Nexusguard — Comprehensive DDoS Protection & Network Security

Introduction & Need for Nexusguard

Nexusguard is a specialized cybersecurity provider focused on Distributed Denial-of-Service (DDoS) mitigation, traffic scrubbing, and network resilience services. Organizations — including enterprises, cloud providers, ISPs, and critical infrastructure operators — need Nexusguard-style services to defend against large-scale, multi-vector attacks that can cause downtime, data loss, and reputational damage. Modern threat campaigns often use techniques like 'carpet bombing' (broad simultaneous attacks across many targets) and multi-vector reflection/amplification; defending requires global scrubbing capacity, tight integration with routing (BGP), and layered protections at both application and network layers.

Document Scope

This document covers four protection phases: Application Protection, Origin Protection, Clean Pipe (ISP model), and DNS Protection. It also explains OSI-layer mapping, DNS amplification attacks, BGP fundamentals, and operational recommendations.

1. Application Protection

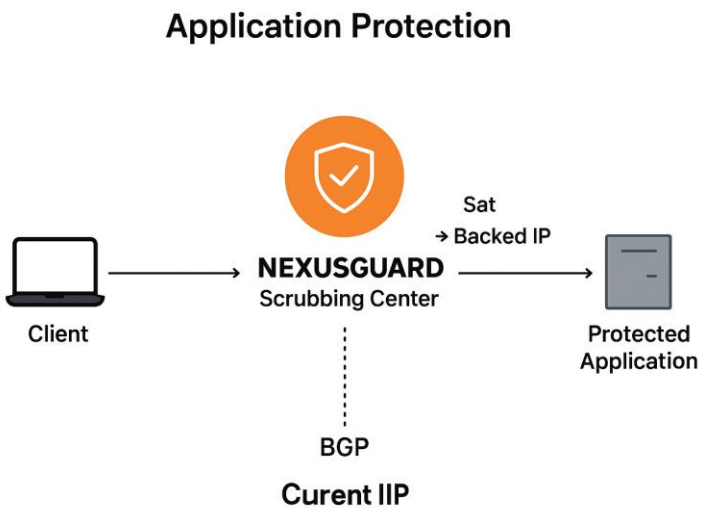
Application Protection focuses on Layer 7 (L7) threats — HTTP floods, slow attacks, application logic abuse, and API-targeted attacks. Key operational concepts include symmetric routing, client VIPs (Virtual IPs), Session Affinity (SAT), and backend origin IP shielding.

- Symmetric routing: inbound and outbound packets follow the same path to preserve session state (necessary for stateful inspection).

- Client VIP: Nexusguard fronts a public VIP to receive client requests; VIP terminates at scrubbing front-ends.

- SAT (Session Affinity / Advanced Traffic Steering): binds client sessions to mitigation nodes to avoid session drops.

- Backend/Origin IP protection: origin IPs are hidden or reachable only via tunnels or ACLs to prevent direct attacks.

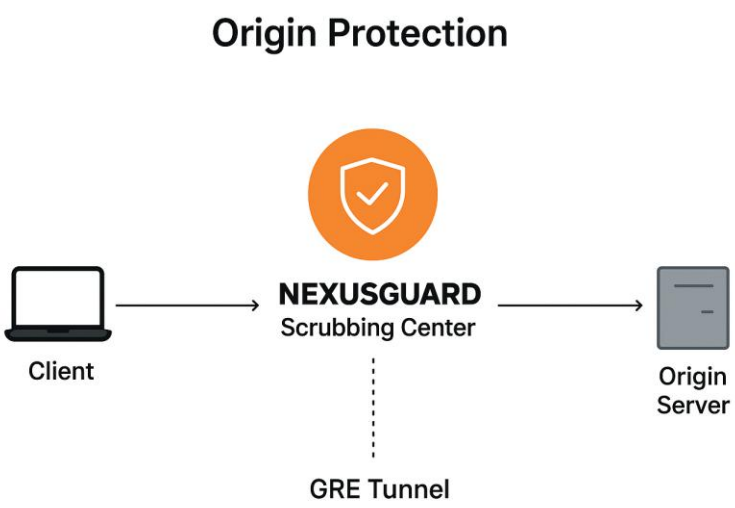


2. Origin Protection

Origin Protection shields the true server IPs from direct internet access. Common deployment methods are GRE tunnels and dedicated circuits.

- GRE Tunnel: Customer tunnels traffic to Nexusguard; scrubbing occurs then packets are decapsulated and forwarded to origin.

- Direct Circuit: Private cross-connect (MPLS, VPLS, or dark-fiber) between customer and Nexusguard for high-throughput, low-latency mitigation.



3. Clean Pipe (ISP model)

Clean Pipe is used by ISPs to prevent attack traffic from saturating transit and peering links. Traffic is steered to Nexusguard for scrubbing, then clean traffic is re-inserted into the ISP network.

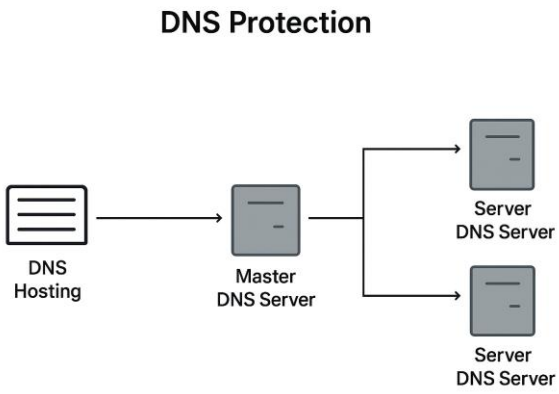
- Bastion Server: management/jump host for hybrid deployments and peering control.

Typical flow: client → ISP → Nexusguard (scrub) → ISP → client.

4. DNS Protection

DNS Protection secures authoritative name servers and DNS hosting services against query floods and amplification attacks. Key practices:

- Anycast DNS edges to distribute query load and localize failures.
- Master (primary) and Slave (secondary) authoritative servers for redundancy.
- Rate limiting (RRL), tight ACLs, and scrubbing at DNS edge nodes.



OSI Layers & Attack Mapping

OSI Layer	Attack Examples	Nexusguard Mitigation
L7 - Application	HTTP floods, slow POST, API abuse	WAF, behavioral, rate-limit, SAT
L4 - Transport	SYN floods, UDP floods	Stateful proxies, SYN cookies, rate-limit
L3 - Network	ICMP floods, fragmentation attacks	Network scrubbing, ACLs, blackholing
L2 - Data Link	ARP spoofing (local)	Local switch controls, not provider primary
L1 - Physical	Fiber cut, port failure	POP redundancy, multi-path transit

DNS Amplification Attacks

DNS amplification uses spoofed source IPs in DNS queries to direct large responses at a victim. The attacker sends small queries that produce much larger responses (amplification factor), often via open resolvers or misconfigured authoritative servers.

Mitigations include disabling open recursion, implementing Response Rate Limiting (RRL), Anycast distribution, and scrubbing at scale.

BGP — The GPS of the Internet

Border Gateway Protocol (BGP) is the inter-domain routing protocol used to exchange route reachability between Autonomous Systems (AS). Because BGP controls how prefixes are announced and reached, it is central to traffic diversion and scrubbing strategies in DDoS mitigation.

Core BGP concepts:

- BGP Table: stores multiple route options to prefixes learned from peers.

- Message types: OPEN, UPDATE, NOTIFICATION, KEEPALIVE.

- FSM States: Idle, Connect, Active, OpenSent, OpenConfirm, Established.

- Common attributes: NEXT_HOP, AS_PATH, LOCAL_PREF, MED, COMMUNITY; used to influence path selection.

BGP Table Example

Prefix	Next Hop	AS_PATH	Local_Pref	Origin
203.0.113.0/24	198.51.100.1	64512 64513	100	IGP
198.51.100.0/24	198.51.100.2	64514	200	EGP

BGP Message Types & Purpose

Message Type	Purpose
OPEN	Establish session and negotiate parameters
UPDATE	Advertise or withdraw routes
NOTIFICATION	Report error and close session
KEEPALIVE	Maintain session liveness

Carpet Bombing Attacks

Carpet bombing refers to large-scale campaigns that spread attack traffic across many IP ranges, ports, and vectors simultaneously. The goal is to overwhelm defensive capacity, complicate attribution, and force defenders to spread mitigation thinly. Defenders need global scrubbing capacity, cross-POP coordination, and rapid BGP/traffic steering playbooks.

Integration & Operational Recommendations

Integrate Nexusguard telemetry (attack summaries, timestamps, vectors, peak PPS/Bandwidth, and BGP reroute events) into SIEM (Splunk, QRadar) and SOAR for automated playbooks. Maintain BGP community tags and route telemetry for faster incident response.

Conclusion:

Nexusguard stands as a comprehensive and resilient DDoS mitigation and network protection platform, designed to safeguard applications, infrastructure, and DNS services across all layers of the OSI model. Its four-phase protection architecture, ensures seamless defense mechanisms that maintain service availability and data integrity even under large-scale, complex attacks such as carpet bombing and DNS amplification. By leveraging advanced technologies like symmetric routing, GRE tunnels, and BGP-based traffic redirection, Nexusguard effectively scrubs malicious traffic before it reaches the origin, offering both enterprises and ISPs unparalleled reliability. With its intelligent routing and mitigation framework, Nexusguard not only protects the digital ecosystem but also reinforces the stability and trust that global internet operations depend upon.

Appendix & References

RFC 4271 (BGP-4), Best practices for DNS RRL, Nexusguard product documentation and whitepapers.