Keysight Optimizes Massive Network Security Infrastructure Upgrade

The Urgency of Ongoing Protection of Network Data

The average cost of a data breach increased to $3.86 million dollars and the average cost of each record stolen or lost rose to $148 dollars (Ponemon Institute, 2018 Cost of a Data Breach Study: Global Overview). With a 28% chance of one or more data breaches in the next two years, enterprises are investing in gear like next-generation firewalls (NGFW). Many CSOs believe that when they implement a new security solution, they are improving their network security posture. However, expensive and complex security solutions do not guarantee a more secure network. They can also be costly both in creating unplanned outages and in disrupting the baseline functionality of the network if IT staff does not have tools and resource for accurate pre-deployment validations.

Keysight Technologies, the world’s leading electronic measurement company, makes protecting its data a priority. The IT team was looking to upgrade its firewalls but was determined to avoid the issues in production they experienced when upgrading in the past. They didn’t have to look far for a test tool that could provide empirical data about the firewalls that were on their short list. Last year, Keysight bought Ixia to round out its business with products for Layer 2-7 network, application, and security testing. Ixia’s BreakingPoint is an application and security test solution that can perform proof of concept (PoC) testing by...
sending real-world application traffic and security strikes to each device to see how network performance and protection is impacted.

Do Vendor Claims Correspond to Real Network and Traffic Profiles?

Keysight’s infrastructure upgrade was a massive and costly endeavor, so the IT team was alarmed when, midway through a worldwide embedded data center firewall deployment, they ran into unexpected issues with the vendor of choice. They used BreakingPoint to figure out why the firewall wasn’t operating as promised and decided to check the performance of the second-choice firewall concurrently. This resulted in a proper bake-off where the two firewall vendors were placed side by side and tested with traffic patterns that closely simulated Keysight’s production traffic flow.

“Using BreakingPoint to hold this bake-off was exciting because it was the first time that we were able to test a firewall without putting it into production,” said Chad Lorenc, senior infrastructure security engineer at Keysight.

For three days, the IT team, aided by Ixia professional services, ran a group of tests on the two short-listed firewalls. To keep the participating firewall vendors anonymous, this case study refers to them as Brand-A and Brand-B. The goal was to find the right NGFW to achieve the highest throughput performance and simultaneous sessions while implementing required protections on the Keysight network.

Tests and Results Analysis

Best-case scenario test

With the help of Ixia professional services, the Keysight IT team first ran best case scenario tests to ensure that the max performance of the devices could be reached with clear-text web traffic with web page responses of various size. With these straight-forward test cases, the team was able to gauge the max performance each device could achieve in different security modes with simple web traffic. This is similar to how automobile companies calculate max performances in pristine driving conditions. The test was focused on opening simultaneous web sessions and keeping them opened for the entire duration while intermittently browsing web pages through those opened sessions. The purpose was to obtain a benchmark that could be referenced later when we move to more complex test scenarios.
Best-Case Scenario Results

Real-world application mix test

In this test, the IT team took great care in using BreakingPoint to create an application mix that closely replicates the actual Keysight network traffic. The traffic pattern information was received from the company’s application monitoring tool log data. This information about the top applications, average packet sizes, and percentage share of each of the applications was fed into BreakingPoint.

Brand-A
- The throughput achieved was 10% higher than promised in the published datasheet (38 Gbps)
- It underachieved the max sessions by only achieving 1.7M versus the 8M published

Brand-B
- The throughput performance achieved was 30 Gbps as published
- It easily achieved the published maximum sessions per second (35M)

[Note: Brand-A did not achieve published performance as we later found out that its max sessions were published with 1460 bytes of full packet data whereas we were using a mix of packets with sizes ranging from 512 to 1460 bytes for our max session test.]
BreakingPoint’s application and threat intelligence has the capability to emulate thousands of configurable application flows that can be customized to have different patterns and packet sizes, multiple applications can be combined with a specified percentage share to create an user-specified application mix. The mix can then be generated through millions of simulated clients and servers to accurately represent any customers production network traffic. The application mix was used to test the NGFW. This representative application mix provided a clear indication of the deviation of the performance from the best-case scenario described in the previous test.

Keysight data center application mix.

**Figure 3**

Application Mix Throughput Performance (Gbps)
Both devices declined considerably when they moved from simple HTTP to the application mix reflected in Keysight’s data center. However, the degradation in throughput is considerably higher in Brand-B than Brand-A. Brand-A also can hold its throughput performance much better Brand-B even when additional security features like “sandboxing” is turned on.

The simultaneous sessions however were a different story, with Brand-A under performing by a long shot and could achieve less than 10% of the data sheet published simultaneous sessions. Brand-B too showed degradation on the max session count, however it was still much higher than Brand-A. Mr. Lorenc stated, “Both brands are deployed in the corporate network and the testing, to our surprise, created some of the same failures we had seen in production, that in many cases we had not been able to identify root cause. This was the first time we really understood what was causing some of our firewalls to fail.”

Apart from showing the shortfalls, these tests also clearly showcased the unique strengths each of these vendors had.

Security efficiency test

This test was designed to have the application mix run along with malware and exploits to determine the efficacy of the NGFW in blocking the malware while maintaining traffic continuity and performance. Apart from the application mix that we had created for the previous test, we also added over 800 of the latest malwares and exploits and created a customized attack list in BreakingPoint. Several malwares were less than a day old and when they were mixed with the application mix traffic, it created an accurate representation of an attack scenario as in a real-life new zero-day attack would always be intermingled with the production traffic.
Since several attacks were recently discovered, both Brand A and B had to employ their sandbox mechanisms to detect the attacks as their signature detections didn’t stop the malicious files.

The catch rate of Brand-A was 10% higher than Brand-B. Brand-A's sandbox took 50% less time to reach a verdict on whether a file is malicious or not. Mr. Lorenc said, “We tuned both firewalls and applied our corporate security policy to them before testing. We believed we had tuned them to a similar level of security protections, so this was a surprise for us and identified some significant differences on how each vendor identifies risk and protections.”

**How This POC Led to an Unexpected Outcome**

The reality is that every device or system connected to the network, even a security device, introduces another element that can be hacked. What it really boils down to is: it’s not about selecting the best firewall but finding the best solution for your environment and business—one that increases the effectiveness of your security architecture. Adding a new breach protection system is really an exercise in risk management.

Keysight wanted to ensure they got the design and architecture right so they could avoid downtime and deploy more confidently. The results of the three-day testing were quite definitive. By using BreakingPoint to showcase how each NGFW performed under various conditions, Keysight knew that one device was far better at handling throughput while blocking attacks and the other better at handling simultaneous sessions. The unexpected decision was to purchase both NGFW devices, but for different locations in the network that had different requirements.
In the end, Keysight deployed one NGFW to protect LAN clients and one to protect data center servers, taking advantage of each NGFW’s strengths by placing them in specific parts of the network based on expected use and traffic profiles.

The Brand-A devices were deployed with all security features turned on across the Keysight local-area network (LAN) that is more prone to attacks and considered higher risk. The Brand-B firewalls were deployed with reduced security features across the internal data centers that were mostly accessed by internal users and had obvious needs for higher sessions, however were less prone to cyber-attacks.

Even though this engagement started off as a vendor bake-off, the testing helped Keysight understand both vendors’ product architectures better and design its network to take advantage of the differentiations of the products, effectively working around the limitations of both firewalls.

“For the first time, we were able to not only see the limits of specific firewalls but also understand why and how to design around them to best protect Keysight’s network,” said Mr. Lorenc.

Now realizing the insights BreakingPoint provides, the Keysight IT team will use it on an ongoing basis to operationalize its software and patch upgrades and when implementing new features and policies like sand-boxing and SSL inspection.

Learn more at: www.keysight.com

For more information on Keysight Technologies’ products, applications or services, please contact your local Keysight office. The complete list is available at: www.keysight.com/find/contactus