NEXUSGUARD

DDoS Protection Made Simple

DNS Protection

What is DNS Protection?

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

Nexusguard DNS Protection service protects mission-critical online services from all DNS attacks and malicious queries. The solution leverages Nexusguard's globally distributed network of scrubbing centers to resolve incoming DNS queries quickly and reliably.

How Does It Work?

DNS servers are often targeted by DDoS attacks, for example, by launching many DNS requests to flood a targeted name server. If perpetrators can successfully disrupt DNS services, all the victims' servers could effectively disappear from the Internet, thereby causing the desired denial of service.

As such, protecting DNS servers from DNS attacks is equally as important as protecting web application servers and other critical components of your IT infrastructure. Built on a globally-distributed Anycast network, DP is designed to provide 24x7 DNS availability, improve user responsiveness and provide the resiliency to defend against the largest DNS-based DDoS attacks.

DP leverages Nexusguard's highly scalable, fully redundant and globally distributed DNS platform with sufficient capacity to absorb large DNS-based DDoS attacks while responding to legitimate user requests. This ensures that organizations can maintain user access to websites and applications, even when they are the target of a DDoS attack. CSPs and enterprises can implement Nexusguard DNS as their authoritative or secondary DNS, either by replacing or augmenting their existing DNS infrastructure. In either case, organisations receive a scalable and secure DNS network to ensure the best possible web experience for their users.

Key Features

Always-On Protection
Protects any DNS domain by hosting DNS domains on cloud to share traffic load

Compliance with DNSSEC Mandates
Supports DNSSEC to enhance data integrity and cryptographic authentication of DNS data

Supports AXFR
Operate as Primary or Secondary Name Server

Flat-Fee Structure
Unlimited queries and domain records

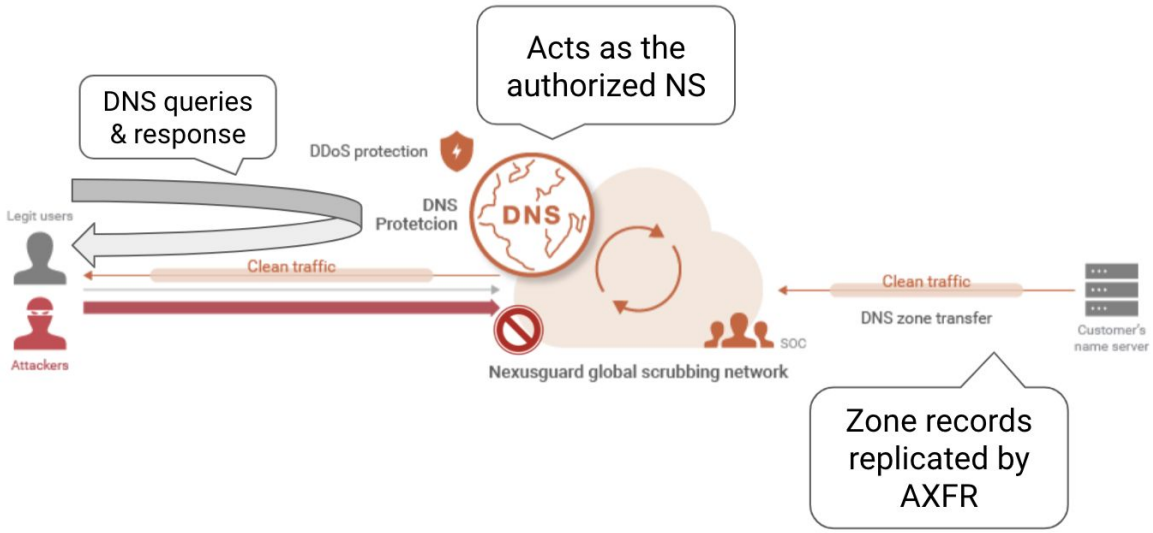
Uptime Assurance
100% Availability SLA

Deployment Method

Hosting Model

In the hosting model, the customer designates Nexusguard DNS as their secondary nameserver by transferring its zone files to Nexusguard DNS via zone file transfer over AXFR protocol. Alternatively, the customer can have its zone files hosted at Nexusguard DNS.

Mapping of an authorized name server to the Nexusguard DNS is achieved through the DNS registry. When accomplished, the IP address of the customer's authoritative nameserver is hidden from potential attackers. All legitimate DNS queries will then be handled and answered by Nexusguard's cloud, while filtering out malicious queries.



Reverse Proxy Model

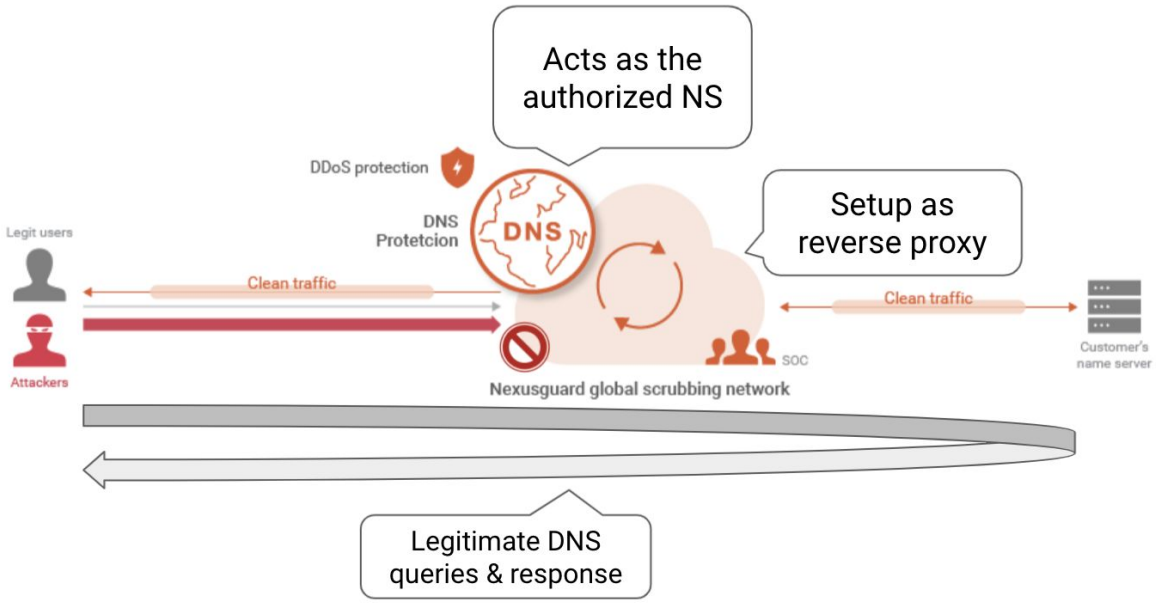
In the reverse proxy model, Nexusguard DNS is set as the authoritative nameserver for the customer's name zone, either replacing or complementing the the existing servers. In this setup, Nexusguard's DNS represents a recursive server containing cached data about the customer's name zone.

If our nameserver lacks information on the same record, it will send a request to the upstream server and cache the received reply. Along with that, all possible variants of attack vector growth are taken into account.

In addition, the reverse proxy model not only offers Always-on DDoS protection to ensure high availability of name servers, but also adds another layer of protection to TCP/UDP based DNS traffic through Nexusguard's DP proxy service to upstream name servers. The following suite of mitigation tools are provided to nullify attacks:

- Allow/Deny IP addresses - allows trusted IPs only and blocks known attacks or unauthorized sources
- Anti-flood - mitigates flooding and drops invalid DNS packets
- Traffic Policing - rate limits traffic to destination name servers

nexusguard.com
contact@nexusguard.com



Types of Attack Mitigated

NXDomain
A DNS server is flooded with queries for a non-existent domain (aka NXDomain). The recursive server doesn't know the domain does not exist until it receives responses from the queries it initiates. The process consumes valuable server resources and overloads the cache. As a result, legitimate DNS queries are dropped or delayed.

Phantom Domain
Attackers set up phantom domains that don't respond to DNS queries. A recursive DNS server is forced to wait for responses, which consumes server resources, resulting in delayed or dropped responses.

Random Sub-domain
Randomly generated attacks target sub-domains on a legitimate domain. To resolve the domains, a recursive DNS server spawns concurrent queries that inevitably hit the limit, while authoritative DNS servers experience DoS.

Look-up Domain
Attackers set up domains that establish TCP-based connections with a recursive DNS server and keep the connections alive with random responses. The server is tied up and eventually exhausts its resources.

Visibility and Control

At Nexusguard's easy-to-use Customer Portal, you can:

- Add, remove and manage domains under protection
- Configure domain settings
- Import and export zone files
- Replicate DNS data using DNS zone transfer
- Manage SOA and NS records

Solution Benefits

- Provides "always-on" protection enabled by Nexusguard's enormous DNS server capacity, which filters all incoming DNS queries and absorbs attacks
- Easily configured and deployed via Nexusguard's DNS Protection Service Customer Portal
- Guaranteed 24x7 availability keeps users connected to websites and applications
- Improved responsiveness to DNS requests connects users with websites and applications in less time
- Better defence against DNS-based DDoS attacks
- Predictable costs with protection against spikes in attack traffic
- Reduced operational overhead to maintain a global DNS infrastructure
- Simplified management through the Portal