

重新定义规划，安全可靠新方案

锐捷网络医疗行业部

陈献文19905910178

2020-3-31



目录



Part One

锐捷在医疗



Part Two

医疗行业
现有业务挑战



Part Three

锐捷医疗
NBAI一键护航方案



- 锐捷网络，中国数据通信解决方案提供商，作为**国家首批“创新型企业”**的代表，锐捷网络拥有**6**个研发中心，**41**个分支机构（不含海外），业务范围覆盖**50**多个国家
- 截至2020年1月，锐捷智慧医疗解决方案已服务于全国**4000余**家医院，在全国三级甲等医院应用**500**余家，占据三级甲等医院**30%**以上市场份额
- 区域卫生信息化解决方案已经在**40**余个省及市卫生信息平台规模应用
- 2015-2019**连续5年**企业级终端VDI市场排名**第1名**（数据来源：IDC）
- 2019年中国IT综合运维软件ITIM市场占有率**第1名**（数据来源：IDC）
- 中国移动医疗无线解决方案市场占有率**第1名**（数据来源：CCW）

锐捷医疗在百强医院

Ruijie Networks 锐捷

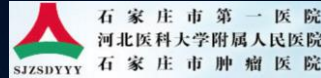
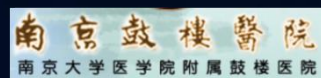
全国百强

60%



省会市属百强

50%



地市百强

45%



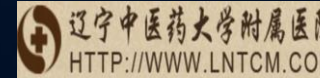
县级百强

40%



中医百强

40%



目录



Part One

锐捷在医疗



Part Two

医疗行业
现有业务挑战



Part Three

锐捷医疗
NBAI一键护航方案



1、如何应对疫情后期物联网增长态势



IBM ↑ 18%

安全准入

安全防护

新型智能终端以年18%
的增速涌入网络

通过攻击IP溯源，发现攻击源居然是该医院的一台胶片打印机。这台放置于医院一角的终端，用于给病人打印病历和检查结果，没有安装杀软，自身染毒并通过“永恒之蓝”漏洞在内网不断扩散病毒。



图片来源：火绒

该医院网管员表示，这台设备没有输入设备，无法操作部署安全软件，而且作为每天都在用的业务设备，无法单独断网隔离。

2、买了那么多的安全设备，还是防不好



图例

万兆链路	——
千兆链路	——
备用万兆链路	- - - -
备用千兆链路	- - - -
广域网链路	——

内网安全裸奔，安全防护失效

ZK统计,80%的有效攻击来自内网



1、web防火墙

2、数据库防火墙

3、网络防火墙

4、网络审计

5、数据库审计

6、运维审计

7、主机安全审计

8、入侵防御设备

9、防毒墙

10、上网行为管理

<https://www.secspace.com/view-...> - 百度快照

[医院屡遭勒索病毒攻击,医疗系统内网安全该何去何从? 腾讯新闻](#)

2019年11月24日 - 近年来,针对医疗系统的网络安全风险和网络安全攻击一直呈现持续上升态势,整个医疗...完善医院的信息化建设,保证重要数据完整、内网核心业务连续,构筑医疗...

<https://new.qq.com/omn/2019112...> - 百度快照

[医院内网出现病毒 真相让人大跌眼镜-PChome](#)

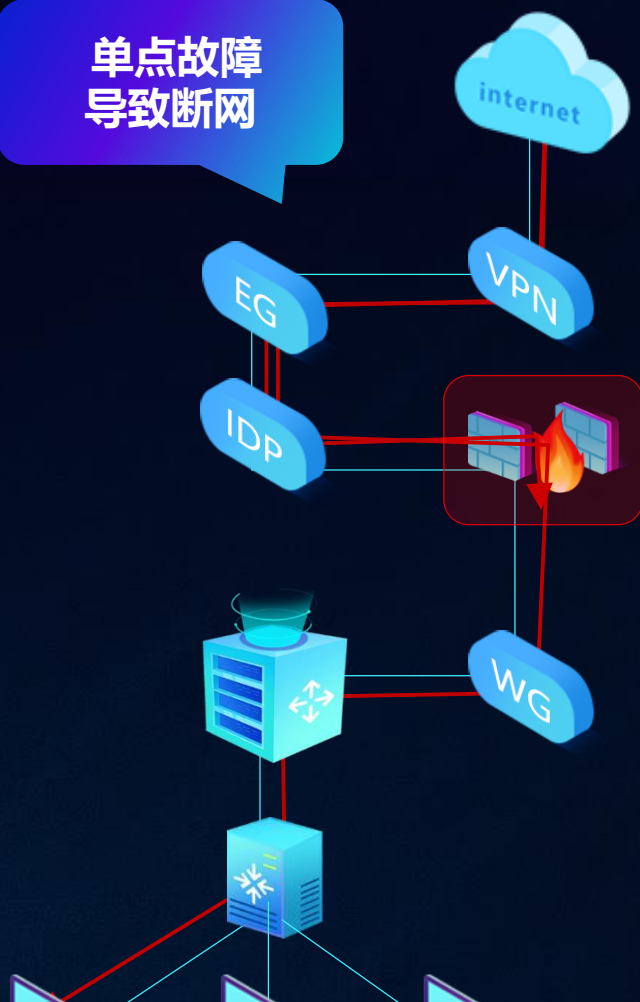


2019年1月31日 - 原题:医院内网病毒屡杀不止 竟是胶片打印机传播 只有你想不到的攻击点,没有黑客做不到。据火绒安全团队发出的真实攻击案例,浙江某医院许多办公电脑...

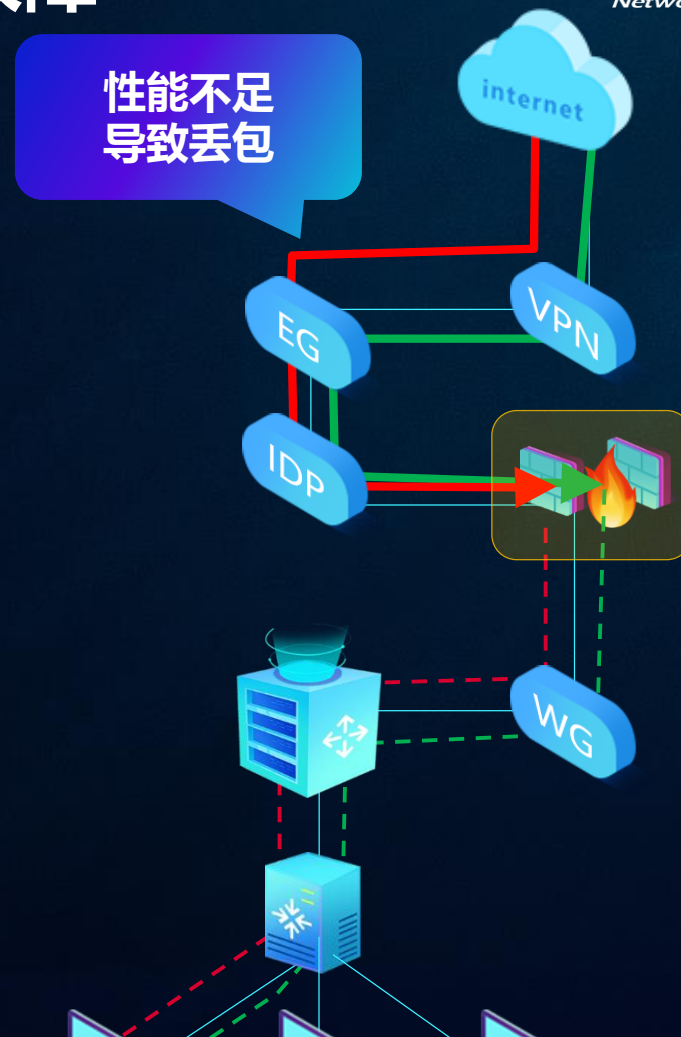
<https://article.pchome.net/con...> - 百度快照

3、“糖葫芦串”部署—单点或性能故障

单点故障
导致断网



性能不足
导致丢包



等保2.0建设，客户需再新购置大量的安全设备，导致更为严重的单点故障的发生

4、县乡远程医疗网络问题



建网效率成本



关键业务保障



后期简化运维

目录



Part One

锐捷在医疗



Part Two

医疗行业
现有业务挑战



Part Three

锐捷医疗
NBAI一键护航方案



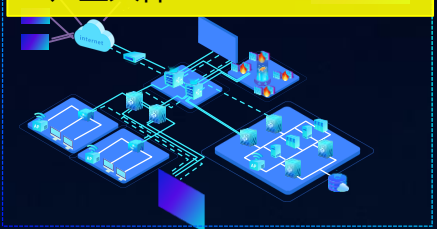
医院NBAI一键护航方案组件

Ruijie锐捷
Networks

8、远程会诊：5G+IDV



9、医共体：5G+SDWAN



10、IOT联网：5G+救护车



5、安全协防与资源池

6、安全与运维管控中心



2、医疗物联网与移动医护

1、即插即用承载网

3、云桌面(IDV)

4、双活数据中心

网络业务以**一键**为指导思想、去帮助用户构建一张**安全、可靠、合规、成本低、易上手**的网络

1、基础网络规划



基础网络：业务即插即用，网络永不调整

Ruijie锐捷
Networks



目的地网	无线网络	无线网络1	演示无线网络
源子网			
无线网络		✓	✓
无线网络1	✓		✓
演示无线网络	✓	✗	



多业务/多网融合

可视化虚拟网络权限调整

业务即插即用/盲插

虚拟承载网



SNMP

NETCONF/YANG

TELEMETRY

外网

内网

设备网

多网融合或者物理隔离



2、桌面建设规划



锐捷与Intel建立联合桌面创新实验室



Technical Support
技术支持



Innovation
联合创新



New business incubation
新业务孵化



Business operation
商务合作



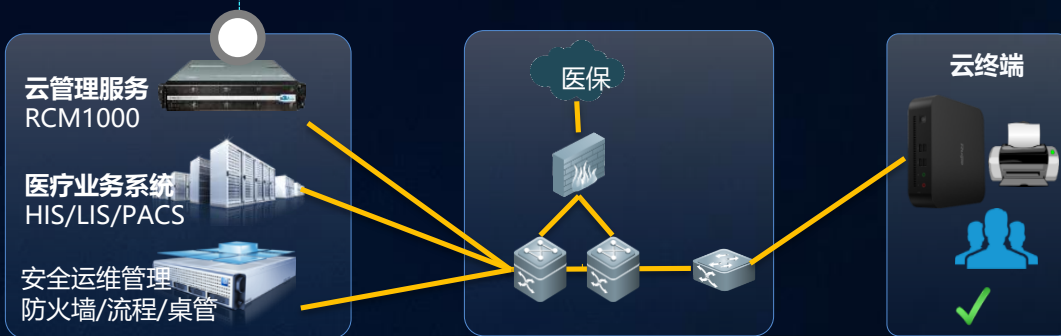
Co-marketing collaboration
市场合作

锐捷携手Intel，推动中国桌面云化进程

医疗云办公方案-集中管理，分布式计算

Ruijie锐捷
Networks

医院生产业务、固定工位办公等场景



主推IDV方案架构设计



系统镜像管理



配置一键恢复

管理

集中管理、分布式计算

计算

高性能终端

软、硬件全兼容

云管离线可用



IDV方案架构设计核心价值

方案：更可靠、性能强、简运维

- 可靠性比PC、VDI更优!
- 性能、业务支撑与PC一致，比VDI更优!
- 操作系统兼容与VDI一致，比PC更优!
- 运维管理与VDI一致，比PC更优!

特色：

- 支持wifi，业务即插即用
- 弱网/断网可用，用户体验好
- 显卡透传，支持XP,WIN7
- 预设WIN黄金镜像，省成本，更安全
- 低功耗省电，更稳定，节约成本
- 一键业务管理，降低重复性劳动

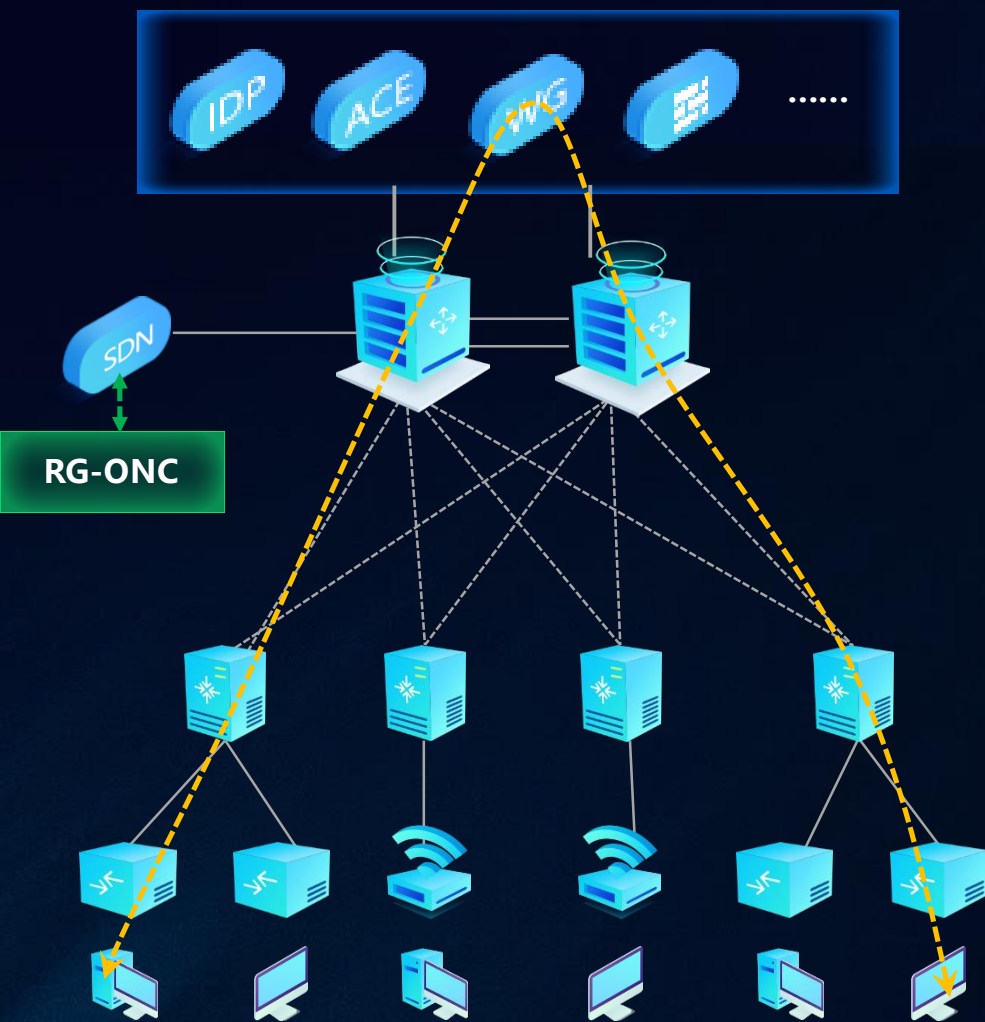
3、安全建设规划



安全方案的设计的核心思想



内网引流方案1:基于SDN横向业务调度

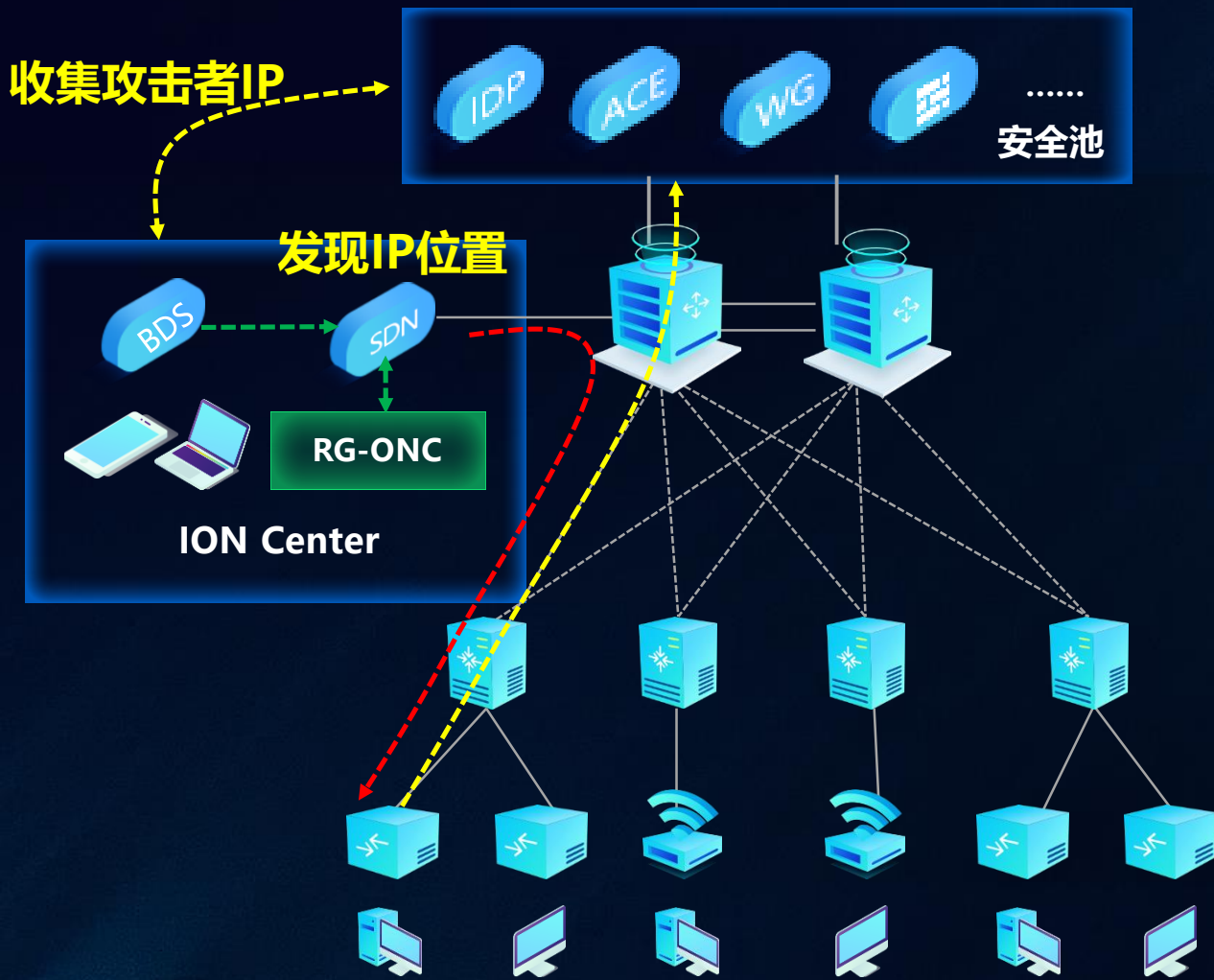


系统逻辑

- 1、接入汇聚上开启端口保护，杜绝横向传播。
- 2、核心上通过SDN的Openflow协议把东西向流量都引入安全设备
- 3、横向流量通过图形化操作顺利引流至防火墙
- 4、如果有二层横向访问诉求：接入上可以更换成支持多业务保护口的接入交换机（29EV3等设备）

安全协防：内网流量无法防护问题，导致恶性病毒任意泛滥

安全协防-SDN&安全大数据联动



✓ 安全威胁感知

BDS/蜜罐诱捕机制等实时监测网络安全威胁。

✓ 秒级边缘阻断

发现威胁后根据告警等级进行评估是否阻断。由策略引擎下发策略，在接入上做安全隔离，秒级。解决内网安全无法阻断问题。

✓ 边界安全资源联动

根据需要，将内网攻击者的横向攻击的流量模型强制引流到安全资源池进一步分析处理，建立联合防护，同时也提高了传统安全产品利用率。

✓ 安全溯源

秒级发现攻击路径、评估攻击区域，全网安全态势实时感知。

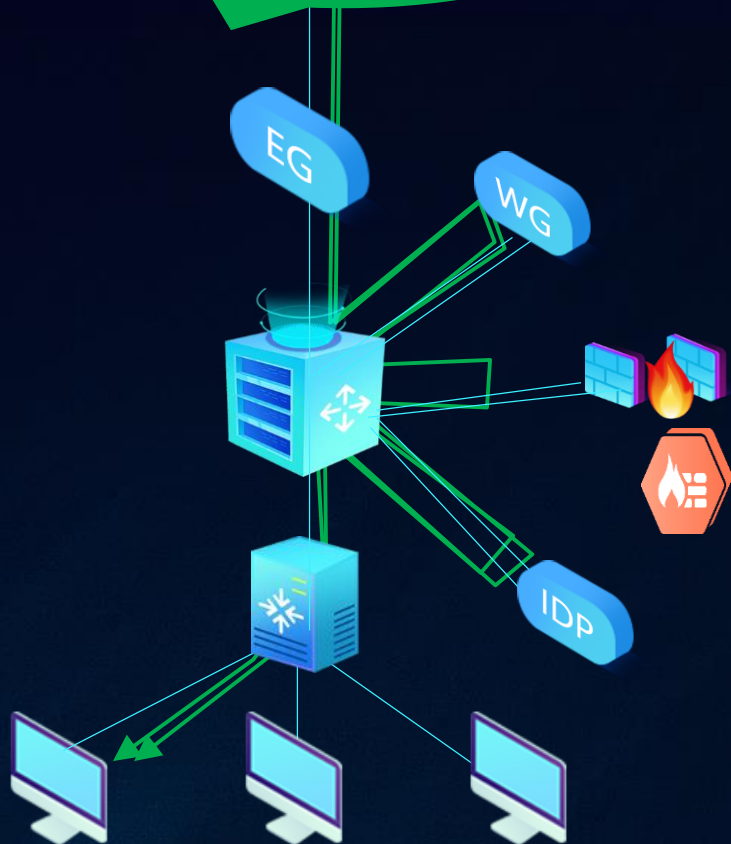
✓ 移动安全

高危安全攻击事件通告至微信，一键隔离&恢复，问题发生即问题发现，把影响降到最低。

安全池化-逻辑串接，物理旁挂

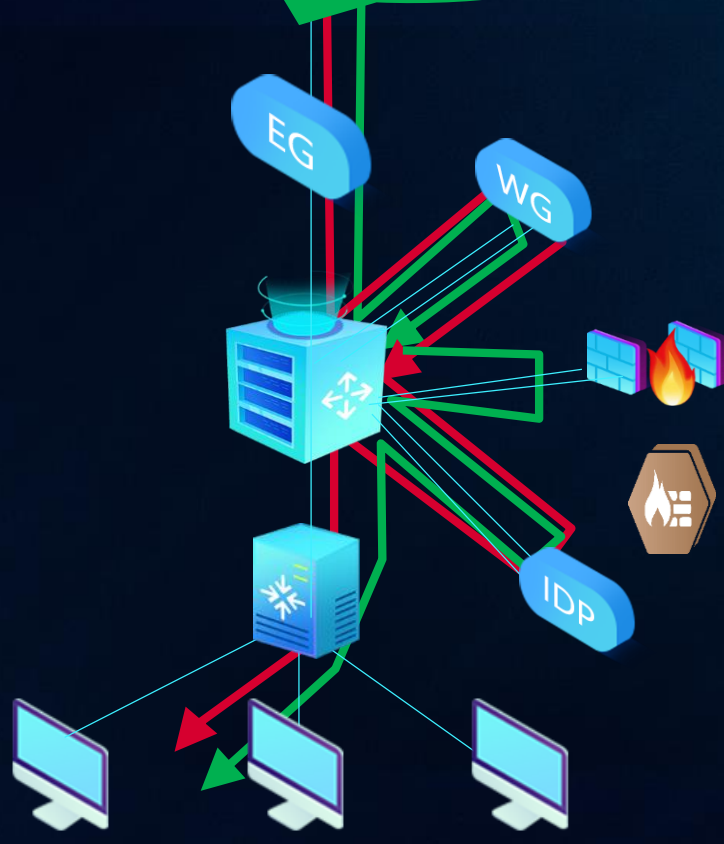
Ruijie锐捷

防火墙故障，故障
自动bypass不断网



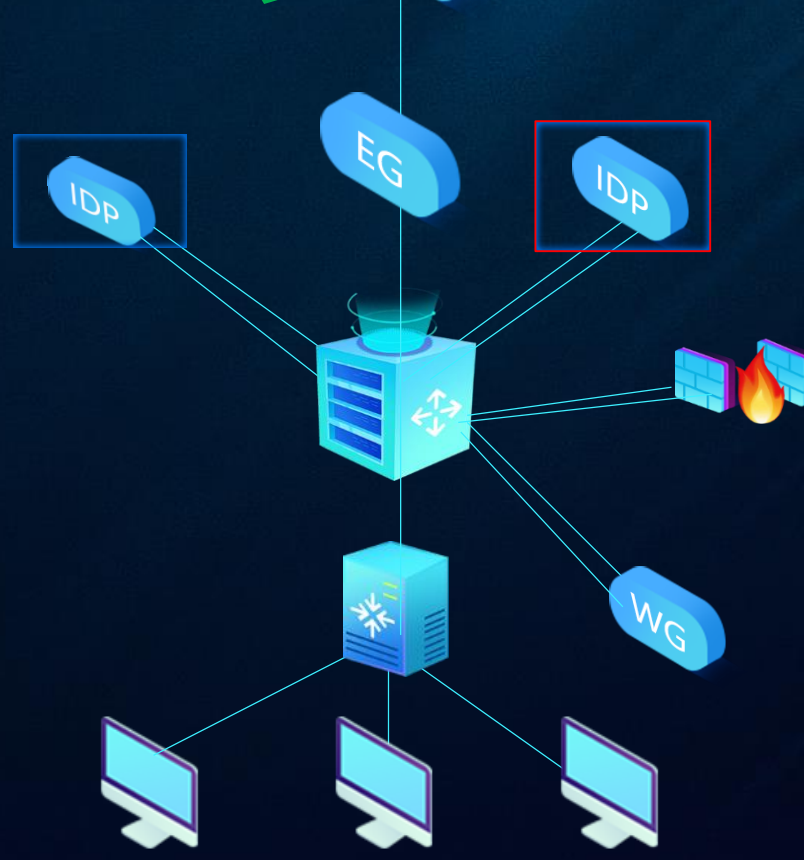
场景一

按需引流，保护
性能，不丢包



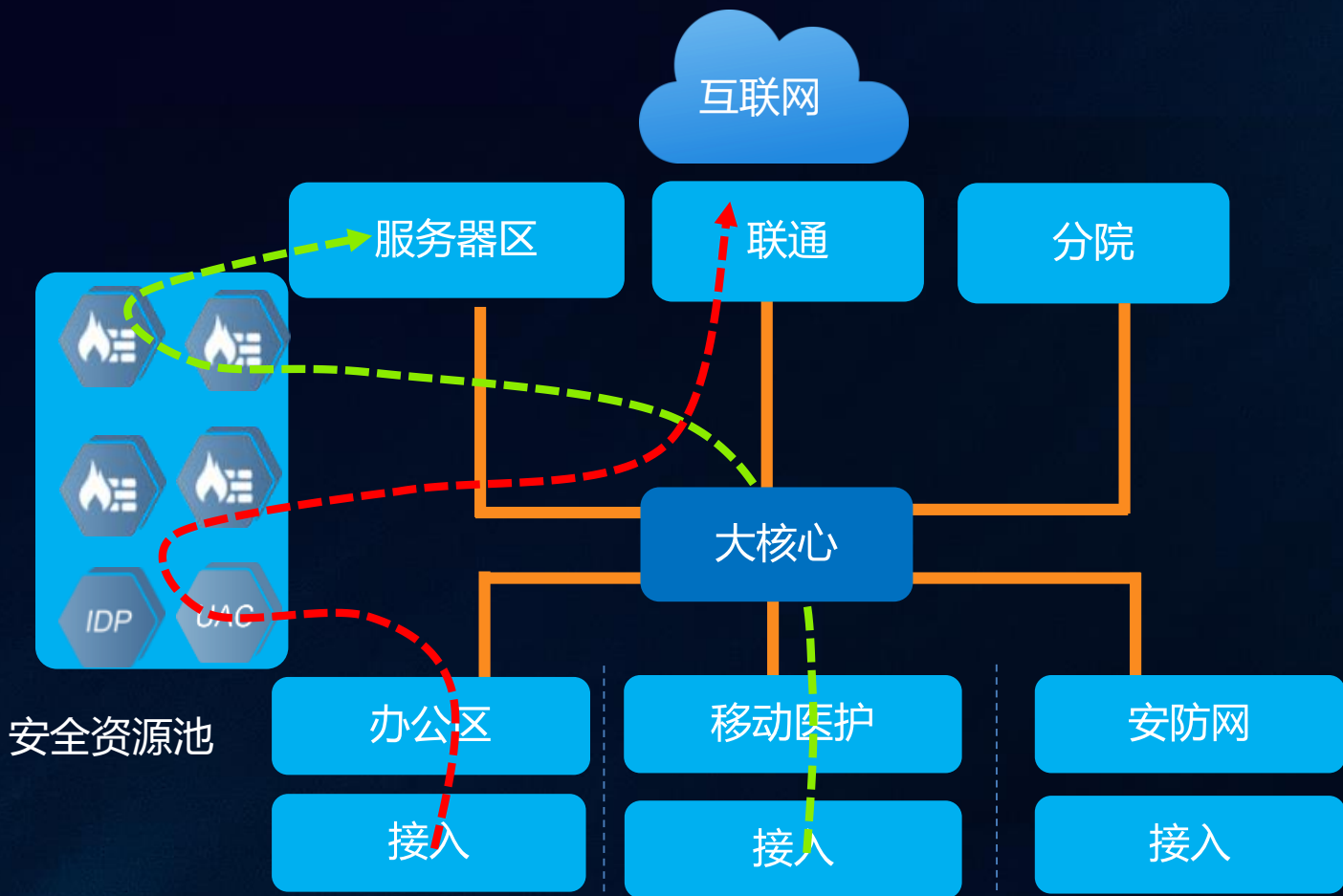
场景二

跨品牌负载均衡提
供冗余备份



场景三

安全池化-逻辑串接，物理旁挂



1、安全资源池化，安全按需编排

2、智能Bypass，消除单点故障

3、开放，兼容第三方安全设备

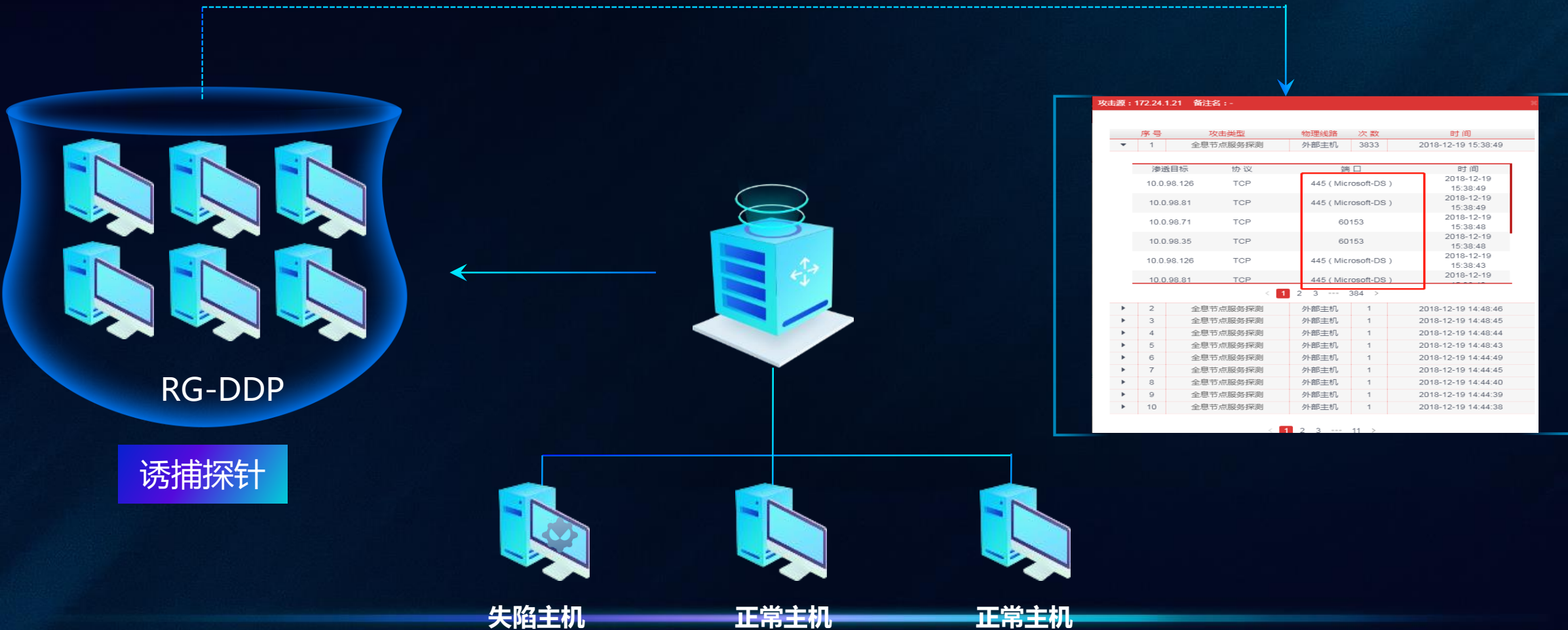
4、异构安全，避免重复投资

资源池价值：降低重复性产品投入，提高安全异构的情况下，保证可靠性不变

内网安全防护-安全蜜罐-未知安全动态防御

动态防御：扩大攻击面、延长被攻克时长，降低攻击成功概率

虚拟出大量的虚拟主机ip地址，增加攻击扫描难度

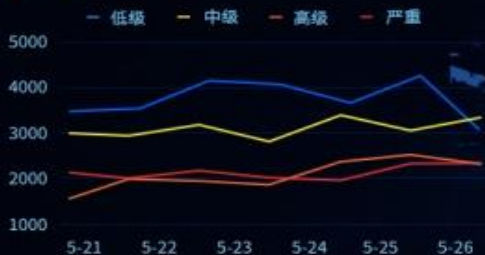


内网溯源：基于态势感知的安全溯源

Ruijie锐捷
Networks

Ruijie 大数据安全平台

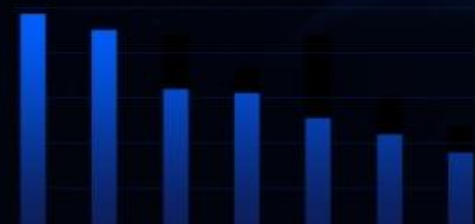
>> 内部外联趋势



>> 木马回连



>> 邮件发送排行



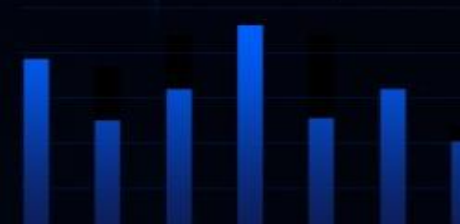
>> 连接吞吐排名



>> 威胁情报命中排名



>> DGA域名检测分布



攻击类型

攻击时间

攻击者

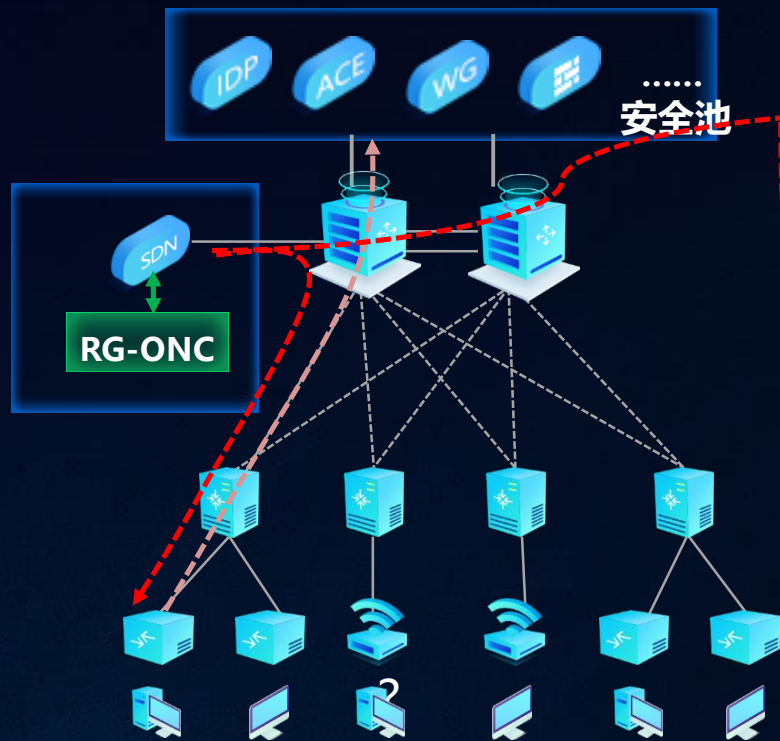
被攻击者

名称	时间	级别	源地址	类型	目的地址	端口	协议类型
CnC Callback IP	2018-05-25 12:33:42	严重	12.3.4.15	网络攻击	100.16.25.3	80	TCP
CnC Callback IP	2018-05-25 12:33:40	高级	12.3.4.15	信息破坏	100.16.25.3	80	TCP
CnC Callback IP	2018-05-25 12:30:22	严重	12.3.4.15	网络攻击	100.16.25.3	80	TCP
CnC Callback IP	2018-05-25 12:33:42	严重	12.3.4.15	威胁情报	100.16.25.3	80	TCP
CnC Callback IP	2018-05-25 12:33:42	中级	12.3.4.15	网络攻击	100.16.25.3	80	TCP

可视化、安全溯源更简单、更全、更准

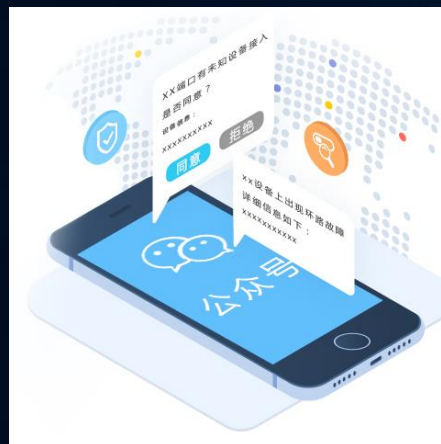
内网防护：基于SDN技术重新定义医疗准入

1、NBAI智能审批制主动推送流程秒级完成准入同时。



☐	终端名称	IP地址	MAC地址	VLAN	接入位置	原因	厂商	创建时间	更新时间	操作
☐		192.168.195.241	00:8c:fa:ed:95:d1	195	192.168.195.4[Gi0/17]	IP冲突	INVENTEC Corp...	2018-03-19 16:47:19	2018-03-19 17:24:30	☒ ☐ ☐
☐		192.168.195.43	00:21:cc:72:78:88	195	192.168.195.4[Gi0/17]	IP冲突	Flextronics Ltd...	2018-03-19 15:23:03	2018-03-19 15:56:44	☒ ☐ ☐

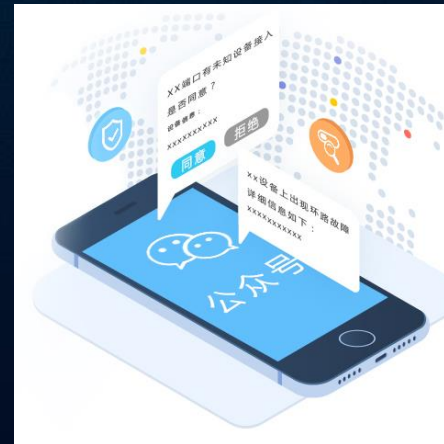
小张



小王



小李



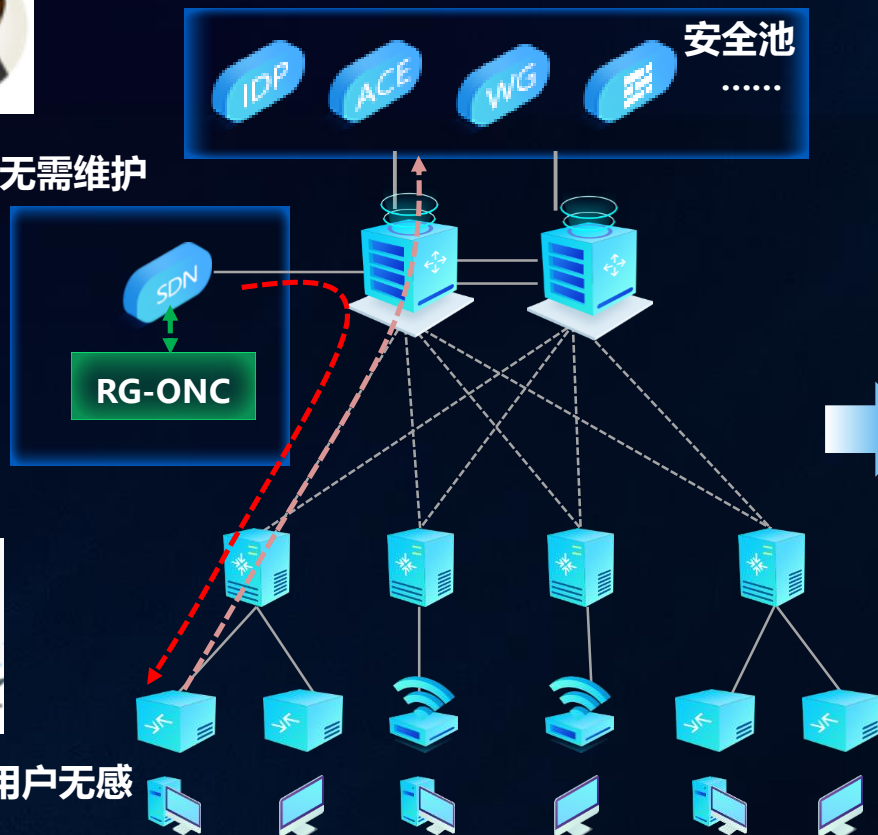
2、分级分权，支持微信手机审批更为便捷

内网防护：无感准入-价值

Ruijie锐捷
Networks



一键管理，无需维护



无客户端，用户无感

适用广泛

支持丰富的统计信息：
终端IP、主机名、位置、状态、上线时间等，辅助管理



1、高可靠，实施快，可远程

- 1、SDN控制器挂掉后也可以进行网络不断网
- 2、实施快，10分钟完成1200台终端安全改造



2、用户无感入网，体验好

无账号、无密码，无需用户操作，开机自动识别，用户体验好，网络中心阻力低



3、维护极致简单

审批制代替客户端：无需收集哑终端MAC 地址，系统极致小巧稳定，由SDN控制器直接管理



4、适用广泛

支持动态IP、静态IP、智能终端、云桌面、有线/无线终端，一套搞定。支持接入、网关、旁挂3种部署模式，对现网架构改动小



5、经济性

无用户LIC，业务扩展不受限制厂家的绑定

内网防护：用好安全，构建无死角的安全防护区

Ruijie锐捷
Networks

安全一键护航方案

智能
调度

安全
编排

统一
运维

无感
准入

安全
协防

全景

好体
验

兼容
开放

更低
成本

更加
可靠

统一运
维区



安全大数据
分析平台



SDN统一
管控平台



统一运维
平台

安全资源池+安全服务编排

异构安全设备



接入



汇聚



核心



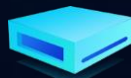
无线AP



无线AC



路由



网关



认证



运维

医院价值层

统一管控层

安全与编排
层

流量
探针层

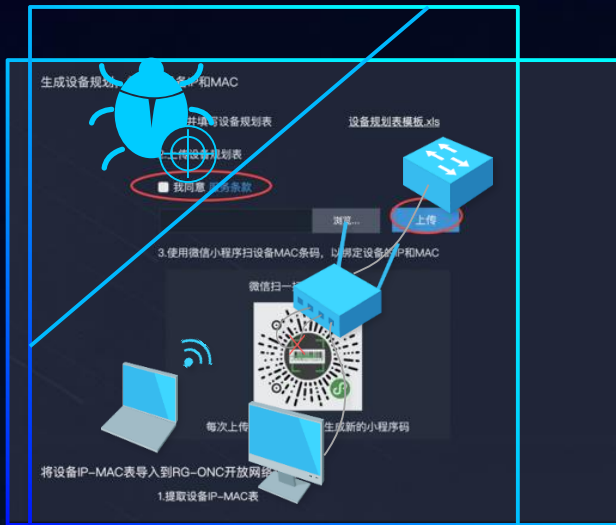
4、运维建设规划



一键运维，释放重复性劳动

Ruijie锐捷
Networks

网络风暴治愈



SDN:交换机即插即用
NEW
FREE



WIS:无线一键网优
NEW
FREE

Ruijie锐捷 | RAIL

2019年中国 IT 综合运维软件 ITIM 市场占有率第一

数据来源: IDC中国 ITUO 市场跟踪报告
(2019年上半年)

1

深度融合场景，激活IT价值
RIIL智能运维时代的领航者

扫一扫
填写您的运维需求

RIIL:综合运维平台

NBAI一键护航方案 “” 一键 “” 总结

Ruijie锐捷
Networks

网络建设

- ✓ 网络一键融合
- ✓ 业务一键隔离
- ✓ 业务一键创建
- ✓ 用户即插即用

.....

- ✓ 终端镜像一键下发
- ✓ 业务一键恢复
- ✓ USB一键禁用与启用
- ✓ 一键远程协助

.....

桌面管理

- ✓ 设备即插即用
- ✓ 地址一键分配
- ✓ 风暴自动治愈
- ✓ 一键预览整网体验态势
- ✓ 一键诊断与回溯
- ✓ 一键问题网优
- ✓ 一键防御异常信号

.....

- ✓ 安全故障自动bypass
- ✓ 安全按需一键引流
- ✓ 安全一键准入
- ✓ 安全一键溯源
- ✓ 终端一键隔离/自动隔离

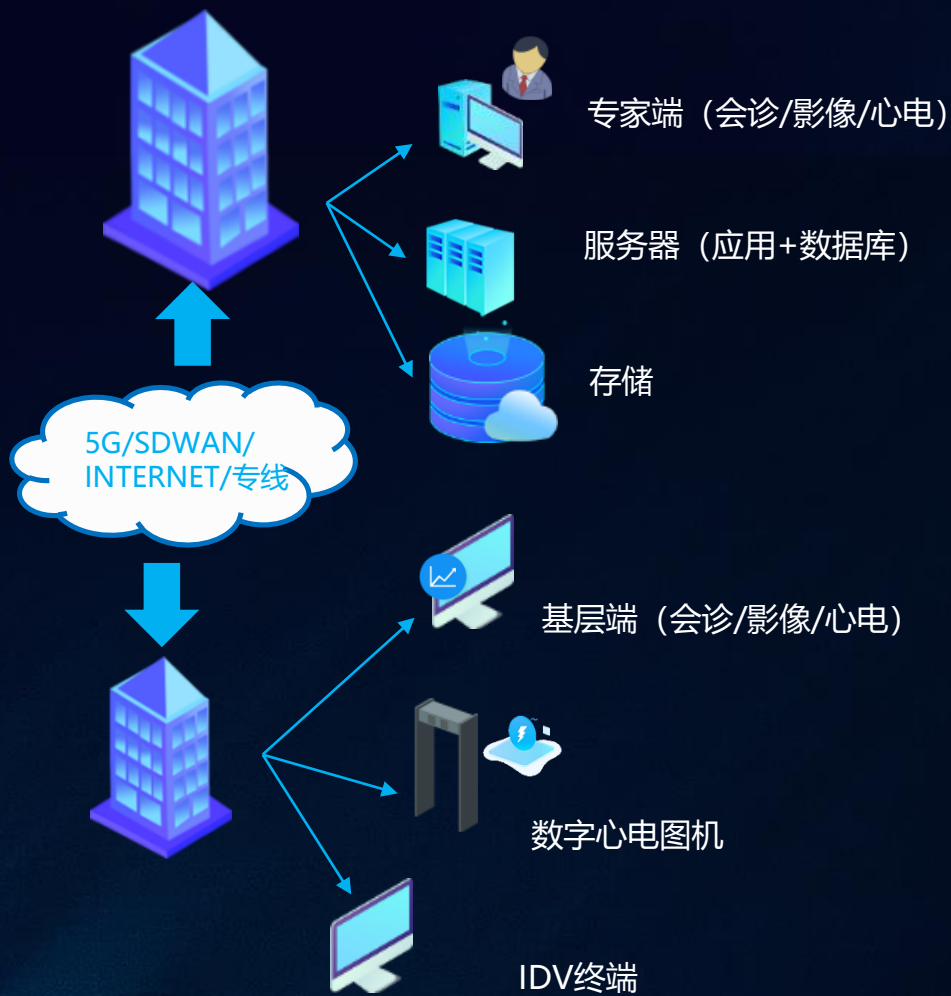
.....

安全管控

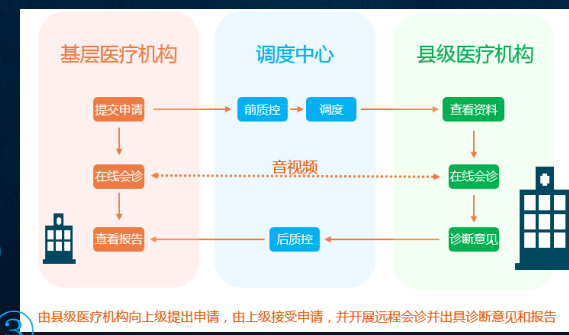
运维管理

5、医联体网络规划与思考

医联体的业务建设基本框架

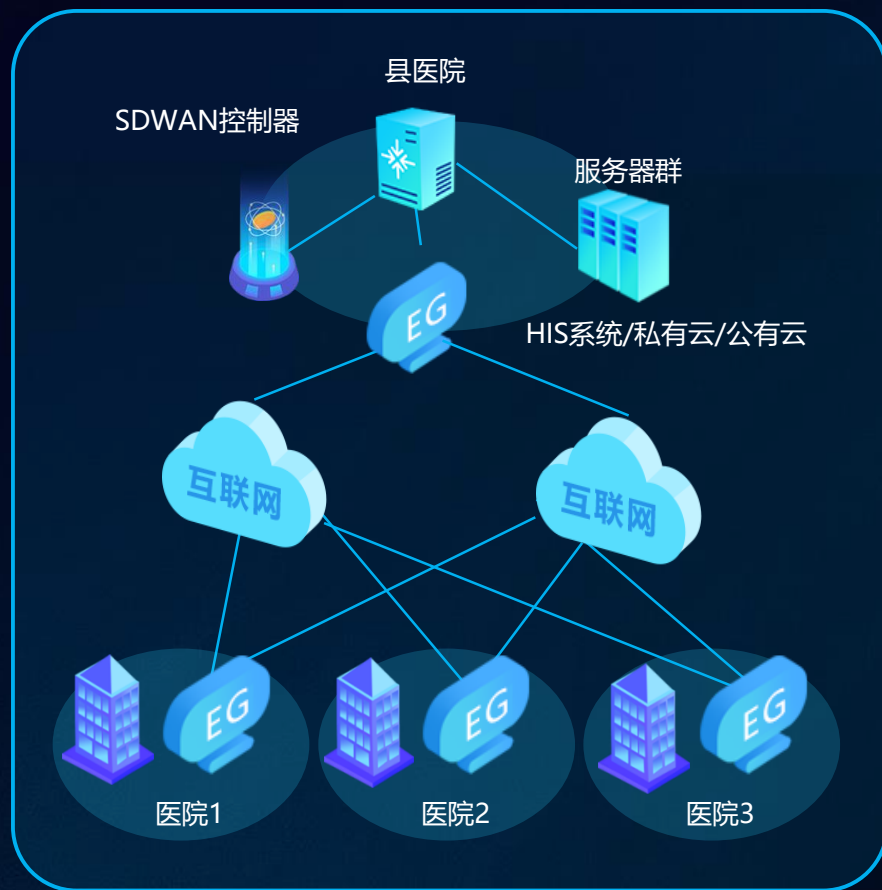


用户远程会诊流程业务流程



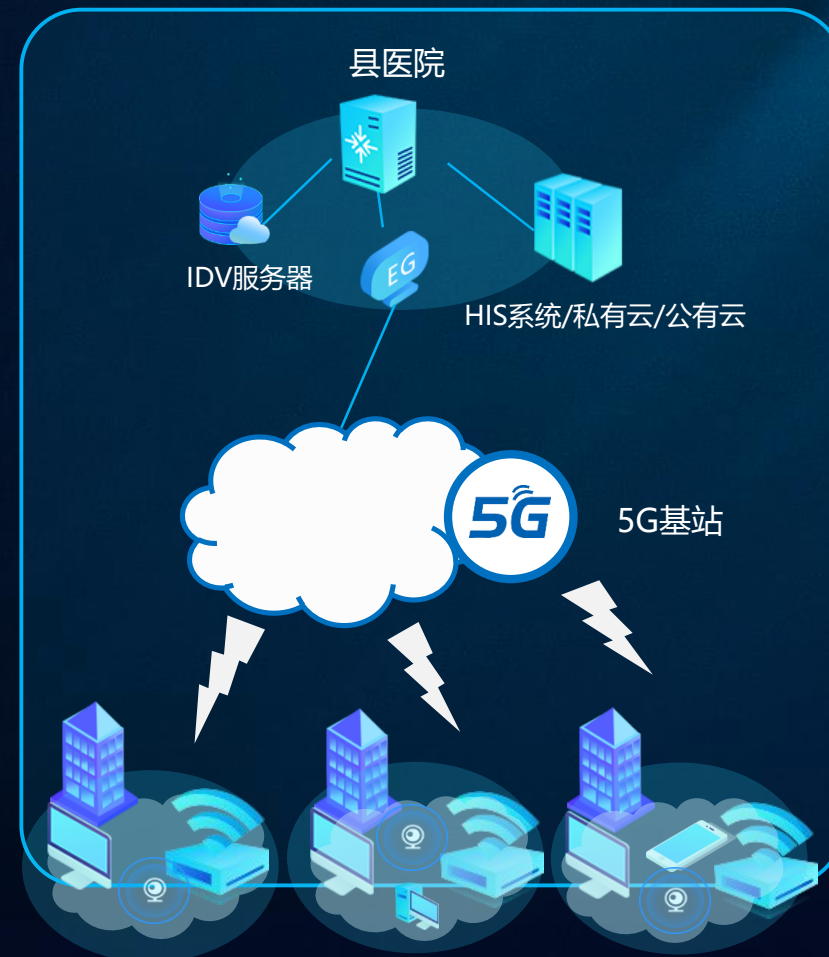
说明：① 远程影像诊断流程
② 远程心电图诊断流程
③ 远程会诊流程

两种业务组网架构



SDWAN+IDV

特点：建网成本低



5G CPE+IDV

特点：业务快速覆盖

THANKS



锐捷网络股份有限公司

地址：北京海淀区复兴路29号中意鹏奥大厦
东塔A座11层

邮编：100036

Office Tel: 010-5171 5999

Fax: 010-5171 5872

www.ruijie.com.cn