网神
SECWORLD

可控安全
Controllable
Security

技术白皮书

网神 SecFox 运维安全管理与审计系统

（运维审计）

网神信息技术（北京）股份有限公司
http://www.legendsec.com

版权声明

文档信息

文档名称	网神 SecFox 运维安全管理与审计系统产品白皮书		
扩散范围	销售/售前/客服/渠道商/用户	**文档版本号**	V5.0.330
作者	彭建超	**日期**	2016/6/2
初审人	杨黎鸿	**复审人**	

版本变更记录

时间	版本	说明	作者
2016/6/2	V5.0		

目录

1 背景

1.1 运维审计能做什么

随着企业信息系统规模的不断扩大，业务范围的快速扩张，运维工作量也随之增多。在运维过程中存在事前身份不确定、授权不清晰，事中操作不透明、过程不可控，事后结果无法审计、责任不明确导致客户业务及运维服务面临安全风险。

运维审计系统可对服务器、网络设备、安全设备的操作进行监控审计，实现账号集中管理、高强度认证加固、细粒度访问授权控制、加密和图形操作协议的审计等功能，让内部人员、第三方人员的操作处于可管、可控、可见、可审的状态下，规范运维的操作步骤，避免了误操作和非授权操作带来的隐患。

运维审计能够极大的保护单位内部网络设备及服务器资源的安全性，使得单位内部网络管理合理化和专业化。

1.2 用户需求背景

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、商务平台的不断推出和投入运行，信息系统在单位的运营中全面渗透。电信行业、财政、税务、公安、金融、电力、石油、大中企业和门户网站，更是使用数量巨大的服务器主机来运行关键业务，提供电子商务、数据库应用、运维管理、ERP 和协同工作群件等服务。由于服务器众多，系统管理员压力太大等因素，人为误操作的可能性时有发生，这会对部门或者单位声誉造成重大影响，并严重影响其经济运行效能。黑客/恶意访问也有可能获取系统权限，闯入部门或单位内部网络，造成不可估量的损失。如何提高系统运维管理水平，满足相关标准要求，防止黑客的入侵和恶意访问，跟踪服务器上用户行为，降低运维成本，提供控制和审计依据，越来越成为各单位关心的问题。

英国政府发布的《BS7799》、美国政府 2002 年颁布的《萨班斯法案(Sarbanes-Oxley Act)》、国际标准化组织发布的信息安全标准《ISO27001》、中国政府发布的《企业内部控制规范》、

《国家信息安全等级保护管理规定》等，均要求所涉及到的企事业单位的经营活动，内部管理、项目和投资等，都要有控制和审计手段。因此，管理人员需要有效的技术手段和专业的技术工具和安全产品按照行业的标准来做的细粒度的管理，真正做到对于内部网络严格控制。可以控制、限制和追踪用户的行为，判定用户的行为是否对单位内部网络的安全运行带来威胁。尤其在目前来自互联网的外部威胁越来越不可控的情况下，企业单位的内网安全形势更是愈加严峻。

网神 SecFOX 运维审计应用了目前先进的技术作为支持，针对单位内部网络设备和服务器进行账号和认证的统一管理，对此类资产的常用访问方式进行监控和审计。例如对字符终端、图形终端等访问方式进行监控和审计，实现对用户行为进行控制、追踪、判定，满足单位内部网络对安全性的要求。

总之，单位内部网络设备和服务器需要更安全的环境，以保障单位的正常运作，网神 SecFOX 运维审计能够为单位内部网络的安全运行保驾护航。

1.3 现存问题

目前，企业单位或机构的运维管理有以下几个特点：

- 存在大量的网络设备和 Windows 服务器，而一些重要的系统（如 ERP）等，则运行在 Unix/Linux 系统设备上；
- 设备管理分散，存在多对多的交叉异构管理的情况；
- 运维人员依赖于 Telnet/SSH/RDP/FTP 等协议对设备进行远程维护，使用 KVM 方式进行本地维护；
- 部分厂商采用 VPN 远程接入进行维护；
- 自身运维人员比较少，大部分运维工作外包给了第三方代维公司或者原厂商；

基于这些现状，在运维管理中必然存在以下突出问题：

1.3.1 运维风险不透明、不可控

目前的运维操作类似一个“黑盒“，我们并不知道：

- 当前管理员/代维工程师正在进行哪些运维操作？
- 是在哪一台设备上发生的操作？
- 操作是谁来执行的？

- 执行的操作是否正确？

由此，日常的技术运维操作主要存在以下操作风险：

- 误操作导致关键应用服务异常甚至宕机；
- 违规操作导致敏感信息泄露；
- 恶意操作导致系统上的敏感数据信息被篡改和破坏。
- 无法有效监控原厂商和代维厂商的维护操作；
- 无法有效取证和举证维护过程中出现的问题和责任

1.3.2 使用共享账号的安全隐患

单位的支撑系统中有大量的网络设备、主机系统和应用系统，分别属于不同的部门和不同的业务系统。各应用系统都有一套独立的账号体系，用户为了方便登陆，经常出现多人共用账号的情况。

多人同时使用一个系统账号在带来管理方便性的同时，导致用户身份唯一性无法确定。如果其中任何一个人离职或者将账号告诉其他无关人员，会使这个账号的安全无法保证。

由于共享账号是多人共同使用，发生问题后，无法准确定位恶意操作或误操作的具体责任人。更改密码需要通知到每一个需要使用此账号的人员，带来了密码管理的复杂化。

1.3.3 密码策略无法有效执行

为了保证密码的安全性，安全管理员制定了严格的密码策略，比如密码要定期修改，密码要保证足够的长度和复杂度等，但是由于管理的机器数量和账号数量太多，往往导致密码策略的实施流于形式。

- 设备多，帐号多，每一个密码都要足够复杂，依靠人工记忆很难
- 对用户来说，安全得保存多个密码的也是一个难题
- 定期修改密码费时，费力

1.3.4 授权不清晰

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。

1.3.5 访问控制策略不严格

目前的管理中，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，在设备自身上做访问控制策略，配置复杂，工作量大；同时缺少有效的技术手段来保证访问控制策略被有效执行。

1.3.6 无法有效审计运维操作

各系统独立运行、维护和管理，所以各系统的审计也是相互独立的。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。

另外各系统的日志记录能力各不相同，例如对于 Unix 系统来说，日志记录就存在以下问题：

Unix 系统中，用户在服务器上的操作有一个历史命令记录的文件，但是用户可以随意更改和删除自己的记录；

root 用户不仅仅可以修改自己的历史记录，还可以修改他人的历史记录，系统本身的的历史命令文件已经变的不可信；

记录的命令数量有限制；

无法记录操作人员、操作时间、操作结果等。

以上问题的存在，迫使我们必须找出新的思路和利用新的技术装备来解决问题，这正是运维审计的擅长之处。

2 产品概述

网神 SecFox 运维安全管理与审计系统（简称：网神运维审计系统）是一种被加固的可以防御进攻的计算机，具备坚强的安全防护能力。网神运维审计系统扮演着看门者的职责，所有对网络设备和服务器的请求都要从这扇大门经过。网神运维审计系统能够拦截非法访问和恶意攻击，对不合法命令进行阻断、过滤掉所有对目标设备的非法访问行为。

网神运维审计系统具备强大的输入输出审计功能，不仅能够详细记录用户操作的每一条指令，而且能够将所有的输出信息全部记录下来；具备审计回放功能，能够模拟用户的在线操作过程，完善了网络的内控审计功能。网神运维审计系统能够在自身记录审计信息的同时在外部某台计算机上做存储备份，可以极大增强审计信息的安全性，保证审计人员有据可查。

网神运维审计系统还具备图形终端操作的审计功能，能够对多平台的多种图形终端操作做审计，例如 Windows 平台的 RDP 方式图形终端操作，Linux/Unix

平台的 X11 方式图形终端操作。

为了给系统管理员查看审计信息提供方便性，网神运维审计系统提供了审计查看检索功能。系统管理员可以通过多种查询条件查看审计信息。

经过多年项目实践和市场考验，满足在政府、金融、能源、教育、医疗、军工、广电等多个行业领域的运维工作和安全管理需求。满足等级保护、各行业风险指引和内控要求中的相关规定。

3 产品功能说明

3.1 系统架构

3.2产品组成

网神运维审计系统产品包括运维审计系统及应用发布服务器。

- 运维审计系统

网神运维审计系统主机，是运维审计系统的核心部件，实现统一用户、统一授权、集中审计、统一 SSO 单点登录，对标准协议的全面单点登录操作审计。（标准协议如：SSH、Telnet、RDP、VNC、SFTP、FTP 等）

- 应用发布服务器

发布服务器可称之为前置机，主要工作为对非标准协议（非标准协议：数据库客户端、IE 访问、其他 C/S 架构软件）的单点登录操作，该组成部分可由用户进行选择内置发布服务器或外置发布服务器。内置发布服务器只在高端型号中提供，外置发布服务器为用户方提供。（操作系统必须为：windows server 2008 R2 或 windows server 2003 R2）

3.3引入 4A 管理理念

网神运维审计系统采用 4A 的管理理念，圆满地解决用户现在面临的种种运维问题。

如图，IT 运维管理由账号管理、认证管理、授权管理、操作管理组成：

帐号管理，需要在各系统上为新用户建立帐号、为已有用户修改帐号、为离职用户删除帐号。

认证管理，要保证各系统不被越权访问，那么就必须做好认证管理，为系统帐号定义密码、定期要求帐号密码修改、控制密码强度等等。

授权管理，授权过程其实就是把各系统上建立的帐号分配给操作人员的过程，管理员要定义帐号的权限，然后做帐号分配，根据用户置位调整做相应的帐号权限修改。

操作审计，管理员要定期做服务器的巡检，分析各系统上的日志，查看是否有越权访问，查看是否有误操作，如果有事故还需要根据日志进行故障排查和事故追踪。

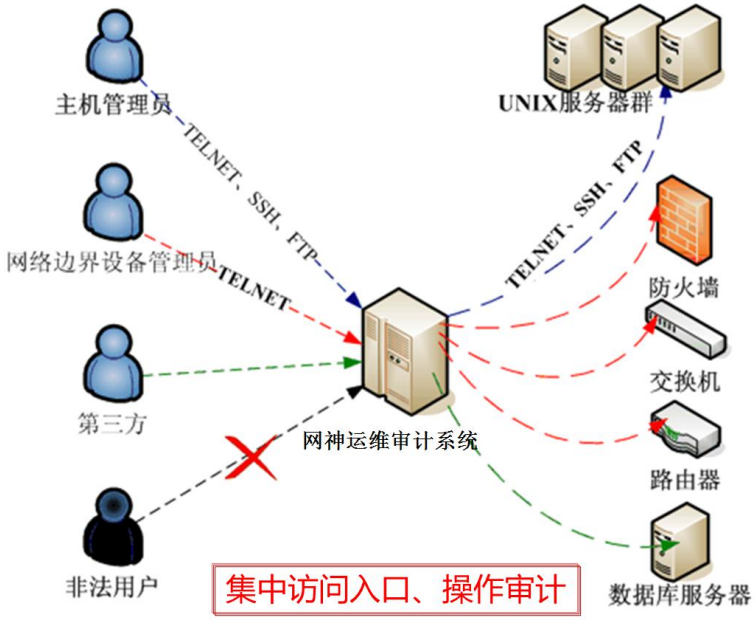
以上也就是 4A 管理，网神运维审计系统融合统一用户账号管理、统一认证管理、统一授权管理和统一安全审计四要素，并且涵盖单点登录（SSO）等安全功能，既能够为客户提供功能完善的、高安全级别的 4A 管理，也能够为

用户提供符合萨班斯法案（SOX）要求的内控报表。

3.4SSO 单点登录

网神运维审计系统提供了基于 B/S 的单点登录系统，用户通过访问 WEB 页面一次登录系统后，就可以无需认证的访问被授权的多种基于 B/S 和 C/S 的应用系统。单点登录为具有多账号的用户提供了方便快捷的访问途经，使用户无需记忆多种登录用户 ID 和口令。它通过向用户和客户提供对其个性化资源的快捷访问提高工作效率。同时，由于系统自身是采用强认证的系统，从而提高了用户认证环节的安全性。

单点登录可以实现与用户授权管理的无缝链接，可以通过对用户、角色、行为和资源的授权，增加对资源的保护和对用户行为的监控及审计。

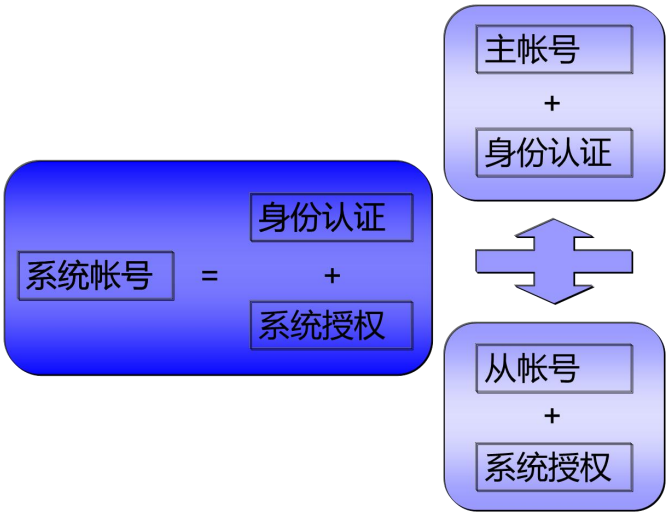


3.5集中账号管理

网神运维审计系统的集中账号管理包含对所有服务器、网络设备账号的集

中管理。账号和资源的集中管理是集中授权、认证和审计的基础。集中账号管理可以完成对账号整个生命周期的监控和管理，而且还降低了管理大量用户账号的难度和工作量。同时，通过统一的管理还能够发现账号中存在的安全隐患，并且制定统一的、标准的用户账号安全策略。

通过建立集中账号管理，单位可以实现将账号与具体的自然人相关联。通过这种关联，可以实现多级的用户管理和细粒度的用户授权。而且，还可以实现针对自然人的行为审计，以满足审计的需要。



3.6集中身份认证

网神运维审计系统为用户提供统一的认证接口。采用统一的认证接口不但便于对用户认证的管理，而且能够采用更加安全的认证模式，提高认证的安全性和可靠性。

集中身份认证支持电子证书、Windows AD 域、Windows Kerberos、双因素、动态口令和生物特征识别等多种认证方式，而且系统具有灵活的定制接口，可以方便的与第三方 LDAP 认证服务器对接。

3.7统一资源授权

网神运维审计系统提供统一的界面，对用户、角色及行为和资源进行授权，以达到对权限的细粒度控制，最大限度保护用户资源的安全。通过集中访问授权和访问控制可以对用户通过 B/S、C/S 对服务器主机、网络设备的访问进行审计和阻断。

在集中访问授权里强调的“集中”是逻辑上的集中，而不是物理上的集中。即在各网络设备、服务器主机系统中可能拥有各自的权限管理功能，运维人员也由各自的归口管理部门委派，这些运维人员可以通过网神运维审计系统对各自的管理对象进行授权，而不需要进入每一个被管理对象才能授权。授权的对象包括用户、用户角色、资源和用户行为。系统不但能够实现授权用户可以通过什么角色访问资源这样基于应用边界的粗粒度授权，对某些应用还可以实现限制用户的操作，以及在什么时间、什么地点进行操作等的细粒度授权。

3.8细粒度访问控制

网神运维审计系统能够提供细粒度的访问控制，最大限度保护用户资源的安全。细粒度的命令策略是命令的集合，可以是一组可执行命令，也可以是一组非可执行的命令，该命令集合用来分配给具体的用户，来限制其系统行为，管理员会根据其自身的角色为其指定相应的控制策略来限定用户。

访问控制策略是保护系统安全性的重要环节，制定良好的访问策略能够更好的提高系统的安全性。

基于细粒度的访问控制下，网神运维审计系统真正做到了：

- Who（谁）： 控制什么用户允许操作。

- Where（什么地点）：控制来源于什么地址的用户允许访问什么资源。
- When（什么时间）：控制在什么时间允许用户操作。
- What（做了什么）：控制用户执行的操作。

3.9运维操作审计

操作审计管理主要审计操作人员的账号使用（登录、资源访问）情况、资源使用情况等。在各服务器主机、网络设备的访问日志记录都采用统一的账号、资源进行标识后，操作审计能更好地对账号的完整使用过程进行追踪。

系统支持对如下协议进行审计：Telnet、FTP、SSH、RDP(Windows Terminal)、Xwindows、VNC 等。

网神运维审计系统通过系统自身的用户认证系统、用户授权系统，以及访问控制等详细记录整个会话过程中用户的全部行为日志。还可以将产生的日志传送给第三方。

对于生成的日志支持丰富的查询和操作。

- 支持按服务器方式进行查询。

通过对特定服务器地址进行查询，可以发现该服务器上发生的命令和行为。

- 支持按用户名方式进行查询。

通过对用户名进行查询，可以发现该用户的所有行为。

- 支持按登录地址方式进行查询。

通过对特定 IP 地址进行查询，可以发现该地址对应主机及其用户在服务器上进行的所有操作。

- 支持按照登录时间进行查询。

通过对登录时间进行查询，可以发现特定时间内登录服务器的用户及其进行过的所有操作。

- 支持对命令发生时间进行查询。

可以通过对命令发生的时间进行查询，可以查询到特定时间段服务器上发生过的所有行为。

- 支持对命令名称进行查询。

通过查询特定命令如 ls，可以查询到使用过该命令的所有用户及其使用的时间等。

- 支持上述六个查询条件的任意组合查询。

如，可以查询“谁（用户名）”“什么时间登录（登录时间）”服务器并在“什么时间（命令发生时间）”在“服务器（目标服务器）”上执行过“什么操作（命令）”。

- 支持对日志的备份操作处理。

支持对日志的删除处理。在各服务器主机、网络设备的访问日志记录都采用统一的账号、资源进行标识后，操作审计能更好地对账号的完整使用过程进行追踪。

系统支持对如下协议进行审计：Telnet、FTP、SSH、RDP(Windows Terminal)、Xwindows、VNC 等。

网神运维审计系统通过系统自身的用户认证系统、用户授权系统，以及访问控制等详细记录整个操作过程。

4 产品技术特色和优势

4.1独有功能

独有功能是目前我们新版本运维审计系统和其他厂家相比独一无二的功能点。

4.1.1智能运维脚本

IT 运维常用的指令的集合，可以编写成脚本的形式，由运维审计系统定时自动执行。

代维人员或者厂家人员，以前是需要授权他们操作设备，现在可以改为由他们提交操作脚本，由业主单位的管理人员审核后付诸实施。

对于基层操作人员和实习人员，也可以改为提交脚本，由领导审核后再提交运行。

4.1.2多种运维管理操作方式

网神运维审计系统在不改变用户使用习惯的前提下，可管理以下多种运维操作方式，支持菜单模式、直连模式的访问方式：

- 字符终端运维操作：
  - 终端命令行操作：Telnet、SSH。
  - 文本菜单终端 HP 的 SAM，IBM 的 SMIT，LINUX 的 SETUP 等。
- 图形终端操作：RDP、X11、VNC。
- 文件传输操作：FTP、SFTP、SCP、RDP 磁盘通道、剪贴板等文件传输。
- 应用终端操作：
  - 基于 WEB 操作：http、https。
  - 基于 C/S 应用终端操作：AS400。
- KVM Over IP 操作：Avocent、Raritan。
  - Avocent 管理终端 DSR、DSVIEW。
  - 力登管理终端：RARITAN、RARITAN_CC。
- 数据库运维操作：Oracle、DB2、Informix、Sybase、MS SQL 等。
- 具备高度扩展性，可支持各种已知和未知的 B/S、C/S 管理终端的操作。

4.1.3 真正意义的智能负载均衡

网神运维审计系统支持分布部署，支持在运维管理过程中，实现对运维管理的负载均衡。

负载均衡配置图

在运维管理大型网络时，当被管资源数量巨大，网络数据链路较为集中的情况下，为了使运维管理不影响正常业务的资源访问，网神运维审计系统提供了“分布部署，集中管理”的负载均衡模式，对当前的运维管理所需的网络资源占用进行智能化分配调度，支持主主模式的工作方式。

4.1.4 漏洞扫描

检测漏洞目标只针对操作系统进行扫描。贴合堡垒机的使用，可供使用人员更加直观明了的查看管理设备的安全情况。可对操作系统进行漏洞检测，可指出系统漏洞及相关薄弱环节，并给出相应的修补措施及安全建议。不影响堡垒机部署环境采用旁路方式部署，通过堡垒机内嵌扫描器进行集中管理的方式，实现对大规模网络的实时及定时漏洞扫描和风险评估，使安全隐患不在“透明”。

4.1.5 基线检测

堡垒机增加合规检测功能，通过建立信息安全基线合规指标库，将信息系统等级保护基本要求、信息安全风险评估准则细化，进一步分解根据具体设备特性形成设备级的基线指标，形成对应的检测项，实现技术体系和管理体系指标内容的落地。更加贴合等保、分保等客户需求。实际应用场景中，客户可对自己设备进行更加安全的检查，提高资产设备的安全性。

4.1.6 自动学习功能

通过 nmap 协议，自动学习资产，可以根据 ip 地址和 ip 网段进行资产离线和在线的扫描发现，可以进行选择或全选导入资源；自动学习到的结果信息包含： IP、mac 地址、操作系统、开放的端口及服务、软件版本等信息；该功能可以快速添加目标资源，减轻运维人员的工作量，保证资源添加的准确性；

4.2优势功能

和其它的类似产品相比，网神运维审计系统具有以下优势。

4.2.1高成熟性和安全性

网神运维审计系统脱胎于国内最早的 4A 项目：黑龙江移动运维支撑平台集中身份和认证管理系统。并在中国移动的全国范围做了多年的部署实施，对于运营商的实际需求满足充分。

严格按照中国移动通信企业标准 QB-W-002-2005《中国移动支撑系统集中账号管理、认证、授权与审计（4A）技术要求》的要求开发完成。

在运营商行业有长达 6 年的使用实践，最多管理省级运维网络高达 3000 多台设备，性能卓越。

系统的开发研制中，我们尽量采用成熟的先进技术，对系统的关键技术在前期的工作中进行了大量实验和攻关及原型建立，在已开发并经广泛测试的产品中，上述的关键技术问题已解决。而且，所选取的硬件平台和软件平台，是具有良好的技术支持和发展前途的成熟产品。

系统运用了先进的加密、过滤、备份、数字签名与身份认证、权限管理等安全手段，建立健全的系统安全机制，保证了用户的合法性和数据不被非法盗取，从而保证产品的安全性。

4.2.2 良好的扩展性

网神运维审计系统产品从 4A 解决方案中抽象出来，提供最便捷的 4A 项目集成方案。在程序结构上充分考虑到 4A 项目和非 4A 项目的使用场景，以先进的体系结构，清晰合理的模块划分实现多种用户场景的适用性。在 4A 项目中网神运维审计系统放弃账号、认证、授权的集中管理，只提供执行单元，完成访问控制和操作审计功能；在非 4A 项目中网神将 4A 的一些理念融合到网神运维审计系统产品中，除提供基础的访问控制和操作审计功能外，还提供精简的账号、认证、授权集中管理功能。

4.2.3 强大的审计功能

网神运维审计系统在审计方面能做到：

- 精确记录用户操作时间；

- 审计结果支持多种展现方式，让操作得以完整还原；
- 审计结果可以录像回放，支持调节播放速度，并且回放过程中支持前后拖拽，方便快速定位问题操作；
- 方便的审计查询功能，能够一次查询多条指令。

4.2.4使用简单，适应各种应用

不增加操作和维护的复杂度，不改变用户的使用习惯，不影响被管理设备的运行。

统一操作入口，统一登录界面，管理员和操作员都使用 WEB 方式操作，操作简单。可对所有 UNIX 类服务器、LINUX 类服务器、Windows 类服务器、网络/安全等重要设备的进行统一操作管理。

统一运维工具，不需要用户安装 SSHClient、Neteam、SecureCRT 等运维工具，即可采用 RDP、Telnet、FTP、SSH 等常用运维方式对被管资源进行操作。

4.2.5绿色部署、迅速上线

物理旁路部署，不需要在被管理设备上安装代理程序，不改变原有的网络拓扑结构，不更改用户网络设备上的配置，不影响任何业务数据流，几分钟就可以部署完毕。（相比传统集中管理而言）

4.2.6实现运维命令的实时审计和拦截控制

对于普通用户登录到目标设备上正在进行的操作，审计管理员可以通过网神运维审计系统的 WEB 界面做到实时监控，做到边操作边审计，真正实现操作透明。同时对于用户的违规操作，审计管理员还可以做到实时切断。（相比传

统的并行网络侦听审计而言）

4.2.7加密协议审计

网神运维审计系统支持对 SSH、SFTP 等加密类协议，以及 RDP、VNC、X11 等图形协议进行全面审计。可以记录操作命令、操作过程中的键盘事件，同时可以对操作过程进行实时监控、录像、回放。（相比并行审计）

4.2.8合规性检查

（针对目标服务基线检查、针对终端安全检查，针对文件进行病毒查杀）

网神运维审计系统针对各行业特点和安全基线规范基准，增加了基线检测功能，使检查过程达到自动化、标准化、持续化、可视化。它可以大大提高检查结果的准确性和合规性，用以在企业的上线安全检查、第三方入网安全检查、合规安全检查（上级检查）、日常安全检查和安全服务任务中，协助查找设备在安全配置中存在的差距，并与安全整改与安全建设相结合，提升各类业务系统的安全防护能力和达到整体合规要求.针对通过 ftp、sftp 上传服务器的文件，可以开启防病毒功能，保证上传文件的安全。

4.2.9漏洞扫描

网神运维审计系统增加漏洞扫描功能可以对不同操作系统下的计算机（在可扫描 IP 范围内）进行漏洞检测。主要用于分析和指出有关网络的安全漏洞及被测系统的薄弱环节，给出详细的检测报告，并针对检测到的网络安全隐患给出相应的修补措施和安全建议。网神运维审计系统最终目标是成为加强中国

网络信息系统安全功能，提高内部网络安全防护性能和抗破坏能力，在网络系统受到危害之前可以提供安全防护解决方案。并可根据用户需求对该系统功能进行升级。

5 关键技术

网神运维审计系统采用系列先进技术，成功实现命令及图形的捕获与控制，为服务器的安全运行提供了强有力的系统工具。

5.1逻辑命令自动识别技术

网神运维审计系统自动识别当前操作终端，对当前终端的输入输出进行控制，组合输入输出流，自动识别逻辑语义命令。系统会根据输入输出上下文，确定逻辑命令编辑过程，进而自动捕获出用户使用的逻辑命令。该项技术解决了逻辑命令自动捕获功能，在传统键盘捕获与控制领域取得新的突破，可以更加准确的控制用户意图。

该技术能自动识别命令状态和编辑状态以及私有工作状态，准确捕获逻辑命令。

5.2智能负载均衡技术

网神运维审计系统采用智能负载均衡技术为运维管理提供了三级全面冗余机制：

1、当多台运维审计系统同时提供访问时，每台运维审计系统可以设为正常工作状态或备份状态，或者同时设定为正常工作状态。系统根据管理员事先设定的负载算法和当前网络的实际的动态的负载情况决定下一个用户的请求

将被重定向到的运维审计系统。而这一切对于用户来说是完全透明的，用户完成了对运维服务的请求，并不用关心具体是哪台服务器完成的。

2、对于整个运维审计系统系统，资源得到充分的利用和冗余。一般情况下不同应用服务的用户数目是不尽相同的，对于被管服务器资源的消耗也有所不同。如果对每一种应用只采取单独的机器提供服务，不但存在单点故障问题，同时每台运维审计系统的利用也是不均匀的，可能存在大量的运维请求，使单一的运维审计系统负荷超重；而同时其它临近的运维审计系统却处在基本空闲状态。这也是一种系统资源的浪费，同时用户得到的服务也不够快捷。在引入了智能负载均衡技术的网神运维审计系统群中，每台运维审计系统的资源得到了充分利用，并减少了单点故障的问题。

3、智能负载均衡也可以引入冗余备份机制。网神运维审计系统负载均衡在网络层次上起到类似"路由器"的作用，并利用专用的数据通信转发技术完成智能的负载分配的工作。它的单点故障问题可以通过在系统中引入另外一台运维审计系统设备来完成。网神运维审计系统冗余备份通过网络互相监测，一旦其中一台不能正常工作，另一台将接管其所有的任务。

5.3Syslog 日志处理

网神运维审计系统采用分布式处理架构进行处理，启用命令捕获引擎机制，通过策略服务组件完成策略审计，通过日志服务组件存储操作审计日志，各组件可以独立工作，也可以分布于不同的服务器上，亦可将所有组件安装于一台服务器上。

所有的操作审计日志可采用 Syslog 转发到统一存储服务器上，如审计中

心，也可以指定 Syslog 网络存储位置。

Syslog 日志输入配置图

这种分布式设计有利于策略的正确执行和操作记录日志的安全。同时，各组件之间采用安全连接进行通信，防止策略和日志被篡改。

5.4正则表达式匹配技术

网神运维审计系统采用正则表达式匹配技术，将正则表达式组合纳入树型可遗传策略结构，实现控制命令的自动匹配与控制。树型可遗传策略适合现代企业单位的管理架构，为服务器的分层分级管理与控制提供了强大的工具。

5.5图形协议代理

为了对图形终端操作行为进行审计和监控，网神运维审计系统对图形终端使用的协议进行代理，实现多平台的多种图形终端操作的审计，例如 Windows

平台的 RDP 方式图形终端操作，Linux/Unix 平台的 X11 方式图形终端操作。

5.6多进程/线程与同步技术

网神运维审计系统主体采用多进程/线程技术实现，利用独特的通信和数据同步技术，准确控制程序行为。多进程/线程方式逻辑处理准确，事务处理不会发生干扰，这有利于保证系统的稳定性、健壮性。

5.7通信数据加密技术

网神运维审计系统在处理用户数据时都采用相应的数据加密技术来保护用户通信的安全性和数据的完整性，防止恶意用户截获和篡改数据，充分保护用户在操作过程中不被恶意破坏。

5.8审计查询检索功能

在《萨班斯法案》、《ISO27001/BS7799》、《企业内部控制规范》等标准中，均明确要求企业内控必须有严格的审查，由此企业的内部审计显得格外重要。

网神运维审计系统能够为企事业单位的内部网络提供完全的审计信息，这些审计信息能够为单位追踪用户行为，判定用户行为等，能够还原出用户的操作行为。

传统审计关联到 IP、MAC、公用账号等，这本身是一个不确定的和不负责任的审计结果，因为 IP、MAC、公用账号信息并不能够真实反应出真实的操作者是谁，同时，各 IT 应用系统的审计是相互独立，没有关联，导致企业单位内部网络出现问题不能有效追踪到操作者。网神运维审计系统能够对这些用户行为进行关联审计，就是说真正能够把每一次审计出的用户操作行为绑定到自

然人身上，便于单位内部网络管理追踪到个人，无法抵赖，真正做到实名制管理。

5.9操作还原技术

操作还原技术是指将用户在系统中的操作行为在真实的环境中模拟显现出来，审计管理员可以根据操作还原技术还原出真实的操作，以判定问题根源所在。

网神运维审计系统采用操作还原技术能够将用户的操作流程自动地展现出来，能够监控用户的每一次行为，判定用户的行为是否对单位内部网络安全造成危害。

6 为用户带来的收益

网神运维审计系统通过对企业 IT 用户和 IT 资源的使用或管理关系的梳理，帮助企业建立用户树和资源树，统一企业安全目录，建立集中的身份认证与访问控制管理平台。帮助企业解决各类异构 IT 资源的帐号密码管理和访问控制管理问题，实现完整的用户帐号管理、安全简洁的认证管理、最合理化的最小授权管理、缜密细致的综合审计管理以及严谨的访问控制管理等与“人”相关的一系列安全管理功能。

6.1统一平台管理

网神运维审计系统为用户提供了横跨所有UNIX类服务器、LINUX类服务器、Windows 类服务器、网络、安全等重要设备的统一操作管理平台，统一操作管理入口，并对用户操作管理等网络访问行为进行控制，避免用户直接接触目标

服务器重要资源，构建安全规范的服务器操作管理唯一通道。

网神运维审计系统不改变用户原有使用习惯，提供了字符终端平台、图形终端平台、文件传输平台、应用中心操作等多种平台，实现虚拟应用集中发布操作统一管理。

6.2全面操作审计

网神运维审计系统支持 Unix/Linux/Windows 等主机及网络设备的运维操作审计，支持主流数据库（DB2、Oracle、MSSQL、Mysql 等）客户端的运维操作审计，还支持各种 B/S、C/S 多业务应用操作审计，网神运维审计系统完整记录会话的整个过程，并形成会话日志和事件回放文件。消除安全审计盲点，全面审计网络操作行为。

6.3提高设备可用性，网络安全性

通过部署网神运维审计系统，可以减轻设备的运维强度，降低 IT 运维管理的复杂度，帮助企业提高 IT 设备的可用性；减少网络中原来所有服务器都需要对外开放维护端口的暴露，做到由单一的运维审计系统提供对外维护端口，提高网络安全性。

6.4完善责任认定体系

通过部署网神运维审计系统，所有系统管理人员、第三方系统维护人员，都将通过运维审计系统来实施网络管理和服务器维护，对所有的操作行为，都做到可记录、可控制，审计人员通过定期对维护人员的操作审计，可以规范运维人员的操作，真正做到“事前可知，事中可控，事后可查”。

6.5规范操作管理

通过网神运维审计系统，可以实现操作透明化，对于用户的任意操作，可以通过 web 界面实时监控，无论是内部运维人员以及外包运维商所做的所有操作都会被真实完整地记录下来。

对于操作实现可控，对于存在风险的操作可以实现事前以及事中的控制。通过权限控制，可以主动切断用户的高危操作，也可以对于用户的违规操作，可以实时切断。

网神运维审计系统将用户从繁琐的密码管理工作中解放出来，投入到其他工作上，对第三方代维厂商的维护操作也不再需要专门陪同，从而有效提高了操作管理效率。

6.6规避操作风险

网神运维审计系统强大的权限控制和安全审计功能，可以用户充分符合《萨班斯法案》、《ISO27001/BS7799》、《企业内部控制规范》等信息安全标准，符合等级保护要求。

规范本行操作人员和第三方代维厂商的操作行为。通过部署网神运维审计系统，所有系统管理人员，第三方系统维护人员，都将通过运维审计系统来实施网络管理和服务器维护，对所有的操作行为，都做到可记录、可控制，审计人员通过定期对维护人员的操作审计，可以提高维护人员的操作规范性。对于第三方代维厂商，通过网神运维审计系统保证让他们所有的操作行为变得可视，可控，可管，可追踪，实现对第三方代维厂商的有效监管。

所有网络设备和服务器上的所有终端命令行以及图形界面的操作，都会被

真实完整地记录在网神运维审计系统内，当发生任何安全问题或对代维方的操作产生争议时，都可通过录像的回放再现真实场景，帮助快速反应定位故障点和责任人。审计过程可根据命令、时间、账号等多种关键字快速检索，并可直接生成报表输出。

7 产品部署

网神运维审计系统接入用户网络中的方式是旁路，仅需要为系统分配一个IP，并确保该地址与需要运维的主机 IP 可达，协议可访问。

- 不需要在被管理设备上安装代理程序。
- 不改变原有的网络拓扑结构。
- 不更改用户网络设备上的配置。
- 不影响任何业务数据流。
- 几分钟就可以部署完毕。
- 支持双机热备。
- 支持主主模式

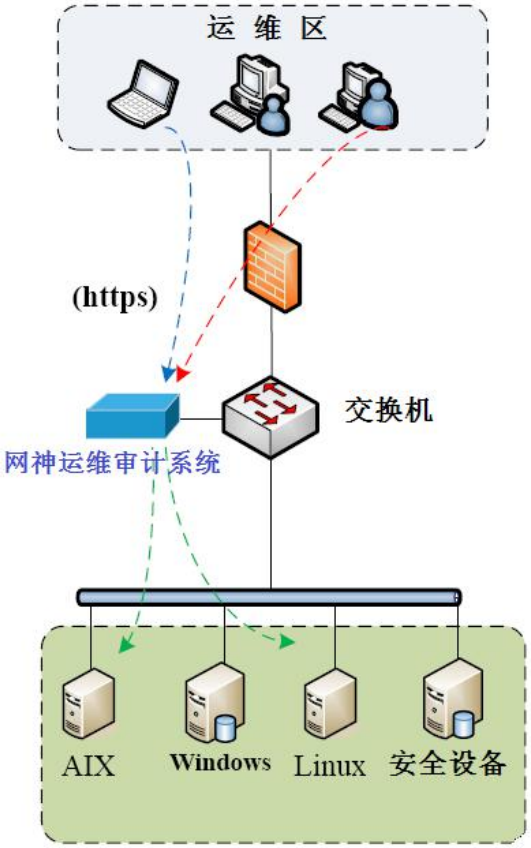
维护人员维护被管服务器或者网络设备时，首先以 WEB 方式登录运维审计系统，然后通过运维审计系统上展现的访问资源列表直接访问授权资源。

不论运维人员以何种方式（局域网直连、VPN、ADSL 拨号等）访问运维审计系统，只要保证运维工作站与运维审计系统路由可达即可。

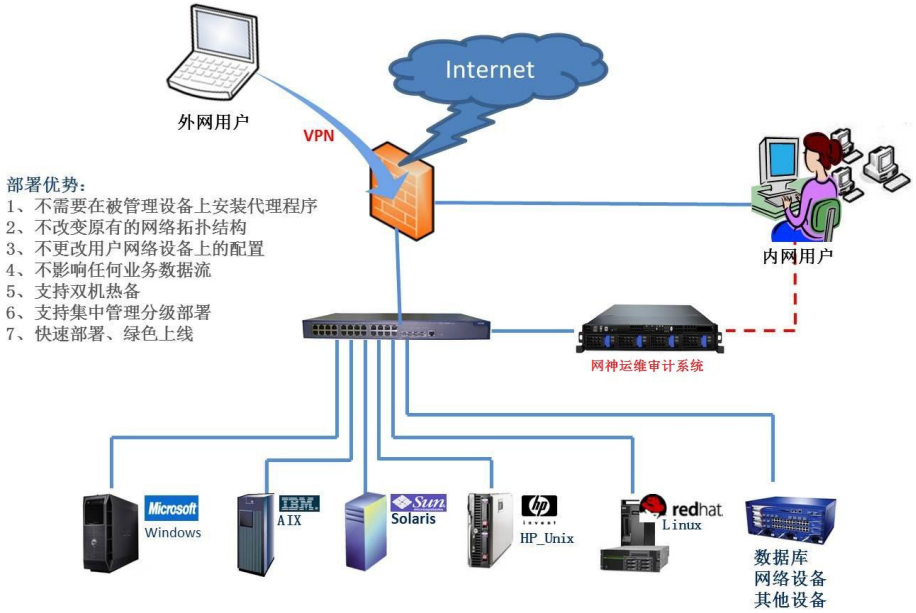
网神运维审计系统部署采用分区域、分安全域部署，根据实际网络环境，每个安全域部署一台（套），采用“分布式部署，集中式管理”模式，即“物理分布，逻辑集中”。

7.1区域内部署

网神运维审计系统部署逻辑图：



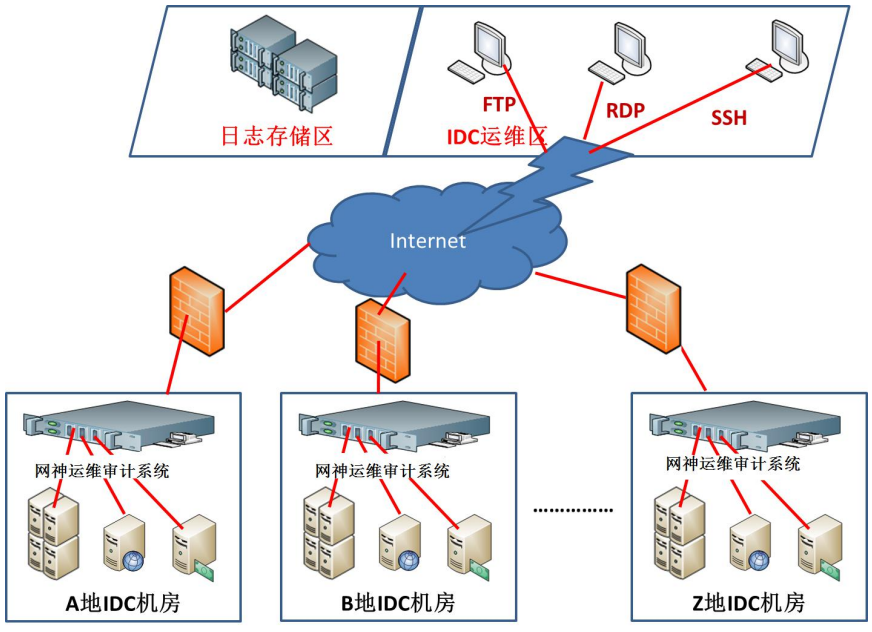
网神运维审计系统部署物理图：



如图，网神运维审计系统部署在被管服务器区的访问路径上，通过防火墙或者交换机的访问控制策略限定只能由网神运维审计系统直接访问服务器的远程维护端口。

7.2分布式部署

网神运维审计系统分布部署图：



如图，以 IDC 机房运维为例，在分布在各地的 IDC 机房内视其网络安全域划分情况部署网神运维审计系统。运维人员只需登陆被管资源所属的网神运维审计系统即可对该资源进行运维操作。

8 应用场景

8.1内部网络行为管理

严重的攻击来自系统内部（80%来自内部攻击），网神运维审计系统主要应用于内部用户行为管理，对各种途径的网络设备及服务器的访问方式进行监控，支持 Telnet、FTP、SSH、RDP，X windows 等，保证内部用户的操作和行为可控、可视、可管理、可跟踪、可鉴定，防止内部人员对机密资料的非法获取和使用，保护企事业单位的核心机密。

8.2对网络设备的管理

网络边界安全设备是企事业单位网络安全防护系统的重要组成部分，网络边界安全设备的安全策略，对企事业单位的内部网络安全起着非常重要的作用。目前关键网络边界安全设备，主要来自于国外巨头和国内领先公司，这些公司一般都提供先进的 CLI 功能，管理员可以通过 SSH 和串口，对网络边界安全设备（如交换机、防护墙、VPN 等）进行安全策略配置。但是，目前没有可靠办法保证系统管理员安全策略配置行为的有效性、合法性以及一致性，一般都通过行政手段，让系统管理员记录安全策略配置过程，这是存在严重的安全隐患的。安全网神运维审计系统提供网关部署方式，可以记录系统管理员对网络边界安全设备的配置过程，保证安全策略的一致性，其生成的日志系统，可以方

便地集成到企事业单位现有的安全策略管理架构中。

8.3对黑客行为的防范

黑客常常通过各种非法手段（如：社会工程、恶意程序、系统设置漏洞、缓冲区溢出程序等）获取用户权限，然后使用该权限登录系统。安全网神运维审计系统可以记录该黑客的操作过程，对于事后查证和数据恢复，有很好的实用价值。安全网神运维审计系统还可以通过地址绑定功能对黑客行为进行限制，即使黑客取得系统权限，也不能对系统做任何操作。

8.4替代 KVM 等的应用

现在很多用户采用 KVM over IP、PC Anywhere、并行审计等来进行服务器运维的管理。KVM 只是简单的键盘、显示器、鼠标的物理集中，没有任何账号、认证、审计的管理功能。采用 PC Anywhere、Dameware 等远程管理工具，并通过集中设置的服务器进行集中管理，虽然能减少跑腿，但是只能控制 windows 主机，对于网络设备、UNIX 系统、数据库等就无能为力了。追其根源，这些工具只是局域网中的桌面远程管理工具，用户服务器等资源的管理是力所不及的。并行审计的缺点就更突出了，完全没有集中管控的功能和作用，只能记录一些流量不大的操作，一旦侦听的流量过大就会丢包，而且对于加密协议和图形协议，也是完全没有办法起作用。

所以，还在使用上述三类方法来管理服务器资源的用户，切换到网神运维审计系统看可以明显提高工作效率和信息资源的安全性。