NEXUSGUARD®

Global Leader in DDoS Mitigation

DNS Protection

What is DNS Protection?

The Nexusguard Cybersecurity Platform encompasses three essential elements: Application Protection, Origin Protection, and DNS Protection.

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?

In a typical recursive DNS query, a client requests the resolution of a domain name or the reverse resolution of an IP address on a local DNS server. The DNS server performs the queries on behalf of the client and returns a response packet with the correct information or an error message. The specification does not allow for unsolicited responses. In a DNS amplification attack, the main indicator is a query response without a matching request.

Residing in front of a customer's infrastructure[1], Nexusguard DNS Protection Service replaces the DNS server by directly fetching zone records from the customer's servers and hosting them in our globally distributed scrubbing centers. The client first has to change the nameservers for the domain and point the domain name to Nexusguard's name servers, which can be accomplished at Nexusguard's self-service Customer Portal.

As the destination for all incoming queries, Nexusguard's cloud-based DNS servers absorb all DNS attacks, while filtering out malicious traffic from incoming queries. Your DNS servers never need to respond to any malicious DNS query — Nexusguard handles everything. Our service protects against direct attacks on DNS services, and abuses of server vulnerabilities as a leverage to launch DNS amplification attacks on other servers.

1 It is up to the Customer to assign Nexusguard to host its DNS server by authorizing it as primary nameserver, or to remain in control of its DNS server but allowing Nexusguard to perform a zone transfer to become secondary nameserver by fetching SOA record.

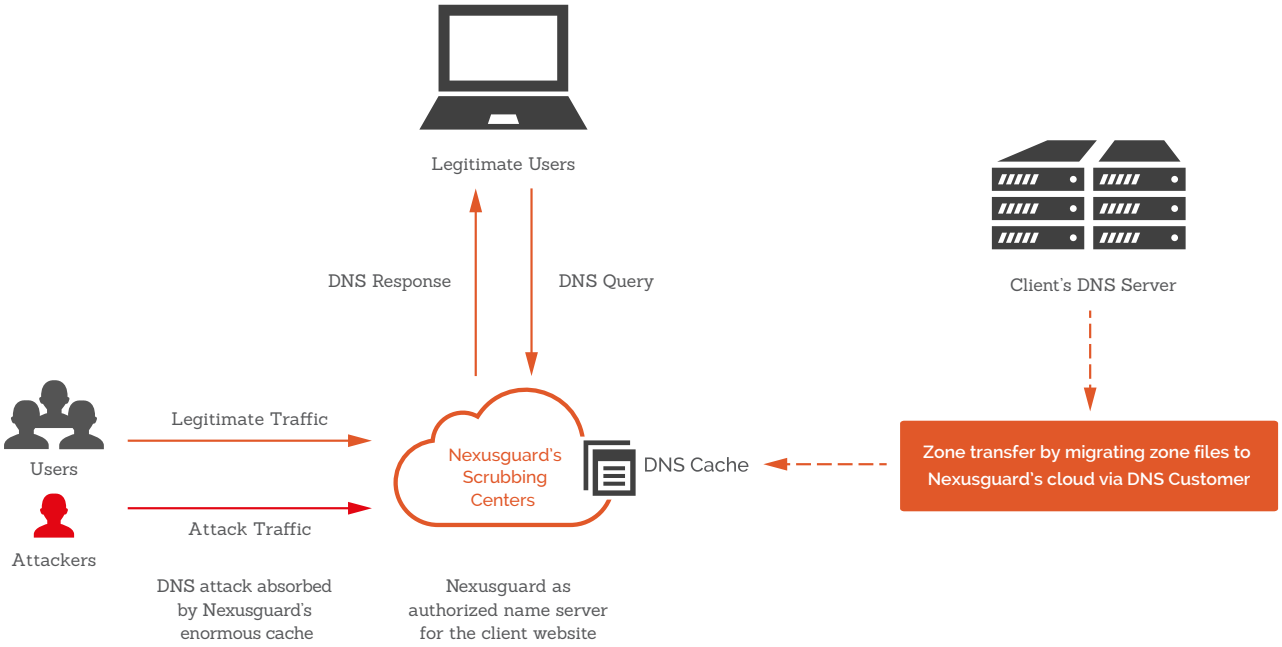
If Nexusguard hosts the Customer's DNS server as primary nameserver, the Customer Portal will provide an interface for the Customer to add/edit/delete DNS records, or add/delete zones when records have to be updated.

However, if the Customer prefers managing its DNS server on its own, the Customer is unable to make the above changes on the Customer Portal, since the Customer's DNS server remains as primary nameserver. Nexusguard's DNS server as secondary nameserver will synchronize with the changes made by the Customer to its DNS server.

nexusguard.com

sales@nexusguard.com

Always-on DNS Protection



Deployment Method

Deployment is easy. All you have to do is migrate zone files on the Customer Portal from your DNS server to Nexusguard's DDoS-proof DNS servers. All legitimate DNS queries will then be handled and answered by Nexusguard's cloud, while filtering out malicious queries.

Types of DNS Attacks Mitigated

- DNS Amplification: The most common form of attack occurs when a DNS response is significantly larger than a query. For instance, if an "open resolver" receives a query packet containing a large buffer advertisement from a "spoofed" requesting IP address, its reply can be quite large, resulting in a denial-of-service attack on the DNS server.

- 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.

Solution Benefits

- Provides "always-on" protection enabled by our enormous DNS server capacity, which filters all incoming DNS queries and absorbs attacks
- Improves DNS responses for faster page loads
- Is easily configured and deployed via Nexusguard's DNS Protection Service Customer Portal
- No surprise overage charges as a result of malicious or flood-type DNS requests

Visibility & 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

Security Benefits

No DNS server cache snooping allowed

DNS cache snooping is when someone queries a DNS server in attempts to find out (snoop) if the DNS server has a specific DNS record cached, and thereby deduce if the DNS server's owner (or its users) have recently visited a specific site. This may reveal information about the DNS server's owner, such as what vendor, bank, service provider, etc. they use. Especially if this is confirmed (snooped) multiple times over a period. This method could even be used to gather statistical information - for example at what time does the DNS server's owner typically access his online banking website. The cached DNS record's remaining TTL value can provide very accurate data for this. To get rid of this possible security loophole, Nexusguard does not cache any DNS records while acting as the authoritative DNS servers on behalf of a client.

Dynamic update security threats eliminated

DNS dynamic updates are a great convenience for the DNS administrator. Instead of being required to manually create records for all your clients and servers, all you need to do is enable dynamic DNS updates on both the clients and servers. Despite that, there are security concerns over dynamic DNS. If the dynamic update process is compromised, the attacker can potentially change the information in key resource records so that names can be redirected to servers that the attacker has set up to attain the attacker's goals. Another example is that the attacker can do is create a simple DoS attack by just deleting key records, such as records for the DNS server or the domain controllers. Nexusguard's DNS Protection platform does not permit dynamic updates and so there is no such dynamic update threat.

Fingerprinting tools blocked

Fingerprinting is a technique for identifying the differences among implementations of the same networking software specification, be it applications, operating systems or TCP/IP stacks. There are a number of tools that can be used to identify different versions of the same application such as fpdns, Nmap, and Nessus. Nonetheless, these fingerprinting tools are unable to identify any information about the software or operating systems that our clients are using. As such, attackers cannot check for the existence of hosts running versions with vulnerabilities.

More secure zone transfer

There is a security issue associated with the zone transfer process since DNS data can be used to decipher the topology of a company's network. The information obtained can be used for malicious exploitation such as DNS poisoning/ spoofing. To make the zone transfer between DNS Nameservers more secure, we primarily use SSL to encrypt the communications in between, followed by DNS Transaction Signatures (TSIG). As the second level of securing zone transfer, DNS TSIG ensures the information from the primary name server is actually from the primary name server. To protect your DNS Protection Service account from unwanted access, you can activate two-factor authentication. Once enabled you are prompted to provide a verification code in addition to the username and password when you log in. The verification code is generated by an authenticator app.