

Customer Secures Their Network From Cradle to Grave

Organization

- Leading financial services institution in the United States

Challenges

- Too many vendor defects getting into production network
- Extremely complex inline security deployments

Solutions

- BreakingPoint security testing and IxLoad performance modules for Keysight PerfectStorm
- iBypass 40-10 switch
- Vision One packet broker

Results

- Created center of excellence to validate network changes
- 120 vendor code defects eliminated per year
- Saved \$800K in first year
- Security tools now connected in a high availability configuration

Leading Financial Institution Implements Lifecycle Approach to Maximize Network Security

The customer is a leading financial institution based in the United States providing international banking services. They wanted to improve network security in two ways: by validating configuration changes before they were inserted into the live network and by implementing a robust, high availability (HA) inline security solution to reduce risk.

Securing the company network is important for any business. But in the financial services industry, it is an absolute necessity from monetary, consumer confidence, and reputation perspectives. One solid defense mechanism is to secure the network using a lifecycle approach.

During each phase of a network's lifespan (pre-production, installation and turn-up, production, change management, and decommissioning), there are distinct vulnerabilities and threat vectors that can be exploited. In this case, the financial institution's IT team sought to use a lifecycle approach with Keysight products to ensure a solid defense against the multitude of threats. The team engaged Keysight to help on three fronts: network performance testing, network security validation, and inline security tool deployment.

Validating the Initial Design

The customer used the Keysight BreakingPoint solution to validate new network architecture designs against various known security threats (such as DDoS, malware, etc.) in their pre-production lab. This involved testing their new next-generation firewalls, wireless access firewalls, IPS devices, load balancers, and a variety of proxy devices to ensure that they performed according to vendor specifications. The test efforts revealed that several of the customer's devices did not work as the vendor stated. According to the "The Keysight BreakingPoint solution enabled us to test all of our security devices in the lab before we actually deployed them. I was able to see exactly how they would perform in the network and adjust my security architecture to maximize effectiveness," said the manager of network operations. Because of the Keysight BreakingPoint data, the security architecture was adjusted before any weakness was exposed externally.

To consolidate their testing capabilities, the financial institution decided to upgrade to the Keysight PerfectStorm solution, which allowed them to keep using the performance tools that they were using (such as IxLoad) and combine them with new capabilities, such as Keysight BreakingPoint, all in a single solution. Now they could test their multi-level, layered security solution design and components against a full spectrum of L2–7 traffic and run it out of a single port using the Keysight PerfectStorm platform.

"The combined Keysight BreakingPoint and PerfectStorm solution allows me to find about 120 flaws a year that I can clearly isolate to vendor equipment. This saves me weeks of troubleshooting time in the production network," stated the manager of network operations.

According to the Ponemon Institute, a flaw detected in development costs \$80 per defect to fix. If detected in QA, it costs \$960 to fix. If detected in the production network, it costs \$7,600 to fix. By identifying 120 flaws in the lab before they made it to the production environment, the customer was able to save approximately \$800,000 in the first year.

"The bypass switch and network packet brokers worked flawlessly. I was able to create a high availability solution that increased my up-time, improved network security, and gave me all sorts of new security options."

Manager of Network Operations

Implementing the Initial Design

Once the initial design was validated, it was installed into the live network. Additional performance testing was then conducted with the Keysight IxLoad solution to make sure that the design was working correctly. Keysight IxLoad simulates today's most-used Internet, video, voice, storage, security, VPN, wireless, infrastructure, and encapsulation/security protocols. This allowed the customer to confirm the deployment.

In addition, a golden baseline was created and documented so IT had a known quantity for network performance and a satisfactory rollback configuration.

High Availability Inline Security Deployments

As part of their new network configuration, the financial institution wanted to implement a more resilient solution for their security monitoring tools in the production network. Their security tools had previously been inserted directly inline in the network. IT wanted high availability for its security tools for enhanced survivability and better control for tool maintenance and configuration updates.

To accomplish this, they installed Keysight iBypass 40-10 bypass switches in the network and connected them to redundant Keysight network packet brokers (NPB). The NPBs were connected to multiple security tools including Palo Alto IPS, FireEye appliances, and NetWitness. The customer was interested in implementing the following NPB features:

- Out-of-band data monitoring filtering to reduce the traffic that requires inspection and ultimately improve tool efficiency
- Load balancing across multiple tools for bandwidth optimization and cost reduction by continuing to use lower speed tools within a higher speed network
- Implementation of high availability for tool redundancy
- Addition of VLAN tags to trace packets better along with the ability to remove the tags without the routers' knowledge

This solution provided them with the opportunity to insert or remove tools as necessary with minimal impact to network uptime or performance. Many of the tool configuration changes no longer required Change Board approvals because the scoring threshold used to determine if a Change Board approval was required was rarely reached now. This allowed the security team to make changes after normal work hours without waiting for maintenance windows.

"The bypass switch and network packet brokers worked flawlessly. I was able to create a high availability solution that increased my up-time, improved network security, and gave me all sorts of new security options," said the manager of network operations.

Looking Ahead — Change Management Improvements

Further along the lifecycle path is the change management phase. This is a critical phase as any change to the network configuration can be a source of performance and security risk. To mitigate the risk, the customer is now consistently using their lab environment to pretest the effects of any configuration change or software update and simulate what-if scenarios. System and device evaluations for future projects are now being conducted while running +1 and +2 code versions. In addition, quality assurance activities continue to be run on production code in the golden system. The customer still finds on average about 100 to 120 defects in vendor code every year in the lab but no longer in their production environment.