Nexusguard and Serro Build Industry's First SDN-Powered DDoS Mitigation Cloud with Juniper Routing

Summary

Company:
Nexusguard

Partner:
Serro

End Customer Vertical:
Web Services

Business Challenges:
Design a robust and agile global routing infrastructure that leverages the power of a software-defined WAN to mitigate large and unpredictable DDoS traffic at scale.

Technology Solution:

- MX960 3D Universal Edge Router
- QFX5100 Switch
- EX3300 Ethernet Switch

Business Results:

- Instantly scale to increasing volumes of DDoS traffic with a new, highly robust software-defined WAN
- Enabled real-time detection and route engineering for multitenant defenses in Nexusguard Automated Intelligence
- Improved customer uptime metrics with faster response and mitigation times
- Maximized existing bandwidth and infrastructure, and lowered overall yearly operational costs by more than 70 percent

With the proliferation of cyber extortion and corporate espionage led by foreign and domestic bad actors, distributed denial of service (DDoS) attacks are growing in size and frequency. More enterprises and service providers use cloud-based defense solutions to mitigate upstream risks, preventing malicious traffic from reaching their production network.

A recent study from Nexusguard reports that DDoS attack size has grown 40 times since 2008. From the fourth quarter 2015 to the second quarter 2016, attacks increased substantially, with more than 1,500 DDoS attacks recorded per day. DDoS infrastructure attacks continue to dominate, accounting for 97 percent of all attacks globally, according to the Nexusguard 2016 Global Threat Report.

Business Challenges

To protect its customers in a world of unprecedented cyber danger, Nexusguard needed to challenge the status quo. As a leading cloud DDoS mitigation service provider, Nexusguard must react intelligently and automate routing changes instantly for multiple customers in the face of sudden and unexpected DDoS volume spikes. Nexusguard wanted to automate route handling for its enterprise and service provider clients, which required a robust and agile routing platform that could effectively integrate with the latest software-defined networking (SDN) and automation architectures.

Before the Nexusguard security operations center (SOC) can mitigate a DDoS attack, traffic must be routed accurately to one of its scrubbing centers. Typically, engineering teams must make these routing decisions manually. There is always risk associated with manual changes to routing and balancing traffic over multiple peering partners, especially with time-critical variables to consider. Effective traffic management during an attack relies on having the real-time pulse of various dimensions, including the status of upstream ISP peers, current scrubbing center capacities, and attack information such as type, size, and source. These dimensions also must be balanced against a customer's application profile and latency threshold requirements.

"Through the technology collaboration with our valued partners Juniper Networks and Serro, we are able to deliver the SD-WAN strength and mitigation capabilities of Nexusguard AI, ensuring that our customers networks will remain strong in the event of a DDoS attack."

Jolene Lee, CEO, Nexusguard

Selection Criteria

Nexusguard protects hundreds of enterprise businesses, hosting providers, and Internet service providers, all with different protection requirements. The company, which has grown rapidly in recent years, quickly realized that to maintain service efficacy at scale, route engineering logic and changes would have to be automated. To do that, Nexusguard didn't follow the lead of others in the industry. Instead, it had the confidence and vision to build a better way.

Technology Solution

Nexusguard Automated Intelligence is the industry's first software-defined DDoS cloud mitigation platform. Nexusguard AI is designed to manage multiple large-scale DDoS attacks concurrently by automatically route engineering and optimizing traffic through Nexusguard's network of service providers. This innovative solution uses Serro Automated Service Manager (AuSM) SDN framework, Juniper Networks® MX960 3D Universal Edge Router, and Juniper Networks Junos® operating system, which runs across all of Juniper's routers, switches, and security products.

Nexusguard partnered with Serro to customize the AuSM framework as a foundational element of Nexusguard AI. AuSM is an open framework with an API that connects various network and compute elements to one platform, allowing universal business policies to be written and managed across all WAN, data center network, and storage systems. AuSM action manager provides real-time event information, applies predefined logic suggesting the most efficient and effective route paths, and automatically propagates changes to all affected elements.

The SDN-ready MX960 router delivers high performance, reliability, and scale. MX960 routers running Junos OS Ansible modules enable machine-to-machine communication for structured workflow automation. Junos OS BGP FlowSpec and multi-context routing tables enable AuSM to precisely control the data path of attack traffic. Predefined automation logic takes the human decision-making out of the process by suggesting real-time actionable information from the flood of data, ultimately delivering appropriate traffic to Nexusguard AI for analytics and attack remediation. Nexus also uses the Juniper Networks QFX5100 Switch and the Juniper Networks EX3300 Ethernet Switch as integral elements in the Nexusguard AI service.

"Through the technology collaboration with our valued partners Juniper Networks and Serro, we are able to deliver the SD-WAN strength and mitigation capabilities of Nexusguard AI, ensuring that our customers networks will remain strong in the event of a DDoS attack," says Jolene Lee, CEO of Nexusguard.

Business Results

The end result is automated route engineering that eliminates manual traffic handling—a particularly difficult task given that DDoS traffic is usually large, sudden, and extremely unpredictable. This automated intelligence allows Nexusguard's SOC staff to more quickly and dynamically manage traffic decisions and avoid upstream network bottlenecks that can lead to outages, which are especially critical when handling a barrage of concurrent attacks.

Today, Nexusguard can rapidly deploy, manage, and operate advanced DDoS mitigation infrastructure and services at a global scale with reliability, agility, and effectiveness. The combined power of Nexusguard AI, Serro AuSM framework, and MX Series 3D Universal Edge Routers means that Nexusguard can scale its services to service providers and enterprise customers and effectively launch new service offerings on the same platform.

"As DDoS attacks continue to grow and become more complex, having the agility to evolve alongside the attacks and customize our protection strategies to serve our clients is paramount. With our valued technology partners Juniper Networks and Serro, we're confident in our ability to do that."

Jolene Lee, CEO, Nexusguard

Next Steps

With MX Series routers running Junos OS and AuSM at the core of Nexusguard AI, Nexusguard is better positioned for the future needs of its customers. "As DDoS attacks continue to grow and become more complex, having the agility to evolve alongside the attacks and customize our protection strategies to serve our clients is paramount," Lee says. "With our valued technology partners Juniper Networks and Serro, we're confident in our ability to do that."

For More Information

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

About Nexusguard

Founded in 2008, Nexusguard is the global leader in fighting malicious Internet attacks. Nexusguard protects clients against a multitude of threats, including distributed denial of service (DDoS) attacks, to ensure uninterrupted Internet service. Nexusguard provides comprehensive, highly customized solutions for customers of all sizes, across a range of industries, and also enables turnkey anti-DDoS solutions for service providers. Nexusguard delivers on its promise to maximize peace of mind by minimizing threats and improving uptime. Headquartered in San Francisco, Nexusguard's network of security experts extends globally. Visit www.nexusguard.com for more information.

About Serro

Serro designs, deploys, and operates the world's largest and most complex technology environments. We specialize in NFV/SDN system design, workflow automation, and core code development. Our global operational experience coupled with our engineering heritage drives business outcomes that enable service automation and process efficiencies to power tomorrow's software-defined businesses. Visit www.serro.com for more information.

About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at www.juniper.net.

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

3530040-001-EN July 2016