NSFOCUS

冰之眼安全审计系统产品白皮书

NSFOCUS

© 2008 绿盟科技

■ 版权声明

本文中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容，除另有特别注明，版权均属绿盟科技所有，并受到有关产权及版权法保护。任何个人、机构未经绿盟科技的书面授权许可，不得以任何方式复制或引用本文的任何片断。

■ 商标信息

绿盟科技、**NSFOCUS**、冰之眼是绿盟科技的商标。

目录

一. 前言 1
二. 为什么需要安全审计系统 1
2.1 安全审计的必要性 2
2.2 安全审计系统特点 3
三. 如何评价安全审计系统 3
四. 绿盟科技安全审计系统 4
4.1 产品功能 4
4.2 体系架构 5
4.3 产品特点 7
4.3.1 网络事件“零遗漏”审计 7
4.3.2 高智能深度协议分析 7
4.3.3 全面精细的敏感信息审计 7
4.3.4 多维度网络行为审计 7
4.3.5 全程数据库操作审计 8
4.3.6 业界首创“网站内容安全”主动审计 9
4.3.7 基于协议的流量分析 9
4.3.8 基于对象的虚拟审计系统 10
4.3.9 强大丰富的管理能力 10
4.3.10 审计信息“零管理” 12
4.3.11 方便灵活的可扩展性 13
4.3.12 高可靠的自身安全性 13
4.4 解决方案 13
4.4.1 小型网络之精细审计方案 13
4.4.2 中型网络之集中审计方案 14
4.4.3 大型网络之分级审计方案 15
五. 结论 15

插图索引

图 2.1 信息安全体系结构模型.....2
图 4.1 冰之眼安全审计系统功能.....4
图 4.2 冰之眼SAS典型部署.....5
图 4.3 冰之眼安全审计体系结构.....6
图 4.4 冰之眼SAS数据库审计.....8
图 4.5 主动审计功能图.....9
图 4.6 虚拟审计系统.....10
图 4.7 单级管理.....11
图 4.8 主辅管理.....11
图 4.9 多级管理.....12
图 4.10 小型网络之精细审计方案.....14
图 4.11 中型网络之集中审计方案.....14
图 4.12 大型网络之分级审计方案.....15

一. 前言

随着信息技术的日新月异和网络信息系统应用的发展，网络技术的应用层次正在从传统的、小型业务系统逐渐向大型、关键业务系统扩展，政府、企业用户的网络应用也逐渐增多。

信息安全是一个动态的过程，在为自身业务提供高效的网络运营平台同时，日趋复杂的ＩＴ业务系统与不同背景业务用户的行为也给网络带来潜在的威胁，如内部业务数据、重要敏感文件通过电子邮件、数据库访问、远程终端访问(TELNET、FTP等)、网络文件共享（NETBIOS）等方式被篡改、泄露和窃取；访问非法网站、发布非法言论等违规上网行为泛滥；严重破坏政府、企业的信息系统安全。

如何对业务系统访问和网络行为进行有效的监控，已经成为政府、企业重点关注的问题。

二. 为什么需要安全审计系统

随着业务系统访问、网络应用行为日益频繁，我们可能经常遇到如下情况：

- 内部系统维护人员对业务应用系统的越权访问、违规操作，损害业务系统的运行安全；
- 企业重要业务数据库，被员工或系统维护人员篡改牟利、外泄，给企业造成巨大的经济损失；
- 员工随意通过网络共享文件夹、文件上传下载、EMAIL 等方式，发送重要敏感信息、业务数据，导致信息外泄事件发生；
- 员工在论坛发表敏感信息、传播非法言论，造成恶劣社会影响；
- 等级保护要求。公安部国家电子政务等级保护、国家保密局 BMB17-2006 号文件中要求政府、涉密单位必须对与涉密敏感信息、业务系统相关的网络行为进行安全审计；
- 萨班斯(SOX)法案。在美国上市公司必须遵循的“萨班斯(SOX)法案” 中要求对企业内部网络信息系统进行评估，其中涉及对业务系统操作、数据库访问等业务行为的审计。

根据调查数据显示，大多数企业虽然已经采用一定的网络安全手段（如防火墙、入侵检测、漏洞扫描等）和管理措施，但是上述安全事件发生后，却仍然无法进行及时告警响应、准确定位事件源头，给企业带来极大的困扰和严重的信息安全隐患。

如何有效监控业务系统访问行为和敏感信息传播，准确掌握网络系统的安全状态，及时发现违反安全策略的事件并实时告警、记录，同时进行安全事件定位分析，事后追查取证，满足合规性审计要求，是企业迫切需要解决的问题。

2.1 安全审计的必要性

随着日益增长的互联网安全风险，安全问题的复杂性日益加大，综合 FBI 和 CSI 对 484 家企业的调查及中国国家计算机网络应急协调中心 CNCERT/CC 的调查结果显示大约 76%的网络安全威胁来自于内部，其危害程度更是远远超过黑客攻击及病毒造成的损失，而这些威胁绝大部分与内部各种网络访问行为有关。

防火墙、入侵检测等传统网络安全手段，可实现对网络异常行为的管理和监测，如网络连接和访问的合法性进行控制、监测网络攻击事件等，但是不能监控网络内容和已经授权的正常内部网络访问行为，因此对正常网络访问行为导致的信息泄密事件、网络资源滥用行为（即时通讯、 论坛、在线视频、P2P 下载、网络游戏等）也无能为力，也难以实现针对内容、行为的监控管理及安全事件的追查取证。

因此，迫切需要一种安全手段对上述问题进行有效监控和管理。安全审计正是在这样的背景下产生。对于任何一个安全体系来说，审计追查手段都是必不可少。计算机信息安全可通过如下图 2.1 所示的信息安全体系结构模型来反映计算机信息系统安全需求和体系结构的共性，其构成要素是安全手段、系统单元及国际标准化组织（ISO）制定的开放系统互连参考模型（OSI）。在图 2.1 的安全手段中，审计是整个安全体系中不可缺少的重要组成部分。

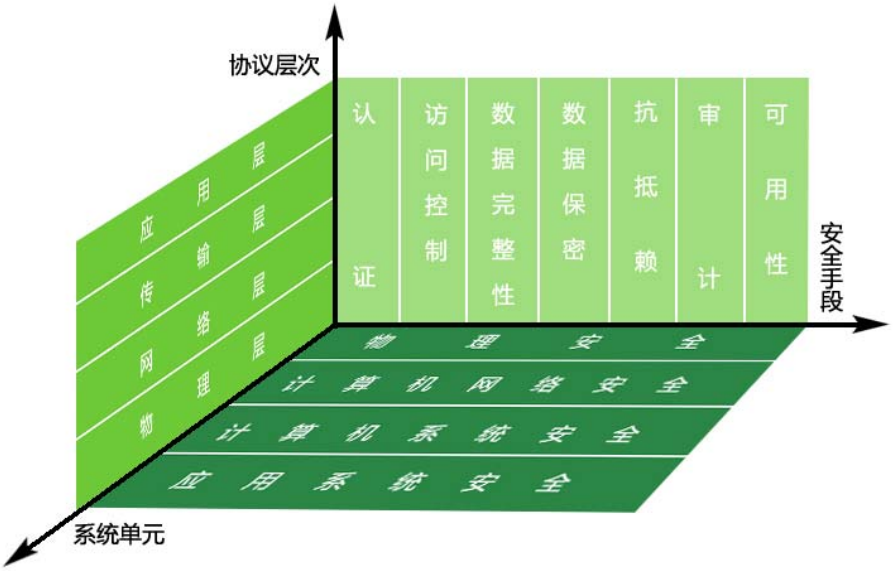

图 2.1 信息安全体系结构模型

同时，在 TCSEC 和 CC 等安全认证体系中，安全审计是评判一个系统是否真正安全的重要标准。根据代表性的安全模型 P2DR 理论，网络信息系统在综合运用防护工具（如防火墙、操作系统身份认证、加密等手段）、检测工具（如漏洞评估、入侵检测等系统）的同时，必

须通过安全审计收集、分析、评估安全信息、掌握安全状态，制定安全策略，确保整个安全体系的完备性、合理性和适用性，才能将系统调整到“最安全”和“最低风险”的状态。

2.2 安全审计系统特点

安全审计系统（Security Audit System）是在一个特定的企事业单位的网络环境下，为了保障业务系统和网络信息数据不受来自用户的破坏、泄密、窃取，而运用各种技术手段实时监控网络环境中的网络行为、通信内容，以便集中收集、分析、报警、处理的一种技术手段。

安全审计系统的主要特点如下：

◆ 细粒度的网络内容审计

安全审计系统可对可对网站访问、邮件收发、远程终端访问、数据库访问、论坛发帖等进行关键信息监测、还原；

◆ 全面的网络行为审计

安全审计系统可对网络行为，如网站访问、邮件收发、数据库访问、远程终端访问、即时通讯、论坛、在线视频、P2P 下载、网络游戏等，提供全面的行为监控，方便事后追查取证；

◆ 综合流量分析

安全审计系统可对网络流量进行综合分析，为网络带宽资源的管理提供可靠策略支持；

因此，通过传统安全手段与安全审计技术相结合，在功能上互相协调、补充，构建一个立体的安全保障管理体系。

三. 如何评价安全审计系统

安全审计系统具有对网络通信内容、网络行为的实时监测、报警、记录等功能。是否能够很好地帮助网络管理员完成对网络状态的把握和安全的评价是安全审计系统的基本标准。

一个完善的安全审计系统（SAS）应该从四个方面评价：

◆ 细粒度的操作内容审计与精准的网络行为实时监控；

◆ 全面详细的审计信息，丰富可定制的报表系统；

◆ 支持分级部署、集中管理，满足不同规模网络的使用和管理需求；

◆ 自身的安全性高，不易遭受攻击；

四. 绿盟科技安全审计系统

针对网络中内部人员的敏感信息泄露、违规网络行为等层出不穷的安全事件，绿盟科技提供了完善的安全审计方案。

冰之眼安全审计系统（ICEYE SAS）是绿盟科技自主知识产权的安全产品，通过网络数据的采集、分析、识别，实时动态监测通信内容、网络行为和网络流量，发现和捕获各种敏感信息、违规行为，实时报警响应，全面记录网络系统中的各种会话和事件，实现对网络信息的智能关联分析、评估及安全事件的准确全程跟踪定位，为整体网络安全策略的制定提供权威可靠的支持。

4.1 产品功能

冰之眼安全审计系统具有三大功能，如图 4.1 所示：

图 4.1 冰之眼安全审计系统功能

◆ 内容审计

冰之眼 SAS 系统提供深入的内容审计功能，可对网页页面内容、邮件、数据库操作、论坛、即时通讯等提供完整的内容检测、信息还原功能；并可自定义关键字库，进行细粒度的审计追踪。

◆ 行为审计

冰之眼 SAS 系统提供全面的网络行为审计功能，根据设定行为审计策略，对网站访问、邮件收发、数据库访问、远程终端访问、文件上传下载、即时通讯、论坛、在线视频、P2P 下载、网络游戏等网络应用行为进行监测，对符合行为策略的事件实时告警并记录。

◆ 流量审计

冰之眼 SAS 系统提供基于协议识别的流量分析功能，实时统计出当前网络中的各种报文流量，进行综合流量分析，为流量管理策略的制定提供可靠支持。

冰之眼SAS支持旁路(Sniffer Mode)部署模式，并支持多个硬件监听口，提供对多网段的同时监听能力，典型部署如下图 4.2 所示：

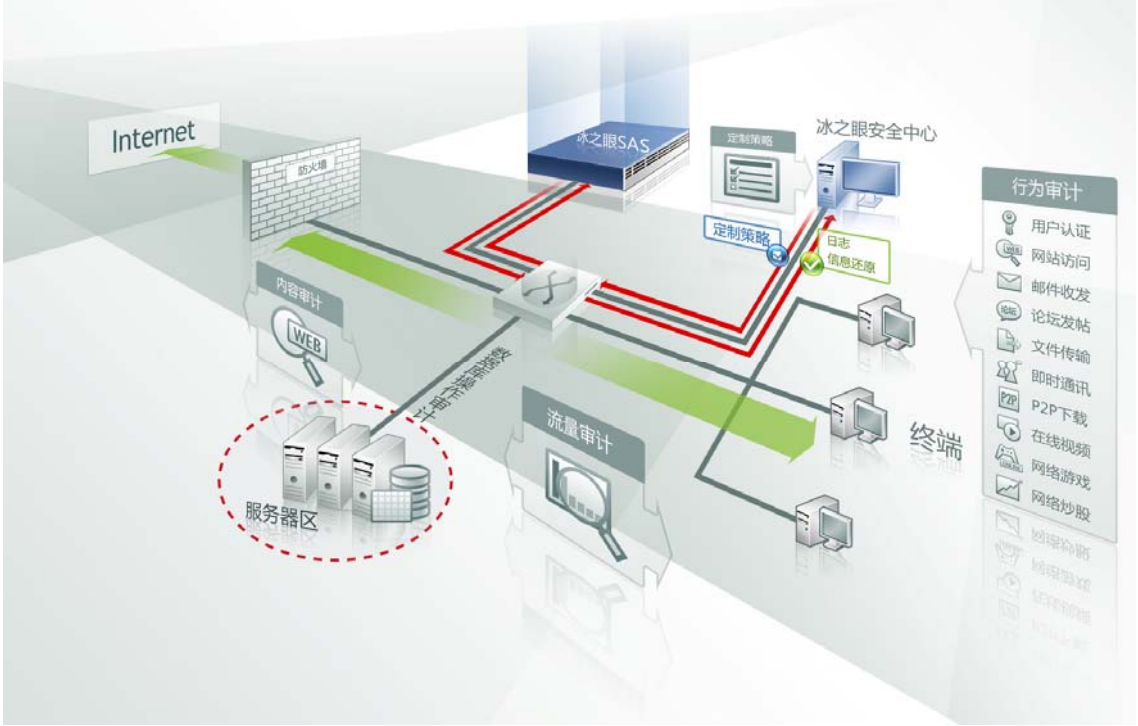

图 4.2　冰之眼 SAS 典型部署

4.2 体系架构

冰之眼安全审计系统的体系架构主要由安全中心/WEB控制台、网络引擎及升级站点三个部分组成，方便各种网络环境的灵活部署和管理。如下图 4.2 所示：

图 4.3 冰之眼安全审计体系结构

- 冰之眼安全中心具有系统监控和日志管理功能，可以集中管理多台网络引擎；并可以实现安全中心的主辅管理；支持任意层次的级联部署，实现多级管理，满足不同管理模式的需要；同时可以统一管理冰之眼安全审计系统、内容安全管理系统、入侵检测系统、入侵保护系统，提供针对网络正常行为和异常行为的全面行为检测手段，实现安全数据的整体挖掘、关联分析管理；
- 冰之眼 WEB 控制台具有系统配置管理、系统监控和日志管理功能，适合在任何 IP 可达地点远程管理。
- 网络引擎采用协议识别、特征检测和智能关联分析技术，全面监测网络数据包，及时发现违反安全策略的事件并实时告警记录；
- 升级站点提供产品补丁、URL 数据库、网络应用协议数据库等及时升级更新支持。

4.3 产品特点

4.3.1 网络事件“零遗漏”审计

冰之眼 SAS 采用先进的数据处理架构，对 64bytes 数据包的处理能力达到千兆线速的处理能力；同时采用先进的 IP 碎片重组与智能 TCP 流汇聚技术，达到接近 100%的检测准确率和几乎为零的漏报率，实现网络事件的“零遗漏”审计。

4.3.2 高智能深度协议分析

冰之眼 SAS 采用业界领先的协议识别和智能关联技术，提供全面深入的协议分析、解码回放，能够分析近 100 种应用层协议，包括 HTTP、TELNET、FTP、SMTP、WEBMAIL、NETBIOS、P2P、IM 等，极大地提高内容分析的准确性，帮助管理员全面掌握网络安全状态。

4.3.3 全面精细的敏感信息审计

冰之眼 SAS 提供全面细粒度的敏感信息审计解决方案。系统支持基于时间、用户、协议、内容等多种条件组合的信息审计策略，对邮件收发（WEBMAIL、SMTP、POP3）、文件上传下载（HTTP、FTP）、论坛、即时通讯等进行全面信息审计，提供实时告警、信息还原功能，同时支持自定义内容关键字库，实现敏感信息的深度检测识别还原，对机密信息外泄、非法言论传播等行为的及时响应处理、事后追查取证提供有力支持。

4.3.4 多维度网络行为审计

冰之眼 SAS 提供全面的网络行为审计解决方案，系统支持用户认证，并通过基于业务运维行为、上网行为和网络应用行为的审计，实现基于用户网络行为的全面多维度审计。

◆ 用户认证

系统支持 WEB 登录认证功能，提供本地用户数据库，并支持本地用户数据库与 LADP、RADIUS 用户数据库集成功能，实现基于用户的上网行为审计；

◆ 业务运维行为审计

冰之眼 SAS 支持对业务运维操作（如 TELNET、FTP、数据库访问等）的命令级审计和全过程记录；对违反审计策略的操作行为实时报警、记录；

◆ 上网行为审计

冰之眼 SAS 具有超过 1000 万条的庞大中英文 URL 数据库，多种精细分类，如不良言论、色情暴力等；并支持针对 URL、网页页面内容、搜索引擎的关键字过滤、审计功能，可告警、过滤非法不良网站；同时全面审计网站访问行为，实时告警、记录和网页还原，实现全面、准确、高效的网站访问监测；

◆ 网络应用行为审计

冰之眼 SAS 具有全程网络应用行为审计功能，支持对即时通讯、在线视频、P2P 下载、网络游戏、炒股等互联网应用行为进行全过程监控。

4.3.5 全程数据库操作审计

冰之眼 SAS 提供全面完整的数据库审计解决方案，系统可实时监控数据库各种帐户（如超级管理员、临时帐户等）的数据库操作行为，准确发现各种非法、违规操作，并及时告警响应处理，降低数据库安全风险，保护企业数据库资产安全。

◆ **全面丰富的审计类型**

系统支持 ORALCE、SQL SERVER、MY SQL、DB2、Sybase、Infomix、Postgresql 等主流数据库系统。

◆ **精细灵活的审计策略**

支持基于内容关键字、IP 地址、用户/用户组、时间、数据库类型、数据库操作类型、数据库表名、字段名等精细组合数据库审计策略，从而全面监测各种非法违规操作。

◆ **完整还原数据库操作**

实时审计用户对数据库系统所有操作（如：插入、删除、更新、用户自定义操作等），精细还原 SQL 操作命令包括源 IP 地址、目的 IP 地址、访问时间、用户名、数据库操作类型、数据库表名、字段名等，实现数据库安全事件准确全程跟踪定位。

数据库审计典型部署如下图 4.4 所示：

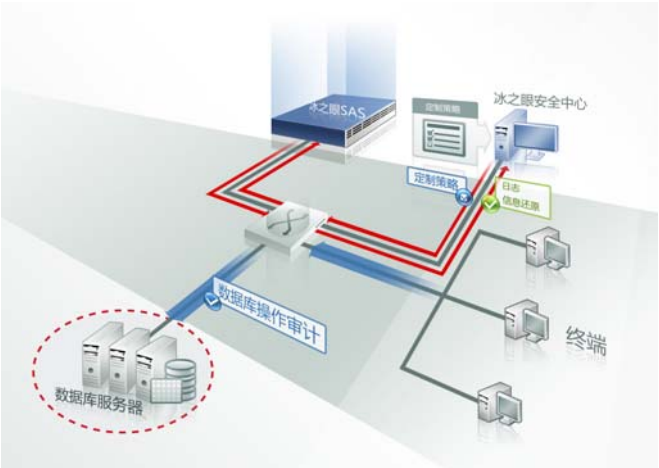

图 4.4 冰之眼 SAS 数据库审计

4.3.6 业界首创“网站内容安全”主动审计

冰之眼 SAS 系统“主动审计”能够帮助用户及时准确发现网站、论坛、博客中的非法敏感信息和网页挂马隐患；系统部署简单方便，接入网络就可以扫描检测。主动审计功能包括：

◆ 不良敏感信息扫描

冰之眼 SAS 系统具有高效智能的内容识别引擎--NCRE（NCRE,Nsfocus Content Recognition Engine），通过基于域名、关键字正则表达式等多种组合主动内容审计策略扫描指定网站，对被检测站点网页页面进行深度内容扫描检测，快速、准确的分析判断网页页面是否含有非法敏感信息，实时告警响应，并支持人工辅助校正扫描结果，从而有效防止不良信息扩散，为追查取证提供有力支持。

◆ 网站挂马扫描

冰之眼 SAS 系通过扫描指定网站，分析检测网页是否被挂马，并实时告警响应，为网站安全提供及时有效支持。

如下图 4.5 所示：

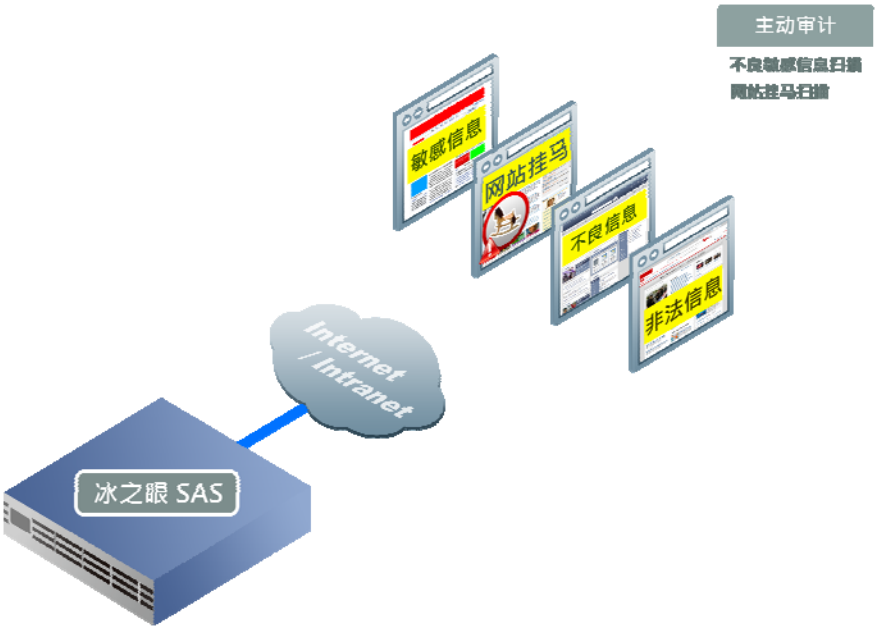

图 4.5 主动审计功能图

4.3.7 基于协议的流量分析

冰之眼 SAS 具有基于协议识别的流量分析功能，如：可识别使用 80 端口的 P2P 协议，避免基于 80 端口的 HTTP 协议流量统计错误，更精确可靠；并支持对即时通讯、P2P、在线

视频等动态协议的流量分析；提供详细的流量报表；可以通过编辑自定义统计指定协议流量的 IP TOPN。

4.3.8 基于对象的虚拟审计系统

冰之眼SAS提供业界领先的基于对象的策略管理系统，完全统一的规则配置方式强大而灵活，实现基于对象的虚拟审计系统（VAS）。冰之眼SAS针对企业不同的网络环境和安全需求，基于安全区、IP地址（组、段）、规则（组）、时间、动作等对象，制定不同的规则和响应方式，就像一台设备上虚拟出很多虚拟审计系统，每个虚拟审计系统分别执行不同的规则集，实现面向不同业务应用、不同部门职能、不同策略的智能化安全审计。如下图 4.3 所示：

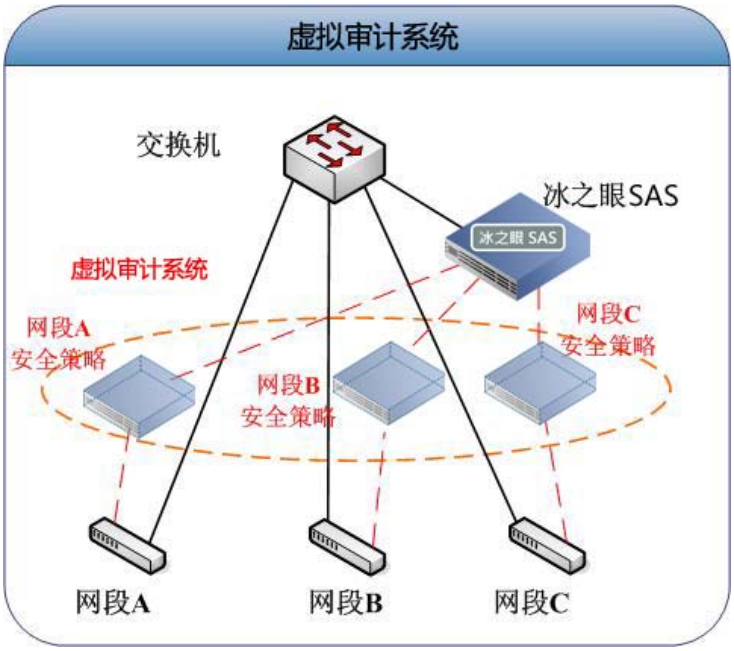

图 4.6 虚拟审计系统

4.3.9 强大丰富的管理能力

- 冰之眼 SAS 同时支持 B/S 和 C/S 两种管理方式，Web 管理灵活方便，适合在任何 IP 可达地点远程管理。Web 界面支持 MS IE、Netscape、Firefox、Opera 等浏览器，真正意义上实现了跨平台；
- 冰之眼 SAS 支持三种管理模式：单级管理、多级管理、主辅管理，能够快速部署在几乎所有的网络环境中，实现从企业网络核心至边缘及分支机构的全面检测，满足不同企业不同管理模式需要。

单级管理模式：安全中心直接管理网络引擎，一个安全中心可以管理多台网络引擎。如下图 4.4 所示：

图 4.7 单级管理

主辅管理模式：网络引擎同时接受一个主安全中心和多个辅安全中心的管理。主安全中心可以完全控制网络引擎；辅安全中心只能接受网络引擎发送的日志信息，不能操作网络引擎。如下图 4.5 所示：

图 4.8 主辅管理

多级管理模式：安全中心支持任意层次的级联部署，实现多级管理。上级安全中心可以将最新的升级补丁、规则模板文件等统一发送到下级安全中心，保持整个系统的完整统一性；下级安全中心可以向上级安全中心传送日志信息。如下图 4.6 所示：

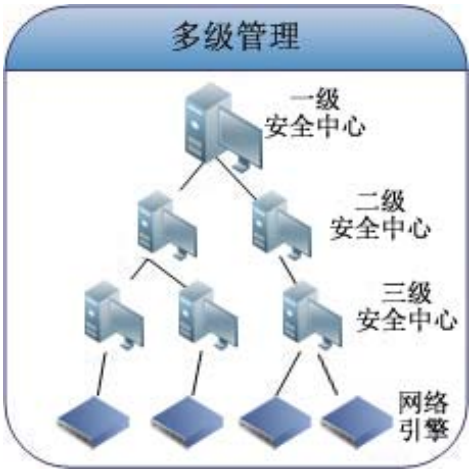

图 4.9 多级管理

- 冰之眼 SAS 安全中心与网络引擎内置了时钟同步机制，所有连接同一安全中心的引擎均保持毫秒一级的精确度；
- 冰之眼 SAS 提供带外管理（OOB）功能，解决远程应急管理的需求，减少用户运营成本、提高运营效率、减少宕机时间、提高服务质量；
- 冰之眼 SAS 支持实时在线升级、自动在线升级、离线升级，使 SAS 提供最前沿的安全保障；

4.3.10 审计信息“零管理”

冰之眼 SAS 完全支持“零管理”技术从实时升级系统到报表系统，从审计告警到日志备份，所有管理员需要日常进行的操作均可由系统定时自动后台运行。系统提供全面的事件日志信息的备份、恢复、清除、归并等功能；日志信息保存到 SQL Server，Oracle 等大型数据库中，并提供基于时间、IP 地址、事件类别等条件的检索功能。

- 日志备份：支持基于日期、事件类型、数据格式等组合备份策略，并支持日志自动备份。
- 日志自动维护：根据日志自动维护计划的设置，系统会在指定时间，在后台自动进行相应的数据备份、清除等操作。
- 日志缓存：网络引擎即使无法进行网络通信也能将检测到的事件保存在本地，等网络恢复正常后再自动同步到控制台或日志数据库中，不会因网络断开而丢失日志信息。
- 审计报表：系统提供了详细的综合分析报表、自定义三种类型 10 多个类别的报表模板，支持生成：日、周、月、季度、年度综合报表。报表支持 MS Word、Html、JPG 等格式导出，并支持定时通过电子邮件自动发送报表至系统管理员；同时冰之眼 SAS 支持对网络引擎的不同网口或不同网络引擎，分别生成对应报表；极大地降低了维护费用与管理员的工作强度。

4.3.11 方便灵活的可扩展性

- 冰之眼 SAS 支持多个硬件监听口，监听口即插即用，提供对多网段的同时监听能力；
- 冰之眼 SAS 支持通过发送邮件、安全中心显示、日志数据库记录、打印机输出、运行用户自定义命令、TCPKiller 等响应方式及时报警。

4.3.12 高可靠的自身安全性

- 冰之眼 SAS 专门设计了安全、可靠、高效的硬件运行平台。硬件平台采用严格的设计和工艺标准，保证了高可靠性；独特的硬件体系结构大大提升了处理能力；操作系统经过优化和安全性处理，保证系统的安全性和抗毁性；
- 冰之眼 SAS 具有更强的高可用性，设备支持热插拔的冗余双电源，避免电源硬件故障时设备宕机，提高设备可靠性；
- 冰之眼 SAS 采用特别定制的操作系统，与安全中心间的通信采用强加密的 SSL 加密传输告警日志与控制命令，完全避免了可能存在的嗅探行为，保证了数据传输的安全；
- 冰之眼 SAS 监听网口无需设置 IP 地址，避免了被扫描和攻击；
- 冰之眼网络引擎与安全中心在网络完全断开的情况下，仍然会将检测到的事件保存在网络引擎本地，等网络恢复正常自动地同步到冰之眼安全中心，提供日志缓存。

4.4 解决方案

绿盟科技提供一整套的安全审计解决方案，实现从网络核心至边缘及分支机构的全面审计。冰之眼安全审计系统的部署方式灵活多样，能够快速部署在几乎所有的网络环境中，满足政府、企业不同管理模式需要。

4.4.1 小型网络之精细审计方案

针对小型网络，绿盟科技安全审计解决方案提供虚拟审计系统精细管理方案，通过基于对象的策略管理，冰之眼SAS针对不同部门/网段，制定不同的规则和响应方式，每个虚拟审计系统分别执行不同的安全策略，实现面向不同对象、实现不同策略的智能化、精细化的安全审计。如下图 4.7 所示：

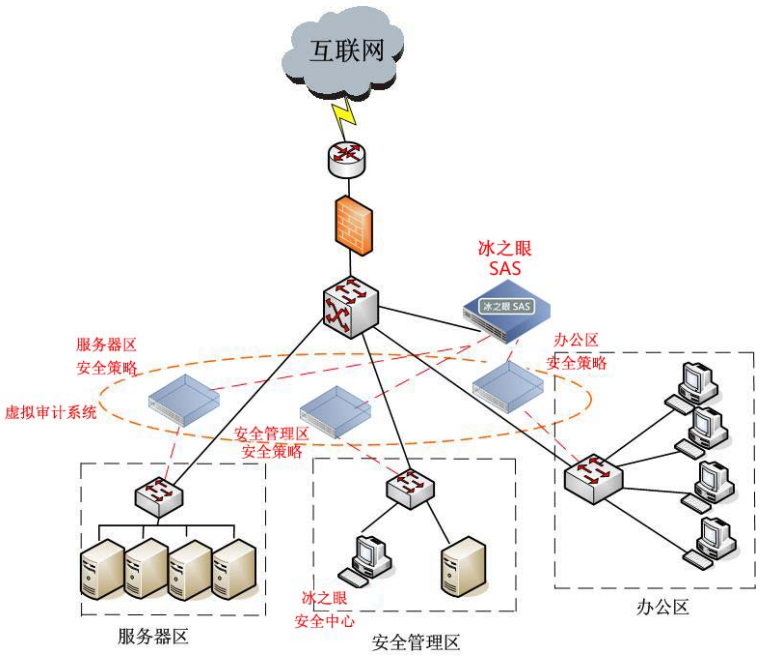

图 4.10　小型网络之精细审计方案

4.4.2 中型网络之集中审计方案

针对中型网络，绿盟科技安全审计解决方案提供集中管理方案，通过将冰之眼SAS部署在多个关键网段，如安全管理区、DMZ区、服务器区及办公区，实现对业务系统访问、互联网访问的全网安全状态监控。利用冰之眼安全中心集中管理多台网络引擎，便于安全信息的集中管理，以便实时掌握全网的安全状况。如下图 4.8 所示：

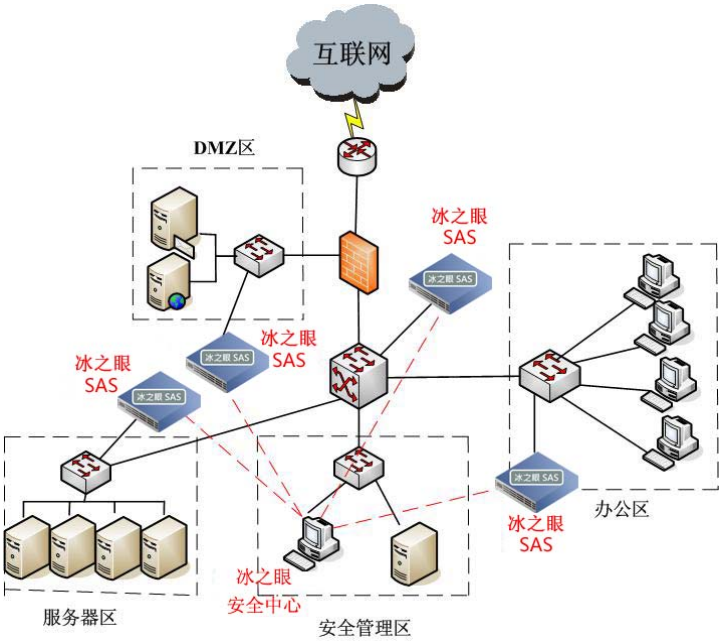

图 4.11　中型网络之集中审计方案

4.4.3 大型网络之分级审计方案

对于跨广域网的大型企业用户，其网络机构相对复杂，不仅有总部，全国各地还有分支机构，总部及下属各分支机构都建有自己的局域网络。用户租用 ISP 的专线建立自己覆盖全国的企业专网，各分支机构通过企业专网与总部建立业务信息交换。因此其对整个网络的管理比较重视，需要保证总部和各分支机构的安全策略的统一性。

针对大型企业用户，绿盟科技安全审计解决方案提供分级审计方案，在各级网络上部署冰之眼SAS的分级安全中心，上级安全中心对下级安全中心进行统一管理，上级安全中心可以将最新的最新升级补丁、审计规则、引擎配置文件等统一发送到下级安全中心，保持整个系统的安全策略的完整统一性。如下图 4.9 所示：

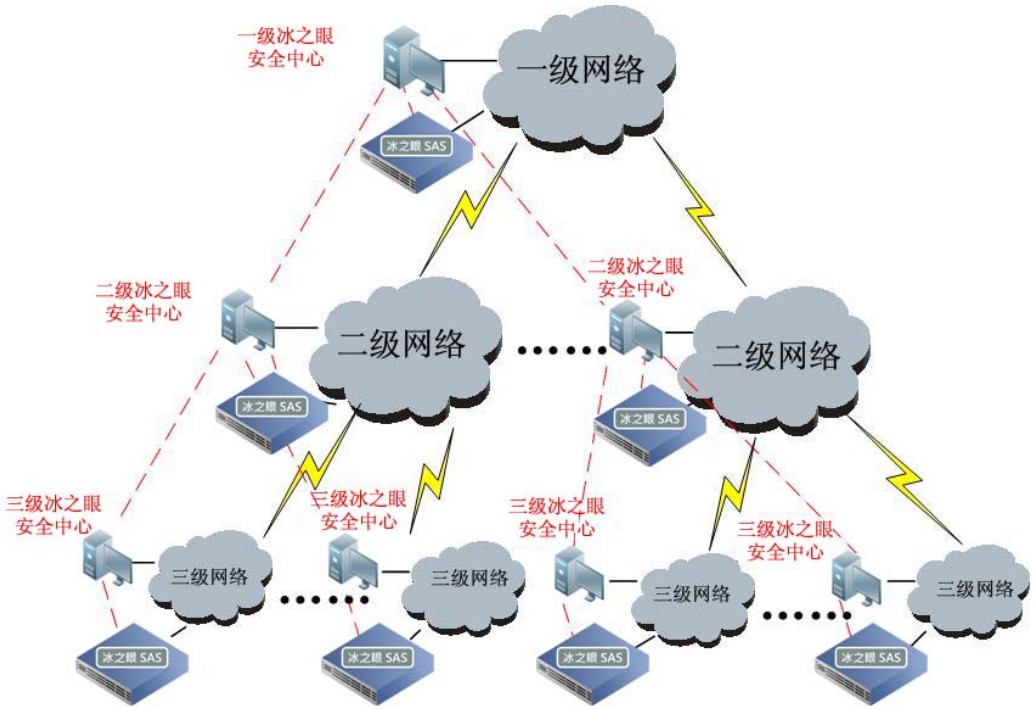

图 4.12 大型网络之分级审计方案

五. 结论

通过冰之眼 SAS 在网络信息系统的部署，可以有效掌握网络安全状态，预防敏感涉密信息外泄，实现对内部网络信息的整体智能关联分析、评估、调查及安全事件的准确跟踪定位，为整体安全策略的制定提供权威可靠的支持。