VOLTDB

SAKURA Internet

CASE STUDY

VOLTDB ENABLES SAKURA INTERNET TO KEEP ENTERPRISE CUSTOMERS ONLINE IN THE FACE OF DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACKS.

Sakura Internet, one of Japan's largest enterprise-class Internet Service Providers (ISP), builds and maintains a proprietary IP backbone in addition to operating several data centers across Japan in order to deliver a diverse range of Internet services to enterprise customers. Those services include website and email hosting, virtual private networks, elastic cloud services (IAAS) and complete data center hosting solutions, including systems management. The company also offers Business Continuity Planning (BCP) to meet its customers' disaster recovery needs.

"Keeping customers connected at all times is of vital importance to Sakura Internet given the ever-increasing range of applications and services being delivered and consumed online," said Tamihiro Yuzawa, network engineer at Sakura Internet. "Unfortunately, large-scale Distributed Denial-of-Service (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."

The stakes are high in preventing a DDoS attack. A 2012 survey estimated the cost of an attack to run from $10,000 to as much as $50,000 **per hour** in lost revenue for each organization targeted.

In order to properly mitigate a DDoS attack, it is critical to understand where to monitor for security breaches, and what to monitor for. Creating and maintaining this situational awareness allows organizations to be aware of anomalous behavior occurring on network traffic at any time.

To achieve that awareness, Sakura created a baseline for normal network activity so that any spike in network traffic caused by a DDoS attack could be quickly identified. Sakura also leveraged knowledge of the exact protocols used for incoming and outgoing communications to take into account pre-planned events that occur on specific days and times, such as timed backup activities. Given the requirements to establish this baseline and identify anomalous behavior on the network, the technology used to provide accurate situational awareness must be capable of not only collecting massive amounts of detailed data about the traffic in transit, but must very quickly generate reports and statistics about the protocols and traffic summary.

In order to minimize downtime and help guarantee safe, reliable Internet services, Sakura developed a cutting-edge DDoS attack mitigation solution to complement more traditional security systems, such as firewalls and Intrusion Prevention Systems (IPS).

In 2012, the company began evolving an in-house DDoS detection application by leveraging VoltDB's in-memory relational database. This 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 an extremely cost-effective and scalable package.

Sakura Internet employed a technique known as designation-based Remotely Triggered Blackholing (d/RTBH) as a countermeasure against large-scale DDoS attacks. This approach avoids collateral damage for customers sharing the same uplink with the DDoS target hosts. Unfortunately, this strategy causes legitimate traffic to those targeted to be blackholed, or discarded, without informing the originating source that its request did not reach its intended recipient. In other words, the ISP was unable to forward legitimate packets to customers under DDoS attacks. Another complicating factor is that it's common for DDoS attacks to grow to several Gb/sec or more in mere seconds, making it critical to identify the intended targets of the attacks as quickly as possible. To solve these challenges, and to identify and deliver legitimate traffic to the targeted destination, Sakura turned to VoltDB.

"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."

The next step for Sakura was to develop a system that allows clean incoming packets to pass through the company's Internet Border Gateway Protocol (BGP) mesh to the non-BGP routers nearest to the targeted host. Sakura executives turned to OpenFlow, using FloodLight's static flow pusher API for this purpose instead of tunneling or virtual routing and forwarding (VRF). "With the help of VoltDB, Sakura's application knows all the necessary information to dispatch appropriate requests to its trigger router for RTBH, and to FloodLight controllers for proactive flow insertions via REST API," said Mr. Yuzawa.

The Sakura DDoS mitigation application communicates only with controllers that will reach out and push flows to the deployed switches. To keep track of DDoS filtering records, it also stores all flow entries as-is in the form of JSON-encoded data into a varchar column that can be indexed and queried directly with VoltDB's powerful field() function, thereby avoiding the overhead of parsing or normalization. The end result is a much cleaner and leaner program that also keeps system maintenance costs controlled.

"As network engineers, we face challenging situations simply trying to get packets to the right destination while combating a DDoS attack," said Mr. Yuzawa. "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. What's more, we were able to implement a scalable monitoring application at a fraction of the cost of expensive commercial appliances."

Sakura Internet created an innovative DDoS mitigation system by leveraging VoltDB's in-memory relational database and combining it with OpenFlow. This system resulted in a practical DDoS attack mitigation solution that keeps those subjected to a DDoS attack connected to the Internet, ultimately saving their customer's upwards of $50,000 an hour during such attacks.

209 Burlington Road, Suite 203
Bedford, MA 01730
Phone: +1.978.528.4660
Fax: +1.978.528.0568
http://voltdb.com