3-L7 DDoS attack vectors.

DEPLOYMENT SCENARIO



In the above scenario, NSFOCUS On-Premises DDoS Defenses is deployed at the customer site. The on-premises defenses can be deployed inline or out-of-path. The defenses are designed to defeat all DDoS attacks that are under the available Internet bandwidth. The defenses also monitor a host of attributes and can easily detect conditions that indicate an impending bandwidth saturation attack. In this instance, the on-premises defenses signal the NSFOCUS Cloud DPS via an always-on BGP session with the cloud. This signal effectively instructs the NSFOCUS Cloud to reroute all incoming traffic through the Cloud Centers for the IP address under attack.

DELIVERING CLEAN TRAFFIC

The NSFOCUS Cloud DPS utilizes BGP diversion for incoming traffic redirection to the Cloud Centers for attack traffic removal. Reinjecting legitimate traffic back to the original destination is achieved in one of two ways:

Option 1 – Dedicated Network Connections – Preferred Method

- Once in place, dedicated network connections eliminate the reliability concerns associated with using GRE tunnels
- Provides an always-on connection to NSFOCUS Cloud Centers

Option 2 – GRE Tunnels

- This approach is used to deliver clean traffic when a dedicated network connection is not possible

WEB PORTAL HIGHLIGHTS

- View active attacks
- View graphs for total & clean traffic
- View previous attack history
- Under attack Panic button
- Automated mitigation
- Remotely Triggered Black Hole (RTBH)
- Disable mitigation to an IP
- Automatic customer alerts
- Enforced password complexity
- Login/account activity audit log
- Reseller/partner views