CASE STUDY

FireEye Solves the Mystery of the CPU Sawtooth Pattern

Protecting the internal systems of this well-known cyber security company requires skill, experience, grit and a willingness to think outside the box

AT A GLANCE

Gigamon Solutions

- Inline bypass so inline tools don't become single points of failure
- Load balancing to spread total throughput across multiple appliances
- Failover that maintains uptime in difficult scenarios

Customer Benefits

- Ability to maintain and troubleshoot inline tools by removing and reconnecting them from the network on the fly
- Avoid overloading security appliances and taxing their CPUs
- Instant and reliable device failover

Challenges

A few years back, cyber security company FireEye's move to a new corporate headquarters ran into a mystery familiar to many NetOps teams. The problem: CPU loads for some inline scanners were shooting through the roof every 30 seconds, like clockwork.

Looked at through monitoring tools, the latency graphs formed repeating sawtooth patterns. And for a few days, the pattern defied explanation for FireEye Senior NetOps Engineer Matthew Baskett.

Quick Thinking Buys Time to Troubleshoot

"Fortunately, we'd previously deployed a pair of GigaVUE-HC2 visibility nodes to provide traffic redirection, inline bypass and packet deduplication to feed our own appliances and our own security stacks," he says.

Matt used the GigaVUE-HC2s' inline bypass feature to dynamically remove and add back the suspect appliances from the device pool, as necessary — without affecting the rest of the stack. This gave the team the necessary breathing room to troubleshoot and find out what exactly was happening.

Putting their heads together, the team soon discovered the answer.

"After much troubleshooting, we found that the inline scanners did not support Q-in-Q VLAN tagging," says Matt. This caused the erratic behavior. "But amazingly, we maintained uptime and throughput while we were figuring this out and correcting the problem."

How FireEye Deploys Gigamon Solutions

The GigaVUE-HC2 nodes sit in the FireEye environment wherever they want to provide that inline packet redirection. Their primary focus is at their ingress/egress points.

"We typically run anywhere from two to eight FireEye NX appliances from a GigaVUE-HC2 node and an inline tool group," says Matt. "We do that for resiliency and redundancy. During standard maintenance we can take down a FireEye NX appliance and upgrade its code with zero impact to traffic flow."

"During standard maintenance we can take down a FireEye NX appliance and upgrade its code with zero impact to traffic flow."

Load Balancing and Fail Over

GigaVUE-HC2 nodes also let FireEye spread out network loads and total throughput across the NX appliances.

"We also get instant and reliable failover for any inline device that might go offline — without having to venture into the expensive and finicky realm of optical failover hardware solutions," says Matt.

Lastly, Matt says that the Gigamon nodes just work. "For a networking team with as much breadth as we are responsible for managing, any device we don't have to worry about on a day-to-day basis, that's a win in my book."

About Gigamon

Gigamon is the company driving the collaboration of networking and security teams. We make threats more visible with the Gigamon Security Delivery Platform, a next-generation packet broker purpose-built for security. Whether on-premises, virtual or in the cloud, organizations use a single platform for visibility to stop tool sprawl and save costs. Learn how you can make your infrastructure more resilient, more agile and more secure at www.gigamon.com, our blog, and Twitter, LinkedIn and Facebook.

Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | www.gigamon.com