SAC安全审计管控系统
技术白皮书

震康科技 ZHENCON

ZHENCON Beijing Co., Ltd.

震康科技（北京）有限公司

（for internal use only）
（仅供内部使用）

Prepared by 拟制		Date 日期	
Reviewed by 审核		Date 日期	
Approved by 批准		Date 日期	

目　　录

1 简介

1.1 目的

本文档为SAC安全审计管控系统的技术白皮书，涵盖系统的各种技术介绍，是了解SAC安全审计系统的技术指南。

1.2 范围

本文档适用于SAC全系列产品。

1.3 约定

安全审计管控系统简称：SAC（security audit control）。也称运维审计系统。是指在某一个特定的网络环境下，为了保障网络和数据不受来自内部合法用户的不合规操作带来的系统损坏和数据泄露，而运用技术手段实时收集和监控网络环境中每一个组成部分的系统状态、安全事件、网络活动，以便集中报警、记录、分析、处理的一种技术手段。

2 背景

2.1 现状

随着信息技术的不断发展和信息化建设的不断进步，业务应用、办公系统、商务平台不断推出和投入运行，信息系统在企业的运营中全面渗透。电信行业、财政、税务、公安、金融、电力、石油、大中型企业和门户网站，使用数量众多的网络设备、服务器主机来提供基础网络服务、运行关键业务，提供电子商务、数据库应用、ERP 和协同工作群组等服务。由于设备和服务器众多，系统管理员压力太大等因素，越权访问、误操作、滥用、恶意破坏等情况时有发生，这严重影响企业的经济运行效能，并对企业声誉造成重大影响。如何提高系统运维管理水平，跟踪服务器上用户的操作行为，防止黑客的入侵和破坏，提供控制和审计依据，降低运维成本，满足相关标准要求，越来越成为企业关心的问题。

2.2 问题

2.2.1 口令管理问题

口令管理主要问题：

1. IT 系统的口令需要定期修改，口令变更工作量巨大。
2. 口令强度要满足安全要求，口令修改难度增加。
3. 高强度口令难于记忆，使用不方便。
4. 口令明文存储，容易泄露。
5. 口令设置为规律性口令，很容易猜测和破解其他系统的口令。

2.2.2 帐号管理问题

帐号管理主要问题：

1、共享帐号，出现问题无法追踪，不符合国家关于信息安全"谁使用，谁负责"的原则。

2、离职员工帐号不能及时删除，留下安全隐患。

3、全局帐号，一旦该帐号出现安全问题，则患及全局。

4、无法将帐号与具体的自然人相关联。

2.2.3 权限控制问题

大多数企事业单位的 IT 运维均采用设备、操作系统自身的授权系统，各系统分别管理所属的系统资源，为本系统的用户分配权限，无法严格按照最小权限原则分配权限。另外，随着用户数量的增加，权限管理任务越来越重，当维护人员同时对多个系统进行维护时，工作复杂度会成倍增加，安全性无法得到充分保证。

2.2.4 访问控制问题

访问控制主要问题：

1、 没有一个清晰的访问控制列表，无法一目了然的看到什么用户能够以何种身份访问哪些关键设备。

2、 无法精细控制：如控制访问的 IP、时间点、登录方式、登录帐号等

3、 缺少有效的技术手段来保证访问控制策略有效地执行。

2.2.5 系统审计带来的安全隐患

企业内网各 IT 系统独立运行、维护和管理，所以各系统的审计也是相互独立的。审计的机制、格式和管理都不尽相同，就会带来各种问题。例如，每个网络设备，每个主机系统分别进行审计，安全事故发生后需要排查各系统的日志，但是往往日志找到了，也不能最终定位到行为人。尤其是针对许多外包服务商、厂商技术支持人员、 项目集成商等在对企业核心服务器、网络基础设施进行现场调试或远程技术维护时，无法有效的记录其操作过程、维护内容，极容易泄露核心机密数据或遭到潜在的恶意的破坏。

2.2.6 面临安全合规性法规遵从的压力

为加强信息系统风险管理，政府、金融、运营商等陆续发布信息系统管理规范和要求，如"信息系统等级保护"、"商业银行信息科技风险管理指引"、"企业内部控制基本规范“等均要求采取信息系统风险内控与审计。

2.2.7 缺少运维管理

很多用户在运维方面，由于没有统一管理系统来收集和分析运维数据。运维随意、缺乏规范，运维导致的事故问题和运维过程中存在的问题无法定位和定性。IT 主管无法得知真实的运维状况。

2.3 案例

2.3.1 内部管理风险

某银行员工使用跳槽同事的帐号在银行系统中掩盖他亏损 49 亿欧元的交易。
某第三方支付公司 20G 用户交易数据被内部非授权员工下载并有偿出售给电商公司。

2.3.2 IT变更风险

某设计研究院全院网络瘫痪 48 小时，无法追踪故障缘由和责任人。事后发现是网管员孙某误修改路由器配置导致。

2.3.3 第三方运维风险

上海市公安局侦破张某每个月都在家里从其所在公司负责维护的上海市卫生局数据库下载数据，导致数十万婴儿信息泄漏。

2.3.4 信息泄漏风险

2013 年一批连锁酒店的 2000 万开房记录遭泄漏，包括入住客人的身份证号，入住退房时间等。如果每个案件法院都能判决被告赔偿 20 万元，总赔偿金额或将高达 4 万亿元，数额史无前例。

3 设计理念

3.1 核心功能

SAC 核心功能包括：**运维管控**和**安全审计**两大功能。
1、能够有效拦截非法访问、恶意攻击等，对不合规字符、命令进行输出阻断，过滤掉所有对目标设备的非法访问行为。
2、能对运维过程进行监控记录，通过查看回放等进行审计。

3.2 三权分立模型

SAC 安全审计管控系统，采用三权分立模型，避免权利集中带来的安全风险。拥有管理权的人员没有使用权且受到有监督权的人员监督。拥有监督权的人员没有使用权且受到有管理权的人员管理。拥有使用权的人员受到有监督权的人员的监督和有管理权的人员的管理。三权相互独立、相互制约，对内部操作进行有效安全的审计。此外所有操作人员的行为和 SAC 系统自身均受到 SAC 系统的审计。

3.3 4A要求

SAC 安全审计管控系统符合 4A 要求，具备集中账号(Account)管理、集中认证(Authentication)管理、集中权限(Authorization)管理和集中审计(Audit)管理功能。

3.4 5W1H授权模型

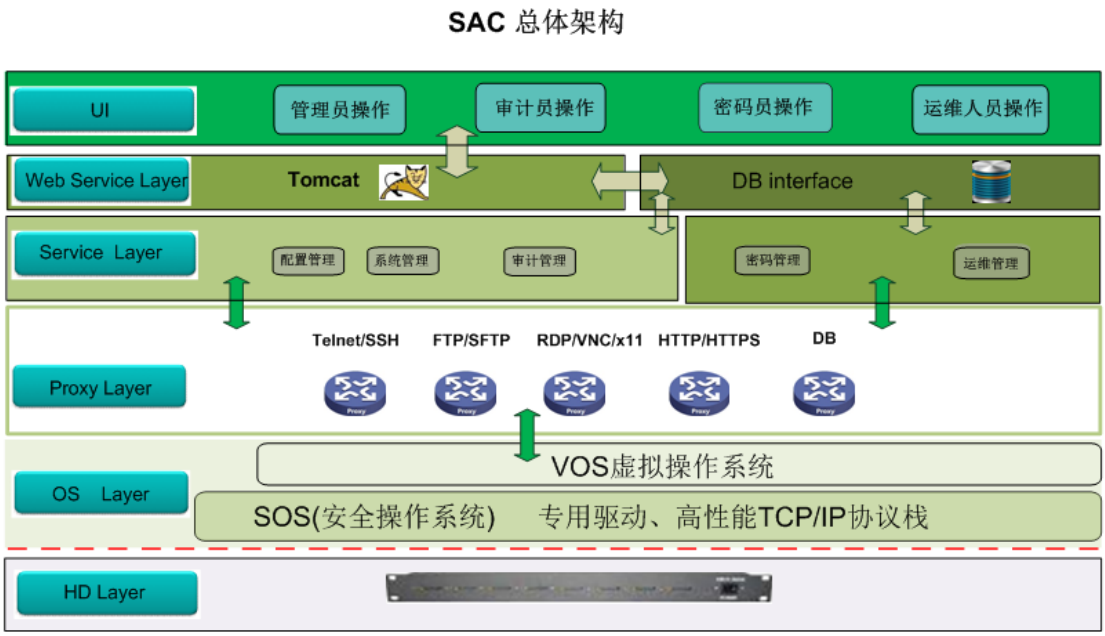
SAC 系统采用独有的 5W1H 模型进行精细授权管理。

谁(who)–什么时间(when)–从哪里(where)–怎么访问(how)–访问哪个设备(which)–能做什么(what)。

通过 5W1H 模型，系统授权覆盖运维操作全部要素。

4 系统概述

4.1 系统架构



4.2 主要功能

4.2.1 设备管理

设备管理提供以下功能：

1. 设备分组管理。
2. 设备拓扑显示。
3. 设备状态、可用性监控。
4. IT 资产管理。

4.2.2 帐号管理

帐号管理提供以下功能：

1、 集中帐号管理，包含对所有服务器、网络设备帐号的集中管理。
2、 帐号和自然人的关联。
3、 帐号整个生命周期的监控。
4、 集中认证管理。
5、 制定统一标准的用户帐号安全策略。

4.2.3 密码管理

系统提供密码管理功能，可以周期性对服务器和设备的密码进行自动修改，并按策略保证密码复杂程度。所有密码进行加密存储。管理员可以密码策略设定改密周期、密码强度等。

4.2.4 授权管理

SAC 授权采用 5W1H 模型。

谁(who)-什么时间(when)-从哪里(where)-怎么访问(how)-访问哪个设备(which)-能做什么(what)。

支持用户对设备，用户对设备组，用户组对设备，用户组对设备组授权。此外增加访问帐号、协议和访问策略（IP、时间、命令）。对整个访问过程全面监管不留权利死角。

4.2.5 单点登录

SAC 系统提供了基于 B/S 的单点登录（SSO）功能，用户一次登录 SAC 后，可以无需认证的访问被授权的多种设备。系统简化账号登录过程并保护账号和密码安全，用户无需记忆多种登录用户名和口令。系统向用户仅提供其授权资源的快捷访问方式，降低了维护的复杂度大大提高了维护工作效率。

4.2.6 密码代填

登录 SAC 系统后，在访问已授权设备过程中，无需输入账号和口令，系统自动代填。用户可以一键登录。且账号和口令对运维用户不可见，有效降低了设备账号和口令在使用中泄密的风险。

4.2.7 集中认证

系统为用户提供不同强度的认证方式，除静态口令方式外，还提供符合双因素认证要求的高强度认证（动态口令、数字证书、一次性口令）。不仅可以实现用户认证的统一管理，而且可以为用户提供统一的认证门户，实现设备资源访问的单点登录。

此外还支持 Windows AD 域、RADIUS、LDAP 等多种认证方式，而且系统具有灵活的定制接口，可以方便的与其它第三方认证服务器结合。

4.2.8 危险阻断

安全审计管控系统能够提供指令级细粒度的访问控制。管理员可以设定每个用户能够使用的指令集和告警规则，系统会自动识别用户输入的命令，对应采取阻断、告警、放行操作。

从而最大限度保护目标设备的安全。系统提供的告警方式包括：邮件、Snmp、syslog 等。

4.2.9 日志审计

系统提供对Telnet、FTP、SFTP、SSH、RDP、X11、AS400等会话的完整记录和审计分析，通过不同方式展现给审计人员。

1、针对命令交互方式的协议，提供逐条命令操作文本结果和回放方式的显示。

2、针对图形协议提供回放，真实直观地重现当时的操作过程。

3、提供以会话为单位的条件查询。条件查询支持按运维用户、源地址、协议、设备地址、起始时间、结束时间、帐号和操作内容关键字等进行组合。

4、支持日志的备份和删除操作。

4.2.10 综合报表

系统根据审计数据进行汇总统计，产生适用于不同身份角色的报表。 包括：运维统计、设备统计、协议统计、告警事件统计、内部操作统计、IT 资产统计等。能从多个纬度进行查询分析，并以柱状图、饼图、曲线图、折线图等形式展示。

5 关键技术

5.1 负载均衡

系统通过底层处理，使网络报文根据不同的网段自动选择相应的网口进行通讯。保证大量运维操作可以并发执行。

5.2 深度协议解析

系统采用透明协议解析，摒弃业界常用的协议转发“黑盒子”，不依赖操作系统某些机制，提高了系统可靠性。对协议进行深度分析处理，可以完整还原操作全过程，大大降低会话日志信息量。

5.3 命令识别

系统采用智能算法，分析输入输出流，结合上下文自动识别操作命令。准确识别命令的不同操作状态。

5.4 多核多线程技术

SAC 系统利用 64 位高性能多核 CPU 的并行处理为协议数据处理提供快速运算。通过流引擎和多核多线程动态调度算法，将每个核的负载进行分担，保证所有业务的高性能流畅运行。

6 产品优势

6.1 专用硬件平台

采用网络安全专用硬件平台。提供强大计算性能和网络报文处理能力。集成了丰富的安全协处理硬件，如：加密、正则匹配，应用加速等。机箱集成液晶面板和专用指示灯，可显示运行状态和故障并能进行异常声光报警，保障设备安全稳定运行。

6.2 嵌入式系统

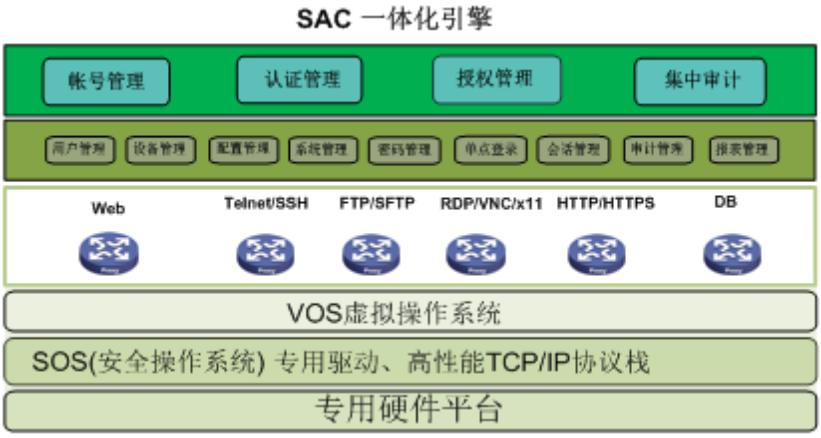
采用嵌入式操作系统，具有高效、智能、安全、健壮、易扩展等特点，实时响应，高可靠性。系统经过内核裁减，只保留了少数相关的服务与功能，系统内核达到最小化，使操作系统的额外开销与不稳定因素减至最小。此外采用特有的文件系统，使系统能抵御突然掉电等物理灾害造成的对系统的损害。

6.3 高效TCP/IP协议栈

采用专用的驱动程序，减少数据在不同模块间的传递环节，使数据通过 DMA 的方式直接传递给应用程序空间，减少 CPU 的参与及数据拷贝的次数，提高处理速度。通过参数调整和目的地址路径选择优化，提高了 socket 的性能保证网络传输速度和可靠性。

6.4 一体化引擎

SAC 系统采用构建在专用硬件平台和 SOS 安全操作系统上的一体化引擎。它将 web、数据库、协议分析、系统管理等多个子系统无缝集成于单一平台。统一架构，去除冗余，优化数据处理流程，实现统一处理。各子系统统一进行负载分担，保证系统高效运行。



6.5 自身安全防护

SAC 系统采用多种措施保证自身安全：

1. 系统采用双固态硬盘存储，确保信息万无一失。
2. 支持热插拔的冗余双电源，避免电源硬件故障时设备宕机，具有更强的高可用性。
3. 系统自带内部防火墙，将攻击挡在外面。
4. 系统仅开放必需的协议标准端口，不给入侵提供可乘之机。
5. 系统采用 https 加密协议进行 web 访问，保证访问过程不被监听。
6. 系统数据加密存储，防止泄漏和篡改。
7. 系统支持 HA 双机热备和 NAS 外部存储。

6.6 多种告警同时支持

SAC 系统提供多种响应方式，支持同时以多种方式发送告警信息。如：Snmp，Syslog，Email、短信等。并可与第三方平台进行联动，使用户第一时间收到告警信息。

6.7 绿色部署

系统采用绿色部署，不需要在被管理设备上安装代理程序，不需要改变网路拓扑结构，不影响原有应用系统运行，全web方式操作，支持分布式部署和级联部署。

6.8 自动运维

系统提供自动巡检、智能监控，IT 资源使用率一目了然。

7 核心价值

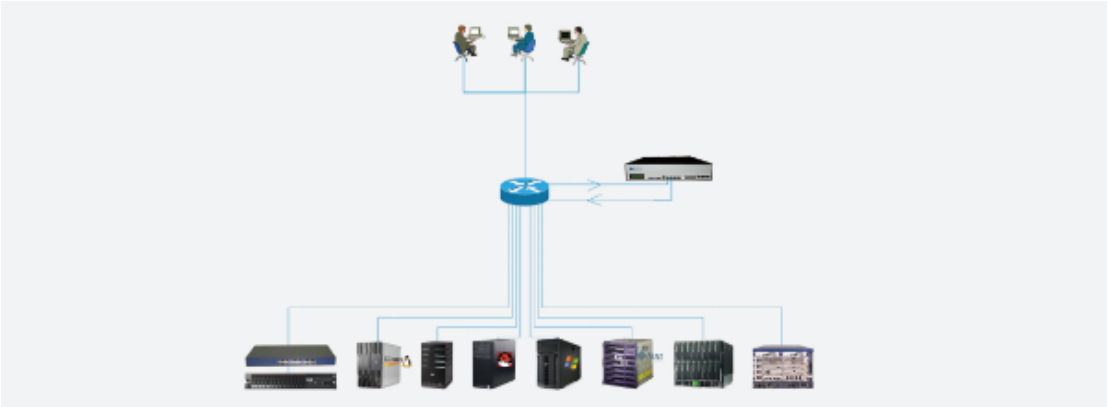
SAC 核心价值

8 产品部署

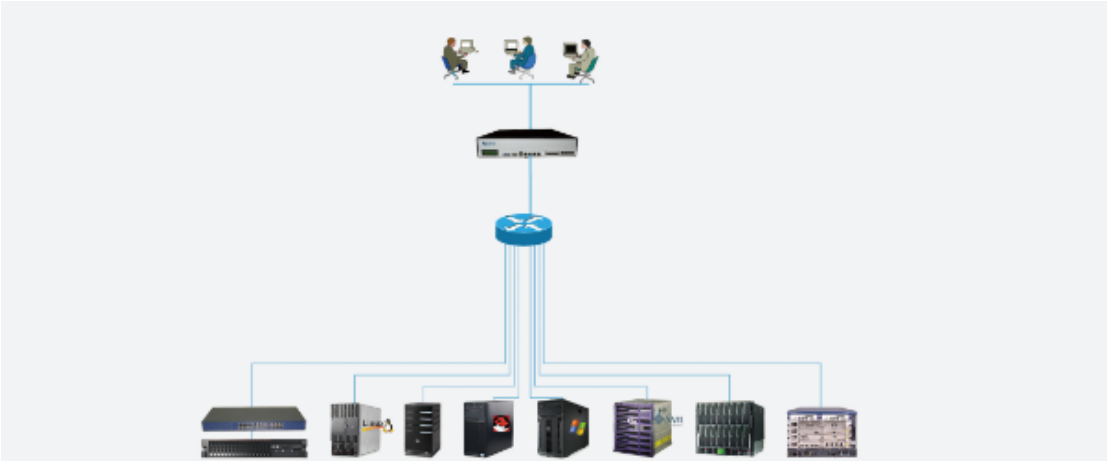
SAC 系统提供了两种常用部署方式：旁路部署方式和直路部署方式。

采用旁路方式部署到网络中时，无需改变原有网络结构。采用直路方式部署到网络中时，具有一定的网闸功能，可以限制对核心 IT 设施的管理访问。

两种部署方式均不会影响原有业务系统，且无需在被管控设备中安装任何软硬件。



SAC 旁路部署



SAC 直路部署

9 技术参数

SAC 规则参数：

产品型号	SAC 100	SAC 200	SAC 500	SAC 1000
体积规格	1U	2U	2U	2U
支持协议	Telnet、FTP、SSH、RDP、Rlogin、VNC、X11			
部署模式	直路/旁路	直路/旁路	直路/旁路	直路/旁路
管理方式	B/S			
HA 模式	不支持	支持	支持	支持
存储容量	500G	1T	1T	2T
电源接口	1	1	1	2
管理设备数	50	100	200	500
外部存储	不支持	不支持	支持	支持

（以上仅供参考，具体以实机为准。）

10 产品服务

10.1 售后服务

安全审计管控系统自产品出售之日起，提供一年期的免费售后服务，具体售后服务包括：

1、 **软件升级服务：**提供一年免费产品升级。
2、 **硬件质保服务：**提供一年免费硬件质保。
3、 **产品培训服务：**提供产品的部署和使用培训。
4、 **技术支持服务：**提供 5 x 8 小时技术支持。
5、 **产品咨询服务：**提供关于产品的功能、配置和使用咨询。

自产品出售之日起满一年后，提供有偿售后服务。有合同约定的，按合同约定执行。具体包括：

1、 **产品升级服务：**帮用户升级最新版本。
2、 **技术支持服务：**提供 7 X 24 小时技术支持。
3、 **产品咨询服务：**提供关于产品的配置、功能和使用咨询。

10.2 技术支持

为用户提供如下技术支持：

远程技术支持：通过电话、网络等方式提供使用、维护和升级支持。

现场技术支持：对无法远程解决的问题，由工程师到用户现场，为用户提供技术支持。

11 联系方式