系统架构

Algoblu (北京肇煜宏泰信息科技有限公司) 成立于 2012 年，总部设在北京，在加拿大设有研发中心，是从事 SD-WAN 技术、产品研发与市场服务的初创公司。做为一家 NaaS（Network as a Service）“网络即服务”运营商，Algoblu 拥有基于自主知识产权的核心专利技术 NEV（Network Element Virtualization）网络资源虚拟化构建的低延时网络，结合 Cloud-native 云原生部署的 SASE（Secure Access Service Edge）服务平台可以为用户提供高级安全服务和低延时弹性网络服务。

Algoblu 基于长期的行业积累与行业共性难题推出由网络层至应用层全栈方案，可解决从 To B 端的 KA 企业用户至 To C 端的家庭用户面临的网络及安全的问题。

图 1.Algoblu 系统全栈

- 基础层：NEV（网络资源虚拟化）基础设施是整个系统的核心，包括自研的 NEV 芯片和 NEV 通信协议栈软件，软终端、用户侧接入设备 CPE，网络侧边缘设备 PE 和控制器等通信诸元；
- 网络层：NEV 骨干网，包括自建的网络以及部署了 NEV 方案的传统运营商网络，这是一个跨地域的广域网，与多家运营商、IDC 和云服务商互联；

- 应用层：SASE 服务平台，基于云原生部署，基于 Identity-driven 用户身份，为在任意地方、以任意方式接入的任意用户提供两大类服务，不依赖用户侧设备的云端高级安全服务和弹性网络服务。
- 业务层：EPL 弹性专线和 EPN 弹性专网解决 KA 企业客户的数据中心互联,网点、分公司互联等需求，2B2C 应用带宽解决 C 端和小 B 客户低延时数据传输需求

TSN 时间敏感网络

物联网、5G、工业互联网等新一代信息通信技术的发展，加快了传统行业转型升级的步伐，万物互联的通信需求也随之增加。例如在智能制造中，实时控制、边缘计算、数字孪生等应用场景对低延时、低抖动和高可靠性的承载需求要求非常严格。传统以太网已经不能满足越来越多的数据和广泛分布的网络需求，时间敏感网络（TSN）技术应运而生。时间敏感网络以传统以太网为网络基础并通过 Algoblu 自研的 NEV 网络虚拟化技术全面构建时间敏感型的骨干网。

NEV（网络资源虚拟化）是 Algoblu 对底层网络资源进行抽象化/虚拟化的专利技术，与 VMware 对 x86 服务器资源进行抽象化/虚拟化的理念相似。NEV 在 OSI 7 层模型中处于 L1 物理层和 L2 MAC 层之间，属于底层技术。通过自行设计的 NEV 芯片可以将底层网络资源（光纤）分割成 10 万个独立的原子信道，在信道层对物理帧进行标识，通过业务编排器编排/组合原子通道形成新的业务接口，并在此基础上创建具有严格 SLA 保证的 NEV 产品。NEV 技术可以池化底层网络资源，把一个光纤端口虚拟化成最大 4096 个虚拟光纤接口，每个虚拟接口具有独立的资源、彼此物理隔离。NEV 实现的效果如同把一条物理光纤最多虚拟成 4096 条虚拟光纤，每条虚拟光纤的性能和操作方式与物理光纤一样。

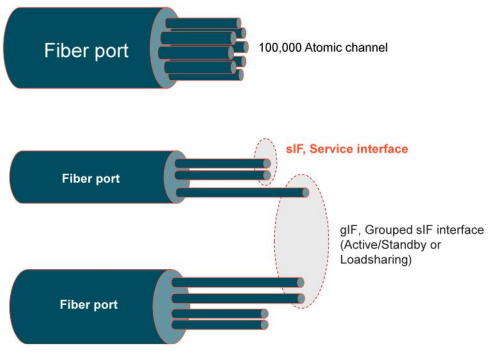

图 2：NEV 实现原理

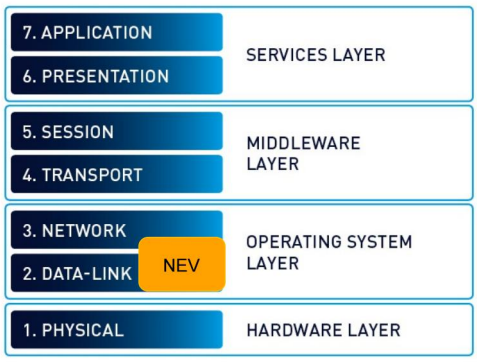

图 3：NEV 在 OSI 7 层模型中的位置

此外，NEV 芯片通过算法实现了 TSN（Time Sensitive Network）中循环队列（IEEE 802.1Qch）、流量调度（IEEE 802.1Qbv）和基于信用的流量整形（IEEE 802.1Qav）等诸多低延时网络服务的功能。

SASE 安全云服务

Secure Access Service Edge (SASE) 是一种全新的网络安全架构，它将广域网和网络安全的不同功能组合到一个统一的云安全平台中，以服务的形式交付。无论用户和应用在哪里，都可以享受统一的连接和保护。Algoblu 基于云原生部署的 SASE 服务平台以原生云服务的方式提供给用户，安全服务分布在所有网络节点上并拥有云原生固有的弹性和扩展性。

Algoblu SASE 安全云不仅具备核心的 ZTNA 零信任接入的功能还可以将传统的安全功能及设备通过云服务的方式进行提供，用户接入骨干网络即可直接获取到安全服务，提供安全服务如下:

- **ZTNA 零信任网络接入**

任何用户在接入 Algoblu SASE 服务平台使用任何服务时首先要经过 ZTNA 零信任网络接入验证，针对不同用户身份 Identity-driven，执行统一的资源管理策略授予不同用户访问不同资源的权限以及相应的路由。针对每个访问请求在授予访问之前进行完全身份验证、授权和加密，应用微分段和特权访问原则减少横向迁移带来的安全隐患。

- **NG-FW 下一代防火墙**

兼容传统防火墙的基本功能，包括包过滤、协议状态检测、NAT，应用感知能力，基于 L7 应用实施精细化的安全管控策略和层次化的带宽管理。

- **防 DDoS 攻击**

对异常流量进行持续监控和检测，采用动态告警基线分析攻击行为并展开流量的牵引和清洗。可高效防护各种类型的 DDoS 攻击，包括传输层（如 SYNC flood、ICMP flood 等）、应用层（DNS 服务等）以及 CDN 代理等各种拒绝服务攻击，结合本地及云端清洗平台可并快速过滤大流量攻击侵害，保障业务安全平稳运行。

- **SWG 安全 Web 网关**

分析 Web/Internet 流量、检查 Web 请求、与已定义的策略进行比较并在恶意数据包到达目标之前将其过滤掉。支持 URL 筛选、恶意代码检测和筛选。

- **IPS 入侵防御**

通过分析网络流量，检测入侵（包括缓冲区溢出攻击、木马、蠕虫等），自动丢弃入侵报文或者阻断攻击源，从而避免攻击行为。支持重组应用数据，协议识别和解析，签名特征匹配。

- **DLP 数据防泄漏**

实时监测经过企业网络的通信数据内容，自动对网络数据文件分类分级，检测、分析并报告企业敏感数据失泄密事件。支持多种协议、多种文本格式、文中语义识别，识别、分析企业高风险的业务流程和员工行为，支持事前预防、事中保护和事后审计。

Algoblu 通过自主研发的 CPE 设备在不改变用户现有网络的结构下快速部署，实现接入即可获得高质

量的 SLA 组网、加速、各类安全措施，用户通过可视化系统灵活调整安全策略，网络结构，助力用户快速实现数字化云化转变。

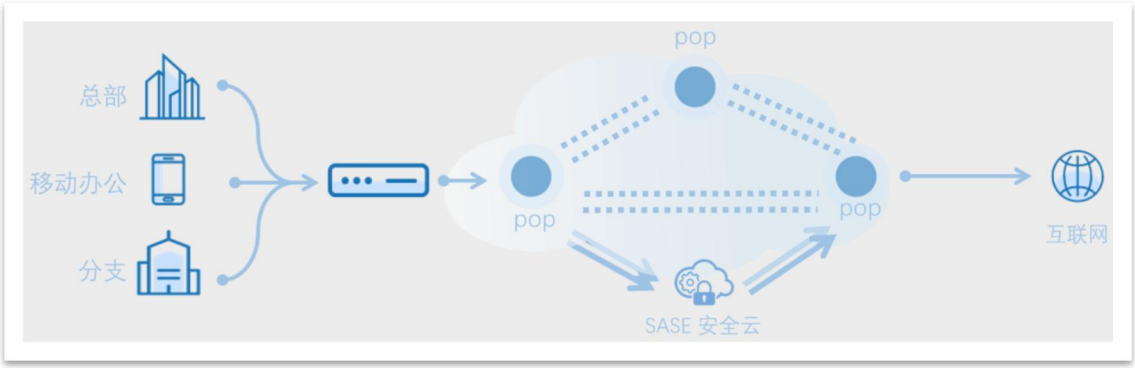

图 4.网络、安全即服务