业界独有的RDP/SSH网络透明审计技术

来自比蒙科技

安全审计利器 — Session Auditor

（最后更新：2011-03-2）

Session Auditor helps your compliance journey!

http://www.bmst.net

北京市海淀区车公庄西路甲 19 号华通大厦 A 座 720
邮编 100048
电话：010-68482518
传真：010-68482519
电子邮件：info@bmst.net

目录

北京市海淀区车公庄西路甲 19 号华通大厦 A 座 720
邮编 100048
电话：010-68482518
传真：010-68482519
电子邮件：info@bmst.net

北京市海淀区车公庄西路甲 19 号华通大厦 A 座 720
邮编 100048
电话：010-68482518
传真：010-68482519
电子邮件：info@bmst.net

1. 事实

作为当前网络信息安全业界一个逐渐得到公认的事实：在安全事件造成的损失中，有75%以上来自内部，其中包括内部人员的越权访问、滥用、以及误操作等。一个针对大型运营商高级IT经理进行的调查问卷显示，66%的经理认为内部滥用和误用、经营数据泄漏，以及病毒是最严重的安全威胁，作为对比，认为黑客入侵是最严重威胁的只有13%。 分析这些内部安全威胁没有得到有效控制的根源，我们可以发现下列主要因素：审计体系没有有效工作或者根本没有、不具备完整的访问授权机制，不具备完善的职责分离机制，人员安全意识和技能方面的不足等。其中，第一点 – 缺少可信的、完备的审计系统是目前普遍存在、首当其冲的最重要的根源因素，必须严肃研究对待。

1.1. 为什么需要审计系统

审计系统帮助记录发生在重要信息系统中各种各样的会话和事件，包括网络中的、主机操作系统中，也包括应用系统中的。

这些审计信息反映了信息系统运行的基本轨迹。一方面，它可以帮助管理层和审计者审核信息系统的运行是否符合法律法规的要求和组织的安全策略；另一方面，这些宝贵的审计信息在信息系统出现故障和安全事故时，就像航空器“黑盒子”一样，帮助调查者深入挖掘事件背后的情报，重建事件过程，直至完整的分析定位事件的本源[1]，并部署进一步的措施来避免损失的再次发生。 风险管理和内控等是现代企业不遗余力地投入资源进行建设的目标，而完备的、健全的、有效的审计系统就是通往这一目标的重要途径和手段。
所以，当前的许多安全标准和规范都要求组织建设并保证审计系统的可靠性。例如：

1.1.1. 普遍接受的安全管理业界标准ISO27001: 2005

北京市海淀区车公庄西路甲 19 号华通大厦 A 座 720
邮编 100048
电话：010-68482518
传真：010-68482519
电子邮件：info@bmst.net

条款A15.1.3明确要求必须保护组织的运行记录;

条款A15.2.1则要求信息系统经理必须确保所有负责的安全过程都在正确执行，符合安全策略和标准的要求。

1.1.2. 美国公众上市公司需要遵循的萨班斯（Sarbanes Oxley）法案，其合规性要求建立严肃的、完备的企业内控体系，而信息系统的安全审计又是内控体系的重中之重。

1.1.3. 国家颁布的安全等级保护技术要求，在确立为第二级（指导保护级）以及以上级的信息系统中必须建立并保存下面的各种访问日志：

网络（网络安全审计8.1.2.4）

主机（安全审计8.1.3.3）

应用（安全审计8.1.4.3）

1.2. 传统审计系统的不足

根据审计信息的收集方式，审计系统主要分为基于主机的审计（HBA）和基于网络的审计（NBA）两大类。 基于主机的审计是指通过收集主机系统上面的各种形式的日志文件实现审计的方式。事件（Event）是HBA系统发生在主机和应用系统中的行为的基本单元，一般来说，它会包含日期和时间、主体用户或应用、访问对象、成功与失败以及事件摘要等信息。 HBA的特点是收集的信息比较深入，比较完整，不受加密协议的影响，其缺点是部署过程较为复杂，通常需要在主机系统上安装代理，这样不容易保持审计策略的一致，不容易保证审计代理工作的正常和健壮。审计的内容容易被篡改或删除。审计的信息通常只是系统的SYSLOG或EVENTLOG。安装在审计对象主机上面的代理可能会被卸载或者停止运行，这样审计代理产生的审计信息的可信性也会大打折扣。审计代理对于应用系统的性能和稳定性影响也是不容忽视的一个问题。 基于网络的审计是指直接从网络中收集各种会话信息，从网络传输的数据（traffic）和行为中提取审计信息。会话（Session）是NBA的基

北京市海淀区车公庄西路甲 19 号华通大厦 A 座 720
邮编 100048
电话：010-68482518
传真：010-68482519
电子邮件：info@bmst.net

本审计单元，其主要内容有：

- 会话标识
- 源目的地址和端口
- 协议
- 日期和时间
- 成功与失败
- 摘要

1.3 特点与挑战

HBA 系统的特点是与被审计主机紧密耦合，能捕捉到操作系统底层的操作细节，如对文件系统的读写等，经过专门定制的审计系统还可以收集到主机上特定应用系统（如 Web 应用服务器）的日志。但 HBA 系统存在一些不可忽视的问题。

首先，HBA 系统的部署过程较为复杂，必须在每一个被审计主机上安装审计代理。这种分布式的部署也给系统升级及系统兼容性带来新的问题。

第二，审计代理可能被卸载或被停止，或被有经验的主机使用者绕过。此外，审计信息在传送到中心审计存储系统前一般会有一个缓存的过程，在一定时间段内存在被篡改的风险。第三，审计代理一般要运行在操作系统的底层，其本身的稳定性及性能开销对被审计主机的影响不容忽略。

第四，目前大部分信息系统是异质结构，同时包含多种不同的操作系统和/或不同操作系统版本，因此 HBA 系统的覆盖性很难得到保证。

NBA 的特点是部署快速，对应用系统影响小，覆盖面大，不容易被绕过，不容易被窜改等。普通的基于网络的审计系统主要通过收集包括路由器、交换机、防火墙、入侵检测等网络

北京市海淀区车公庄西路甲 19 号华通大厦 A 座 720
邮编 100048
电话：010-68482518
传真：010-68482519
电子邮件：info@bmst.net

和安全设备记录的日志来实现。这样实现的审计系统容易丢失网络会话的绝大部分内容，无法提供事件分析所需的完整的网络行为回放（Replay）。而回放却是安全事件分析中最为重要的技术手段之一。 当前也出现了一些通过交换机镜像方式工作的网络审计系统，它们能够完整的记录网络中流经的数据，但是却不容易深入到敏感数据和应用、不容易定位到用户。另外，最为致命的缺陷是它们不能有效地审计那些使用了加密协议的会话。

当前为了对抗网络窃听，大多数网络维护和业务操作都采用加密协议来完成，例如 SSH 已经广为使用，基本上代替了 Telnet 的位置；而普遍使用的远程桌面（Windows Remote Desktop， RDP）也采用了加密协议。这些普通的基于网络的审计系统针对 SSH/RDP 只能望洋兴叹、无能为力。

综上所述，除去性能和稳定性代价之外，单纯依赖主机日志建立的审计系统是不完善的，没有足够的可信度。而普通的基于网络的审计系统又无法解决承担大部分运维工作的 RDP/SSH 等加密通信协议的问题。上面两种类型传统审计技术实现的审计系统存在的缺陷是显而易见的。我们需要一种既能快速部署、全面覆盖，又能全面记录、理解加密协议、帮助深入挖掘的审计系统，它需要同时具备两种类型审计系统的综合优势。 扎根于网络信息安全领域的比蒙科技深刻地感受到了安全审计遇到的这些挑战，充分挖掘核心团队在安全领域多年耕耘的经验和技术潜能，研究开发了新型的基于网络的审计系统 – Session Auditor。为审计系统带来了深入的分析和回放功能，全面覆盖管理维护活动中常用的网络协议，克服了普通审计系统不能理解加密协议的不足，成为企业信息系统运行过程中值得信赖的“黑盒子”和分析师。

为什么防火墙、入侵检测、网络设备等是不够的？ 我们知道，防火墙、入侵检测系统和网络设备在运行过程中，都会产生大量的日志和告警，这些日志和告警都是重要的审计信息。也是普通的基于网络的审计系统的重要支柱。但是，受限于其工作方式和设计目标，它们

北京市海淀区车公庄西路甲 19 号华通大厦 A 座 720
邮编 100048
电话：010-68482518
传真：010-68482519
电子邮件：info@bmst.net

都不可能细致的分析高层应用协议并进行详细的记录，当前也都不能分析加密协议内部的应用信息。

2. 比蒙科技解决之道

大型企业和组织的核心业务系统由大量的Unix/Linux服务器、Windows服务器、网络设备，以及运行其上的各种应用组成，这些应用系统可能包括ERP、CRM、资源管理系统、计费系统、办公自动化、电子运行维护系统、知识管理系统，以及其它各种C/S或B/S应用。 通常，运行维护人员使用Telnet/SSH来管理Unix/Linux服务器和网络设备，使用Windows Remote Desktop Protocol （RDP）来远程管理Windows服务器，另外，VNC /HTTP /FTP /Rlogin等协议在日常维护过程中也多有使用。 Session Auditor是一个基于网络的行为审计系统。传统的基于日志的审计系统记录的是计算机系统中分立时刻产生的各种单个事件。而Session Auditor则记录用户在一个登录会话中与所有应用交互的全过程，包括屏幕的更新、鼠标的移动与点击以及来自键盘的输入。因此在回放会话时，您可以看到用户所有行为的全过程，就像站在他身边看着他操作一样。

Session Auditor的传感器（SAS）以透明方式运行，可以智能识别流经它的各种网络协议包括上面提到的RDP和SSH等多种加密协议，将这些网络数据严格地按照会话进行重组并且记录下来，传送回数据中心（SAD），以备审计和查询使用。控制台（SAC）可以根据审计策略实时改变传感器的工作方式和审计的范围、协议和粒度。 依靠Session Auditor可以实现功能强大的审计体系：

覆盖大多数加密和非加密网络协议，包括RDP、SSH、ICA、SNMP、POP3、SMTP、Telnet、VNC、FTP、HTTP、Oracle、Sybase、MS SQL、文件共享CIFS/SMB等。

基于网络、透明方式工作，不影响网络结构和业务系统

面向操作员和运行维护操作细节

北京市海淀区车公庄西路甲 19 号华通大厦 A 座 720
邮编 100048
电话：010-68482518
传真：010-68482519
电子邮件：info@bmst.net

可以对操作进行回放和检索查询

提供开放的脚本定制和管理接口，帮助构建全面的审计平台

2.1. 支持众多协议

Session Auditor支持的协议非常广泛，主要有以下：

Windows远程桌面协议：支持RDP，支持VNC，支持CITRIX，支持RGS；

Unix远程访问协议：支持SSH，支持SCP，支持SFTP，支持XWINDOWS，支持TELNET、RLOGIN、TN5250等；

传输协议：支持FTP，支持SAMBA、CIFS；

WEB协议：支持HTTPS，支持HTTP；

数据库协议：支持ORACLE，支持SYBASE，支持DB2，支持INFORMIX，支持MS SQL等；

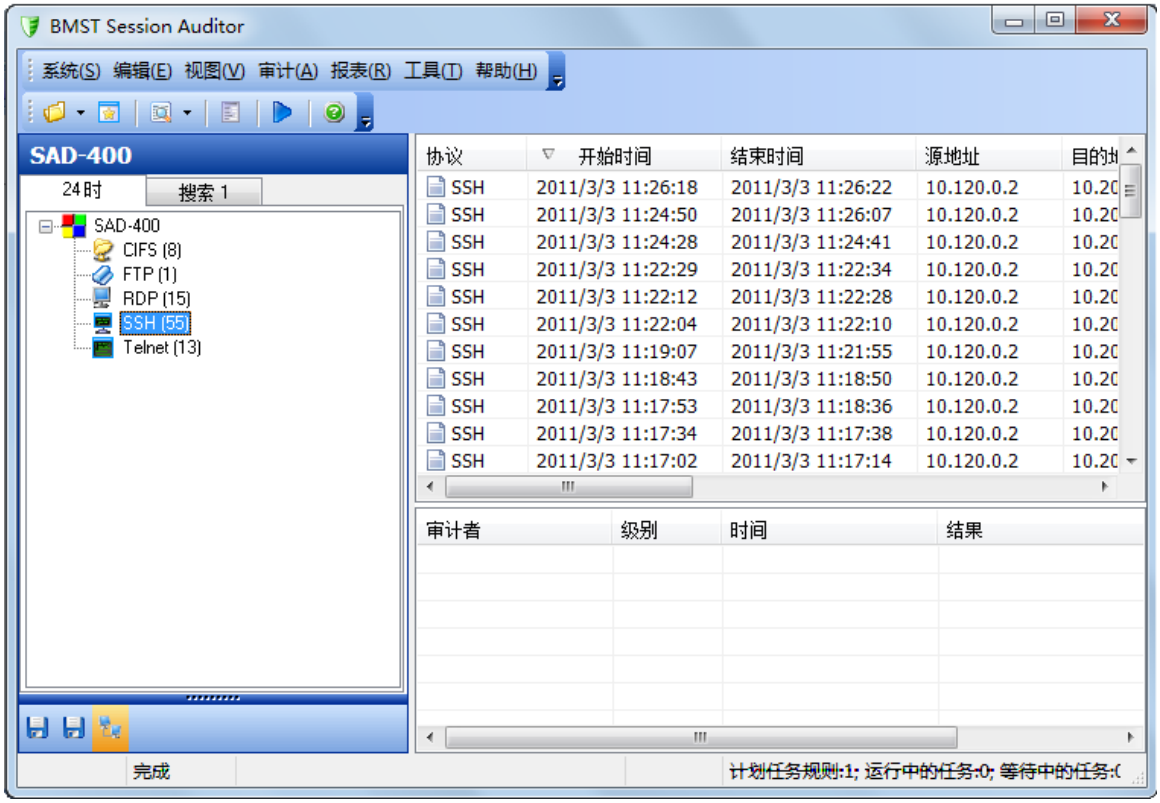
邮件协议：支持SMTP、POP3，支持SMTPS、POP3S；

未知协议：支持未知协议的通过和记录，可通过二次开发对未知协议进行审计。

2.2. 网络会话的全面记录

在主控台的左面可以直观地看到当前记录的网络会话，它们按照数据机和传感器分别按序排列，管理员可以按照需要对其中每个会话选择回放、下载、导出、审计等。在屏幕的右面则显示了选中的会话的审计记录，包括二进制显示和ASCII显示。

北京市海淀区车公庄西路甲 19 号华通大厦 A 座 720
邮编 100048
电话：010-68482518
传真：010-68482519
电子邮件：info@bmst.net

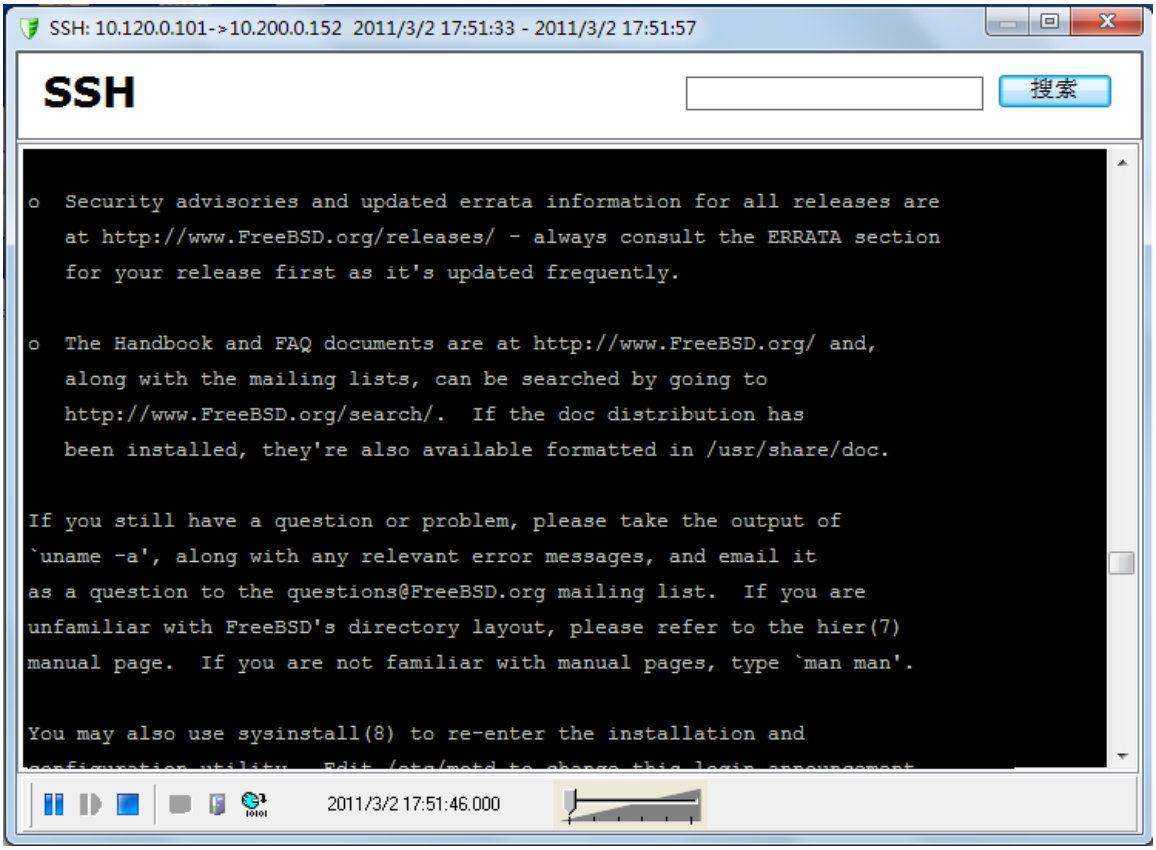


附图**1.** 网络会话的全面记录

2.3. 会话回放

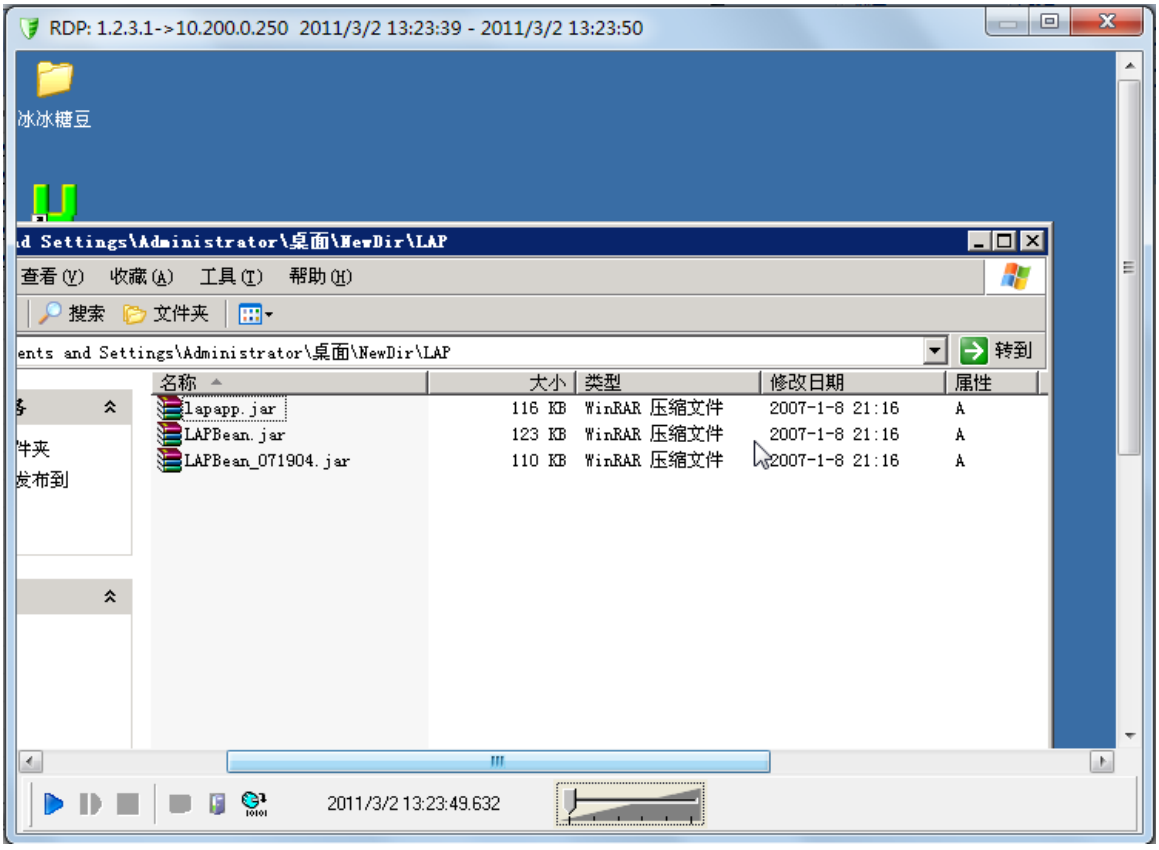
完整的网络会话记录提供了事件分析和审计的技术基础，而回放则是在此基础上的重要分析手段，而又是当前普通的审计系统和主流的安全信息管理和安全运行中心（SIM/SOC）产品所不具备的。比蒙的Session Auditor可以做到这一点。 如下图所示，分别是针对网络中的SSH会话、RDP会话和Oraccle会话进行回放的屏幕。审计员可以使用条件搜索，选择特定的时间、特定的通信方式以及特定的会话等进行回放。在会话回放过程中，可使用控制按钮控制回放的速度、进行暂停、停止以及拖拽等操作。会话回放能精确定位到“每一帧”，可以“步进”的方式进行查看。在进度条上有会话操作者的操作频度显示，通过曲线图能轻松找到操作密集的区域进行查看。

北京市海淀区车公庄西路甲 19 号华通大厦 A 座 720
邮编 100048
电话：010-68482518
传真：010-68482519
电子邮件：info@bmst.net



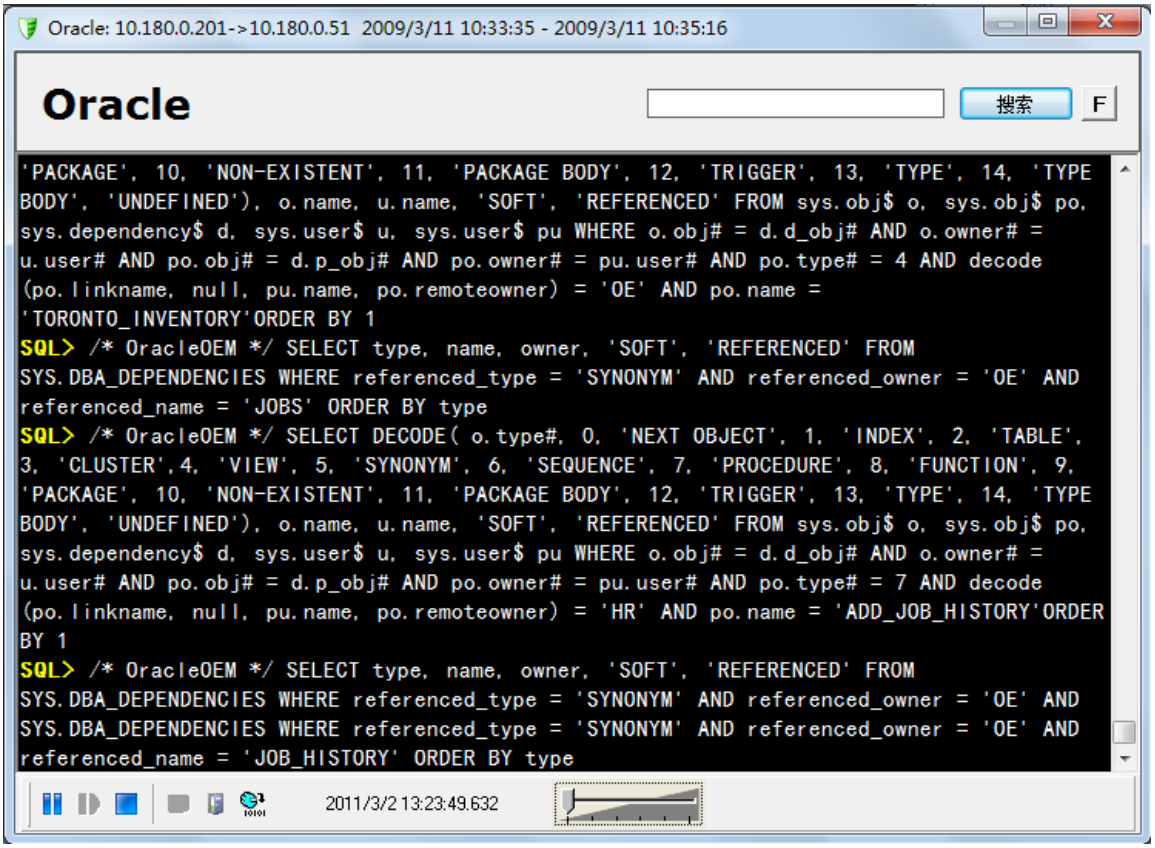
附图2. SSH会话的回放

北京市海淀区车公庄西路甲 19 号华通大厦 A 座 720
邮编 100048
电话：010-68482518
传真：010-68482519
电子邮件：info@bmst.net



附图3. RDP会话的回放

北京市海淀区车公庄西路甲 19 号华通大厦 A 座 720
邮编 100048
电话：010-68482518
传真：010-68482519
电子邮件：info@bmst.net

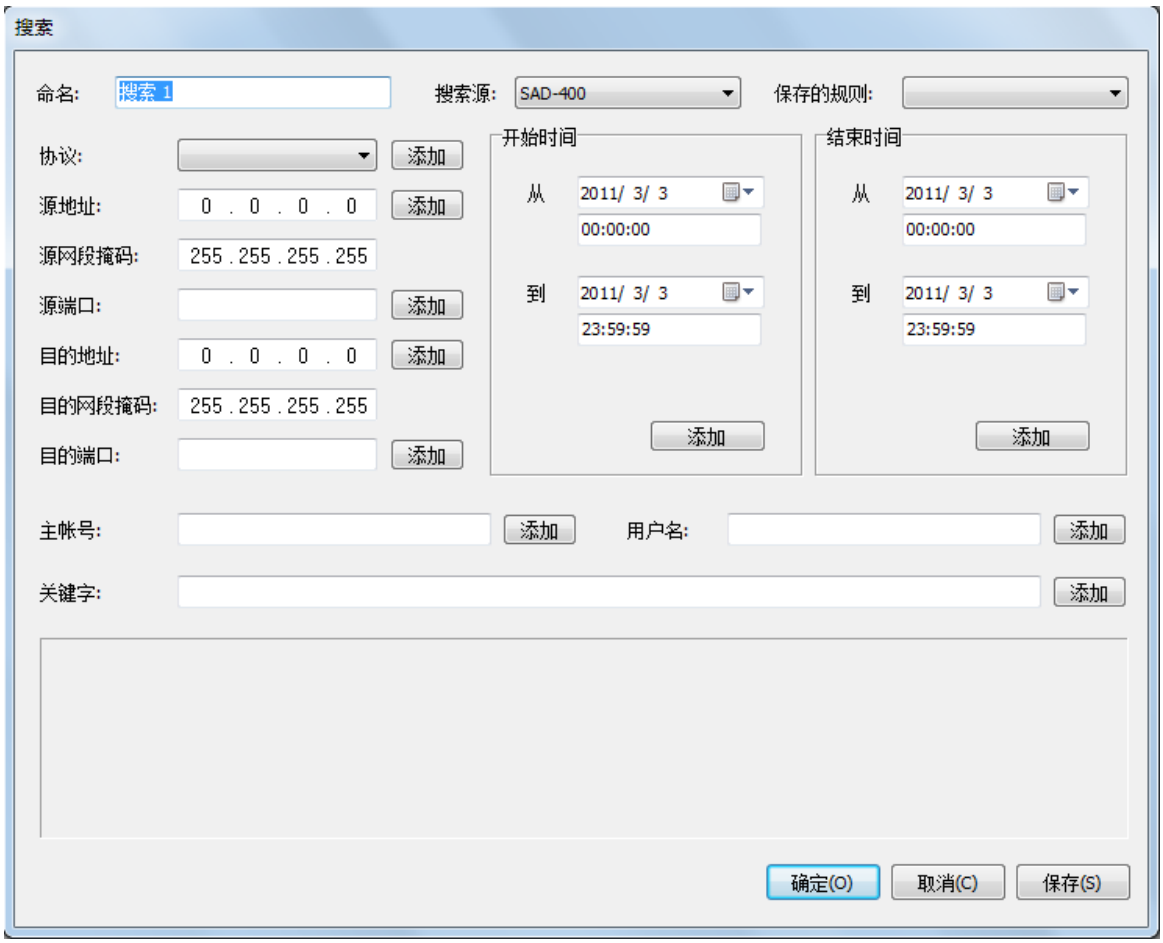


附图4. 数据库会话的回放

2.4. 审计记录查询

Session Auditor提供针对审计记录的多功能组合查询，如下图所示，查询条件包括开始和结束时间、协议、源地址、源端口、目的地址、目的端口等，查询的结构可以直接生成报表。查询的方式非常灵活，各条件之间自动识别与/或，单个条件或者条件范围都支持多达65536个。查询功能同时还支持关键字搜索，搜索规则支持正则表达式，搜索内容支持中文，搜索的协议缺省为文本协议，例如SSH、TELNET、数据库、RLOGIN等等。

北京市海淀区车公庄西路甲 19 号华通大厦 A 座 720
邮编 100048
电话：010-68482518
传真：010-68482519
电子邮件：info@bmst.net



附图5. 审计记录搜索查询

2.5. 访问权限控制

Session Auditor将网络目标抽象为对象进行管理，这种基于对象管理的方式，不但提供了高效便捷的管理方式，而且增强了配置的灵活性。对象可以细化到每一个服务器上的每一个协议。

2.6. 支持PPTP-VPN认证

北京市海淀区车公庄西路甲 19 号华通大厦 A 座 720
邮编 100048
电话：010-68482518
传真：010-68482519
电子邮件：info@bmst.net

Session Auditor支持在PPTP-VPN部署，以适应多种网络需求和安全数据传输，在VPN配置过程中可配置用户和组，进行权限和组织的配置，来实现对用户的认证和管理。

2.7. 支持RADIUS认证

Session Auditor支持radius认证模式，RADIUS协议已经被广泛实施在各种各样的需要高级别安全且需要网络远程访问的网络环境，在SA console界面中进行详细配置即可实现对认证管理。

2.8. 支持外部MYSQL认证与授权

Session Auditor支持外部MYSQL数据库认证及目标帐号授权信息，通过外部数据库可以支持多个SAS共同使用一套认证及目标帐号授权库。

2.9. 支持WEB认证

当以上三种认证方式不能满足用户网络认证需求时，Session Auditor可提供WEB认证方式。该方式是通过WEB页面输入账号和密码来实现一次性认证，使用方便。

2.10. 支持NAT

Session Auditor支持NAT功能，在NAT选项中配置好源地址和目的地址，并指出具体接口，即可启用NAT功能实现地址转换功能。

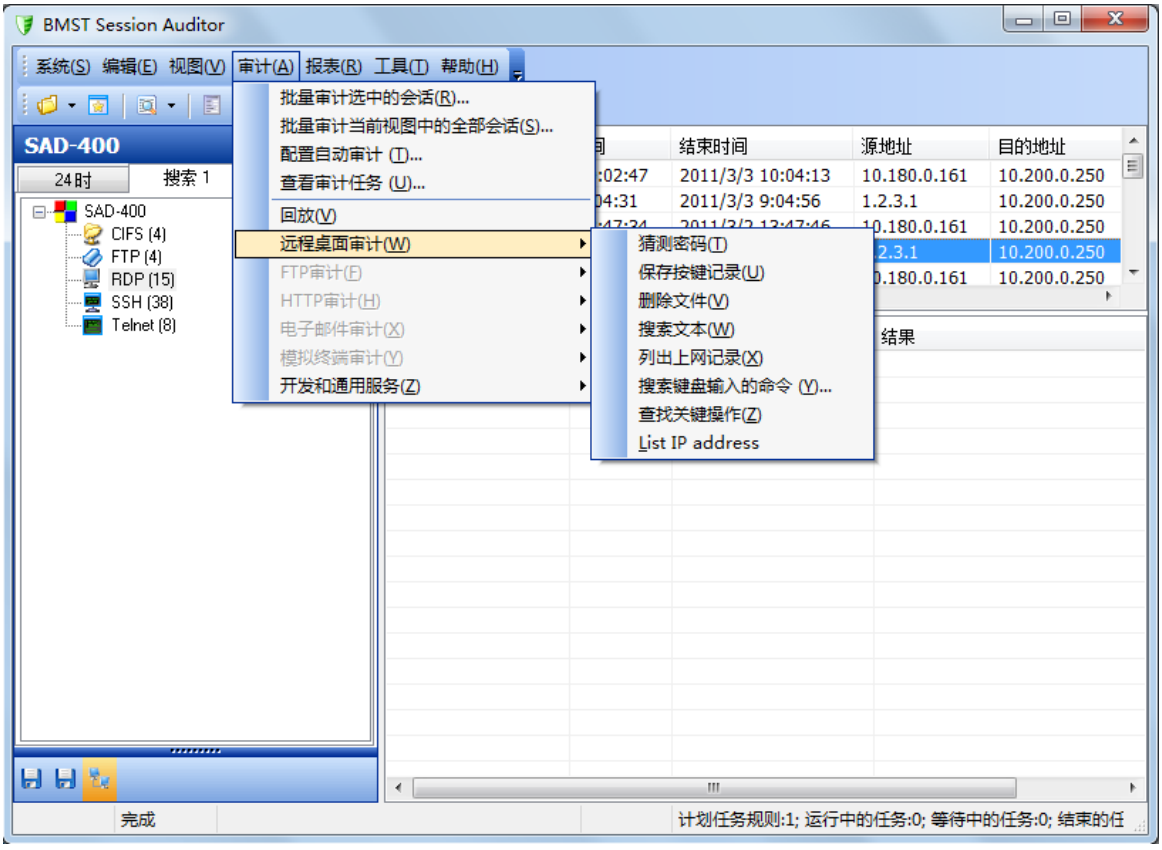
2.11. 支持密码代填

Session Auditor支持密码代填功能，此功能需要和认证一起使用，不支持未经认证的会话使用密码代填。此功能方便了运维人员的操作和网络管理员对企业网络的管理。

2.12. 智能审计系统

北京市海淀区车公庄西路甲 19 号华通大厦 A 座 720
邮编 100048
电话：010-68482518
传真：010-68482519
电子邮件：info@bmst.net

智能审计是Session Auditor的又一大功能特色。主要功能分为定制审计计划、批量审计、以及单项审计等。这些审计功能都可以通过定制审计脚本，实现用户自义的内容审计规则。审计的数据源支持除了Terminal(SSH/TELNET)、数据库、FTP等各种文本协议，更能支持RDP的图形协议。审计内容的实用性是审计系统的核心。



附图6. 智能审计脚本

智能审计系统提供了大量的通用审计脚本，同时用户还可以根据自己业务的需求定制各种专用审计脚本。例如：对于RDP图形协议，通过脚本的定制，实现对密码的猜测，用户名的更换，删除任何文件（未知文件）的操作、以及特定的敏感字符串等等。审计结果将能直接定位到用户操作的实时回放界面。又例如：对于数据库可以定制脚本，将多条SQL语句

北京市海淀区车公庄西路甲 19 号华通大厦 A 座 720
邮编 100048
电话：010-68482518
传真：010-68482519
电子邮件：info@bmst.net

关联为一项行为操作等。 智能审计系统甚至能区分人为鼠标的移动与程序自动的鼠标移动，能识别整个会话有效操作与闲置的时间段并以曲线图形方式进行迅速定位。智能审计系统还能对于未纳入审计计划的数据源进行警示和定制处理。 定制审计计划可以使用计划任务的方式，将需要审计的内容统一纳入即时计划，可以定制一些事件触发时，自动执行这些任务计划。批量审计是采取人工方式，定制批量审计计划，对现有数据源进行审计。单项审计可以针对某一种特定的协议，进行特殊的审计，很适合进行事后取证分析。 智能审计系统还提供审计功能模块的接口，方便进行二次开发，更加适合用户业务环境的定制与开发。

2.13. 故障Bypass

Session Auditor 设备以透明的 inline 方式部署在网络中，如果一旦出现掉电或硬件故障，可能会影响网络的可用性。因此，Session Auditor 设备提供了故障 bypass 功能，当出现掉电或软硬件故障时，其两个流量转发端口将直接相连，使得用户的流量可以正常通过 Session Auditor 设备。

2.14. 审计内容的数据挖掘

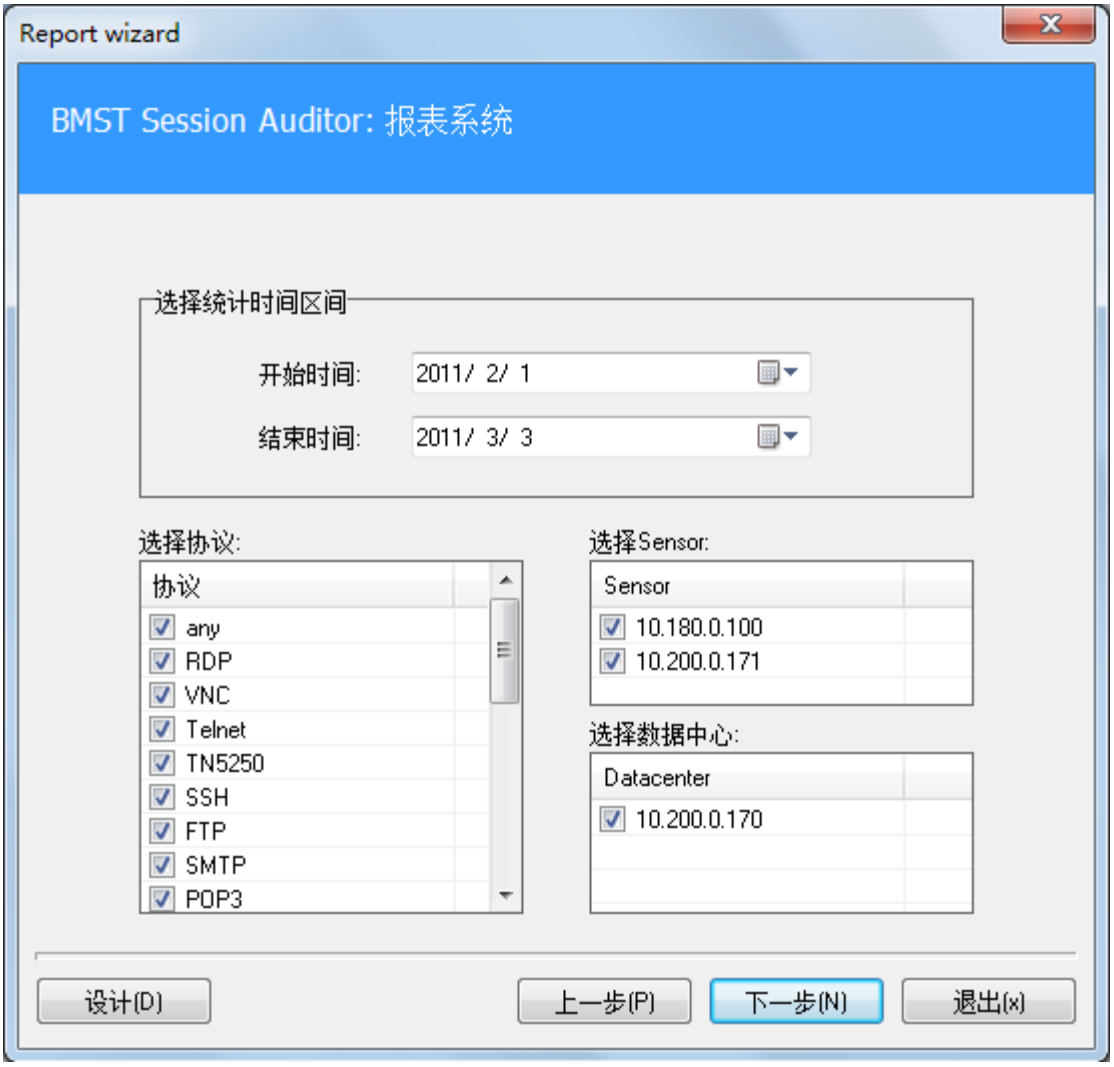
SA GUI Console 提供对会话审计记录的多功能组合查询。查询条件包括源/目的地址、源/目的端口、协议、会话起始时间或时间段、会话结束时间或时间段等。这些条件可以进行任意组合，复杂条件搜索可以制定对特定对象的审计条件过滤，还可以存为模板为下次使用。

2.15. 报表系统

Session Auditor提供灵活的报表系统，帮助管理员掌握一定时间段内的网络运行维护的整体状况和轨迹，

北京市海淀区车公庄西路甲 19 号华通大厦 A 座 720
邮编 100048
电话：010-68482518
传真：010-68482519
电子邮件：info@bmst.net

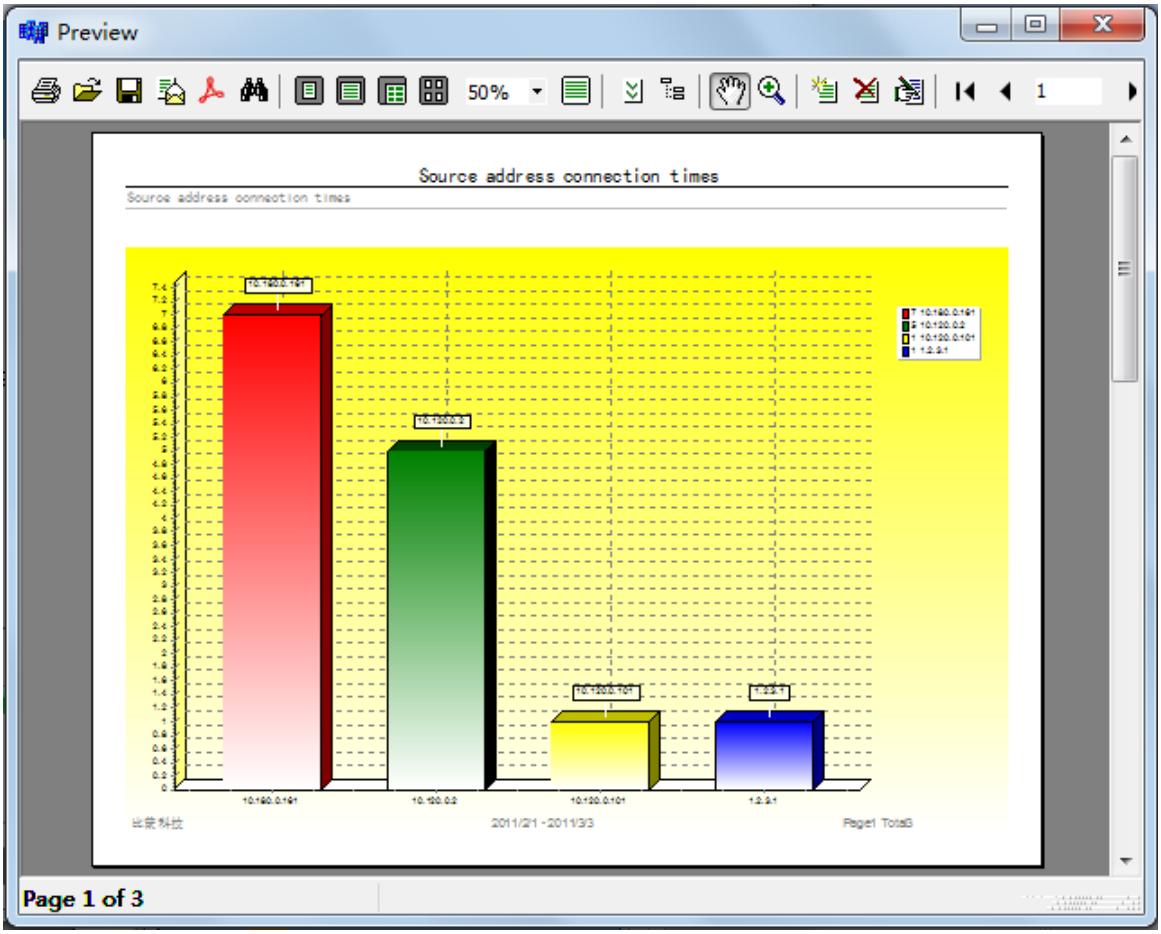
灵活易用的向导系统：



附图7. 报表定制系统

直观详尽的报表内容：

北京市海淀区车公庄西路甲 19 号华通大厦 A 座 720
邮编 100048
电话：010-68482518
传真：010-68482519
电子邮件：info@bmst.net

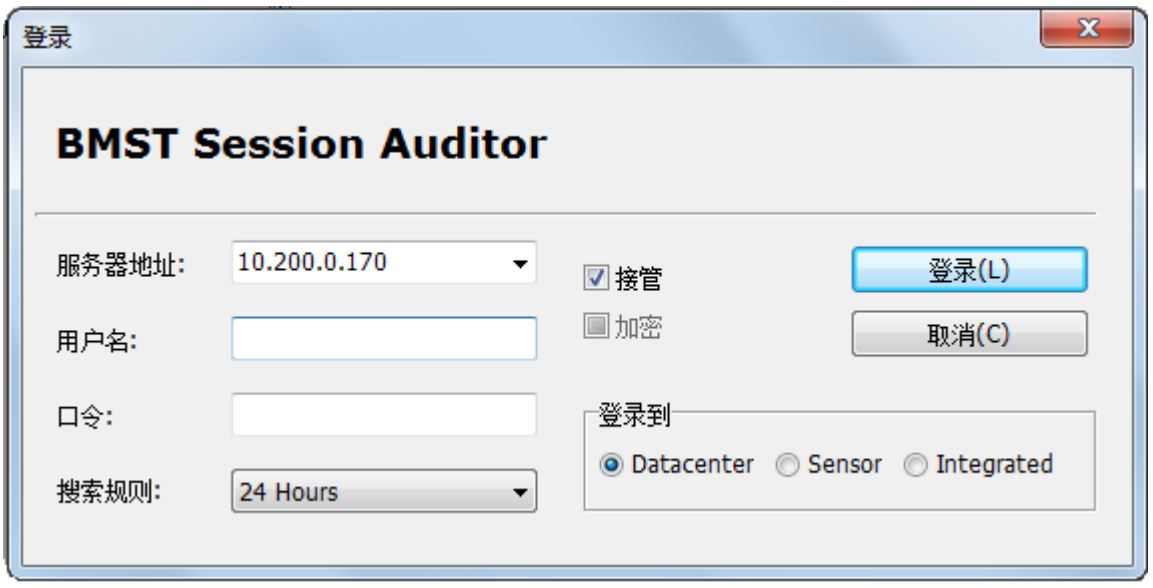


附图**8.** 友好的报表界面

2.16. 系统登录

Session Auditor的主控台采用专门开发的图形界面，如附图9 所示，管理员可以选择加密登录数据机和传感器，以规避窃听等安全威胁。另外，在主登录界面，管理员还可以选择已经保存过的历史查询条件，已提高管理效率。

北京市海淀区车公庄西路甲 19 号华通大厦 A 座 720
邮编 100048
电话：010-68482518
传真：010-68482519
电子邮件：info@bmst.net

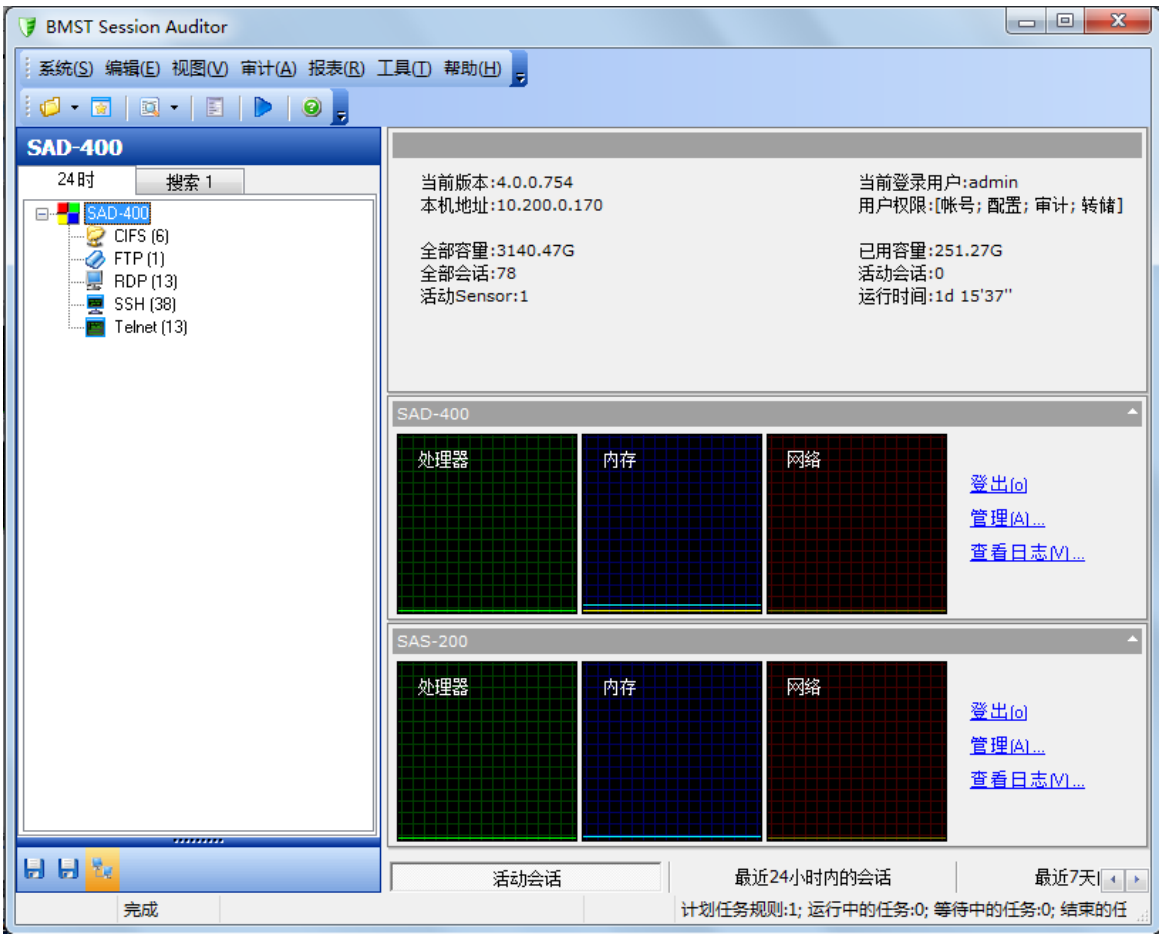


附图9. 控制台登录界面

2.17. 系统运行状态监视

Session Auditor的控制台提供对系统各个组件、整体系统运行状态以及审计输出结果的实时监视，如下图8所示。并且可以根据审计员设定的条件，对系统状态和审计输出产生报警事件。

北京市海淀区车公庄西路甲 19 号华通大厦 A 座 720
邮编 100048
电话：010-68482518
传真：010-68482519
电子邮件：info@bmst.net

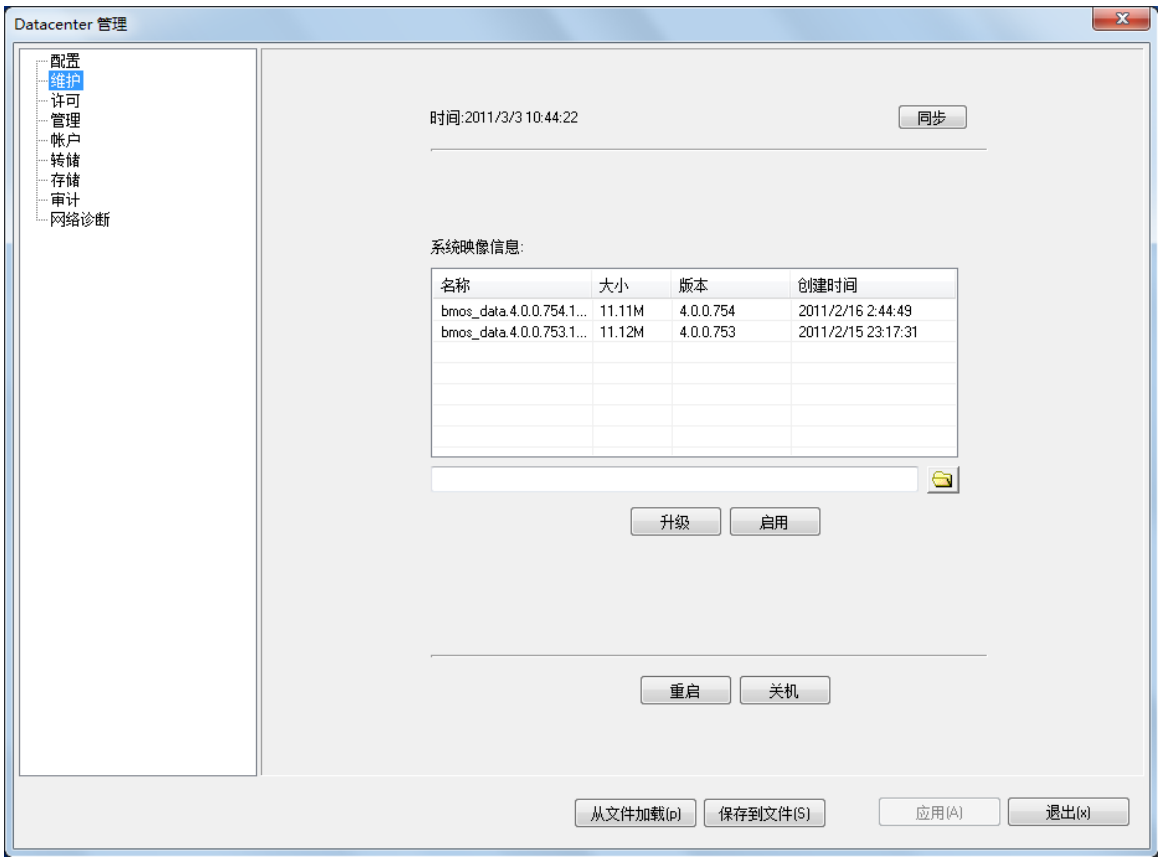


附图**10.** 系统运行状态监视

2.18. 系统在线升级与时间同步

Session Auditor除了提供强大的网络记录和审计外，还提供高效的运行维护手段。整体系统可以通过控制台在线方式的远程升级。如附图9. 所示，在控制台，可以集中地、远程查询并管理各个传感器和数据中心设备的系统版本和许可证，可以远程在线升级并即时启用。另外，控制台还可以对各个传感器和数据中心设备进行时间同步，以保证所有采集的审计数据的时间是真实、完整、可信的。

北京市海淀区车公庄西路甲 19 号华通大厦 A 座 720
邮编 100048
电话：010-68482518
传真：010-68482519
电子邮件：info@bmst.net



附图**11.** 系统维护和自动升级

2.19. 数据转储

通常审计数据可能需要保存若干年，Session Auditor提供会话数据转储功能，可以把保存在Session数据机上的会话数据转储到本地或者其他介质。同时，Session Auditor控制台也可以加载转储到本地的历史会话数据，并进行查询、回放等操作。

2.20. 实时事件通知功能

Session Auditor 控制台可以实时显示来自数据机与传感器的实时事件。实时事件包括实时

北京市海淀区车公庄西路甲 19 号华通大厦 A 座 720
邮编 100048
电话：010-68482518
传真：010-68482519
电子邮件：info@bmst.net

审计事件与设备运行过程中产生的需要管理员关注的事件。事件实时通知功能让管理员能立即发线。

2.21. 实时会话显示功能

Session Auditor 控制台界面中能实时感知新的会话开始及已连接会话的结束。实时会话显示方便监控特定的敏感会话。

2.22. 加密的通信协议

Session Auditor各个组件和模块之间采用高强度的加密通信协议以保证认证及审计数据传输过程中的安全性。2048位高强度RSA算法、随机生成密钥及挑战响应认证方式保证了通信的机密性，128位快速RC4加密算法保证了网络通信的高性能。

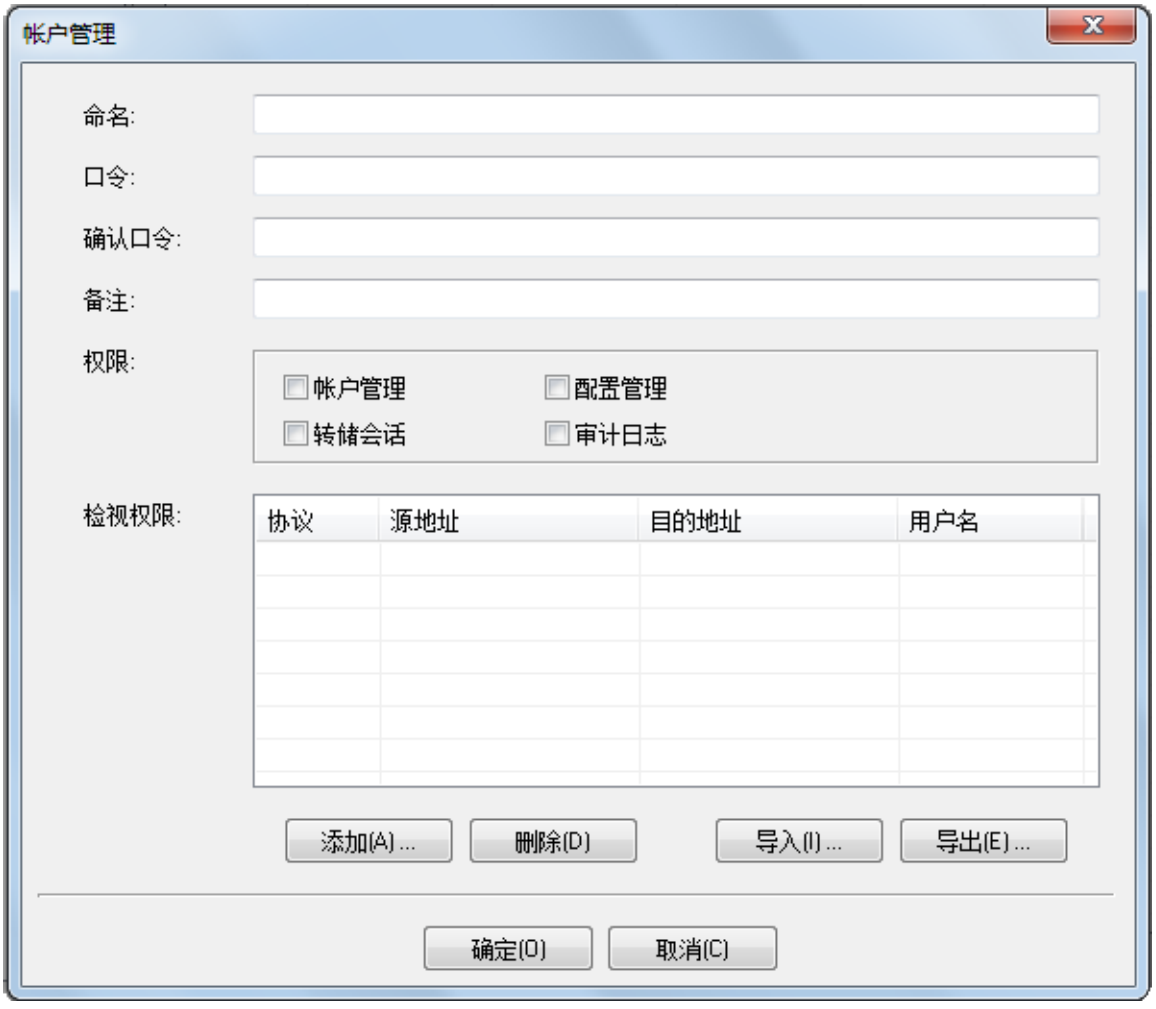
2.23. 传感器部署支持VLAN TRUNK

传感器可完全透明地部署在VLAN TRUNK中，以适应多种网络拓扑。

2.24. 分权的系统管理模式

Session Auditor系统中可创建多个具有不同权限的管理员，对系统配置的读写\转储\管理员账号的管理等权限进行分配。如附图12. 所示。

北京市海淀区车公庄西路甲 19 号华通大厦 A 座 720
邮编 100048
电话：010-68482518
传真：010-68482519
电子邮件：info@bmst.net



附图**12.** 创建不同权限的帐号

2.25. 对系统本身操作的完全审计

Session Auditor提供对系统本身操作的完全审计记录，例如系统帐号变更、配置变更、查询和转储操作等等。

2.26. 方便快速的串口配置功能

北京市海淀区车公庄西路甲 19 号华通大厦 A 座 720
邮编 100048
电话：010-68482518
传真：010-68482519
电子邮件：info@bmst.net

传感器及数据机都提供串口配置界面，管理员可通过菜单界面快速地对传感器及数据机进行基本配置，包括网络地址、恢复口令、恢复出场设置等。

2.27. 网络部署灵活多样

Session Auditor以完全透明的方式部署，这种部署方式对网络拓扑改动最小。一般情况下，只需把交换机与路由器之间的网络连接线取下，并分别与设备的转发端口相连即可完成部署。

这种网关类型的部署方式特点是会话信息不可旁路，采集到的审计信息不会有丢包，信息内容不可能被篡改。

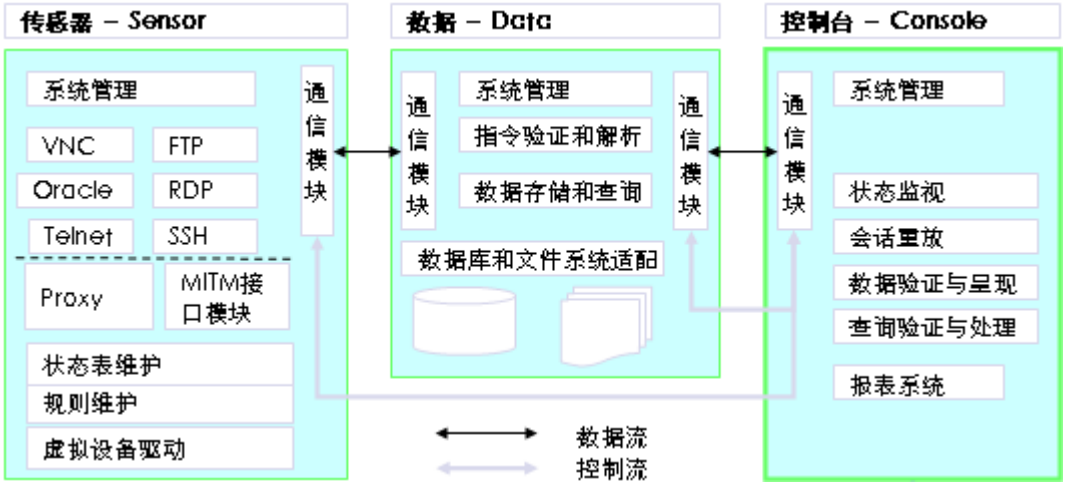
Session Auditor以VPN的方式部署，这种部署方式可以满足需要将业务流量和管理流量分开的网络环境，这种部署方式支持VPN认证，可将业务流量和管理流量分开，仅对管理流量进行审计。

Session Auditor以路由、桥方式部署，这种部署方式适合多元化的网络环境，既可满足透明的部署需求，又可以满足将业务流量和管理流量分开的需求；同时也减少了投资成本。

3. Session Auditor系统架构

如图所示，Session Auditor由传感器（SAS）、数据中心（SAD）和控制台（SAC）等三个系统模块组成，它们的主要功能分别是：

北京市海淀区车公庄西路甲 19 号华通大厦 A 座 720
邮编 100048
电话：010-68482518
传真：010-68482519
电子邮件：info@bmst.net



- 传感器：收集并预处理各种网络会话对应的数据，并上传至数据机
- 数据：收集传感器获得的各种网络会话数据，并按照控制台的控制指令进行相应的处理和查询
- 控制台：人机界面，提供各种管理功能，并且负责监视审计系统的整体运行状况。

附图**13.　Session Auditor**系统架构图

传感器-SAS

- 内核模块独立保证系统高效稳定运行
- 用户模块实现数据的采集，对协议扩充的灵活支持
- 防火墙/防DOS模块的嵌入和灵活配置
- 以桥方式工作，支持VLAN TRUNK，使部署容易，对使用者/被监控者完全透明
- 内核模块工作在三层以下，支持对所有正常/异常包的记录和检测
- 用户模块基于会话(Session)的记录，使记录的结果具有意义，并能完全回放

北京市海淀区车公庄西路甲 19 号华通大厦 A 座 720
邮编 100048
电话：010-68482518
传真：010-68482519
电子邮件：info@bmst.net

数据中心-SAD

- 数据机的使用，保证对四层以上数据的独立分析，而完全不影响网络性能
- 数据机的集中分布式管理能进行灵活的部署，并保护投资
- 数据机与其他部件的加密通信，保证记录和审计数据的安全
- 数据机自动进行时钟同步，保证所有分布记录的时间准确性和唯一性
- 数据机的海量存储能保证所有记录的完全备案可查
- 数据机的智能审计与高效搜索查询能方便快速定位

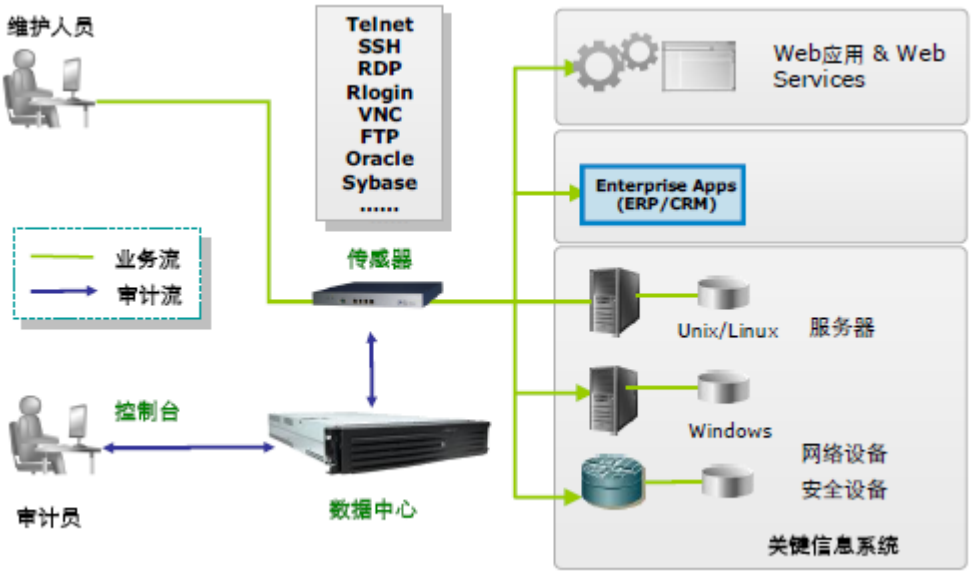
控制台-SAC

- 控制台支持集中地对数据机、传感器的分布分权管理
- 控制台能实现对所有记录协议数据，按照会话过程的完全回放
- 业界唯一的远程桌面操作(RDP)会话的透明支持与完全记录及回放
- 业界唯一的SSH、VNC等多种协议的透明支持与完全记录及回放
- 多种数据库协议、常用协议透明支持及按照会话过程的完全回放
- 使用文件共享的文件读、写操作完全记录。
- 能实时获取、显示各种设备事件与审计事件
- 控制台能对监控数据、统计数据实时获取，友好的界面对图形图表方式直观显示
- 报表系统能定制和自动生成中文报告

4. Session Auditor的部署

北京市海淀区车公庄西路甲 19 号华通大厦 A 座 720
邮编 100048
电话：010-68482518
传真：010-68482519
电子邮件：info@bmst.net

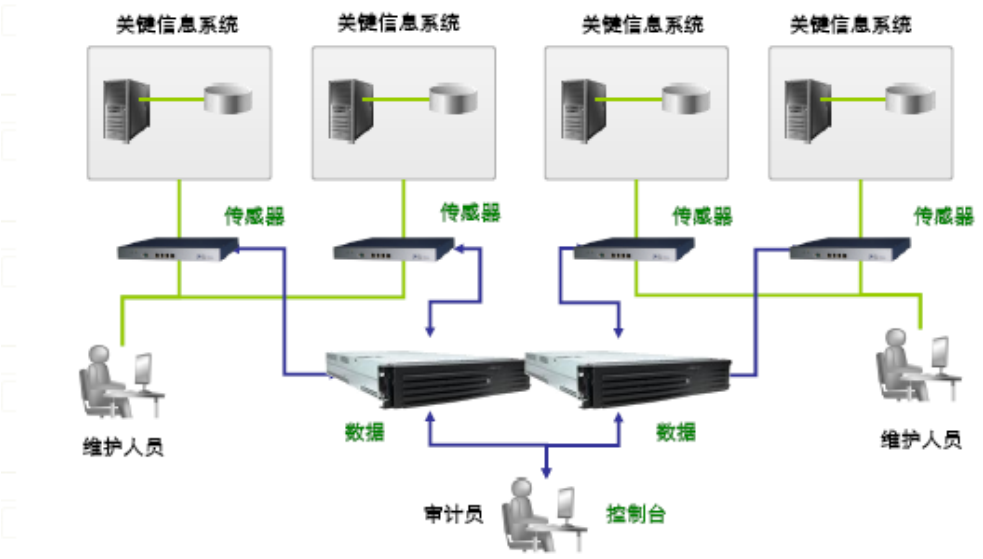
部署机架式硬件构成的传感器和数据机是一件非常轻松的工作。如附图12. 所示是一个典型的信息系统环境，大量的关键服务器设备集群布放于右图所示的设备间，而管理、运行、维护、开发人员在左面所示的操作间工作，中间通过交换机连接。SA的传感器就以透明方式桥接在这个链路上面。传感器通过第三个端口与数据机和控制台通信。



附图**14.　Session Auditor**部署示意图

传感器和数据机都支持层次化部署和管理维护，可以按照业务分布和流量分别部署多个，支持大规模、两级架构的网络和管理环境，提供良好的可扩展性和性能均衡，提高审计系统覆盖面和可用性。

北京市海淀区车公庄西路甲 19 号华通大厦 A 座 720
邮编 100048
电话：010-68482518
传真：010-68482519
电子邮件：info@bmst.net



附图**15.　Session Auditor**支持层次化的部署

5. Session Auditor的优势

在内控和安全审计的重要性与日俱增的今天，Session Auditor为大型企业和组织的内控和符合性旅程带来了前所未有的系统增益。它的主要优势体现在：

- 业界唯一的远程桌面操作(Windows Remote Desktop Protocol)、Citrix ICA、VNC等会话的透明支持，能够对WINDOWS远程维护进行完全记录及回放，实现了对图形界面操作的审计。

- 业界唯一的SSH、SFTP、SCP以及SSH PORT FORWADING会话的SSH系列全功能的透明支持，能够对UNIX下加密登录远程维护进行完全记录及回放。

- 旁路/监听方式会因为仅丢失一个数据包而导致数据的不可用，不符合审计全面性的基本要求；为克服这个弊端，Session Auditor产品采用的是PROXY方式，保证不会丢失

北京市海淀区车公庄西路甲 19 号华通大厦 A 座 720
邮编 100048
电话：010-68482518
传真：010-68482519
电子邮件：info@bmst.net

任何数据，并且能够完全回放；支持BYPASS功能。

- 强大的智能审计系统，方便进行用户内容审计脚本的定制，除了支持SSH/TELNET、数据库等文本协议，更能支持RDP的图形协议。
- 内置防火墙的访问控制功能，灵活定制策略，可以完全取代内网防火墙。
- 支持Telnet、FTP、SNMP 、Rlogin、Oracle、Sybase、MS SQL、POP3、SMTP以及CIFS/SMB等多种加密和非加密协议的审计。
- 支持对未知协议（用户自定义协议）的RAW数据记录，只需要指定未知协议的端口号就可进行记录，并且可以方便地进行二次开发。
- 透明桥方式的网络部署，不用改变客户端和服务器端的任何配置，客户端不需要经过堡垒主机/二次跳转方式登录服务器，大幅降低审计系统的部署和管理维护负担。
- 层次化的集中分布式的部署方式提供了非常强的灵活性和可扩展性，支持大规模的网络环境。
- 完善的自身认证和加密方案，确保审计过程的保密性和完整性。
- 审计机制不可旁路、审计信息不可窜改。
- 基于角色的访问控制系统和数据备份恢复机制，确保审计数据的保密性、完整性和可用性。
- 灵活的部署方式可以满足不同用户的网络需求。
- 支持外部数据库认证、RADIUS认证、VPN认证和WEB认证，多种认证方式可供用户灵

北京市海淀区车公庄西路甲 19 号华通大厦 A 座 720
邮编 100048
电话：010-68482518
传真：010-68482519
电子邮件：info@bmst.net

活选择。

关于比蒙科技

北京比蒙科技有限公司（以下简称“比蒙科技”）总部设在北京中关村科技园区，成立于2006年3月，是目前中国优秀的专注于网络安全产品和技术创新的高科技公司之一。创业团队成员拥有多年的电信运营商运营维护经验，以及多年的网络安全产品设计和研发经验，他们在国际国内领先的网络安全专业技术公司有令人自豪的职业经历。他们对安全运营和技术需求有着充分的理解和认识，对于安全产品的创新和开发拥有敏锐的观察和触觉。比蒙科技通过对市场的感知和对技术的深入研究，可以为各行业、各层次的客户群提供实时的、有效的网络安全解决方案和专业化的信息安全服务。

北京市海淀区车公庄西路甲 19 号华通大厦 A 座 720
邮编 100048
电话：010-68482518
传真：010-68482519
电子邮件：info@bmst.net