NEXUSGUARD

DDoS Protection Made Simple

Origin Protection

The Nexusguard Managed DDoS Mitigation Platform encompasses four essential modules: Application Protection (AP), Clean Pipe (CP), DNS Protection (DP) and Origin Protection (OP).

Geared towards safeguarding large network owners, especially ASN-level CSPs, and those managing hundreds of Class C networks, Nexusguard's OP is a highly effective and responsive platform that protects critical network infrastructure as well as all downstreams against L3-L4 DDoS attacks. OP complements Nexusguard's AP by protecting backend infrastructure from L3 and L4 attacks, and covers all network components, including internal websites, email servers, FTP servers, and other applications against volumetric and protocol-based DDoS attacks, such as SYN floods, fragmented packets attacks, Ping death, Smurf DDoS, and the like.

How Does It Work?

Upon detection of a malicious attack, the Border Gateway Protocol (BGP) route of the /24 IP prefix under attack is advertised to the Internet via Nexusguard and traffic will be diverted to Nexusguard's global scrubbing centres for scrubbing. After malicious traffic has been dropped at the scrubbing centers, clean traffic is then returned to customer networks over Generic Routing Encapsulation (GRE) tunnels. Traffic diversion can be triggered manually, or automatically through the use of Nexusguard's proprietary Cloud Diversion App without the need of any on-premise equipment.

Key Features

Safeguard against Volumetric Attacks
Protects CSPs and downstream customers from the largest L3-L4 DDoS attacks using best-of-breed DDoS attack mitigation techniques

Smart Mode Detection
AI-driven Smart Mode that is capable of detecting cyber-attacks with improved speed and precision.

Highly Autonomous Traffic Diversion
Cloud Diversion feature enables fully automated traffic diversion

Surgical Mitigation
Automatically removes only attack traffic while ensuring the flow of legitimate traffic is uninterrupted

Flow Data Analysis Capability
Multi-layered detection engine to analyze traffic data and detect traffic anomalies

Wide Range of Flow Protocols
Supports Netflow v5/9, IPFLIX, sflow v2/4/5 and Netstream v5/8/9

Clean Traffic Delivery
After scrubbing, clean traffic is routed back to customers' networks via GRE tunnels

Flexible Attack Detection Modes

Nexusguard's OP module offers three modes of detection that offer flexibility to operators' adaptation to dynamic attack scenarios. The three modes are *Normal, Rapid* and *Smart*.

- Normal Mode is suitable for continuous flows of attack traffic, monitoring traffic flow from customer networks to give advance warning of an attack, and triggering the corresponding mitigation action needed when the traffic exceeds a predefined detection threshold for a specified time frame.

- Rapid Mode is suitable for continuous flows of attack traffic, bursty traffic and hit-and-run attacks, monitoring traffic flow from customer networks to forewarn of an attack, and triggering the corresponding mitigation action needed when the traffic exceeds the product of the predefined detection threshold and 60 seconds..

- Smart Mode is suitable for dynamic traffic profiles that are dynamic in nature and, is based on Nexusguard's proprietary AI detection system that employs deep learning technologies to deliver intelligent and accurate detection capabilities that are context-aware, ultimately increasing accuracy and drastically reducing false positives.

Connectivity Alternatives to GRE

OP allows for Direct Connect from CSPs' network edge as an alternative means of returning clean traffic directly from our scrubbing centres to customer networks. For CSPs whose data centres are geographically located in the vicinity of our POPs or co-located with our data centres, they can opt for a direct connection with our network by establishing a direct physical connection with Nexusguard's scrubbing centres.

GRE is the main deployment method used for the delivery of clean traffic, and although Direct Connect is an alternative method, it is not designed to replace GRE, rather it is used to further enhance the overall solution when combined with GRE. The combination of Direct Connect and GRE is hugely effective during very large attacks as attack traffic is shared and distributed between our logically connected scrubbing centres via GRE and directly connected scrubbing centres, thus ensuring that customer networks are always fully protected.

Direct Connect is not limited to IDCs within the proximity of Nexusguard PoPs or sharing the same IDC, point-to-point connectivity can also be extended through Virtual Private Connect (VPC) service providers at their location.

DDoS Attack Alerts

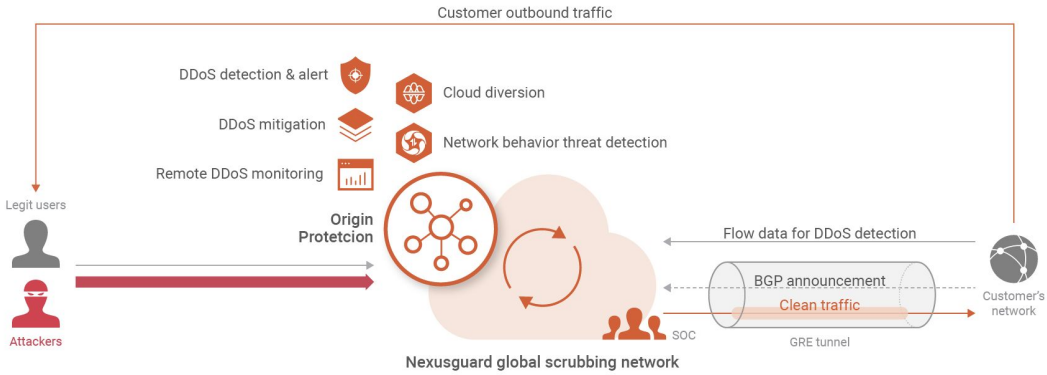
Attack alerts are sent to the Customer/ Partner Portal, and email alerts are sent to the CSP via the Nexusguard Notifier App in the event of attacks or traffic anomalies. Apart from signatures and behavioural-based attack detection, operators can configure specific conditions and thresholds that will generate alerts once triggered.

Mitigation Layers

Upon activation, mitigation profiles will be applied to incoming traffic to mitigate attacks. Mitigation can be set hierarchically, allowing network operators to cascade mitigation filters for large networks and yet maintain the flexibility to define specific profiles for up to individual IP addresses. Multiple mitigation templates can be created with its own policies to be applied quickly to each site, network or host IP.

A mitigation template contains six core mitigation rule-sets, i.e. Allow/block list, Bogons, Anti-Flood, FlexFilter, Zombie and Traffic Policing, that are activated by default upon detection of threats. In other words, these rules are automatically enforced when the threshold values (e.g. upper limits) defined by detection policies are reached.

To manage policies more effectively, they can be custom-defined at a Site level. You can also further customize policies at Network/Host levels to suit your specific needs.



Cloud Diversion Feature

Nexusguard's OP module offers a Cloud Diversion feature that automatically diverts the customer's traffic in a matter of minutes whenever it exceeds a pre-defined bandwidth, without requiring any on-premise appliance nor any intervention from the customer.

Types of Attacks Mitigated

Category	Attack Type	
Bandwidth / Network Depletion Attacks	Protocol Flood / Exploitation Attacks	TCP Flood UDP Flood ICMP Flood (Smurf, Ping Flood, Ping of Death, ICMP Echo) TCP SYN, SYN/ACK, RST, FIN Flood (Spoofed and Non-spoofed) IP Null Fragmentation (IP/UDP, IP/ICMP, IP/TCP, Teardrop) DNS Amplification Fraggle Nuke TCP Flag Abuse Zombie / Bots Attack

Solution Benefits

- Delivers comprehensive protection for the entire network
- Provides individual IP address protection for mission-critical online services
- Enables consistent uptime connections and high availability
- Enables effective security cost management through real-time network insights
- Offers superior end-user experience
- Manages risk through optimized mitigation
- Ensures the integrity of mission-critical applications
- Enhances end-user confidence and trust
- Offers network protection to customers not yet connected to CSP access service
- Reliable uptime is a customer expectation -- compromise is not an option