

信息安全与企业内控

---四川移动公司4A案例分享

刘忆
13408084242

议题

Ø 天懋公司简介

Ø Trustmo-4A解决方案

Ø 四川移动4A平台案例分享



天懋 值得信赖的IT系统管理服务提供商

- 始终专注IT系统管理领域
- 多年IBM软件分销服务经验,深厚行业背景
- 众多成功案例
- 公司资质
 - 广东省软件企业认定证书
 - IBM软件部技术支持中心
 - IBM Tivoli 金牌级认证服务合作伙伴



成功案例

Government

广东省公安厅
广东省环保局
广州市交通委员会
珠海市劳动和社会保障局
.....

I

中国银行广东分行
招商银行
成都银行
江门供电局
广州联合电子收费公司
安利（中国）有限公司

Telecom

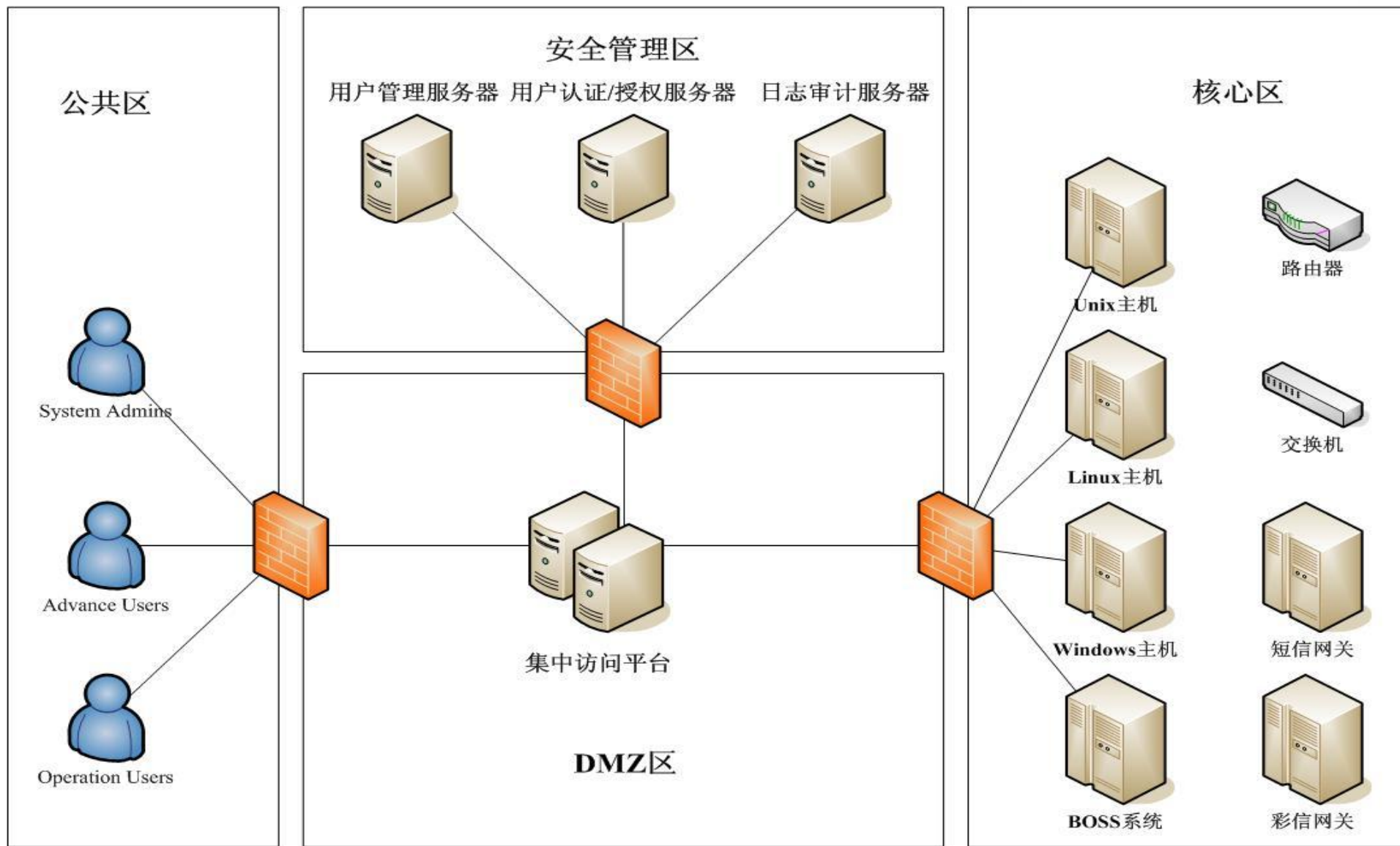
四川省移动通信有限公司
广西省电信
广西省移动通信有限公司
珠海移动通信有限公司
.....

在中国，天懋的客户已覆盖电信、电力、烟草、金融、政府等行业，其产品和服务越来越受到市场与用户的肯定。其实施的多个项目已经成为中国行业标准 and ITIL 规范试点单位。

议题

- Ø 天懋公司简介
- Ø Trustmo-4A解决方案
- Ø 四川移动4A平台案例分享

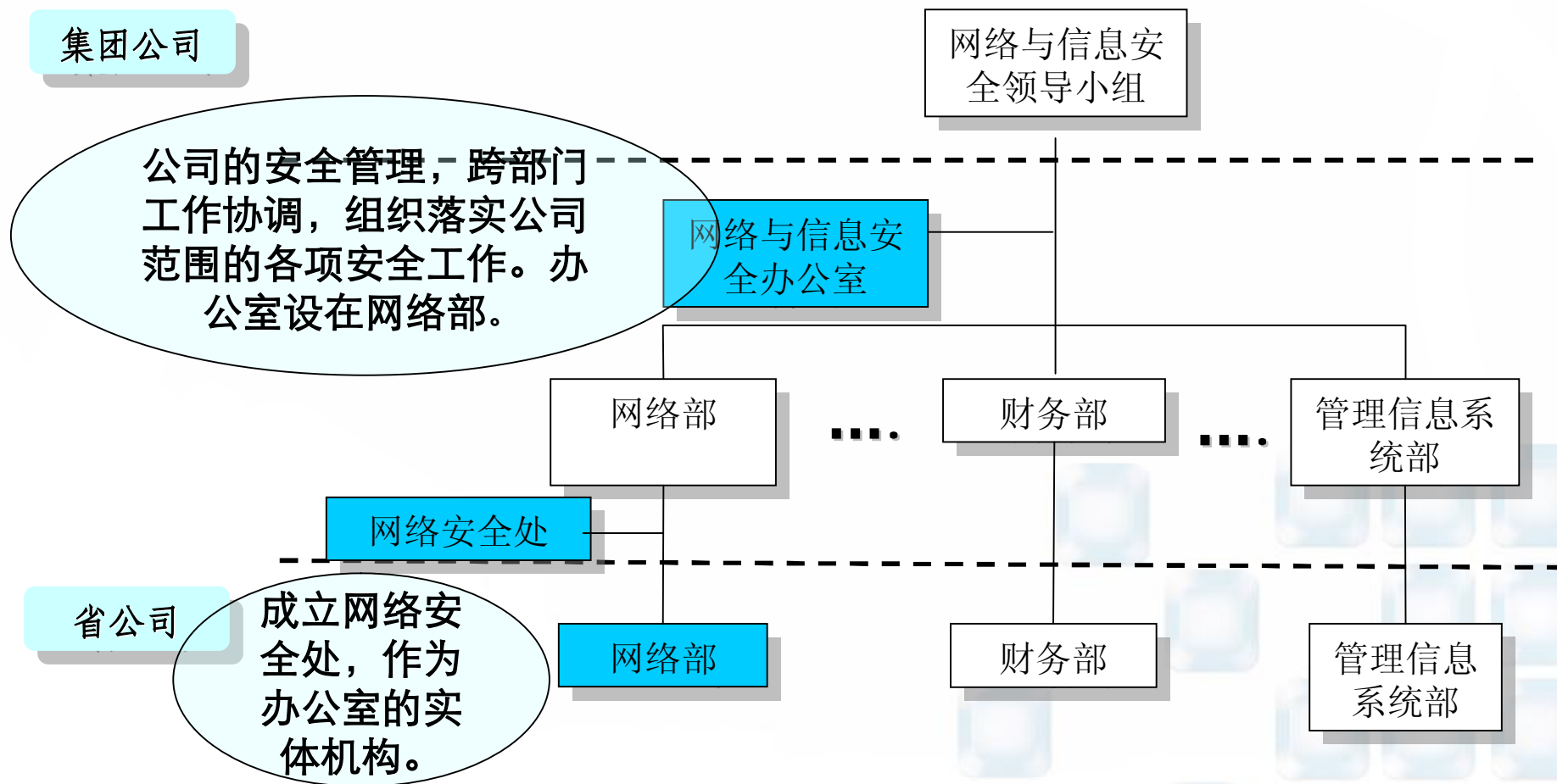
Trustmo-4A解决方案



四川移动4A平台案例分享

- 一、中国移动信息安全管理框架
- 二、中国移动4A规范
- 三、四川移动4A平台框架及建设情况

中国移动信息安全管理体系组织架构



四川移动日志审计平台

- 一、中国移动信息安全管理框架
- 二、中国移动4A规范
- 三、四川移动4A平台框架及建设情况

4A（账号、认证、授权、审计）管理定义

- Ø 账号管理 (Account) 是将自然人与其拥有的所有系统账号关联，集中进行管理，包括按照密码策略自动更改密码，不同系统间的账号同步等。
- Ø 身份认证 (Authentication) 是信息安全的第一道防线，用以实现支撑系统对操作者身份的合法性检查。对信息统中的各种服务和应用来说，身份认证是一个基本的安全考虑。身份认证的方式可以有多种，包括静态口令方式、动态口令方式、基于公钥证书的认证方式以及基于各种生物特征的认证方式。
- Ø 授权管理 (Authorization) 是指对用户使用的支撑系统资源的具体情况进行合理分配的技术，实现不同用户对系统不同部分资源的访问。
- Ø 审计 (Audit) 是指收集、记录用户对支撑系统资源的使用情况，以便于统计用户对网络资源的访问情况，并且在出现安全事故时，可以追踪原因，追究相关人员的责任，以减少由于内部计算机用户滥用网络资源造成的安全危害。

四川移动日志审计平台

一、中国移动信息安全管理框架

二、中国移动4A规范

三、四川移动4A平台框架及建设情况



运维用户的管理挑战

多种设备有各自的日志存储方式，无法实现集中展现，关联分析

多套系统多个帐号多种日志，怎样做到有效、完整的授权和审计？多人共用帐号，无从定位到底是谁做了什么事情

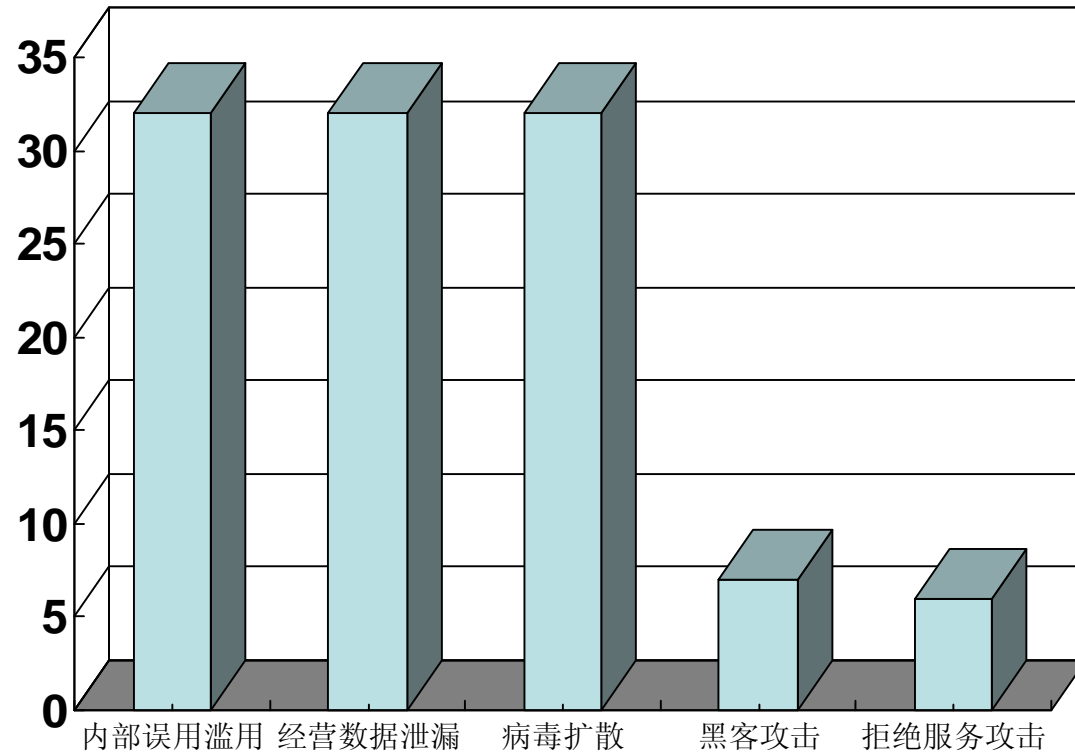
各种设备自存储系统不可能对日志进行过滤、组合

帐号授权/认证的日志信息的审计？



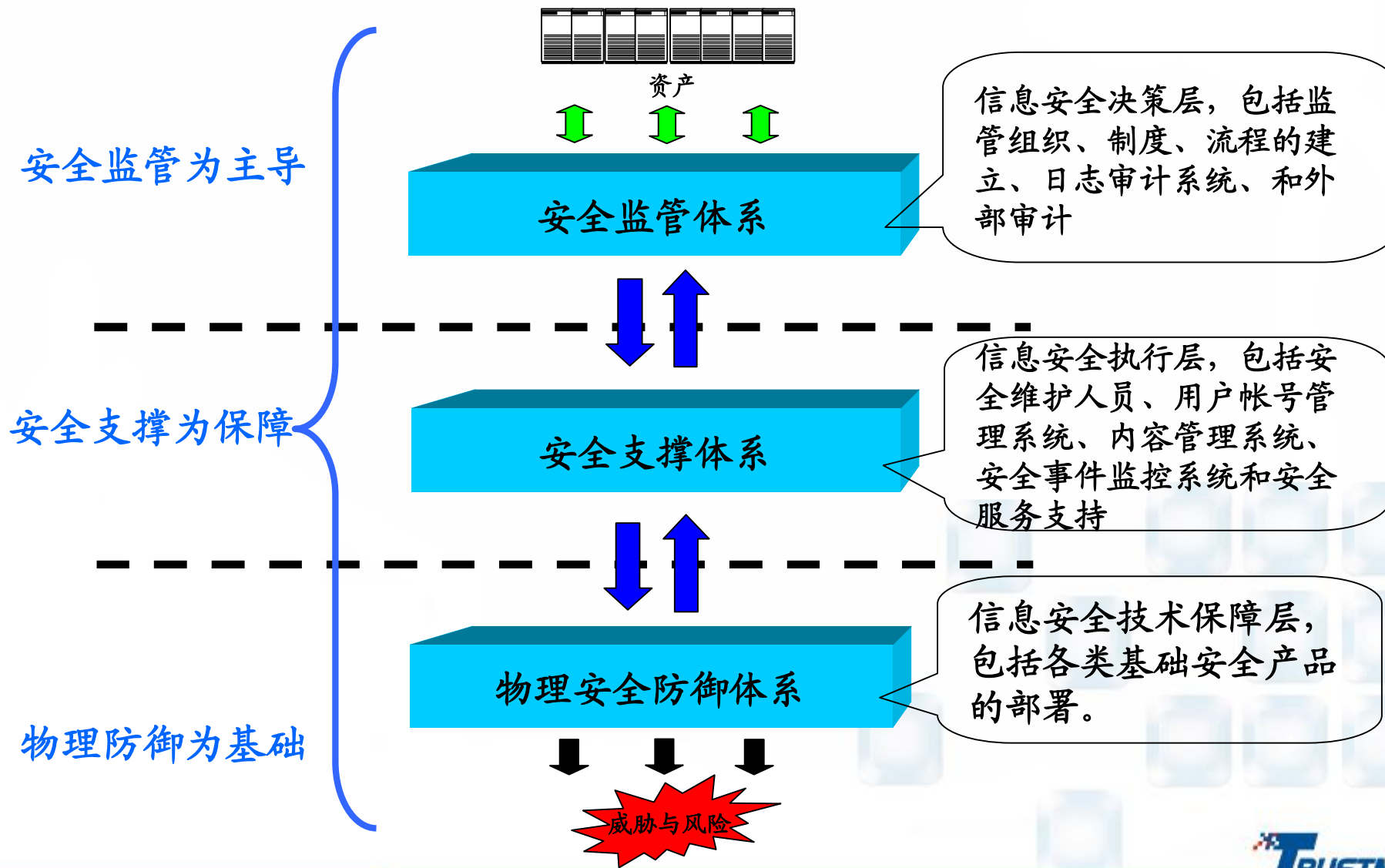
信息系统面临的威胁

- 内部误用滥用、经营数据泄漏和病毒扩散是普遍最为关注的安全威胁
- “内控”是降低数据泄漏、误用滥用威胁的有效手段
- 理顺流程、建立身份访问管理机制、控制流程节点等是建立“内控”的有效途径
- 安全域划分、AAAA、防病毒、终端桌面管理等是重要的安全防护基础设施



→ 其中，安全审计是保持安全基础设施和“内控”的有效性的关键！

四川移动的安全管理体系



4A平台三大子系统功能说明

4A平台

集中帐号管理
平台

集中认证鉴权
平台

集中审计管理
平台

能够实现四大中心各主机、网络设备、业务系统账号的集中存放，单点登录以及提供账号生存期管理。

实现在一点集中对所有用户登录业务系统的行为进行认证和授权，将使用信息系统资源的具体情况进行合理分配，实现不同用户对系统不同部分资源的访问控制。

采取集中管理的方式在更高的层面上接收和深层分析来自四个业务中心相关安全设备、业务系统报送来的各种安全事件以及信息资产自身产生的各种和安全有关的日志。

4A平台支撑软件说明

- 帐号平台

IBM Tivoli Identify Manager

- 审计平台

IBM Tivoli Security Operations Manager

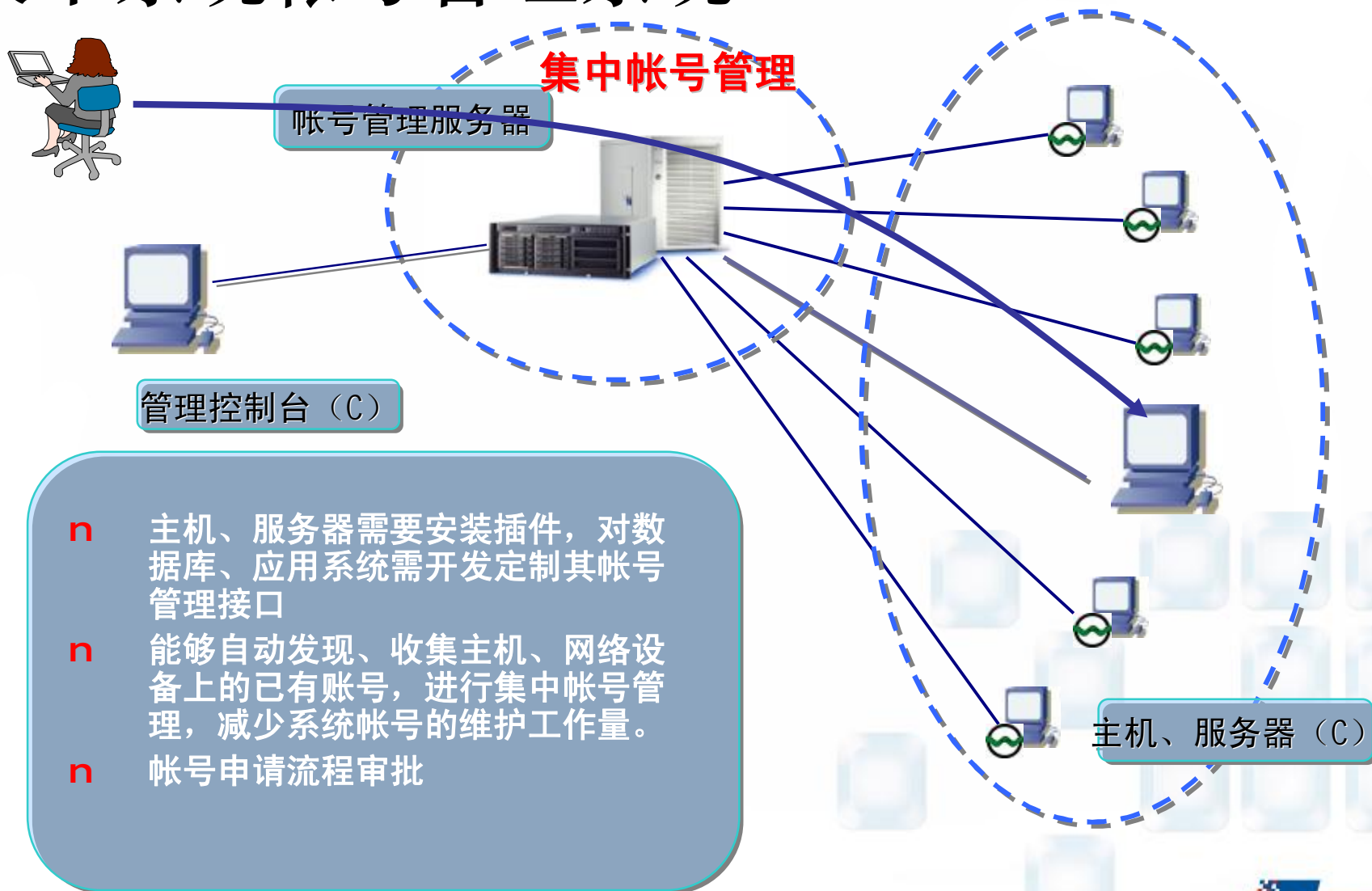
- 单点登陆

IBM Tivoli Access Manager for Enterprise Single Sign-on

集中帐号管理平台主要功能

- Ø 实现用户账户的全面管理，包括创建、修改、检查、删除等
- Ø 建立组织架构和用户的全局视图
- Ø 支持业界广泛的账户资源，并且提供灵活的扩展
- Ø 实现基于角色的用户账户管理策略
- Ø 实现被管理系统的统一用户口令策略和用户口令的集中管理
- Ø 建立用户帐号管理的审批流程，并和用户账户服务实现联动
- Ø 提供全面的查询、日志和审计报告

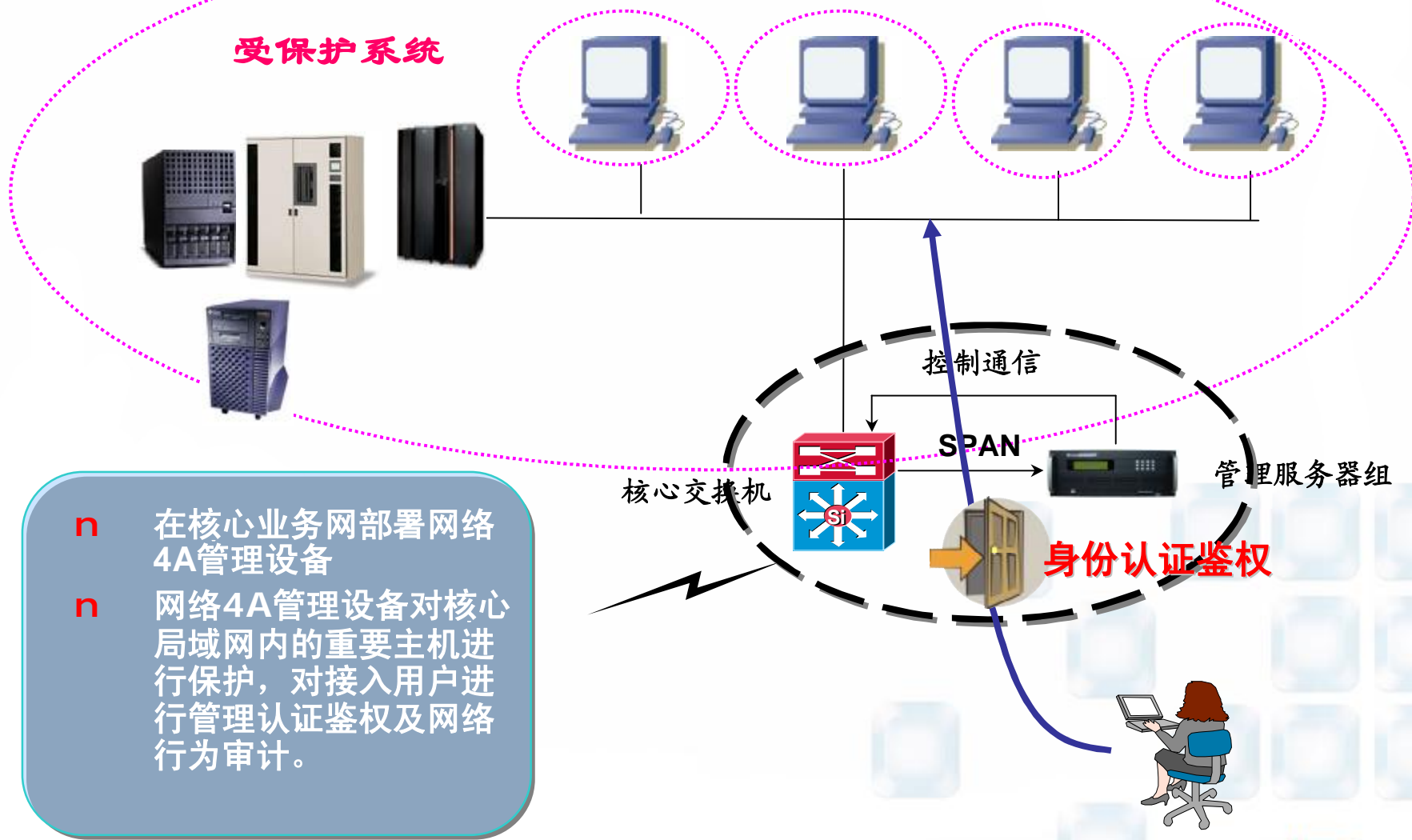
集中系统帐号管理系统



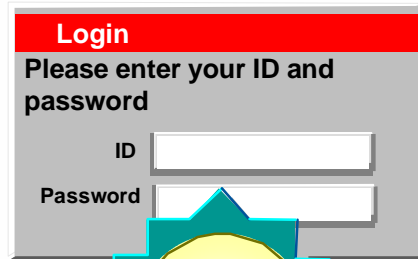
帐号管理系统组织架构

- Sichuan Mobile			
	名称 ▾	状态 ▾	定制显示 ▾
- 网管中心	<input type="checkbox"/> 杜筠	活动	dudu@sc.chinamobile.com
+ 动力中心	<input type="checkbox"/> 李晶	活动	lijing@sc.chinamobile.com
- 监控中心	<input type="checkbox"/> 廖彬涵	活动	liaobinhan@sc.chinamobile.com
+ 分析室	<input type="checkbox"/> 廖祖文	活动	liaozuwen@sc.chinamobile.com
- 支撑室	<input type="checkbox"/> 林波	活动	linbo@sc.chinamobile.com
+ 奥赛	<input type="checkbox"/> 谭蓉	活动	tanrong@sc.chinamobile.com
+ 亿阳	<input type="checkbox"/> 田丰	活动	tianfeng@sc.chinamobile.com
+ 直真	<input type="checkbox"/> 徐瑾	活动	xujin@sc.chinamobile.com
+ 维护中心	<input type="checkbox"/> 杨云	活动	yangyun@sc.chinamobile.com
	<input type="checkbox"/> 张伟	活动	zhangwei@sc.chinamobile.com

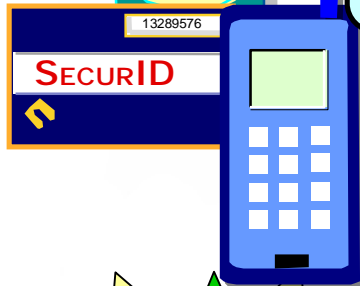
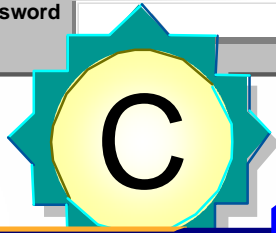
集中认证鉴权平台



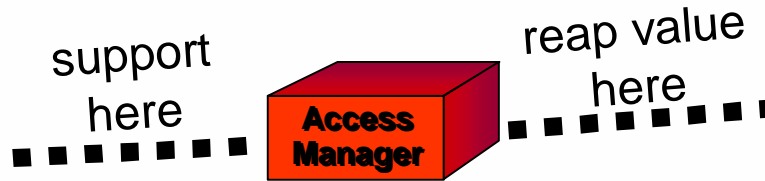
支持多种认证技术



Login
Please enter your ID and password
ID
Password



**Easy
accommodation of
authentication methods
and other security**



Prove incoming users identity

- Basic authentication (W3C)
- Forms-based authentication
- X.509 Certificate
- Kerberos ticket
- RSA SecurID Token
- DigiPass
- Daon
- Mobile device
- EAI (External Authentication Interface)
- Others via Pluggable Authentication



Acquire credentials for user

Build a credential/EPAC



单点登录

支持多种方式

-Telnet

-SSH

-Xmanager

-Windows 远程桌面



单点登录

Tools

-  Administration Tool
-  Support Assistant
-  Secure FTP
-  Logout

Published Applications



TIM Login
Address



Windows_10.101.50.100



telnet
10.101.50.66



telnet
10.101.16.17



Windows_10.101.17.45

集中日志审计

集中审计

日志服务器

将来自不同区域、不同设备、不同系统的日志信息集中存储，便于检索和分析

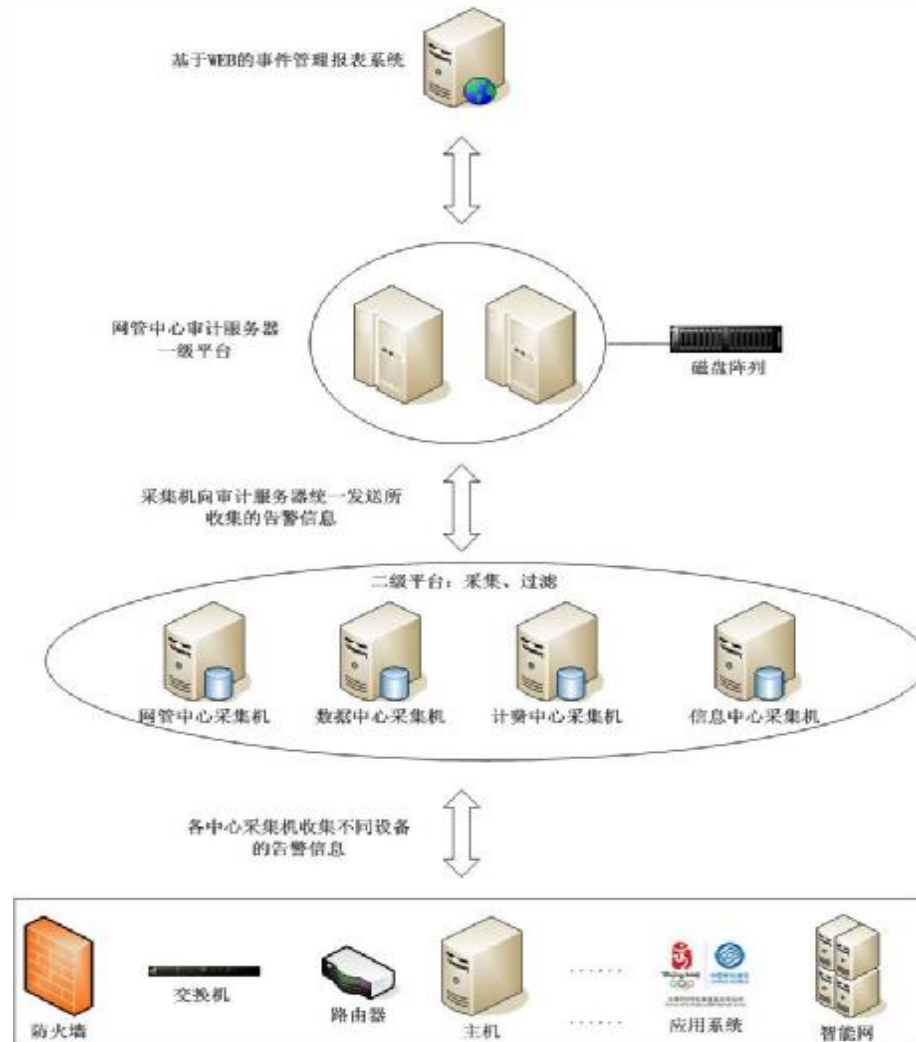
日志采集机

分布部署在各个业务中心，可进行日志收集及预处理功能。通过部署网络审计设备进行网络操作的获取。

管理服务器

对系统进行集中管理、配置、策略定制、数据分析、处理等

审计管理体系架构



集中审计——实时监控

网管中心 admin/admin 2009-07-28 13:53:03登录 [重新登录](#) [在线帮助](#) [退出系统](#)

中国移动通信 CHINA MOBILE 四川移动集中日志审计平台 [待办任务](#) [工单系统](#) [帐号口令管理系统](#) [综合维护接入平台](#)

首页 | 实时监控 | 综合查询 | 审计流程 | 审计策略 | 参数定制 | 事件响应 | 报表管理 | 知识库 | 系统管理

当前位置: 实时监控>>原始日志实时监控>>原始日志分类监控

原始日志监控

按级别监控

序号	告警级别	发生数量	查看详情
1	无害	0	查看详情
2	未知	0	查看详情
3	紧急	0	查看详情
4	致命	0	查看详情
5	警告	0	查看详情
6	轻微	0	查看详情

按系统监控

序号	系统名称	发生数量	查看详情
1	防火墙_Cisco_数维	0	查看详情
2	华为防火墙	0	查看详情
3	集团短信通	0	查看详情
4	防火墙_NetScreen	0	查看详情

按中心监控

序号	中心名称	发生数量	查看详情
1	业务支撑中心	0	查看详情
2	数维中心	0	查看详情
3	信息中心	0	查看详情
4	音乐中心	0	查看详情
5	网管中心	0	查看详情

集中审计——综合查询

中国移动通信 CHINA MOBILE 四川移动集中日志审计平台

网管中心 admin/admin 2009-07-28 13:53:03登录

重新登录 在线帮助 退出系统

待办任务 工单系统 帐号口令管理系统 综合维护接入平台

首页 | 实时监控 | 综合查询 | 审计流程 | 审计策略 | 参数定制 | 事件响应 | 报表管理 | 知识库 | 系统管理

当前位置: 综合查询>>原始日志查询

原始日志查询

查询 导出

用户名: 设备地址: 日志分类: 所属中心:

源地址: 目标地址: 日志级别: 所属系统:

事件内容: 入库时间: 2009-07-01 2009-07-28 [高级搜索](#)

序号	所属系统	级别	分类	发生时间	入库时间	事件内容	设备地址	源地址	目标地址	用户名
1	防火墙_NetScreen [数维中心]	警告	安全日志	2009-07-23 13:49:47	2009-07-23 13:38:28	icmp	211.137.84.250	211.137.84.149	130.158.6.56	
2	防火墙_NetScreen [数维中心]	警告	安全日志	2009-07-23 13:50:40	2009-07-23 13:37:44	icmp	211.137.84.250	125.71.209.90	218.205.231.65	
3	防火墙_NetScreen [数维中心]	警告	安全日志	2009-07-23 13:50:41	2009-07-23 13:37:44	icmp	211.137.84.250	125.71.209.90	218.205.231.65	
4	防火墙_NetScreen [数维中心]	警告	安全日志	2009-07-23 13:49:40	2009-07-23 13:37:36	icmp	211.137.84.250	211.137.84.149	130.158.6.56	
5	防火墙_NetScreen [数维中心]	警告	安全日志	2009-07-23 13:49:34	2009-07-23 13:36:19	icmp	211.137.84.250	211.137.84.149	130.158.6.56	
6	防火墙_NetScreen [数维中心]	警告	安全日志	2009-07-23 13:50:30	2009-07-23 13:36:09	icmp	211.137.84.250	125.71.209.90	218.205.231.65	
7	防火墙_NetScreen [数维中心]	警告	安全日志	2009-07-23 13:50:31	2009-07-23 13:36:09	icmp	211.137.84.250	125.71.209.90	218.205.231.65	
8	防火墙_NetScreen [数维中心]	警告	安全日志	2009-07-23 13:49:27	2009-07-23 13:35:26	icmp	211.137.84.250	211.137.84.149	130.158.6.56	
9	防火墙_NetScreen [数维中心]	警告	安全日志	2009-07-23 13:41:13	2009-07-23 13:34:14	icmp	211.137.84.250	211.137.84.149	130.158.6.56	
10	防火墙_NetScreen [数维中心]	警告	安全日志	2009-07-23 13:42:10	2009-07-23 13:33:54	icmp	211.137.84.250	125.71.209.90	218.205.231.65	
11	防火墙_NetScreen [数维中心]	警告	安全日志	2009-07-23 13:42:11	2009-07-23 13:33:54	icmp	211.137.84.250	125.71.209.90	218.205.231.65	
12	防火墙_NetScreen [数维中心]	警告	安全日志	2009-07-23 13:41:07	2009-07-23 13:33:13	icmp	211.137.84.250	211.137.84.149	130.158.6.56	
13	防火墙_NetScreen [数维中心]	警告	安全日志	2009-07-23 13:42:00	2009-07-23 13:32:25	icmp	211.137.84.250	125.71.209.90	218.205.231.65	
14	防火墙_NetScreen [数维中心]	警告	安全日志	2009-07-23 13:42:01	2009-07-23 13:32:25	icmp	211.137.84.250	125.71.209.90	218.205.231.65	
15	防火墙_NetScreen [数维中心]	警告	安全日志	2009-07-23 13:41:00	2009-07-23 13:32:19	icmp	211.137.84.250	211.137.84.149	130.158.6.56	

上一页 | 第 1/1575 页 | 下一页 | 共47239行 | 每页30行 | go | 转到第 1 页



集中审计——审计报表



网络操作日志审计——会话监控、查询

会话查询

设置查询条件 回放会话 新建查询 刷新 导出列表

会话 (总数: 320)

保护主机	服务	用户	系统身份	服务器IP:端口	用户IP:端口	开始时间	结束时间	审计条数	上行IP报个数	下行IP报个数	上行数据量	下行数据量
基础数据库...	Telnet	吴宗宪	edis	10.101.16.21:23	172.30.30.19:1203	2007-01-22 14:48:11		0	19	13	439	488
基础数据库...	Telnet	吴宗宪	edis	10.101.16.21:23	172.30.30.19:1210	2007-01-22 15:02:44		0	36	32	796	2093
基础数据库...	FTP	吴宗宪	edis	10.101.16.21:21	172.30.30.19:1215	2007-01-22 15:08:19	2007-01-22 15:23:49	0	114	129	3759	7638
数据仓库/e...	FTP	黄科 (pc)	informix	10.101.16.41:21	172.30.30.26:1063	2007-01-22 08:43:04	2007-01-22 08:43:24	0	12	13	338	819
三期数据库...	Telnet	曹福利	informix	10.101.16.18:23	172.30.30.1:1032	2007-01-22 08:58:58	2007-01-22 09:00:13	0	62	191	1376	124605
eoms数据库	Informix	曾涵凯	informix	10.101.16.33:...	172.30.30.44:1292	2007-01-22 09:02:34	2007-01-22 09:09:10	0	469	0	65691	0
eoms数据库	Informix	杨梅	informix	10.101.16.33:...	172.30.30.30:1115	2007-01-22 09:13:53	2007-01-22 10:18:13	0	476	0	65230	0
基础数据库...	Informix	吴宗宪	informix	10.101.16.21:...	172.30.30.39:1670	2007-01-22 09:20:33	2007-01-22 09:41:42	0	1743	0	58466	0
eoms数据库	Informix	陈世丽	informix	10.101.16.33:...	172.30.30.2:1273	2007-01-22 09:29:30	2007-01-22 09:29:47	0	10	0	964	0
eoms数据库	Informix	曾涵凯	informix	10.101.16.33:...	172.30.30.44:2432	2007-01-22 09:54:11	2007-01-22 10:14:36	0	608	0	75215	0
三期数据库	Telnet	曹福利	informix	10.101.16.17:23	172.30.30.1:1055	2007-01-22 10:07:23		0	43	51	990	2020
三期数据库	Telnet	曹福利	informix	10.101.16.17:23	172.30.30.1:1057	2007-01-22 10:19:51		0	46	55	1045	2104
eoms数据库	Informix	陈世丽	informix	10.101.16.33:...	172.30.30.2:1347	2007-01-22 10:32:23	2007-01-22 11:00:17	0	36	0	2614	0
eoms数据库	Informix	吴维薇	informix	10.101.16.33:...	172.30.30.7:2084	2007-01-22 10:39:20	2007-01-22 10:41:11	0	220	0	35333	0
三期数据库	Telnet	曹福利	informix	10.101.16.17:23	172.30.30.1:1139	2007-01-22 10:46:19	2007-01-22 11:03:47	0	184	196	3957	7192
三期数据库	Telnet	曹福利	informix	10.101.16.17:23	172.30.30.1:1149	2007-01-22 11:06:00	2007-01-22 11:28:33	0	52	60	1170	1583
三期数据库	Telnet	曹福利	informix	10.101.16.17:23	172.30.30.1:1388	2007-01-22 11:49:27		1	22	43	540	10204

快速浏览 审计信息

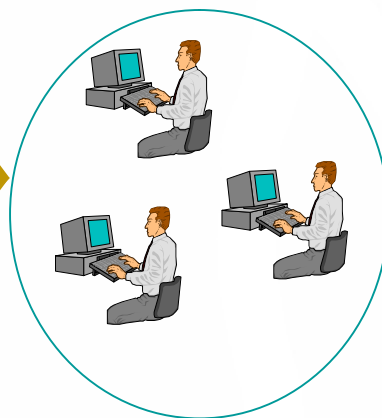
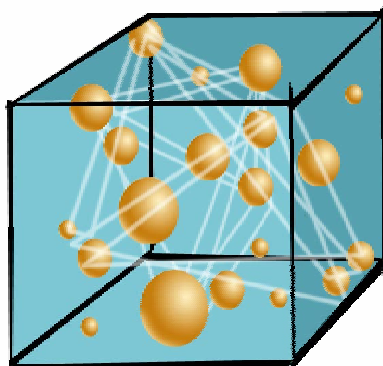
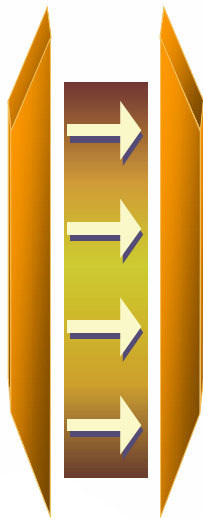
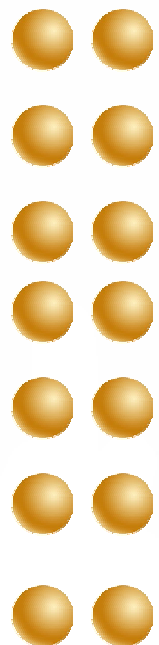
显示下行数据 (服务器-客户) 查询中... (数量: 0)

查看内容

查找 导出

方向	时间	响应时间	命令结果大小	命令	语意
↓	2007-01-22 08:58...			# \$#\$	
↓				sunOS 5.8	
↑	2007-01-22 08:58...		0Byte	login: informix	
↑	2007-01-22 08:58...		0Byte	Password:	
↓	2007-01-22 08:58...			Last login: Mon Jan 22 09:00:56 from sc3db1	
↓				Sun Microsystems Inc. SunOS 5.8 Generic Patch October 2001	
↓				You have new mail.	
↓	2007-01-22 08:58...			错误字符串	
↑	2007-01-22 08:59...		0Byte	sc3db2% dmesg	
↓				2007年01月22日 星期一 09时01分56秒 CST	
↓	2007-01-22 08:59...			Jan 19 20:50:07 sc3db2 MQSeries: [ID 483849 user.error] FFST record created in /var/mq...	
↓				Jan 19 20:50:08 sc3db2 MQSeries: [ID 483849 user.error] FFST record created in /var/mq...	
↓				Jan 19 20:50:08 sc3db2 MQSeries: [ID 483849 user.error] FFST record created in /var/mq...	

事件关联分析



事件
日志



日志
过滤



日志
关联



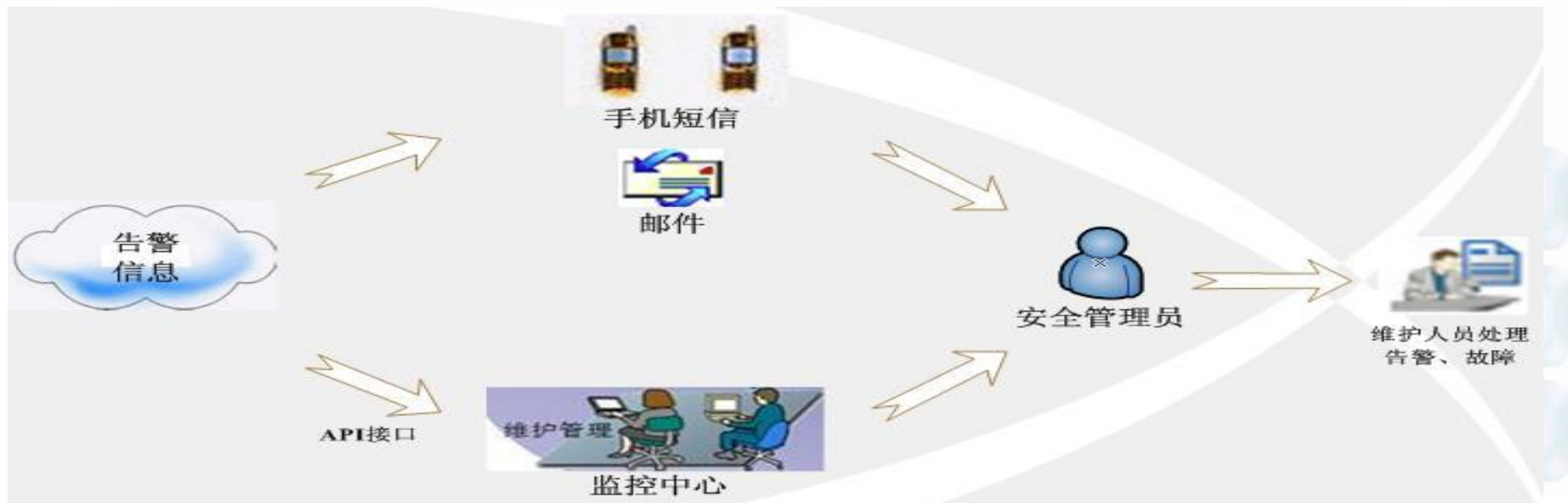
事件
定位



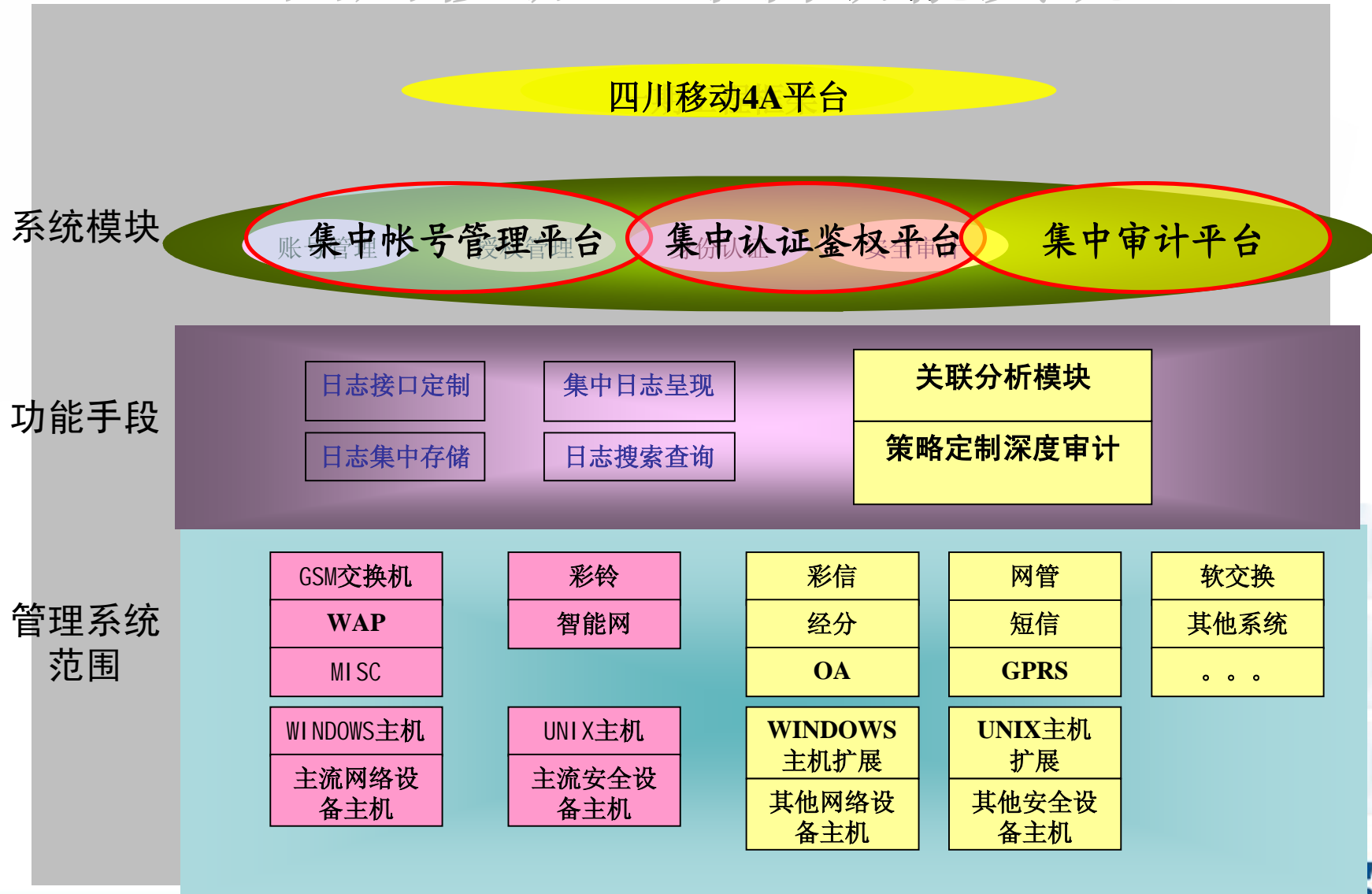
事件
响应

事件响应

- Ø支持紧急事件定义，记录紧急事件，发生紧急事件时能够报警
- Ø基于非法源地址、非法客户应用、非法数据库用户名、非法数据库对象访问、非法操作类型、非法SQL语句和非法时间进行报警。
- Ø支持Email、短信等报警方式。
- Ø允许用户选择配合交换机、防火墙等网络设备或者独立对来自非法源地址的操作进行阻断的能力。



四川移动4A平台功能实现



धन्यवाद

HindHindi

多謝

Traditional Chinese

ขอบคุณ

Thai

Спасибо

Russian

Gracias

Spanish

شكراً

Arabic

Thank

English

You

多谢

Simplified Chinese

Obrigado

Brazilian Portuguese

Grazie

Italian

Danke

German

Merci

French

நன்றி

Tami Tamil

ありがとうございました

Japanese

감사합니다

Korean