NEXUSGUARD®
Global Leader in DDoS Mitigation

Origin Protection

What is Origin Protection?

The Nexusguard Cybersecurity Platform encompasses three essential elements: Application Protection, Origin Protection, and DNS Protection.

Nexusguard Origin Protection Service guards against threats that target network resources. The service is especially beneficial for organizations that can't afford any downtime of network assets. The service complements Nexusguard's Application Protection Service by safeguarding the backend infrastructure from all DDoS threats, and covers all network components: internal websites, email servers, FTP servers, and other applications, against volumetric and protocol-based DDoS attacks, such as SYN floods, fragmented packets attacks, Ping death, Smurf DDoS, and more.

How Does It Work?

Using BGP announcements, all incoming traffic is routed through Nexusguard scrubbing centers, collectively equipped with over 2.24Tbps of mitigation capacity. Only clean traffic is routed through a secure Generic Routing Encapsulation (GRE) tunnel back to our customers' servers. Nexusguard advertises all protected IP range announcements on your behalf.

Mitigation Layers

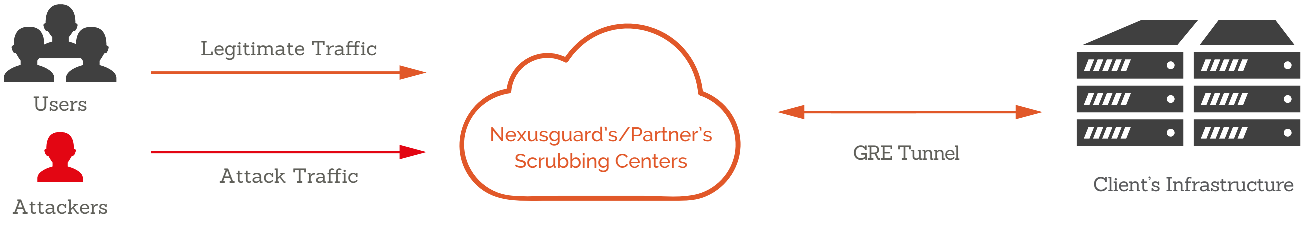
- Direct Circuit is achieved by establishing a direct physical connection between Nexusguard scrubbing centers and the customer network — if it is in close proximity. "Always-on" mode allows for the highest level of protection with a dedicated connection for optimal reliability and security.

- BGP Routing offers comprehensive protection of the entire network. Inbound traffic is routed to our worldwide scrubbing centers. After scrubbing, clean traffic is then routed back to your network via a GRE tunnel. Nexusguard's routing solution is highly scalable for enterprises with sizeable network deployments.

- Two-way GRE Tunnel enables smaller organizations to protect multiple service types and protocols, even for a single IP address, without using BGP routing (ideal for clients without an entire Class C subnet).

Customers receive a "protected IP address," which inspects and filters all incoming traffic. A redundant and secure two-way GRE tunnel is used to forward clean traffic to the origin IP and return outbound traffic from applications to users. Once in place, the tunnel is used to route clean traffic from our network to your origin server, and vice versa. You can then broadcast the assigned IP addresses to your users via DNS, making these your nominal "origin" addresses. All traffic that flows through Nexusguard's network is inspected by our global scrubbing centers.

Individual IP address protection is ideal for services with high-traffic, critical non-HTTP assets with low IP counts, as well as cloud deployments looking for direct-to-IP attack prevention. Clients relying on a small number of IP addresses or even a single IP address to deliver high-traffic, non-HTTP services, and clients using cloud services over the public Internet via a dedicated IP address, will find Nexusguard Origin Protection service exceptionally cost effective and valuable.



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)
		TCP SYN, SYN/ACK, RST, FIN Flood (Spoofed and Non-spoofed)
		IP Null
		Fragmentation (IP/UDP, IP/ICMP, IP/TCP, Teardrop)
		DNS Amplification
		Fraggle
		Nuke
		TCP Flag Abuse
		Zombie / Bots Attack
Others		Malicious Headers
		Malicious Payloads
		Pucodex
		Zero Day Exploits

Solution Benefits

- Delivers comprehensive protection for the entire network
- Provides individual IP address protection for mission-critical online services
- Enables consistent uptime connections and high availability
- Delivers “Always On” reliability
- Enables effective security cost management through real-time network insights
- Offers a superior end-user experience
- Manages risk through optimized mitigation
- Ensures the integrity of mission-critical applications
- Enhances end-user confidence and trust
- Reliable uptime is a customer expectation — compromise is not an option

Visibility & Control

On the Customer Portal, you can view the distribution of incoming raw traffic that flows through the network segment as well as clean traffic routed to yours network after scrubbing. You can also view the distribution of raw traffic by geographic location (per scrubbing center) on a real-time, global traffic map. “Top Talkers” provides a quick glance at the IPs that are using the most network bandwidth within a given period of time.

24/7/365 SOC & Technical Support

Nexusguard has Security Operations Centers (SOCs) in Asia and the Americas staffed with security experts to monitor and respond to attacks and threats around the clock, while also providing responsive support. Each SOC provides the best DDoS protection at all times, with local language support.