QRATOR LABS

qrator.net

QRATOR.ANTIDDOS

Solution’s guide

Industry Leading DDoS Attacks Mitigation

Qrator Availability Network allows small and large businesses to protect their applications from all types of DDoS attacks, regardless of bandwidth or complexity.

Qrator Labs own unique geo-distributed filtering network based on united BGP Anycast architecture provides reliable, low latency web infrastructure protection from any network attacks leading to unavailability of web resources.

Empowering businesses with high network availability and clients loyalty through cloud-based DDoS mitigation

With 15 scrubbing centers around the globe and throughput of more than 4,000 Gbps Qrator Labs filtering network ensures excellent connectivity in the regions of North America, LatAm, Europe, MENA, and APAC. Qrator Labs filtering centers are located in global points of the Internet traffic concentration, connected to transcontinental TIER1 providers as well as leading regional backbone Internet providers.

Why QRATOR.ANTIDDOS

1 **Mitigating attacks at all OSI layers, including L7**

The Qrator Labs network automatically provides security up to and including the L7 (application layer) on all billing plans and for all customers

2 **99.95% the highest SLA in the industry for availability of customer´s infrastructure**

Customers don't pay for the service in case it does not meet the declared quality (guaranteed by a contract)

3 BGP-Anycast architecture

BGP-Anycast guarantees a geographically distributed, fault-tolerant network to protect applications with a high degree of connectivity. Failure of any filtering node will have no impact on the quality of service and performance of customers' applications due to traffic balancing between major Internet service providers

4 Easy connection

Any web infrastructure may be protected within 15 minutes with two connection methods: DNS and BGP

5 Always-on 24/7 automatic protection

No need for manual configuration or involvement of qualified specialists to get reliable protection against complex DDoS attacks

6 Easy integration with mobile apps and APIs

The Qrator Labs API can be integrated with your authentication system, database or device monitoring service providing a wide range of system managing features.

7 Transparency for legitimate users

We don't use CAPTCHA or other annoying user checks

8 24/7/365 technical support

Online Ticket System Dashboard, phone, email, and chat support. Response time is less than 15 minutes to every customer's request

9 SSL (PCI-DSS ready)

HTTPS filtration with no key disclosure allows to analyze and filter HTTPS traffic without disclosing encryption keys and without breaching the customer’s security polcies

10 No effect on Search Engine Optimization

Can improve a website's SEO by reducing page load times and improving security

3 levels of traffic filtering:

1 Traffic redirection of the protected site to the Qrator Labs network

Traffic is analyzed at all layers of the protocol stack, including the application layer (the seventh layer of the OSI model). The traffic of application-level attacks closely resembles the activity of ordinary users, which makes them very hard to detect and neutralize.

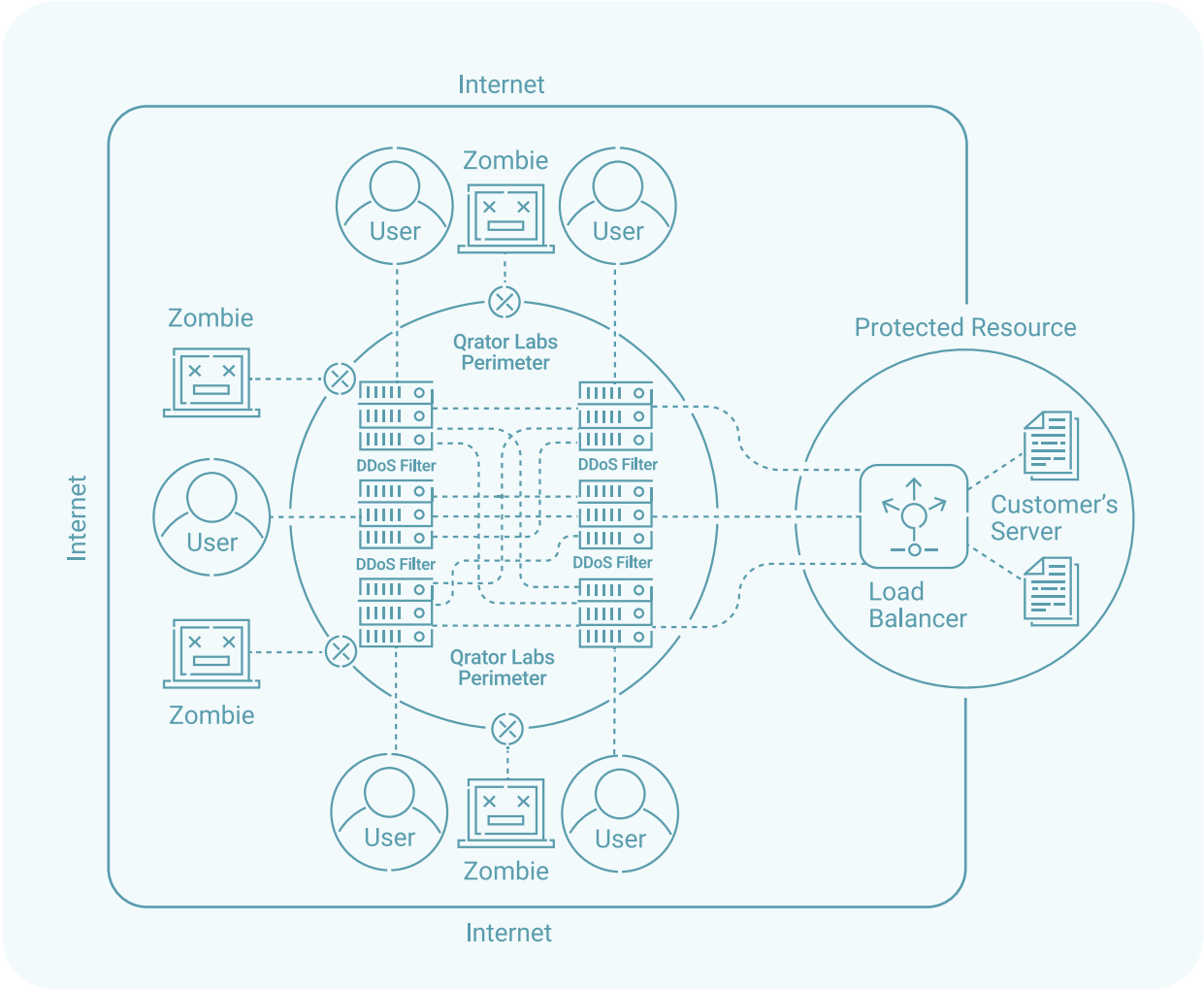
2 Multilayer traffic filtering using behavioral, heuristic, and signature algorithms

By continuously studying the traffic patterns regardless of the DDoS attacks, Qrator Labs improves the algorithms and makes online adjustments to the available filtering methods, allowing it to detect any anomalies and respond immediately to DDoS attacks.

3 Directing clean traffic to the protected site

The filtered traffic is forwarded to the protected site either through the public Internet or through a specially deployed L2 VPN. DDoS attack traffic is blocked at the perimeter of the Qrator Labs network, never reaching the client's resources. Qrator Labs network operation is completely invisible, both to the business and its website visitors, and Qrator Labs clients will eventually learn about the attack only from the reports in their personal accounts.

How Qrator.AntiDDoS Works



100% SLA for Qrator Labs platform availability

Free 7-day trial period

You get a 7-day trial period in case your application is not under a DDoS attack, or a 1-day trial period if you come under attack.

Comprehensible online reports in the Personal Dashboard

You can access the results of the analysis of your application's traffic for any period you've been using our services. Using the API, you can connect your existing monitoring system (Nagios, Zabbix etc.) with Qrator Labs and receive notifications on the incidents in the format most convenient for you.

Integration with monitoring systems

Using the API, you can connect your existing SOC / monitoring system / SIEM with Qrator Labs and receive notifications on the incidents in the format most convenient for you.

Minimum false-positive incidents: no more than 5% during an attack

The algorithms implemented by Qrator Labs allow the determnation of the cause for increasing resource attendance — whether it is a DDoS attack or rising interest from the visitors.

Qrator Labs reaction time to a DDoS-attack — up to 30 seconds in 97% of attacks vectors

4 EASY STEPS TO ENABLE DDoS ATTACKS MITIGATION WITHIN 15 MINUTES

1

Register in your Personal Dashboard

2

Get a Qrator IP

3

Install an SSL certificate chain

4

Redirect your traffic to the Qrator Labs IP

QRATOR LABS

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