政府保安机关

Bloombase® Spitfire StoreSafe™
安全存储服务器

Bloombase® Spitfire KeyCastle™
密钥管理服务器

客户案例

采用 Bloombase® Spitfire StoreSafe™ 存储加密解决方案，为敏感的政府信息交互及政府安全存储数据提供加密保护，保证端到端的动态及静态数据的私密性。

项目背景

客户背景

- 政府保安机关
- 员工: 10,000 多人

项目简介

为来自各种可信任数据提供方的敏感交互数据、子系统的存储数据以及备份磁盘中的数据，提供安全的加密保护，防止来自未授权方的物理或电子信息窃取

主要挑战

- 支持 Microsoft Windows, IBM AIX 等各种操作系统
- 不改变最终用户、管理员及操作员使用流程
- 无需编码或二次部署
- 敏感数据任何时候都以密码保护物理方式存储，不容许任何未加密的原本或拷贝
- 可兼容 IBM WebSphere 应用服务器和 IBM DB2 Universal Database (UDB) 服务器
- 存档文件加密存储在备份磁带上
- 高性能的加密和解密

项目目标

- 保护第三方经 HTTP 模式传来的动态数据
- 保护文件系统对象、关联数据库和备份介质
- 保护存储区域网 (SAN) 中的动态数据库数据

解决方案与服务

- Spitfire KeyCastle™ 密钥管理服务器
- Spitfire StoreSafe™ 企业安全存储服务器

概述

市政府保安机关利用自主研发的智能信息系统，快速调配各个工作单位，自动应对潜在事件。该系统每分钟都要从数百个数据源采集信息，信息量多达数百乃至数千条，包括天气预报、本地新闻、海外新闻、交通状况、边境及海岸数据、大型事件等。这些杂乱或有序的实时信息以普通文件的形式，经过分析、读取及压缩后载入中央数据仓库。

基于各种预先定义的数据挖掘规则，实时的安全数据经分析后生成报告、重大事件以及预警，从而提前监控潜在的威胁和风险。7x24 运营组全天候严密监控和追踪事态发展，保安机关负责动态地作出应对，并调配资源处理这些潜在的意外事件，从而更好地控制可能恶化的情况，甚至阻止意外事件的发生。

在这些实时信息采集中，数据仓库和报告仓库非常敏感，必须遵守极为严格的政治和安全私密法规的要求。在应用层面，安全措施确保数据读取仅对授权人员开放，从而防止未经授权的外泄。安全套接层 (SSL) 的 AES 256 位加密，带有安全的密钥交换，为这些机密信息的网络存取提供加密保护，杜绝敏感数据遭到窃取而发生外泄的情况。无论在主站数据中心或灾难恢复

BLOOMBASE®
博隆兴中

(DR) 站点，以物理方式访问电脑硬件，都会受到安全的隔离和严格的访问控制，从而阻止可能发生的物理篡改及数据或硬件窃取。

有了这些外围或周边安全措施，数据系统仍然无法抵御内核攻击、未知攻击以及操作员/内部人员攻击、间谍工具攻击、病毒爆发等其它威胁。

关键的加密任务

为了解决这些问题，同时遵循国家数据保密法规的要求，最终客户需要部署有效的数据加密方案，与各个数据提供方进行安全的信息交换，保护主站以及灾难恢复系统中的数据知识库、数据仓库及备份存档数据的安全。

要在这个关键任务系统上部署数据加密，可谓处处受限，最低限度也要确保动态及静态数据受到 AES 256 位密码的安全保护，保证系统的高可用性和容错能力，并实现可防止篡改的密钥保护和管理。另一方面，加密方案还需要在不改变系统架构、应用和数据库对象的前提下，与现有三层架构完美融合，且对应用层面、管理员、操作员及用户保持完全透明。

经过三个月的评估，最终客户在众多竞争者中选择 Bloombase® Spitfire™ 企业安全解决方案，采取基于内核、数据库、硬件兼容的加密部署。

部署 Bloombase® Spitfire™ KeyCastle 密钥管理服务器和 Spitfire™ StoreSafe 安全存储服务器花了 3 天时间，而新进信息库、IBM DB2 UDB 数据文件及报告存储数据的原始数据迁移，竟出人意料地在 2 天内全部完成。

在每个数据提供方的内部网络中，都有一个用来抓取最新信息的自运行活动组件，在敏感信息载入智能系统时，带有 SSL 安全保护的 Spitfire™ StoreSafe 安全存储 API 即自动为这些信息加密。加密信息以普通文件的形式，暂时存储在 IBM TotalStorage DS4100 SAN 的临时物理存储区。每隔一分钟，IBM WebSphere 应用服务器就会运行一次任务，获取最新的信息，Spitfire™ StoreSafe 安全服务器为加密文件的读取提供虚拟浏览，然后读取并分批载入到 IBM DB2 UDB 数据仓库。

DB2 UDB 的读/写访问是通过具备高可用性的 Spitfire™ StoreSafe 服务器集群来实现的。因此，在信息批量输出时，敏感信息首先由 Spitfire™ StoreSafe 进行实时加密处理，然后保存在 SAN，相反，在执行数据挖掘任务时，密码保护数据仓库的数据，首先按需求经过实时解密，然后才能被查询和读取。数据记录或大型二进制对象的分析结果，存储在另一个 DB2 UDB 环境中，同样受到 Spitfire™ StoreSafe 存储加密服务器的保护。同理，只有在授权人员访问和浏览时，这些敏感数据才会由 Spitfire™ StoreSafe 进行高速解密。基于密码防护的 SAN 存储，通过即将建设并应用于灾难恢复 SAN 子系统的虚拟专线，自动从主站同步到灾难恢复站点。备份存档文件由加密的物理存储系统直接创建，并保存在磁盘盒中进行备份及站外安全存储。

Spitfire™ StoreSafe 为敏感信息提供了整个生命周期内完全透明的加密保护。文件、磁盘数据组、数据库录入及磁盘等数字数据，在强大的全程加密保护下，安全地保存在企业存储架构中，以最低的成本投入和实施风险，有效地防止可能发生的核心攻击及由此导致的严重私密数据外泄。

选择 BLOOMBASE 的理由

- 实现动态及静态数据安全的全方位解决方案
- 平台独立性
- NIST FIPS-140-2 level-3 防篡改及篡改阻止密钥保护
- 全生命周期密钥管理

实施特征

首个客户能为端到端高度敏感的业务数据交换和存储提供安全动态及静态数据保护

主要优点

- 无需培训第三方数据提供方的终端用户
- 应用透明性
- 高性能的数据加密
- 高可用性及容错性
- 防篡改及篡改阻止密钥保护

硬件

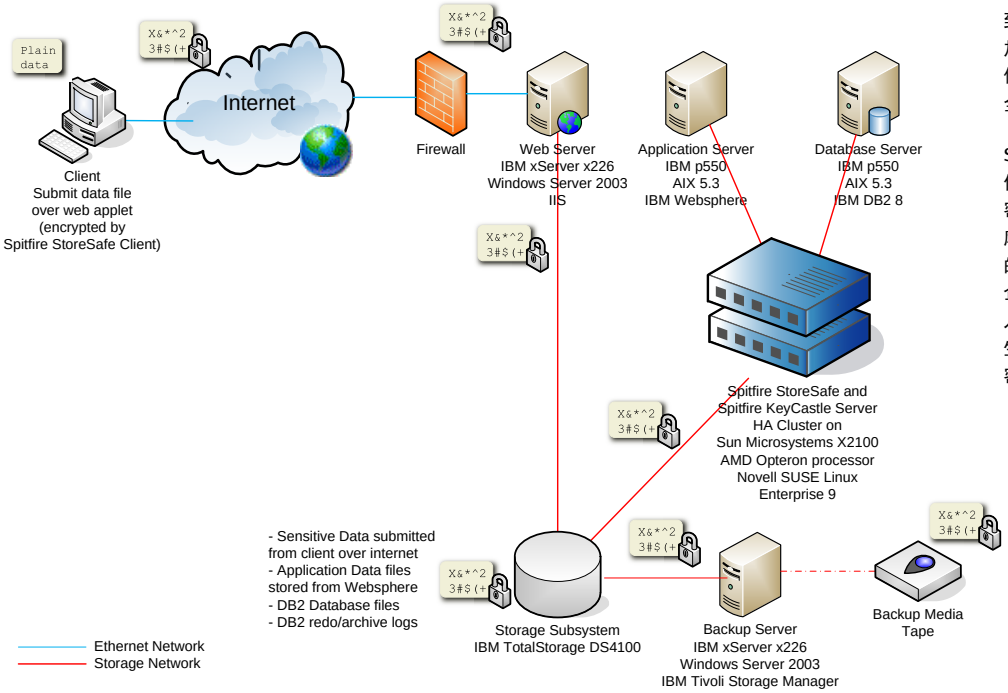
- IBM x-Series 服务器
- IBM p-Series 服务器
- IBM TotalStorage DS4100 SAN 存储
- IBM 磁带库
- Sun Microsystems Sun Fire X2100 服务器

操作系统

- Microsoft Windows Server 2003
- IBM AIX 5.3
- Novell SUSE Linux Enterprise 9

软件

- IBM WebSphere 应用服务器
- IBM DB2 Universal Database
- IBM Lotus Domino 通讯服务器



4AA0-0696AAC 09/2006

BLOOMBASE®
博隆兴中