ssh communications security

CASE STUDY

THIRD-PARTY ACCESS CONTROL FOR REGULATORY COMPLIANCE – Trusted Access for a Securities Broker Firm

One of the largest Chinese securities brokerage firms in Hong Kong realized their need to gain visibility into and control over the third-party access to their network. SSH Communications Security provided a solution with CryptoAuditor®, an encrypted traffic monitoring solution.

QUICK FACTS ABOUT THE CUSTOMER

- A subsidiary from a global top 20 bank listed in the Hong Kong Stock Exchange and the Shanghai Stock Exchange.
- Facilitating companies in their IPO projects, financing and M&A deals, involving total considerations of over HK$1 trillion.

CHALLENGES

IT outsourcing is widespread and common in the financial sector. Institutions rely on outsourced IT experts to manage their critical business infrastructure, a practice that enables smooth, best-practices operations and allows effective cost control. Trusted third parties such as cloud computing providers, networking services, and data center experts are an everyday phenomenon in most organizations.

With the increasing popularity of IT outsourcing, regulators also demand auditors and stakeholders alike to present how the third-party risk is monitored and managed. Various compliance mandates from regulatory authorities call the financial institutions to fulfill stringent requirements for privileged access management.

For example, the **Hong Kong Monetary Authority** posts **General Principles for Technology Risk Management guidelines** for financial institutions. The following are the highlighted guidelines for *Authentication and Access Control*.

3.2 Authentication and Access Control	3.2.1 Access to the information and application systems should be restricted by an adequate authentication mechanism associated with access control rules. For each application system, all users should be identified by unique user-identification codes with appropriate method of authentication to ensure accountability for their activities. 3.2.3 Extra care should be exercised when controlling the use of and access to privileged and emergency IDs. The necessary procedures include e.g. monitoring of the activities performed by privileged and emergency IDs (e.g. peer reviews of activity logs).

(continued to the back page)

3.3 Security Administration and Monitoring	3.3.1 A security administration function and a set of formal procedures should be established for administering the allocation of access rights to systems, and monitoring the use of system resources to detect any unusual or unauthorized activities.
3.4 System Security	3.4.1 Adequate logging and monitoring of system and user activities should be in place to detect anomalies, and the logs should be securely protected from manipulation.

SSH Communications Security's customer needed to scrutinize their third-party access policy to map the high-level security requirements to their internal and third-party access controls. More importantly, they also needed to ensure that their privileged access management is up to date and capable of protecting their well-developed reputation.

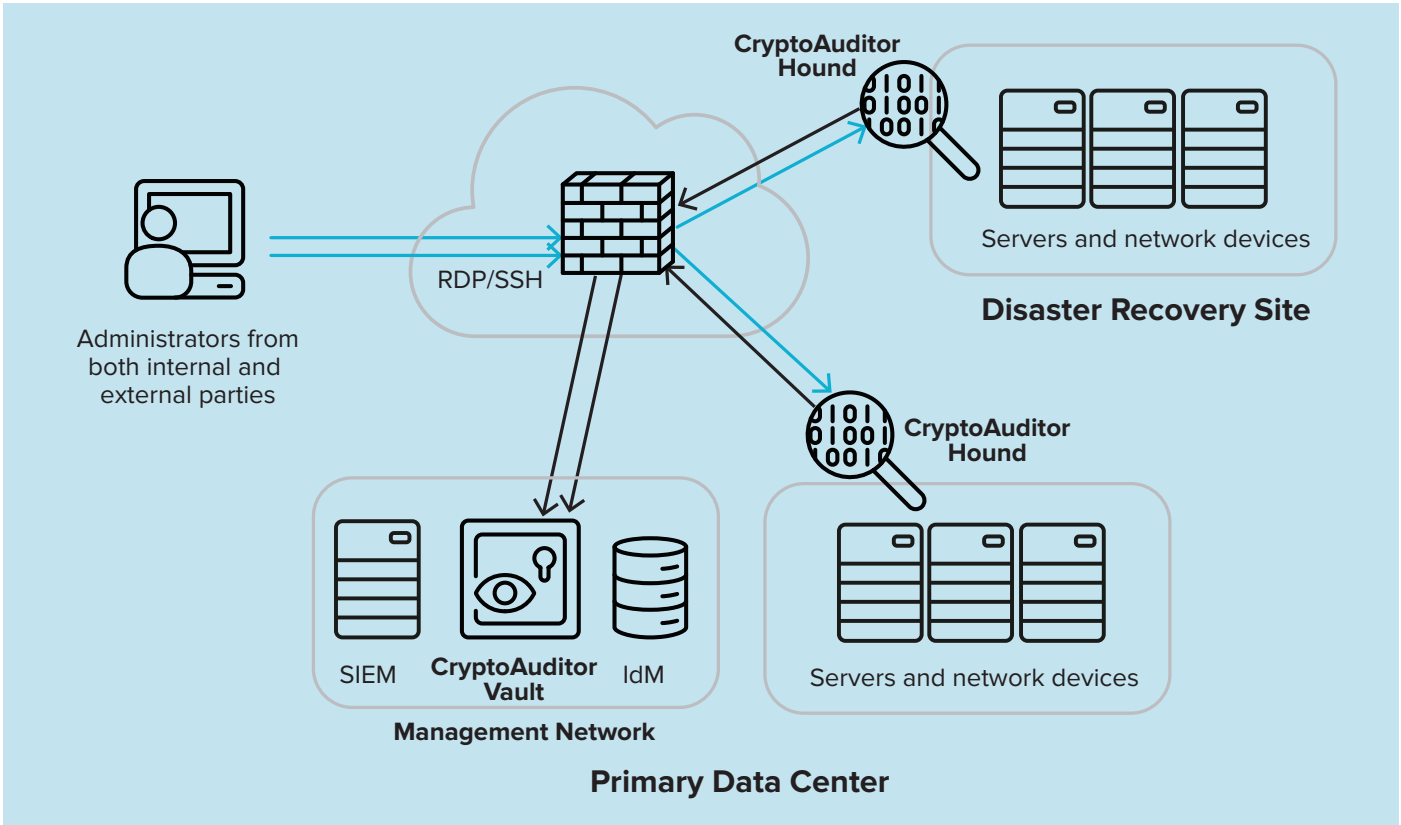
When the trusted third parties access the customer's network, usually through VPN tunnels, the established encrypted channels (SSH, RDP, HTTPS) must be monitored, and the actions controlled. Hence, a solution that "sees inside" the encryption is required to ensure that encryption is not used to hide malicious actions.

TOP 4 UNBEATABLE BENEFITS OF CRYPTOAUDITOR

To gain visibility and control over encrypted privileged access, the customer selected CryptoAuditor because of the following benefits:

1. Transparent auditing of encrypted privileged sessions.
2. Monitoring and peer review capabilities - full video replay and real-time monitoring.
3. Access control to shared accounts. Enforcing accountability for individual users.
4. Transparent integration to monitoring solutions (such as DLP, IDS, IPS, and SIEM).

Network Environment



ssh®, Tectia®, Universal SSH Key Manager® and CryptoAuditor® are registered trademarks of SSH Communications Security Corporation in the United States and in certain other jurisdictions. SSH and Tectia logos and names of other SSH products and services are trademarks of SSH Communications Security Corporation and are protected by international copyright laws and treaties. Logos and names of the products may be registered in certain jurisdictions. All other names and marks are the property of their respective owners.
Copyright © 2016 SSH Communications Security Corporation. All rights reserved.