龙马 Net@Audit 安全审计系统
技术白皮书

龙马科技

产品概述

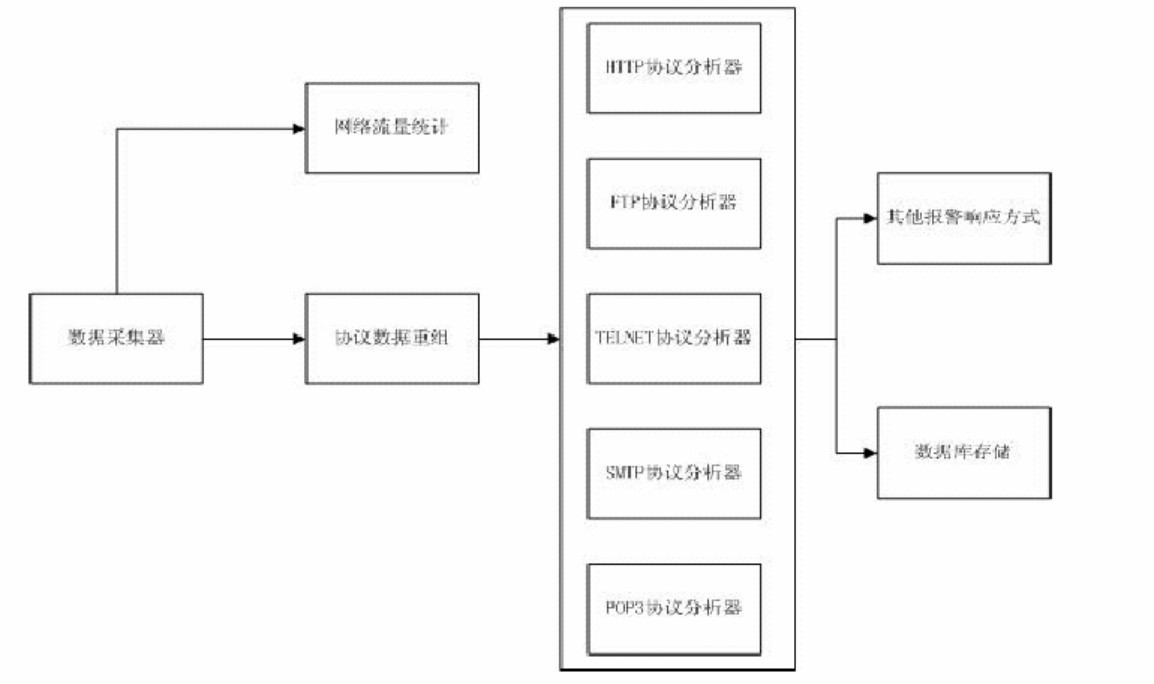
随着近年来互联网的迅速普及，在给大家带来了方便性的同时，也带来了许多严重的安全问题，不仅仅是来自互联网的各种攻击行为会破坏企业、政府信息系统的正常运行，与此同时，使用互联网访问非法站点，传递和发布非法信息，企业内部网络中的资源滥用，企业内部商业信息泄漏等等问题都日益凸现出来。

安全审计技术的出现正是针对上述问题而提出的一种网络监控手段，其基本思想是通过对网络数据的实时采集，解包，以及对各种上层应用协议数据的实时分析和还原，对被监控网络中的Internet 使用情况进行监控，对各种网络违规行为实时报告，甚至对某些特定的违规主机进行封锁，以帮助网络管理员或政府机构对互联网信息资源进行有效的管理和维护。

作为国内最早从事信息安全研究的公司之一，龙马科技很早就开展了对安全审计技术的跟踪和研究，并结合多年从事入侵检测系统 ，防火墙产品研发的经验，从2004 年开始，公司开始在国内市场上推出了自主研发的安全审计产品。其强大的功能和较好的易用性也得到了广大用户的好评和认可。

产品体系结构

信息审计系统以操作系统的数据零拷贝技术为基础，结合核心级的协议数据过滤技术，对网络数据进行各种协议格式分析，对这些协议数据进行合法性检测和数据还原，以发现和捕获各种网络违规行为，产品的整体架构如下图所示：



产品功能特征

- **HTTP 协议审计，主要包括：**

  对敏感IP 使用HTTP 协议的审计；
  对敏感URL 的审计；
  对网页内容的关键字审计；

- **FTP 协议审计，主要包括：**

  对每次FTP 协议的登录行为进行记录；
  对敏感IP 使用FTP 协议的审计；
  对FTP 的命令行进行审计，包括对命令、参数以及反馈值的审计；
  能够对触发敏感主机规则或敏感命令行规则的FTP 连接的过程进行恢复、重现；

- **TELNET 协议审计，主要包括：**

  对每次TELNET 协议的登录行为进行记录；
  对敏感IP 使用TELNET 协议的审计；
  对TELNET 的命令行进行审计；
  能够对触发敏感主机规则或敏感命令行规则的TELNET 连接的过程进行恢复、重现；

- **SMTP 协议审计，主要包括：**

  对敏感IP 使用SMTP 协议的审计；
  对通过SMTP 发送邮件的源、目的邮箱的审计；
  对通过SMTP 发送邮件标题的关键字审计；
  对通过SMTP 发送邮件内容的关键字审计；
  能够对触发敏感主机规则或关键字规则的SMTP 邮件进行恢复；

- POP3 协议审计，主要包括：

  对敏感IP 使用POP3 协议的审计；
  对每次POP3 协议的登录行为进行记录；
  对通过POP3 接收到的邮件的源、目的邮箱进行审计；
  对通过POP3 接收到的邮件的标题进行关键字审计；
  对通过POP3 接收到的邮件的内容进行关键字审计；
  能够对触发敏感主机规则或关键字规则的POP3 邮件进行恢复；

- **流量统计功能，主要包括：**

对网段上单位时间内IP 包的数量、IP 协议的流量进行统计；
对网段上单位时间内TCP 包的数量、TCP 协议的流量进行统计；
对网段上单位时间内UDP 包的数量、UDP 协议的流量进行统计；
对网段上单位时间内ICMP 包的数量、ICMP 协议的流量进行统计；
能够对用户自定义端口的应用协议的包数量和流量进行统计；

产品特色

高性能的核心抓包机制

信息审计系统通过独有的核心抓包技术，在系统的核心态下直接控制网卡状态，抓取网络数据帧，再通过核心态与用户态之间的专用数据通道完成数据帧从核心态到用户态的传递，从而减少了系统在用户态与核心态之间进行系统状态切换和数据拷贝的次数，大大提高了核心抓包的性能。

优化的数据库结构设计

信息审计系统的所有审计记录均通过数据库进行管理，独特的数据库结构设计使其能够实现数据的高速入库，快速查询，浏览，数据库中使用了内存表技术和多表循环的管理机制，后台在内存表中实现高速的数据插入，前台也对内存表进行查询，数据定期备份到硬盘数据表中。由于内存表存储在内存中，而且容量较小，确保了查询和插入速度，同时大量的历史数据备份到硬盘数据表中，供用户查询和下载，确保了数据的完整性。

高可用性的界面设计

信息审计系统的所有用户操作全部通过浏览器完成， B/S 模式的用户界面存在着许多优点：

其一，对用户环境没有任何特殊要求，无须用户为满足产品使用进行任何环境改变；

其二，B/S 模式的数据处理过程全部在服务器端完成，不会增加管理主机系统负载。

第三，通过超链接的作用，对数据记录的浏览能够实现非常灵活的跳转，用户可以在浏览过程中任意切换到关联内容中，通过这个特性，用户可以很容易的发现各种类型告警或者统计数据之间的关联性，从而更全面和深入地了解审计事件；

第四，WEB 界面是一种为大多数用户所熟悉的界面，用户无需花费太多时间，就能轻松掌握界面的使用方法。

可灵活配置的监控规则

系统支持用户定义所需审计的协议的目的端口，并且可以根据具体情况对一种协议定义多个目的端口。

系统支持用户自定义审计规则，包括对协议命令行的定义、协议内容的关键字的定义、敏感主机的定义等。

系统支持用户自定义所需监测流量的协议的目的端口，使用户能够及时获取特定协议流量异常信息。

系统支持用户定义审计域，即用户可以根据具体情况定义所需审计网段的范围，有效克服安全审计的盲目性，提高安全审计的效率和准确率。并解决部分由于高带宽带来的处理能力有限的难题。同时可以从审计域中去掉对某些主机的IP，以保护该主机的网络信息不受监测。

完备的自身安全性设计

操作系统的安全加固：

信息审计系统使用了我们自行裁减的安全操作系统，该系统 提供了多项安全功能，根用户权限分割，系统调用时的权限验证等等，同时我们关闭了系统中所有无用服务，确保外部攻击者无法通过有问题的服务端口对产品进行攻击。

隐藏自身的IP 地址：

信息审计系统的所有探测端口均屏蔽了自身的IP 地址，使攻击者无法通过探测端口对信息审计系统进行扫描和攻击，用户对设备的访问以及探头与控制中心之间的通信过程均通过带外方式进行，与用户网络隔离，由此来确保设备的安全性。

界面中的多级用户管理：

在信息审计系统的界面访问中，为了确保不会出现越权访问和操作，我们对用户进行了权限分配，包括四级用户，用户包括系统管理员，日志管理员，普通管理员，普通用户，用户通过口令进行身份验证，不同用户具有不同权限，用户之间彼此制约，相互监督，确保系统操作的安全性。

系统日志保存：

由于用户对信息审计系统的所有操作均通过界面来完成，因此记录用户在界面上的所有操作，将有助于在出现安全问题时，能够通过这些原始记录寻找问题的原因，信息审计系统中保存了用户尤其是管理员用户对于设备的所有关键操作的日志，而这些日志只有日志管理员才能够查看，从而确保了其安全性和可靠性。

产品典型应用环境

对于用户不同的网络拓扑和应用环境，信息审计系统的安装方式和网络结构均有所不同，以下通过两个范例说明信息审计系统在典型应用环境下的安装：

图1. 普通集线器上的安装示意图

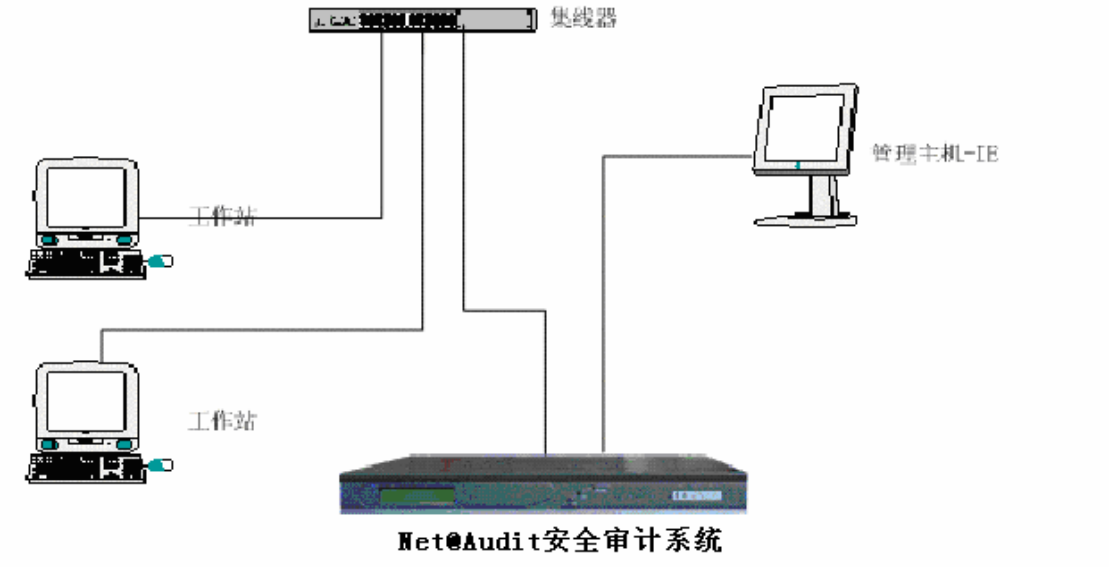
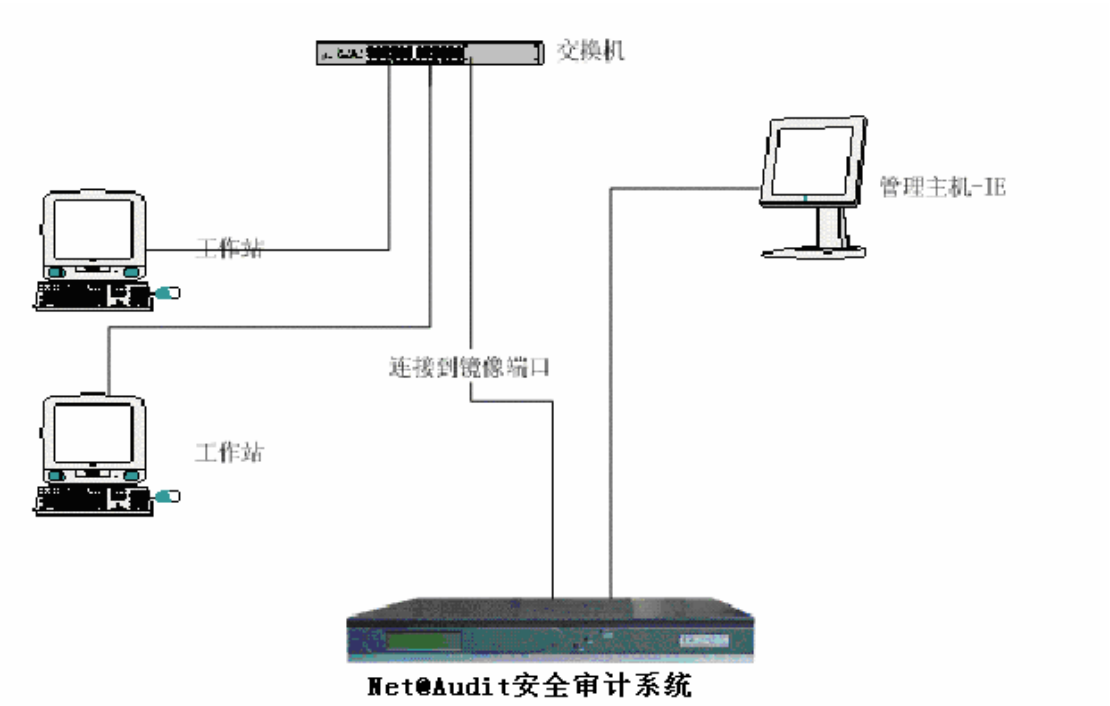


图2. 支持镜象端口交换机安装示意图上面的应用结构中，用户通过管理主机，以带外方式对设备进行管理。



产品技术指标

产品硬件规格

机箱高度：1U
尺寸：高43.2mm 宽482.6mm 深431.8mm
重量：6.0KG
工作温度：0℃-50℃
相对湿度:：5～95%.40℃（不凝露）

网络支持

支持的网络环境：TCP/IP
支持的网络带宽：10/100M
网络接口：
一个10/100M 探测端口
一个10/100M 管理端口
（可根据客户需求附加两个探测端口）

安全审计能力

支持同时对五种主流应用协议的数据进行安全审计

HTTP，SMTP，POP3，FTP，TELNET

响应方式

客户端实时报警；
数据库记录；
攻击过程恢复；

系统稳定性

MTBF：＞5000（H）