NEXUSGUARD®

DDoS Protection Made Simple

Network Protection

Inbound traffic during a DDoS attack can severely compromise a CSP's infrastructure or its upstream bandwidth, impacting both the availability and overall service quality of the CSP. Designed and built specifically to protect the local network infrastructure of partner CSPs, Nexusguard's Network Protection fends off the threat of attack traffic attempting to inundate the network by maximizing network availability, thereby reducing congestion caused by the attack.

How Does It Work?

Nexusguard Bastions service is purpose built to mitigate all forms of L3/4 attacks that aim to saturate the networks of partner CSPs. In the event that attacks threaten to saturate local capacities, scrubbing kicks in at the local Bastions PoP, instantly suppressing local attacks close to their source, while clean traffic is returned to the partner CSP's network via local routing through the on-premise Bastions servers.

Key Features

Safeguard against Volumetric Attacks

Protects partner CSP local infrastructure from the largest L3-L4 DDoS attacks.

Robust and Efficient Mitigation

Automatically removes only attack traffic while ensuring the flow of legitimate traffic is unimpeded.

Multi-layered Defence

Multi-layered detection engine to analyze traffic data and detect traffic anomalies.

Proven Proprietary Technologies

Leverages Nexusguard detection and mitigation technologies, e.g. Netshield to pinpoint and nullify malicious patterns.

Secure Clean Traffic Delivery

Following scrubbing, clean traffic is routed back to partner CSP networks via local routing through Nexusguard Bastions servers.

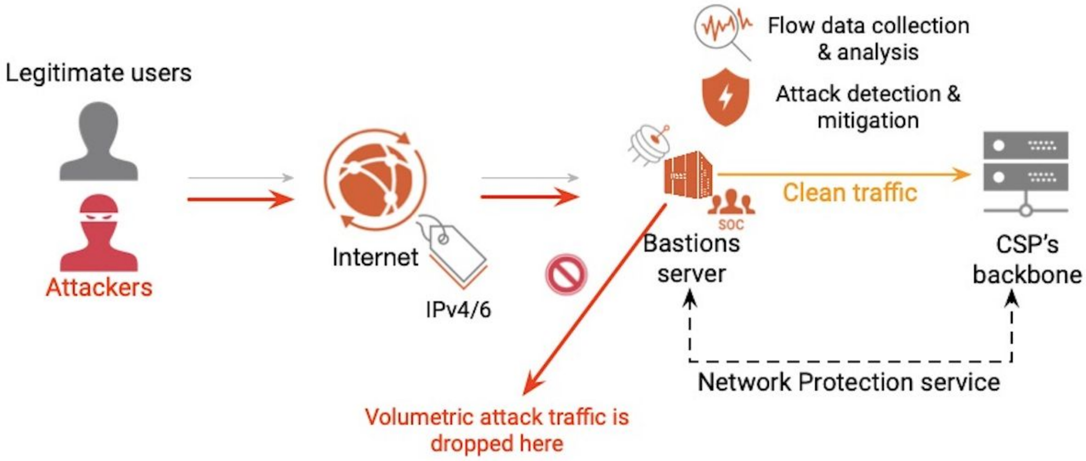
Legitimate users
Attackers
Internet
IPv4/6
Volumetric attack traffic is dropped here
Flow data collection & analysis
Attack detection & mitigation
SOC
Bastions server
Clean traffic
CSP's backbone
Network Protection service

Figure 1 - Nexusguard Network Protection

Flexible Attack Detection Modes

Nexusguard 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.

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. Effectively, 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.

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) Amplification

Solution Benefits

- Maximizes network availability and prevents congestion to CSP backbones due to volumetric attacks
- Ensures network quality is not degraded within CSP backbone
- Lowers operating costs by reducing the number of switchovers to cloud protection
- Provides protection for all registered IP prefixes
- Auto-mitigation offload supported by in-house Security Operations Centre (SOC)