Qrator selects Arista as the critical technology foundation for DDoS mitigation service to deliver improved reliability whilst reducing cost and complexity.

Highlights

Challenge

Following massive customer growth and international expansion, Qrator needed a high performance and ultra-reliable switching architecture as a critical component underpinning its innovative DDoS mitigation services.

Solutions

- Arista 7150S Family Switches
- Arista EOS® Extensibility

Results

- Line rate performance without packet dropping to ensure highest levels of service availability
- EOS architecture supported installation of critical third-party daemon to deliver flowspec functionality
- 75% reduction in CAPEX with higher performance than alternative load-balancer and router vendors
- Lower latency, higher reliability, and room to scale to a 100Gbps capable network design

Qrator is one of Eastern Europe's most widely used and highly regarded Distributed Denial of Service mitigation service providers. Following major international expansion, Qrator has upgraded its critical infrastructure to innovative software and Arista Networks technology which has offered an efficient, scalable and cost-efficient foundation for future innovation whilst delivering critical levels of reliability.

QRATOR LABS

Project Background

In 2006 Alexander Lyamin, then a staff member at the Moscow State University, began a research initiative focused on the problems presented by Distributed Denial of Service attacks. For several years his team studied the mechanics of DDoS attacks and developed algorithms and measures that would allow users to counter these potentially devastating threats effectively. By early 2009, the team had created a specialized application capable of automatic attack detection and filtering. To field-test the algorithms and hardware they developed, Lyamin released an open beta of the product. For 18 months, anyone vulnerable to DDoS attacks could test-drive the technology at no charge, and over that period more than 600 companies and individuals took advantage of this opportunity, allowing Lyamin and his developers to assess the efficacy of the application in actual DDoS attacks, collect unique statistics, and fine-tune algorithms. In 2009, Lyamin founded Qrator Labs, turning a highly innovative research project into a successful commercial DDoS mitigation cloud which is today one of the largest services of its kind in Eastern Europe, providing protection for organizations in financial services, media, gaming, government and many other areas.

Challenge

With an established regional customer base, from 2014 onwards Qrator took the opportunity to expand past its borders to meet the increasing global demand for pre-emptive, comprehensive DDoS protection at flexible, affordable pricing. This expansion phase saw the creation of offices and supporting data centre infrastructure in the US, Netherlands, Sweden, Kazakhstan and Hong Kong.

With more clients using its DDoS services, Qrator began to look at how it could scale its technology to cope with growing customer numbers and increased volumes of internet traffic. As Dmitry Shemonaev, Head of NOC (Network Operations Center) for Qrator explains, "We have our filtration node connected directly to the upstream internet service provider's equipment and they have routers and switches with load balancing capabilities although it was never directly managed by ourselves."

"This configuration worked, but with our almost exponential growth, we need to have more direct control over this process to deliver the quality of service, along with the metrics we collect and monitor that are necessary to react as quickly as possible to attacks."

Mitigating enormous and complex DDoS attacks requires significant uplink connection bandwidth and computing resources. For Qrator, the plan was to increase the number of points of presence it operates. However, whilst evaluating its options, it identified that using ISPs equipment was very expensive. "The huge monthly costs simply weren't suitable for our company, which doesn't have any third-party financing and grows the business on its own, using only our profits," says Mr. Shemonaev.

With this in mind, it was decided that Qrator would need to deploy its own load balancers at each PoP. Qrator Labs created set criteria to help make the selection. Each device would need to support ECMP with source and destination IP-address, plus a sufficient amount of 10Gb ports for interconnecting its hardware with uplinks and clients. The platform must have no packet loss at the load level close to the line rate of the hardware. Besides, the cost was a major consideration.

Solution

The company initially considered specialist load balancers from vendors including F5 Networks but these proved both expensive and offered features around traffic management that they simply did not need or were duplicated within its own DDoS application. Consideration was made around Juniper MX, and Cisco ASR routers but high costs along with larger rack space and electricity consumption plus added complexity of operation were negatives - as was the inability to inspect OSI L7 traffic.

Although unorthodox, a layer 3 switch could offer a perfect solution although Mr. Shemonaev points out, "Switches tend to have smaller routing table size which could potentially be negative, so it was not an option we had evaluated previously which meant we were dealing with a real unknown." However, based on the rapid growth of Qrator, the longer term benefits included the ability to easily scale whilst keeping costs down prompting Qrator to run a set of deep tests around various technology alternatives.

As Dmitry Shemonaev explains, "We evaluated several separate types of equipment from Cisco, Juniper, Arista, and Extreme. Using traffic generators, we closely watched the packet loss as the load rose close to the hardware line rate. Additionally, we tested ECMP and PBR on numbers close to the line rate."

During the test, some of the equipment suffered from unacceptable levels of packet loss which is critical for a service designed to filter legitimately from attack traffic. In tests at higher ECMP traffic rates of between 100-500 Mbits, some of the devices simply shut down without warning.

"In our tests, the Arista switch was the only one that proved itself best on both the hardware and software side," notes Mr. Shemonaev.

For the Qrator service to operate at optimum efficiency, it needed to manage BGP flow spec, an extension to the BGP protocol that allows the transfer of the firewall filter rules from one machine to another using BGP protocol. Although the Arista switch did not support the BGP daemon required, the open nature of the Arista EOS architecture meant that Qrator could install a third-party daemon - ExaBGP for flowspec injection, into its uplinks.

Qrator has added a number of additional applications and extensions directly into the Arista switch to enhance the functionality of its DDoS services. As an incredibly technical solution, Qrator occasionally ran into issues when trying to work around the limitations of smaller route tables and ECMP and turned to Arista for help, "Not only did we get an answer but Arista offered an SDK and an engineer to help us with setup," says Dmitry Shemonaev. "With the support of SDK, we found that our solution to updating routes did not implement correctly with ECMP, so we reported that and within a week Arista delivered! Again, a pleasure to work with such a company."

Conclusion

With the fundamental technical limitations overcome and the Arista switching layer providing both the performance and reliability demanded of the Qrator service, the company began rolling out Arista switches to all of its PoPs. With the custom created daemons and Qrator software running within each switch, the service is also able to deliver the custom telemetry it needs to identify and block DDoS attacks.

According to Head of Qrator Labs NOC, the goals of the upgrade project have been comfortably met, and the choice of using Arista layer 3 switching has proven a viable foundation for continued expansion.

"Just looking at the Arista switch utilisation and reliability, we now have an uptime of more than 1000 days- it just doesn't drop," says Dmitry Shemonaev, "We had an accident in January of 2016 when a switch lost its memory (NAND flash), and although it continued working we had to restart it."

"However, we did not know if it would normally work after going back online since everything was stored within the switch flash memory. We contacted Arista TAC, during which time the switch restarted and has performed flawlessly ever since."

With growth continuing including a major new contract with a top 3 global internet retailer, Qrator is now looking at the future. "Arista offered us good value, solved our problems on the hardware and software side and has proven very stable," says Mr. Shemonaev, "For us the future is a fully 100Gbps architecture, so our plan is to bring the next generation of Arista kit back into our labs and put it through its paces – and we know that behind us we have the Arista engineers and support team that are simply awesome!"

Santa Clara—Corporate Headquarters
5453 Great America Parkway,
Santa Clara, CA 95054

Phone: +1-408-547-5500
Fax: +1-408-538-8920
Email: info@arista.com

Ireland—International Headquarters
3130 Atlantic Avenue
Westpark Business Campus
Shannon, Co. Clare
Ireland

Vancouver—R&D Office
9200 Glenlyon Pkwy, Unit 300
Burnaby, British Columbia
Canada V5J 5J8

San Francisco—R&D and Sales Office 1390
Market Street, Suite 800
San Francisco, CA 94102

India—R&D Office
Global Tech Park, Tower A & B, 11th Floor
Marathahalli Outer Ring Road
Devarabeesanahalli Village, Varthur Hobli
Bangalore, India 560103

Singapore—APAC Administrative Office
9 Temasek Boulevard
#29-01, Suntec Tower Two
Singapore 038989

Nashua—R&D Office
10 Tara Boulevard
Nashua, NH 03062