

Clean Pipe

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

Internet Clean Pipe is an essential DDoS mitigation solution usually delivered both for on-line businesses and mission critical websites that require real-time protection against DDoS attacks. It is most commonly delivered as a value-add on top of existing or new connectivity offerings such as Direct Internet Access Services.

Nexusguard's Clean Pipe (CP) module is designed for Communications Service Providers (CSPs) to immediately expand or strengthen their existing product offerings, by providing optimum attack detection, notification and mitigation response times to deliver a truly differentiated clean pipe service. The local scrubbing facility is deployed on-premise via a local server when traffic exceeds the capacity of on-premise infrastructure, with offload to Nexusguard's global scrubbing network available as an option in our OP module.

How Does It Work?

The defence mechanism effectively protects against large L3-L4 DDoS attacks, which attempt to flood the core and downstream networks. Behind the mechanism is a comprehensive mitigation platform that inspects traffic, detects threats and blocks attacks against protected network resources, in real-time.

Key Features

Safeguard against Volumetric Attacks

Protects CSPs and downstream customers from the largest L3-L4 DDoS attacks using best-in-class DDoS attack mitigation techniques

Surgical Mitigation

Automatically removes only attack traffic while ensuring the flow of legitimate traffic is uninterrupted

Clean Pipe As-A-Service

Ability to deliver Clean Pipe as-a-service to CSP downstream customers

Flow Data Analysis Capability

Multi-layered detection and mitigation 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

Clean Traffic Delivery

Zero latency as mitigation is performed locally within the CSP's local scrubbing centre.

Flexible Detection Modes

Nexusguard's CP module offers three modes of detection, namely Normal, Rapid and Smart for L3-L4 DDoS attack types.

- **Normal Mode** suitable for continuous flows of attack traffic, monitors traffic flow from customer networks to give advance warning of an attack, and triggers the corresponding mitigation action needed when the traffic exceeds a predefined detection threshold for a certain time frame, aka. LSP (latency start period which is usually 120 seconds).
- **Rapid Mode** suitable for continuous flows of attack traffic, bursty traffic and hit-and-run attacks, monitors traffic flow from customer networks to forewarn of an attack, and triggers the corresponding mitigation action needed when the traffic exceeds the product of the predefined detection threshold and 60 seconds.
- **Smart Mode** suitable for dynamic traffic profiles, is based on a revolutionary AI-based 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.

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 the predefined threshold value defined in the mitigation policy.

Mitigation Layers

The defence mechanism has an intelligent, built-in filtering system to identify and mitigate attacks while keeping the user experience intact. The CSP's local scrubbing facility will work in tandem with Nexusguard's global scrubbing centres to mitigate attacks globally. The filtering structure for the mitigation process is composed of the following:

- Blacklisting / Whitelisting
- Bogons
- Anti-flooding
- Flexfilter
- Zombie
- Traffic policing

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/ICMP, IP/TCP, Teardrop)
	DNS Amplification
	Fraggle
	Nuke
	TCP Flag Abuse
	Zombie / Bots Attack

Enhanced Service Coverage for CSP Downstream Customers

Nexusguard's Clean Pipe not only provides improved bandwidth management, but also protects the connectivity and service of existing customer networks from the threat of evolving DDoS attacks, ensuring that first-rate network quality is always maintained for existing CSP downstream customers.

Solution Benefits

- Real-time network protection against DDoS attacks
- Provides individual IP address protection for mission-critical online services
- Consistent uptime connections and high, 24/7 availability
- Enables effective security cost management through real-time network insights
- Offers superior end-user experience
- Manages risk through optimized mitigation