NEXUSGUARD®

DDoS Protection Made Simple

Origin Protection

Comprehensive Anti-DDoS Solution for Large-Scale Networks

Features

- Fully managed DDoS protection solution for your network infrastructure.
- Continuous development by Nexusguard against latest threats.
- Real-time mitigation with customized Dashboard, view real-time traffic & attack events with periodic reports.
- High-availability service with more than ten mitigation POPs.
- Real-time alerts via the web portal and/or email notifications.
- Real-time 24x7x365 monitoring from our ISO27001 and PCI DSS Certified SOC.
- Ability to perform mitigation manually or automatically.

Benefits

- Protect Internet uplink bandwidth by diverting the under attack IP prefixes to Nexusguard Cloud for mitigation.
- Focus on your core business & leave DDoS mitigation to the experts.
- Protects your network infrastructures and devices from Layer 3/4 (volumetric) DDoS attacks.
- SLA commitments with monthly performance review reports.
- Avoid negative publicity & customer churn.
- Attain regulatory compliance & avoid monetary penalties.

Origin Protection Portal

Overview
An aggregation of key metrics related to the selected site is displayed in intuitive graphs and reports, allowing for quick corrective action.

Active Mitigation
Contains a list of ongoing events on IP addresses grouped by networks or hosts currently managed by the mitigation platform.

It also indicates the bandwidth consumed by clean traffic and attacker traffic. The most recent events are displayed first.

DDoS Alerts
Recent DDoS alerts are listed, with ongoing events shown first. Each event includes the following attributes:

- Unique identifier (ID) of the alert event.
- IP address of the attack target.
- Profile of the networks and hosts under protection.
- Event severity, categorized as high, medium, or low.
- Start and end time (for past alerts) of the alert.
- Event impact, measured by the size of the attack.

Flexible Attack Detection Modes

Our service has three modes for DDoS attack detection and mitigation:

Normal Mode

The attack alert is triggered when traffic continuously exceeds predefined detection thresholds for 3 minutes. This mode is suitable for detecting the continuous flow of attack traffic.

Rapid Mode

The attack alert is triggered within a few seconds when the volume of traffic exceeds the product of the high-level detection threshold. In this mode, alerts are generated more quickly but the false positive rate rises.

Smart Mode

Attack alerts are automatically generated once the traffic matches any of the patterns learned by the system. This mode uses multiple characteristics of traffic for attack detection, including type and protocol characteristics of the traffic.

Attacks that can be mitigated

Modo normal

- ACK Attack or ACK-PUSH Flood
- DNS Amplified (Reflective)
- DNS Flood
- Fake Session Attack
- Fraggle Attack
- Fragmented ACK Flood
- ICMP Flood
- ICMP Fragmentation Flood
- IP NULL
- Memcached Attack
- Non-Spoofed UDP Flood
- NTP Amplified (Reflective)
- Carpet Bombing Attack
- Zero Day Attack 1

L3/4 Volumetric Protection

- NTP Flood
- Ping Flood
- RST/FIN Flood
- Same Source/Dest Flood (LAND Attack)
- Smurf Attack
- SSDP Amplified (Reflective)
- SYN Flood
- SYN-ACK Flood 2
- TCP Null
- TOS Flood
- UDP Flood
- UDP Fragmentation

Some level of application protection when inspecting inbound traffic without decryption

- TCP Connection Flood
- HTTP Flood
- HTTP Slow Attack
- SSL/TLS Malformed
- SSL/TLS Renegotiation
- SSL/TLS Session (Per Source IP)
- SIP Malformed
- SIP Spoofing
- SIP REGISTER Request Flooding
- SIP INVITE Request Flooding
- Source Half Open Connection
- Source IP Idle Connection
- Slow Rate Connection

DDoS Detection & Alerts

Remote DDoS Monitoring

Auto Detection & Mitigation

Managed SOC

Network Baseline App

Flow Spec App

Smart Filter App

Cloud Diversion App

20250318

NEXUSGUARD®

www.nexusguard.com