Ruijie Networks 锐捷

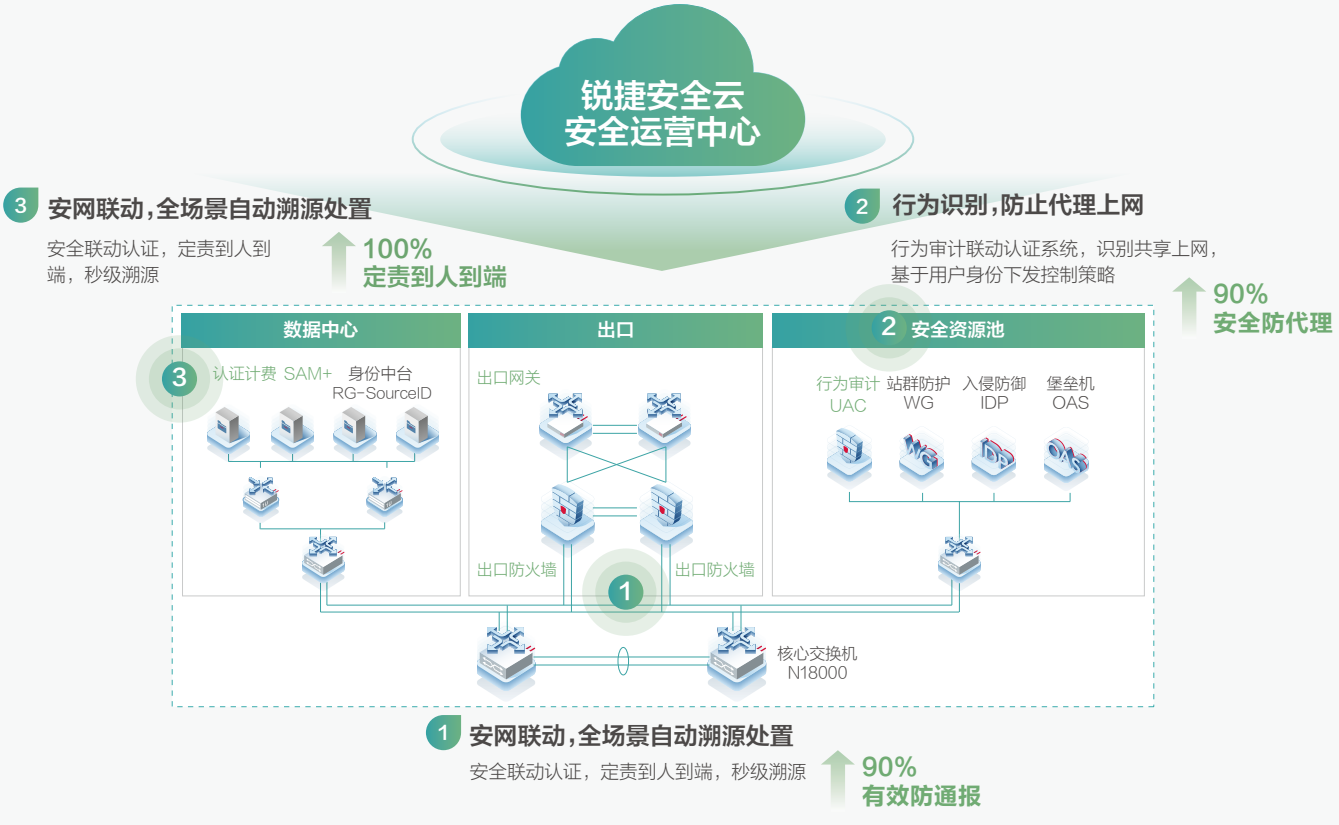
出口安全防护
保障智慧校园网络安全

锐捷高校出口安全解决方案

锐捷安全出口方案要解决什么问题?

校园网络安全全方位识别及防护

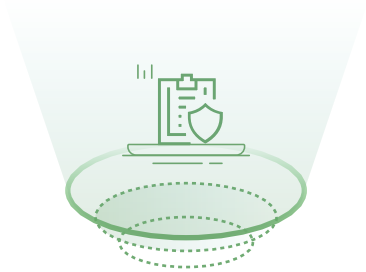
网络+安全联动3.0



整体方案架构：“两防一定”保无忧

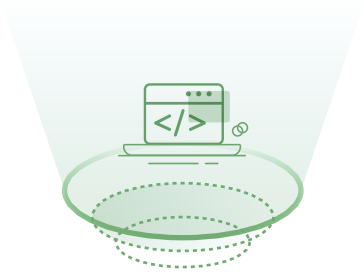
防通报

高性价比横向安全问题检测，
高安全纵向威胁防外溢



防代理

多维度精准识别代理上网，
联动SAM+认证强制账号下线

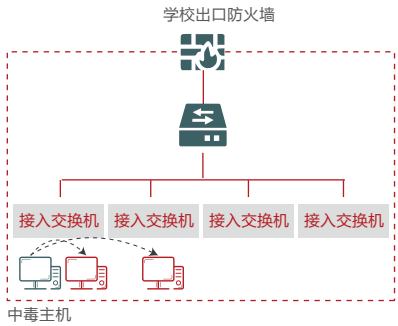


定责溯源处置

全场景之东溯源处置
2小时缩短到 1秒钟

防通报：“安网”联动简架构，全域横向流量精准检测，内网防扩散

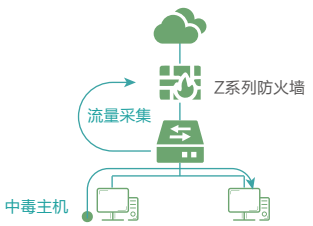
传统方案：横向风险探测成本高，代价大



- 检测横向流量，需在接入交换机部署探针，成本高，管理复杂
- 阻断病毒传播需要终端部署 EDR，管理压力大

VS

新方案：联动交换，全域横向风险检测全覆盖

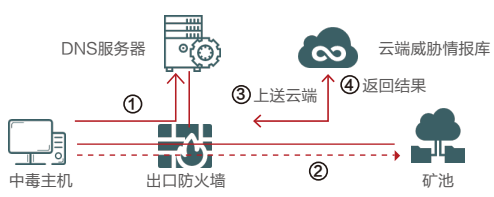


替换探针，联动交换机，将横向流量采集并发送到防火墙进行分析；

一台 FW 实现横向检测和阻断，简架构，成本低，范围覆盖广

防通报：“本地情报+云墙联动”，纵向风险及时精准防护，威胁防外溢

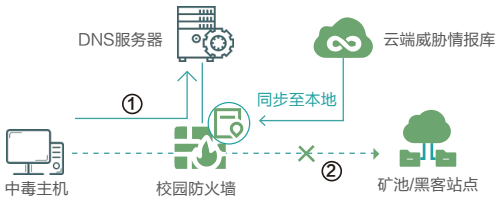
传统防火墙：难以避免纵向安全外溢



传统防火墙遇到威胁时会先放行 DNS 解析，到云端威胁情报库进行校验，导致风险流量外漏，上级部门及监管单位发现木马病毒外联，会对学校进行通报；

VS

新方案：“本地情报+云墙联动”威胁情报



遇到威胁本地海量情报及时精准阻断，确保风险不外溢，防通报云墙联动及时更新，确保本地情报库针对威胁及时、精准防护

防通报：多源+共享情报，覆盖全、检测准、阻断快

边缘设备威胁检测代价大，恶意流量难阻断

IPS/AV 库拦截

加密流量无法监测新型攻击无能为力 IPS 拦截相比情报效率低消耗大

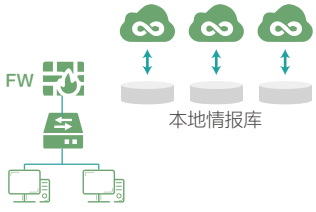
矿池 DNS 变化快，需要丰富的威胁情报库

部分木马直接使用 IP 传输，传统方式难检测，内部传播难发现

情报源单一，与上级单位情报源不一致，风险无法及时同步，易被通报

VS

新方案：多源情报

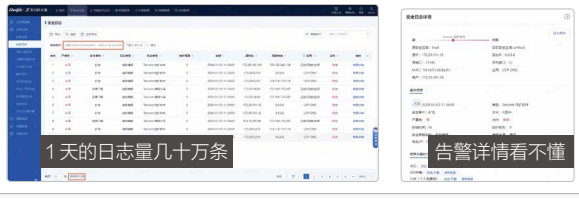


- 多源情报，多擎同时驱动，覆盖范围相比传统方案大幅提升，有效保障出站安全
- 威胁情报技术 + 动态 DGA 技术驱动，APT 攻击、挖矿木马、蠕虫、僵尸网络、勒索软件等威胁及时检测拦截，有效提升情报拦截率，且上下级情报源一致，有效防通报

防通报：轻量化安全云联动，智能分析鉴别威胁，安全防护无忧

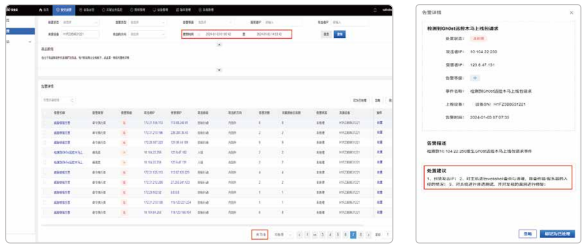
传统方案：安全威胁难识别，难确认

偶尔登录设备　安全告警看不懂　海量告警依靠人工处置



- 只能登录设备查看告警，难以及时发现威胁；
- 大部分安全告警看不懂，不知道如何处置；
- 每天的海量安全告警依赖人工分析确认，速度慢，效果差

云墙联动，实时分析，工作量大幅下降，威胁处置率大幅提升



- 只能登录设备查看告警，难以及时发现威胁；
- 大部分安全告警看不懂，不知道如何处置；
- 每天的海量安全告警依赖人工分析确认，速度慢，效果差

防代理：联动认证下线代理账号

传统方案：安全威胁难识别，难确认

学校宿舍网普遍存在学生共享一个实名账号、代理上网的情况，该问题带来诸多安全隐患，且严重影响运营商收益。

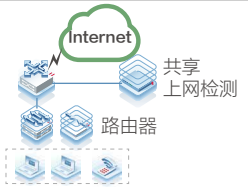
安全问题

不符合“一人一号”实名上网政策多人使用同一账号上网后,无法精确追踪上网记录到个人，安全问题无法具体溯源

收益问题

运营商投建宿舍网，代理共享现象影响学生账号开户率，影响校园网缴费收益。

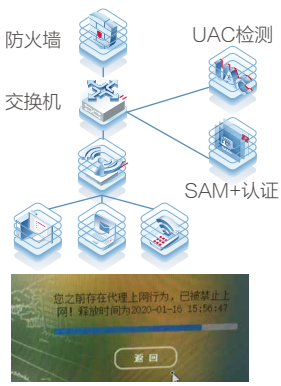
传统方案



业界不少方案检测机制还停留在UA识别阶段，检测手段单一，误判率高，实测效果较差

业界防代理方案识别出代理上网风险终端后，无法采取有效的闭环处置策略。

新方案：联动认证多维度防代理



代理识别：通过UA识别、长链接检测、虚拟身份识别、路由器识别等多种方式交叉识别代理行为

代理处置：1、串行部署：UAC直接阻断；2、旁挂部署，发现代理后同步联动认证平台进行告警/下线处理；

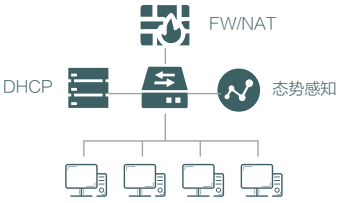
- **多维度**精准识别代理上网，准确率提升至90%，避免误判造成的不良影响；
- 直接阻断/联动阻断，**闭环处置；**

溯源定责到人：认证联动，自动化溯源，高效省时省力

传统方案：溯源全靠多系统手动查询，效率低，代价大

日常安全运营过程中

- 被通报难以及时溯源无法交代
- 发现可以威胁溯源困难，难以保障业务安全



1. 收到**通告信息**或发现**可疑威胁**

外网 IP 和时间点

2. 查询防火墙 / 探针 /IDP 等多系统的**安全日志**和 **NAT 日志**

内网 IP 和时间点

3. 认证场景查询**认证系统日志**

失陷 IP 对应的实名信息

4. 无认证场景查询 DHCPServer ARP

效率低：①1 个告警 10 分钟，每天几十个告警，**需要查 2 小时，费时费力。**
②各产品**日志时间不一致，**造成难以查询；

多系统来回查询，工作量大，**技术门槛要求高**

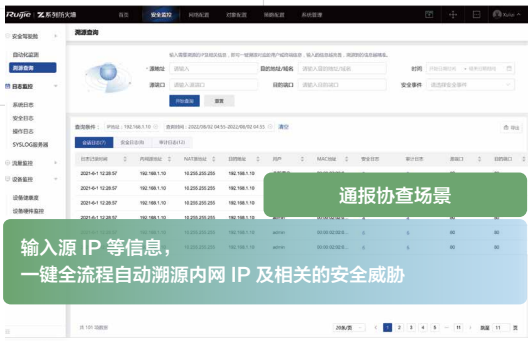
DHCP 无认证环境下终端不断变换地址，**找不到 MAC 地址**

低效率、成本代价大、技术要求高、
动态场景下找不到MAC导致威胁得不到及时溯源处置

简架构低成本，一台防火墙完成全场景自动化溯源

常态安全运营分析工作

认证场景：联动 SAM+/SMP/ 锐捷安全产品 / 深澜等实名系统，定责到人
无认证场景：镜像 DHCP Server 报文自动检测分析定责到终端 MAC



通报协查场景

输入源 IP 等信息，
一键全流程自动溯源内网 IP 及相关的安全威胁

全场景自动化溯源处置，**2小时 缩短到 1秒钟**
让溯源和处置成为一种基本能力，让安全运营工作更高效

定责溯源处置：威胁一键处置，自动提醒和解封，高效闭环不添乱

传统方案：多系统联动处置，人工提醒，人工恢复工作量大

①封禁威胁用户或 MAC 要到认证系统或网络设备上操作，操作麻烦，技术要求高，人工维护阻断记录难

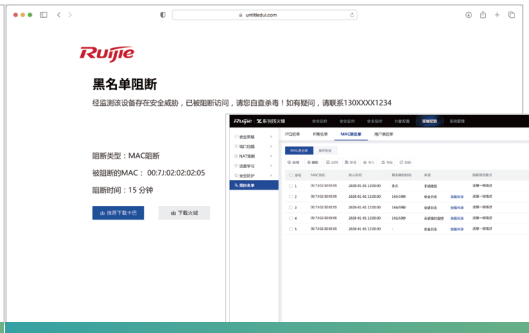
②阻断后，难以提醒用户，需要打电话或邮件，跨部门通知协调困难，**轻易不敢阻断**，怕电话被打爆

③阻断后，还要等着用户处置威胁，手动进行恢复，增加工作量

④事后无记录，阻断无依据，难以指导安全工作开展

⑤威胁溯源处置工作难统计，运营工作效率和成果难保障

一台防火墙完成全场景自动化溯源



一键阻断IP、阻断用户、阻断MAC多手段处置威胁，有效降低安全风险

自动解封用户，无需人工干预

自动提醒用户，提效不添乱，整体安全运营工作溯源处置闭环提效70%+
自动留存记录，事后可追溯，依据可导出，针对性加强安全意识教育

定责溯源处置： 5G安全合规，认证联动，灵活权限，实名溯源

传统运营商方案	新方案：锐捷安全+5G融合认证联合方案
学校未掌握管理权限：谁能访问校园内网由谁决定？如何确定用户是否合法？	
人员状态变化，权限难做：校园用户身份生涯状态变化如何处理？休学、辞职、毕业是否还能访问？	
安全风险高：校内业务系统谁能访问，如何保障安全性？	
5G 上网行为管理：敏感信息无法审计，管理失职？	
管理溯源困难：针对安全风险如何溯源定责？	

锐捷5G认证+安全联动，**用户动态、实时管理** 行为审计、流量监测、专网防护，**极简架构、高安全**	认证联动，区分用户策略， **业务系统访问更安全**	实名认证联动 **秒级自动溯源**

应用案例

客户介绍

西南交通大学是教育部直属全国重点大学，国家首批“双一流”“211工程”“特色985工程”“2011协同创新计划”重点建设并设有研究生院的研究型大学。学校创建于1896年，是中国第一所工程教育高等学府。现有全日制本科生28914人、硕士研究生15053人、博士研究生2630人、留学生536人。现有专任教师2700余人，其中，中国科学院院士10人（含8名双聘院士）、中国工程院院士17人（含15名双聘院士）。

客户痛点

部署防火墙、探针后依然有挖矿行为：现有防火墙由于默认放行挖矿木马的DNS请求报文，无法杜绝挖矿行为；

实名溯源费时费力：学校采用DHCP动态分配地址，每次溯源需要查询NAT日志、认证日志等多个平台，每次溯源需要花费2-3个小时；

解决方案

部署锐捷Z系列防火墙、日志审计等防护措施，将交换机作为微探针，交换+安全联动，实现精准防御、溯源闭环。

价值落地

告警数量动态清零：快速实现全网“挖矿”检测，“云边”情报联动检测南北流量防外溢，交换替代探针检测东西流量防扩散、多源情报、共享情报，多手段全面精准防御，减少被通报风险；

实名认证，一键溯源：可疑风险，与SAM+联动，一键溯源，2小时缩短到1秒，高效省时省力；

锐捷网络股份有限公司

欲了解更多信息，欢迎登录www.ruijie.com.cn，咨询电话：400-620-8818