NEXUSGUARD

DDoS Protection Made Simple

Application Protection

What is Application Protection?

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

Any organization that delivers content or applications over the Internet can and should use cloud-based DDoS protection to keep their business online during an attack with minimal impact to users. Engineered to respond to the surge and increasing sophistication of DDoS attacks, the AP platform offers multi-layered L3–L7 protection against attacks on public-facing websites, applications, APIs, and so forth.

Strategically placed in the world's major internet traffic hubs and peering with major Internet exchange points (IXPs), Nexusguard's scrubbing centers are equipped with industry-leading and proprietary technologies to detect, identify and mitigate threats in real time and return clean traffic to the client server. The platform can run continuously to monitor all traffic and stop attacks from ever reaching your network.

How Does It Work?

A multi-layered mitigation mechanism, including Nexusguard's proprietary technologies, is used to analyze, identify and mitigate attacks effectively and responsively. Since it is a pure-cloud solution, there are no upfront costs or ongoing maintenance and upgrade costs for hardware. Multi-layered protection is based on two methods of protection: signature-based detection complemented by statistical behaviour analysis.

Key Features

Always-On DDoS Protection
Safeguards against the largest application/ volumetric DDoS attacks to websites or TCP applications using leading-edge DDoS attack mitigation techniques

Always-On WAF Protection
Protects web applications, mobile apps, and application program interface (API) apps against the OWASP Top 10 threats

Proxy Connectivity
Supports applications running TCP such as HTTP/HTTPS and TCP applications on IPv4 or IPv6, and TLS to ensure secure HTTPS sessions

Wide Range of Protocols
Supports HTTP/HTTPS, TLS v1.3/1.2/1.1/1.0, L3-L4 protection for other TCP protocols, Proxy protocol/ TOA

Load Balancing
Provides algorithms to fulfill customer requested policies such as Active/Standby group, weighted load balancing and Source IP hashing to maintain stickiness

Performance Optimization
Caching improves download speed and reduces loading on the original web server. Geolocation optimization distributes traffic to the nearest scrubbing centre to optimize network latency and improve user experience

Detection Mode

To efficiently detect DDoS attacks, Nexusguard's AP deploys one its flexible attack detection modes that is best suited for continuous flows of attack traffic. It works by monitoring traffic flow from customer networks to give advance warning of an attack, and then triggering the corresponding mitigation action needed when the traffic exceeds a predefined detection threshold for a specified time frame.

Smart Route Policy

Offered as a value-added option with AP, Nexusguard Smart Route Policy is an advanced geolocation routing method, designed and built to customize and optimize the experience of website users from across multiple regions across the globe. This is achieved by mapping and distributing website users' geolocation to pre-assigned Nexusguard scrubbing centres to deliver optimal network latency, increased reliability and continuous availability.

Specifically designed to handle large attacks, the built-in Warzone feature is a dedicated VIP pool in which the attack is redirected to, and used to isolate the under attack website from other websites, so as to allow Security Operations Centre (SOC) teams to continue handling and mitigating that attack effectively without causing any impact to other customers.

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 that an attack exceeds predefined threshold values defined in the mitigation policy. Apart from signatures and behavioral-based attack detection, operators can configure specific conditions and thresholds that will generate alerts once triggered.

Mitigation Layers

Available to the Security Operations Centre (SOC) when handling DDoS attacks, the filtering structure for the mitigation process is composed of a comprehensive suite of mitigation tools, as follows:

Bogons refers to the address space outside the allowed range for public Internet use. This area of address space includes reserved private address and link-local address ranges. Nexusguard's Mitigation Platform drops private or reserved IP address ranges.

Anti-flooding is composed of a set of rules designed to defend against flood attacks. Flood attacks are a form of DoS attack in which the attackers send a large number of requests to a target system to consume enough resources to make the system unable to respond to legitimate requests.

Flex Filter is a combination of parameters which defines the mitigation policies that fulfills the customer's traffic pattern and security needs. FlexFilter goes one step beyond custom filters in Anti-Flood policies by offering more metrics and data visualization in one place.

Zombie is a computer that has been compromised by a hacker, computer virus or trojan horse. It is very often used by attackers to launch DDoS attacks. Nexusguard's Mitigation Platform rate limits the zombie host from sending traffic

Traffic Policing limits the traffic by defining a threshold after mitigation, before sending it to another system or network for further processing. It can be used as a safeguard to prevent tunnel congestion and disruption to other networks using the same tunnel.

Blackholing a.k.a. null route, is a network route that drops all traffic to the victim IP. On the Nexusguard Mitigation Platform, when bandwidth usage exceeds the predefined threshold value, all traffic to the target is blackholed.

Allow or Deny IP Addresses is one of the core policies Nexusguard's Mitigation Platform enforces. It allows trusted IPs and blocks known attacks or unauthorized sources.

HTTP Filter Policy allows redirection/ blocking of certain HTTP requests matching the defined conditions.

HTTP Compliance Policy specifies the HTTP protocol version to follow.

IP Authentication ensures suspicious requests made by an original IP undergo Nexusguard's IP authentication engine, which is based on tracing and tracking the IP behavior of the requester. It extends the existing 7-tier DDOS protection application scenarios and improves the experience of its unfriendly protection objects, such as API calls, 302 jumps, and so on.

HTTP Authentication ensures suspicious requests undergo Nexusguard's HTTP authentication engine, structured in a three-layered filtering system. The level of authentication test can be selected, i.e. low, medium or high or the whole authentication process can be fully automated.

Deployment

Deployed as the proxy on behalf of the client server, Nexusguard provides Anycast virtual IP (VIP) addresses that can be published via DNS forwarding to direct all inbound raw traffic to our scrubbing network and return only clean traffic to the client server. In doing this, there is no need to make changes to your infrastructure.

Proxy mode supports any application running TCP such as HTTP, HTTPS and more on either IPv4 or IPv6. It is especially useful for those preferring minimum network changes and do not control a full Class C network, or those who simply need protection on individual applications.

These Anycast VIPs are part of the Nexusguard ASN and are routed "always on" through the Nexusguard scrubbing network. Once traffic reaches our network, Network Address Translation is applied and the protected IP is forwarded for end user traffic. Clean traffic will then be routed back to the client's origin.

Technical Features

- Patented Crawler Detection Technology blocks malicious crawlers, spammers, hackers, and bad bots and even those using forged IP addresses before they can do damage, steal site content or login information, and launch DDoS attacks on customer websites.

- SSL Attack Mitigation protects against SSL-based attacks. SSL decryption and challenge-response mechanisms are enforced only on suspicious traffic. Nexusguard SSL certification management follows the PCI Data Security Standard and ISO 27001 to ensure the highest security standards.

- Content & Network Optimization compresses and caches all traffic going through the cloud, effectively speeding up the delivery of high-traffic websites and online service access for users worldwide. Load-sharing traffic services support multiple backend configurations. Automatic backend failover is also implemented in the event of a backend server failure.

- Progressive C/R Algorithms defends the application layer against all abuses and attacks. Nexusguard's proprietary C/R protocol employs non-intrusive authentication challenges depending on user behavior and delivers a non-disruptive browsing experience and zero false-positive mitigation errors.

- Web Application Firewall (WAF) employs blocklist rules to address known security risks, especially OWASP Top 10 Most Critical Web Application Security Risks. Clients can also define site-specific rule sets on the Customer Portal. Moreover, the WAF implements Secure Headers to bolster web application security by adding an extra layer of security, as well as CSRF tokens to validate that HTTP referrers are from a trusted domain.

Solution Benefits

- Enables consistent uptime connections and high availability
- Delivers "Always On" reliability
- Manages risk through optimized mitigation
- Keeps public-facing websites and applications online during DDoS attacks
- Stops DDoS attacks before they reach your network and affect your business
- Comprehensive protection, including support for OWASP top 10 - 2017 web security risks, zero-day exploits, and more
- Comprehensive attack traffic and mitigation visibility, reports and event logs via the Portal
- Fast content and application delivery
- Non-intrusive, progressive C/R authentication keeps user experience intact
- SSL attack mitigation while retaining private key
- Reliable uptime is a customer expectation - compromise is not an option