



REAL-TIME DDoS MITIGATION GIVES LINODE AN EDGE IN COMPETITIVE CLOUD MARKET

Summary

Company:

Linode

Industry:

Web Services

Business Challenges:

Offer real-time DDoS mitigation as a foundational service to differentiate business in a highly competitive cloud infrastructure market.

Technology Solution:

- MX960 5G Universal Routing Platform
- QFX10002 Switch
- Corero SmartWall Threat Defense Director

Business Results:

- Ensured service quality and created a competitive service differentiator with automated DDoS mitigation
- Eliminated the need for stressful and ineffective manual intervention for DDoS attacks
- Added DDoS detection while maximizing network infrastructure investment

When it comes to cloud, developers have exacting standards, and premium service is exactly what Linode delivers. Linode is a cloud provider for developers who demand maximum performance, reliability, and value for their cloud applications. A privately held, open cloud provider, Linode operates 11 data centers around the world. More than 800,000 developers globally depend on Linode to build and scale their server infrastructure.

Cloud Servers Made Easy

Developers can get a Linux virtual server running in seconds from the Linode cloud. Developers can deploy, boot, resize, and clone virtual servers with just a few clicks. Linode calls its infrastructure “drool worthy,” with native solid-state drive (SSD) storage, a 40GbE network, and blazing fast processors.

Linode has added real-time DDoS mitigation services to its list of drool-worthy features. DDoS attacks are a scourge for any business, as criminals, nation-states, and protesters disrupt the digital operations of the intended target as well as wreaking havoc on other customers at the same provider.

“Customers have told us that DDoS protection is a top priority,” says Dan Spataro, director of infrastructure operations at Linode. “Offering DDoS-mitigation-as-a-service based on Juniper and Corero is a competitive advantage for Linode.”

“We still see about 1000 attacks over a three-month period. But those attacks don’t take customers down because we can successfully mitigate them with Juniper and Corero.”

- Dan Spataro, director of infrastructure operations, Linode

Protect Against DDoS Disruptions

“We aren’t seeing an uptick in the frequency of attacks, but we’re seeing greater complexity and volume in DDoS attacks,” says Spataro. “The potential impact of DDoS attacks is increasing as attacks get smarter.”

After a DDoS attack a few years ago that disrupted operations, Linode re-architected its Internet edge to use the Juniper Networks® MX960 5G Universal Routing Platform for high-performance scalable routing. But as DDoS attacks continued to pummel the cloud provider, manual DDoS mitigation was no longer

effective. Instead of creating a stressful, all-hands-on-deck situation every time the provider was hit, Linode wanted a more proactive approach that would allow it to automatically block and mitigate even the largest DDoS attacks in seconds.

“We needed more granular control over DDoS attacks,” Spataro says. “With static DDoS mitigation, we could keep our data centers up, but our customers would still feel the pain. We wanted to limit collateral damage.”

Leverage Existing Network

Spataro discovered a solution at Juniper’s 2018 NXTWORK conference. The addition of Corero SmartWall Threat Defense Director, in combination with the MX960 routing platforms that Linode already used, would provide real-time DDoS mitigation. “We were one of the first proof-of-concept tests of the combined solution,” says Spataro.

Linode can dynamically scale DDoS mitigation to the size of the attack. Linode’s MX960 routers monitor ingress traffic via sampled mirrors (which are essentially samples of the packets coming into the router). The routers forward the sampled traffic to Corero, which inspects every packet in search of a DDoS attack. All of this occurs in seconds.

If an attack is detected, Corero automatically generates firewall-match filters so the MX960 routers can mitigate the event. Once normal operations resume, network telemetry continues to flow from the Juniper routers to monitor for the next attack. And because MX960 can filter traffic in real time, legitimate traffic flows on to its destination without any performance degradation.

“Offering DDoS-mitigation-as-a-service based on Juniper and Corero is a competitive advantage for Linode.”

- Dan Spataro, director of infrastructure operations, Linode

Security as Business Enabler

Linode’s automated DDoS protection scales to thwart multi-terabit attacks. “We still see about 1000 attacks over a three-month period,” says Spataro. “But those attacks don’t take customers down because we can successfully mitigate them with Juniper and Corero.”

Automated DDoS mitigation has enabled Linode to maintain the level of service quality and uptime its demanding developer-customers expect. The solution leveraged Linode’s existing network infrastructure investment, putting state-of-the-art DDoS mitigation within reach of a fast-growing business.

Linode also saw rapid time-to-value for the combined solution. From the initial testing to the first deployment, Linode had real-time DDoS detection and mitigation in place in three months. Linode then rolled out the solution to its 11 data centers in North America, Frankfurt, London, Tokyo, and Singapore.

Continuing the Automation Journey

Linode is a big believer in automation as the company continues to grow. The network team uses automation to speed the setup of new data centers and make ongoing configuration changes.

“Everything is templated and automated,” says Spataro. “For example, when we launch a new data center, we now bring a Raspberry Pi to do the initial configuration instead of plugging in a laptop. We’ve even automated the setup for the Juniper switches in our data center spine.” Linode uses the Juniper Networks QFX10002 Switch as the data center spine.

“Automation enables us to scale our footprint globally without needing to hire more people,” Spataro says. “Automation is also beneficial for our customers because we can react to events programmatically. They don’t have to wait for humans to get to a keyboard. If a link is failing in the middle of the night, we can automatically take traffic off the link so customers aren’t affected, and then engineers can troubleshoot the problem in the morning.”

Scaling the business efficiently is key. Building on the company’s recent expansion to Toronto and Mumbai, Linode plans to open its newest data center in Sydney in the fall of 2019. “We’re looking at new geographies and exploring edge deployments to support 5G services or broadband providers,” he says.

With the high levels of performance, reliability, and capacity of a Juniper network, now with real-time DDoS mitigation, Linode can scale its business with a simple, highly efficient network.

For More Information

To find out more about Juniper Networks products and solutions, please visit <http://www.juniper.net>.

About Juniper Networks

Juniper Networks brings simplicity to networking with products, solutions and services that connect the world. Through engineering innovation, we remove the constraints and complexities of networking in the cloud era to solve the toughest challenges our customers and partners face daily. At Juniper Networks, we believe that the network is a resource for sharing knowledge and human advancement that changes the world. We are committed to imagining groundbreaking ways to deliver automated, scalable and secure networks to move at the speed of business.

Corporate and Sales Headquarters

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters

Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700
Fax: +31.0.207.125.701

JUNIPER
NETWORKS | **Engineering
Simplicity**



Copyright 2019 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.