Security Level:

华为医院信息防泄漏解决方案

Author/ Email: Author's name/Author's email

Version: V1.0(20YYMMDD)

HUAWEI TECHNOLOGIES CO., LTD.

HUAWEI

目　　录

- 医院核心业务数据安全现状和挑战
- 华为医院信息防泄漏解决方案
- 华为医院信息防泄漏应用场景及案例

医院信息泄露事件案例

三〇一医院“统方”事件

三〇一医院的处方信息被统计后提供给医药代表，而后医药代表按照处方开具药品数量为响应的医师提供回扣。

江西南昌“恶意篡改”事件

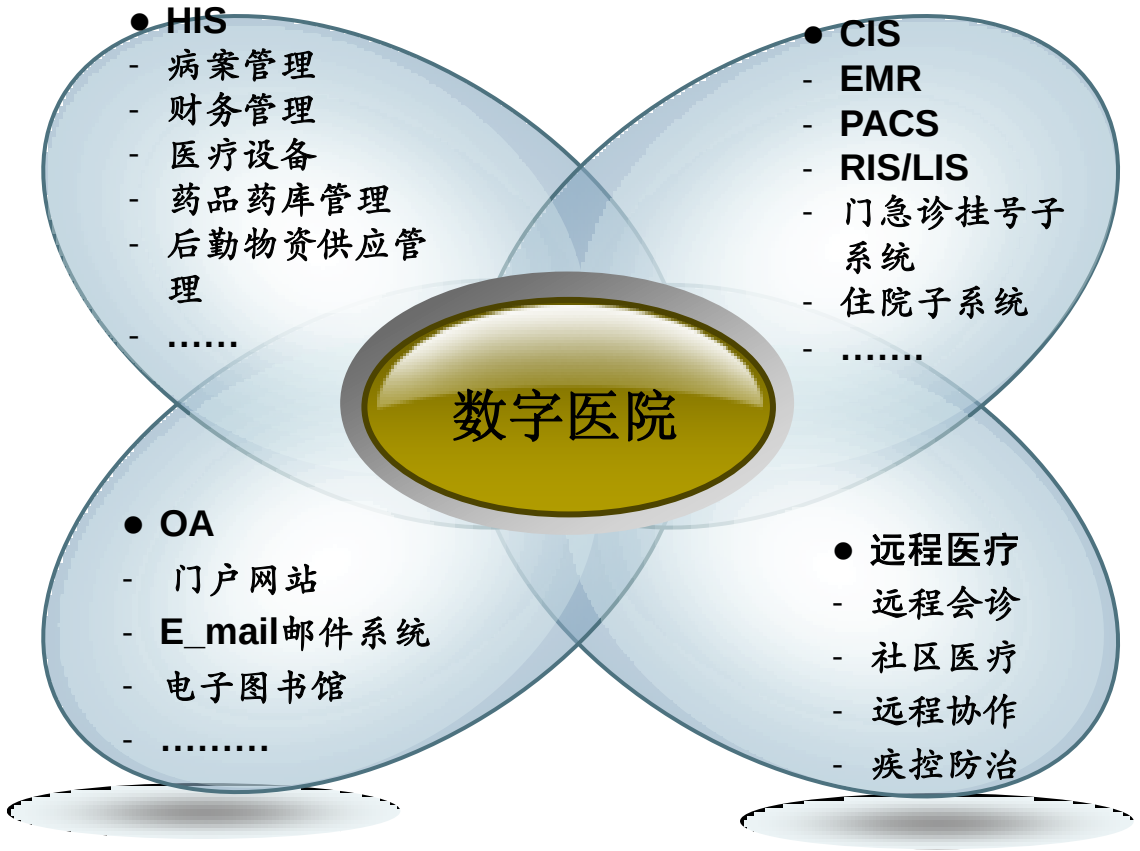
江西南昌某医院的一个科室医生因与院信息中心有矛盾，在网吧通过非法手段登入医院计费HIS系统，蓄意删除数据。

江西南昌某医院 一个病人登入计费系统数据库更改个人消费记录，出院时账单反映不仅无需支付费用，反而医院还欠该人一笔费用。

某某医院“病人资料外泄”事件

某高龄老人在该医院做了髋关节置换手术，几年后的一天，老人接到该医院复查通知，医院派车接送，结果把老人接到一小区，强制要求老人高价购买保健品，最后老人交完身上所有现还打上2000多块钱的欠条后才得以脱身。病人资料泄露，造成老人受骗，给病人带来了损失，同时也极大的影响了医院的声誉。

医院信息系统现状及面临的挑战



一方面由于没有有效的监控和管理手段，致使一部分人在利益面前存在侥幸心理。
另一方面因为没有足够的证据，使得监管部门的治理、惩罚工作举步维艰。

医护人员、软件提供商、医药代表、数据维护人员

1. 如何保护患者隐私信息安全？
2. 如何防止非法统方和统方信息外泄？
3. 恶意篡改信息系统数据
4. 非法删除日志、掩盖非法操作
5. 规范IT管理流程，建立审计追踪机制

非法手段

病人信息、业务数据、统计报表、核心机密

医院面临的信息安全挑战

卫生部《关于进一步深化治理医药购销领域商业贿赂工作的通知》，要求医院加强医院信息系统药品、高值耗材统计功能管理，**严禁为商业目的统方，**建立医药购销领域商业贿赂不良记录，坚决打击商业贿赂行贿行为。


中央纪委驻卫生部纪检组
监察部驻卫生部监察局
MINISTRY OF HEALTH OF THE PEOPLE'S REPUBLIC OF CHINA

主站首页 | 本站首页 | 机构职能 | 政策法规 | 规划计划 | 行政许可 | 卫生标准 | 卫生统计 | 通告公告 | 工作动态 | 征求意见

当前位置： 首页 > 最新信息 > 行风建设 > 动态　站内搜索　请输入关键字　搜索

浏览字体：【大、中、小】　打印页面　关闭页面

卫生部关于进一步深化治理医药购销领域商业贿赂工作的通知

中华人民共和国卫生部　www.moh.gov.cn　2010-06-30 15:40:45

卫办发[2010]59号

各省、自治区、直辖市卫生厅局，新疆生产建设兵团卫生局，部直属各单位，部机关各司局：

自2006年以来，全国卫生系统按照中央统一部署，加强组织领导，采取有效措施，整体推进宣传教育、自查自纠、查办案件和长效机制建设，治理医药购销领域商业贿赂专项工作取得了阶段性明显成效，卫生系统广大干部职工的法制纪律观念、廉洁从业意识明显增强，医药购销秩序得

卫生部发布《电子病历系统功能规范（试行）》，要求医院对电子病历电子病历设置保密等级，对电子病历的使用做到**权限范围控制和审计**，以保护**患者隐私**。


MINISTRY OF HEALTH OF THE PEOPLE'S REPUBLIC OF CHINA

主站首页 | 本站首页 | 机构职能 | 政策法规 | 规划计划 | 行政许可 | 卫生标准 | 卫生统计 | 通告公告 | 工作动态

当前位置： 首页 > 最新信息 > 医疗质量评价管理 > 政策　站内搜索　请输入关键字　搜索

浏览字体：【大、中、小】　打印页面　关闭页面

卫生部关于印发《电子病历系统功能规范（试行）》的通知

中华人民共和国卫生部　www.moh.gov.cn　2011-01-04 09:13:22

卫医政发〔2010〕114号

各省、自治区、直辖市卫生厅局，新疆生产建设兵团卫生局：

按照深化医药卫生体制改革有关工作安排，为规范医疗机构电子病历管理，明确医疗机构电子病历系统应当具有的功能，更好地发挥电子病历在医疗工作中的支持作用，促进以电子病历为核心的医院信息化建设工作，我部组织制定了《电子病历系统功能规范（试行）》。现印发给你们，请遵照执行。

目　　录

- 医院核心业务数据安全现状和挑战
- 华为医院信息防泄漏解决方案
  - 总体方案设计
  - 医院业务数据防护方案
  - 医院终端控制解决方案
  - 医院安全管控中心方案
- 华为医院信息防泄漏应用场景及案例

华为医院信息防泄密设计思路

Who（谁会接触和使用）

- 医务人员
- 软件提供商
- 数据维护人员
- IT外包服务人员
- 医药代表

（Where）数据放在那里

- 数据库服务器
- 文件服务器
- 终端电脑

Way(机密信息泄漏途径)

- 医务人员非授权访问、统计
- 数据维护人员非法拷贝、统计
- 外来终端非法接入，窃取数据
- 软件提供商、外包服务人员利用服务之便，窃取数据
- 内部人员的误操作、滥操作、恶意行为。

（What）什么是机密数据

- 电子病历，患者隐私信息
- 药品统方数据
- 医院财务数据
- 科研成果

How（如何防范）

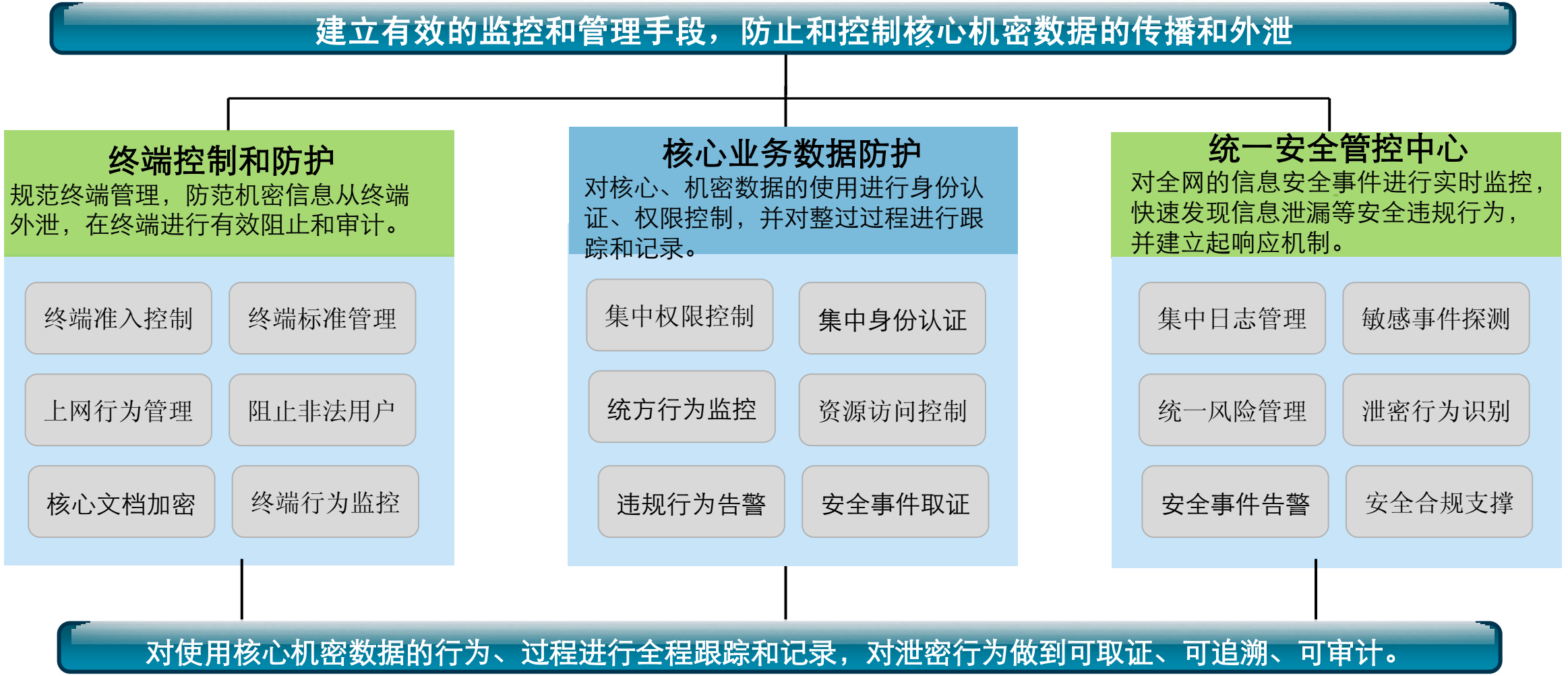
- 对重要、机密数据的访问进行授权，并对使用过程进行全程监控和记录，
- 对医院重要文件进行加密存储。
- 对终端进行规范管理，建立准入机制，防止移动拷贝、打印、外发。
- 建立安全管控中心，监控和分析网络中各种行为，对泄密行为实时告警。

4W+H What->Where->Who->Way->How

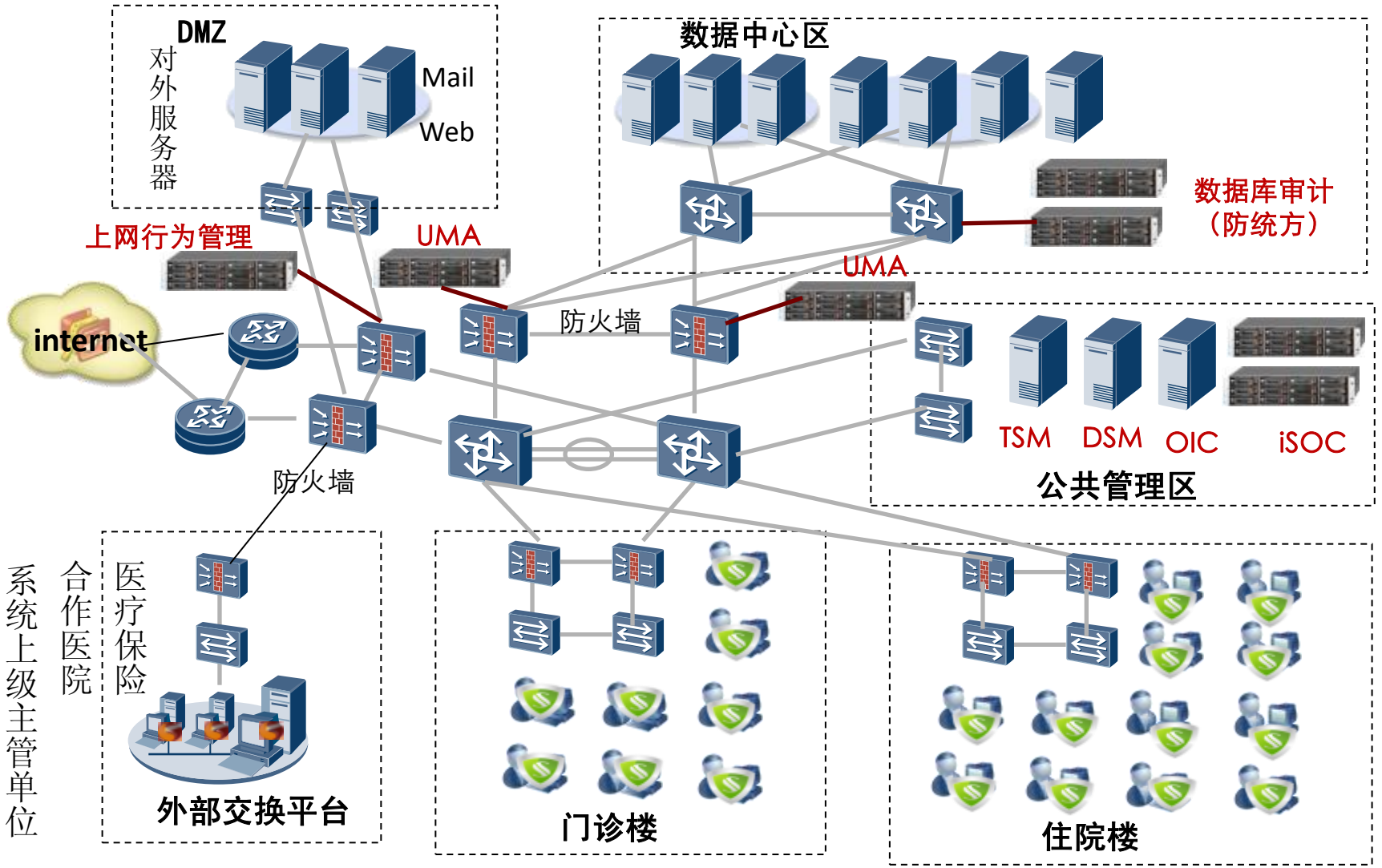
医院防泄密关键点

- 终端准入控制、规范管理
- 核心数据使用授权、监控
- 重要文件进行加密保存
- 员工上网行为监控和管理
- 建立监控和审计机制，追溯跟踪泄密行为

华为医院防泄密解决方案框架



华为医院防泄密方案整体部署图



➢终端泄密控制和防护、规范终端管理，防范机密信息从终端外泄，在终端进行有效阻止和审计。

- 终端管理系统TSM
- 文档管理系统DSM/OIC
- 上网行为管理ASG

➢核心业务系统、数据管理，对核心、机密数据的使用进行身份认证、权限控制，并对整过过程进行跟踪和记录。

- 统一运维审计UMA
- 数据库审计（防统方）

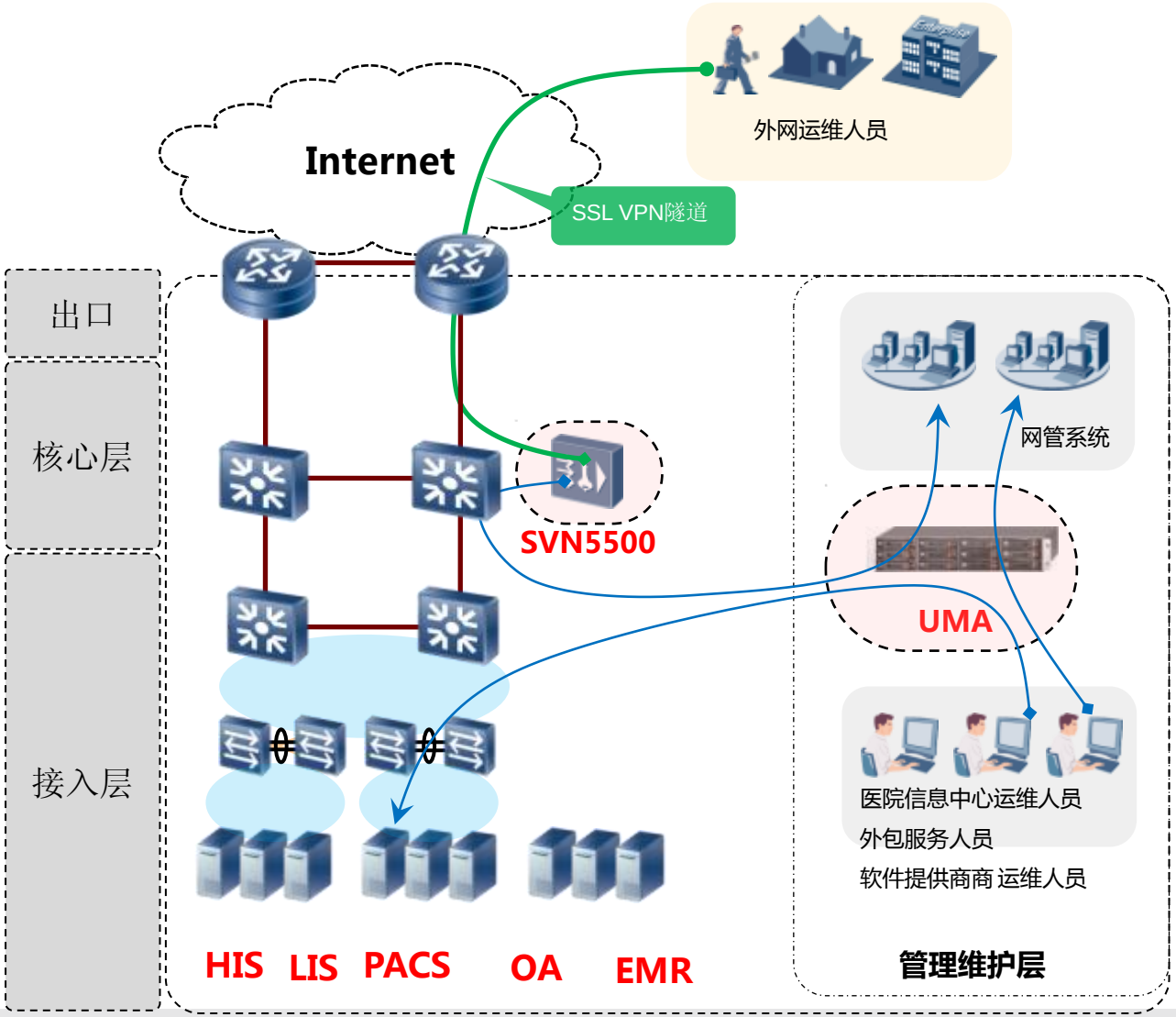
➢安全管理中心，对全网的信息安全事件进行实时监控，快速发现信息泄漏等安全违规行为，并建立起响应机制。

- 安全管控中心iSOC

目　　录

- 医院核心业务数据安全现状和挑战
- 华为医院信息防泄漏解决方案
  - 总体方案设计
  - 医院业务数据防护方案
  - 医院终端控制解决方案
  - 医院安全管控中心方案
- 华为医院信息防泄漏应用场景及案例

医院综合运维审计解决方案



安全需求

✓在医院信息中心建立运维统一接入、认证、授权和审计

✓对核心业务数据的运维可管理、可追踪

✓对医院信息安全事件可审计

华为UMA统一运维方案

✓UMA统一运维审计系统，运维人员进行单点登录、操作审计

✓外网运维人员通过SSL VPN隧道安全接入内网，登录UMA系统.

方案价值和优势

✓规范医院运维管理、降低机密信息风险、完善责任认定、满足合规要求。

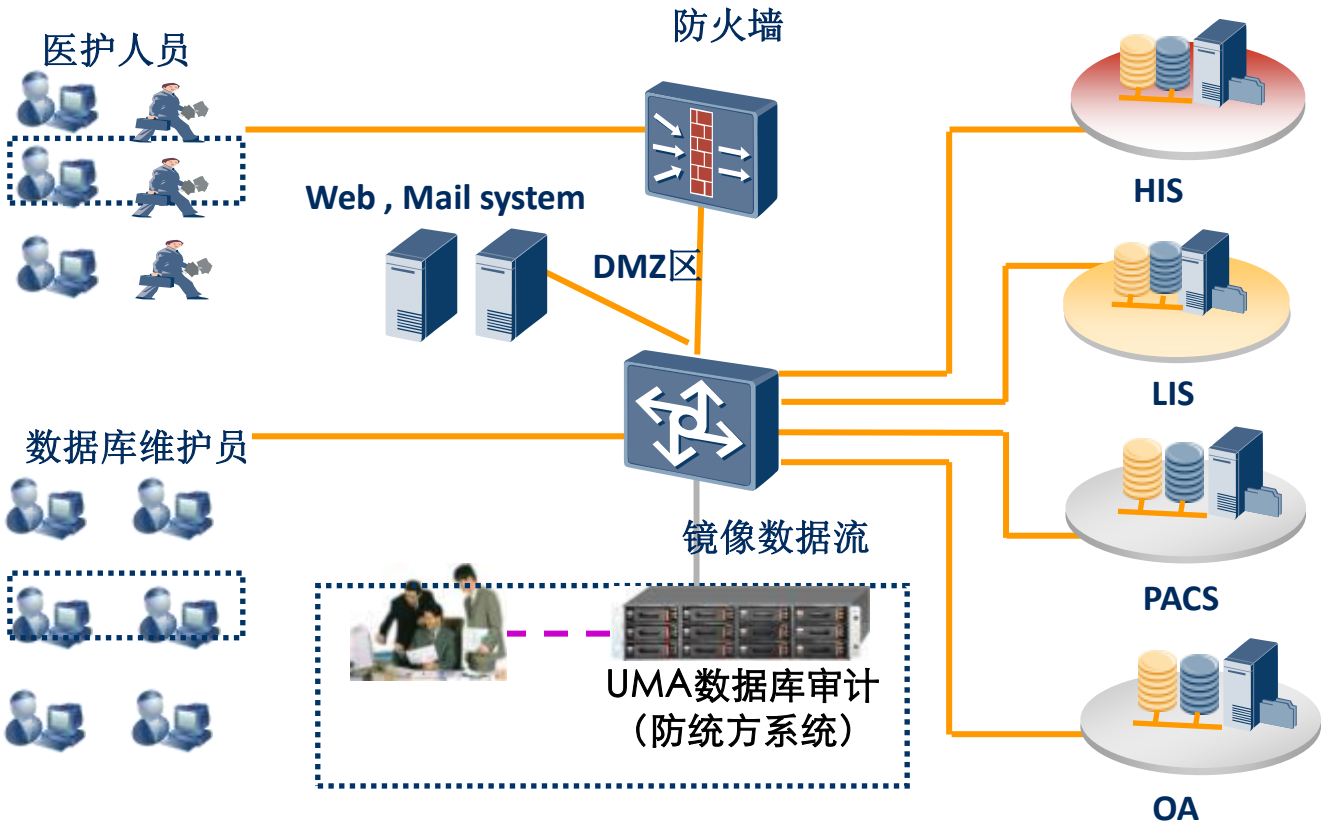
✓为医院业务系统提供统一维护操作入口，实现单点登录。

✓记录所有对医疗系统运维操作过程，快速故障定位和责任追踪。

✓实现了自然人与设备帐号之间的一 一对应，并提供定期密码修改功能；

✓为不同用户分配不同的权限，实现命令级的控制，确保合法用户对资源的操作，杜绝越权访问。

医院数据库审计解决方案（防统方）



安全需求

✓医院业务数据的泄漏和篡改。

✓防范统方事件。

✓数据库访问状态的监控和策略告警。

华为数据库安全审计方案

✓华为数据库审计系统通过旁路侦听的方式对医院各系统数据的访问和操作数据流进行采集、分析和识别。

✓实时监视统方、非法数据访问等违规行为，监控异常访问操作。

方案价值和优势

✓提高医院数据库安全可用性，降低数据风险、提供实时告警。

✓记录和还原所有对核心业务数据的访问和操作过程，并长期保存。

✓可视化定义各种安全策略，实时告警违规行为。

✓绑定变量支持，有效关联应用账号同数据库系统账号，精确审计到人。

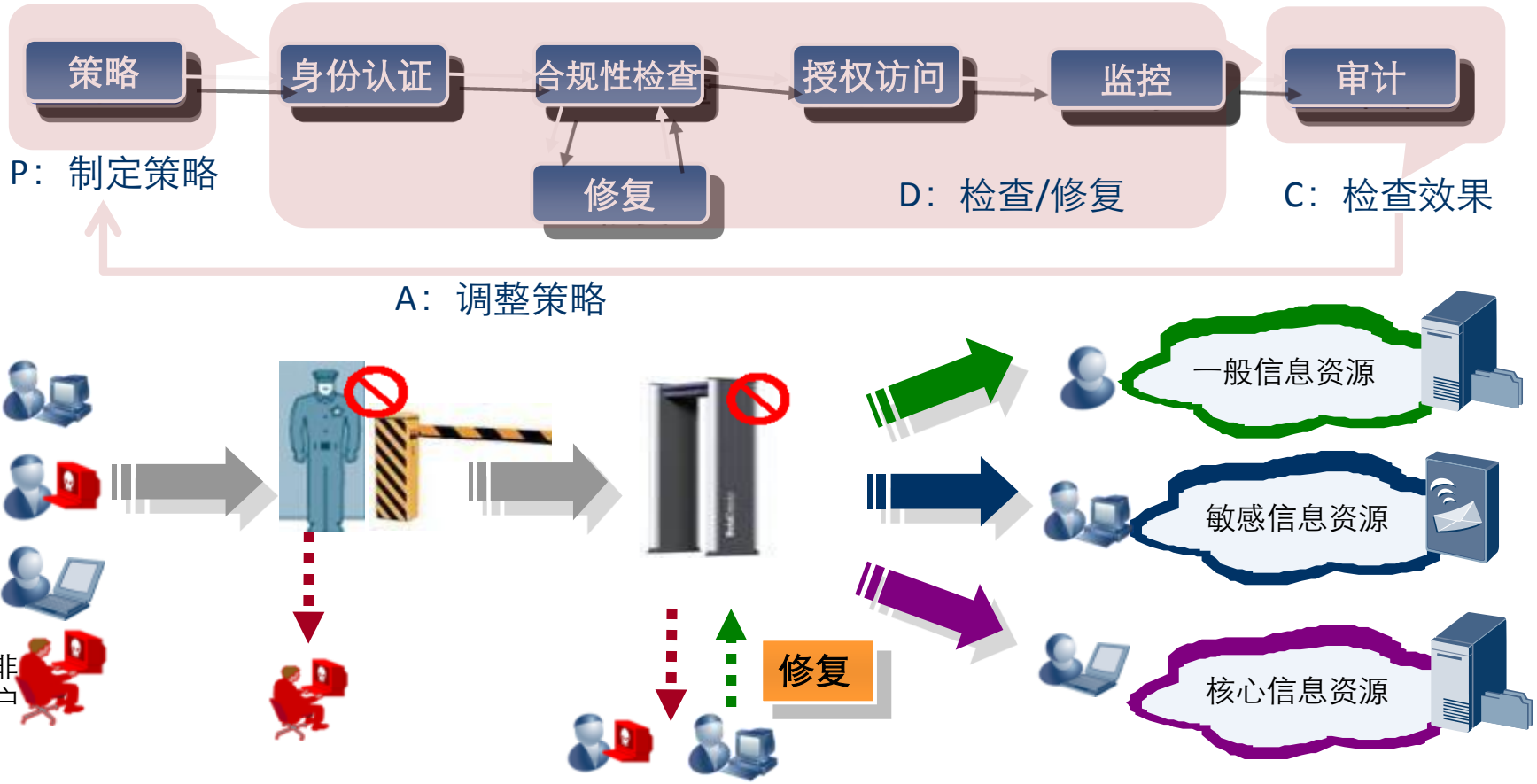
✓提供会话级审计日志，长SQL语句解析，操作返回值解析，原始pcap包捕获。

✓提供直观的视图实时监控数据库的各项使用状态，不安装服务端引擎。

目　　录

- 医院核心业务数据安全现状和挑战
- 华为医院信息防泄漏解决方案
  - 总体方案设计
  - 医院业务数据防护方案
  - 医院终端控制解决方案
  - 医院安全管控中心方案
- 华为医院信息防泄漏应用场景及案例

医院终端安全管理方案



三大功能模块全面保障办公终端的安全

准入控制

- 访客管理
- 设备管理
- 网络访问权限控制
- 身份认证
- 合规性检查
- 一键式自动修复
- 基于时间段的NAC

安全管理

- 安全加固
- 办公行为管理
- 自定义各种安全策略
- 信息泄密防护
- 网络防护
- 策略自适应

桌面管理

- 补丁管理
- 资产管理
- 软件分发
- 远程协助
- 消息工号

医院文档安全管理方案

多种数据来源

在线/离线安全管控

全生命周期审计

三大功能模块实现文档集中安全管理

- **集中管理，避免信息流失**
  - 多业务多来源信息数据集中存管
  - 汇集信息便于查阅检索
- **安全管理，保证信息安全**
  - 统一设置数据安全级别
  - 查阅、加密、打印、追踪等不同管控手段
- **增值服务，便捷共享，提升信息价值**
  - 个人空间存储服务
  - 多格式在线编辑和播放

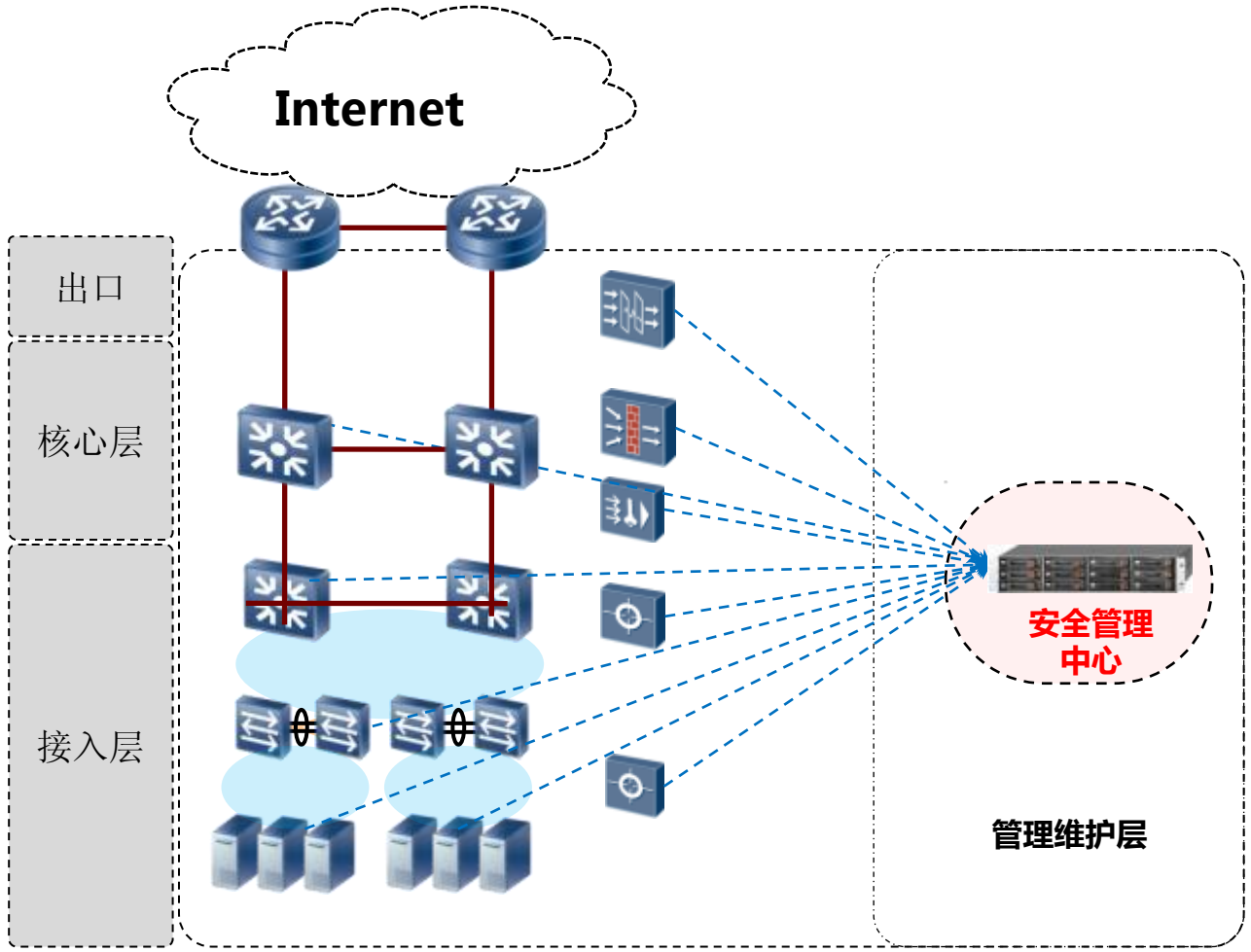
建立信息中心，提供加密、审计等管控手段，协助用户安全管控信息资产

医院上网行为管理解决方案

目　　录

- 医院核心业务数据安全现状和挑战
- 华为医院信息防泄漏解决方案
  - 总体方案设计
  - 医院业务数据防护方案
  - 医院终端控制解决方案
  - 医院安全管控中心方案
- 华为医院信息防泄漏成功案例

医院安全管理中心解决方案



安全需求

✓医院整网安全监控、告警，事后追溯

✓医院安全事件关联分析、高效运维

华为医院安全管理中心方案

✓i统一安全管控中心，对整网设备及业务系统信息进行采集、关联分析、告警呈现；针对可能发生的医院信息泄漏事件及其他对医院影响较大的安全事件，通过iSOC能够及时发现、定位、告警以及事后审计。

方案价值和优势

✓及时发现统方事件、信息泄密事件和所有其他安全事件。

✓定位泄密事件的发生源、时间、人员及其影响范围。

✓对于重要事件及时报警通知管理员采取措施

✓医院所有安全事件可以被审计、分析、评、追溯，并生成分析报表。

目　　录

- 医院核心业务数据面临的挑战
- 华为医院信息防泄漏解决方案
- 华为医院信息防泄漏成功案例

上海闸北卫生局案例

- **客户挑战：**

  上海市闸北卫生局及下属各医院、医疗机构，已经建立起完善的VPN网络，实现了卫生局及下属医疗机构的高效互联；通过防火墙（UTM）实现了对外部接入的安全防控。但是，来自内部运维人员对核心业务系统如HIS系统的维护和使用没有进行有效的监管、控制和审计，常常导致病人信息、医院核心数据被外泄，给病人和医院都带来严重的影响。

- **华为方案：**

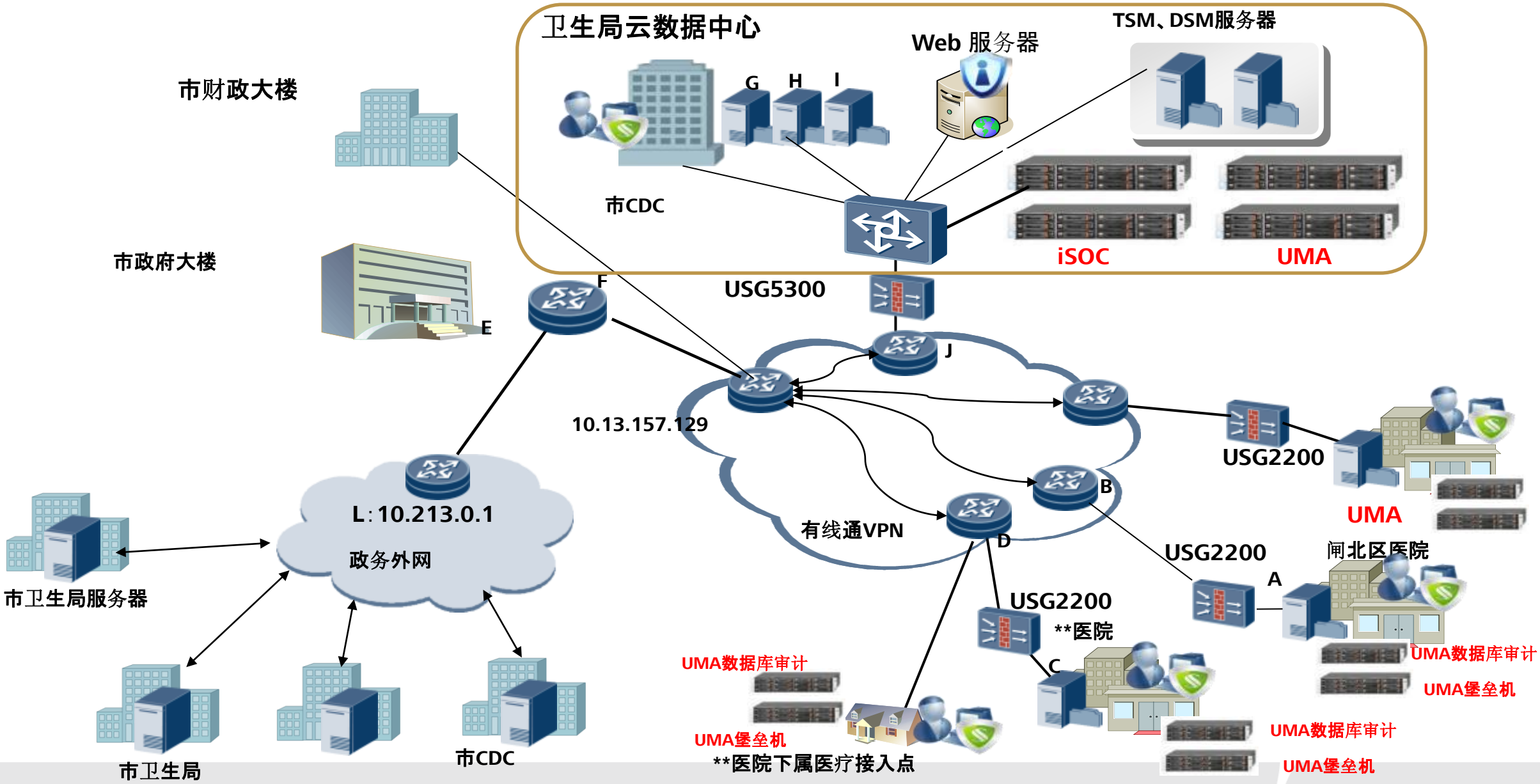
  在市卫生局云数据中心部署一套统一安全管控中心iSOC，对市卫生局和下属医疗机构的IT设备和业务系统日志进行集中采集、分类存储和关联分析，从海量安全事件中产生精确告警、定位安全问题；在上海市闸北卫生局及下属18家医院各部署一套UMA堡垒主机，对医院核心业务系统的运维和访问进行监管和审计；同时在各家医院部署一套UMA数据库审计系统，对HIS系统数据进行监控和审计，有效防范统方事件、病人信息泄露、恶意篡改数据等安全事件。

- **客户收益**

  建立了统一运维接入与审计平台，提高系统运维管理水平，满足相关法规标准要求，降低运维风险，实现了医院业务操作的规范化管理，有效的解决了医院核心业务违规操作、数据外泄问题；建立了统一安全管控中心，对上海市闸北卫生局云数据中心及下属医疗机构的IT设备及应用的日志进行集中管理和分析，实现了安全的可视化和集中化管理。

Page 20

上海闸北卫生局信息防泄漏解决方案



广西壮族自治区人民医院终端安全

广西壮族自治区人民医院
THE PEOPLE'S HOSPITAL OF GUANGXI ZHUANG AUTONOMOUS REGION

面临的挑战

在当前复杂的网络环境下，保证终端用户的安全接入，对医院中心网络各大核心业务的访问权限提供有效控制，同时提供丰富而详细用户行为审计，约束终端用户行为，实现对所有员工办公电脑的软件标准化管理，防病毒系统的统一安装和及时更新，加强安全管理，提高终端维护水平。

解决方案

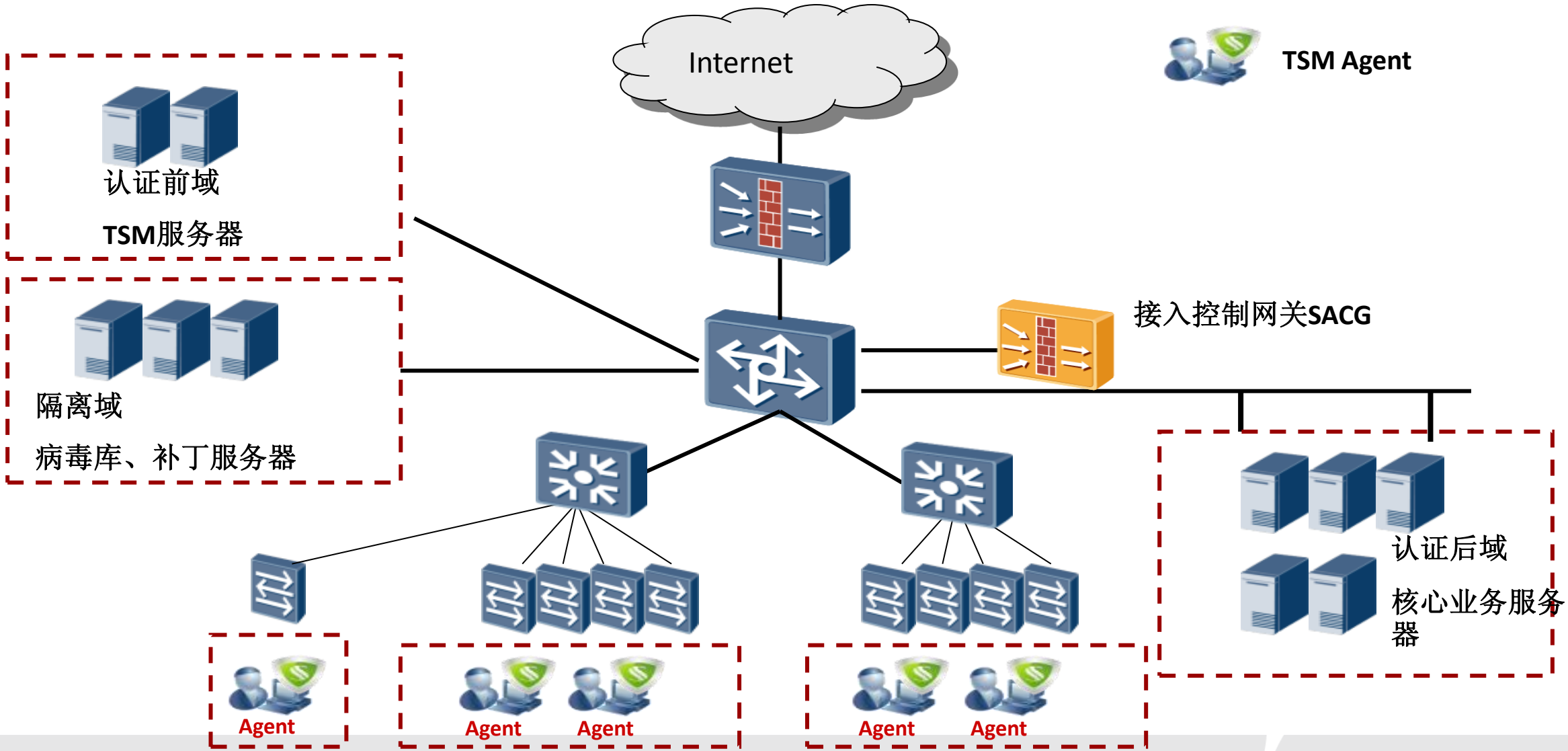
此次信息化安全建设是从内网安全管理入手，加强对内网的安全管控能力。

本期规划采用Secospace TSM终端安全管理系统实现一体化内网安全解决方案，在广西壮族自治区人民医院内部部署500个点的终端安全管理授权（包含中心机房集中管理的服务器），建立基于用户角色的细粒度访问控制，使访问人员安全接入企业网络，保证终端安全受控，将威胁屏蔽在网络之外，并为企业构建一个完整、简单和易于管理的终端安全环境。通过在核心交换机出侧挂一台安全接入控制网关（SACG），作为整个内网控制的要塞。Secospace TSM能通过六个方面的功能对内网系统进行有效管理：安全接入控制、用户行为管理、安全策略管理、资产管理、软件分发、补丁管理。

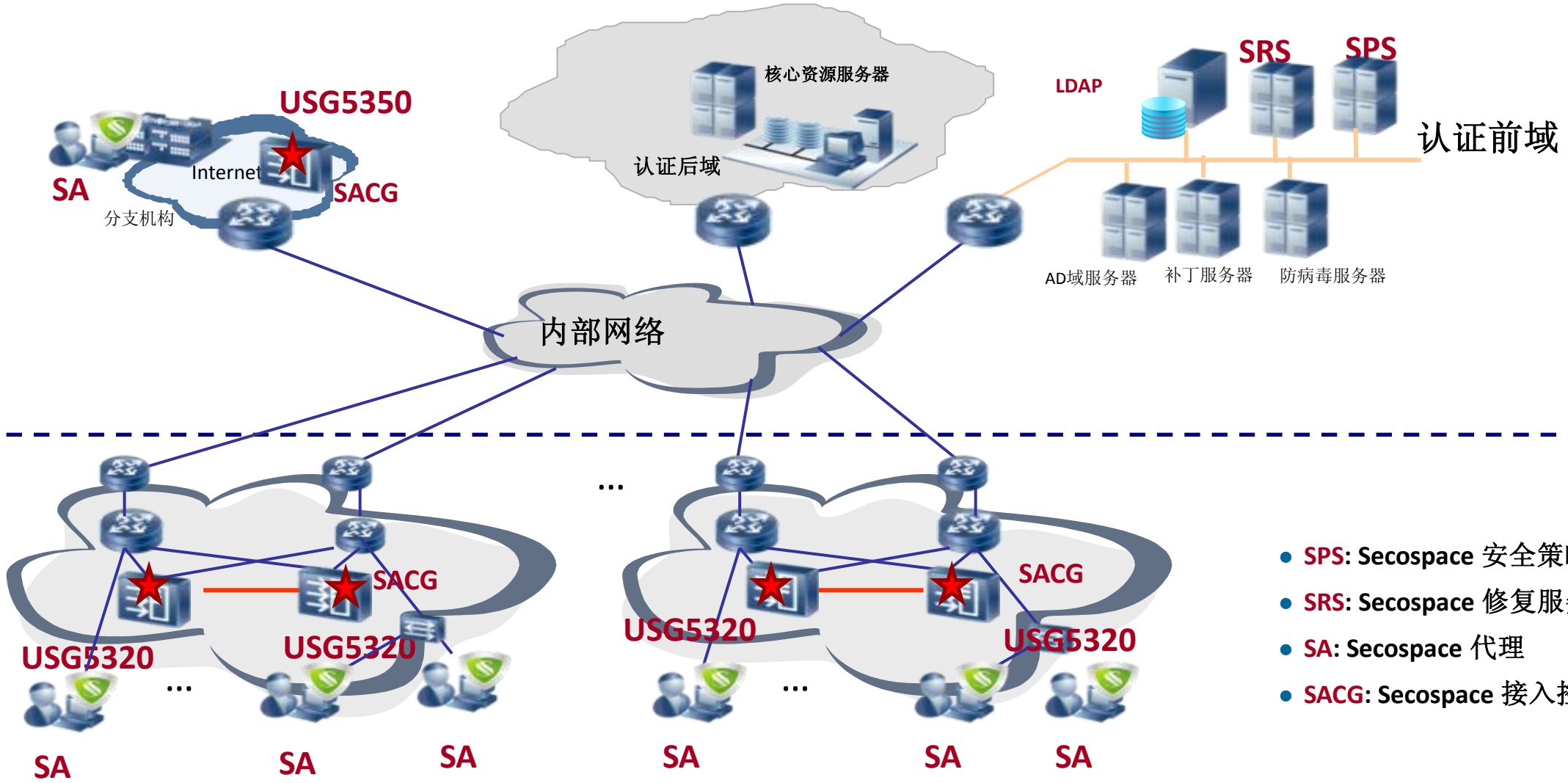
客户价值

完全解决客户面临的内网安全所有问题，为广西壮族自治区人民医院建立一个一体化、完整的终端安全管理体系，同时还保证了整个网络的稳定性和安全性。

广西壮族自治区人民医院终端安全解决方案



新疆医学院第一附属医院TSM+DSM项目



- SPS: Secospace 安全策略服务器
- SRS: Secospace 修复服务器
- SA: Secospace 代理
- SACG: Secospace 接入控制网关

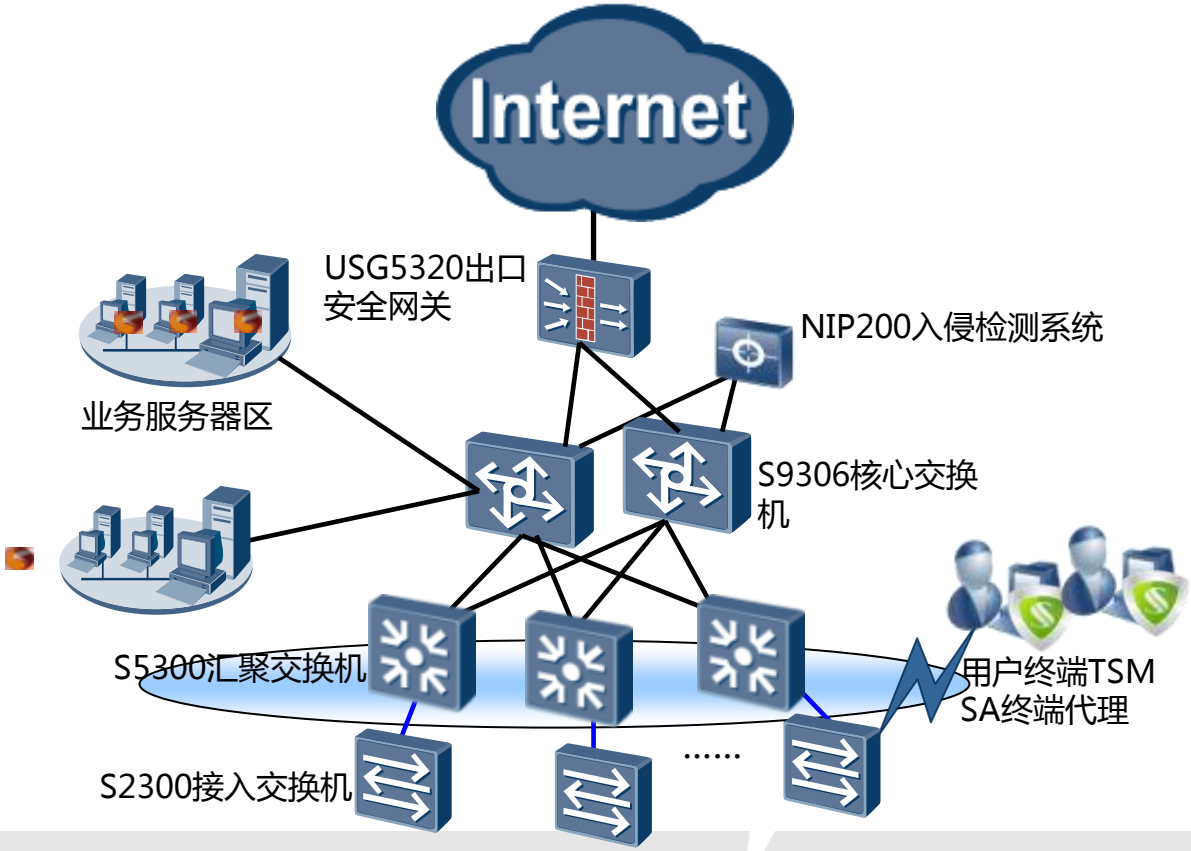
华为助力南方医科大学附属三院全院信息化建设

- 项目背景
  - 医院新建大楼成为业务整型的数据中心，由于就诊量巨大，业务规划的规模更大，需要考虑后期的业务增长以及网络的可扩展性，同时新楼和老楼的安全性和互通性需要得到保证。另外,日益增长的业务数据量需要医院建立完善的数据平台,以保证医院老楼业务和新大楼业务的连续和可靠.

客户价值

- 华为公司全网网络、安全、存储等一揽子解决方案方便的将采用先进的电子信息技术融合在医院的现网中，在提高生产力创造条件的同时，充分满足南医三院对医疗信息化的迫切需求。

南方医科大学第三附属医院
The Third Affiliated Hospital of Southern Medical University



中山中医院全网安全防护方案

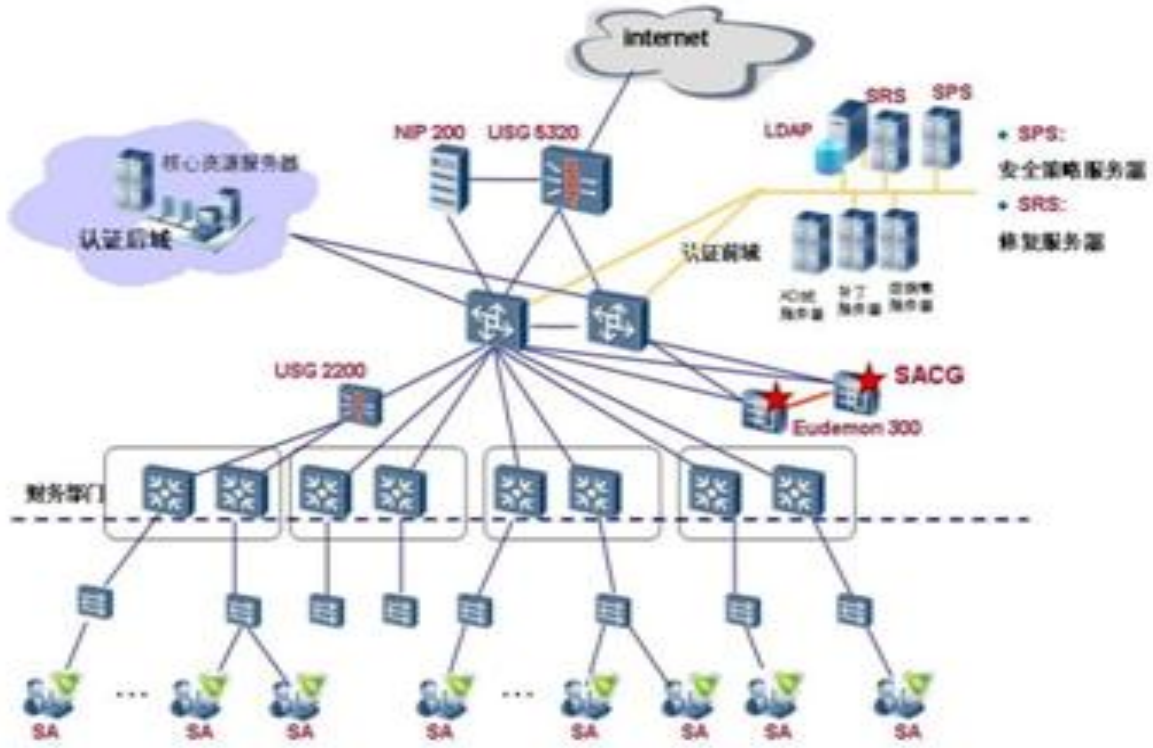
项目背景

- 对于内网来说园区内部的非法入侵访问和病例等机密信息泄露威胁到医院的内部的网络安全。另外，忽略管理,安全漏洞视而不见,资产设备缺乏有效管理，控制薄弱，不能有效的接入控制，对于医院来说，网络安全建设迫在眉睫。

客户价值

- 全面的防护体系保证中山中医院的网络安全，在不改变用户体验的同时，实现了在医院的一个网络物理平台上，承载多个系统业务，结合华为的USG系列防火墙，并考虑到网络可扩展、维护等方面的问题，实现了安全隔离与互访的动态需求。

中山市中医院
广州中医药大学附属中山医院
HOSPITAL OF TRADITIONAL CHINESE MEDICINE OF ZHONGSHAN



更多医疗行业用户名单

四川卫生厅新农合
河北省医科大学第一医院
江苏淮安第二人民医院
四川石油总医院
宁波姜山医院存储容灾系统
望京医院
新疆医科大学第一附属医院
浙江德清人民医院
诸城市人民医院
云南省第三人民医院
黑龙江省卫生统计网络直报平台及数据中心
广州市红十字会医院
广医附属羊城医院
广州中山大学附属六院
暨南大学附属第一医院

深圳市卫生局数据中心
深圳市医学信息中心
深圳市第四人民医院
深圳市蛇口人民医院
深圳市第三人民医院
深圳市恒生医院
深圳市龙岗人民医院
东莞市企石医院
东莞市凤岗医院
东莞市妇幼保健医院
东莞市万江医院
中山中医院

谢谢！

www.huawei.com