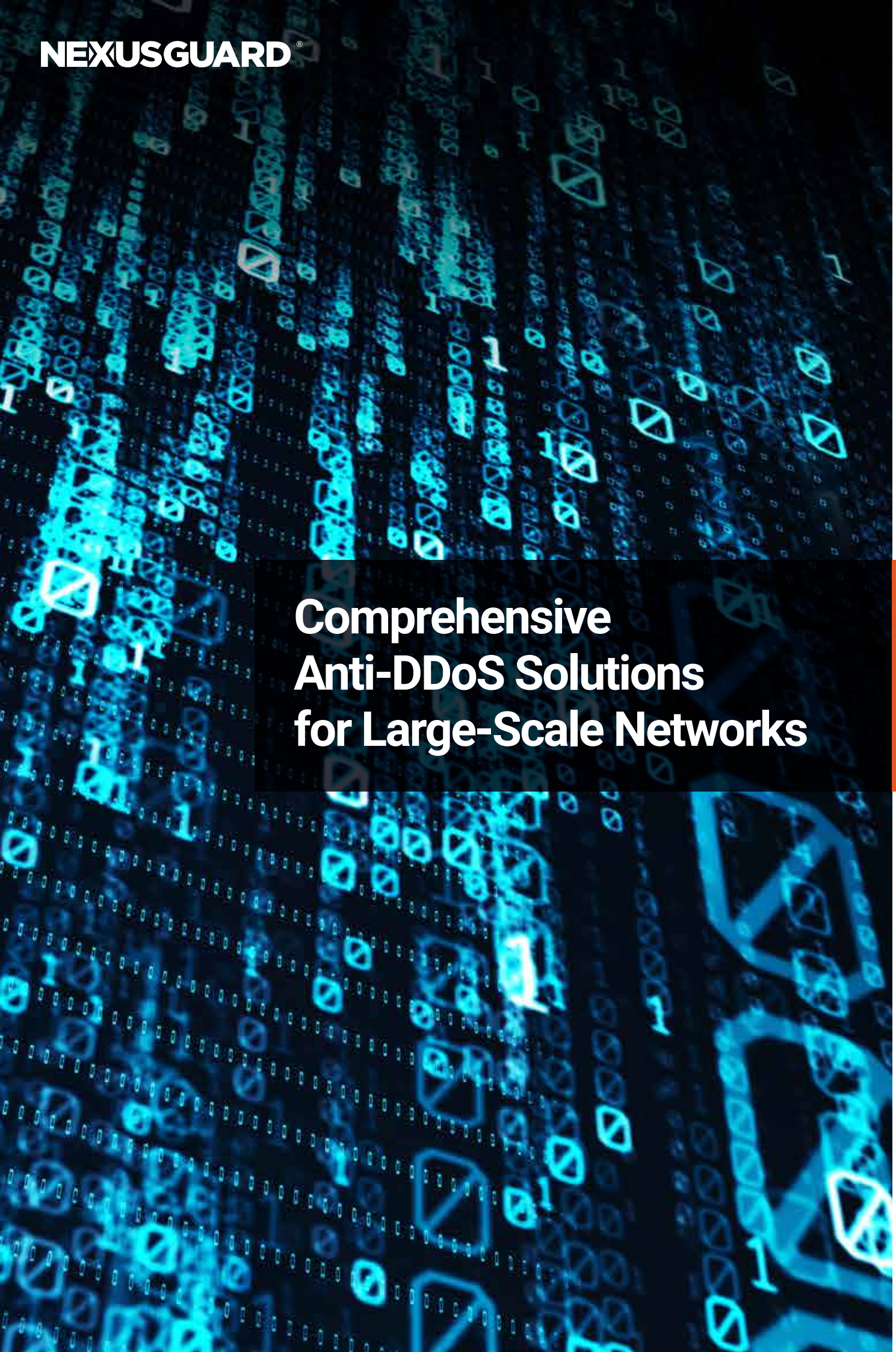
NEXUSGUARD®



Comprehensive Anti-DDoS Solutions for Large-Scale Networks

WHITE PAPER

Abstract

The ever-increasing prevalence and complexity of Distributed Denial of Service (DDoS) attacks have significantly transformed the security landscape, necessitating organizations to adapt their defense strategies. This white paper explores purpose-built anti-DDoS solutions that can effectively protect against a broad range of DDoS attacks, enabling uninterrupted operation for organizations. We delve into the comprehensive features and capabilities offered by Nexusguard's Origin Protection service, tailored to meet the requirements of large-scale environments managing extensive networks. Supported by a dedicated Security Operations Center (SOC) and leading-edge technologies, Nexusguard's anti-DDoS solutions empower organizations to proactively combat evolving threats and safeguard their digital assets.

Introduction

Background on DDoS Attacks

In today's interconnected world, the threat of DDoS attacks looms large, posing significant risks to network infrastructure and web applications. These attacks can disrupt the availability, performance, and security of critical systems, causing extensive damage to businesses and organizations. The increasing prevalence and sophistication of these attacks have transformed the security landscape, making it imperative for organizations to adapt their defense strategies.

Importance of Robust DDoS Protection

As the scale and complexity of DDoS attacks continue to grow, traditional security measures are often insufficient to protect against these threats. Large-scale environments managing hundreds of Class C networks are particularly vulnerable, as they require solutions that can scale and adapt to evolving attack patterns. Effective DDoS protection must be able to mitigate a wide range of attacks, from volumetric floods to sophisticated application-layer exploits, ensuring the uninterrupted operation of mission-critical services.

Overview of Nexusguard’s Origin Protection Service

Nexusguard's Origin Protection service is an advanced, purpose-built solution designed to provide unparalleled protection for mission-critical services across expansive networks. Specially crafted to cater to the unique demands of large-scale environments, Origin Protection stands as a formidable defense, protecting subnets at Layers 3 and 4.

Leveraging a highly scalable, fully redundant, and globally distributed scrubbing network, Nexusguard's Origin Protection service mitigates the largest and most sophisticated DDoS attacks. Supported by a dedicated Security Operations Center (SOC) and cutting-edge technologies, Nexusguard empowers organizations to proactively combat evolving threats and safeguard their digital assets.

The Problem: Understanding DDoS Attacks

Layer 3/4 Attacks

Layer 3/4 attacks target the network infrastructure itself, disrupting services by overwhelming the network with a flood of traffic. There are two main types of attacks within this category: flooding attacks and amplification attacks. Flooding attacks involve overwhelming the network with an excessive amount of traffic, leading to internet link saturation, severe packet loss, and increased round trip latency. Amplification attacks, on the other hand, exploit vulnerabilities to amplify the volume of attack traffic, causing similar detrimental effects on the network.

Examples of Layer 3/4 attacks include:

- **TCP SYN flood**: Overwhelms a server by sending a large number of SYN requests, consuming server resources and rendering it unresponsive.
- **PUSH/ACK flood**: Targets the server with PUSH and ACK packets, causing resource exhaustion.
- **Invalid TCP options/flag combinations**: Exploits vulnerabilities in TCP implementations to disrupt services.

Layer 7 Attacks

Layer 7 attacks target the application layer, exploiting vulnerabilities in web applications to compromise their functionality and security. These attacks aim to exhaust server resources or manipulate application inputs to execute malicious code or gain unauthorized access to sensitive data.

Examples of Layer 7 attacks include:

- **Slowloris**: Keeps multiple connections open for as long as possible, exhausting server resources.
- **Cross-site scripting (XSS)**: Manipulates web application inputs to execute malicious scripts in the user's browser.
- **SQL injection**: Exploits vulnerabilities in web application input fields to execute arbitrary SQL code, potentially gaining unauthorized access to sensitive data.

The Solution: Nexusguard's Origin Protection

Description of Nexusguard Origin Protection Service

Nexusguard Origin Protection is an advanced and purpose-built service that provides unparalleled protection for mission-critical services across expansive networks. Specially crafted to cater to the unique demands of large-scale environments managing hundreds of Class C networks, Origin Protection stands as a formidable defense, protecting subnets at Layers 3 and 4, leveraging our highly scalable, fully redundant and globally distributed scrubbing network to mitigate the largest and most sophisticated DDoS attacks.

Figure 1 - Nexusguard Origin Protection

When a malicious attack is detected, the Border Gateway Protocol (BGP) route associated with the targeted /24 IP prefix is announced to the Internet via Nexusguard. Consequently, the traffic is automatically redirected to Nexusguard's globally distributed scrubbing centers for thorough cleansing. Once the malicious traffic has been effectively dropped at these scrubbing centers, the clean and legitimate traffic is securely returned to the customers' networks through Generic Routing Encapsulation (GRE) tunnels.

The process of traffic diversion can be initiated either manually or automatically. Manual triggering allows operators to take control and initiate the diversion process when necessary. Alternatively, our proprietary Cloud Diversion App provides an automated approach, eliminating the need for any on-premise equipment. This App seamlessly and autonomously diverts traffic to ensure swift and effective attack mitigation without any disruptions to the customers' networks.

Nexusguard Attack Management Framework

Nexusguard's attack handling process operates as a perpetual loop, designed to effectively address and mitigate the ever-evolving nature of attacks. When an attack is detected, the flow initiates with the raising of an attack alert, triggering a series of subsequent actions, including traffic diversion, mitigation measures, and the ultimate delivery of clean traffic back to the client's infrastructure.

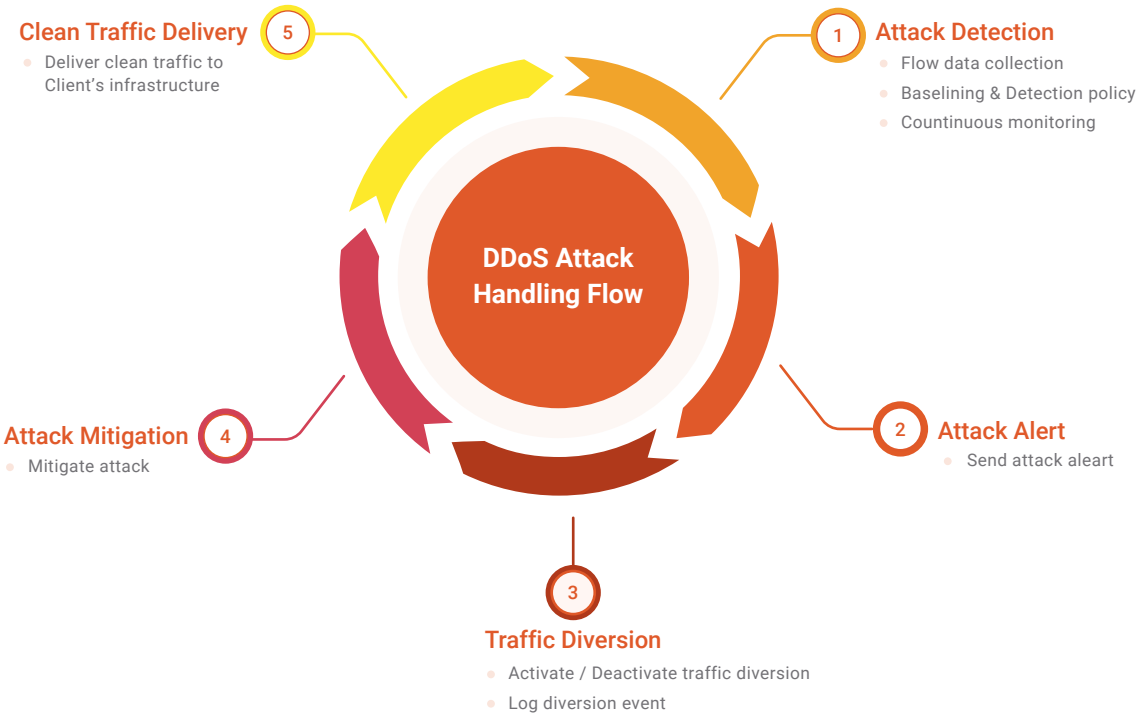


Figure 2 - Nexusguard DDoS Attack Handling Flow

It is important to recognize that attacks are dynamic in nature, constantly changing and adapting. Attackers possess the capability to launch multi-vector attacks, simultaneously targeting multiple vulnerabilities. Moreover, they can swiftly shift their focus to attacking both Applications and DNS infrastructure concurrently, among other tactics. In light of this dynamic landscape, Nexusguard's attack handling process operates continuously, providing ongoing protection and resilience.

The subsequent sections delve into the interconnected sub processes, components and Apps that form an integral part of this ongoing cycle of attack handling. These elements function collaboratively, working harmoniously in unison to ensure effective defense against L3/L4 attacks.

Attack Detection

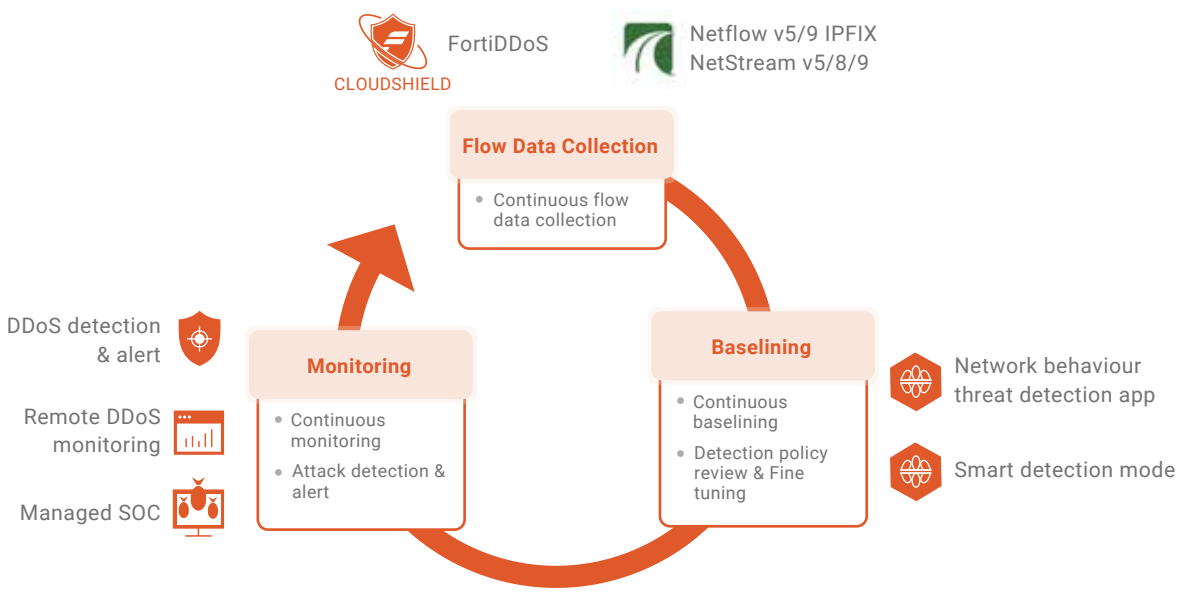


Figure 3 - Continuous Flow Data Collection, Baselining and Monitoring

Flow Data Collection

Origin Protection offers extensive support for flow data collection, encompassing a diverse range of flow collection protocols. When it comes to flow-based collection, our system facilitates session sampling, as well as supporting widely utilized protocols such as Netflow v5/9, IPFIX, and NetStream v5/8/9. These protocols are compatible with routers, ensuring seamless integration and efficient flow data collection.

In addition to flow-based collection, Origin Protection also extends its capabilities to packet-based sampling, and supports sflow v2/4/5 protocols, which are commonly used in switches. This extensive support for packet-based sampling enables efficient packet-level data collection, enhancing the visibility and monitoring capabilities of the system.

Baselining

Utilizing advanced technology known as Smart Baselining, Origin Protection employs deep learning algorithms to meticulously observe and analyze traffic patterns within the protected network over a specified timeframe. This intelligent solution provides access to recommended detection threshold values that are finely tuned to the specific characteristics of the network.

Through the power of deep learning, Smart Baselining effectively reduces false alarms and achieves rapid anomaly detection. Learning the distinct traffic patterns unique to the network, it establishes precise baseline thresholds, facilitating swift identification of potential threats, enabling immediate mitigation, and minimizing any potential disruptions to network operations.

Detection Policy Configuration

Nexusguard's attack detection policy for L3/4 operates within a hierarchical framework, encompassing site, network, and host levels. At the host level, a host-based profile is employed to safeguard against attacks specifically targeting an individual host or IP address. This profile focuses on protecting the integrity and availability of the targeted host's resources. Moving up to the network level, a network-based profile is implemented to counter attacks that target a network or a range of IP addresses. This profile is designed to detect and mitigate attacks that attempt to exploit vulnerabilities across multiple hosts within a network. At the highest level, the site profile provides comprehensive protection for the customer's entire infrastructure, addressing potential threats that may impact the overall network environment.

Figure 4 - L3/4 Detection Policy

Real-time Monitoring

In the realm of bandwidth monitoring, Nexusguard maintains a vigilant watch over multiple essential metrics. These include internet link utilization, network bandwidth level, packet rate, network latency, and packet loss. By consistently monitoring these parameters, Nexusguard is able to swiftly identify any irregular patterns or sudden surges in network traffic, which may serve as indicators of ongoing attacks or potential resource exhaustion.

To ensure round-the-clock monitoring, Nexusguard's team of skilled SOC experts remain on hand 24/7, facilitated through the Nexusguard Portal that consolidates analytics, detection, and mitigation tools, in a single pane of glass.

Flexible Detection Modes

Origin Protection offers three flexible modes of attack detection, allowing operators to adapt to dynamic attack scenarios seamlessly. These modes include Normal, Rapid, and Smart, each catering to different types of attack patterns.

In Normal Mode, there is constant monitoring of attack traffic, providing advanced warning prior to an attack. It diligently tracks traffic from customer networks and initiates appropriate measures if the traffic surpasses a predetermined threshold within a defined timeframe.

Rapid Mode is designed to effectively manage bursty traffic and swiftly identify hit-and-run attacks by actively monitoring the traffic flow from customer networks, enabling early detection of potential threats. Smart Mode is specifically tailored for dynamic traffic profiles. Leveraging Nexusguard's proprietary AI detection system, this mode utilizes Deep Learning technologies to deliver intelligent and precise detection capabilities, enhancing accuracy and significantly reducing false positives.

Figure 5 - Smart Mode Detection

Whether it's continuous attacks, sudden bursts, or dynamic traffic profiles, Origin Protection provides comprehensive and adaptable detection capabilities to safeguard client network infrastructures.

Attack Alert Notification

Nexusguard's Event Notifier App plays a vital role as a centralized platform, facilitating the management and delivery of diverse alert types. This effective tool supports the three widely used communication channels: email, SNMP Trap, and syslog. Leveraging these channels, alerts are seamlessly transmitted through preferred methods of communication, ensuring efficient notifications. Moreover, the App empowers users with customization capabilities, allowing them to define and personalize alert levels to align with their specific needs. With the Event Notifier App, organizations gain the ability to proactively monitor and swiftly respond to critical events, ensuring timely and pertinent notifications for effective incident management.

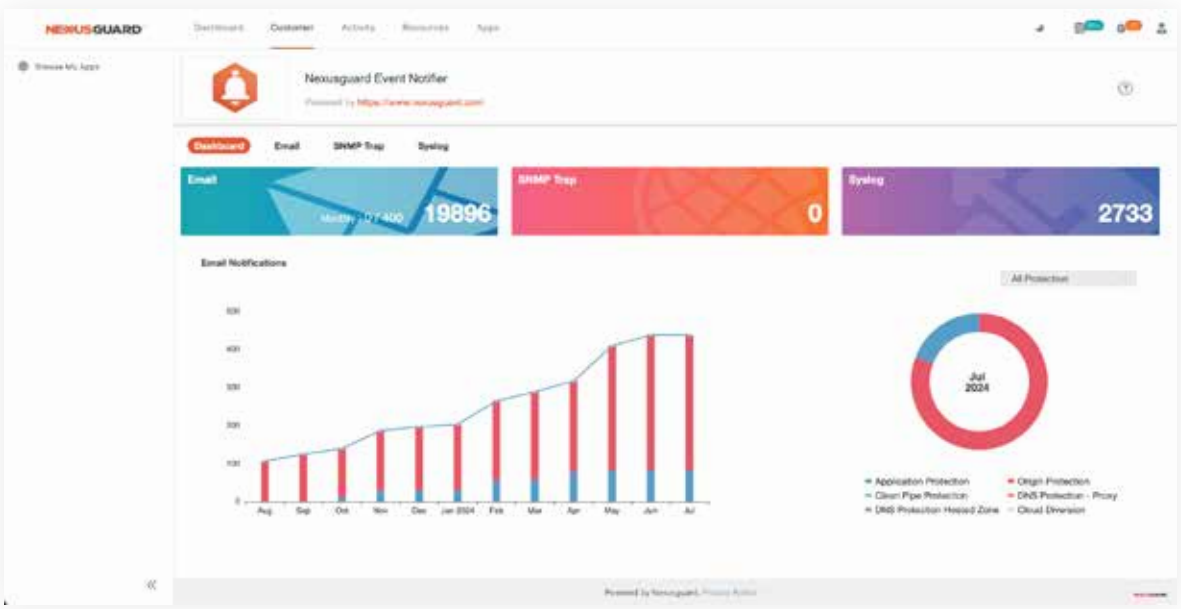


Figure 6 - Nexusguard Event Notifier

Traffic Diversion

Auto BGP Route Diversion Assisted by Cloud Diversion App

Origin Protection encompasses a Cloud Diversion App that enables seamless and automated traffic diversion for customers. The App swiftly diverts customer traffic to the Nexusguard network within minutes when it surpasses a pre-defined bandwidth threshold, eliminating the need for on-premise appliances or customer intervention.

With the Cloud Diversion App, traffic diversion becomes effortless and automatic, seamlessly redirecting traffic to the Nexusguard network as soon as anomalies are identified by our advanced proprietary technologies. This proactive measure ensures that attack mitigation takes place promptly, guaranteeing that only legitimate traffic enters client networks, thereby maintaining the highest level of network security at all times.

Attack Mitigation

Origin Protection adopts a comprehensive approach to safeguarding networks against various types of attacks. One key aspect of this approach is multi-layered filtering, which involves a resilient cloud-based network capable of defending against large-scale bandwidth and resource flood-based attacks. Additionally, Nexusguard employs heuristic-based algorithms to intelligently detect and mitigate application-based attacks, ensuring precise and effective protection. The solution also incorporates static and dynamic content caching and acceleration techniques, optimizing web application performance and enhancing user experience. With the combination of all these elements, Nexusguard offers a robust defense mechanism that addresses different attack vectors while ensuring optimal network performance and user satisfaction.

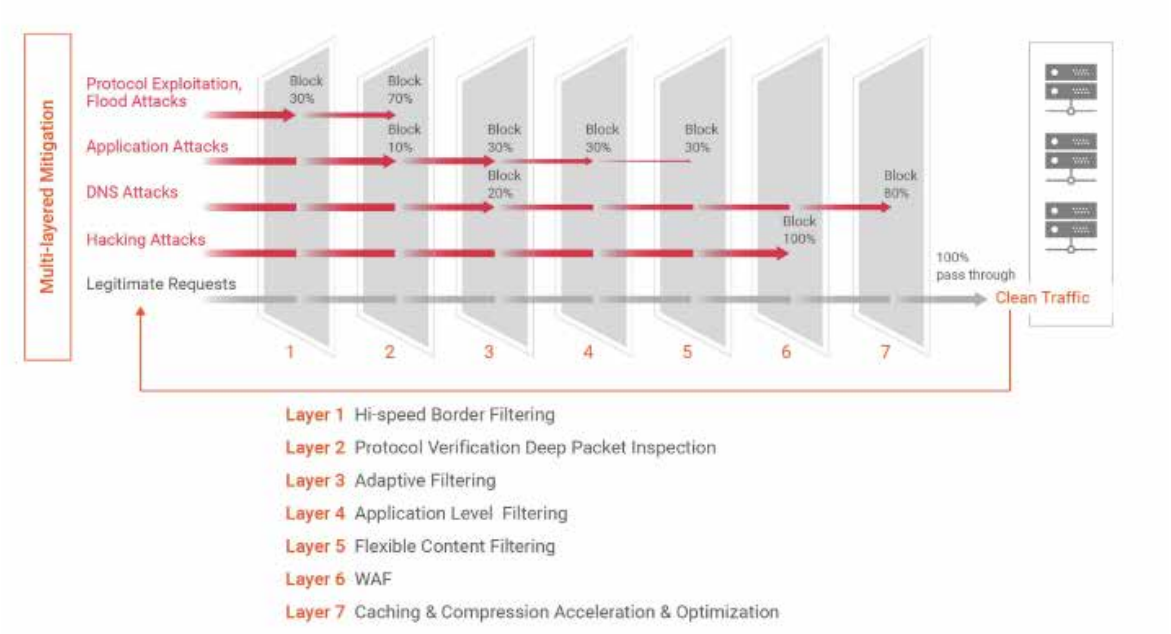


Figure 7 - Multi-layed Mitigation Approach

Clean Traffic Delivery

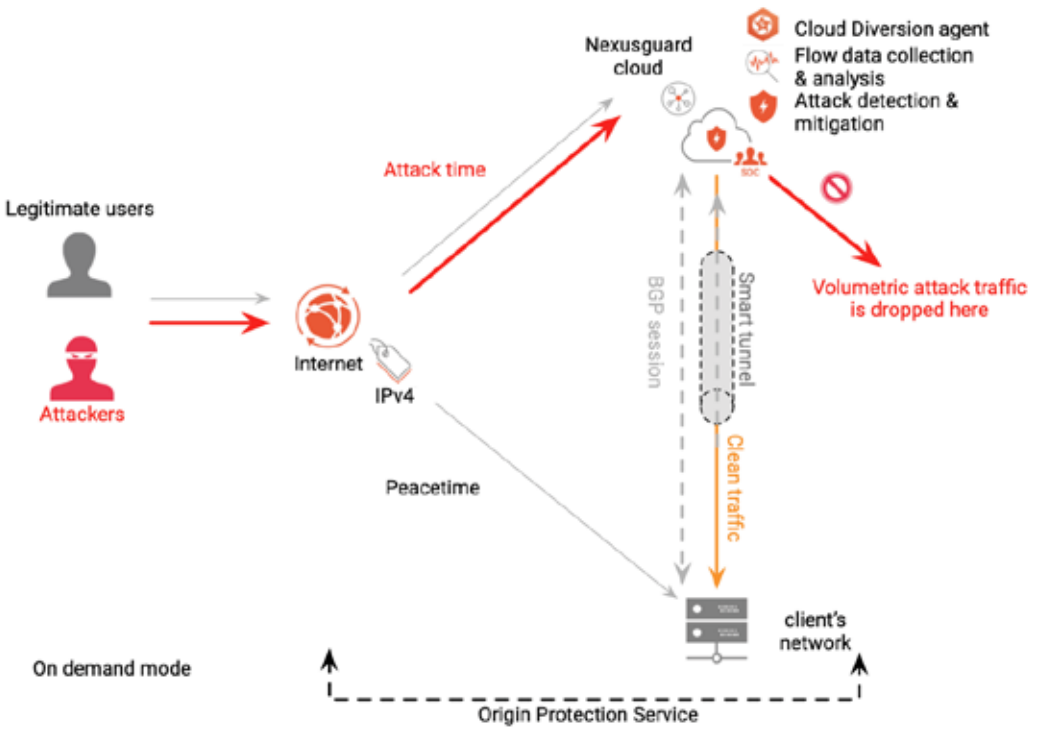


Fig 8 - Clean Traffic Delivery

GRE Tunnels

When a malicious attack is detected, Nexusguard takes swift action by announcing the BGP route associated with the targeted /24 IP prefix to the Internet. This announcement redirects the incoming traffic to Nexusguard's globally distributed scrubbing centers, where comprehensive cleansing takes place. At these centers, the malicious traffic is effectively dropped, ensuring that only clean and legitimate traffic remains. The securely filtered and sanitized traffic is then returned to the customer networks through GRE tunnels, guaranteeing the safe and uninterrupted flow of legitimate data.

Direct Connect

Origin Protection provides OP clients with an alternative approach called Direct Connect, enabling the direct flow of clean traffic from our scrubbing centers to customer networks. This option is available to OP clients whose data centers are strategically located near our POPs or co-located with our data centers. Establishing a direct physical connection with Nexusguard's scrubbing centers enables OP clients to seamlessly connect to our network.

While GRE remains the primary deployment method for delivering clean traffic, Direct Connect serves as a valuable complement rather than a replacement for GRE. When combined with GRE, Direct Connect further enhances the overall solution. This combination proves exceptionally effective, particularly during large-scale attacks, whereby attack traffic is intelligently shared and distributed between our logically connected scrubbing centers via GRE and the directly connected scrubbing centers, ensuring that customer networks are continuously and comprehensively safeguarded.

Nexusguard's Suite of Apps

The seamless integration of Nexusguard's suite of Apps plays a pivotal role in facilitating the operation of Nexusguard's Origin Protection service, providing organizations with a comprehensive and advanced security solution. These Apps work in perfect synergy to detect, mitigate, and defend against L3/L4 attacks, ensuring the utmost protection for networks, data, and operational continuity.

Network Behavior Threat Detection App

Nexusguard's Network Behavior Threat Detection (NBTD) App serves as a baselining tool that integrates seamlessly with the Origin Protection service. By monitoring recent traffic profiles, the NBTD App establishes a baseline for normal network activity. When the current traffic exceeds the historical baseline by a significant margin, it indicates an increased likelihood of a DDoS attack.

CloudShield App

Integrated with FortiDDoS appliances, the CloudShield App plays a crucial role in collecting attack information from local FortiDDoS devices deployed at the client's site, providing dedicated local protection against attacks. Simultaneously, the inclusion of the Nexusguard Cloud further enhances the setup by providing cloud offload capabilities, particularly when confronted with massive attacks that surpass the capacity of the FortiDDoS appliances or the available Internet uplink. This integration creates a robust and comprehensive anti-DDoS hybrid solution that not only safeguards investment but also strengthens the overall protection against large-scale DDoS attacks.

SmartFilter and FlowSpec Apps

Amalgamated with Origin Protection, the Nexusguard SmartFilter App generates mitigation rules automatically based on Nexusguard's Smart Detection baselining, adapting and self-adjusting dynamically during an attack. Equipped with pre-configured mitigation policies, including Amplification Attacks and Threat Intelligence, SmartFilter provides comprehensive attack mitigation against well-known and zero-day reflection attack signatures. Threat information obtained from newly discovered IP addresses infected by malware used as 'zombies' by botnets is also used in combination with Good User database intelligence to help mitigate attacks more swiftly.

Nexusguard's BGP Flow Specification (Flowspec) App enables rapid deployment and propagation of filtering and policing mechanisms across numerous BGP peer routers. This capability effectively mitigates the impact of DDoS attacks on a network, while also helping to prevent congestion by protecting the Internet uplink.

Real-World Application and Case Study

Nexusguard showcased their expertise in recently mitigating a complex cyber attack after its Origin Protection service quickly identified it as a sophisticated Carpet Bomb attack. It transpired that a leading integrated telecommunications and information services provider in the Middle East, renowned for its robust security measures against DDoS attacks, found itself under siege by a DDoS attack, hammering its network with a barrage of DDoS traffic ranging from 1 to hundreds of gigabits per second that lasted for 24 hours. Despite their advanced detection systems, the source and target of the attack remained a mystery, leaving the ISP vulnerable and unable to effectively mitigate the onslaught.
In their desperation, the ISP turned to Nexusguard for assistance. Within hours, Nexusguard's engineers deployed their Origin Protection service and the attack was swiftly mitigated, restoring normalcy for the ISP and its customers.

Activation of Origin Protection involved remote DDoS detection, traffic diversion to Nexusguard scrubbing centers for mitigation using BGP and peering, and sophisticated attack mitigation measures, including SMART (Statistical, Mitigation, Analysis, and Response Technology). Once the traffic was scrubbed, clean traffic was returned to the origin network using predetermined GRE tunnels.

Nexusguard's Origin Protection service demonstrated its efficacy in protecting networks from complex and aggressive DDoS attacks, ensuring continuous service availability and network resilience. The case study highlighted the importance of comprehensive DDoS protection and illustrated Nexusguard's proficiency in mitigating complex and relentless attacks, safeguarding the connectivity and reputation of organizations worldwide.

Nexusguard Integrated Portal and Support

Nexusguard Portal

The Nexusguard Portal provides an intuitive and integrated interface for continuous traffic analysis, alerting, traffic redirection, scrubbing, and clean traffic delivery. It offers a dynamic dashboard that visually presents a multitude of metrics, event logs, and reports, simplifying the ongoing monitoring and management of security measures.

Security Operations Center (SOC)

Nexusguard's SOC is staffed by a team of highly skilled security professionals, operating around the clock to monitor and protect against emerging threats including zero day attacks. Equipped with advanced threat intelligence systems and real-time monitoring capabilities, the SOC ensures prompt detection and response to security incidents.

Round-the-Clock Service

Nexusguard offers 24/7 support to its clients, providing timely assistance and expert guidance. This commitment to accessibility ensures that clients receive the support they need, regardless of their geographical location or preferred language.

Conclusion

Nexusguard's Origin Protection service provides comprehensive and adaptable DDoS protection for large-scale networks. By leveraging advanced detection and mitigation technologies, continuous real-time monitoring, and a dedicated Security Operations Center, Nexusguard empowers organizations to proactively combat evolving threats and safeguard their digital assets.

Call to Action

Organizations are encouraged to adopt Nexusguard's Origin Protection for comprehensive security against DDoS attacks. Contact Nexusguard today to learn more about how their solutions can protect your mission-critical services and ensure uninterrupted operation.

References

[Nexusguard Origin Protection Datasheet; Nexusguard Solution-based Article - Safeguard Your Internet Uplink and Network Infrastructure with Nexusguard Origin Protection]

About Nexusguard

Founded in 2008, Nexusguard is a leading distributed denial of service (DDoS) security solution provider fighting malicious internet attacks. Nexusguard ensures uninterrupted internet service, visibility, optimization and performance. Nexusguard is focused on developing and providing the best cybersecurity solution for every client across a range of industries with specific business and technical requirements. Nexusguard also enables communication service providers to deliver DDoS protection solution as a service. Nexusguard delivers on its promise to provide you with peace of mind by countering threats and ensuring maximum uptime.

NEXUSGUARD®

www.nexusguard.com

20240806-EN-A4

© 2024 Nexusguard Limited. All Rights Reserved