

国内某知名高等学府校园网出口 SDN 安全服务链改造和升级

项目背景与挑战

国内某知名高等学府自 20 世纪 50 年代建校至今已有近 70 年的历史。校园覆盖面积高达 1550 亩，在校师生约 30000 人，是一所涵盖了除军事以外所有 12 大学科门类的综合性全日制普通高等学校。截至 2017 年，学校已建成覆盖全校、承载各种数字校园业务的校园网络。随着信息化高速发展，数字化校园网络正向 SDN 网络时代迈进，同时学校规模也在不断扩张，原有的出口网络已经不能完全满足学生上网的需求以及多元化的校园数字化业务承载需求。学校原有出口网络架构图如图 1 所示，该架构给校园网络带来了多方面的挑战，主要包括：

- 挑战一：安全设备升级难，将千兆出口带宽升级至万兆，千兆安全设备端口速率和性能都无法匹配带宽升级需求；
- 挑战二：安全设备在出口链路中串联部署，设备故障、维护、扩展和更替都需要动网断网，运维复杂，影响业务；
- 挑战三：安全设备性能有效利用率低，部分流量无需安全监测，却消耗设备大量性能，如宿舍区；
- 挑战四：安全设备在出口链路中串联部署，造成出口性能瓶颈。

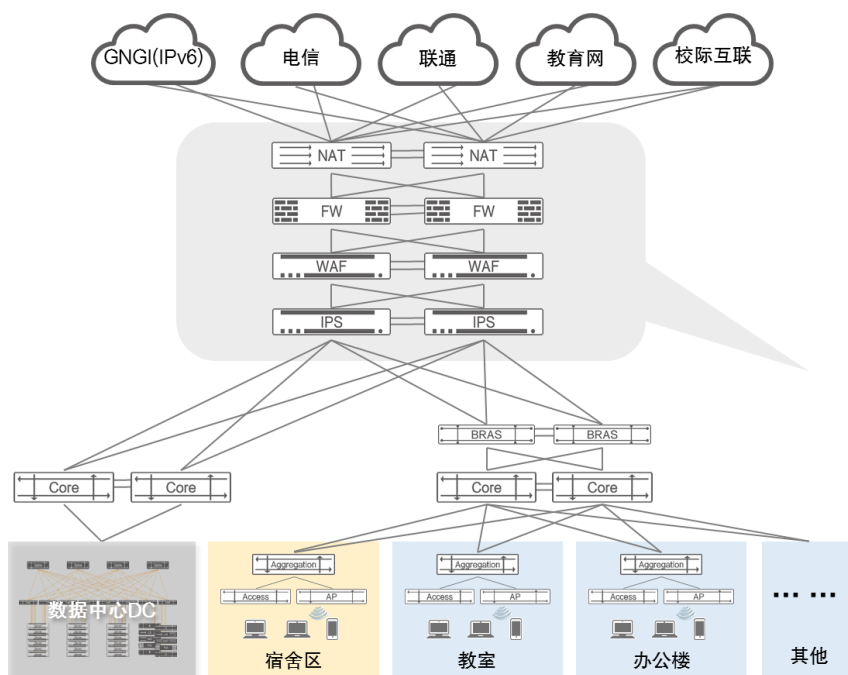


图 1：学校原有的出口网络架构图

为了使学校信息化建设与网络技术发展步伐保持一致，方便学生利用互联网络更快捷的获取知识，方便学生利用引入的先进网络设备进行深入研究，2018 年，该校进行了校园网出口 SDN 安全服务链改造和升级。

与此同时，该项目还响应了国家对加快高教信息化建设的号召：《国家中长期教育改革和发展规划纲要（2010-2020 年）》专门提出教育信息化发展规划“信息技术对教育发展具有革命性影响，必须予以高度重视”，以及教育部也颁布《关于全面提高高等教育质量的若干意见》（高教三十条）的二十九条意见：“加快推进教育信息化进程，加强数字校园、数据中心、现代教学环境等信息化条件建设。”

Asterfusion 解决方案

针对该高等学府原有出口网络所面临的挑战，Asterfusion 设计了针对性的解决方案，经改造和升级后的网络架构图如图 2 所示。

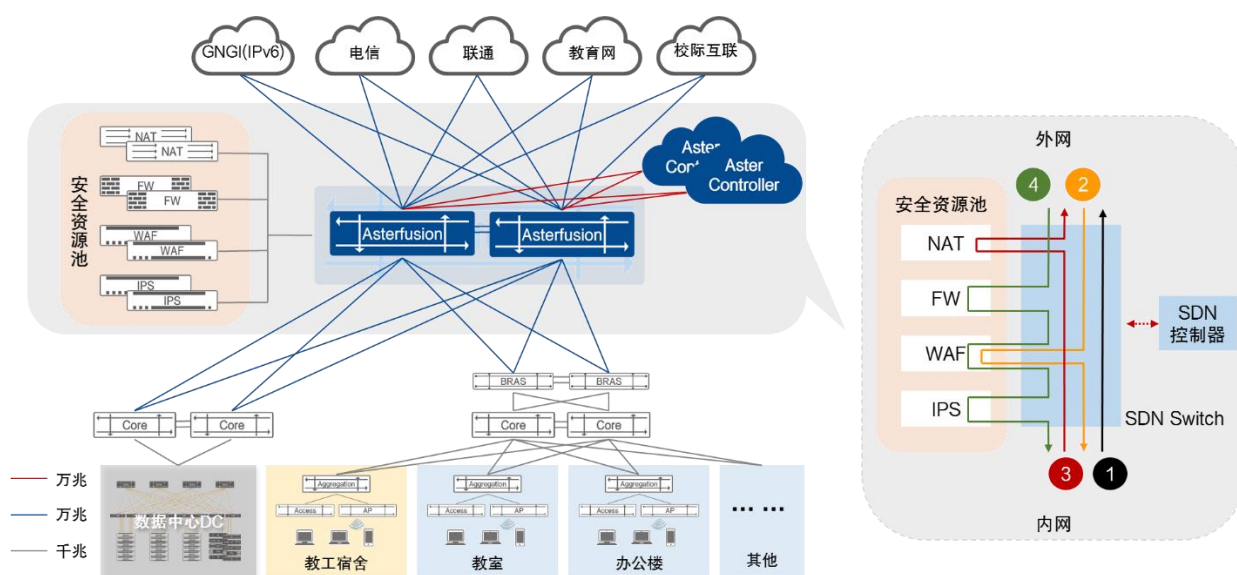


图 2：学校改造和升级后的出口网络架构图

相比于原有校园出口网络主要进行了以下几方面的改造和升级：

- 1) 新增两台高性能的 Asterfusion Switch，作为统一调度和转发出出口数据流量的交换设备，部署两台交换设备进行流量的负载均衡，保证流量转发的高效性，以及网络和链路的高可靠性；
- 2) 千兆出口带宽升级至万兆，与出口交换设备实现万兆连接，出口设备还需预留 25G、40G/100G 等超高速率端口，为后续出口网络线路升级提前做好准备；
- 3) 将出口串联的所有设备，包括防 FW、WAF、IPS、NAT 等，分别旁挂在 Asterfusion Switch 旁边，根据设备的性能，选用千兆或万兆线路连接；
- 4) 增加两台 SDN（Software Defined Network，软件定义网络）控制器，将网络设备控制面与数据面分

离开来，通过控制 Asterfusion Switch，实现网络出口流量的灵活控制和智能管理。同时部署两台 SDN 控制器做主备冗余，实现网络的高可靠性的保证；

5) 在 SDN 控制器上重新编排安全服务链，优化网络出口流量出入路径：

- EXT → INT，从外部访问学校内网的流量，需要根据流量类型引入不同的安全设备
 - 访问内网网站的流量中，有些流量需要先经过 WAF 设备检查，再发送到内网；
 - 有些流量在经过 WAF 设备之前，还需要先经过防火墙做映射，经过 IPS 检查，再发送到内网等。
- INT → EXT，从学校内网出去的正常流量
 - 如是公网 IP，不经过安全设备直接出去；
 - 如是私有 IP，需要经过诸如防火墙设备等安全设备，做 NAT 后再出去；
 - 如出去的流量检测到异常，需发送到相应的安全设备进行检查后再出去。

特色亮点与客户价值

Asterfusion 解决方案对校园出口网络进行 SDN 安全服务链的改造和升级后，解决了原有出口网络所面临的各种挑战，同时还为校园出口网络带来了许多亮点和价值：

- 安全设备旁挂，千兆出口带宽升级至万兆，千兆安全设备无需升级，端口速率也不会对出口带宽升级带来影响；同时，利旧网络出口设备，能降低改造成本，实现资源的充分利用；
- 网络出口设备改串联为旁挂，设备故障、维护、扩展和更替等无需动网断网，不影响现有网络业务；
- 提供 SDN 安全服务链，通过 SDN 控制器与 Asterfusion 云交换机的密切配合，实现对流量的灵活调度，按需调配安全资源，提升安全资源的有效利用率。两台 SDN 控制器进行主备冗余，两台云交换机采用负载均衡，通过这一措施保证流量转发的高效性，以及网络和链路的高可靠性；
- 安全设备性能不再成为网络出口的性能瓶颈，出口交换设备性能与出口带宽保持一致；
- SDN 集中控制交换流量，大幅度简化复杂的路由规划、策略配置等部署，显著提高网络响应速度和综合运维水平，实现对出口网络流量的灵活控制和智能管理；
- 软件定义网络是信息化的发展方向，高等学府使用该技术能为学校人才培养提供实验设备、技术研究方向和动力。



关于星融元数据

星融元数据技术有限公司（Asterfusion Data Technologies Co., Ltd.）为云计算提供领先的、真正意义上的软件定义网络解决方案。凭借所拥有的专利技术，基于高度软件定义的整体架构、完全开放透明的操作系统、突破传统限制的硬件平台，星融元数据帮助用户重新定义云计算的网络基础设施，并且为云计算的使用者赋予真正弹性与超高性能的虚拟网络、为云计算的管理者提供纯粹的开放接口和自动部署调度、为云计算的开发者构建可编程和可视化的业务环境。

星融元数据的核心团队来自于中美两国多家知名的通信和 IT 企业，共执对客户需求的透彻理解、对产品技术的笃定热爱、对下一代云计算网络的美好梦想，源于中国、面向全球，致力于成为中国最优秀的云计算公司。星融元数据坚信云计算将为用户、产业与我们带来多方共赢的美好未来。

联系方式

苏州（总部）

苏州市工业园区星湖街 328 号
2 栋 B401
0512-62982976

北京

北京市海淀区宝盛南路 1 号
奥北科技园 20 号楼 207
010-62672668

西安

西安市曲江新区旺座曲江
C 座 2605
029-89834058

希望获取更多有关星融元数据公司、产品及解决方案的信息，请登录 www.asterfusion.com、或发送邮件至 sales@asterfusion.com、或关注我们的官方微信、微博。

“星融元数据”、“Asterfusion”、“ASTERFUSION”，及其徽标均为星融元数据技术有限公司在中国的商标或注册商标。其他所有商标为其各自所有者之财产。本文件所包含的信息可能会发生修改，恕不另行通知。未经书面许可，本文件所含内容不作为合同或许可证的一部分。

©2018，星融元数据保留一切权利。