CASE STUDY

SAKURA Internet

GLOBAL DATA CENTER USES VOLTDB TO MITIGATE DDOS ATTACKS

SAKURA Internet, one of Japan's largest data centers, provides a complete range of services for enterprise-grade customers whose profitability and survival depend on their networks staying up. With a modern data center powering its worldwide operations, SAKURA offers website and email hosting, virtual private networks, elastic cloud, data center solutions, and business continuity planning.

Delivering an always-on experience, without any downtime or data quality loss, is essential to SAKURA's core business. Like other operators, they are regularly targeted with distributed denial-of-service (DDoS) attacks that flood the targeted customers with fraudulent traffic and keep them offline. To minimize downtime and deliver secure, high-speed, and highly available internet and data services, SAKURA developed an innovative DDoS attack mitigation solution and leveraged VoltDB's high-velocity decisioning engine to do it.

THE CHALLENGE — MITIGATE DDOS ATTACKS IN REAL TIME

One in three US businesses have experienced DDoS attacks. A single attack costs between $2.3 million and $4 million, with a median downtime of 7 to 12 hours. Cybersecurity experts logged 10 million DDoS attacks in 2020, averaging over 27,000 in a day.

"Keeping customers connected at all times is of vital importance to SAKURA given the ever-increasing range of applications and services being delivered and consumed online," said Tamihiro Yuzawa, a SAKURA network engineer. "Unfortunately, large-scale DDoS attacks directed toward service providers and private enterprises have demonstrated all too clearly that traditional perimeter defenses are not enough to combat today's sophisticated DDoS attacks."

And the stakes are ever-increasing. With 5G-enabled IoT devices, networks now need to support a million connected devices per square kilometer. Taking advantage of this proliferating connectivity, hackers can grab control of millions of vulnerable devices, servers, routers, and other network nodes and use these to launch wide-scale, highly damaging DDoS attacks.

THE SOLUTION — REAL-TIME ATTACK PREVENTION

As fraudsters find increasingly sophisticated ways to attack networks, operators need to evolve their defenses as well.

SAKURA was employing remotely triggered, designation-based black hole routing to counter large-scale DDoS attacks and avoid collateral damage for customers that share an uplink with the DDoS target. Unfortunately, this can cause legitimate traffic to be blackholed or discarded, making it difficult to forward legitimate packets to customers under DDoS attacks. SAKURA turned to VoltDB to solve this problem.

"We began revamping our in-house DDoS detection application with VoltDB's high-velocity, in-memory relational database as its backend," said Mr. Yuzawa. "We needed something that could not only do the heavy lifting of sFlow data processing, but also tell us, in real-time, who is under attack, complete with detailed profiles including incoming bits-per-second per source IP. With this capability, we can finally move forward from d/rtBh to source-and-destination-based filtering—a critical step in the evolution of DDoS attack mitigation solutions."

SAKURA developed an innovative DDoS attack mitigation solution to complement traditional security measures like firewalls and intrusion prevention systems. The system learns what normal application and service traffic looks like and uses situational awareness to detect and respond to threats within milliseconds.

SAKURA chose VolDB to power this solution.

The VoltDB Data Platform can power real-time applications that must react in single-digit milliseconds to fight fraud and prevent revenue loss. Volt's in-memory relational database is capable of ingesting massive IP traffic-flow data streams from SAKURA's backbone communications infrastructure, and combines high-velocity data ingestion with real-time data analytics and decisioning in one extremely cost-effective and scalable package.

SAKURA also leveraged Volt to develop a powerful DDoS mitigation application that communicates only with controllers that will reach out and push flows to the deployed switches, ensuring data packets get to the right destination while combating a DDoS attack.

THE RESULTS — MONEY SAVED IN REAL TIME

"By using VoltDB, we've been able to narrow the gap from the point of data ingestion to the point of decision-making from minutes, or even hours, to milliseconds," said Yuzawa. "What's more, we were able to implement a scalable monitoring application at a fraction of the cost of expensive commercial applications."

SAKURA leveraged Volt to create an innovative DDoS mitigation system and integrate that system with its own defense networks.

The result?

A lean, clean, and cost-effective anti-DDoS solution that crushes DDoS attacks, saving SAKURA's customer's millions of dollars (upwards of $5,000 a minute).

ABOUT VoltDB

VoltDB enables enterprise-level companies to innovate faster, perform better, and create new revenue streams by unlocking the full value of their 5G data. The only data platform built for real-time, sub-10 millisecond decisioning, we empower companies to re-engineer their latency-dependent solutions to process more data than ever before at a faster pace than ever before, allowing them to not just survive but thrive in the world of 5G, IoT, and whatever comes next. By combining in-memory data storage with predictable low-latency and other key capabilities, we can power BSS/OSS, customer management, and revenue assurance applications that need to act in single-digit milliseconds to drive revenue or prevent revenue loss, without compromising on data accuracy. For more information, visit voltdb.com.