DATASHEET

NSFOCUS

Cloud DPS

CLOUD DDOS PROTECTION SERVICE

KEY BENEFITS

Ensure business continuity
Protect business reputation and brand
Launch DDoS mitigation service to customers for ISP/IDC/Hosting/IaaS/PaaS providers

KEY FEATURES

7 Global Scrubbing Centers and 7T+capacity

Interconnect with world's major ISPs and Internet Exchange Points

Always-On or On-Demand mitigation based on customer interest (BGP Diversion)

Support http/https/TCP/UDP protocol (DNS Diversion)

IPv6 Ready

Up to unlimited mitigation usage

Zero Time-To-Mitigate, mitigation resources always ready after the initial order

Backed by unique Threat Intelligence source from China and all over of the world

Hybrid deployment ready with NSFOCUS on-premises appliance

OVERVIEW

Along with the 5G technology and the increase of IoT devices, DDoS attacks are continuing to increase in frequency, volume and duration to affect a business's continuity and reputation. Today's threat actors understand how easy and inexpensive it is to launch DDoS attacks that result in Internet outages and potential damage to enterprise infrastructure.

However, enterprises often face the dilemma of heavy equipment investment (CAPEX), lack of security professionals, complex production location (as enterprises shift their production and development into AWS, Azure and other IaaS/PaaS providers), more importantly, insufficient bandwidth resources.

CLOSE TO SOURCE MITIGATION WITH GLOBAL SCRUBBING CENTERS

With 7 global Scrubbing Centers carrying 7Tbps capacity, NSFOCUS Cloud DPS ensures its customers will be protected against even the largest DDoS attacks in the history.

Worldwide business hotspots include United States, Europe, Asia Pacific and Latin America are covered with local Scrubbing Centers.

Well selected transit providers combined with Anycast technology ensures all customers could enjoy the consolidated mitigation by all Scrubbing Centers simultaneously, not worrying about traffic congestion in local Scrubbing Center due to mass DDoS attack volume.

DNS DIVERSION - EASY AND QUICK ACCESS FOR EVERY BUSINESS

NSFOCUS Cloud DPS - DNS is a service which allows customers use DNS diversion to send its traffic to Scrubbing Centers.

Scrubbing Centers will act as a proxy once the customer has appointed its DNS to the protected public IP offered by NSFOCUS, customer origin server IP are masked and volumetric malicious traffic will be blocked before its arriving. Only legitimate traffic will be sent to origin sites via internet after mitigation.

Customers do not need to have IP space, ASN or running BGP to benefit from this service to reduce the DDoS risk, typical customers include:

- OTT/Online entertainment/Gaming
- Government/Finance
- Small and medium enterprise

BGP DIVERSION –PROTECT THE WHOLE PREFIX FOR SERVICE PROVIDERS

Customers who own or manage an Autonomous System (AS) cloud enjoy the benefit from using NSFOCUS Cloud DPS – BGP to protect the whole IP subnet at once. By using Border Gateway Protocol (BGP), Customer's traffic is automatically diverted to its nearest NSFOCUS Scrubbing Centers where attacks are mitigated.

Legitimate traffic is routed to customer selected location via NSFOCUS global backbone network and this ensures customers always receiving its traffic from nearest Scrubbing Center even when the mitigation is executed at other locations, optimum network quality can be expected.

GRE tunnels, Direct Connect or Partner Connect can be selected for peering with the customer network.

NSFOCUS cloud or on-premises traffic monitoring solution is available to enable automated traffic diversion. Always-on mode is also possible up on customer need.

Typical customers include:

- ISP/IDC/Hosting
- IaaS/PaaS provider
- Enterprise

CROSS CONNECT– ENABLE VALUE ADDED SERVICE FOR SERVICE PROVIDERS

To have an in-house DDoS Mitigation Service for its on-net customers would be perfect for service providers who have set-up their goal for Managed Security Service Provider transformation. NSFOCUS is offering a shortcut for service providers to launch a DDoS Mitigation service within a few months, via a cross connect between service provider POP and NSFOCUS scrubbing centers for both traffic diversion and re-injection. Customer traffic will remain in service provider AS and almost no noticeable latency will be introduced.

Commercial and technical highlights may include:

- Revenue Share / Pay-as-You-Use
- Go-to-Market Support
- 24/7 Security Operation Center Support

DDOS PROTECTION

- Comprehensive, stateless, multi-layered protection against volumetric, application, and web application attacks
- Protected Protocols: HTTP, HTTPS, POP3, SMTP, SIP, DNS, FTP, NTP, SNMP
- Advanced protection against SYN Flood, ACK Flood, UDP Flood, ICMP Flood, TCP No-Flag Flood, HTTP Flood, HTTPS Flood, DNS Query Flood, FIN/RST Flood, Connection Flood, SIP Flood, TCP Misuse, TCP Fragment, UDP Fragment, DNS Amplification, NTP Amplification, SSDP Amplification, SNMP Amplification, CHARGEN Amplification, Memcached Amplification, Low and Slow, Slow Read, Slowloris, fragments floods, connection exhaustion, header manipulation and more
- Integrated with NSFOCUS Threat Intelligence for enhanced Botnet Attack Protection
- 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

- Botnet & IP Behavior Analysis, Trusted Source IP Control, Empty Connection Check
- HTTPS SSL Connection Control, HTTPS Authentication, HTTPS Renegotiation Protection, HTTPS Non-Decrypted Traffic Protection, HTTPS Decrypted Traffic Protection.
- Always-on mitigation for Hit-and-Run and Carpet-Bombing Attacks

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
- SYN Check, ACK Check, Port Check, Connection Exhaustion, URL-ACK Filter Lists, Anti- spoofing
- ICMP Fragment Control, ICMP Traffic Control
- UDP Regular Expression Filtering, UDP Payload Check, UDP Fragment Control, UDP Packet Length Check, UDP Traffic Control, UDP Session Authentication, UDP Watermark Check
- HTTP&HTTPS Authentication, Decrypted and Non-decrypted Https Traffic Analysis.
- Pattern Matching, Reflection Amplification Rules, Botnet& IP Behavior Control, SIP Authentication, Programmable Rule, Protocol ID Check

ENHANCED DDOS DETECTION

- Multi-Stage DDoS Detection Engine: Employs over 30 detection vectors to accurately identify DDoS traffic from legitimate traffic streams.
- Traffic Flow Monitoring: Analyzes xFlow data (e.g., NetFlow, sFlow) from border, core, and edge routers to monitor network activity.
- Customizable Alert Plugins: Allows users to create specific signatures to extend detection capabilities.
- Machine Learning-Based Thresholds: Automatically generates dynamic threshold baselines using machine learning for adaptive detection.
- Integration with NSFOCUS Threat Intelligence (NTI): Enhances detection by querying the reputation of suspicious source IPs.
- Automated Response Actions: Supports multiple response mechanisms, including BGP diversion, Flowspec BGP, and Remotely Triggered Black Hole (RTBH).
- Scalable Deployment: Can be deployed as a standalone system or integrated with NSFOCUS Anti-DDoS System (ADS) and ADS Manager (ADS-M) for comprehensive protection.
- Low False Positives: Designed to minimize false positives while maintaining high detection accuracy.
- Multi-Tenant Support: Offers multi-tenant configurations for service providers, allowing separate administrative domains per customer.
- Flexible Licensing Model: Provides on-demand licensing to accommodate varying network sizes and requirements.

24*7 SECURITY OPERATIONS CENTER (SOC)

Email: cloud-support@nsfocusglobal.com

Phone:

USA: +1-844-673-6287 or +1-844-NSFOCUS
UK: +44 808 164 0673 or +44 808 164 0NSF
Australia: +61 2 8599 0673 or +61 2 8599 0NSF
Netherlands: +31 85 208 2673 or +31 85 208 2NSF
Brazil: +55 13 4042 1673 or +55 13 4042 1NSF
Japan: +81 3-4510-8673 or +81 3-4510-8NSF
Singapore: +65 3158 3757
Hong Kong: +852 5803 2673 or +852 5803 2NSF
Middle East: +973 1619 7607

SELF-SERVICE CUSTOMER PORTAL

- Traffic visibility
- Attack analytics including type, volume, source region, Top N source IPs
- Self-serviced report, online, downloadable or in email
- SSO Support (OAuth 2.0/OpenID)
- Restful API ready

MANAGED SECURITY SERVICE

Basic and Advanced Managed Security Service are open to all customers regardless of the level of service package they booked.

- Optimized SLA include mitigation effect
- Proactive traffic monitoring
- Protection policy tuning
- Attack response with expert intervention
- Advanced report by expert
- Dedicated Service Account Manager
- Governance meeting

INQUIRIES AND ORDERS

https://nsfocusglobal.com/contact-us/

NSFOCUS

NSFOCUSGLOBAL.COM 690 N McCarthy Blvd, Suite 170, Milpitas, CA 95035