任子行® SURFILTER | 网络应用审计专家
（证券代码 300311）

任子行运维安全审计

（SURF-HAC）

任子行网络技术股份有限公司
SURFILTER NETWORK TECHNOLOGY CO.,LTD.

介绍目录

IT运维概念

管理人员：部门经理或主管、设备密码管理员、审计人员

运维人员：是指对运维对象进行维护操作的人，包括系统管理员(目标设备)、网络管理员、代维人员以及设备厂商等相关人员

运维对象：是指运维操作的对象，包括各种服务器、网络设备、数据库等。设备上的某一种服务叫做资源。

运维操作：是指运维人员通过系统自身提供的远程访问协议（包括Telnet、SSH、RDP、VNC、HTTPS等）登陆到运维对象上进行的远程维护操作

运维管理面临的风险


系统管理员
数据库管理员
网络管理员
程序开发人员
代维厂商等
操作者
账号共享
交叉管理
IBM
AIX
Microsoft
Windows
Sun
UNIX
redhat
Linux
安全设备
网络设备
存储设备
资源设备
多点登录
分散管理
总部信息中心
各网点
分支机构
软件外包厂商
设备代维厂商
办公地点

运维安全事故

案例一

- 某员工大学毕业后在某网络设备公司从事软件研发工作，曾为哈尔滨、辽宁、西藏等多家移动公司做过技术工作，2005年3月，他利用为西藏移动做技术服务时使用的密码(此密码离开后一直没有更改），轻松进入西藏移动的服务器，并通过西藏移动的服务器，跳转到北京移动数据库，2005年3月至7月，先后4次侵入北京移动数据库，修改充值卡的时间和金额，将已充值的充值卡状态改为未充值，共修改复制出上万个充值卡密码，共获利370余万元

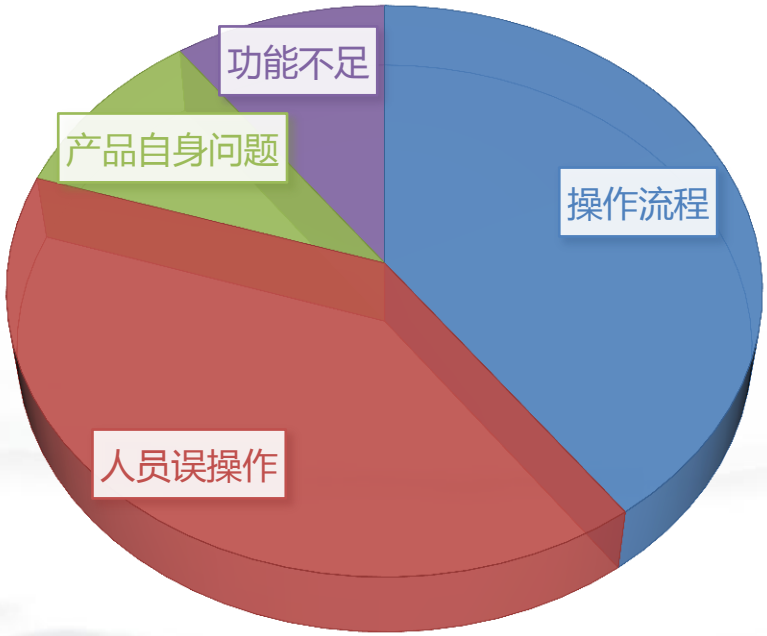
案例二

- 上海天游公司
- 问题：淘宝上有人非法销售他们开发游戏里的道具
- 真相：内部的某开发人员和DBA人员修改数据库的数据来牟利，这影响到了他们的合法收入

市场调查

国际著名咨询调查机构Gartner集团的调查：

在经常出现的运维事故中，源自技术或产品本身方面的问题其实只占20%，而**操作流程失误**问题占40%，**人员的误操作**问题占40%；面对这种情况，企业需要一套完善的运维管理解决方案。

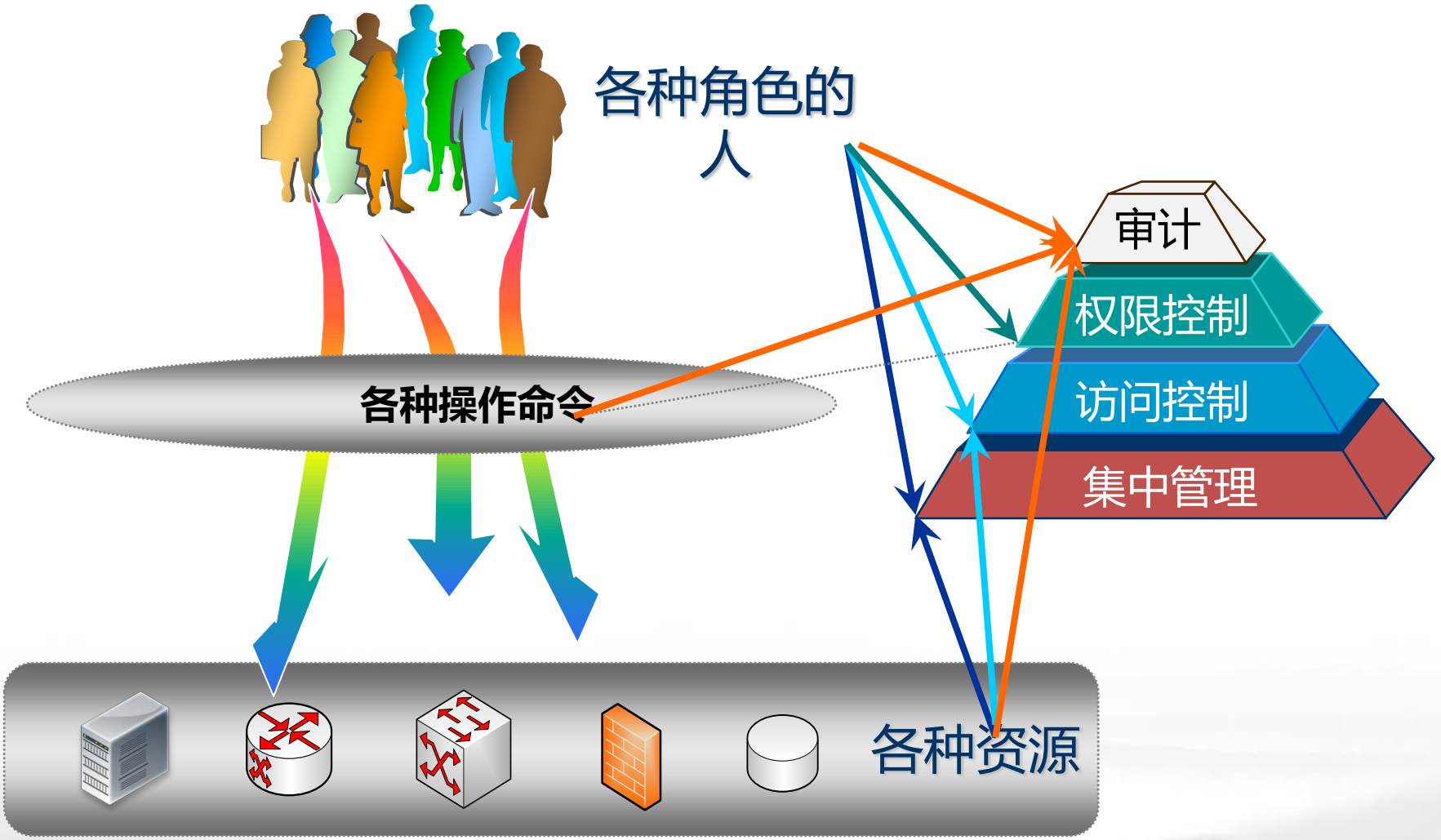


政策背景

- 萨班斯.奥克斯利法案（Sarbanes-Oxley）
- 《信息系统安全等级保护基本要求》
- 《企业内部控制基本规范》

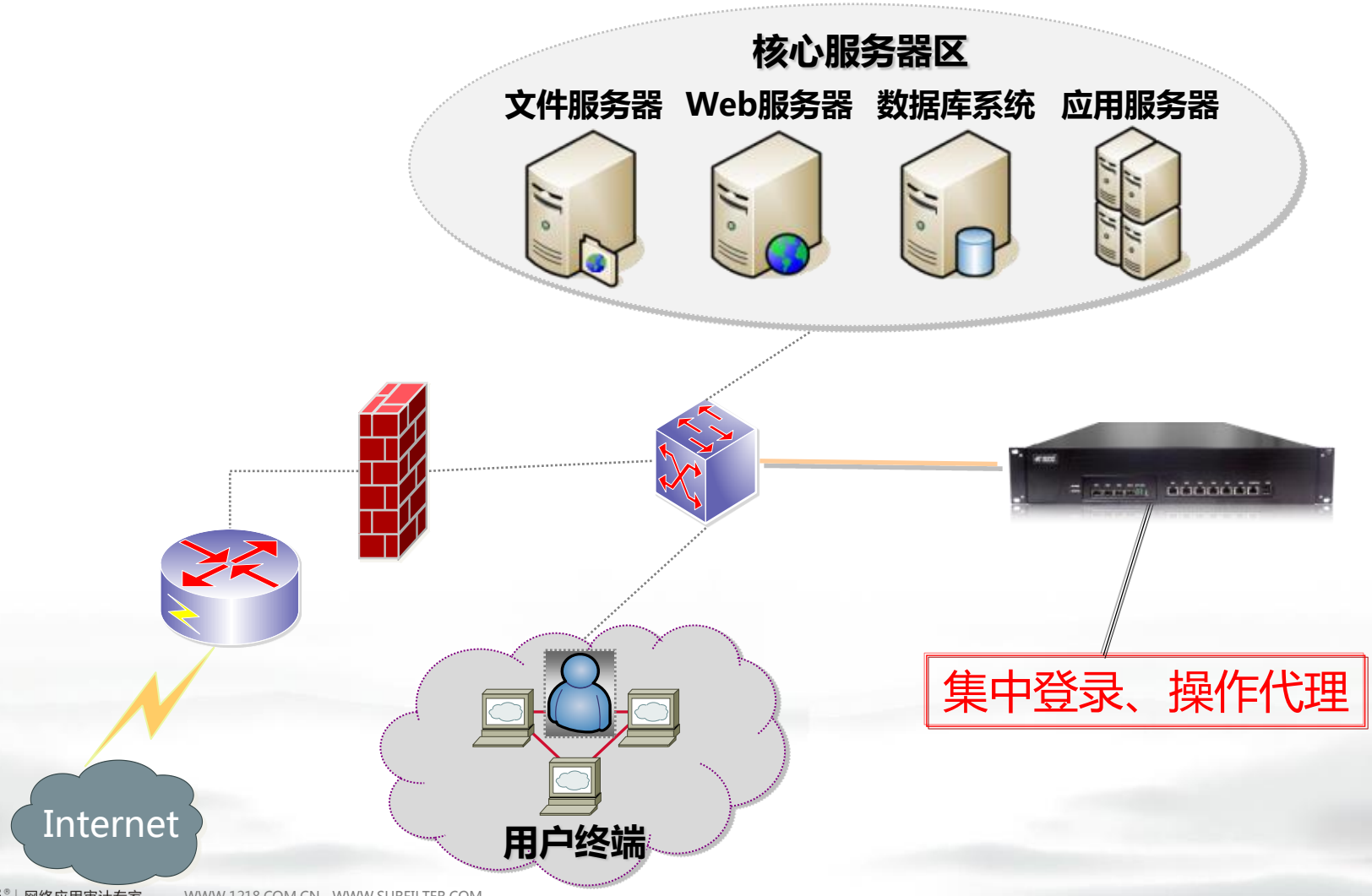
介绍目录

IT运维审计核心内容

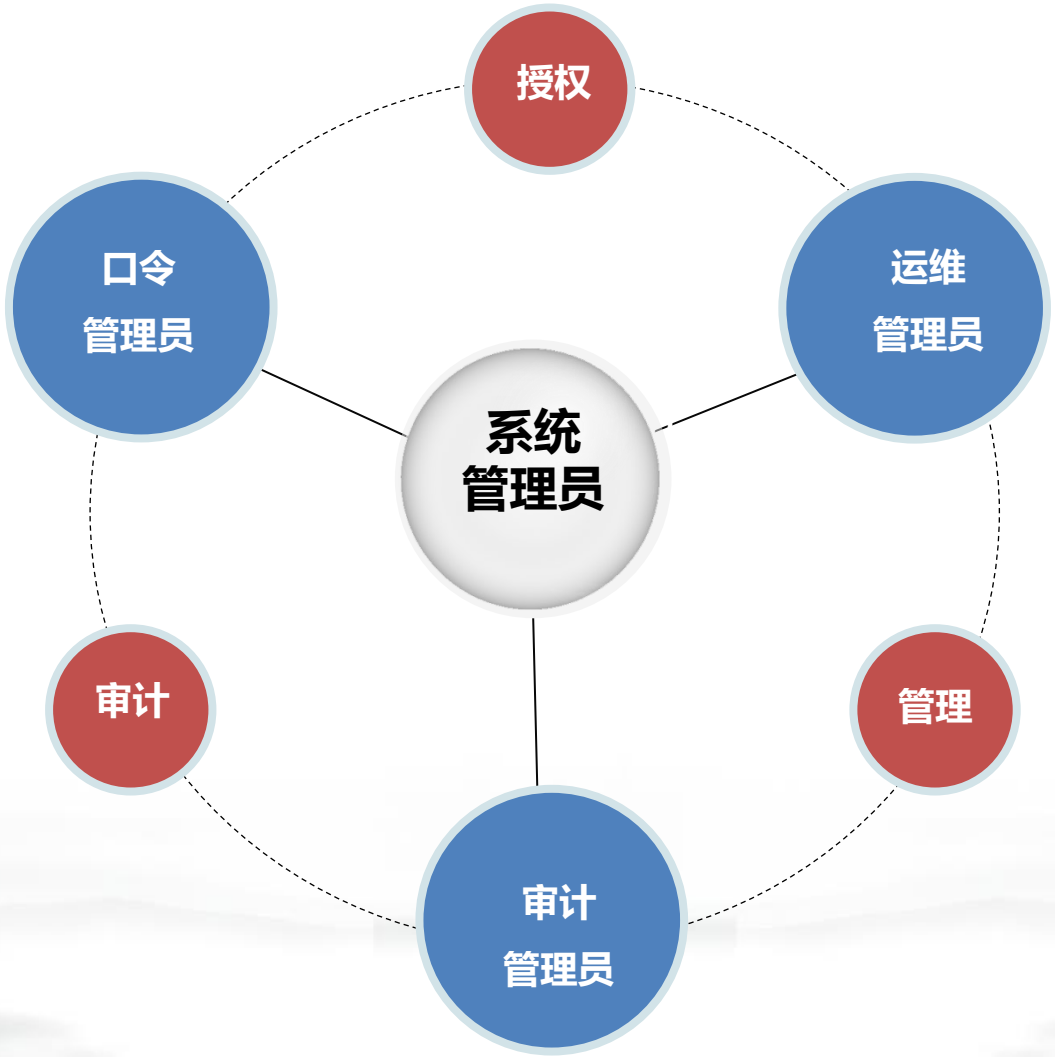


集中管理

需要从网络层做访问控制，保证所有的用户只能通过IT运维来访问所有的资源

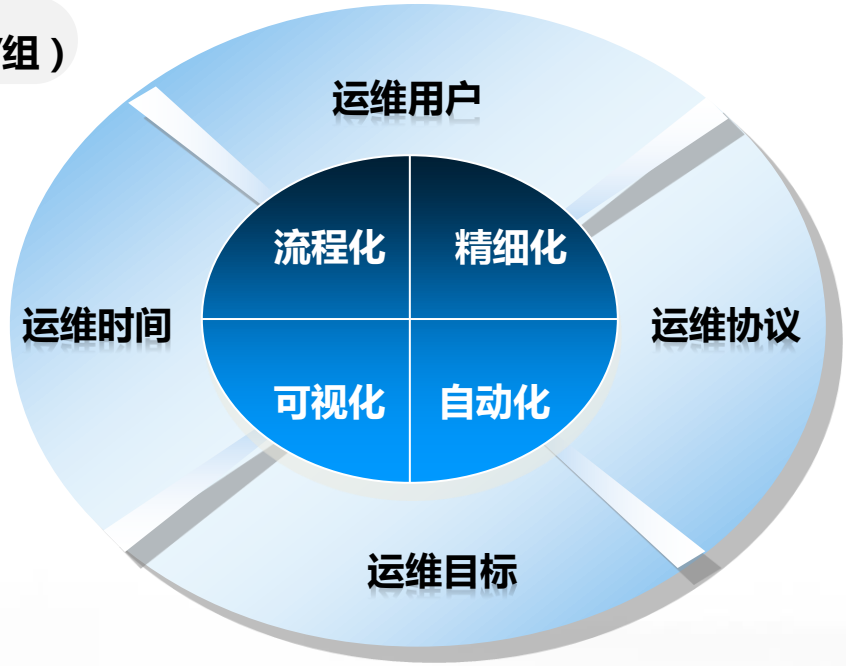


授权管理



访问控制

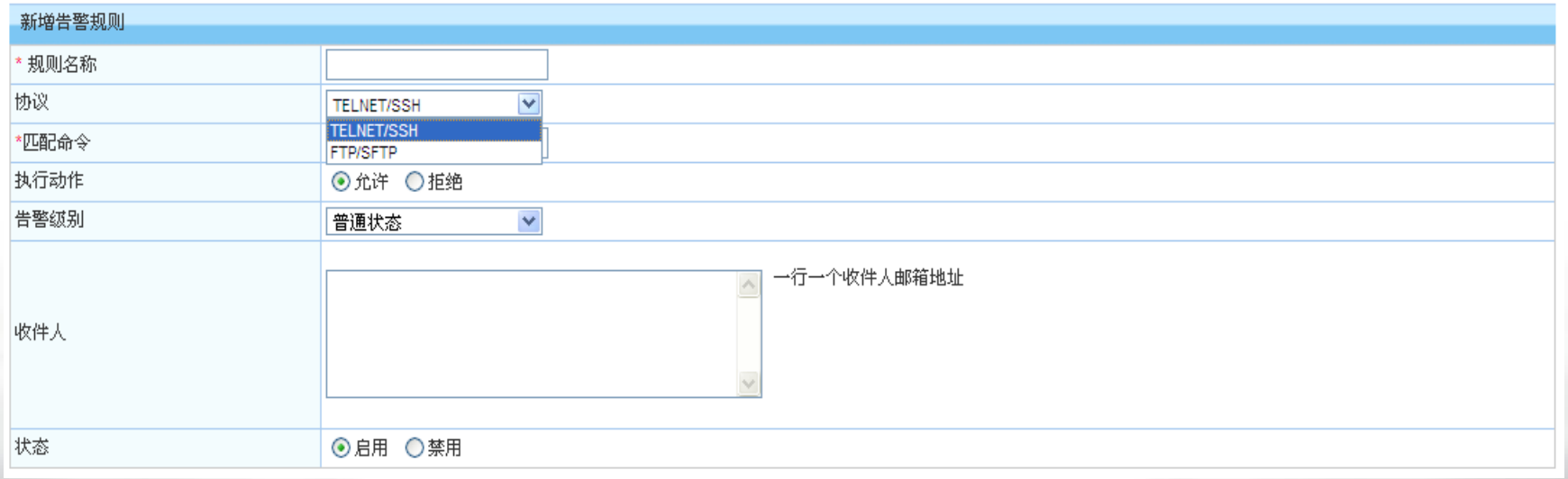
1. 多样化资源授权（用户/组、资源/组）
2. 资产管理，防拷贝防打印
3. 运维目标病毒防护、恶意软件
4. 双人运维、紧急运维



权限控制

违规操作实时告警|阻断

- ✓ 根据安全策略实施运维过程敏感操作检测，对违规操作提供实时告警和阻断
- ✓ 支持使用者分级，针对不同使用者级别采取不同的响应方式
- ✓ 告警与会话实时监控、会话审计与回放关联



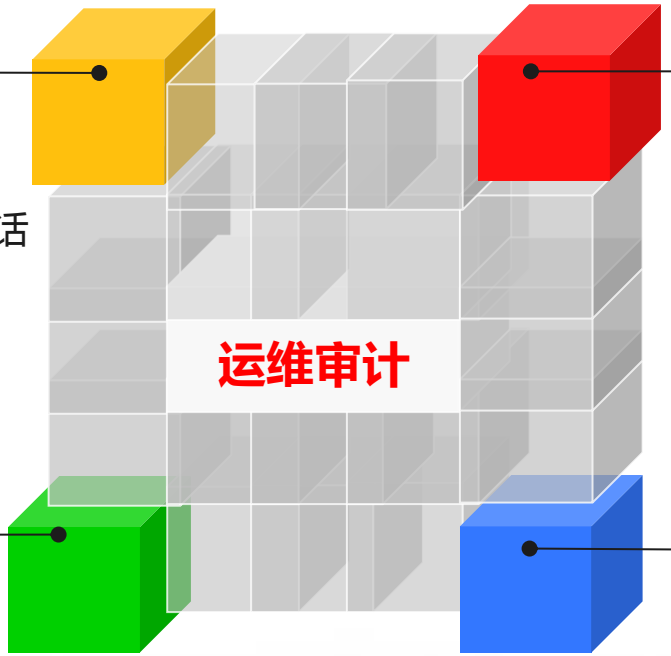
运维阻断


```
login successful



root@ubuntu6T:~# ls
cmd deny by firewall!

root@ubuntu6T:~# cd /etc/
cmd deny by firewall!

root@ubuntu6T:~# touch test.py
root@ubuntu6T:~# rm -rf test.py
cmd deny by firewall!

root@ubuntu6T:~#
```

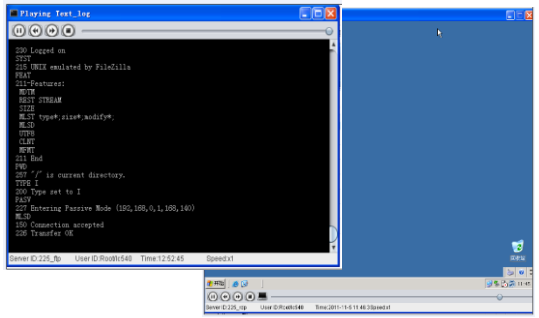
运维审计

▪实时监控

- 监控在线运维会话
- 监控后台资源存取情况
- 可实时终止异常在线运维会话
- 在线存取操作的实时监控



▪审计日志



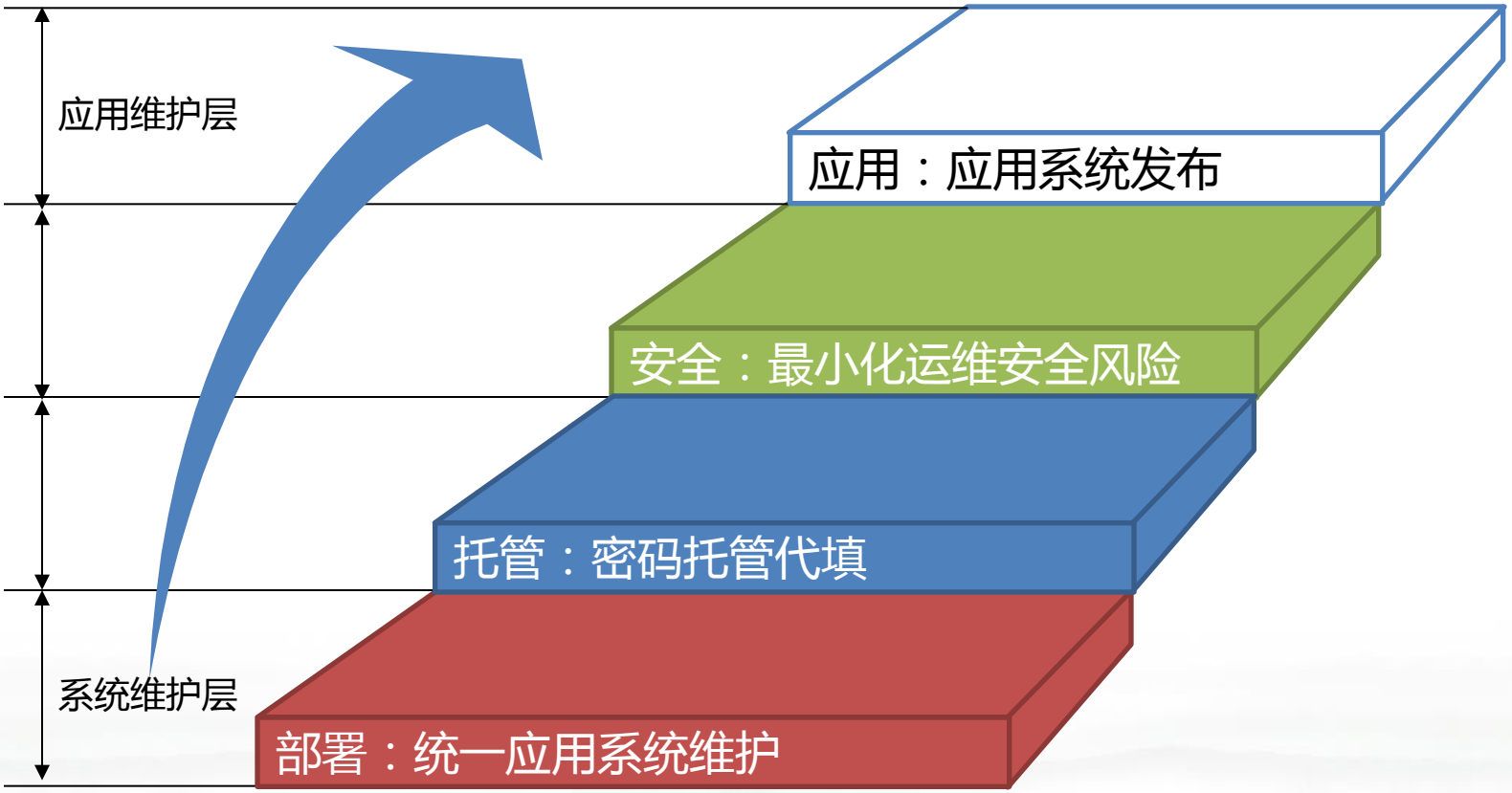
▪运维协议

- 命令行字符运维
- 图形操作运维
- 应用发布软件

▪ 日志报表

- 告警日志报表
- 自动报表
- 手动报表

应用发布



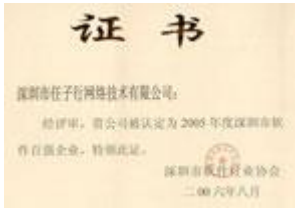
荣誉资质


国家高技术产业化
示范工程
国家发展和改革委员会
二零零七年颁发


省级
网络安全应急服务支撑单位


守合同重信用企业


自主创新行业龙头企业
深圳市人民政府


证 书
深圳市任子行网络技术有限公司:


深圳市重点软件企业
认定证书


广东省计算机信息系统安全服务等级证


荣获


高新技术企业


深圳市2011年优秀软件企业
任子行网络技术股份有限公司


软件企业认定证书


CNCERT/CC


证 书
第十届中国国际软件博览会
INT'L SOFT CHINA 2006
金 奖


广东省重点新产品
证 书


国家重点新产品
证 书

介绍目录

产品部署

第三方运维人员

Internet

移动运维

防火墙

内网运维人员

SURF-HAC

IBM AIX

Microsoft Windows

Sun UNIX

redhat Linux

安全设备
网络设备
存储设备

介绍目录

应用案例-企业

客户需求：

1、运维设备多，运维人员少，路由器、交换机、服务器等需要经常运维。

2、企业OA系统数据库内容要求审计。

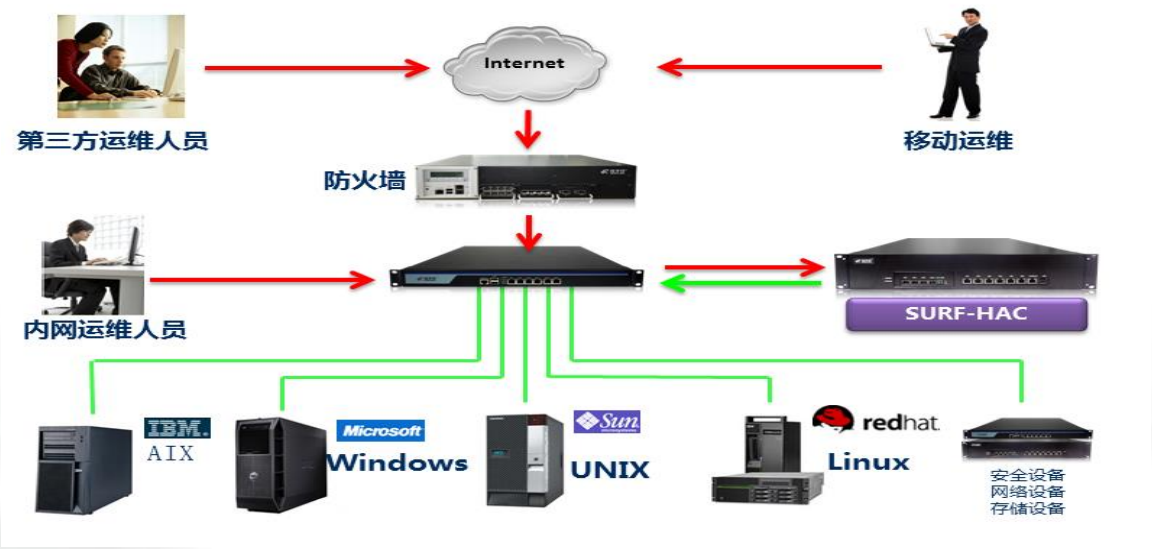
3、对于经常出差的运维人员，需要远程在外地接入运维，对此过程需要有授权机制和审计机制

方案效果：

1、只需要一台堡垒机即可实现对所有运维设备的快速访问、运维。

2、对企业办公系统数据库审计，保障数据库操作合法性。

3、通过运维授权机制保障对外地运维人员进行有效的监管。



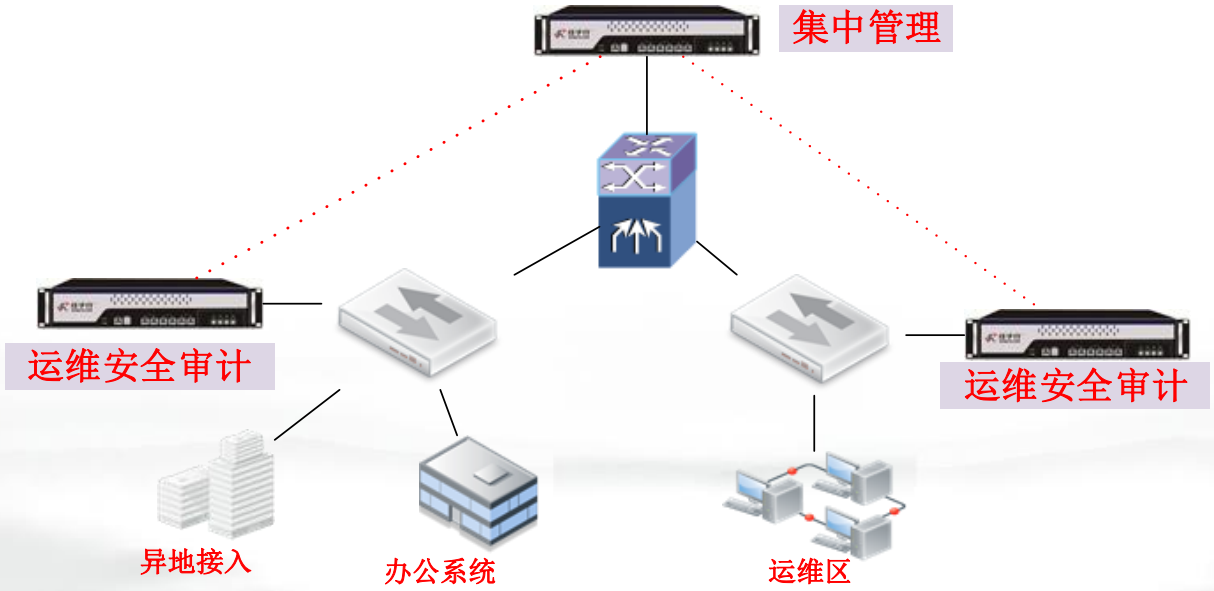
应用案例-运营商

客户需求：

1、服务器和网络设备的帐号管理混乱，存在僵尸帐号、共用帐号等问题。
2、服务器硬件厂商、第三方应用服务提供厂商，需要定期维护，分配给他们的用户名/密码容易混乱。
3、各支撑系统独立运行、维护和管理，所以各系统的审计也是相互独立的，缺乏集中统一的系统访问审计。
4、无法对支撑系统进行综合分析，不能及时发现内部破坏和外部入侵行为。

方案效果：

1、服务器和网络设备的帐号集中管理，便于维护。
2、堡垒机对网络运维设备统一密码托管，人员无法破解或泄露。
3、对运维人员运行行为录屏审计，事后提供追责依据。



Thanks

全国统一服务热线：400 700 1218

任子行® SURFILTER | 网络应用审计专家
（证券代码 300311）