NEXUSGUARD®

Empowering CSPs: Enhancing Security with Nexusguard Edge Protection

WHITE PAPER

Abstract

The increasing frequency and intricacy of Distributed Denial of Service (DDoS) attacks have drastically altered the security landscape, prompting organizations to revise their defense strategies. This document investigates specialized anti-DDoS solutions that can efficiently shield against a wide array of DDoS attacks, ensuring uninterrupted operations for organizations. We delve into the attributes and benefits provided by Nexusguard's Edge Protection service, designed to swiftly enhance the mitigation capabilities of CSPs, thereby improving their capacity to effectively counter threats. Supported by a dedicated Security Operations Center (SOC) and cutting-edge technologies, Nexusguard's anti-DDoS solutions empower organizations to proactively combat emerging threats and secure their digital assets.

Introduction

Background on DDoS Attacks

In today's interconnected landscape, the looming threat of DDoS attacks presents substantial risks to network infrastructure and web applications. These malicious attacks have the potential to disrupt the availability, performance, and security of critical systems, causing significant damage to businesses and organizations. With the increasing frequency and sophistication of such attacks, the security environment has undergone significant changes, prompting organizations to adjust and enhance their defense strategies accordingly.

The Call for Comprehensive DDoS Protection

With the dynamic evolution of the security environment, DDoS attacks are growing in complexity, necessitating organizations to refine their security strategies. To effectively counter the escalating menace of DDoS attacks, organizations must implement resilient DDoS protection solutions capable of mitigating diverse attack patterns. These solutions should adeptly manage volumetric surges and intricate application-layer breaches, safeguarding the availability of network infrastructure and upholding the integrity of websites, applications, and digital assets.

Overview of Nexusguard’s Edge Protection Service

Nexusguard's Edge Protection service presents a truly integrated and cohesive user experience bridging the gap between on-premise and cloud protection. CSPs with Nexusguard Bastions deployed gain the most from the benefits offered by the Nexusguard Edge Protection service. By leveraging this service, CSP partners can greatly enhance the security and performance of their Internet connections, leading to a smooth and continuous connectivity experience. This, in turn, strengthens the provision of dependable and high quality services to their customers.

The Solution: Nexusguard's Edge Protection

Description of Nexusguard Edge Protection Service

The primary goal of the Nexusguard Edge Protection service is to support CSP partners by protecting them from attacks that could potentially overwhelm their designated bandwidth and the capacity of the Bastions server, achieved by diverting the traffic to the Nexusguard Cloud.

When an attack poses a threat of overwhelming the local CSP scrubbing capacity, Nexusguard Edge Protection springs into action. The scrubbing process occurs within the Nexusguard scrubbing cloud, swiftly neutralizing attacks near their origins, while legitimate traffic is rerouted back to the destination network through a GRE tunnel facilitated by the local Bastions deployment.

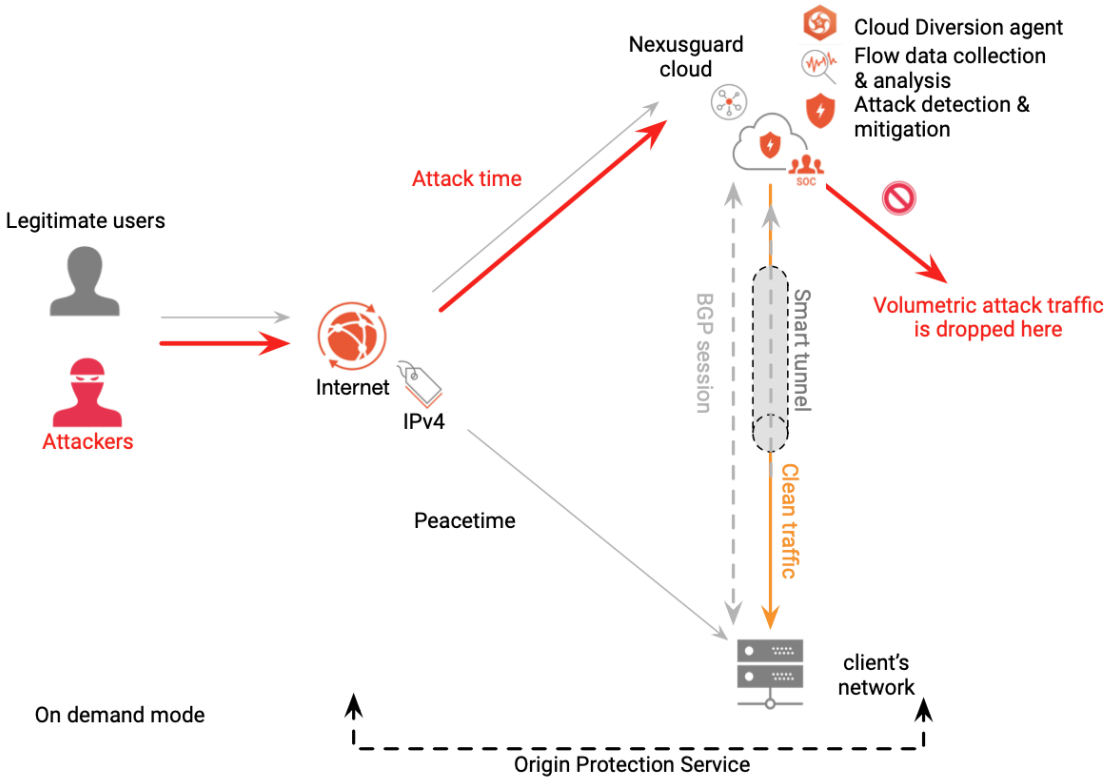

Figure 1 - Nexusguard Edge Protection

Securing CSP Networks with Nexusguard's Edge Protection

Bandwidth sizing holds significant importance in CSP operations, yet the Nexusguard Edge Protection solution introduces a distinctive perspective to this procedure. Let's examine the factors that impact the ideal distribution of bandwidth.

Mitigation Capacity of Bastions Server

Assessing the mitigation capacity of the Bastions server plays a crucial role in bandwidth sizing. Within Nexusguard's solution, the Bastions R650-G2 server stands out with its remarkable 100 Gbps traffic-handling capability. Nevertheless, it's essential to understand that the internet bandwidth allocated by a CSP partner for managing attacks may not always match the server's capacity; these two elements can vary independently.

Allocation of Bandwidth for Volumetric DDoS Attacks

Assigning enough internet bandwidth to withstand volumetric DDoS attacks is a pivotal decision. Yet, accurately gauging the necessary bandwidth is more art than science. This determination hinges on diverse factors such as the the cost of bandwidth, spare internet capacity, risk profile and frequency of attacks faced by the safeguarded clients. The individual attack data of each CSP partner may not offer a perfect template for bandwidth allocation.

Nexusguard’s Edge Protection Strategy

When deciding how much internet bandwidth to allocate for managing sudden spikes in volumetric DDoS attack traffic, several factors come into play. This includes not just the financial aspects, like the cost of bandwidth and spare capacity of Internet links, but also operational factors that help determine the best time frame to divert traffic to the Nexusguard Cloud.

If an attack nears or surpasses the designated bandwidth, delaying the diversion of traffic to the Nexusguard Cloud can lead to excessive internet bandwidth usage, potentially impacting other customers. On the other hand, diverting traffic too early may underutilize the Bastions server capacity or result in higher costs for the Edge Protection service, depending on dynamic usage.

The key focus of Edge Protection lies in maximizing benefits while minimizing costs. Operators, through financial analysis and experience can make adjustments to strike the right balance in deciding when to switch over to the Nexusguard Cloud. This fine-tuning is crucial for optimizing the advantages of Edge Protection while managing costs effectively and establishing the most optimal internal operational protocols.

The Transformative Benefits of Nexusguard Edge Protection

1. Immediate Enhancement of Mitigation Capacity

Through Edge Protection, the mitigation capacity of Bastion Points of Presence (PoPs) is promptly bolstered within the Nexusguard cloud infrastructure. This instant scalability guarantees network resilience, empowering it to manage volumetric DDoS attacks effectively without overburdening the CSP partner's infrastructure.

2. Distributed Attack Risk

Edge Protection efficiently shifts the DDoS attack risks to the Nexusguard cloud infrastructure. By delegating attack mitigation to Nexusguard, CSPs can concentrate on their primary business functions without jeopardizing network security and availability.

3. Minimized Collateral Damage

In the face of an imminent threat that could overpower the local CSP scrubbing capacity, Nexusguard Edge Protection swiftly engages, harnessing the Nexusguard scrubbing cloud to effectively quell attacks at their sources. This proactive approach minimizes collateral damage and guarantees that performance and latency of other clients remain unaffected.

4. Effortless Traffic Control with Cloud Diversion App

Nexusguard's innovative Cloud Diversion app streamlines and automates the traffic diversion processes. Through seamless redirection of malicious traffic to dedicated scrubbing centers, the CSP partner's network remains shielded from attacks, guaranteeing uninterrupted service delivery to customers.

Real-World Application and Case Study

A regional CSP was struggling with frequent volumetric DDoS attacks that overwhelmed their infrastructure during peak traffic hours. Their existing defenses, supported by Nexusguard Bastions, managed to mitigate smaller attacks, but larger incidents continued to strain their bandwidth, leading to service disruptions and latency issues for legitimate users. The CSP needed a solution that could seamlessly scale and coordinate between their on-premise defense and cloud mitigation.

By deploying Nexusguard's Edge Protection, which is fully integrated with their existing Bastions infrastructure, the CSP overcame this challenge. Unlike typical hybrid solutions offered by competitors, where on-premise and cloud solutions operate independently, Nexusguard's Edge Protection provided a unified approach. The CSP could manage both on-premise mitigation and cloud scrubbing through a single dashboard, with real-time statistics and unified policies. This integration ensured seamless traffic redirection to Nexusguard's cloud when local resources were overwhelmed, without operational gaps or delays.

The result was uninterrupted service during large-scale attacks, with improved efficiency in traffic management, enhanced mitigation capabilities, and consistent service quality for end users. The CSP experienced reduced downtime, enhanced security posture, and greater customer satisfaction.

Nexusguard Integrated Portal and Support

Nexusguard Portal

The Nexusguard Portal offers an intuitive and unified interface designed for seamless traffic analysis, real-time alerts, traffic redirection, scrubbing, and secure traffic delivery. With its dynamic dashboard, the portal provides a visual representation of various metrics, event logs, and reports, making it easier to continuously monitor and manage security measures with simplicity and efficiency.

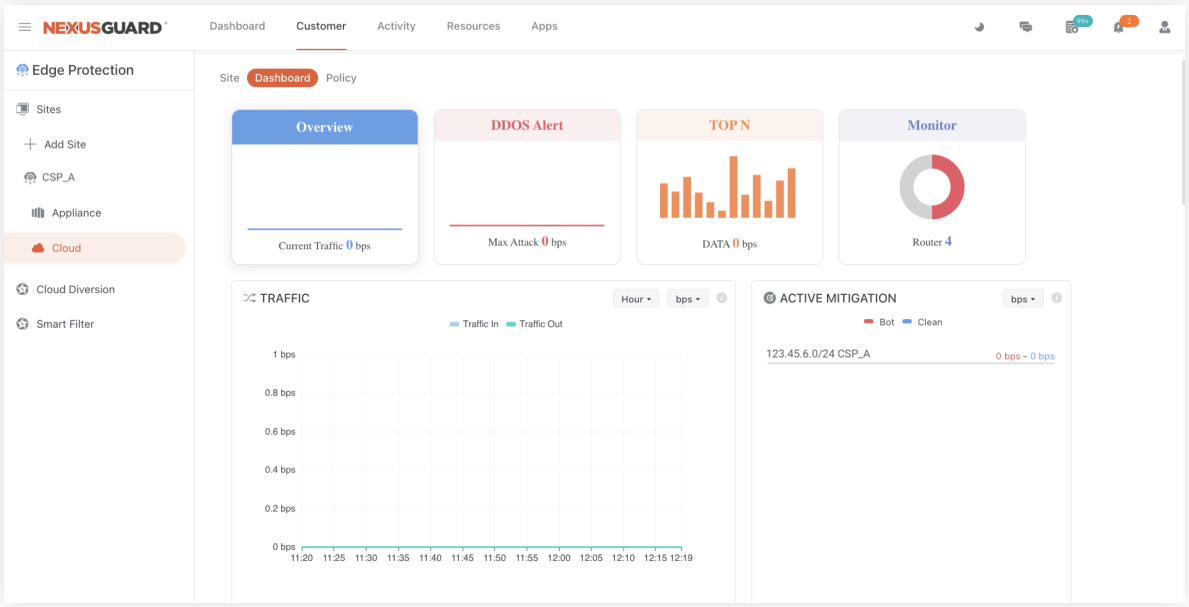

Figure 2 - Nexusguard Portal

Security Operations Center (SOC)

Nexusguard's Security Operations Center (SOC) comprises a dedicated team of exceptionally skilled security professionals who work tirelessly 24/7 to monitor and safeguard against emerging threats. With access to cutting-edge threat intelligence systems and real-time monitoring capabilities, the SOC ensures swift detection and response to any security incidents that may arise, providing proactive protection for the organization.

Round-the-Clock Service

Nexusguard is committed to delivering round-the-clock support to its clients, offering timely assistance and expert guidance whenever they need it. This unwavering commitment to accessibility ensures that clients receive the support they require, regardless of their geographical location or preferred language.

Conclusion

Nexusguard's Edge Protection service delivers extensive DDoS protection for CSP networks. Utilizing Nexusguard Bastion Servers and the Nexusguard Cloud, along with continuous real-time monitoring and a dedicated Security Operations Center, Nexusguard enables CSPs to actively counter evolving threats and protect their digital assets.

Call to Action

CSPs are encouraged to embrace Nexusguard's Edge Protection for thorough defense against DDoS attacks. Reach out to Nexusguard today to discover how their solutions can safeguard your essential services and guarantee uninterrupted operations.

References

Nexusguard Edge Protection Datasheet; Solution-based Article - Redefining CSPs' Internet Uplink: Maximizing Availability with Nexusguard Edge 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