任子行运维安全审计产品白皮书

■ **文档编号**	1.0	■ **密级**	内部
■ **版本编号**	V1.0	■ **日期**	2015-06-05

■ 版权声明

■ 版本变更记录

时间	版本	说明	修改人
2014-6-5	V1.0	产品白皮书	刘磊

■ 适用性声明

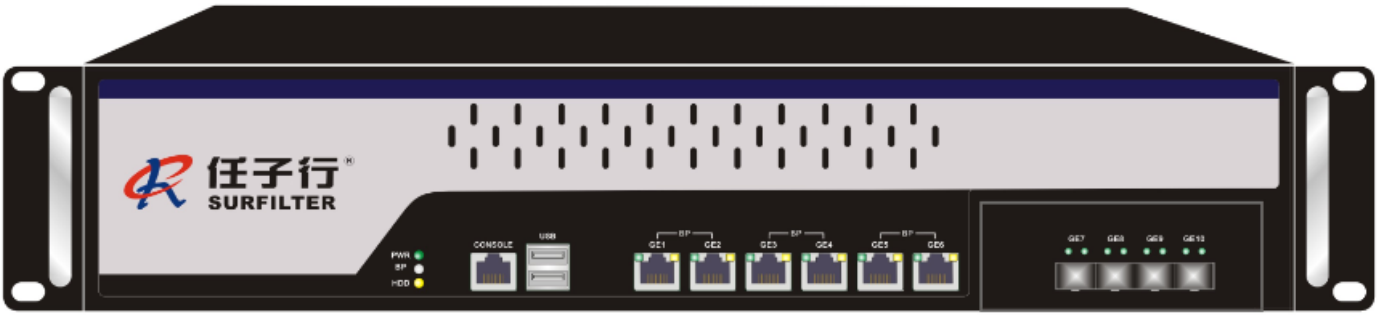
本模板用于撰写任子行内外各种正式文件，包括技术手册、标书、白皮书、会议通知、公司制度等文档使用。

目录

一 产品概述

传统的安全设备都是管理和审计组织内部员工的上网情况，对 IT 管理员的管理是一片空白。“SURF-HAC 运维安全审计系统”是一款管理“管理员”的设备，其目标是为组织 IT 系统核心服务器的运维操作提供强有力的监控、审计手段，使其切实满足内控管理中的合规性要求。

SURF-HAC 运维安全审计系统可对主机、服务器、网络设备、安全设备等的管理维护进行安全、有效、直观的操作审计，对策略配置、系统维护、内部访问等进行详细的记录，提供细粒度的审计，并支持操作过程的全程回放。SURF-HAC 运维安全审计系统弥补了传统审计系统的不足，将运维审计由事件审计提升为内容审计，并将身份认证、授权、管理、审计有机地结合，保证只有合法用户才能使用其拥有运维权限的关键资源。SURF-HAC 运维安全审计系统为组织在 IT 操作风险控制、内控安全和合规性等方面提供一套完善、有效的审计手段。



图：任子行运维安全审计系统

二 产品特点

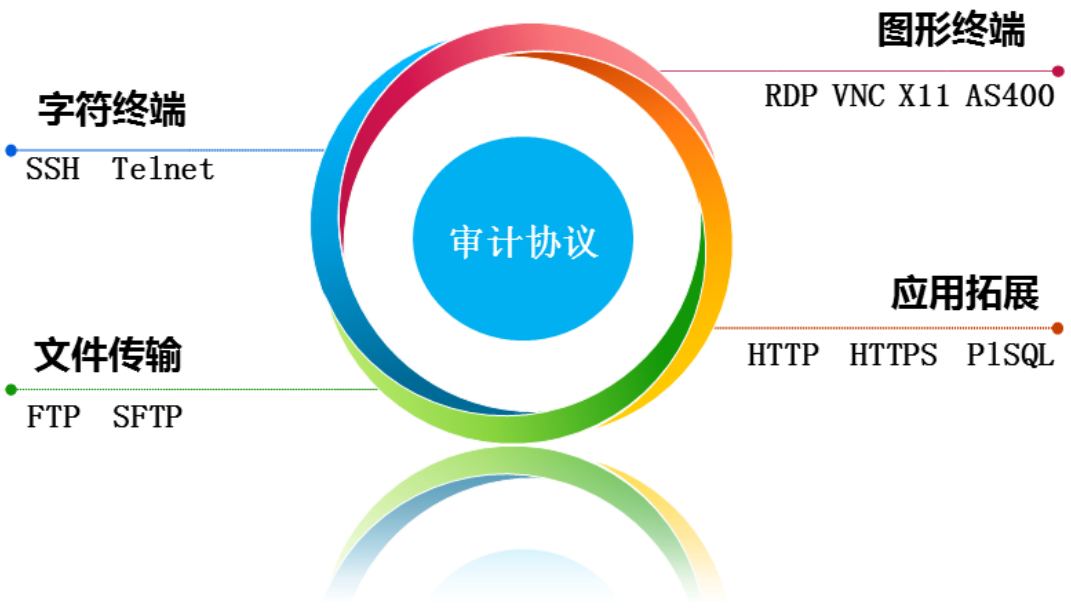
全面的运维审计

系统采用协议分析、基于数据包还原虚拟化技术，实现操作界面模拟，将所有的操作转换为图形化界面予以展现，实现 100%审计信息不丢失。

针对运维操作图形化审计功能的展现外，同时还能对字符进行分析，包括命令行操作的命令以及回显信息和非字符型操作时键盘、鼠标的敲击信息。

系统支持的审计协议以及工具包括：

- 终端字符命令操作：Telnet、SSH
- Windows 图形：RDP、VNC、X11 pcAnywhere、DameWare 等
- Unix/Linux 图形：Xwindows
- AS400 主机图形：AS400
- 文件上传和下载：FTP、SFTP
- 应用终端操作操作：HTTP、HTTPS
- 数据库管理工具：PLSQL 等工具

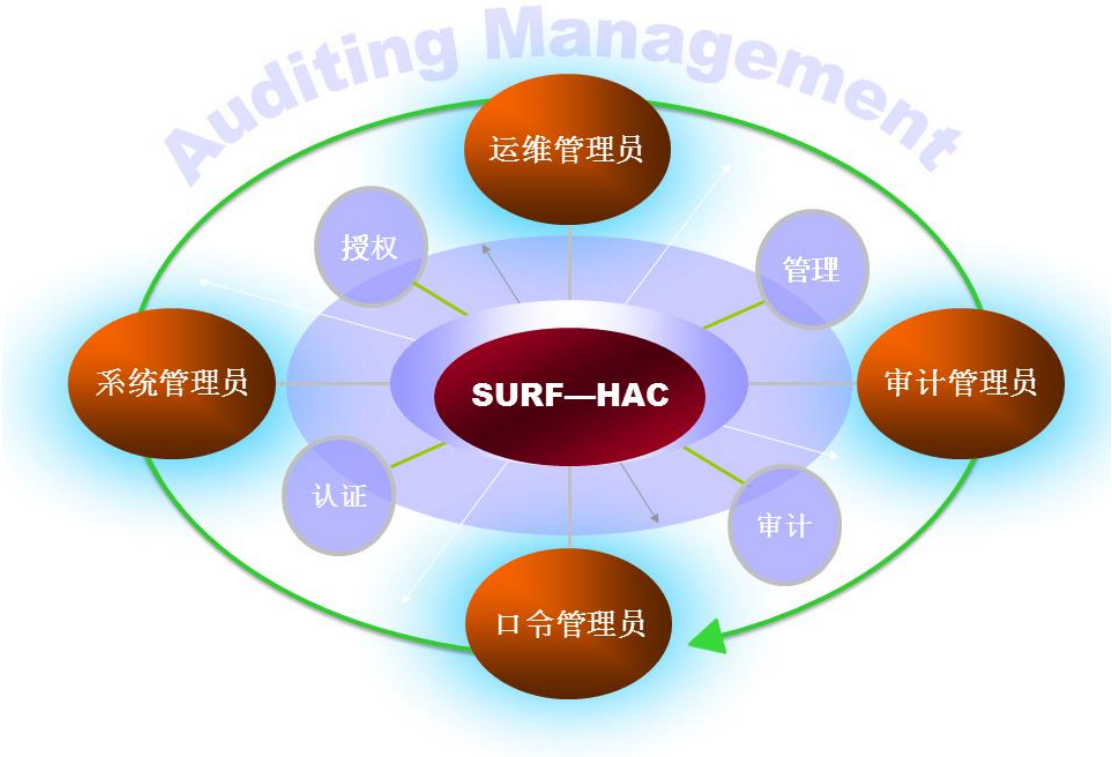


更专业的审计管理

系统提供四权分立的管理模式，包括系统管理员、运维管理员、口令管理员和审计员四种管理员角色，可灵活定制管理员角色，进一步细化管理员权限，从技术上保证系统管理安全。

系统集认证、授权、管理和审计有机地集成为一体，有效地实现了事前预防、事中控制和事后审

计。



高效的处理能力

系统具有业界最强的协议转发处理能力，摒弃业绩常用的协议转发“黑盒子”，能够对 Telnet、FTP、SSH、SFTP、RDP（Windows Terminal）、Xwindows、VNC、AS400、HTTP、HTTPS 协议进行完整的透明转发，特别是对图形化操作协议的转发性能远远优于其它同类型产品.

丰富的报表展现

系统提供多种报表展示的同时还能够提供客户自定义报表生成；

系统提供多种报表格式，包括 PDF、Word、Execl 等

系统提供列表、饼状图、柱状图、线性图等多种图表，动态展现运维趋势，便于分析与管理。

三 关键技术

- 精简的内核和优化的 TCP/IP 协议栈；
- 基于 HTTPS/SSL 的自身安全管理与审计；
- 严格的安全访问控制和管理员身份认证支持强认证；
- 审计信息加密存储；
- 口令信息加密存储；
- 完善的审计信息备份机制；
- 完整全面的自审计功能；

四 产品部署