基于 SRv6 技术的算网安全资源池的研究和应用

刘玲 葛良 曹怡 何娟 袁友鹏
中国移动通信集团江苏有限公司 210029

【摘 要】本文通过建设算网安全资源池，三层架构部署：集中运营管理平台、算网安全能力底座、安全能力近源POP节点。将原有单一的算力中心IDC配套网络安全设备协同使用，并进行全网纳管，再结合SRv6技术进行大网引流，实现多项安全能力产品输出。通过集中运营平台统一对外，为全网边缘云、专线、IDC等客户网络安全需求提供点对点的安全能力服务，实现封堵、清洗、入侵检测、WAF等安全防护，实现业务转型和增值创收。

【关键词】SRv6；算网；安全；DDOS；WAF

Research and Application of a Computing-Network Security Resource Pool Based on SRv6 Technology

Liu Ling Ge Liang Cao Yi He Juan Yuan Youpeng
China Mobile Communications Group Jiangsu Co.，Ltd. 210029

【Abstract】This paper proposes the construction of a computing-network security resource pool with a three-layer architecture: centralized operation management platform，computing-network security capability foundation，and security capability near-source POP nodes. By integrating existing standalone cybersecurity devices from computing center IDCs into a collaborative framework and implementing centralized network-wide management，combined with SRv6 technology for large-scale traffic steering，the system enables multi-dimensional security service delivery. Through the centralized operation platform，it provides point-to-point security services for network security demands of edge cloud，dedicated lines，IDC，and other customers across the network. These services include threat blocking，traffic scrubbing，intrusion detection，WAF（Web Application Firewall），and other security protections，thereby driving business transformation and value-added revenue generation.

【Key words】SRv6；Computing-Network；Security；DDOS；WAF

1.引言

近年来，随着数字经济的蓬勃发展，全球云计算市场规模持续扩张。5G、人工智能、物联网、云计算等新技术不断向各领域渗透，极大地推动了云计算需求的提升。与此同时，云安全防护需求也随之急剧增加，为企业客户提供更加安全可靠、按需供给的安全服务成为迫切需求。为了打造全网安全增值服务，赋能各行各业，当前网络架构中，安全设备普遍呈现“烟囱式”部署特征：防火墙、入侵防御系统（IPS）等设备分散在各地市 IDC 机房，形成资源孤岛。这种模式导致三大核心矛盾：其一，设备利用率不足（平均低于 40%），区域性攻击高峰时无法实现跨节点资源调度；其二，安全能力与网络流量解耦，防护时延居高不下，如何集中管理安全设备，将安全能力应用于全网，提高安全设备利用率，并在 CMNET 网内进行调度，实现安全服务的一点对外，满足大部分客户的安全服务需求，并将其整合成一个全网安全产品，成为亟待解决的问题。

文旨在利用全网安全产品构建全网安全资源池服务能力，通过三层架构：集中运营管理平台、算网安全能力底座、安全能力近源 POP 节点，集中运营管理平台集团侧运营，算网安全能力平台和近源 POP 节点省侧运营，为全网边缘云、专线、IDC 等客户提供安全服务需求。本文将重点介绍客户通过集中运营管理平台订购安全服务后，算网安全底座和安全能力近源 POP 节点之间通过 SRv6 进行引流实现安全服务的原理。算网安全资源池系统整体架构。

1.1 安全资源池三层架构

算网安全资源池系统采用三层架构，旨在初步构建全网安全资源池服务能力。这一架构由集中运营管理平台、算网安全能力底座以及安全能力近源 POP 节点组成。总部负责集中运维，而各省节点则构建多种安全能力，实现安全能力的内置。这些安全能力与市区县边缘节点互为补充，基于“连接+算力+安全能力”覆盖全国客户，提供云安全增值服务，实现安全功能和服务能力的灵活调度。

随着安全发展趋势和用户需求的变化，该系统将持续迭代优化，推动业务转型和增值创收。系统架构如图 1 所示：

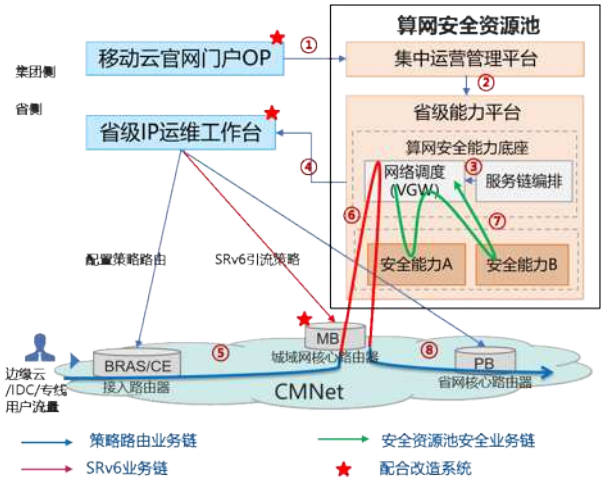

图 1　系统架构

在这一架构下，客户在移动云门户 OP 订购安全业务，OP 将订单下发给集中运营管理平台。集中平台根据地域信息将订单下发至对应省份的省级能力平台。省级能力平台根据客户位置编排就近的省级安全能力或 POP 点安全能力进行服务。安全能力底座依据客户订购信息进行安全能力编排，生成安全服务链编排信息下发至 VGW。同时，省级能力平台向省级 IP 运维工作台下发引流策略。用户采用策略路由方式将流量从 BRAS/CE 引流到 MB。当用户流量引流至安全资源池对接的 MB 设备时，MB 设备建立至安全资源池 VGW 的 SRv6 隧道。安全资源池 VGW 对 SRv6 流量进行重新解封装，并按照对应的安全服务链依次引流至各安全网元。各安全网元根据省级能力平台下发的安全策略完成安全服务。安全服务完成后，安全资源池 VGW 配置策略将流量重定向到 SRv6 隧道到 MB 设备，用户流量回到大网转发至访问目的地。

2.能力平台部署

2.1 算网安全能力底座及近源 POP 节点

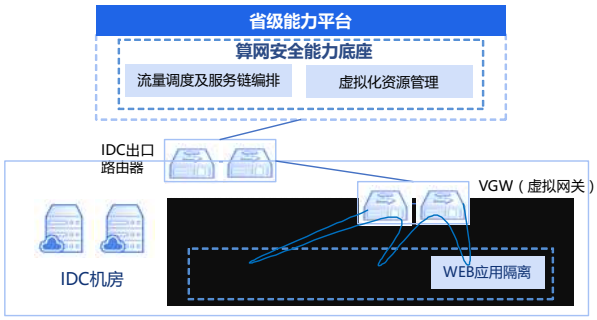

图 2　算网安全能力底座及近源 POP 节点部署

近源 POP 节点部署在各地市 IDC 机房内，这一布局便于边缘云、互联网专线和 IDC 客户流量的就近分流，从而实现敏捷灵活的用户服务。近源 POP 节点具备下一代防火墙、入侵防御和 Web 应用隔离等安全服务能力。POP 节点还部署了 VGW 网元，以实现用户流量出入安全资源池的引流。此外，POP 节点与省级能力平台通过 CMNet 互通，实现管理流量的对接。能力平台部署图如图 2 所示：

2.2 SRv6 引流技术原理

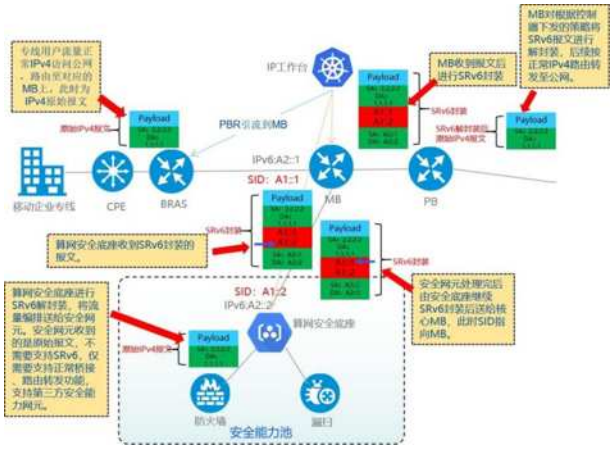

图 3　SRv6 引流技术原理

算网安全资源池作为一个 SRv6 节点在 IP 工作台注册。IP 工作台根据业务需要下发引流策略至省内服务于互联网专线、边缘云和 IDC 客户的 CE、BRAS、MB 设备，并为执行 SR 策略的路由器分配 SID。MB 收到策略后对 IPv4 数据包进行 SRv6 封装，加入 IPv6 报文头和 SID 信息，将路由信息更新至 SRH 的 Segment List。后续数据包根据该路由进行流转。算网安全底座收到 SRv6 封装的报文后解封装，并将流量编排给安全网元。安全服务执行完成后，算网安全底座负责将流量进行 SRv6 封装，封装后的流量送至 MB。MB 收到 SRv6 的封装报文后进行解封装，后续按正常 IPv4 路由转发至目的地。SRv6 引流技术原理如图 3 所示：

3.安全能力产品输出

3.1 黑洞路由能力

黑洞路由能力是一种重要的安全防护手段，客户通过移动云官网门户 OP 下黑洞订单，订购黑洞路由封堵服务，由集中运营管理平台下发到省内安全底座，再下发到相应的安全能力设备，在地址受到相应攻击达到一定阈值时，受攻击地址会被执行为黑洞封堵地址，用户访问时，访问到这个地址就会被 SRV6 引流到黑洞设备，从而达到黑洞封堵的目的。

通过省内安全底座或者集中运营管理平台均可以看到相应时间段内受攻击的 IP 数量以及被牵引地址的趋势图，如图 4。

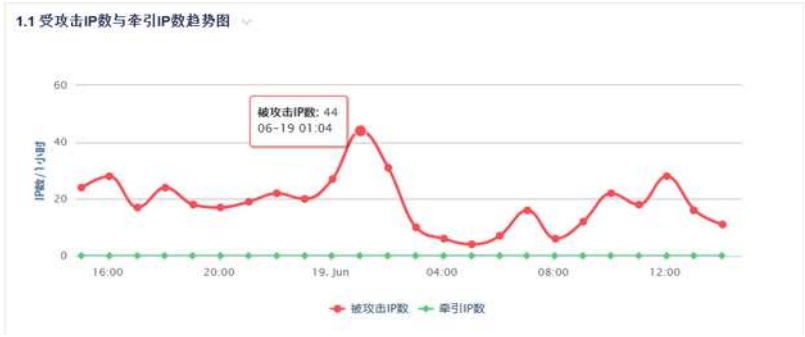

图 4　受攻击 IP 数与牵引 IP 数趋势图

3.2 流量清洗能力

流量清洗能力是另一种关键的安全防护手段，客户通过移动云官网门户 OP 下黑洞订单，订购流量清洗服务，由集中运营管理平台下发到省内安全底座，再通过下发到相应的安全能力设备，在用户访问时，通过 IP 运维工作台进行 SRv6 引流，将访问流量牵引至省内安全底座的流量清洗能力平台，通过平台进行清洗，清洗后再通过 SRv6 返回给原 MB 等设备，再根据正常 IPv4 路由转发至目的地。

通过省内安全底座或者集中运营管理平台可以看到相应时间段的入流量、攻击流量以及出流量，如图 5，同时可以看出攻击峰值、攻击源、攻击占比、攻击流量类型、攻击源地址等信息，方便客户了解攻击情况。

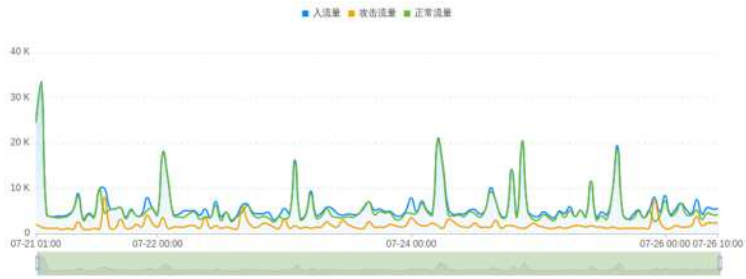

图 5　流量清洗趋势图（bps）

3.3 入侵检测能力

通过省内安全底座或者集中运营管理平台可以看到入侵监测的威胁地址，还可以实时检测网络流量，监控各种网络行为，对非法的、不正常的、含攻击行为的报文能及时报警和检测，实现从事前检测、事中告警到事后取证全流程保护客户信息系统和网络架构安全。

总结

本文通过融合网内安全设备，建设算网安全资源池，构建了多维度高防系统，多样化网络安全服务，针对各类攻击威胁秒级响应，超强的处理能力，极低的清洗时延，能够高效为全网边缘云、专线、IDC 等客户应对大流量 DDos 攻击和 WEB 攻击等，同时为客户提供一站式服务，按需定制，自主进行监控管理。

随着数字经济的不断发展和新技术的不断涌现，算网安全资源池将面临更多的挑战和机遇。一方面，需要不断跟进安全发展趋势和用户需求，持续优化和完善系统功能和服务；另一方面，还需要应对日益复杂和多样化的攻击手段和技术挑战，提升系统的安全防护能力和响应速度。为了应对这些挑战和抓住机遇，我们将进一步加强技术研发和创新投入，推动算网安全资源池的持续优化和升级。同时，还将加强与行业内其他企业和机构的合作与交流，共同推动云计算和网络安全领域的发展与进步。

参考文献

[1]赵鹏程，于俊清，李冬.一种基于深度学习的 SRv6 网络流量调度优化算法[J].信息网络安全，2024，24（02）：272-281.
[2]肖定.浅谈 SRv6 在新型城域网中的云网一体承载应用方案[J].通讯世界，2024，31（01）：4-6.
[3]王宏杰，徐胜超，杨波，等.基于 SRv6 技术的云网安全服务链自动编排方法[J].计算机与现代化，2024（01）：1-5+12+28.
[4]徐宝辰，余思阳，李长连，等.基于 SRv6 和流量负载的新型高防系统研究[J].邮电设计技术，2023（08）：38-41.
[5]杨波，徐胜超.基于 SRv6 服务链的云网专线场景安全防护方法[J].计算机与现代化，2023（08）：107-111.