新疆自治区人民医院
People’s Hospital of XinjiangUygur Autonomous Region

新形势下建立零信任网络安全实践和思考

彭建明

汇报大纲

1.新疆自治区人民医院简介

2.医院信息安全实践

3.建立零信任安全网络的思考

新疆自治区人民医院是新疆地区最大的三级甲等综合医院之一，编制床位2700张，年门诊量220万人，出院量16万人、手术（操作）量9万人。

目前自治区人民医院信息系统100多个，云平台，IBM小型机6台，两个虚拟化平台14节点、一个6节点超融合平台、PC服务器76台，存储阵列柜12多台，终端电脑5000多台(内网3000多台）。PDA 700多台，iPad 100多台，在病区无线网络全覆盖的基础上，通过PDA和iPad应用实现了所有核心医疗行为的闭环管理。

信息中心介绍

Lorem ipsum dolor sit amet, consectetuer adipiscing elit.

国家卫健委

六级电子病历（2016）

互联互通四级甲等（2019）

等保三级（2018）

HIC(艾力比)

全国排名第16名(2020)

信息中心组织架构

网络安全大事记

1. 2018年开始全国数量庞大的系统中勒索病毒，其中包括很多医院（上云医院）

2. 2018年比特币2万人民币左右，2021年4月比特币40万人民币

3. 一家单位22个ORACLE数据库同时坏

4. 一家安全做的很好的单位（等保2.0，专业维护团队），突然几台服务器中勒索病毒

- 密码滥用：2020年4月19日，云头条发布新闻：公司夏某工程师因为私自应用三甲医院数据库密码，运行开发数据库监控软件，导致HIS系统2小时无法正常工作，损失近800万，被判5年半。
- 黑客入侵：《法制日报》2017年披露：某部委医疗服务信息系统遭“黑客”入侵，超过7亿条公民信息遭泄露，8000余万条公民信息被贩卖。
- 数据被盗：2019年央视披露，温州某医院被外部人员盗取统方数据，通过U盘等方式拷走。

当前网络安全形式

1. 互联网+医疗 、医保、商保等应用使医院内网不再封闭，医院相对银行、证券、保险等行业，信息安全投入不足，技术力量相对薄弱，并且医院有大量有价值的数据，这些都是不法分子攻击医院的重要因素

2. HIS、LIS、PACS、EMR、手术麻醉、合理用药、院感、集成平台等信息系统越来越多，各个系统都互相联系，任何一个信息系统出问题都可能影响全院信息系统的稳定运行，甚至造成系统瘫痪

3. 信息技术越来越复杂，服务器、存储、交换机、云平台、虚拟化、集群、超融合， Linux 、UNIX、Windows ，现在信息系统安全性大幅提高，已不容易出事，但出事就是出大事，且问题很难处理。精通这么多技术几乎不可能

4. 医院电脑、PDA、平板、手机等终端设备越来越多，信息系统也越来越多且各个系统都互相关联，数据量越来越大，这些因素都会直接影响信息系统的稳定和安全。

5. 医院病毒越来越多，破坏性也越来越大，杀毒软件能防止一些病毒但对一些新病毒却无可奈何，同时杀毒软件可能会误杀一些文件，造成系统、数据库、或应用程序不可用

6. 信息系统流程优化是每家医院都很重视的工作，伴随着频繁的程序升级，由于程序功能繁多，很难进行严格的全面程序测试。升级也会导致信息系统无法正常使用。

医院网络安全压力

1. 医院是真正7*24小时不间断运行的信息系统

2. 互联网+医疗、智慧医院建设，提高患者和医务人员感受的同时，网络安全压力巨大

3. 医院信息安全投入、人员技术水平、责任心还不能确保网络安全

4. 传统网络安全架构已不能适应网络安全发展的需要（零信任网络）

2018年信息规划

网络安全现况

互联网+医疗开展医院有了很多互联网应用服务器，有的服务器是第三方公司提供的、有的是银行提供、医院买的……这些服务器都是单点故障

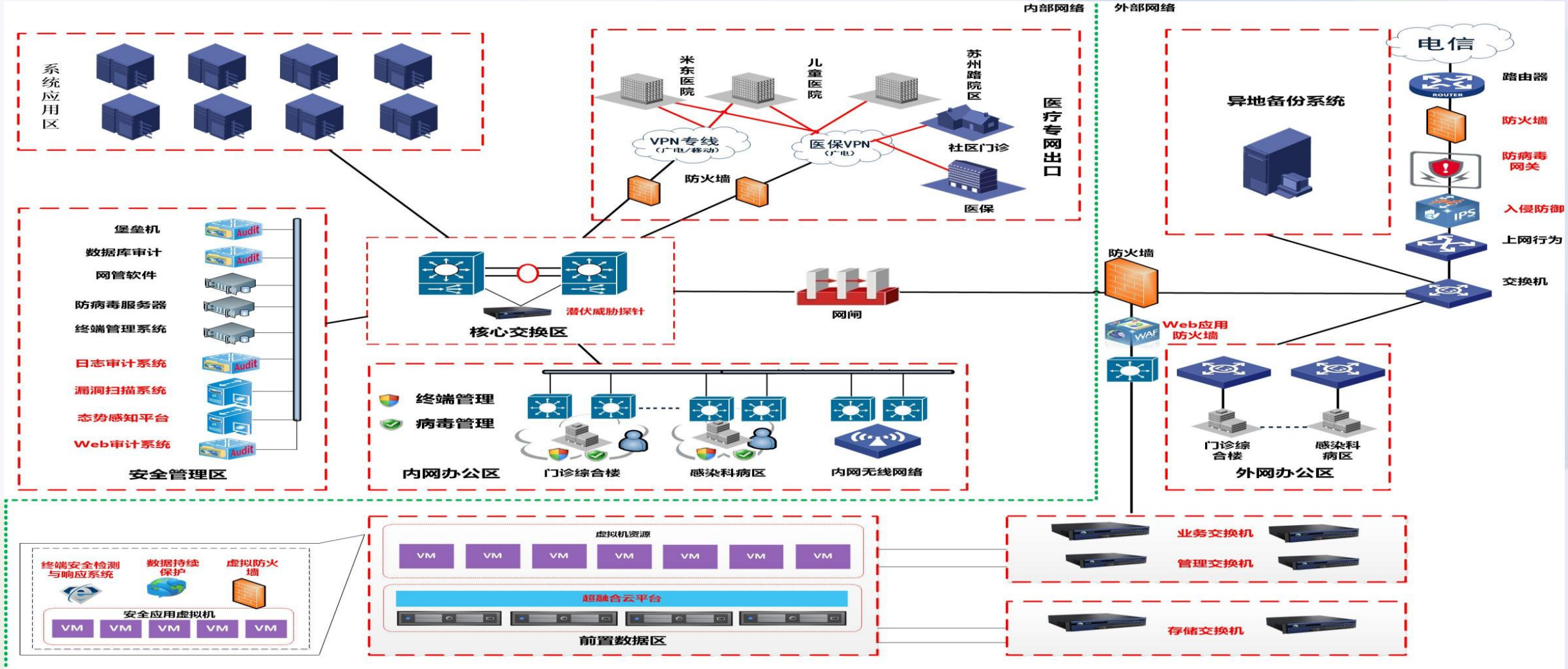
网络安全环境混乱，医院有一堆小防火墙 ，没有系统整体安全防护

服务器上架没有整体规划，混乱，安全程度低，维护困难

网络安全规划

希望建立一个理论上硬件没有单点故障的安全网络环境,并且通过国家等保三级

2018-2020安全计算环境



安全设备.防火墙

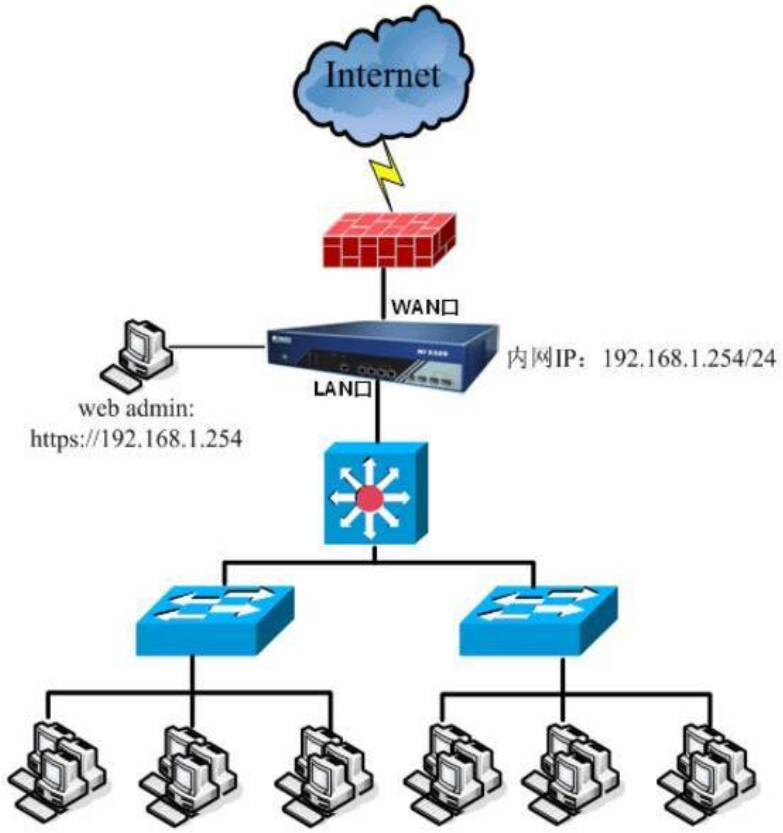
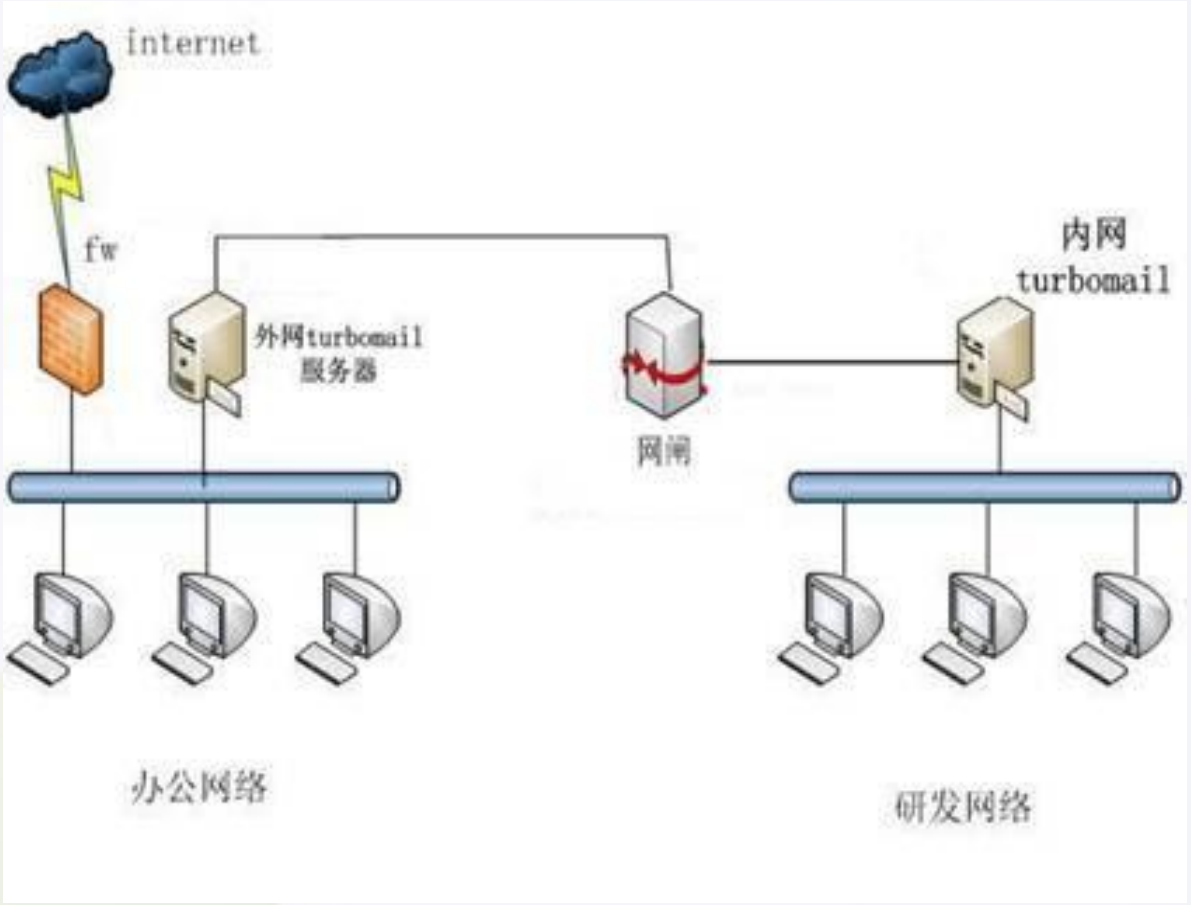


图 2 - 3 网关模式下网络拓扑实例图

数据从Internet经过防火墙进入业务内网

1. 防火墙首先使用ACL进行数据包过滤，合规的数据通过
2. 进行严格状态化监控，主要是TCP、UDP、ICMP协议
3. 利用互联网相关协议对数据包内容进行匹配，检查数据是否合规
4. 可以防止一些已知的威胁，不能保证网络绝对的安全
5. 防火墙工作在网络层，直接进行数据包转发

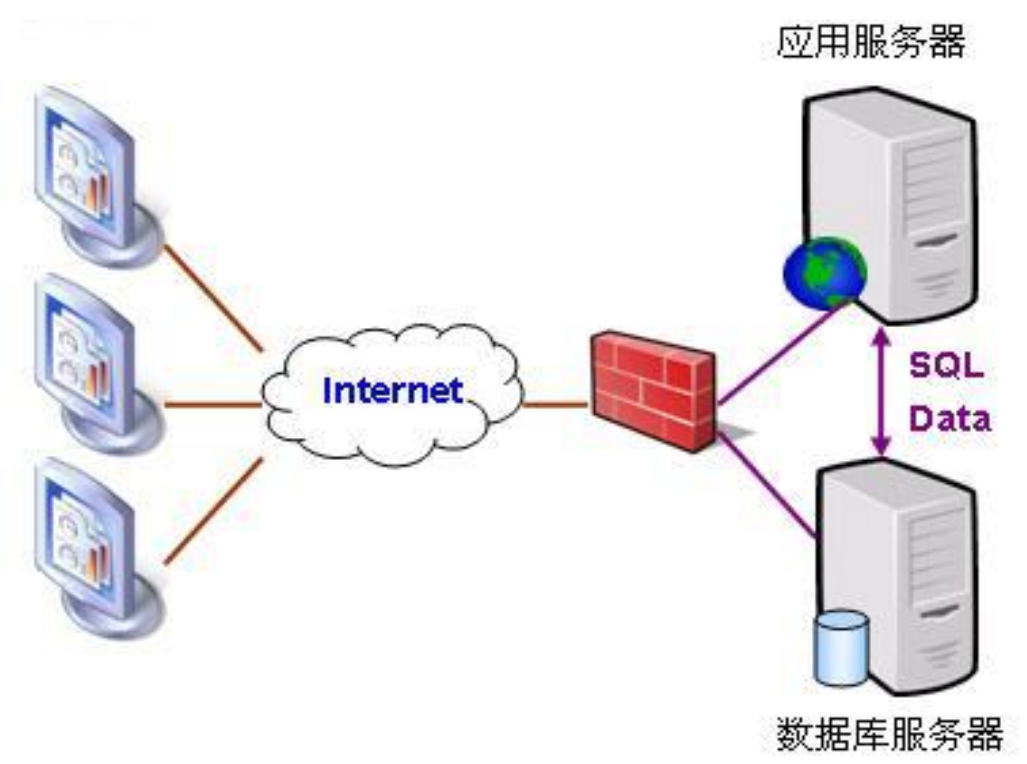
安全设备.网闸



数据从办公外围经过网闸进入研发内网

1. 外网办公数据首先达到网闸外网处理单元,被剥离IP数据封装,只留原始数据
2. 通过防病毒、入侵检测模块对原始数据进行检查
3. 通过预先设置白名单，过滤规则等安全策略进行检查
4. 通过摆渡技术（类似U盘拷贝）把外网办公数据传送到研发内网
5. 网闸工作在应用层，所有数据需要落地转换，完全屏蔽内部网络信息；

网络安全经验



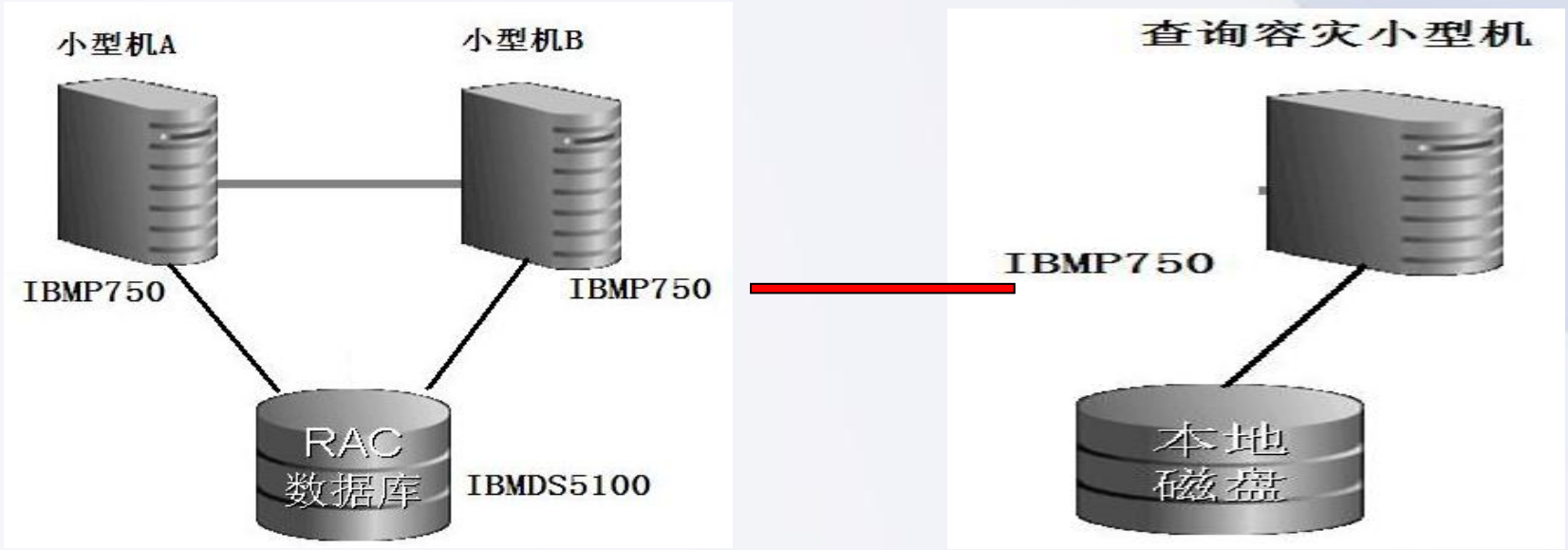
广泛使用LINUX操作系统及功能

1.WINDOWS 如果可能都换成LINUX

2.CS架构ORACLE数据库服务器， CS两层架构升级为CS三层架构（性能安全大幅提升）

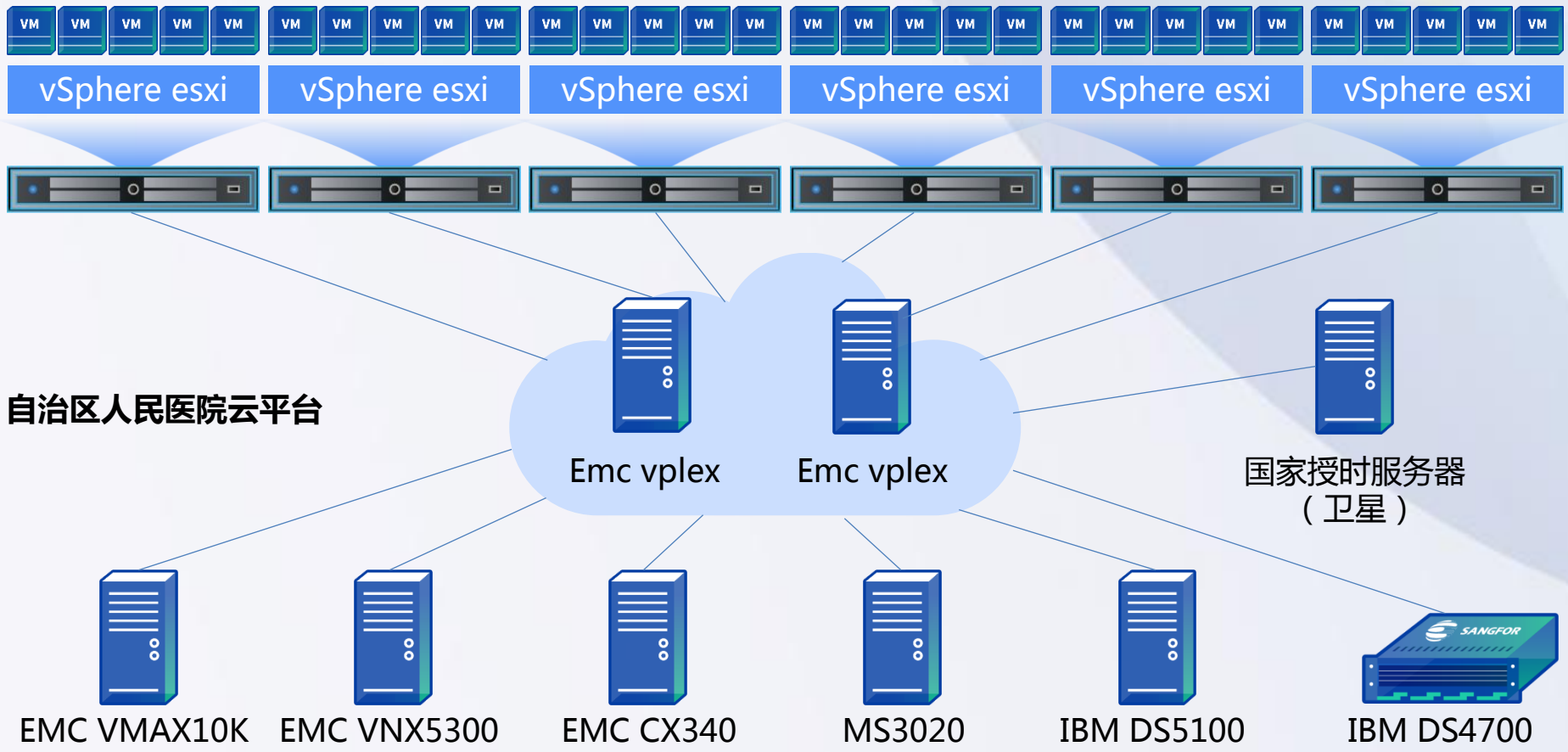
3.LINUX LVM、 XFS等功能应用

高性能平台HIS系统



HIS系统2004年至今 3T数据库
11G RAC +IBM AIX 小型机平台 2012年至今　性能良好
计划2022年迁移到LINUX

2012年
2018年



没有单点故障的高度安全网络环境

云平台定义：是指基于硬件资源和软件资源的服务，提供计算、网络和存储能力

2012年 医院建设第一个云平台VMWARE

2018年 医院建设第二座云平台VMWARE

目前平台资源 14台高端PC服务器 12T内存 12台存储 1500T容量

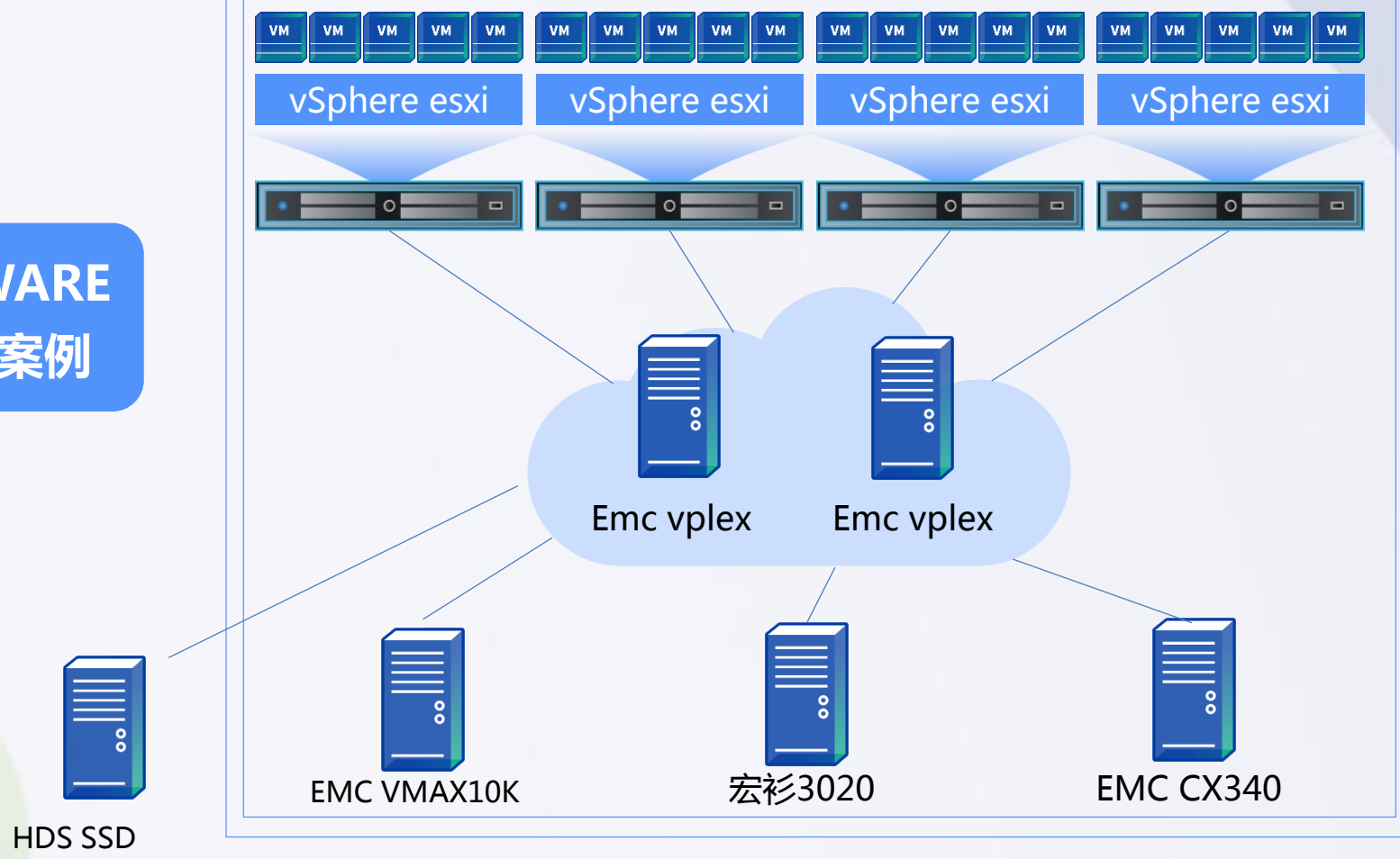
（主要存储日立全闪存、EMC VMAX10K、EMC VNX 5300、EMC CX340

IBM DS5100 IBM DS4700 MS7000G2 MS3000G2等）

核心内网业务除HIS系统全在云平台上运行

VMWARE 应用案例

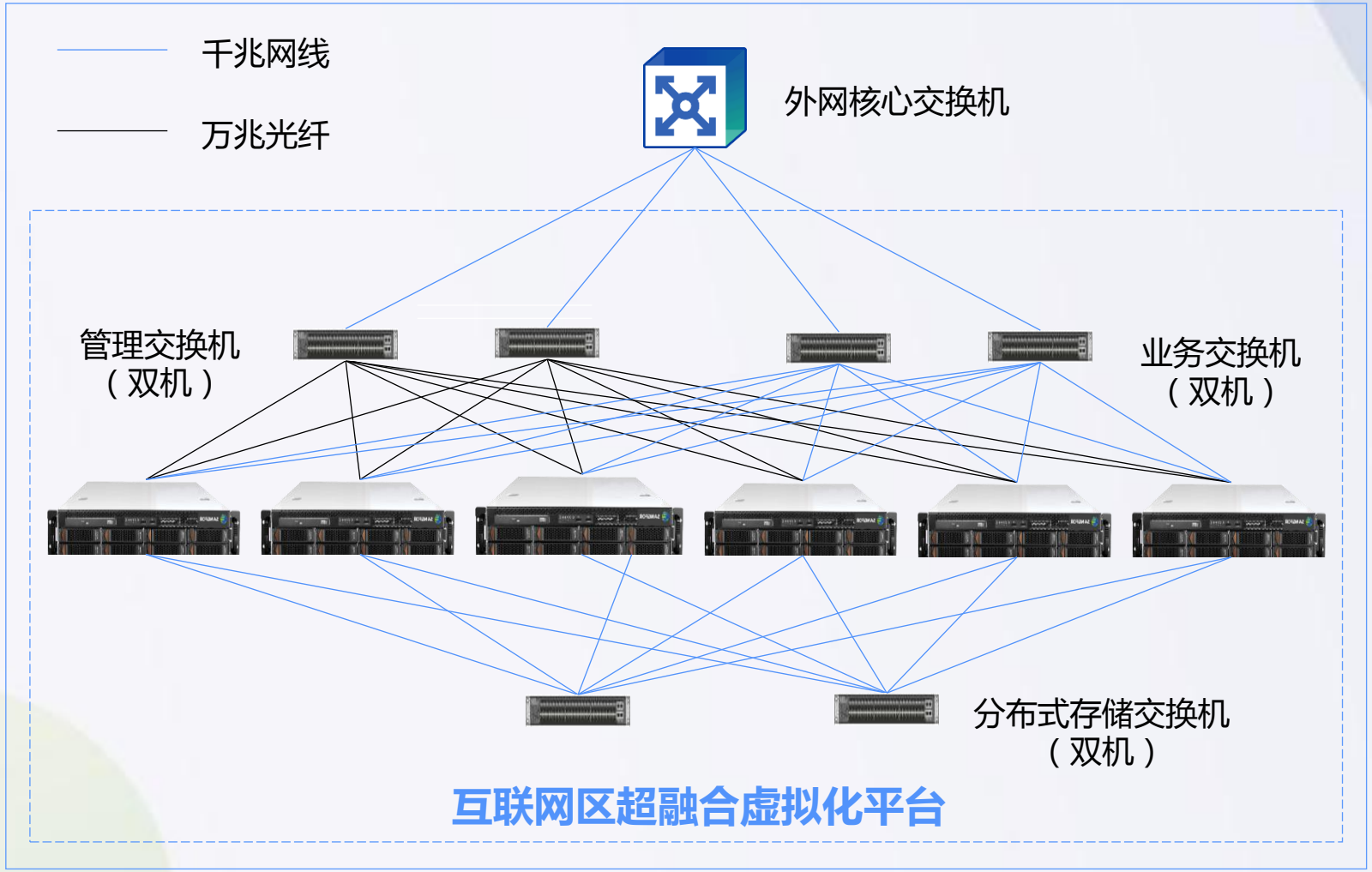
云平台应用案列



两套PACS性能优化

- 业务连续性（linux免费操作系统）
- 减少盘符，实现存储的三级架构，且可以根据需要动态扩展（lvm xfs）
- 充分利用存储设备

互联网区超融合实践分享



资源池规模：

8节点，总共提供322vCPU，4T内存，20TSSD高速缓存空间，100TSATA存储（双副本）。

承载业务系统：

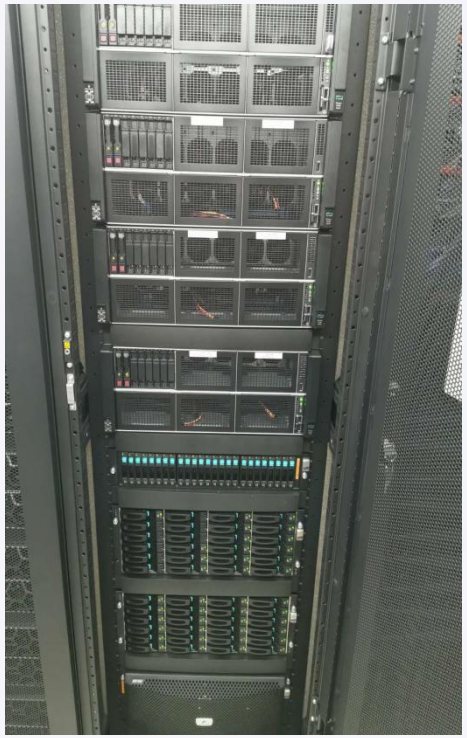
平安预约挂号、健康卡、微信体检、银医二期、慢病管理等336套业务系统。

2019年改造完成

核心业务机房

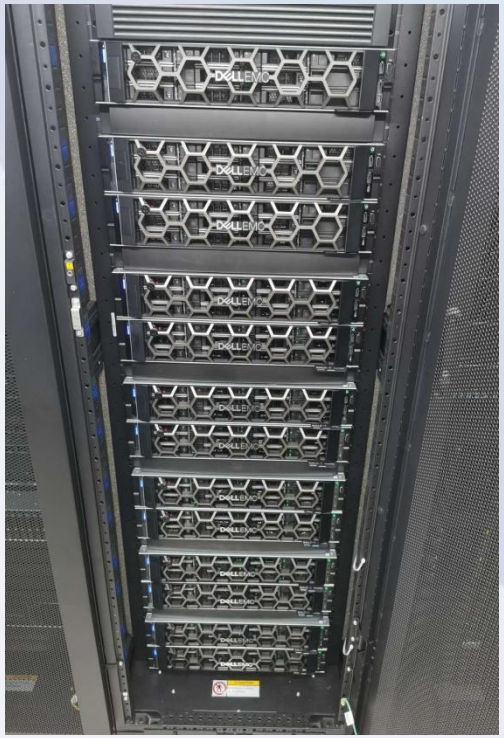
DMZ机房

2019年改造完成



VMWARE

HCL

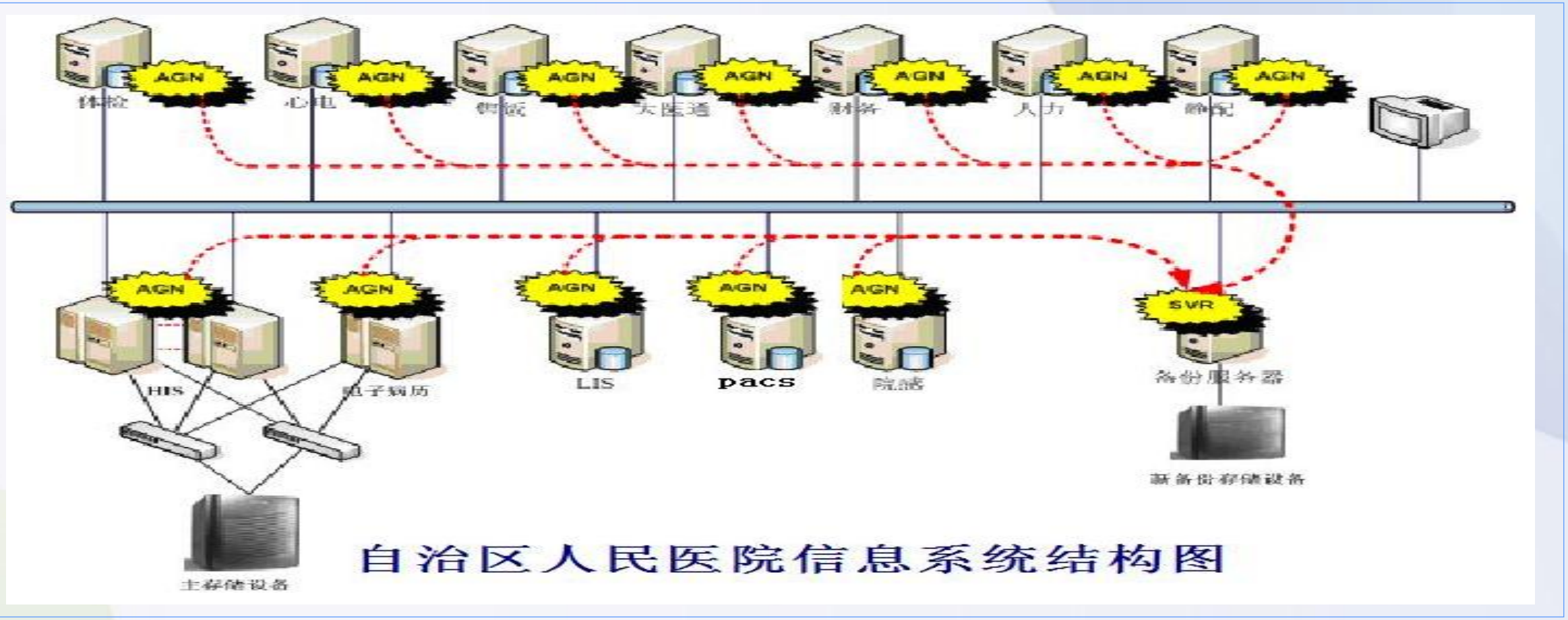


HADOOP

安全介绍

Lorem ipsum dolor sit amet, consectetuer adipiscing elit.

新疆自治区人民医院备份平台



安全介绍

Lorem ipsum dolor sit amet, consectetuer adipiscing elit.

新疆自治区人民医院经过三年建设2018-2020

三区两道防线、三级等保

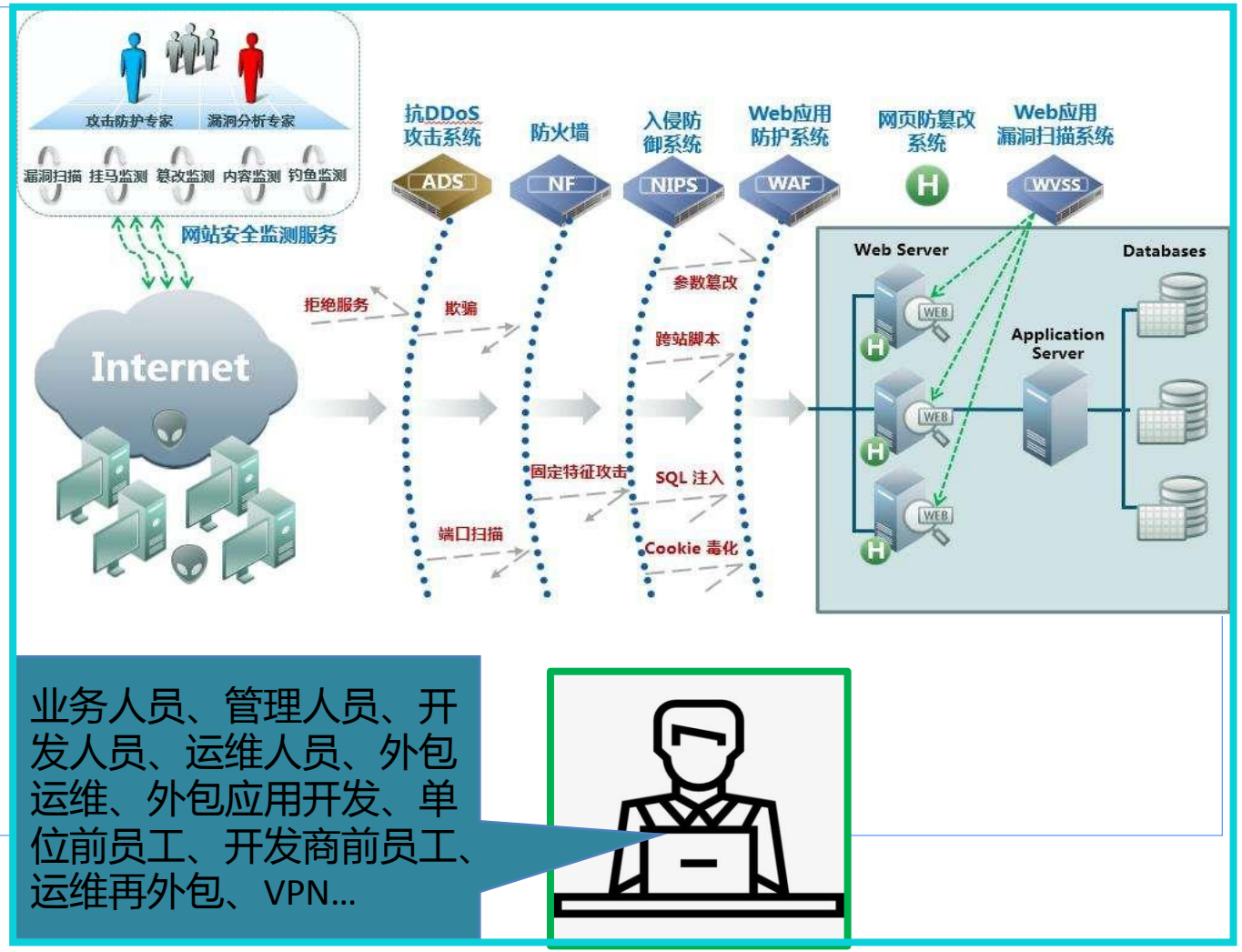
整个网络环境没有单点故障

网络已经很安全了吗？

安全介绍

Lorem ipsum dolor sit amet, consectetuer adipiscing elit.

网络马奇诺防线：网络边界安全VS.内部安全



业务人员、管理人员、开发人员、运维人员、外包运维、外包应用开发、单位前员工、开发商前员工、运维再外包、VPN...

安全介绍

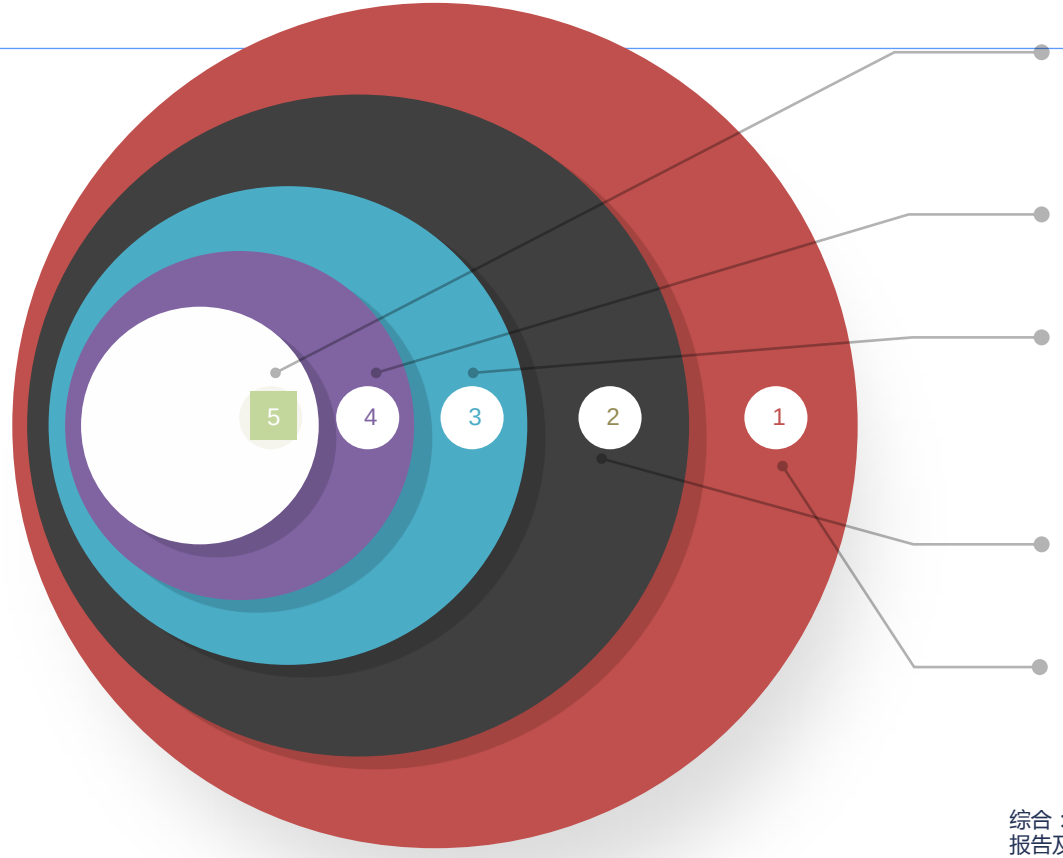
Lorem ipsum dolor sit amet, consectetuer adipiscing elit.

90%

绝大部分的精力和投资用于最外层的网络安全防护。

10%

仅有少量精力和投资用于防范误操作、内部泄露、内部犯罪、内部篡改等数据安全运维。



5% 人员故意的犯罪

11% 方案不完善、管理漏洞、资金不足造成的安全风险。

24% 系统原因如设备故障、防护失效等造成损失和泄露。

27% 人为失误造成的损失或者泄露

33% 网络报道的外部攻击事件

综合：Source: IBM&Ponemon 2018年度数据泄露成本分析报告及其他网站分析报告。

面临挑战：用10%的预算抵御67%的风险

安全介绍

Lorem ipsum dolor sit amet, consectetuer adipiscing elit.

零信任网络安全

2010年，零信任网络安全概念正式出现

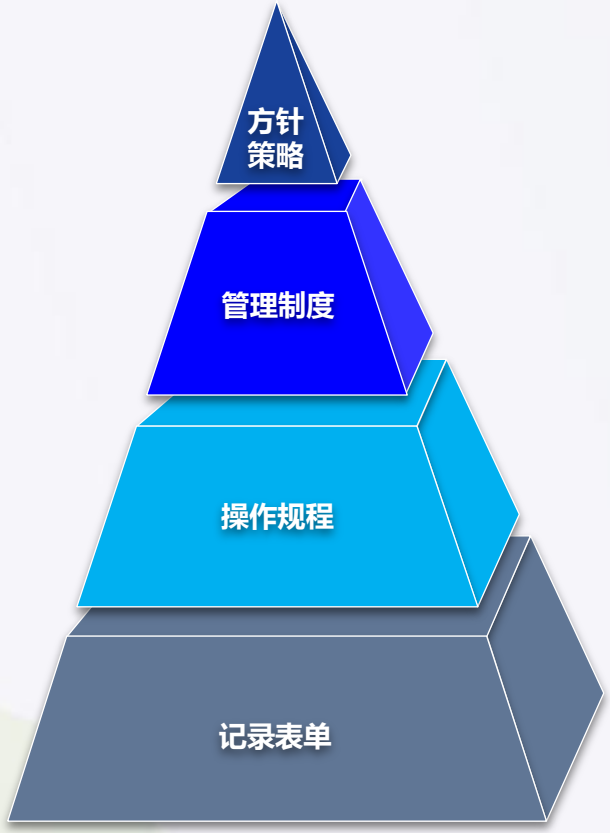
2014年，Google构建零信任网络

零信任网络安全五个准则

- 网络无时无刻不处于危险的环境中；
- 网络中自始至终存在外部或内部威胁；
- 网络的位置不足以决定网络的可信程度；
- 所有的设备、用户和网络流量都应当经过认证和授权；
- 安全策略必须是动态的，并基于尽可能多的数据源计算而来。

零信任网络安全将颠覆传统网络安全

总结



三分技术七分管理

- 信息中心下面成立了网络安全管理科
- 制定了安全管理方针和制度
- 做好有效的数据备份
- 严格按照制度执行运维
- 加强网络安全技术人才培养
- 通过科学管理手段提高运维效率

抬头看天是一种方向，低头看路是一种清醒

总 结

世界上没有绝对安全的方案

一定要加强管理，一定要做好异地备份