NEXUSGUARD
DDoS Protection Made Simple

Edge Protection

Communications Services Providers (CSPs) offering on-premise DDoS protection either acquire or partner with cloud providers to put together a "hybrid" solution, but in reality they are two separate solutions sold as one product. This results in a disjointed user experience stemming from the service being delivered by two different teams, different dashboards and reporting mechanisms, and different escalation processes.

What is Edge Protection?

To address instances where large volumes of attack traffic congest the uplink Internet connection of partner CSPs, Nexusguard's Edge Protection service leverages Nexusguard's globally distributed scrubbing cloud to scale up protection of not only the partner CSP's infrastructure, but also the Bastions servers from being crippled by attacks that might overwhelm the CSP's capacity.

How Does It Work?

As soon as an attack threatens to saturate the local CSP scrubbing capacity, Nexusguard's Edge Protection is set in motion, tasked with protecting the uplink of partner CSPs. Scrubbing takes place at the Nexusguard scrubbing cloud, terminating attacks close to their source instantly, while clean traffic is returned to the destination network via a GRE tunnel through the local Bastions deployment.

Nexusguard's Edge Protection delivers a truly integrated and unified user experience, while providing an instantaneous increase in mitigation capacity to any Bastions deployment using the Nexusguard Cloud, scaling up protection instantly.

Key Features

Safeguard against Volumetric Attacks
Protects local network infrastructure and uplink Internet connection of partner CSPs from L3-L4 DDoS attacks.

Auto-Traffic Diversion
Leverages Nexusguard Cloud Diversion app to initiate traffic swing to global scrubbing centres when an attack exceeds the bandwidth allocated to handle DDoS attacks.

Surgical Mitigation
Automatically removes only malicious traffic while ensuring the flow of legitimate traffic is unimpeded.

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.

Secure Clean Traffic Delivery
After scrubbing, clean traffic is routed back to destination networks via GRE tunnels through the local Bastion servers.

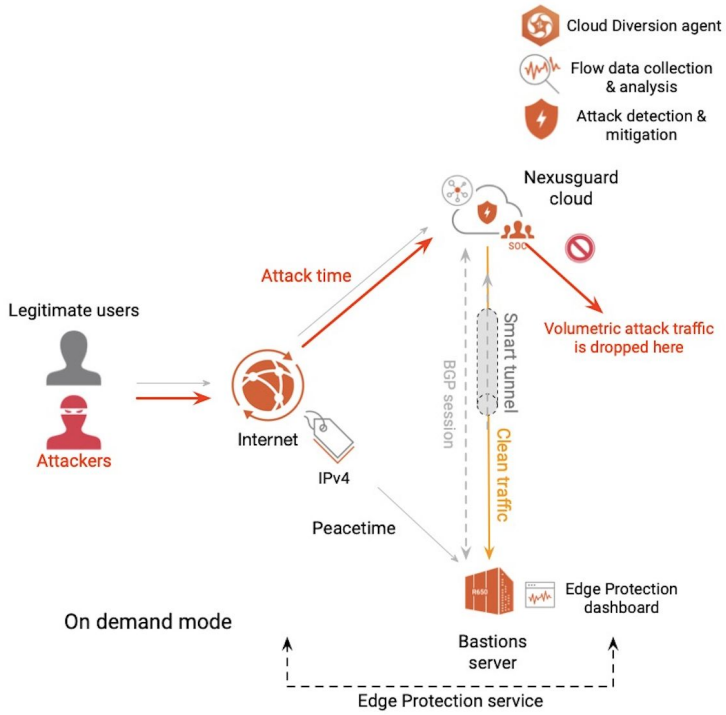

Figure 1 - Nexusguard Edge Protection

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.

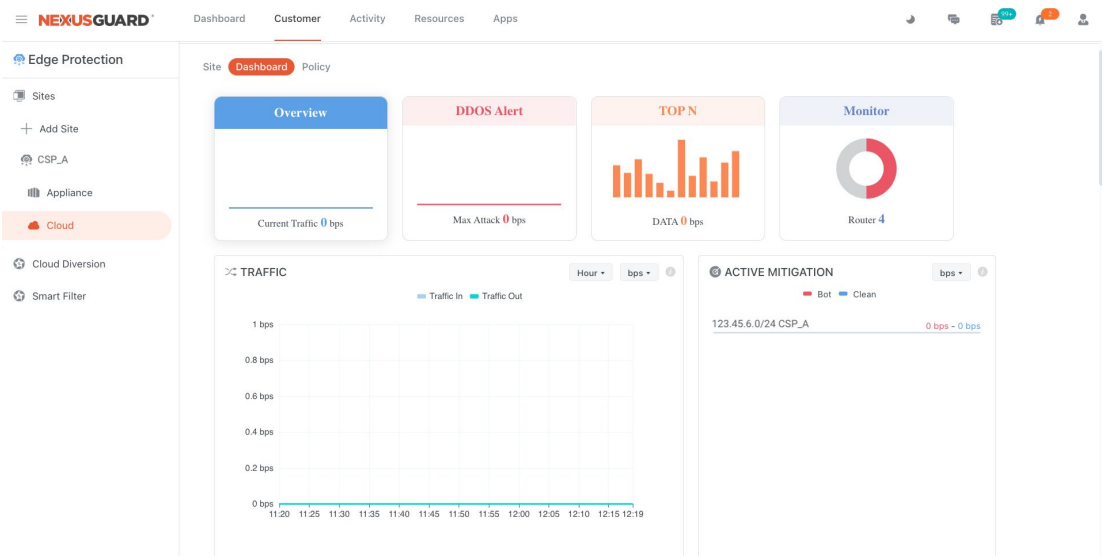

Figure 2 - Nexusguard Integrated Dashboard

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 or profile.

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 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

- Provides an immediate increase in mitigation capacity to Bastions PoP from Nexusguard Cloud
- Reduces demand for large mitigation bandwidth from CSPs
- Implements Cloud Diversion App to facilitate and automate traffic diversion
- Diverts attack risk to Cloud
- Edge Protection portal improves transparency of attack event status