移动互联网下的医疗信息安全

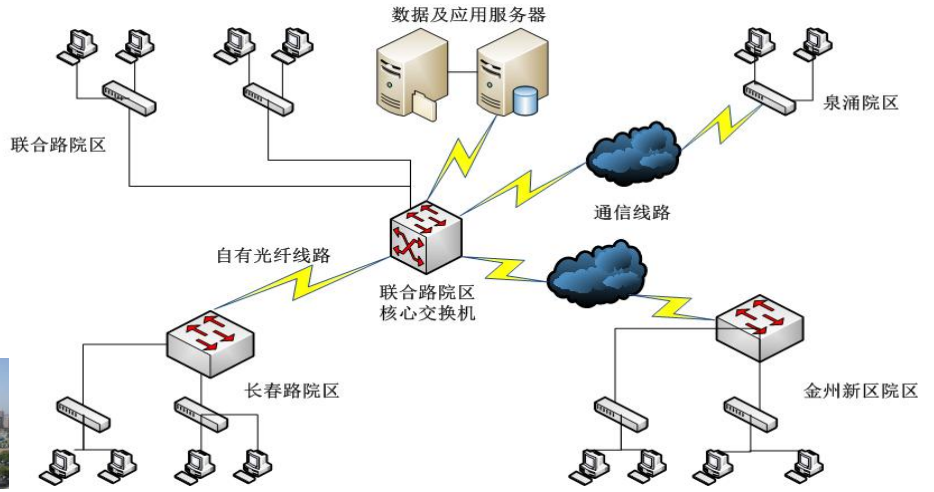
大医一院网络安全设计方案介绍

大连医科大学附属第一医院 牛铁

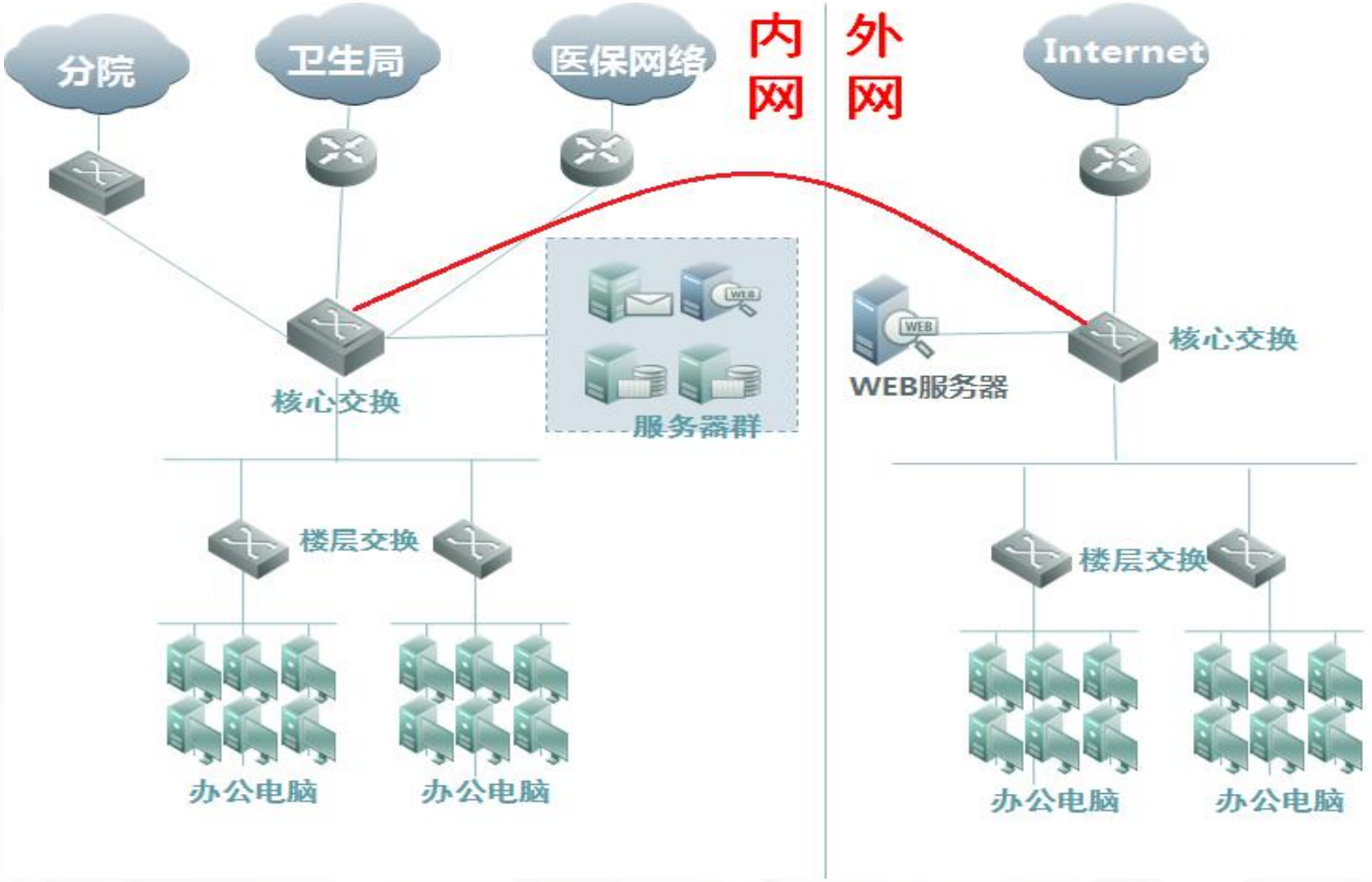
大連醫科大學附屬第一醫院
THE FIRST AFFILIATED HOSPITAL OF DALIAN MEDICAL UNIVERSITY

大医一院网络架构概况

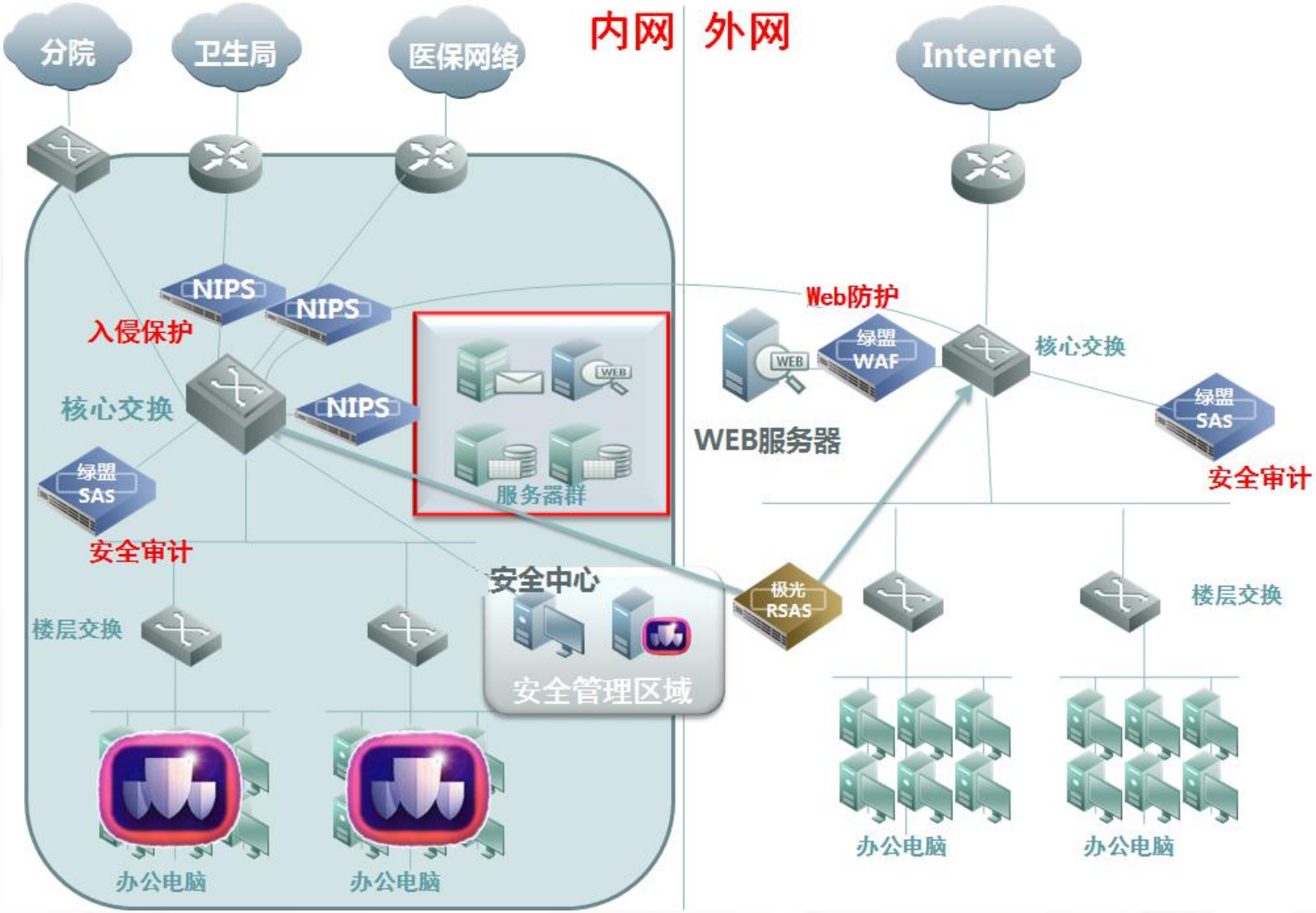
医院现共有4个院区，分别是长春路院区、联合路院区、金州新区院区、泉涌院区。院区间通过独自铺设光纤和租用通信线路连接，避免服务器硬件重复投入，医院数据统一存储管理，四个院区数据高度共享。各院区核心网络交换机采用高端设备，制定网络设备单点故障点的备份解决方案。



无安全机制的内外网互联



WEB防护和安全审计

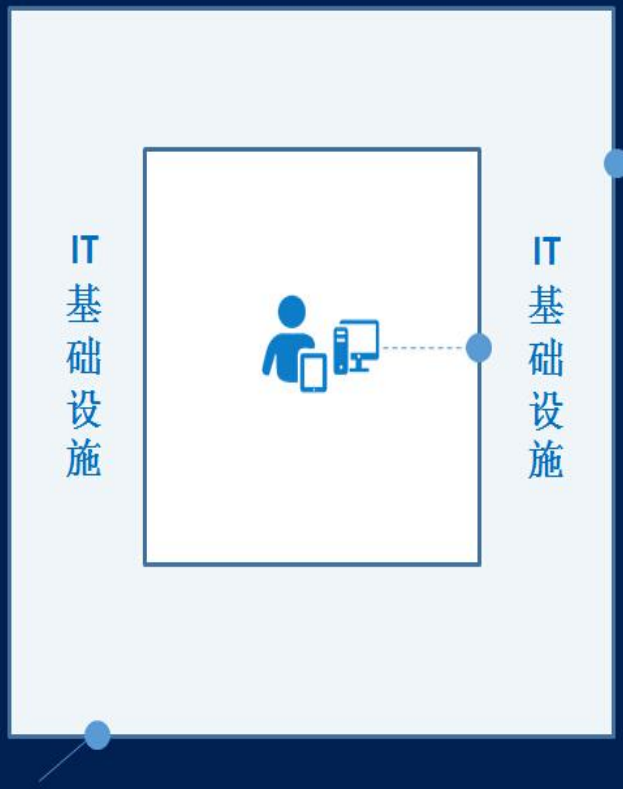

分院
卫生局
医保网络
内网
外网
Internet
NIPS
NIPS
入侵保护
核心交换
NIPS
绿盟
SAS
安全审计
服务器群
Web防护
WEB
绿盟
WAF
核心交换
WEB服务器
绿盟
SAS
安全审计
安全中心
极光
RSAS
楼层交换
楼层交换
安全管理区域
办公电脑
办公电脑
办公电脑
办公电脑

WAF

Web应用监测平台

防火墙

网络边界和边界安全



- 网络边界
  - 互联网与医院内网之间
  - 医院内网各安全域之间
  - 合作医疗、远程用户、终端

  ……
- 边界安全
  - 域间隔离（Tust/Untrust/DMZ）
  - 访问控制（Policy/ACL）
  - 威胁检测（IPS/AV/DDoS）

  ……

防火墙

迅速失控的网络边界

- 海量应用成为威胁载体
  - 木马蠕虫
  - 间谍软件
  - 数据泄露
- 未知威胁挑战传统模式
  - 0-Day
  - 隐蔽通道
- 新IT正加速安全域变化
  - 合作医疗互联
  - 远程接入患者
  - 终端和BYOD

成功的攻击中，92%是由于外部攻击者

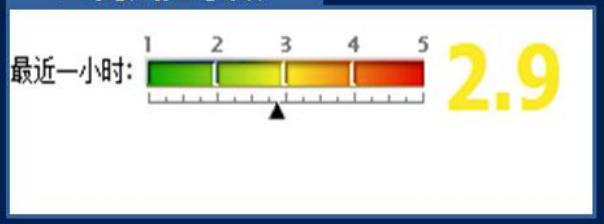
攻击大多不能通过现有安全设备发现，87%源自外部的报告

重要假设：内部员工同样不可信

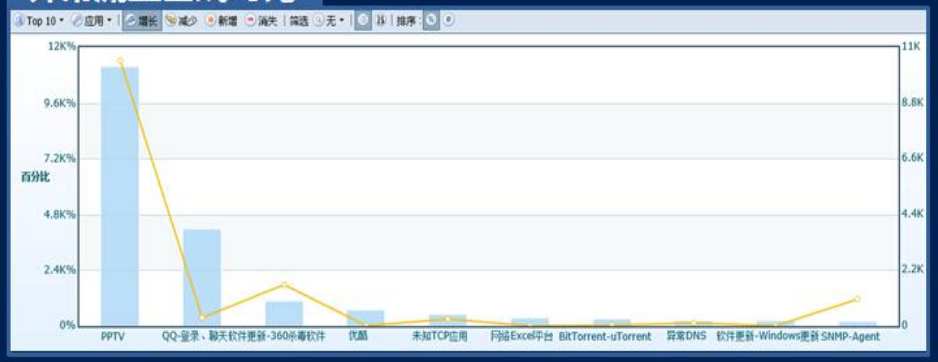
防火墙

以风险为视角发现问题

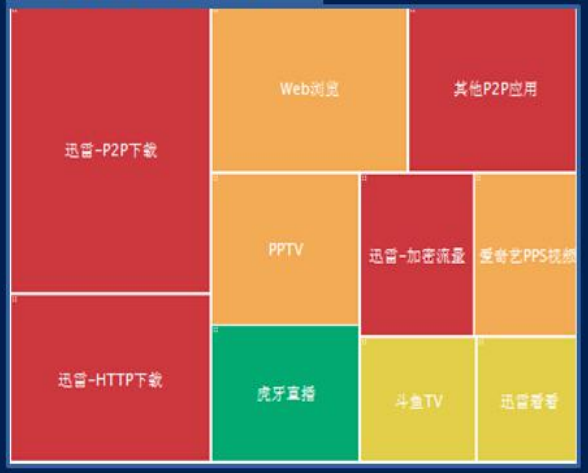
全网风险系数



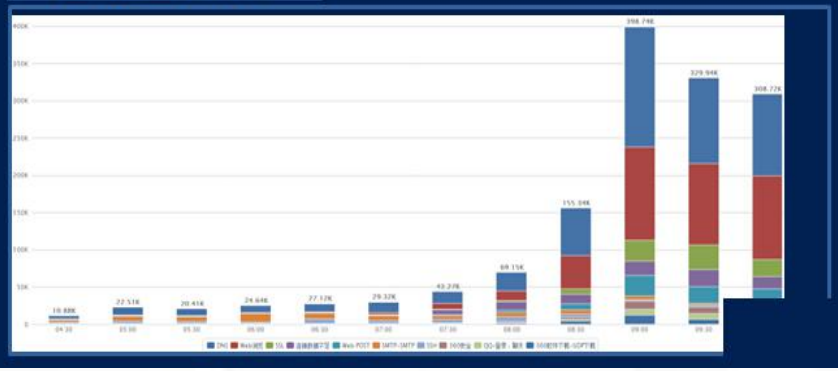
异常流量基线对比



高危应用统计



应用趋势统计



防火墙

以应用为视角关联分析问题

1. 统计信息关联

应用

	风险	应用名称
1	3	Web浏览

威胁

	严重性	威胁名称
1	中	畸形HTTP报文-双Accept域
2	高	Microsoft IIS cmd.exe访问
3	中	百度工具栏提取用户数据
4	高	Win.Trojan.Badur 木马变种外向连接尝试
5	高	恶意软件SProtector.A客户端通信尝试

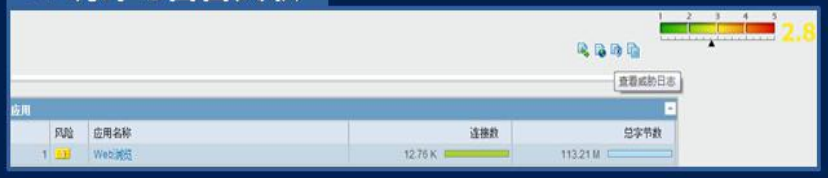
源地址

	源地址	源用户
1	192.168.134.198	第三方用户/xiao_ma
2	192.168.131.184	第三方用户/yu_zheng

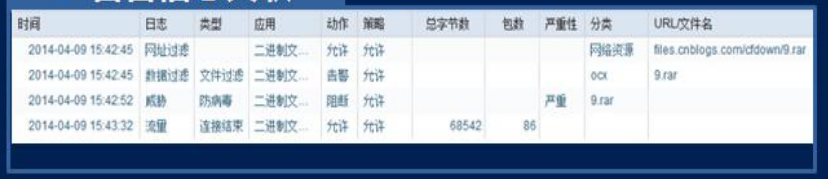
目的地址

	目的地址	目的用户
1	119.75.220.50	未定义账号
2	119.75.217.109	未定义账号

2. 统计与告警关联



3. 告警信息关联



防火墙

以威胁为视角处理问题

1. 待处理安全事件

事件类型	事件摘要	待处理事件
间谍软件	发现感染设备13台 阻断71次,告警0次	6
僵尸网络	发现僵尸主机0个	0
病毒	阻断4次,告警64次	20
高风险应用	发现高风险应用20个	20
漏洞	发现被攻击设备54台 阻断865次,告警1144次	16

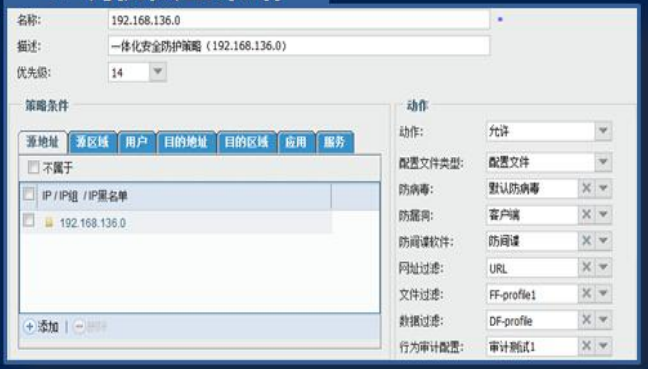
2. 提供处理建议

高风险应用	应用分析	应用类别	总流量	影响	多少企业封堵此应用	行动建议
其他P2P应用		其他应用	1.33 G	容易逃逸,极耗带宽,易被滥用,文件传输,威胁利用,存在漏洞,使用广泛	57.59%	根据您单位的上网制度可考虑加入黑名单
巨人		游戏	186.03 M	极耗带宽,威胁利用,存在漏洞,使用广泛	55.38%	根据您单位的上网制度可考虑加入黑名单
FlashGet-P2P下载		下载工具	41.82 M	容易逃逸,极耗带宽,易被滥用,文件传输,威胁利用,存在漏洞,使用广泛	47.20%	根据您单位的上网制度可考虑加入黑名单
百度影音		视频	6.14 M	容易逃逸,极耗带宽,易被滥用,文件传输,存在漏洞,使用广泛	53.87%	根据您单位的上网制度可考虑加入黑名单
WinMX		下载工具	2.07 M	容易逃逸,极耗带宽,易被滥用,文件传输,威胁利用,存在漏洞,使用广泛	59.25%	根据您单位的上网制度可考虑加入黑名单
皮皮影视		视频	1.16 M	容易逃逸,极耗带宽,易被滥用,文件传输,存在漏洞,使用广泛	55.48%	根据您单位的上网制度可考虑加入黑名单
迅雷-资源搜索		下载工具	931.8 K	容易逃逸,极耗带宽,易被滥用,文件传输,威胁利用,存在漏洞,使用广泛	47.85%	根据您单位的上网制度可考虑加入黑名单
飞信游戏中心		游戏	587.52 K	极耗带宽,威胁利用,存在漏洞,使用广泛	55.38%	根据您单位的上网制度可考虑加入黑名单
QQ视频桌面版		视频	584.38 K	容易逃逸,极耗带宽,使用广泛	56.77%	根据您单位的上网制度可考虑加入黑名单

3. 快速处理威胁

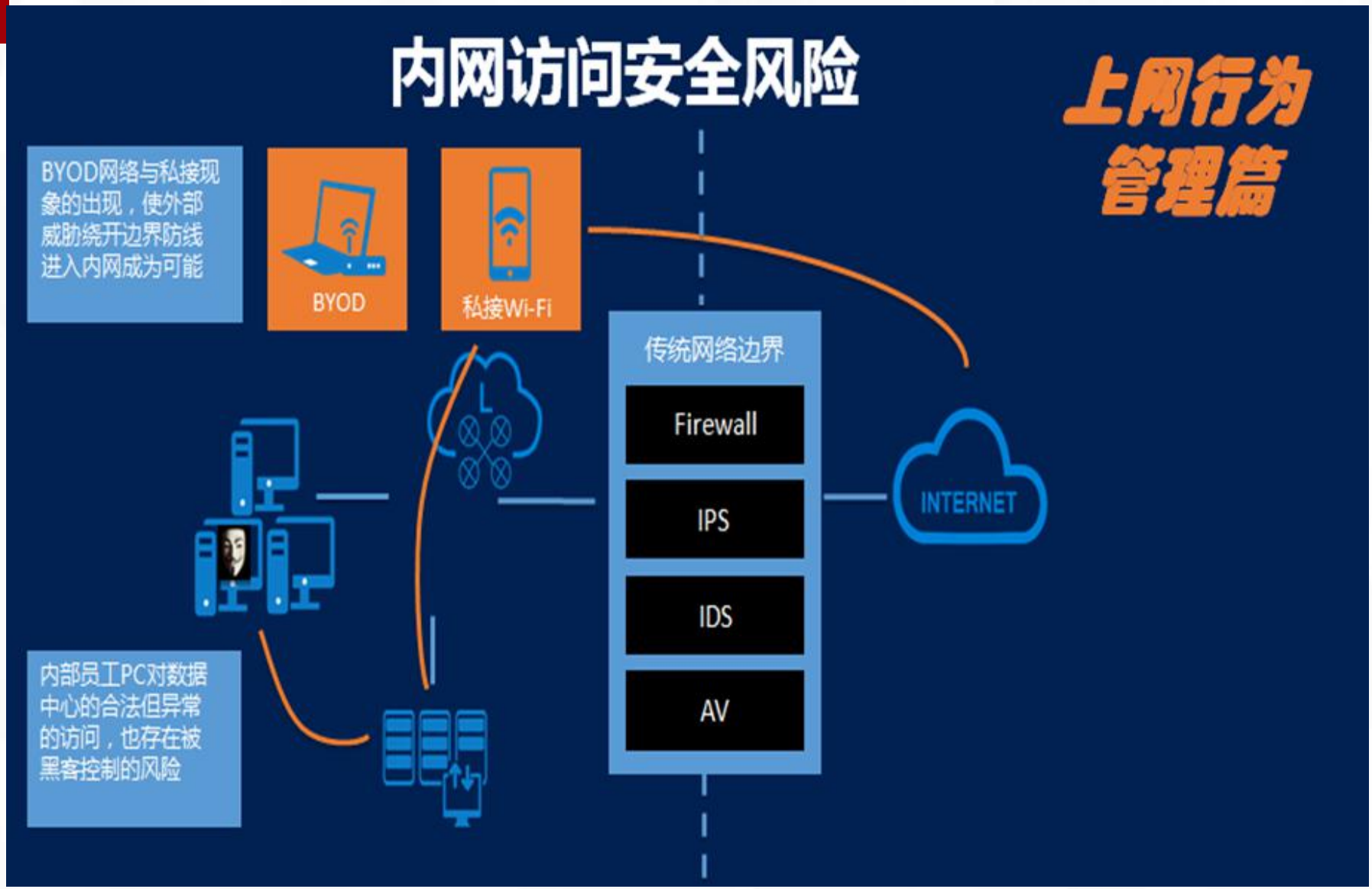
全部加入黑名单	全部信任应用
加入黑名单	信任应用
加入黑名单	信任应用
加入黑名单	信任应用
加入黑名单	信任应用

4. 调优安全策略



内网访问安全风险

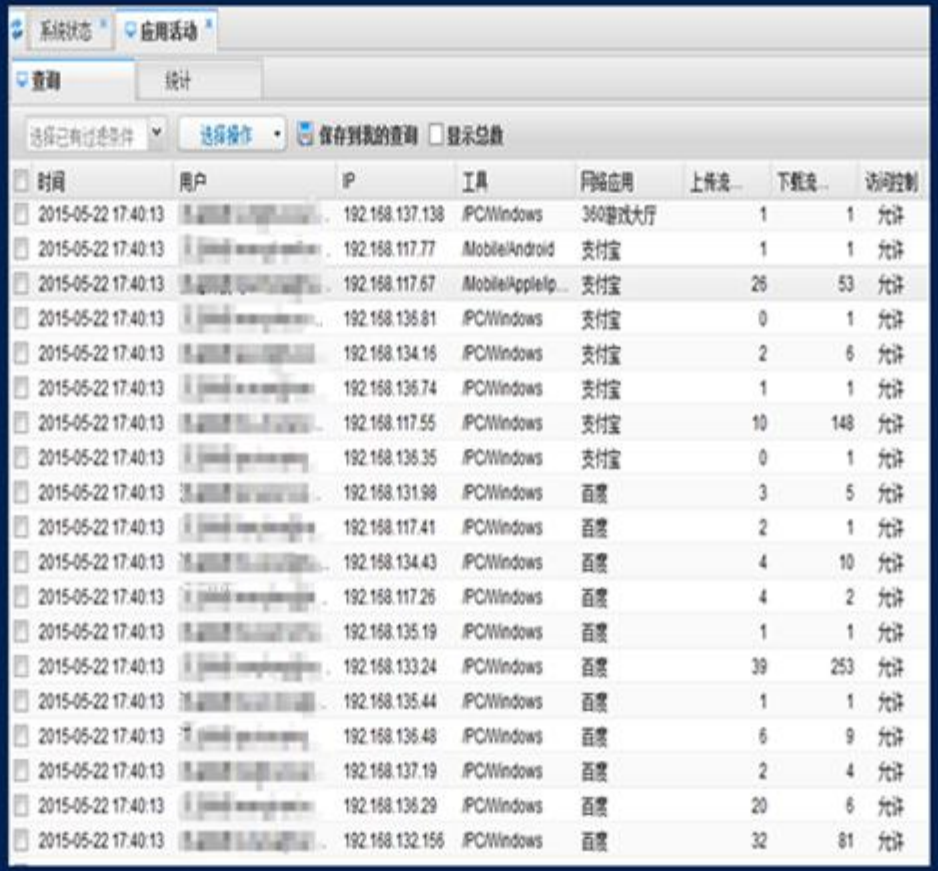
上网行为管理篇



完整的上网行为审计能力

上网行为管理篇

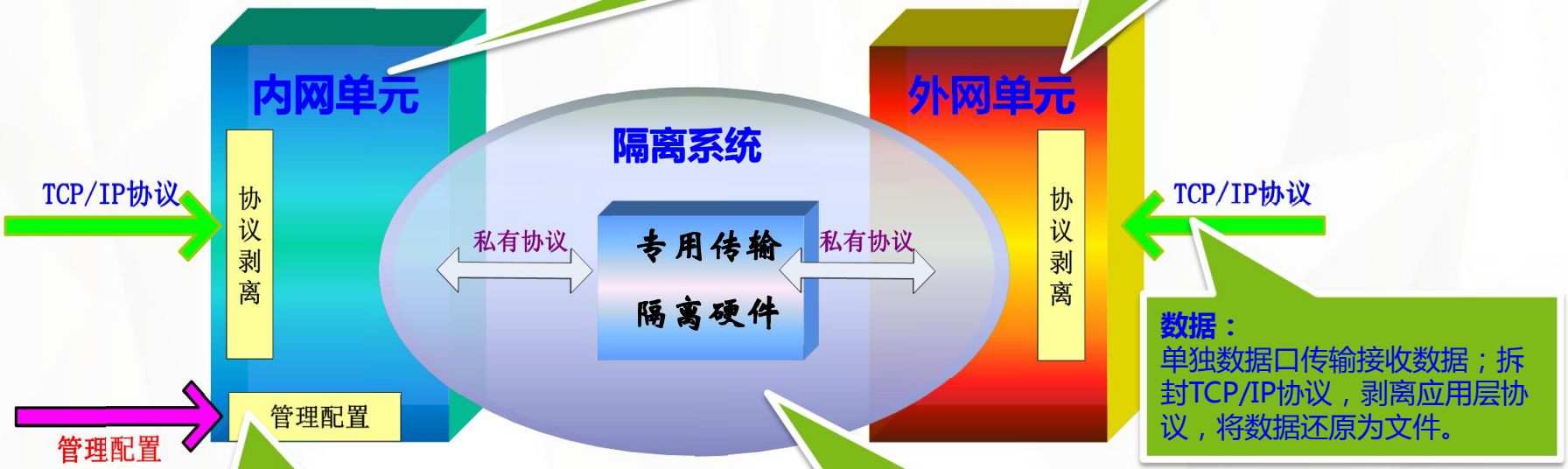
- 网址访问审计
- 论坛发帖审计
- 邮件收发审计
- IM聊天审计
- 应用行为审计



时间	用户	IP	工具	网络应用	上传流...	下载流...	访问控制
2015-05-22 17:40:13		192.168.137.138	/PC/Windows	360游戏大厅	1	1	允许
2015-05-22 17:40:13		192.168.117.77	/Mobile/Android	支付宝	1	1	允许
2015-05-22 17:40:13		192.168.117.67	/Mobile/Apple/ip...	支付宝	26	53	允许
2015-05-22 17:40:13		192.168.136.81	/PC/Windows	支付宝	0	1	允许
2015-05-22 17:40:13		192.168.134.16	/PC/Windows	支付宝	2	6	允许
2015-05-22 17:40:13		192.168.136.74	/PC/Windows	支付宝	1	1	允许
2015-05-22 17:40:13		192.168.117.55	/PC/Windows	支付宝	10	148	允许
2015-05-22 17:40:13		192.168.136.35	/PC/Windows	支付宝	0	1	允许
2015-05-22 17:40:13		192.168.131.98	/PC/Windows	百度	3	5	允许
2015-05-22 17:40:13		192.168.117.41	/PC/Windows	百度	2	1	允许
2015-05-22 17:40:13		192.168.134.43	/PC/Windows	百度	4	10	允许
2015-05-22 17:40:13		192.168.117.26	/PC/Windows	百度	4	2	允许
2015-05-22 17:40:13		192.168.135.19	/PC/Windows	百度	1	1	允许
2015-05-22 17:40:13		192.168.133.24	/PC/Windows	百度	39	253	允许
2015-05-22 17:40:13		192.168.135.44	/PC/Windows	百度	1	1	允许
2015-05-22 17:40:13		192.168.136.48	/PC/Windows	百度	6	9	允许
2015-05-22 17:40:13		192.168.137.19	/PC/Windows	百度	2	4	允许
2015-05-22 17:40:13		192.168.136.29	/PC/Windows	百度	20	6	允许
2015-05-22 17:40:13		192.168.132.156	/PC/Windows	百度	32	81	允许


准确快速的私接管控能力
上网行为
管理篇
用户A
账号A
权限1
小路由
随身WiFi
用户B
账号A
权限3
上网行为管理
用户C
账号A
权限3

网闸技术原理



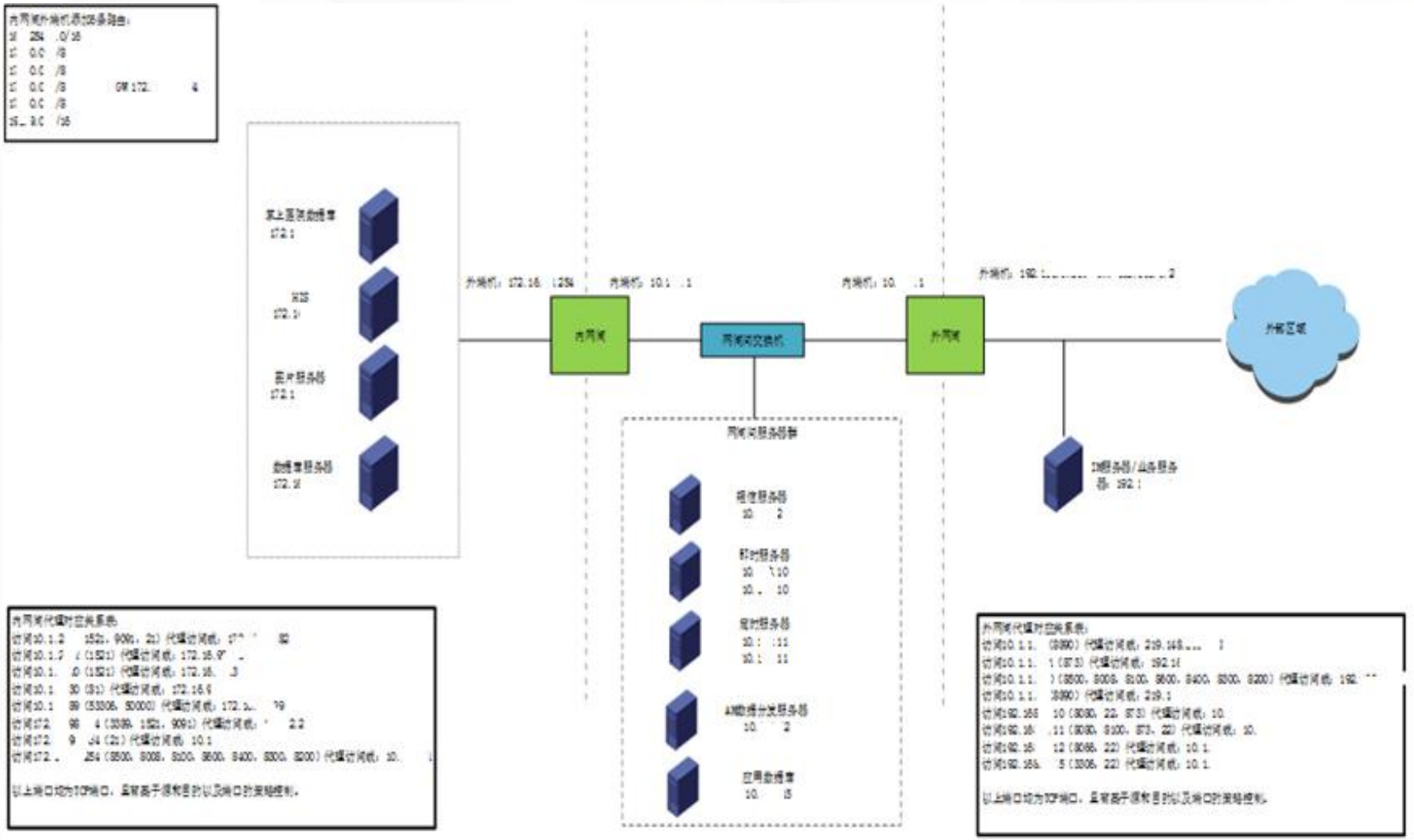
内网单元、外网单元：
独立主板、总线及CPU控制；
专用安全操作系统，多层次的高强度安全防护

数据：
单独数据口传输接收数据；拆封TCP/IP协议，剥离应用层协议，将数据还原为文件。

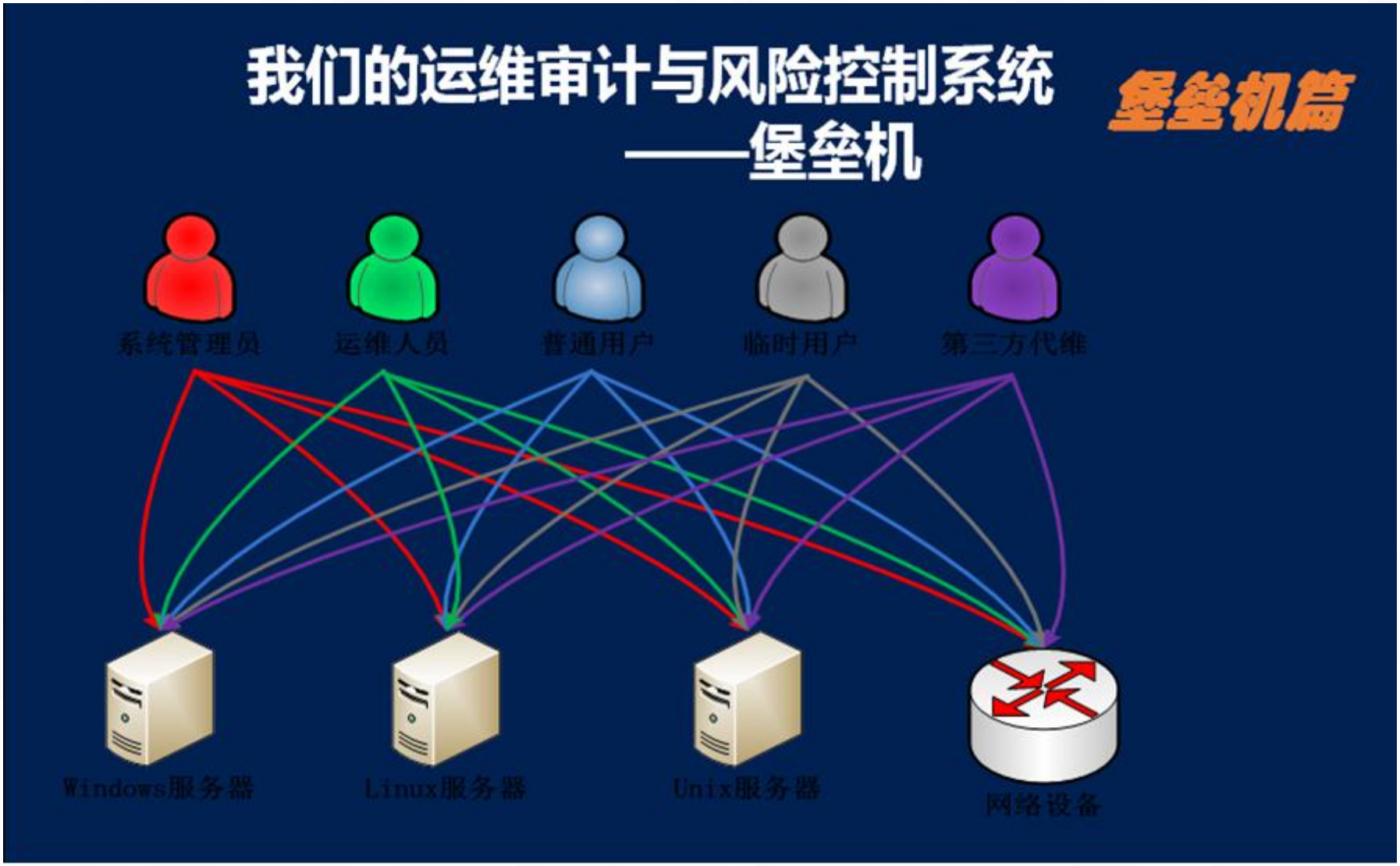
管理：
管理端口、业务端口相互独立；内网管理；
多种管理员登陆认证保密机制。

数据迁移控制单元 ：
独立硬件数据迁移逻辑，无操作系统；
专用隔离硬件，内外单元的数据高效摆渡；
私有协议。

网闸部署拓扑&具体策略



堡垒机


我们的运维审计与风险控制系统
——堡垒机
堡垒机篇
系统管理员
运维人员
普通用户
临时用户
第三方代维
Windows服务器
Linux服务器
Unix服务器
网络设备

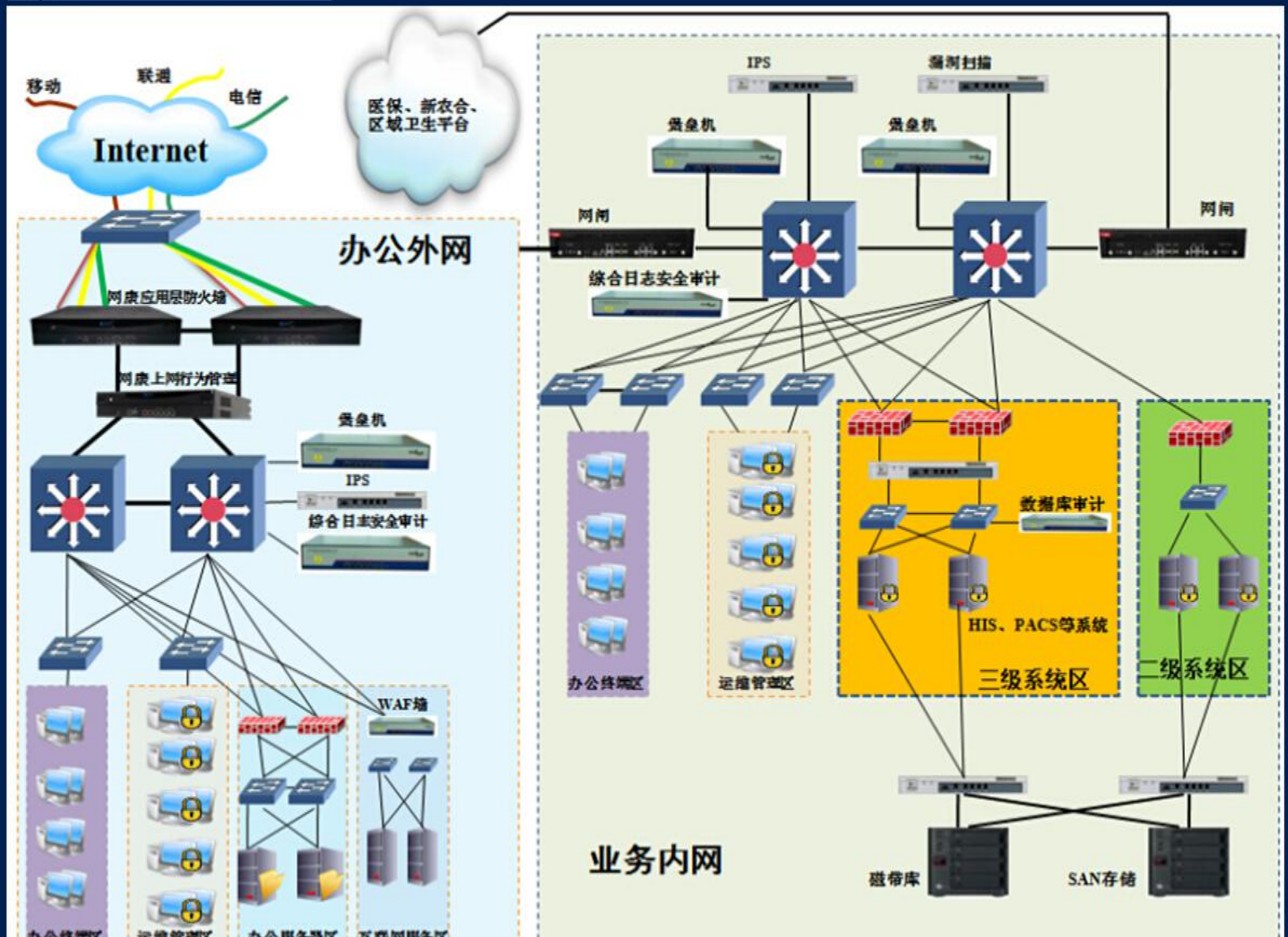
堡垒机

我们的运维与风险管理

堡垒机篇

- **账号管理：**集中统一管理用户帐号，实现将帐号与具体自然人相关联，实现针对自然人的行为审计。
- **单点登录：**运维用户可以在单点登录页面中对资产进行统一管理，只需要进行堡垒机的一次登录，即 可可免去登录资产的帐户认证繁琐操作，同时也保障了资产的帐户和密码的安全性。
- **资产授权：**明确身份后，把账号与资产账号相关联，限制操作者合法访问资源，有效降低未授权访问所所带来的风险。
- **访问策略：**支持基于用户属性、资产属性、IP段等组合，制定细粒度的行为策略，当操作者越权访问时时，可自动告警告、阻断，确保信息系统安全运行。
- **运维审计：**提供实时监控，完整的操作记录回放，日志查询以及报表分析等功能，能够快速定位事故，还原事故现场和举证

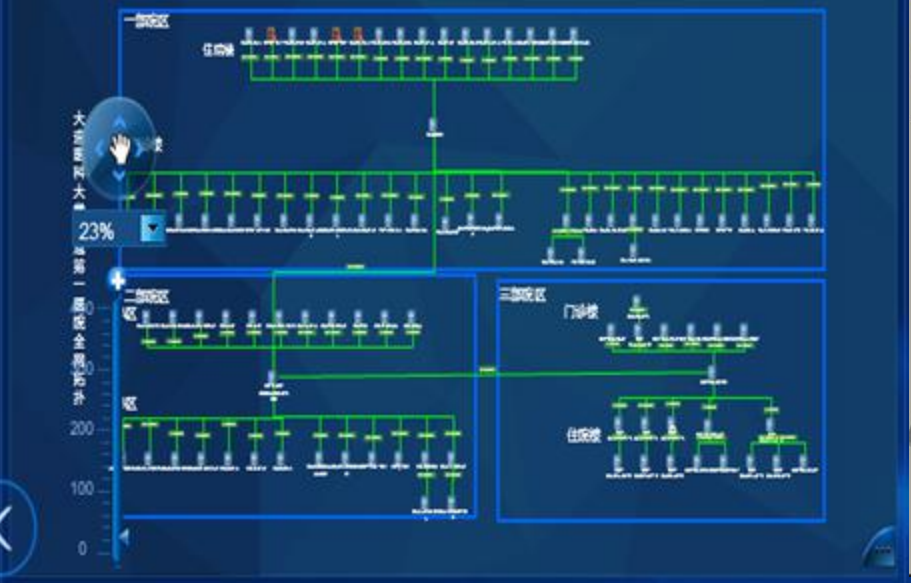
我们的拓扑


移动
联通
电信
Internet
医保、新农合、
区域卫生平台
办公外网
网康应用层防火墙
网康上网行为管理
贵阜机
IPS
综合日志安全审计
WAF墙
IPS
漏洞扫描
贵阜机
贵阜机
网闸
网闸
综合日志安全审计
办公终端区
运维管理区
数据库审计
HIS、PACS等系统
三级系统区
二级系统区
业务内网
磁带库
SAN存储

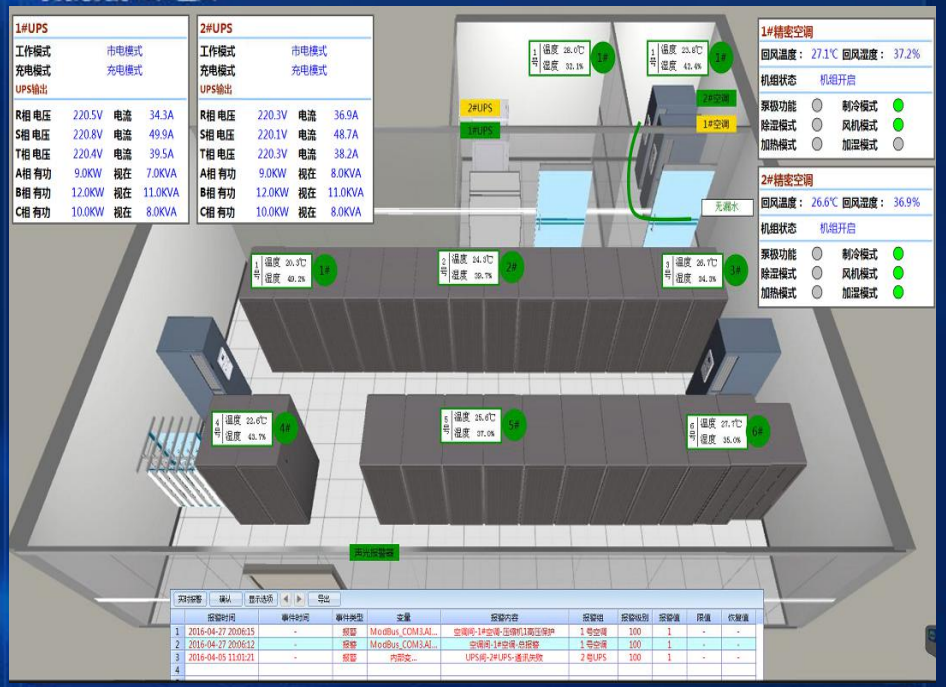
网络拓扑图URL(BMC)

拓扑管理 -> 大连医大一院网络拓扑 (节点数：108 物理链路数：95 未监控：0)

告警



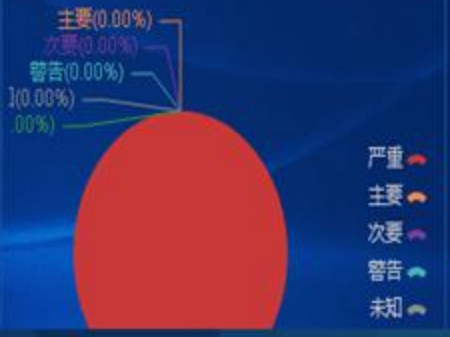
可视化机房3D户型图



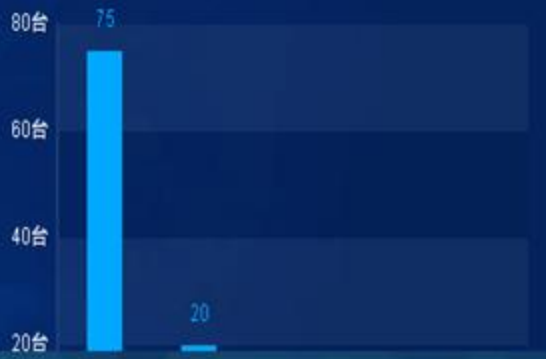
资源指标一览

状态	资源名称	IP地址	CPU利用率	内存利用率
	San-Bu_ZY1_14F-1	172.1[illegible]	30%	57.17%
	YB-JG-4F	172.16.[illegible]	30%	60%
	EB_3F_shoushushi	172.16.[illegible]	23%	48%
	YB_2F_TD	172.16.[illegible]	22%	75%
	YB-MZ-1F_1	172.16.[illegible]	20%	67%
	YB-GRK	172.16.1[illegible]	20%	74%

当前告警级别占比



资源数量排行(按设备类型)-TOP5



微信掌上医院

引入互联网+概念，改善患者就医体验

国发〔2015〕40号文件：《国务院关于积极推进“互联网+”行动的指导意见》11项行动计划，“互联网+益民服务”中指出：推广在线医疗卫生新模式：1）积极利用移动互联网提供在线预约诊疗、候诊提醒、划价缴费、诊疗报告查询，药品配送等便捷服务等；

微信掌上医院

大连市最具影响力的三甲医院，
年门诊量220多万人次。

三长一短现象严重，
每天人工排队30分钟

通过掌上医院操作5分钟，
每天零点线上号源一经推出，
30分钟内便被预约完。

微信掌上医院

掌上医院的建设，也带来医院内部的一些变化：

1. 建立了实名制就诊制度

2. 加强了健康教育

3. 促进了新闻动态传播

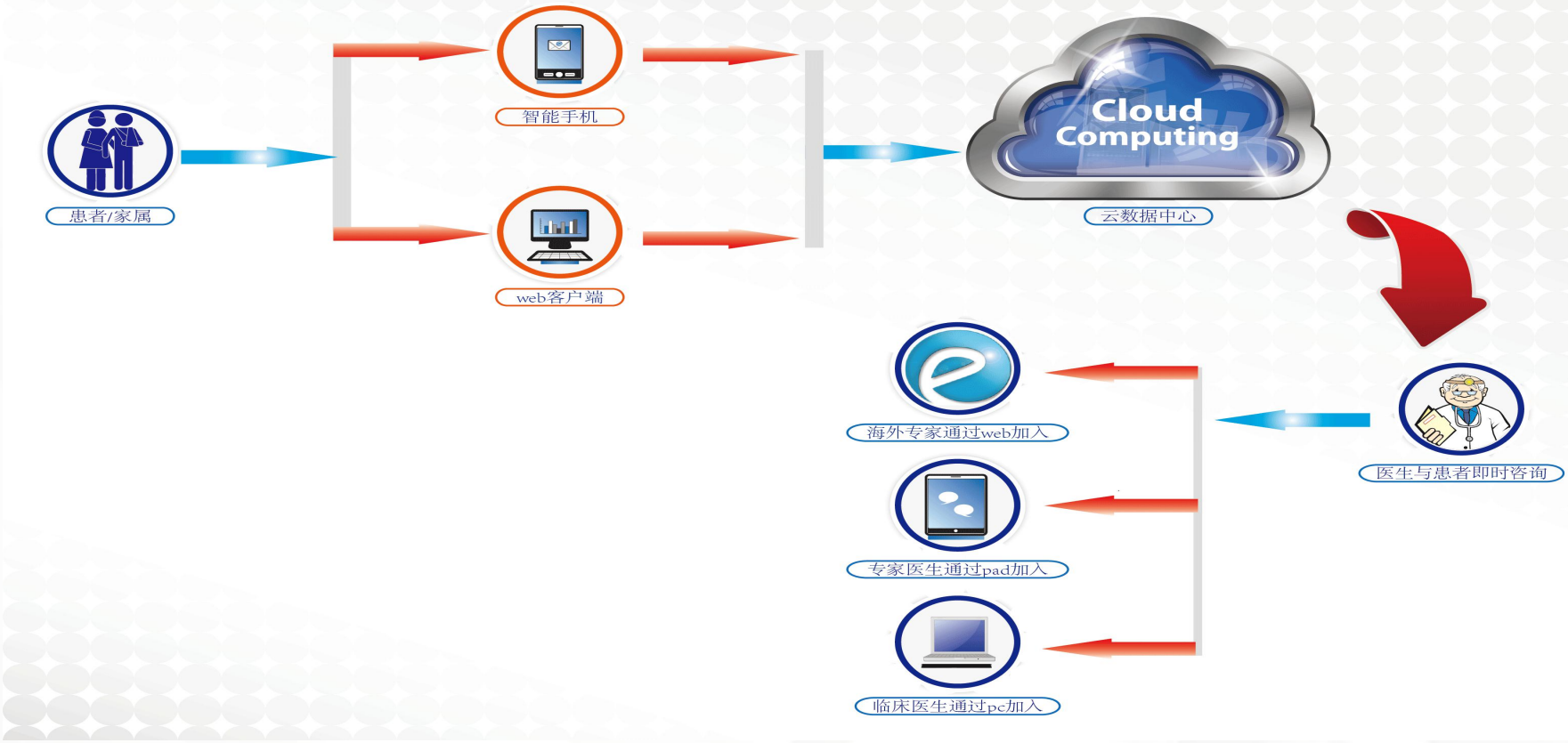
微信掌上医院

大连医科大学附属第一医院
THE FIRST AFFILIATED HOSPITAL OF DALIAN MEDICAL UNIVERSITY

院内外移动端会诊及随诊管理

打造一个无地域限制的工作平台，实现院内数据融合互通、远程/移动会诊、远程/移动医嘱、HIS、RIS、LIS、CIS、PACS、CPR多平台数据整合、医学研究数据调研。

院内外移动端会诊及随诊管理



（1）医生端移动会诊：医生通过移动端对患者提供在线健康咨询服务，提供在院患者的院内请会诊
（2）医患互动：患者可以将请求发布在科室公众工作平台上，由医生对患者的咨询进行回复；通过互动，医生了解病人出院后的治疗效果、病情变化和恢复情况，指导病人用药、康复、复诊、病情变化后的处置意见等专业技术性指导。
（3）慢性病管理：高血压，糖尿病，帕金森综合症
（4）体检人员的综合评估：为临床提供精准服务。

大连医科大学附属第一医院

THE FIRST AFFILIATED HOSPITAL OF DALIAN MEDICAL UNIVERSITY

弘道笃行 精诚大医

感谢您的聆听！

服务、创意，做什么都要好

聚焦医疗前沿，注重患者感受

弘道笃行 精诚大医

建设国内一流、国际知名的 医疗研究型大学附属医院