CASE STUDY

Changing Compliance Mandates Drive an Urgent Need for Inline Security Solutions

KEYSIGHT

Organization

- Large European payment services financial institution

Challenges

- Impending fines for lack of PCI DSS compliance
- Inline security deployments were extremely complex

Solutions

- 2 Keysight inline network packet brokers
- 16 Keysight iBypass inline copper bypass switches
- 22 Keysight iBypass inline fiber bypass switches

Results

- Saved $3M on purchase of new firewall and IPS appliances
- Delivered a 10x ROI vs. initial deployment plan
- Security tools now connected in a high availability configuration
- Freed up budget for additional security tool investments

Inline Security Solution Saved $3 Million for Inline Firewall and IPS Deployment

Financial institutions worldwide are revamping their data centers to comply with fast-changing industry regulations. This particular institution, a leading payment processing technology and solutions company in Europe, provides businesses with card and online payments and processing. In fact, their network carries more than 30 million transactions per day. After audits found limited visibility into their network, the firm faced fines of $10,000 USD per day until Payment Card Industry Data Security Standard (PCI DSS) compliance was established.

Complying with Rigorous PCI DSS Regultions

The company urgently needed to demonstrate PCI DSS compliance, which requires firms to build and maintain a secure network, specifically by installing and maintaining a firewall to protect cardholder data. To satisfy this requirement, the company selected Cisco firewalls and Sourcefire intrusion prevention system (IPS) devices to improve their inline security. In addition, they needed to restrict access internally to cardholder data.

The company approached Keysight to help deploy their new security appliances in a high availability configuration to eliminate the risk of downtime.

To meet this requirement, Keysight provided its inline packet broker, allowing the company to install their new firewall and IPS devices in a highly scalable, high availability configuration. The solution also allowed them to restrict physical access to cardholder data through detailed role-based access controls, packet stripping, and data masking.

This solution ultimately saved the company approximately $3 million from a $290,000 investment in Keysight equipment. This amounts to a full 10X return on investment (ROI).

Scalable Firewall and IPS Deployments

The company initially looked to connect their new security appliances directly inline in their networks. But this model created a complex, difficult-to-scale security infrastructure. Keysight proposed deploying the more flexible Keysight network packet brokers (NPB). This approach allowed the company to easily aggregate its inline traffic to make optimal use of its firewall and IPS inspection capacity. Consolidating the firewall and IPS appliances generates economies of scale, making the most efficient use of security tool capacity possible. This eliminated the need to deploy a 10Gbps firewall on every 10Gbps network link, many of which might only have 2Gbps to 3Gbps of traffic.

These savings allowed the company to eventually add BlueCoat SSL Decrypt and FireEye security appliances to further fortify their security posture. And with the Keysight security solution, these new security tools were deployed with little to no downtime.

High Availability Firewall and IPS Deployments

The security team was particularly enthusiastic about the resiliency of Keysight's inline security solution and the easy-to-use interface of its NPBs. Having end-to-end control of all their data sources from one central location minimized the need to involve network personnel in gaining access to network traffic for inspection, monitoring, and troubleshooting.

The original proposed inline deployment model also introduced multiple new points of failure in each network link, which concerned the networking team due to the increased risk of tool failures that cause network downtime. Instead, redundant Keysight iBypass switches and NPBs were deployed to monitor all security tools using high speed heartbeat packets and configured to route traffic around any device in the event of a failure condition. The resilient Keysight solution eliminated network downtime due to inline security tool failures, tool performance and congestion issues, and configuration activity.

As financial data centers worldwide are overhauled and upgraded, IT teams are seizing the opportunity to implement new or enhanced security fabrics that combine leading bypass switches and network packet brokers.

Future Dividends

As financial data centers worldwide are overhauled and upgraded, IT teams are seizing the opportunity to implement new or enhanced security defenses that demand more robust deployment architectures. Keysight's powerful, inline visibility solution combines bypass switches and NPBs to provide a single-source, end-to-end security solution ideal for complying with the demands of PCI DSS.

This remarkably cost-efficient solution helps companies harden their security architectures with the flexibility and scalability to meet future needs.

For more information on Keysight Technologies' products, applications, or services, please visit: www.keysight.com