QRATOR LABS

QRATOR.SecureDNS

Solution's Guide

qrator.net

Qrator.SecureDNS

High-availability false-safe DNS service designed to mitigate DNS-based attacks and improve resilience and availability of DNS infrastructure

Understanding the Risk and Importance of DNS hardening

Like many other Internet protocols, DNS wasn't designed with security in mind which makes DNS infrastructure vulnerable to a wide range of DDoS attacks. Yet despite being a vital component of business infrastructure DNS hardening often turns out to be overlooked.

Why are DNS attacks dangerous?

Instead of attacking a website itself, attackers can target availability and stability of a network's DNS server containing IP addresses for every website on the Internet. In case of a DNS attack, users' browsers will not be able to determine an IP address that will make a website unavailable. An attacker can constantly generate DNS queries for a DNS server in order to overload its resources.

Without a special protection, the only way to mitigate such an attack is to increase servers' power. However, a constant inc-rease in capacity may result in leveraging DNS server for carrying out further DDoS attacks on other websites. Failure of a DNS server can lead to partial or complete unavailability of a web resource.

Best-in-class Ultra-Fast DNS protection

Distributed and reliable cloud Qrator.SecureDNS is an integral part of our enterprise solution for continuous online business availability.

Qrator.SecureDNS provides minimal response time and a high level of protection against even the most complex and high-speed DDoS attacks.

Qrator.SecureDNS Key Benefits

Takes seconds to deploy with the Unique Reverse Proxy feature

Truncate functionality protects enterprise DNS servers against IoT-based DDoS attacks

Qrator Labs Anycast network reduces DNS query latency

Make your DNS server available 24/7

Cloud solution based on Qrator Labs network

There is no need to install additional software or purchase hardware. Our global anycast network ensures high availability at no additional cost, and in case of a DNS attack at least one server remains up and constantly running.

Additional Qrator Labs DNS Server

It implements advanced DNS attack mitigation techniques and a special bot request processing logic working differently from the logic of handling legitimate user requests.

Easy to connect

Configure DNS security choosing one of two implementation options: Qrator Secondary DNS (protection with full disclosure of a domain zone) or Qrator DNS Reverse Proxy (protection without full disclosure of a domain zone).

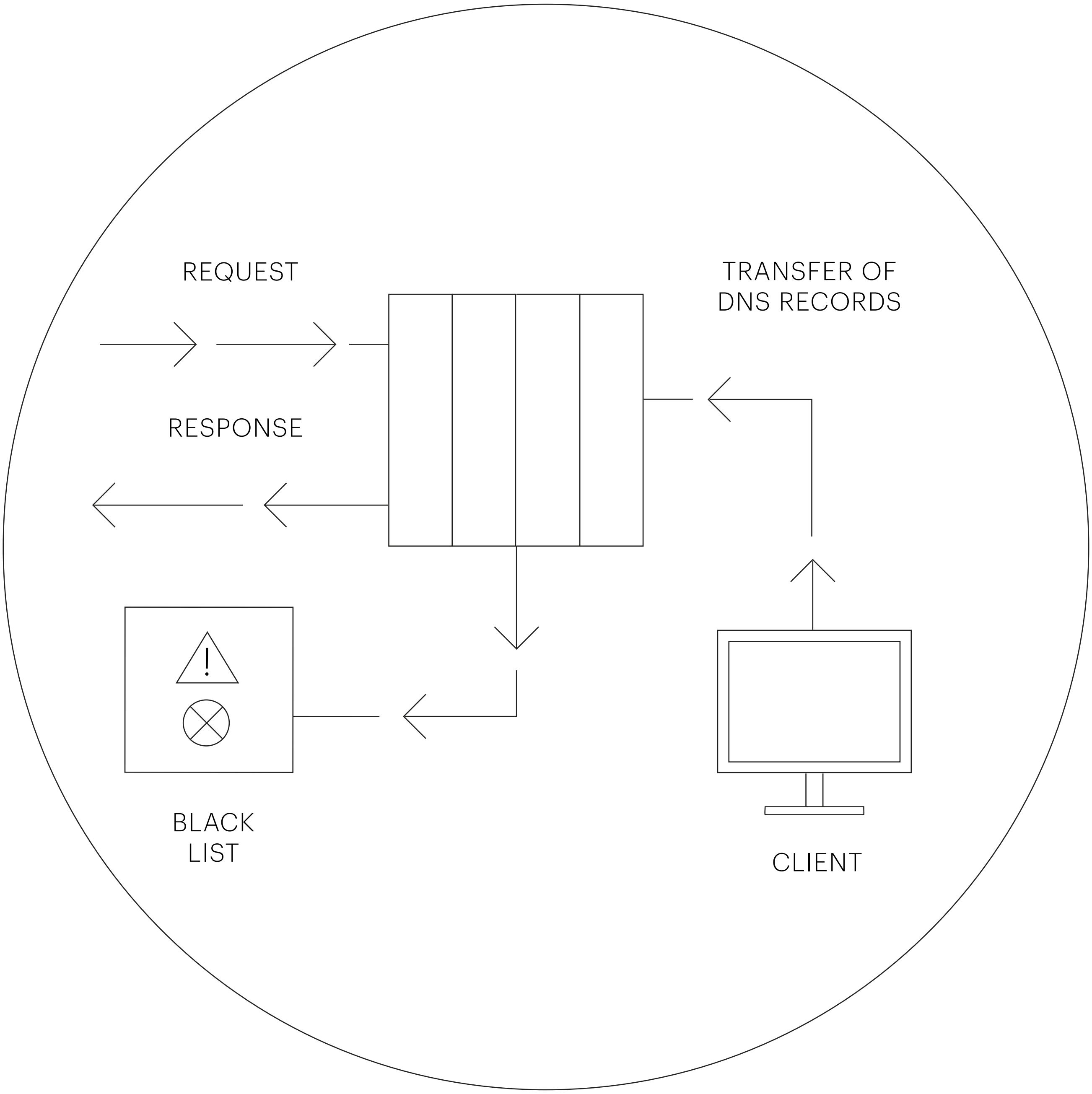
Built-in DNSSEC

The DNSSEC protocol is a DNS Security Extension created to increase security level of DNS record authentication using digital signatures. Qrator.SecureDNS provides built-in support of DNSSEC to minimize risks of attacks and improve data integrity.

Detailed DNS traffic analysis

Advanced DNS traffic analytics is always available online in Qrator Labs dashboard. Customers can generate detailed DNS statistics reports in their personal accounts filtered by response statuses, request types, etc.

How it works


REQUEST
TRANSFER OF DNS RECORDS
RESPONSE
BLACK LIST
CLIENT

Easy deployment with better performance and availability

QRATOR SECONDARY DNS
(protection WITH full disclosure of a domain zone)

- A client allows transfer of his domain zone from the current NS server to the Qrator Labs server ns.qrator.net.
- A client specifies an IP address allocated by Qrator Labs as the authoritative server address for its zone.
- Qrator Labs configures transfer of a domain zone file from the main client's NS server which address is no longer known to attackers (Hidden Primary).

QRATOR SECONDARY DNS
(protection WITHOUT full disclosure of a domain zone)

- Applies when a client does not have an opportunity to provide control of a domain zone.
- A client reports Qrator Labs on IP address(-es) of authoritative servers (or a Hidden Primary NS server) and specifies an IP address allocated by Qrator Labs as the address of an authoritative server for the own zone.
- With this connection scenario, a Qrator Labs NS server will act as a recursor server with a cache of data about a client's connected zone.
- If Qrator Labs server does not have information about a record, it will send a request to an upstream server and keep a response.

QRATOR LABS

qrator.net
sales@qrator.net
+420 602 558 144