

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

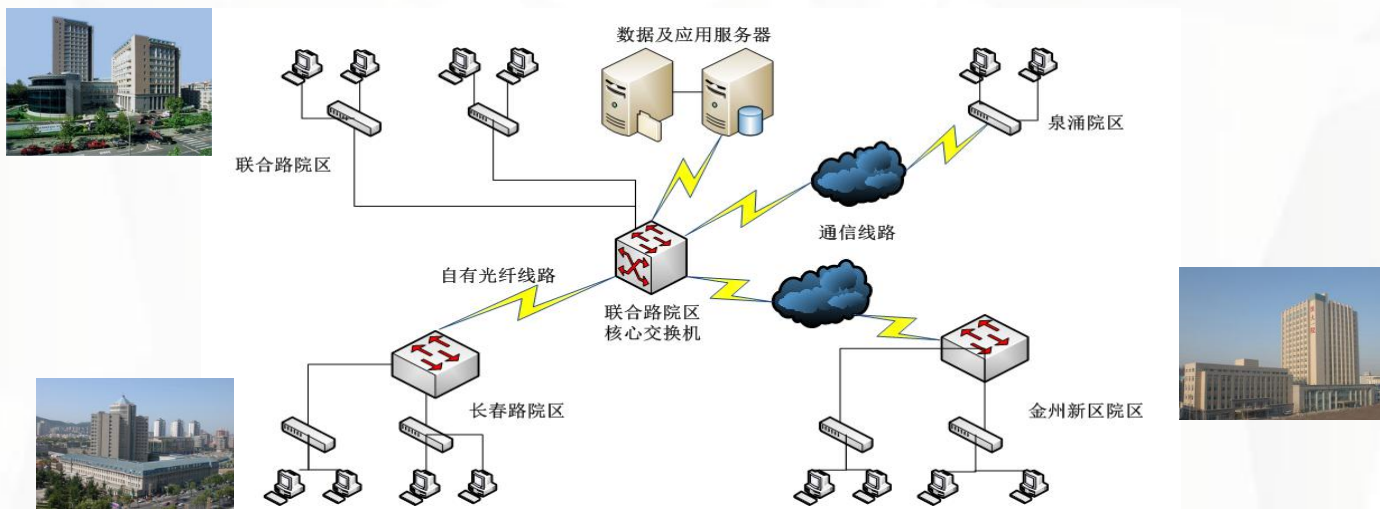


大连医科大学附属第一医院

THE FIRST AFFILIATED HOSPITAL OF DALIAN MEDICAL UNIVERSITY

大医一院网络架构概况

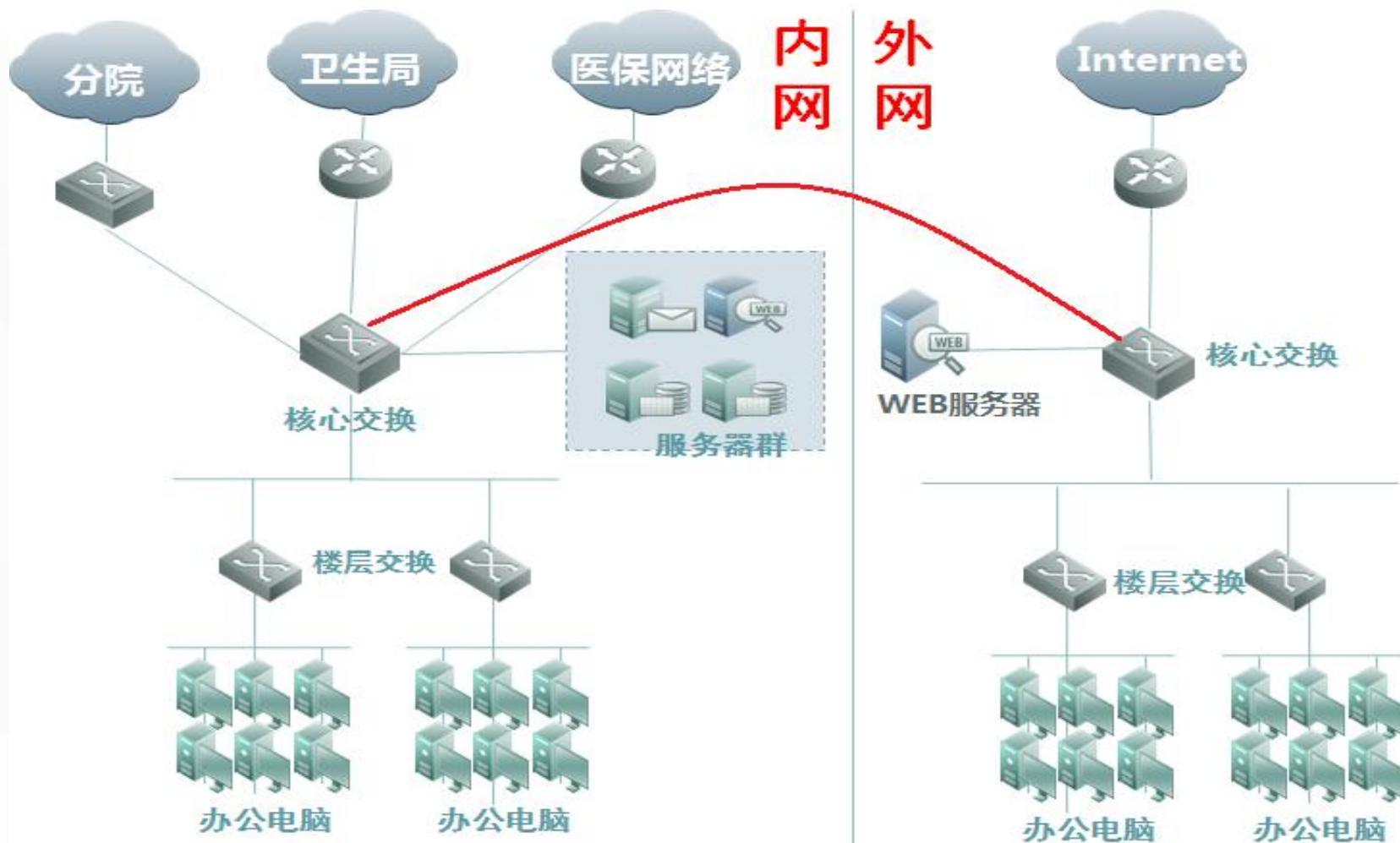
医院现共有4个院区，分别是长春路院区、联合路院区、金州新区院区、泉涌院区。院区间通过独自铺设光纤和租用通信线路连接，避免服务器硬件重复投入，医院数据统一存储管理，四个院区数据高度共享。各院区核心网络交换机采用高端设备，制定网络设备单点故障点的备份解决方案。



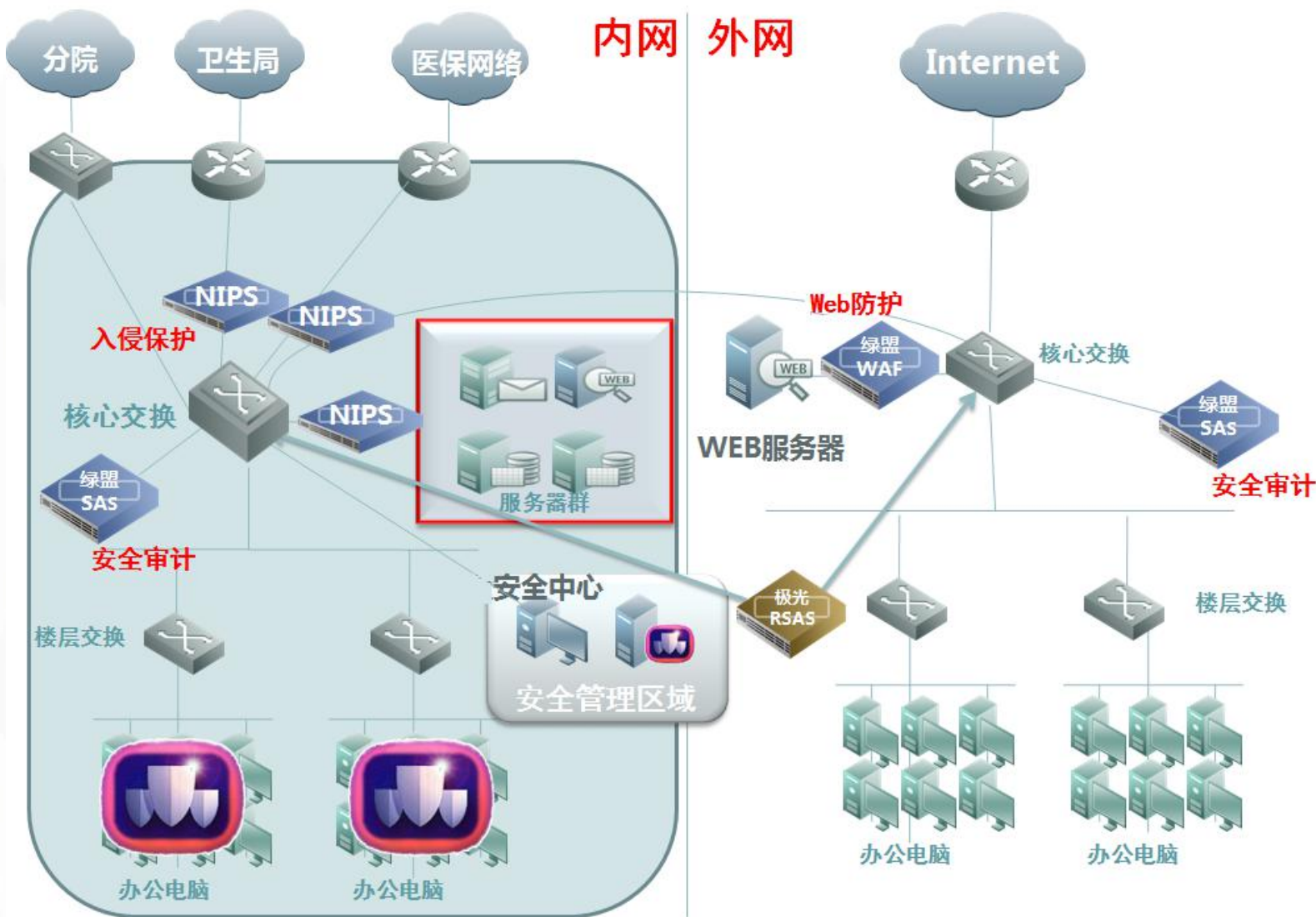
大连医科大学附属第一医院

THE FIRST AFFILIATED HOSPITAL OF DALIAN MEDICAL UNIVERSITY

无安全机制的内外网互联



WEB防护和安全审计



大连医科大学附属第一医院

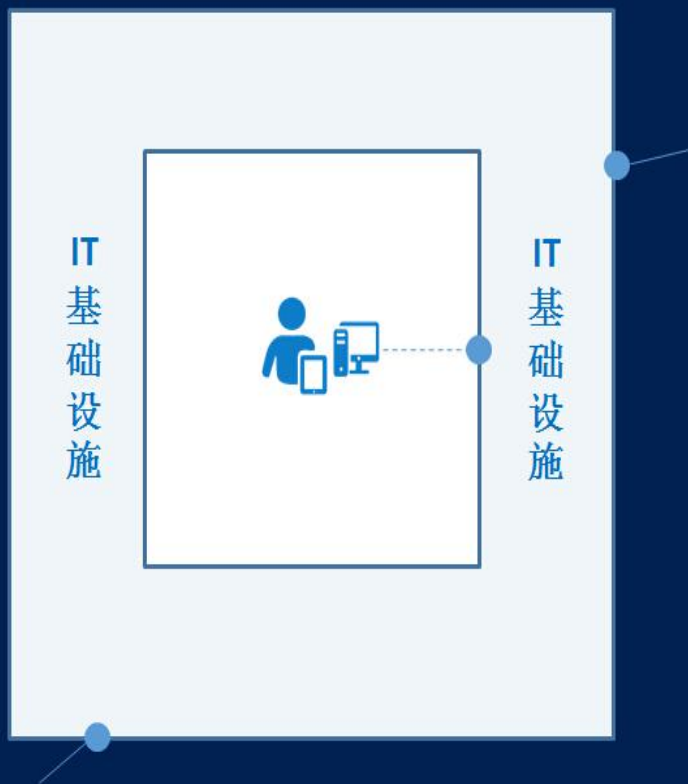
THE FIRST AFFILIATED HOSPITAL OF DALIAN MEDICAL UNIVERSITY

Web应用监测平台

网站网址	网站名称	漏洞类型	漏洞URL	网站安全分数	开始时间	结束时间	操作
实时报警 -> 查看报告 [切换为列表视图]						08-03 14:54	查看报告 导出报告
http://192.168.29.4:8088/wavsep/index-full.jsp (416)						08-03 10:31	查看报告 导出报告
SQL错误信息注入 (58)						08-02 20:21	查看报告 导出报告
SQL盲注 (43)						08-02 16:11	查看报告 导出报告
数据库错误 (78)						08-01 19:17	查看报告 导出报告
实时报警 -> 查看扫描详情 [切换为列表视图]						08-01 14:25	查看报告 导出报告
本次扫描结束时间 2011-08-03 14:54:40		上次扫描结束时间 2011-08-03 14:12:42					
本次发现漏洞总数 416		上次发现漏洞总数 370					
本次包含漏洞类型 Web应用程序错误,VIEWSTATE参数未加密,SQL盲注,框架注入,表单跨域,跨站脚本,SQL错误信息注入,链接注入,跨站伪通用请求,数据库错误		上次包含漏洞类型 Web应用程序错误,VIEWSTATE参数未加密,SQL盲注,框架注入,跨站脚本,表单跨域,链接注入,SQL错误信息注入,跨站伪通用请求,数据库错误					
已经修补漏洞的URL (0)		未修补漏洞的URL (370)		新发现漏洞的URL (46)			
漏洞名称	漏洞URL	漏洞描述					
SQL错误信息注入	http://192.168.29.4:8088/wavsep/SInjection-Dete...	参数: transactionDate=2010-01-01, 数据库类型: Mysql					
SQL错误信息注入	http://192.168.29.4:8088/wavsep/SInjection-Dete...	参数: transactionDate=2010-01-01, 数据库类型: Mysql					
SQL错误信息注入	http://192.168.29.4:8088/wavsep/SInjection-Dete...	参数: transactionId=1, 数据库类型: Mysql					
SQL错误信息注入	http://192.168.29.4:8088/wavsep/SInjection-Dete...	参数: msg=1, 数据库类型: Mysql					
SQL错误信息注入	http://192.168.29.4:8088/wavsep/SInjection-Dete...	参数: transactionDate=1, 数据库类型: Mysql					
SQL错误信息注入	http://192.168.29.4:8088/wavsep/SInjection-Dete...	参数: transactionDate=1, 数据库类型: Mysql					
SQL错误信息注入	http://192.168.29.4:8088/wavsep/SInjection-Dete...	参数: msgid=1, 数据库类型: Mysql					



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 (Trust/Untrust/DMZ)
- 访问控制 (Policy/ACL)
- 威胁检测 (IPS/AV/DDoS)

.....



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



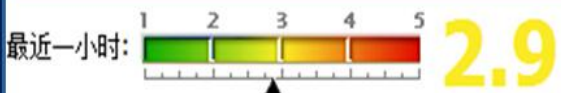
攻击大多不能通过现有安全设备发现，87%源自外部的报告

重要假设：内部员工同样不可信



以风险为视角发现问题

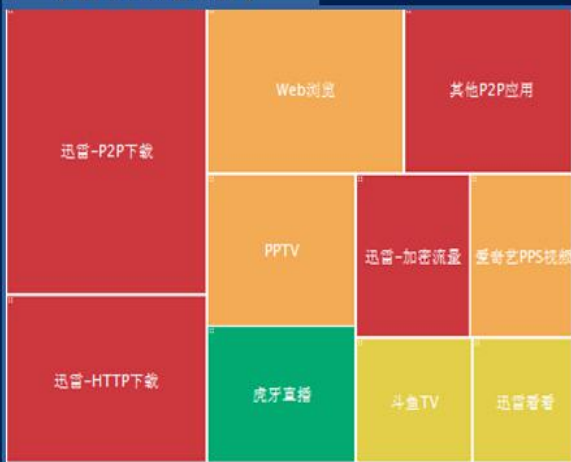
全网风险系数



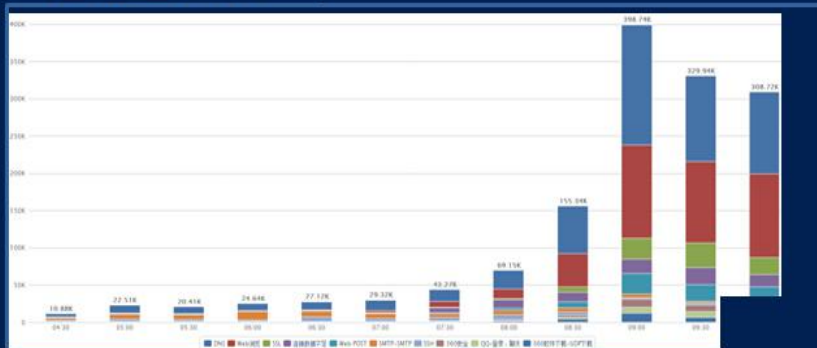
异常流量基线对比



高危应用统计



应用趋势统计



以应用为视角关联分析问题

1. 统计信息关联

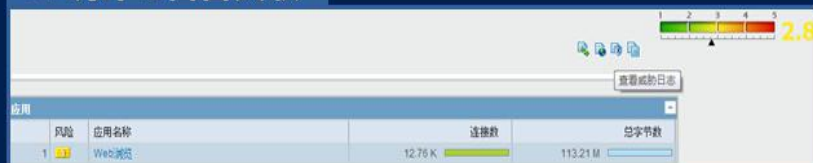
应用		
	风险	应用名称
1	3	Web浏览

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

时间	日志	类型	应用	动作	策略	总字节数	包数	严重性	分类	URL文件名
2014-04-09 15:42:45	网址过滤		二进制文...	允许	允许				网络资源	files.cnblogs.com/ctdown/9.rar
2014-04-09 15:42:45	数据过滤	文件过滤	二进制文...	告警	允许				ock	9.rar
2014-04-09 15:42:52	威胁	防病毒	二进制文...	阻断	允许			严重	9.rar	
2014-04-09 15:43:32	流量	连接结束	二进制文...	允许	允许	68542	86			



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	多少企业封锁此应用	行动建议
其他P2P应用		其他应用	1.33 G	容易逃逸, 消耗带宽, 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	消耗带宽, 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, 消耗带宽, 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, 消耗带宽, 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, 消耗带宽, 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, 消耗带宽, 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, 消耗带宽, 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	消耗带宽, 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, 消耗带宽, 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

名称: 192.168.136.0

描述: 一体化安全防护策略 (192.168.136.0)

优先级: 14

策略条件

源地址 源区域 用户 目的地址 目的区域 应用 服务

不属于

IP / IP组 / IP黑名单

192.168.136.0

动作

动作: 允许

配置文件类型: 配置文件

防病毒: 默认防病毒

防漏洞: 客户端

防间谍软件: 防间谍

网址过滤: URL

文件过滤: FF-profile1

数据过滤: DF-profile

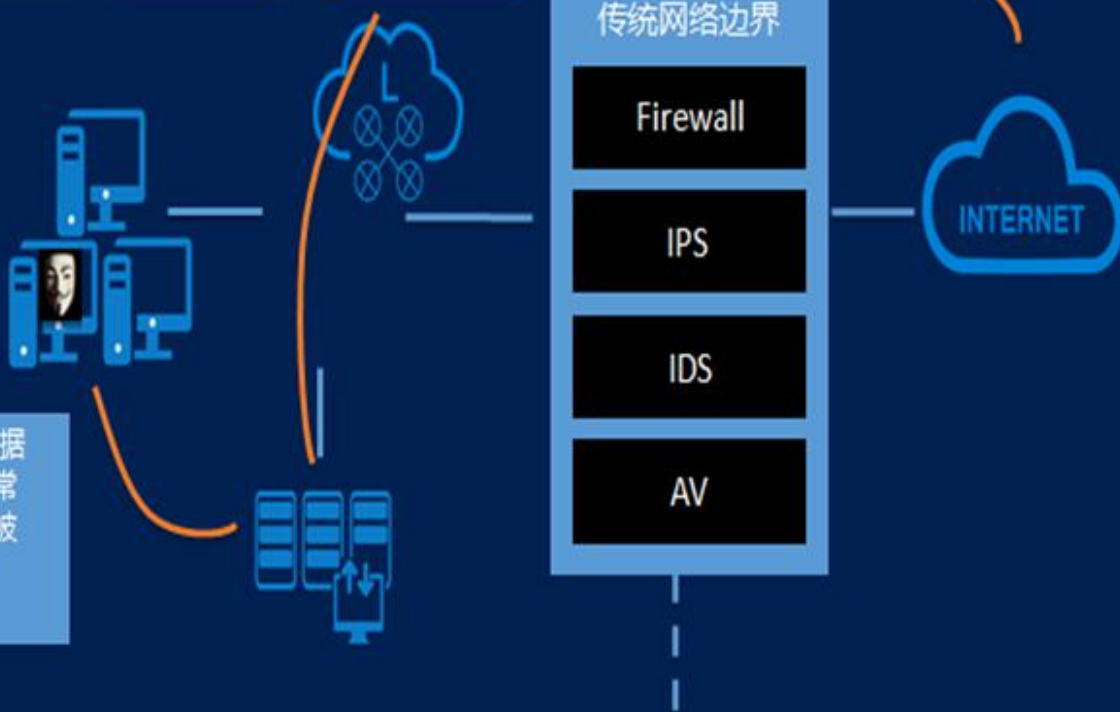
行为审计配置: 审计测试1



内网访问安全风险

上网行为 管理篇

BYOD网络与私接现象的出现，使外部威胁绕开边界防线进入内网成为可能



大连医科大学附属第一医院

THE FIRST AFFILIATED HOSPITAL OF DALIAN MEDICAL UNIVERSITY

完整的上网行为审计能力

上网行为 管理篇

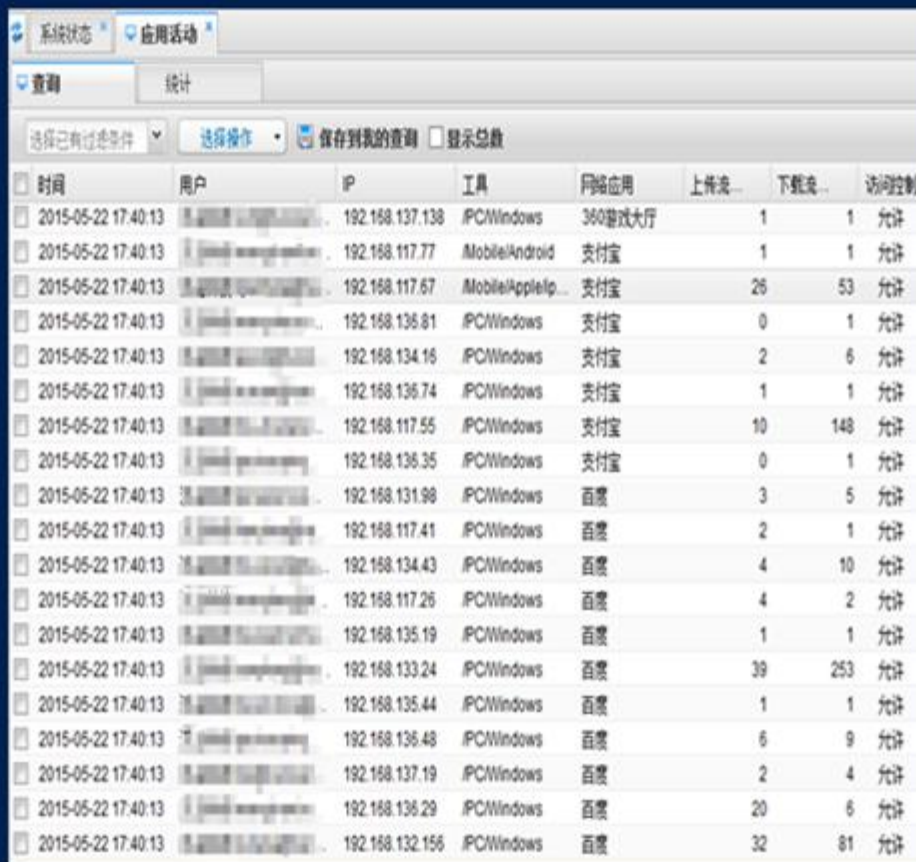
网址访问审计

论坛发帖审计

邮件收发审计

IM聊天审计

应用行为审计



The screenshot displays a software interface for network monitoring. It features a search bar at the top with options for '查询' (Search) and '统计' (Statistics). Below the search bar, there are checkboxes for '选择已有过滤条件' (Select existing filter conditions), '选择操作' (Select operation), '保存到我的查询' (Save to my queries), and '显示总数' (Show total count). The main area is a table with the following columns: '时间' (Time), '用户' (User), 'IP', '工具' (Tool), '网络应用' (Network Application), '上传流量' (Upload Traffic), '下载流量' (Download Traffic), and '访问控制' (Access Control). The table contains 18 rows of data, all from the date 2015-05-22 at 17:40:13. The users listed are various IP addresses, and the tools are either 'PCWindows' or 'MobileAndroid'. The network applications include '360游戏大厅', '支付宝', and '百度'. The upload and download traffic values are also listed, along with an '访问控制' status of '允许' (Allow) for all entries.

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

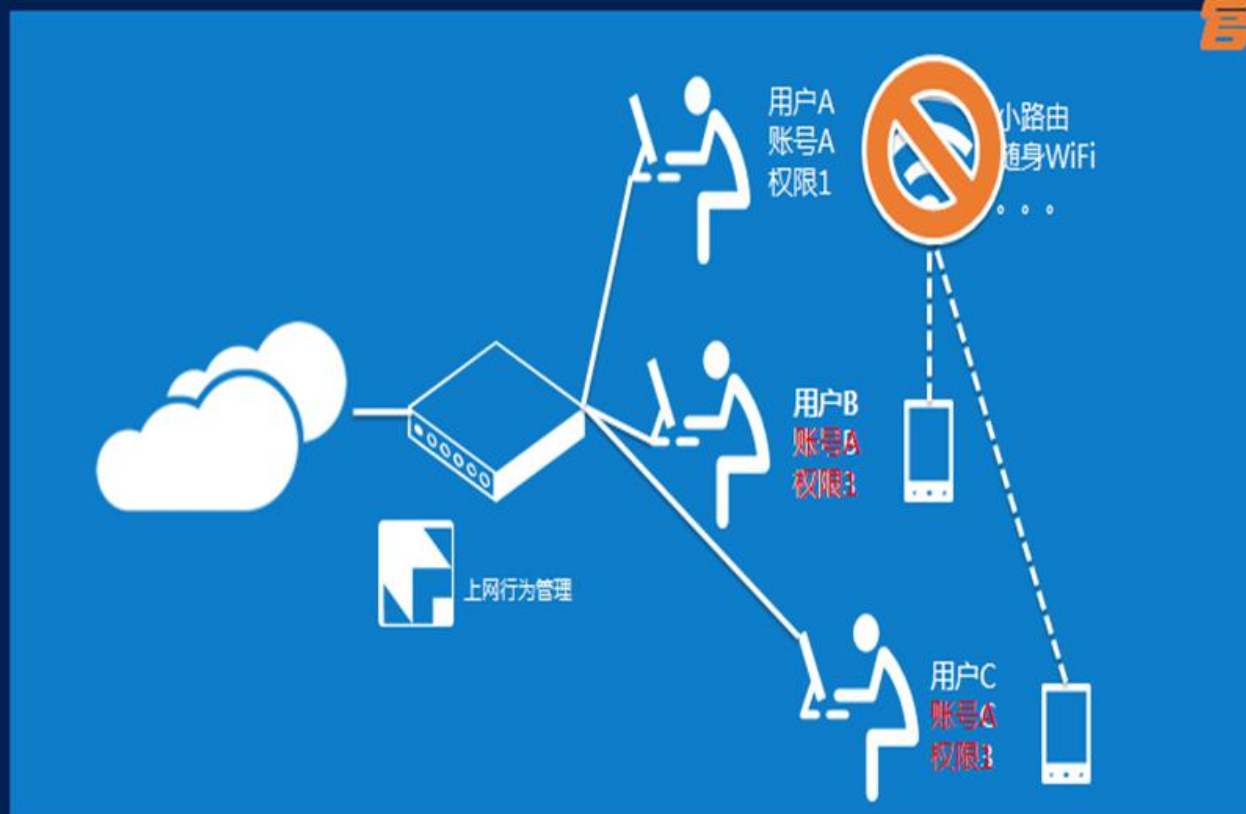


大连医科大学附属第一医院

THE FIRST AFFILIATED HOSPITAL OF DALIAN MEDICAL UNIVERSITY

准确快速的私接管控能力

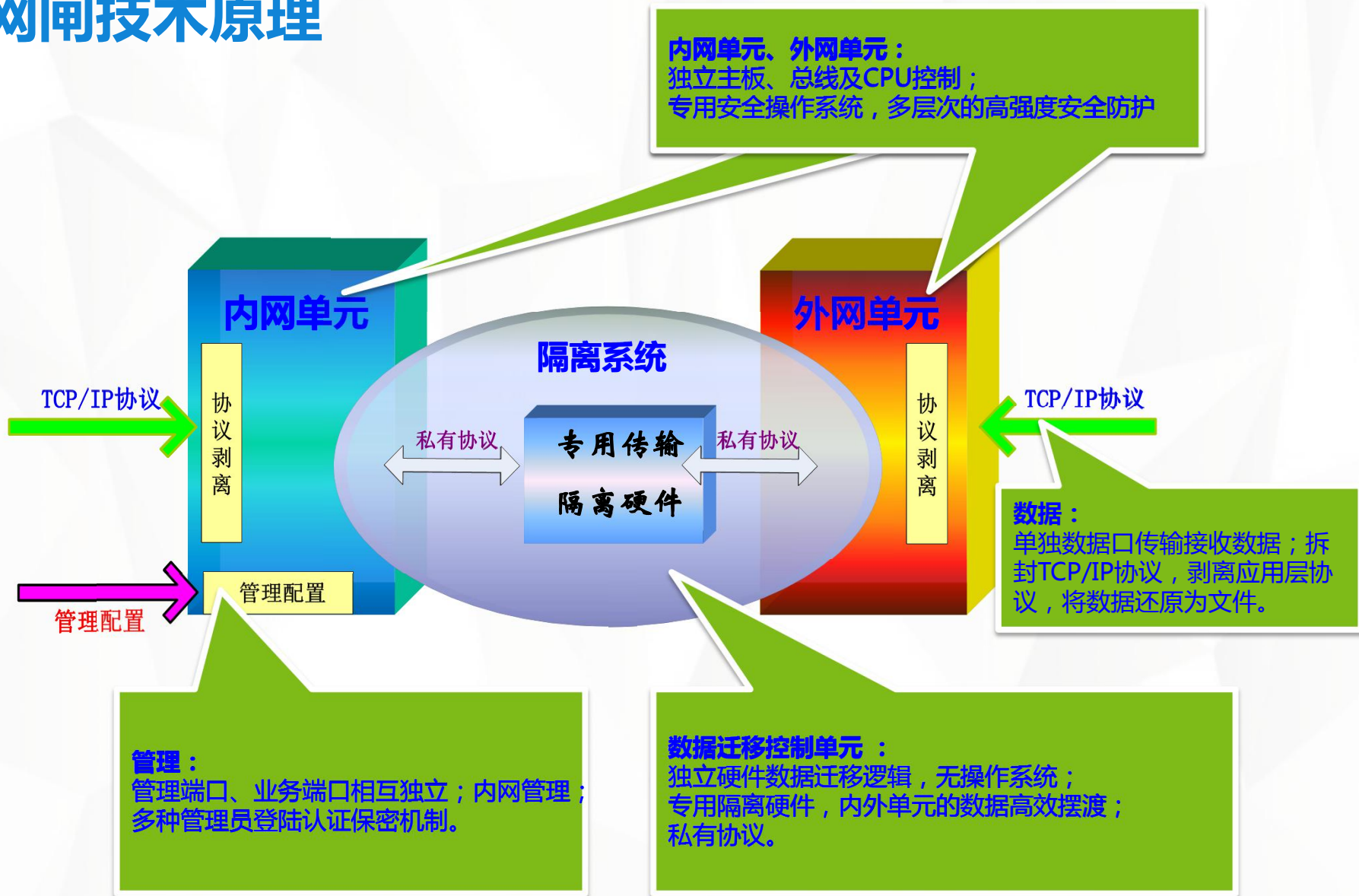
上网行为管理篇



大连医科大学附属第一医院

THE FIRST AFFILIATED HOSPITAL OF DALIAN MEDICAL UNIVERSITY

网闸技术原理

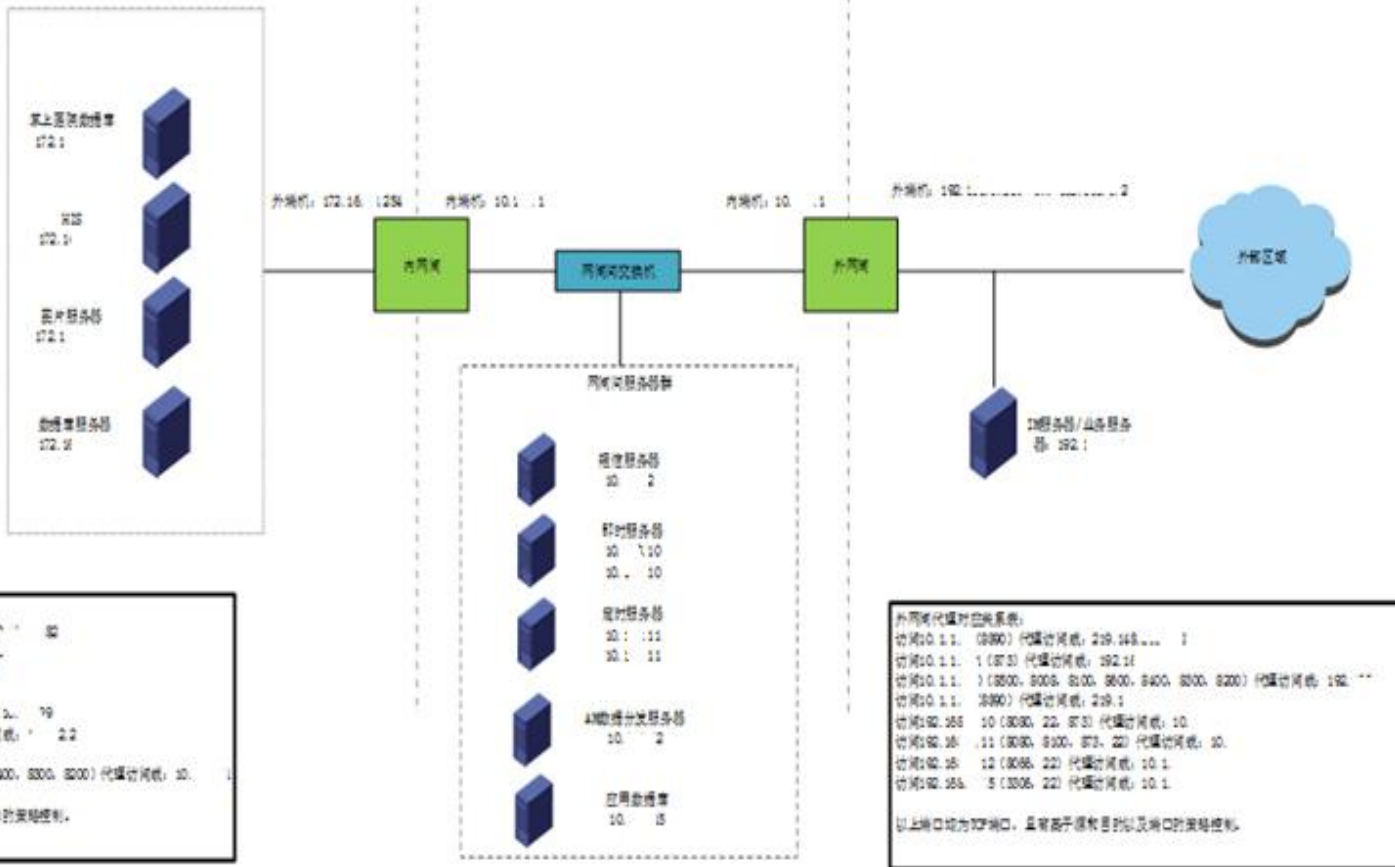


网闸部署拓扑&具体策略

内网和外网机器的连接路由：

```

R1 254.0/25
R1 0.0/8
R1 0.0/8
R1 0.0/8
R1 0.0/8
R1 0.0/8
R1 0.0/8
R1 0.0/8
    
```

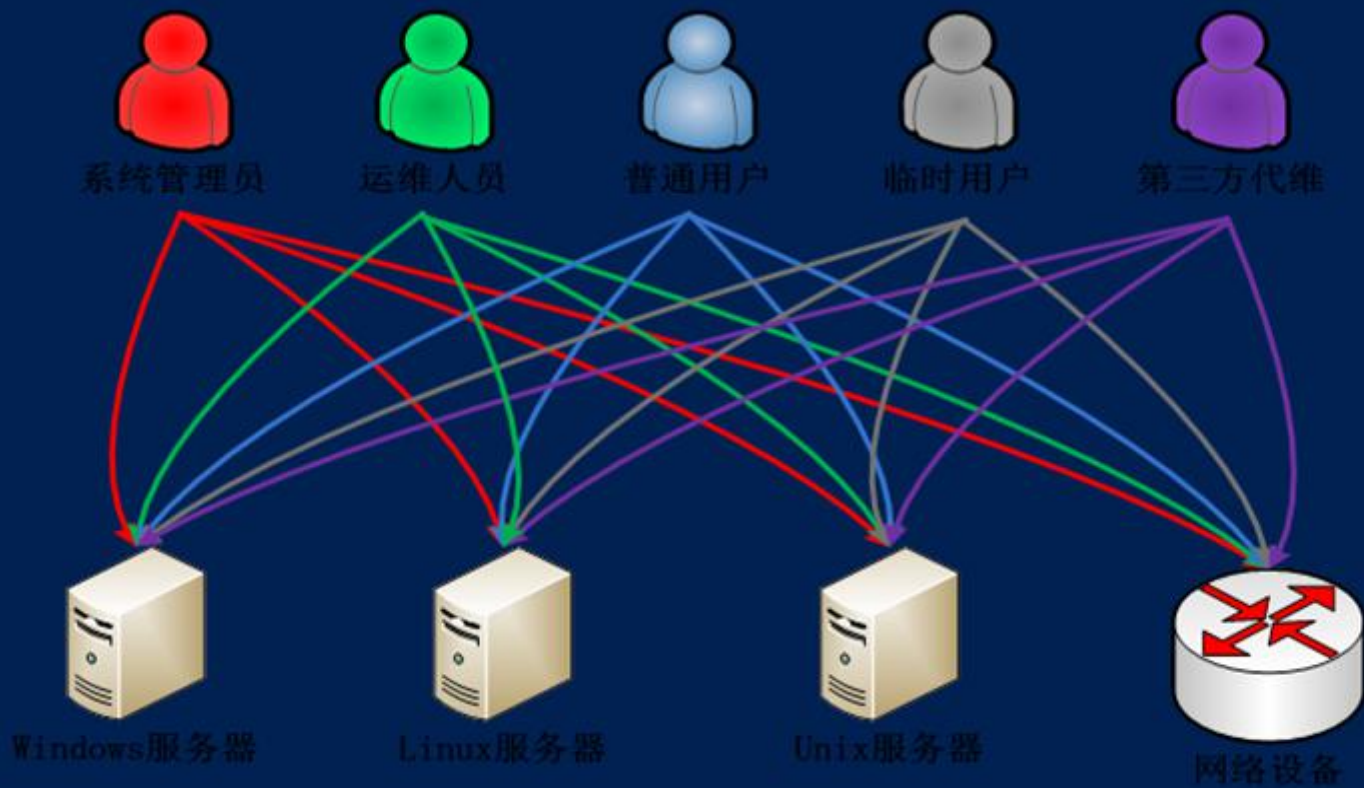


大连医科大学附属第一医院

THE FIRST AFFILIATED HOSPITAL OF DALIAN MEDICAL UNIVERSITY

我们的运维审计与风险控制系统 ——堡垒机

堡垒机篇



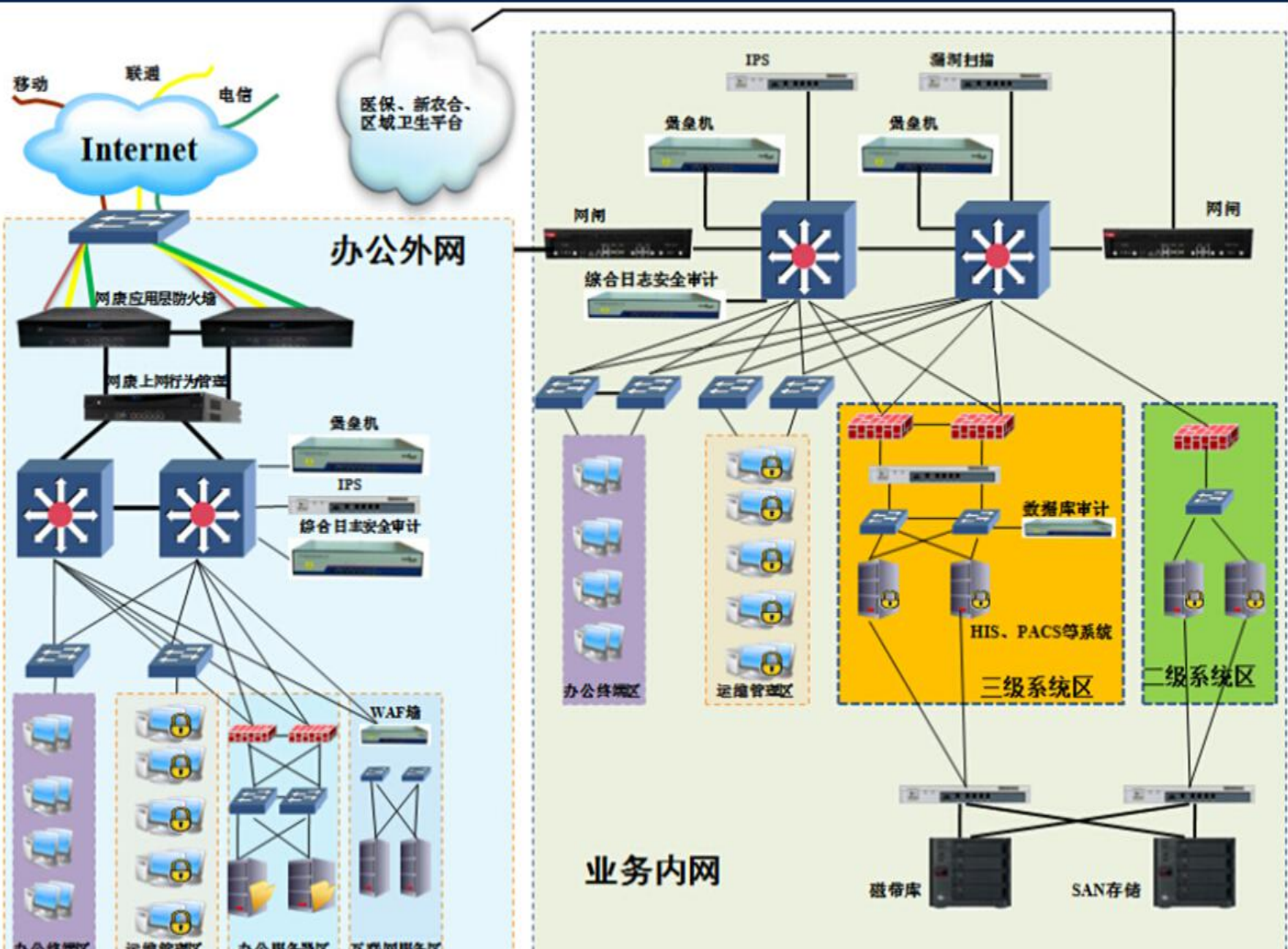
我们的运维与风险管理

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，把帐号与资产帐号相关联，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，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



网络拓扑图URL(BMC)

拓朴管理 -> 大连医大一院网络拓朴 (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

1#UPS				2#UPS			
工作模式	市电模式	UPS输出	UPS输出	工作模式	市电模式	UPS输出	UPS输出
R相电压	220.5V	电流 34.3A		R相电压	220.3V	电流 36.9A	
S相电压	220.8V	电流 49.9A		S相电压	220.1V	电流 48.7A	
T相电压	220.4V	电流 39.5A		T相电压	220.3V	电流 38.2A	
A相有功	9.0KW	视在 7.0KVA		A相有功	9.0KW	视在 8.0KVA	
B相有功	12.0KW	视在 11.0KVA		B相有功	12.0KW	视在 11.0KVA	
C相有功	10.0KW	视在 8.0KVA		C相有功	10.0KW	视在 8.0KVA	

1#精密空调	
回风温度	27.1°C 回风湿度: 37.2%
机柜状态	机柜开启
高级功能	<input type="radio"/> 制冷模式 <input checked="" type="radio"/> 除湿模式 <input type="radio"/> 加热模式

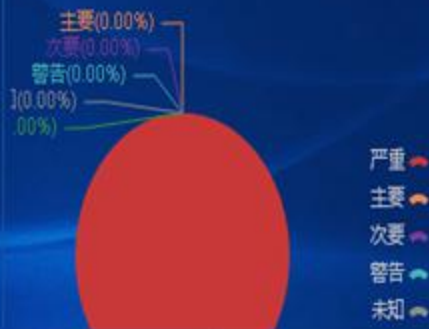
2#精密空调	
回风温度	26.6°C 回风湿度: 36.9%
机柜状态	机柜开启
高级功能	<input type="radio"/> 制冷模式 <input checked="" type="radio"/> 除湿模式 <input type="radio"/> 加热模式

时间	确认	事件名称	告警	设备名称	变量	报警内容	报警组	报警级别	报警值	恢复值
2016-04-27 20:06:35	-	报警	Modbus_COM_LAI...	空调-1#精密-压降门限报警	1号空调	100	1	-	-	-
2016-04-27 20:06:32	-	报警	Modbus_COM_LAI...	空调-1#精密-压降门限报警	1号空调	100	1	-	-	-
2016-04-05 11:01:21	-	报警	内部...	UPS-2#UPS-通信失败	2号UPS	100	1	-	-	-

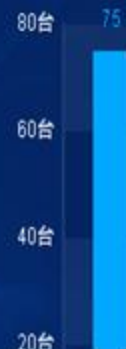
资源指标一览

状态	资源名称	IP地址	CPU利用率	内存利用率
●	San-Bu_ZY1_14F-1	172.16.1.149	30%	57.17%
●	YB-JG-4F	172.16.1.100	30%	60%
●	EB_3F_shoushushi	172.16.1.100	23%	48%
●	YB_2F_TD	172.16.1.100	22%	75%
●	YB-MZ-1F_1	172.16.1.100	20%	67%
●	YB-GRK	172.16.1.100	50%	74%

当前告警级别占比



资源数量排行(按设备类型)-TOP5



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。



大连医科大学附属第一医院

THE FIRST AFFILIATED HOSPITAL OF DALIAN MEDICAL UNIVERSITY

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



大连医科大学附属第一医院

THE FIRST AFFILIATED HOSPITAL OF DALIAN MEDICAL UNIVERSITY

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



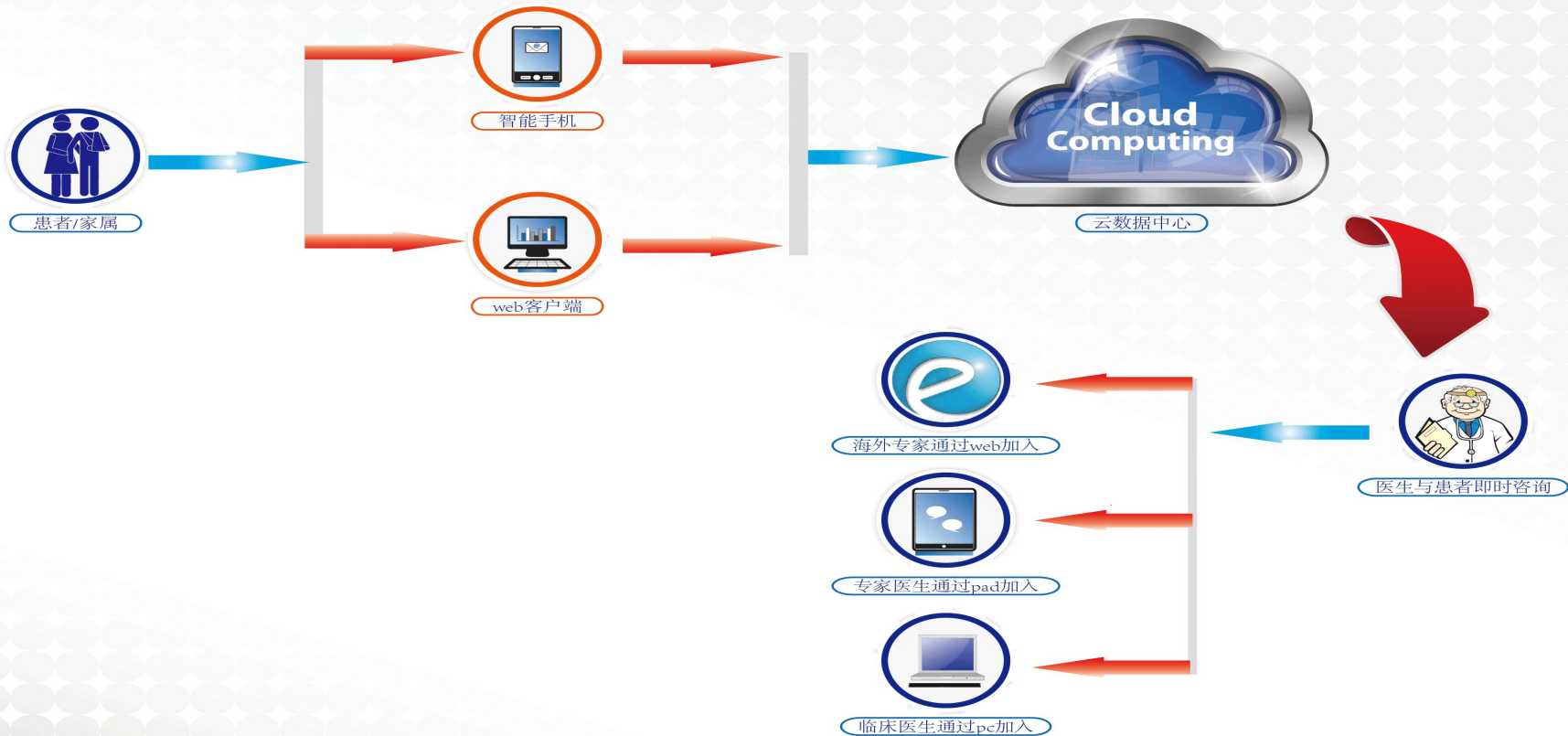
打造一个无地域限制的工作平台，实现院内数据融合互通、远程/移动会诊、远程/移动医嘱、HIS、RIS、LIS、CIS、PACS、CPR多平台数据整合、医学研究数据调研。



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



- (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



大連醫科大學附屬第一醫院

THE FIRST AFFILIATED HOSPITAL OF DALIAN MEDICAL UNIVERSITY

弘道篤行 精誠大醫

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

弘道篤行 精誠大醫

建设国内一流、国际知名的 医疗研究型大学附属医院

