网神
SECWORLD

可控安全
Controllable
Security

技术白皮书

网神 SecFox 安全审计系统

网神信息技术（北京）股份有限公司
http://www.legendsec.com

● 版权声明

● 文档信息

文档名称	网神 SecFox 安全审计系统技术白皮书		
扩散范围	销售/售前/客服/渠道商/用户	**文档版本号**	V16.8.1
作者	程磊	**日期**	2016/8/20
初审人	程磊	**复审人**	

● 版本变更记录

时间	版本	说明	作者
2015/08/20	V10.8.1	内容修订	程磊
2016/01/20	V11.1.1	内容修订	程磊

目 录

1. 产品概述

SecFox 安全审计系统是对网络访问数据库操作行为进行细粒度分析的安全设备，它可提供实时监控、违规响应、历史行为回溯等操作分析功能，是满足数据库风险管理和内控要求、提升内部安全监管，保障数据库安全的有效手段。

2. 产品特点

2.1 专业的数据库审计

SecFox 安全审计系统能够对业务网络中 Oracle、SQL-Server、DB2、Informix、Sybase、MySQL、PostgreSQL、Cache、达梦等数据库进行全方位的安全审计。具体包括：

1)数据访问审计：记录所有对保护数据的访问信息，包括主机访问、文件操作、数据库执行 SQL 语句或存储过程等。系统审计所有用户对关键数据的访问行为，防止外部黑客入侵访问和内部人员非法获取敏感信息。

2)数据变更审计：统计和查询所有被保护数据的变更记录，包括核心业务数据库表结构、关键数据文件的修改操作等等，防止外部和内部人员非法篡改重要的业务数据。

3)权限操作审计：统计和查询所有用户的登录成功和失败尝试记录，记录所有用户的访问操作和用户配置信息及其权限变更情况，可用于事故和故障的追踪和诊断。

2.2 先进技术和灵活部署

SecFox 安全审计系统利用网神的业务协议检测技术，系统能够识别各类数据库的访问协议、FTP 协议、TELNET 协议、HTTP 等协议，经过审计引擎的智能分析，发现网络入侵和操作违规行为。

SecFox 安全审计系统部署十分方便，即插即用，对业务网络没有影响。系统不仅支持多个网段审计；更可分布式部署，实现对大规模业务网络的审计。

2.3 业务操作实时监控回放

SecFox 安全审计系统对访问数据库操作进行实时、详细的监控和审计，支持过程回放，真实地展现用户的操作。

借助网神独有的基于会话的行为分析（Session-based Behavior Analysis）技术，审计员可以对当前网络中所有访问者进行基于时间的审查，了解每个访问者任意一段时间内先后进行了什么操作，并支持访问过程回放。SecFox 安全审计系统真正实现了对“谁、什么时间段内、对什么（数据）、进行了哪些操作、结果如何”的全程审计。

3. 主要功能

3.1 全方位的数据库审计

3.1.1 多数据库系统及运行平台支持

SecFox 安全审计系统产品能够对多种操作系统平台下各个品牌、各个版本的数据库进行审计。产品能够审计的数据库系统包括：

Oracle 8i / 9i / 10g / 11g

SQL Server 2000 / 2005 / 2008

IBM DB2 7.x / 8.x / 9.x

IBM Informix Dynamic Server 9.x /10.x /11.x

Sybase ASE12.x / 15.x

MySQL 4.x / 5.x /6.x

国产数据库，例如达梦

产品能够审计的数据库运行平台包括：Windows、Linux、HP-UX、Solaris、AIX。

3.1.2 细粒度数据库操作审计

SecFox 安全审计系统能够深入细致地对数据库的各种操作及其内容进行审计，并且能够用户通过各种方式访问数据库的行为。

系统审计的行为包括 DDL、DML、DCL，以及其它操作等行为；审计的内容可以细化到库、表、记录、用户、存储过程、函数、调用参数，等等。如下表所示：

操作行为	内容和描述
用户行为	数据库用户的登录、注销
数据定义语言（DDL）操作	CREATE、ALTER、DROP 等创建、修改或者删除数据库对象（表、索引、视图、存储过程、触发器、域，等等）的 SQL 指令
数据操作语言（DML）操作	SELECT、DELETE、UPDATE、INSERT 等用于检索或者修改数据的 SQL 指令
数据控制语言（DCL）操作	GRANT，REVOKE 等定义数据库用户的权限的 SQL 指令
其它操作	包括 EXECUTE、COMMIT、ROLLBACK 等事务操作指令

3.2 实时回放数据库操作

传统的数据库或者网络审计系统都采用基于指令的操作分析（Command-based Record Analysis）技术，可以显示出所有与数据库主机相关的操作，但是这些操作都是一条条孤立的指令，无法体现这些操作之间的关联，例如是否是同一用户的操作、以及操作的时间先后，审计员被迫从大量的操作记录中自行寻找蛛丝马迹，效率低下。借助网神独有基于会话的行为分析（Session-based Behavior Analysis）技术，审计员可以对当前网络中所有访问者进行基于时间的审查，了解每个访问者任意一段时间内先后进行了什么操作，并支持访问过程回放。SecFox 安全审计系统真正实现了对“谁、什么时间段内、对什么（数据）、进行了哪些操作、结果如何”的全程审计。

3.3 事件精准定位

在信息安全及虚拟化背景时代下，单靠某一个信息去定位违规操作者已经成为不可能，如内网用户大多采用 DHCP 分配 IP 地址，没有做 IP-MAC 绑定及相应的准入规则，用户可通过更改操作系统名、IP 地址、MAC 地址等方式逃避追踪，传统的数据库审计定位往往局限于 IP 地址和 MAC 地址，很多时候不具备可信性。因此只有通过关联尽可能多的身份定位信息进行定位以及做一定的准入权限设置，其审计结果才具有可靠性，才能作为电子证据。SecFox 安全审计系统产品可以对 IP、MAC、操作系统用户名、使用的工具、应用系统账号等一系列进行关联

分析，从而追踪到具体人。

3.4 事件关联分析

SecFox 安全审计系统可对响应事件进行关联，如根据 IP 关联出某段时间内该 IP 所触发的告警数量等；根据一段时间内的数据库或应用系统登录失败次数判断出暴力破解密码的可能性；根据账号的多次登录判断账号信息泄密或共享账号的可能性；相似 SQL 语句执行时间过长从而判断该语句设计的合理性等。根据事件关联性分析，自动涌现一批对客户具有实用价值的信息，帮助客户管理和维护好现有应用。

3.5 访问工具监控

SecFox 安全审计系统自动扫描连接数据库的访问工具。从访问数据库的源头进行分析，应用系统和客户端工具根据不同的数据库类型可通过 ODBC、JDBC、直连等方式连接数据库，直接连接工具如 Winsql、Plsql 及 C/S 架构的客户端工具等。如发现审计记录中出现未知的数据库连接工具或出现规定之外的连接工具，审计员可根据工具监控记录分析出使用过该工具的 IP 及关联的操作记录，进而取证使用该工具的源头及操作的合法性。

3.6 黑白名单审计

SecFox 安全审计系统可根据客户意见及实际审计情况，将 IP、操作语句、账号等相关信息加入黑白名单。同时，在应用系统中，因应用系统对应后台的 SQL 语句固定，一旦发现其中含有危险信息则可将对应的 SQL 加入黑名单，而一旦应用系统中有某些语句疑似风险操作但其实际并不产生危害则可加入白名单。

3.7 变量审计

在不同数据库及应用系统中，很多值的传递都是通过变量进行，如在 oracle 数据库中有绑定变量，在其它数据库中也有变量一说。如审计不到变量则无法对 SQL 指令的危险性进行判断。SecFox 安全审计系统可对不同数据库的不同变量进行审计。

3.8 关注字段值提取

SecFox 安全审计系统可根据配置，自动提取 SQL 指令中某关键字段的值，如查询语句中涉及的时间范围、查询的条件。由其是在金融、高值耗材等信息中，可通过查询条件查询出财产、费用、联系人等敏感信息，通过提取关注字段的值，并通过该值设置规则，则可更精确的对数据库访问操作进行精确审计。

4. 产品优势

4.1 简单易用

SecFox 安全审计系统采用旁路侦听的方式进行工作，对业务网络中的数据包进行应用层协议和流量分析与审计，就像真实世界的摄像机。利用网神先进的业务协议检测技术，能够识别各类数据库的访问协议、FTP 协议、Telnet 协议、Http 等多种应用层协议，经过审计系统的智能分析，发现网络入侵和操作违规行为。

SecFox 安全审计系统部署十分方便，即插即用，不必对业务网络结构做任何更改，对业务网络没有任何影响。SecFox 安全审计系统可以同时审计多个不同的网段；多个系统可以级联，实现分布式部署，实现对大规模业务网络的审计。系统部署后立竿见影，即可自动发现所侦听网络中的数据库访问行为。

4.2 海量存储

SecFox 安全审计系统可以将采集到的所有数据包和告警信息统一存储起来，建立一个企业和组织的集中事件存储系统，满足国家标准和法律法规中对于事件存储的强制性要求，为安全事故增加追查取证的信息来源和依据。

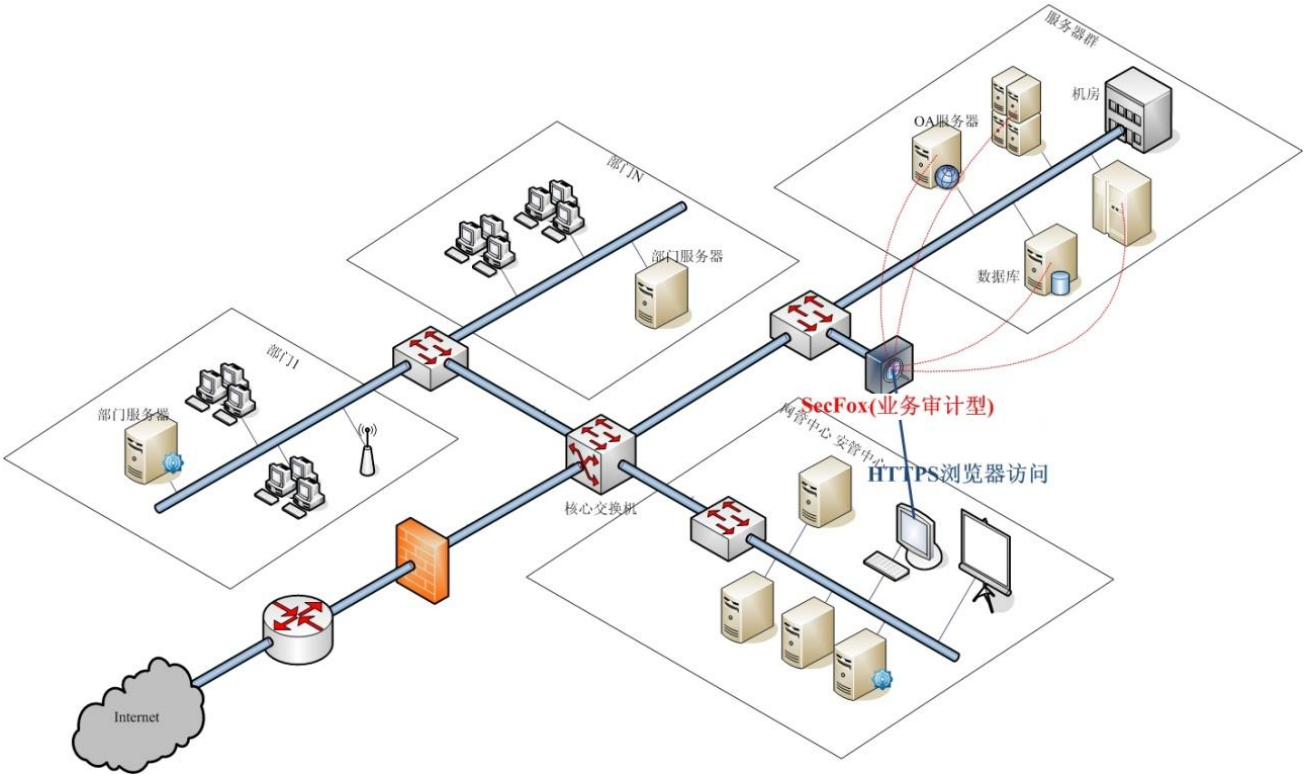
SecFox 安全审计系统具有海量事件处理和存储的能力。单台 SecFox 安全审计系统能够以每秒 6000 条到 24000 条的规模接收数据包，能够在线存储 10 亿到 40 亿条事件记录。加上系统的数据归档与离线存储功能，SecFox 安全审计系统能够存储的数据量大小仅取决于服务器磁盘存储空间的大小；产品自带 1TB～4TB 的存储空间，用户亦可以在后期进行容量扩展。

SecFox 安全审计系统在进行数据管理的时候，对数据存储算法进行了充分优化，使得使用小型数据库的情况下就达到了上述性能。此外，用户在使用本系统的时候，无需购买额外的数据库管理系统和许可，也不必花费专门的精力去维护数据库，这些都大大降低了用户的总体拥有成本。

5. 典型应用

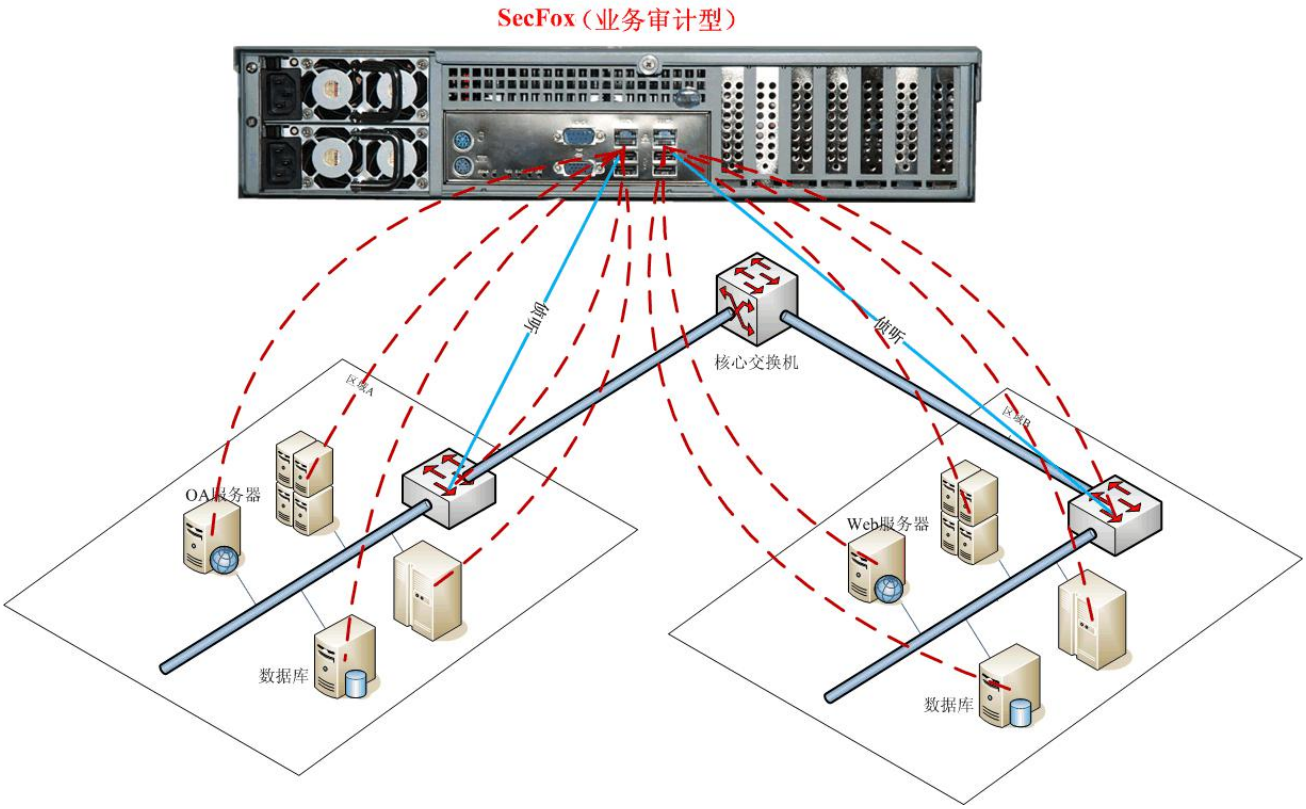
SecFox 安全审计系统可应用于大中小型企业，用于保护业务网中的数据库和网络主机，一般部署于被保护数据源的附近，通过端口镜像或者 TAP 方式连接到网络中。

SecFox 安全审计系统放置在业务服务器集中的交换机上，对交换机的端口做镜像，接到设备。管理员通过浏览器可以从任何位置登录 SecFox 安全审计系统设备进行各项操作，如下图所示：



用户部署 SecFox 安全审计系统无需对现有网络结构做任何改动，用户也不会有任何察觉。而且设备自身的可用性也不会对整个网络可用性造成任何影响。

借助 SecFox 安全审计系统产品独有的多端口侦听（Multi-Port Detection）技术，系统支持同时侦听多个不同网段的网络通讯。这种部署方式适用于对分散在不同交换机上的多个数据库系统进行审计，或者是对在物理或逻辑上隔离的多个网络进行审计。


SecFox（业务审计型）
侦听
侦听
核心交换机
区域A
区域B
OA服务器
数据库
Web服务器
数据库