

Global Financial Services Company Automates PCI DSS Compliance with Skybox Security

Background: This large financial services company operates one of the world's largest retail electronic payments network and is one of the most recognized global financial services brands. The company provides secure convenient and reliable payment options in 170 countries and territories.

Challenges: The financial services firm processes a high volume of credit card transactions and must demonstrate compliance with the most stringent Level 1 PCI DSS requirements. In addition the publicly-traded company has fiduciary responsibilities as well as responsibilities to its customers to ensure the confidence of their sensitive credit card data. And of course brand name protection is critical.

In addition to achieving and maintaining PCI DSS compliance, the security team of the company is required to comply with California SB1386 and AB1950 privacy requirements, supporting the audit information needs of litigation defense when necessary. Many of the PCI requirements that the company must meet are network-related and therefore complex issues to tackle due to:

- The dizzying pace of firewall changes
- A staggering number of rules
- Difficulty in determining whether changes are in compliance
- Interpretation of firewall policies by engineers
- Optimizing firewall rules

The complexities of a firewall audit for a typical Fortune 500 company are high and for this large global financial services company the complexities are exponentially higher as illustrated in the table below.

Industry Firewall Comparison

Description	Typical Fortune 500 Company	This Global Financial Services Company
Average Rules	144	2,000
Maximum Rules	700	40,000
Objects	968	5,000
Interfaces	4	8



Best Deployment Scenario - PCI DSS Compliance

Solution provided: The company determined that an automated firewall audit approach was necessary to meet the goals of its PCI DSS compliance process. They evaluated a variety of solutions based on the evaluation criteria below:

Evaluation Criteria

Regulatory reporting (NIST PCI)	Impact or What-If analysis	Stability and Usability
Firewall compliance to policy	Comparison analysis	Performance
Customizable policies	Multi vendor product support	Scalability
Rules optimization	Topology awareness and graphical display	Support (fast quick changes)
No latency or risk to production environment	Adhoc queries	Direct & automated data collection

The company chose Skybox Security due to its unique risk-based approach to firewall and network compliance analysis and change assurance. First introduced in 2007, the Skybox solution for this deployment is composed of two products, Firewall Compliance Auditor and Network Compliance Auditor.

By continuously collecting and analyzing information from multiple firewalls and network access devices, this solution automates the process of conducting firewall and network audits. IT security and IT operations managers can easily and quickly obtain a comprehensive view of their firewall or network compliance status. Pinpointing the root cause of policy violations is quick, as is predicting and validating proposed configuration changes before they are deployed. The customer reports a dramatic reduction in the time to complete compliance audits - from weeks to just minutes. This is particularly important for organizations that must maintain PCI compliance. When used together the products also enable network operation professionals to eliminate unused or ineffective rules and objects.

The company chose Skybox Security in order to achieve all their firewall compliance needs while at the same time ensuring that there are no wide open sources destinations or ports that would compromise the security of their systems and enforcing key controls and security policies. The company identified and completed these five deployment stages

Summary: By automating the PCI DSS compliance process with Skybox Security the company is able to move faster more efficiently and with confidence that they are compliant every day of the year -- not just during audit season. The company achieved the following benefits: -

- 3-6 months ROI
- 60% reduction in change research effort
- Security engineers do not need to be policy experts
- Operations teams don't need to know multiple firewalls rules syntax
- Brings to light redundant misplaced or non-optimized firewall rules
- Processes are better communicated easier to follow and more consistent

Plus the company reported the unexpected benefits of regaining credibility with customers; establishing an authoritative single source of information; and easier federation of firewalls. These two tables demonstrate the ROI of manual firewall related audits compared to an automated approach.

Automated vs. Manual Firewall and Network Audits

Description	Previous process at Company	Results with Skybox Security
Mitigation research – minimum time	15 minutes	10 seconds
Mitiation research – average time	2 hours	30 seconds
Mitigation research – maximum time	16 hours	2 minutes
Research expertise	Not a core competency	World-class results
Packet analysis combinations	Analysis limited to 5 most critical rules	In millions
Typical firewall analysis time	10 hours	2 minutes
Per change analysis speed	300x, 9FTE's required	1x, 3FTE's required
Analysis accuracy	70%	95%
Firewalls analyzed	1, Weekly	100+, Daily
Vulnerabilities detected	5-10	In millions
Employee burnout	2 weeks	None
Compliance assessments	Annually, and VERY stressful	Daily, automated, easy

Skybox Security
2077 Gateway Place Suite 550
San Jose CA 95110