



qrator.net

QRATOR.SECONDARYDNS

Resilient secondary DNS server



CURATOR.SECONDARYDNS

A secondary authoritative DNS server built to maintain uninterrupted availability of your DNS infrastructure.

Availability of online services depends on DNS

Virtually all network interactions — whether accessing websites, email, or internal corporate services — begin with a DNS query that translates a human-readable domain name into its corresponding IP address.

This often makes DNS a single point of failure in a company's infrastructure. An attacker only needs to disable a DNS server to make the rest of the resources effectively inaccessible to users. While the services themselves may remain fully operational, users won't be able to connect to them without DNS resolving their IP addresses.

And the problem goes beyond attacks — it also includes technical failures in data centers, hardware outages, or connectivity issues. In any of these scenarios, the failure of the DNS server responsible for a company's domain can result in most of its online services becoming unavailable.

Building resilient DNS infrastructure

The solution lies in creating a distributed, fault-tolerant DNS infrastructure capable of withstanding the failure of individual components without compromising service availability. This requires deploying multiple authoritative DNS servers using Anycast architecture, and properly setting up interactions between primary and secondary DNS servers.

One of the key components of a reliable DNS infrastructure is a resilient secondary DNS server — one that can take over the processing of incoming DNS queries while withstanding even the largest-scale attacks. This is exactly what we offer our customers with QRATOR.SECONDARYDNS.



Key advantages of QRATOR.SECONDARYDNS

1 Guaranteed DNS availability

The Anycast architecture gives QRATOR.SECONDARYDNS the same 99.999% availability level as the entire QRATOR filtering network — thanks to automatic traffic distribution and resilience against network attacks of any type or intensity.

2 Full customer control over the domain zone

The secondary DNS server operates in read-only mode — all DNS record changes are made on the primary DNS server and replicated to the secondary using zone transfer protocols (AXFR/IXFR). This ensures the customer retains full control over the domain zone.

3 Handling all incoming DNS queries

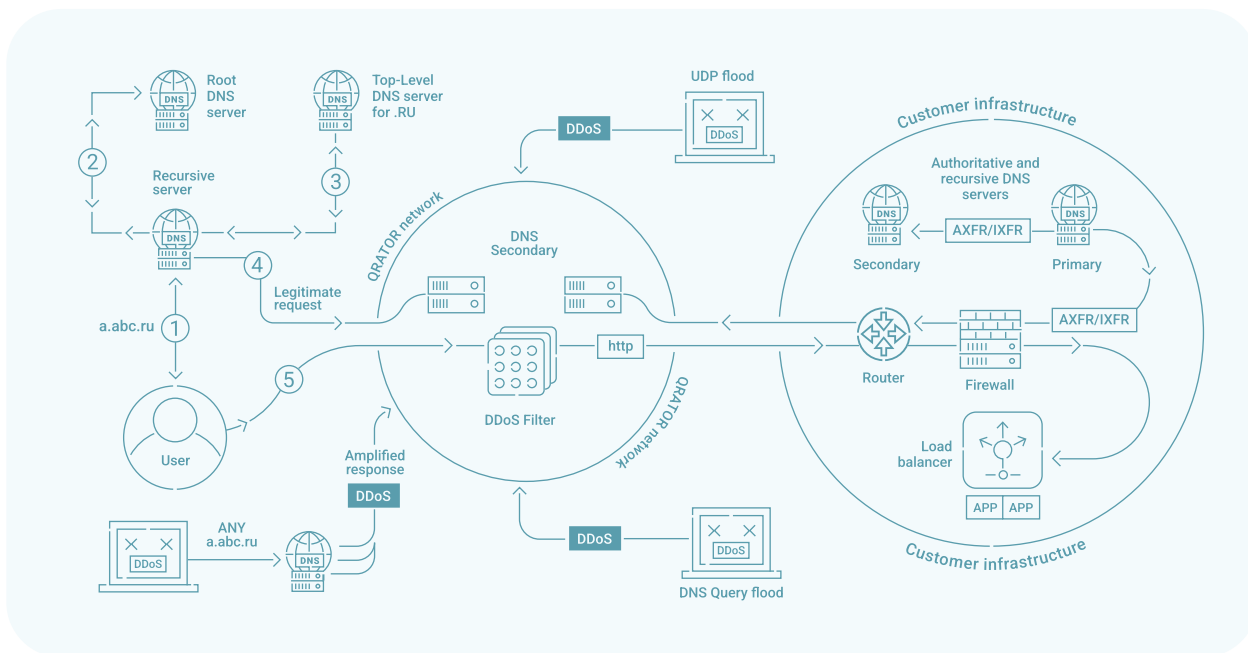
If needed, QRATOR.SECONDARYDNS can fully take over the processing of incoming DNS queries, completely isolating the primary DNS server from external traffic. This provides maximum protection by eliminating direct external access to the primary server.

4 Fast onboarding

QRATOR.SECONDARYDNS can be deployed in just three simple steps and takes around 15 minutes to set up.



How QRATOR.SECONDARYDNS works



How to connect QRATOR.SECONDARYDNS

1

Configure DNS Notify for the QRATOR secondary DNS server

2

Provide QRATOR with a list of zones to protect

3

Add the new NS server at your domain registrar and specify the dedicated QRATOR IP address



QRATOR.SECONDARYDNS capabilities for building a resilient authoritative DNS architecture

1 Continuous availability of authoritative DNS infrastructure

The global QRATOR filtering network, built on Anycast architecture, ensures guaranteed availability of QRATOR.SECONDARYDNS and enables complete isolation of the customer's primary DNS server from external traffic. In the event of an attack or failure, at least one DNS server remains operational and continues processing DNS queries — regardless of the type or scale of the incident.

2 DNSSEC support

QRATOR.SECONDARYDNS supports the DNSSEC protocol — a security extension that protects the integrity of DNS records using digital signatures. DNSSEC minimizes the risk of DNS spoofing attacks and ensures the authenticity of transmitted data, while full control over records and signatures remains with the customer.

3 Detailed DNS traffic analytics

The QRATOR.SECONDARYDNS dashboard features advanced DNS traffic analytics with detailed reports filtered by response codes, query types, and other key parameters.

4 Easy integration

QRATOR.SECONDARYDNS requires no additional software installation or hardware purchases. The service is set up in three simple steps, and onboarding can take as little as 15 minutes.

The logo consists of two overlapping circles, the left one being larger and partially behind the right one, both rendered in white outlines.

QRATORLABS

qrator.net