Solution Guide

THE VITAL ROLE OF DNS SECURITY: AN ESSENTIAL GUIDE

NEXUSGUARD®

DDoS Protection Made Simple

Introduction

Your business has managed adequately without knowing much about the intricacies of DNS or its functionalities. Perhaps, you hadn't paid much heed to it. However, everything changed in October 2021 when Facebook encountered a significant DNS error, leading to its most prolonged period of downtime since 2008. Suddenly, many organizations started asking, "What is DNS, and why should DNS security rank among the top priorities when fortifying an organization against cyber threats?"

To explain what DNS security is and why it is of paramount importance, this guide will explore prevalent threats to your DNS system, best practises to fortify its security, and techniques to detect and address vulnerabilities effectively, safeguarding your DNS infrastructure from potential attacks.

But let's first answer the following questions:

What is DNS?
How does DNS work?
Why is DNS important?

What is DNS?

DNS, or the Domain Name System, stands as a cornerstone of the Internet, playing a pivotal role in defining the digital landscape we navigate today. Analogous to a digital phonebook, DNS comprises an extensive network of servers dispersed worldwide, housing a decentralized repository of domain names and their associated IP addresses. Its primary function revolves around accurately pairing domain names with their respective IP addresses, facilitating seamless connectivity across the Internet.

How does DNS work?

Let's first establish the foundational workings of the DNS system. Each Internet-connected device possesses a unique IP address, serving as its identifier during data exchanges. To ensure data packets reach their intended destinations, it is crucial to determine their correct routing.

By default, web browsers handle these exchanges by querying Internet Service Provider DNS servers. DNS servers themselves fall into two primary categories: authoritative servers and recursive resolvers. Authoritative servers store the actual IP addresses of websites, while recursive resolvers, lacking precise addresses, know where to seek this information.

This system was devised to streamline user interactions. Consequently, DNS servers retrieve lengthy IP addresses in the background, allowing users to simply recall website names. Every time you access a website, you unknowingly engage with a DNS server. This underappreciated system stands as one of the foundational pillars enabling the Internet's functionality.

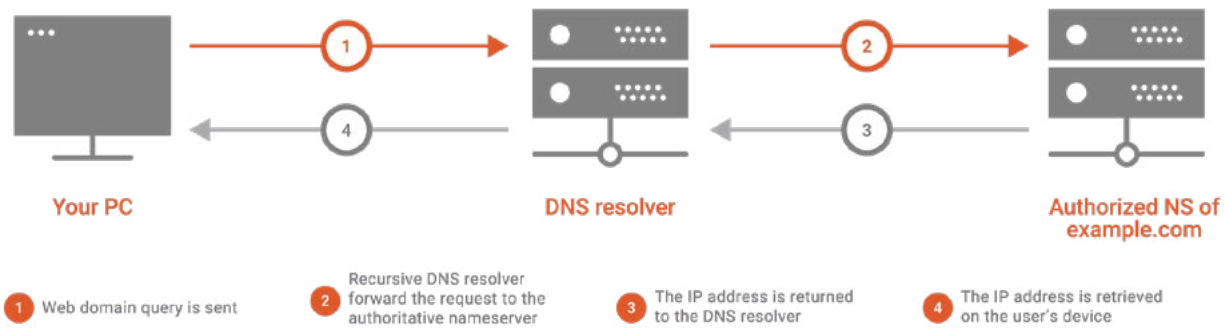

Figure 1 - How DNS Works

Why is DNS important?

At its core, DNS is the unheralded champion of our online experiences, bridging human-readable domain names to machine-readable IP addresses. This essential service facilitates seamless access to websites, email communication, and a multitude of online interactions. Without DNS, traversing the Internet would resemble decoding a complex array of numerical addresses - a formidable challenge even for the tech-savvy.

Why is DNS Security important?

No matter how robust your application and network security measures are, without adequate DNS protection, your overall cyber defense strategy is only as strong as the weakest link. DNS operates as the unsung hero of the Internet, rescuing us from the complexities of numerical IP addresses. When network complications surface, DNS often shoulders the blame. Despite its pivotal role, organizations tend to allocate significant resources towards enhancing application and network security while neglecting DNS security. Viewed as a cost-effective service, DNS often finds itself sidelined in cybersecurity strategies, lacking the attention it deserves in terms of safeguarding.

This oversight poses a significant risk, as history abounds with instances where DNS failures have brought down entire networks and services.

One such landmark case is the 2013 Spamhaus DDoS Attack, where a huge DDoS attack targeted Spamhaus, a nonprofit organization specializing in threat intelligence provision. Despite being an anti-spam entity regularly targeted by attacks and equipped with existing DDoS protection measures, this attack, a reflection attack estimated at 300 gigabits of traffic per second, was large enough to knock its website and a proportion of its email services offline.

Another notable case is the DDoS attack on Dyn. On October 21, 2016, a massive DDoS attack targeted Dyn, a prominent DNS provider. This attack wreaked havoc, causing widespread disruption for numerous prominent websites such as Airbnb, Netflix, PayPal, Visa, Amazon, The New York Times, Reddit, and GitHub. The attackers employed malicious software known as Mirai.

The Perils of DNS Security Negligence

The vulnerabilities within DNS transcend mere service interruptions and outages, venturing into the domain of cyber warfare. Malevolent actors exploit weaknesses such as DNS cache poisoning, DDoS attacks, and DNS hijacking to unleash havoc on unsuspecting targets. The consequences extend beyond disruptions, as financial ramifications can be severe, with organizations facing hefty charges stemming from exceeding DNS query thresholds.

In a cybersecurity landscape fraught with ever-evolving threats, neglecting DNS security equates to leaving the front door ajar while fortifying the rear entrance. Despite the seemingly simplistic nature of DNS technology, its significance is paramount. Just as a phone directory remains indispensable despite technological advancements, DNS stands as the Internet's critical backbone.

Impacts of DNS attacks on your organization

An unavailable DNS server leads to profound repercussions, encompassing financial losses, data theft, and reputational harm as serious consequences of DNS attacks.

Financial Losses

DNS attacks have the potential to result in substantial financial repercussions. Service interruptions, decreased productivity, and the expenses tied to incident mitigation and recovery efforts can lead to considerable monetary losses.

Data Security Risks

A compromised DNS infrastructure opens the door for attackers to intercept sensitive information, paving the way for costly data breaches and potential legal consequences.

Reputational Damage

Successful DNS attacks can severely damage customer trust and tarnish the reputation of your organization. A compromised reputation can hinder business prospects and place you at a competitive disadvantage in the market.

DNS Attacks

DNS was primarily designed to provide accurate and efficient responses to queries, without questioning their intent. Consequently, DNS exhibits genuine vulnerabilities, making it a potential vector for cyberattacks. Threat actors operate with diverse goals in mind, spanning from redirecting traffic to nefarious sites, intercepting sensitive data, to inundating DNS servers to trigger service interruptions. These attacks often exhibit high levels of complexity, rendering them challenging to identify, thus presenting a substantial menace to organizations of every scale. The following section delves into the most common types of DNS attacks.

DNS Cache Poisoning

DNS cache poisoning entails the manipulation of DNS records to distort the reliability of essential information provided by DNS. Essentially, DNS cache poisoning deceives the system by introducing false data into the caches of DNS resolvers, pivotal intermediaries tasked with translating user-friendly domain names into machine-readable IP addresses.

By corrupting these caches with inaccurate IP assignments, malevolent actors can reroute unsuspecting users to deceptive websites, intercept sensitive communications, and potentially create openings for further cyber intrusions. This subtle stratagem underscores the vulnerability inherent in the foundational strata of digital communication, emphasizing the critical need to comprehend and address the risks associated with DNS attacks.

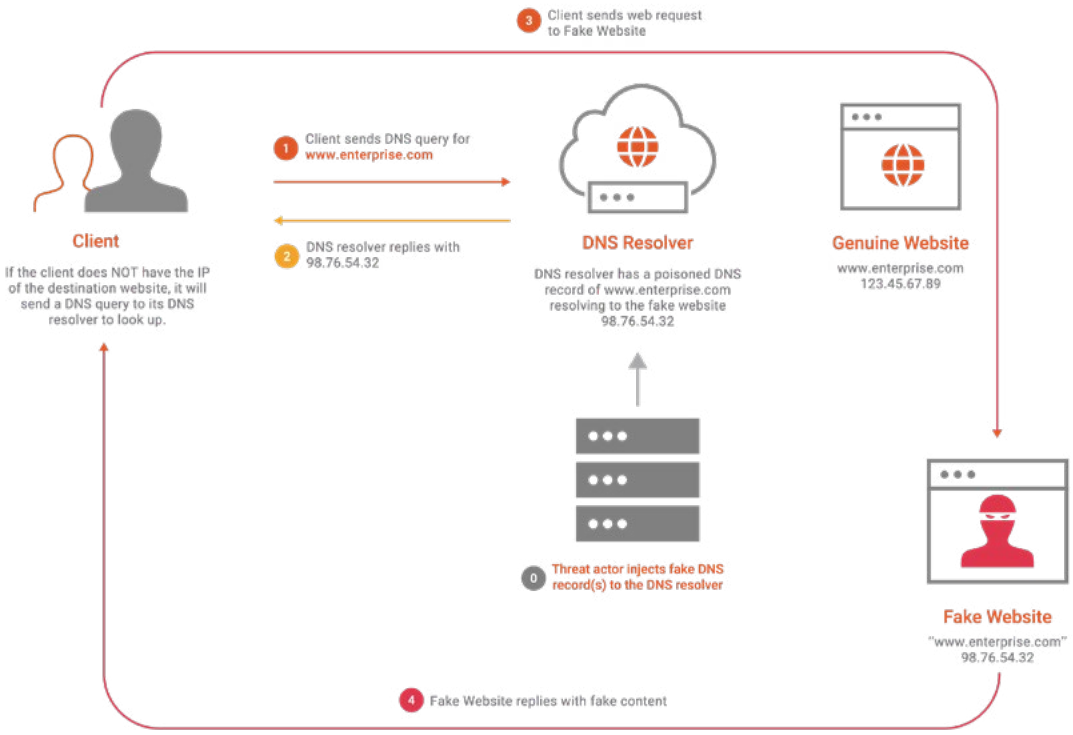

Figure 2 - DNS Cache Poisoning

DDoS Attacks

In a distributed denial-of-service (DDoS) attack, a form of cyber attack, a cyber threat actor floods a website, server, or network resource with malicious traffic. Consequently, the target system crashes or becomes inoperable, depriving legitimate users of service and impeding genuine traffic from reaching its intended destination.

Botnets represent the predominant method through which DDoS attacks are executed. Attackers infiltrate computers or devices to implant a malicious piece of code, known as a bot. These infected machines collectively establish a network termed a botnet. Subsequently, the attacker commands the botnet to inundate the victim's servers and devices with an excessive volume of connection requests, surpassing their processing capacities.

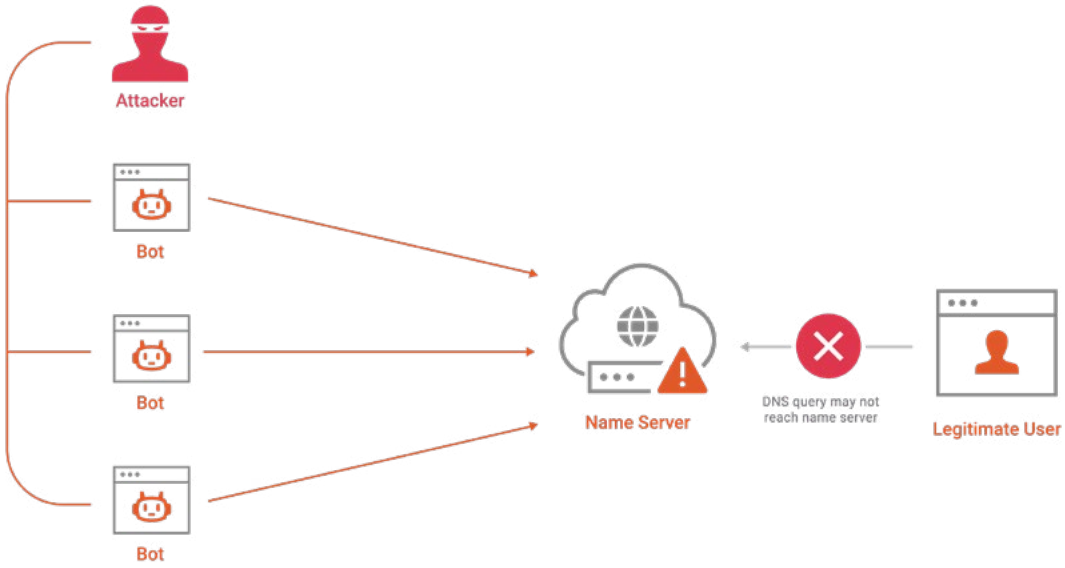

Figure 3 - DDoS Attacks

DNS Tunneling

Another prevalent method of DNS attack, and one of the enduring ones, is DNS tunneling. These attacks capitalize on the DNS protocol to create tunnels for transmitting malware and other information through a client-server framework. This data transfer can commandeer a DNS server, granting attackers control over the server and its applications.

Through tunneling, a covert link is established between the attacker and the target via the DNS resolver, circumventing firewall defenses. This tunnel can be exploited by cybercriminals for nefarious purposes such as data exfiltration.

DNS tunneling often hinges on the external network connectivity of a compromised system, enabling entry into an internal DNS server with network privileges.

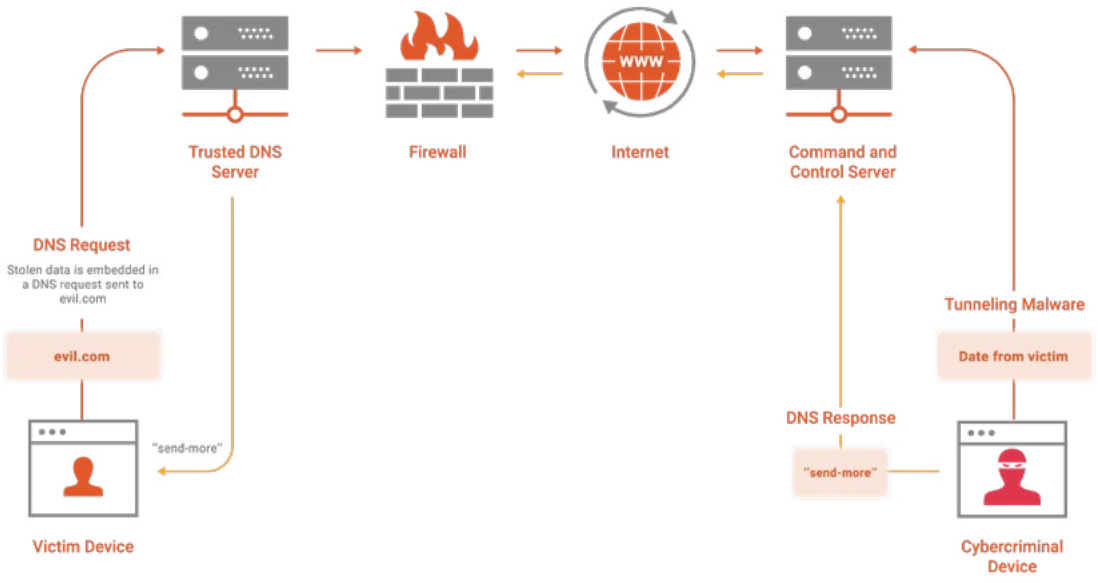

Figure 4 - DNS Tunneling

DNS Amplification

A prevalent form of DDoS attack known as a DNS amplification attack exploits publicly accessible DNS servers to inundate a target system with overwhelming DNS response traffic.

The primary technique involves the attacker dispatching a DNS name lookup request to an open DNS server, with the source address falsified to mimic the target's address.

Upon receiving the DNS record response from the DNS server, it is redirected to the target. Attackers typically seek extensive zone information to maximize the amplification effect. In the majority of such attacks, the falsified queries submitted by attackers are of the "ANY" type, which elicits all available data about a DNS zone in a single request.

Due to the considerable discrepancy between the size of the response and the initial request, the attacker can escalate the volume of traffic aimed at the target systems. And by harnessing a botnet to generate numerous falsified DNS queries, an attacker can effortlessly generate a substantial volume of traffic.

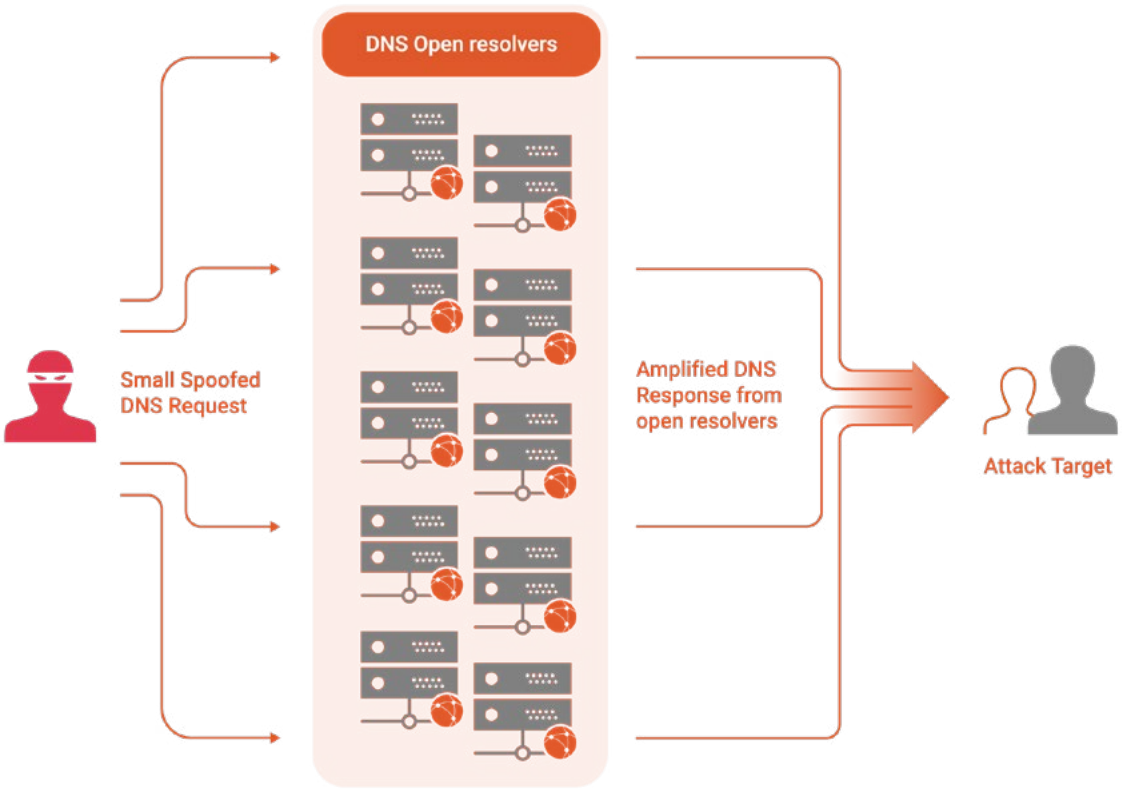

Figure 5 - DNS Amplification

DNS Hijacking

DNS hijacking, also termed as domain theft, represents an attack method centered on seizing control of a domain name through illicit methods. In this form of attack, DNS servers commonly serve as the initial point of compromise. Essentially, the manipulation of DNS records redirects traffic towards nefarious websites. While primarily employed to pilfer sensitive data like login credentials, DNS hijacking can also facilitate malware distribution and phishing endeavors.

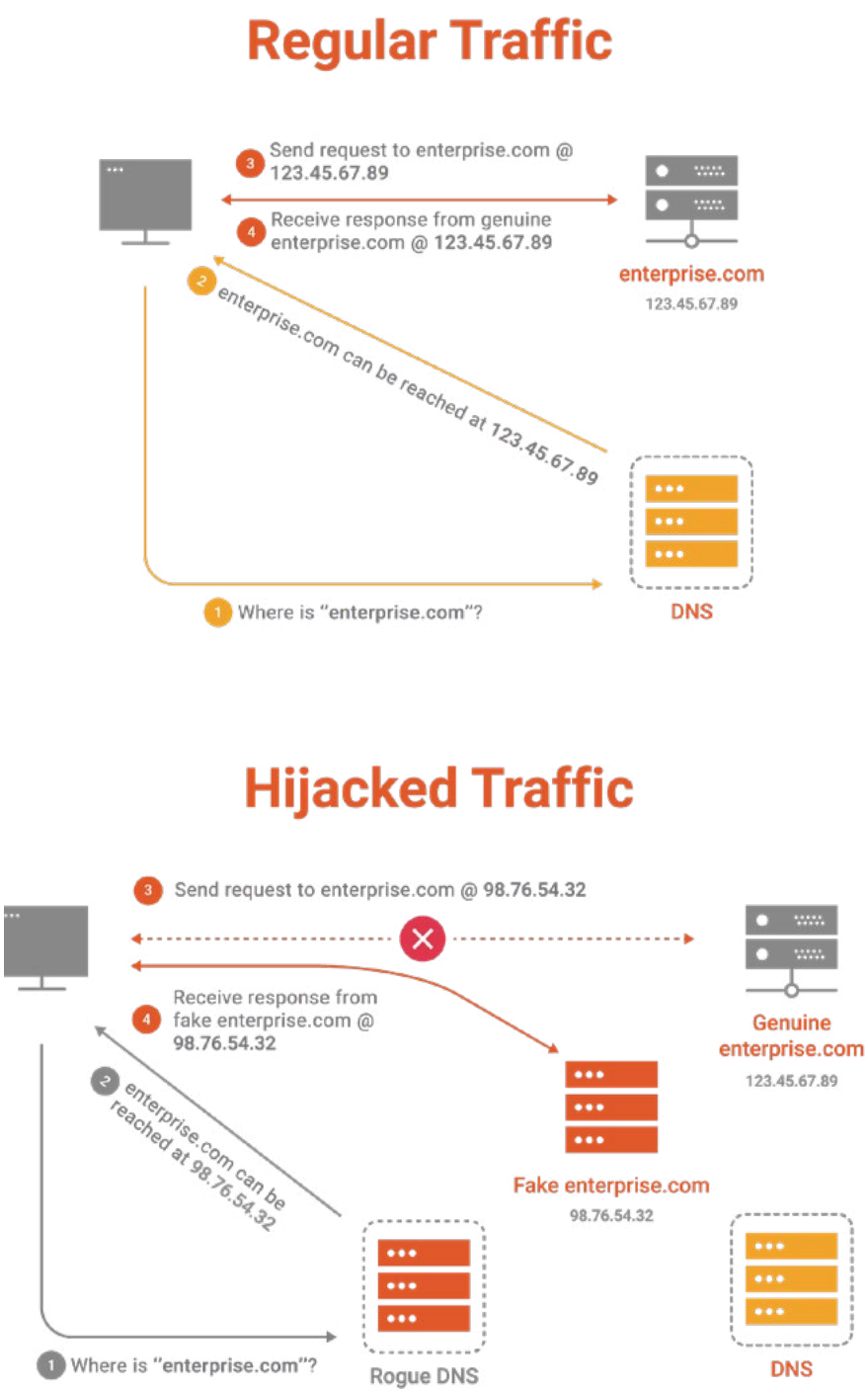

Figure 6 - DNS Hijacking

Best Practices on how to secure DNS

Organizations can adopt a number of practices to help reduce the vulnerability to DNS attacks. Here are some recommended practices:

Implementing DNSSEC

Integrate DNSSEC (DNS Security Extensions) to incorporate digital signatures into DNS records, enhancing the ability to authenticate DNS responses and prevent DNS cache-poisoning assaults.

Mandating Multifactor Authentication

Prevent unauthorized access by requiring multifactor authentication to access DNS settings.

Monitoring DNS traffic

Vigilantly monitor DNS traffic for signs of suspicious behavior, such as unusual spikes in activity or atypical query patterns, enabling security teams to swiftly counter DNS threats.

Network Segmentation

Mitigate the impact of a DNS attack by segregating critical systems from less critical systems.

Regular System Updates and Patching

Maintain system integrity by consistently updating and patching systems to preempt threat actors from capitalizing on vulnerabilities.

Integrating DNS attack readiness into your incident response

An effective method to fortify your systems against DNS attacks is to create and uphold an incident response strategy. This plan can be customized to handle DNS attacks, delineating roles, responsibilities, and systematic protocols for containment, investigation, and recovery.

Nexusguard DNS Protection Service

Introducing Nexusguard DNS Protection Service (DP) - a robust solution designed to safeguard an organization's DNS infrastructure and enhance its cybersecurity resilience. Nexusguard DP stands as a vital cybersecurity safeguard designed to enhance the resilience of Name Servers against various threats and malicious assaults. Serving as the frontline defense, DP plays a crucial role in maintaining the availability and accessibility of communication across the expansive digital landscape of the Internet.

Salient Features of Nexusguard DP

With Nexusguard DNS Protection, organizations can guarantee availability and optimal performance of their name servers, reducing disruptions and downtime that could negatively affect their users.

Continuous Protection

Nexusguard DP operates continuously, ensuring uninterrupted defense for your DNS infrastructure. This perpetual protection remains active at all times, creating a persistent barrier against potential threats. By maintaining this "always-on" mode, any risks during DNS changes' propagation phase are preemptively addressed, guaranteeing constant security.

Advanced Defense Technologies

The implementation of Nexusguard DP leverages advanced in-house detection and mitigation technologies to combat various attacks effectively. This integrated suite of technologies works cohesively to identify and neutralize a wide spectrum of threats, ensuring sustained security for the DNS infrastructure.

Compliance with DNSSEC

Within DP hosting, Nexusguard fortifies security through DNSSEC, enhancing DNS integrity by verifying that domain data originates from the legitimate domain owner. DNSSEC effectively eradicates the risk of DNS data manipulation through the utilization of public key cryptography and digital signatures.

Optimized Performance

Nexusguard DP can be implemented in an ANYCAST mode, facilitating DNS traffic distribution across multiple Points of Presence (PoPs) to bolster the DNS infrastructure's reliability and performance.

Resilient Cloud Infrastructure

Nexusguard DP utilizes the resilient cloud bandwidth offered by Nexusguard, enabling the DNS infrastructure to manage high traffic volumes and uphold optimal performance even during peak usage periods.

DANE Integration

Nexusguard incorporates DANE support into its DP hosting service, providing users with heightened security benefits. By leveraging DANE, Nexusguard guarantees the validation and authentication of SSL/TLS certificates utilized in hosting environments through the DNS records linked to the corresponding domains. This effectively reduces the exposure to risks such as certificate impersonation, man-in-the-middle attacks, and various other certificate-related vulnerabilities.

Zone Verification and Management

In response to Sitting Duck Attacks, Nexusguard has a protocol in place that combines software and procedural solutions.

New zones subscribing to Nexusguard DP hosting must successfully undergo zone authentication before being integrated.

In instances of dispute, Nexusguard's service team will carry out manual verification of zone ownership. Any zones lacking proper ownership validation will be swiftly removed. The legitimate owner can then easily re-add the zone through the Nexusguard Customer Portal.

Get in touch with us now to discover additional information about our cybersecurity offerings and how we can safeguard you in an ever more interconnected environment. Click here for additional insights into Nexusguard's dependable and flexible anti-DDoS solutions.

About Nexusguard

Founded in 2008, Nexusguard is a leading cloud-based 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 communications service providers to deliver DDoS protection solutions as a service. Nexusguard delivers on its promise to provide you with peace of mind by countering threats and ensuring maximum uptime.

www.nexusguard.com

contact@nexusguard.com