基于APN6的威胁溯源与网安联动防护技术研究

Research on Threat Tracing and Network Security Coordinated Defense Technology Based on APN6

黎　宇[1]，周婧莹[1]，梁洪智[1]，彭紫璇[2]（1. 中国联通广东分公司，广东 广州 510000；2. 中讯邮电咨询设计院有限公司广东分公司，广东 广州 510627）

Li Yu[1], Zhou Jingying[1], Liang Hongzhi[1], Peng Zixuan[2] (1. China Unicom Guangdong Branch, Guangzhou 510000, China; 2. China Information Technology Designing & Consulting Institute Co., Ltd. Guangdong Branch, Guangzhou 510627, China)

摘　要：

随着互联网技术的发展，IPv6网络规模不断扩大，安全威胁也不断增加。传统防护方式存在部署贵、溯源难、处置慢等问题。对基于APN6、SDN和网络感知技术的威胁溯源进行研究，并提出了一种基于APN6威胁溯源与网安联动的网络安全防护方案。该方案将IPv6原生、APN6流量标识、业务灵活编排的特性与网络安全需求巧妙结合，能够有效识别和定位网络威胁，并采取相应的防护措施形成进源阻断，快速精准地溯源威胁，确保IPv6网络的稳定运行。

关键词：

APN6；威胁溯源；网安联动；SDN

doi：10.12045/j.issn.1007-3043.2026.05.010

文章编号：1007-3043（2026）05-0051-06

中图分类号：TN915

文献标识码：A

开放科学（资源服务）标识码（OSID）：

Abstract:

With the continuous advancement of Internet technology, the scale of IPv6 networks has been expanding substantially, accompanied by escalating security threats. Traditional security protection methods face challenges such as high deployment costs, difficulties in threat traceability, and delayed incident response. It focuses on research concerning threat traceability based on APN6, SDN, and network sensing technologies. It proposes a cybersecurity protection scheme featuring collaborative APN6-based threat tracing and network security linkage. The proposed solution effectively integrates native IPv6 characteristics, APN6 traffic identification capabilities, flexible service orchestration features with cybersecurity requirements. It enables efficient threat identification and precise localization while implementing source-based blocking through coordinated protective measures. This approach achieves rapid and accurate threat tracing, thereby ensuring stable operation of IPv6 networks.

Keywords:

APN6; Threat traceability; Cybersecurity coordination; SDN

引用格式：黎宇，周婧莹，梁洪智，等. 基于APN6的威胁溯源与网安联动防护技术研究[J]. 邮电设计技术，2026（5）：51-56.

1 概述

IPv6网络作为下一代互联网的重要组成部分，在全球得到了广泛应用。然而，随着IPv6规模的扩大，网络攻击和安全威胁也随之增加[1-2]。传统网络安全方案难以应对IPv6网络的多样性和复杂性，因此亟需一种高效、智能的网络安全防护机制。

应用感知型IPv6网络（Application-aware IPv6 Networking，APN6）技术作为IPv6网络的安全防护工具，在威胁检测与响应方面具有重要应用价值。结合SDN架构，可以通过网安联动的方式实现对潜在威胁的提前识别和快速处置。本文基于某运营商的一项实际应用案例，提出了一种基于APN6威胁溯源与网安联动的网络安全防护方案。

收稿日期：2026-03-25

目前，安全威胁增长迅猛，根据瑞星《2023年中国网络安全报告》，2023年病毒样本总量为8 456万，增长了14.98%[3]，感染次数为0.9亿次；勒索软件样本为65.59万，增长了13.24%，感染次数为19.68万次；网络钓鱼攻击事件总数约16亿起，增长了166%；挖矿病毒样本量为315.24万，增长了20.78%，感染次数为21.62万次。

而传统防护方式存在部署贵、溯源难、处置慢三大痛点。

a）企业末梢节点部署专用安全防御设备成本高。按照传统边界防护的思路，需在所有分支边界部署防火墙和未知威胁检测设备，而企业分支众多，部署成本高且无法做到所有分支均部署。

b）威胁难以快速溯源，隐患长时间无法消除。网络检测到威胁之后，无法快速准确定位威胁发生的源头，需要通过人工比对、排查等方式进行溯源，在此期间无法阻断威胁扩散。

c）威胁处置效率低，无法形成近源阻断。安全设备部署位置较高且集中，无法在网络边缘处置威胁，导致威胁处置效果不佳。

国内主流的网络设备厂商、安全厂商均已认识到威胁自动处置的必要性，但传统的网络厂商由于缺乏安全威胁检测和处置能力，无法很好地协同安全和网络。安全厂商对威胁检测和处置有较强的技术优势，但仅能通过联动传统的安全设备如防火墙对威胁进行处置；且由于安全设备部署位置较高且集中，无法在网络边缘处置威胁，威胁处置效果不佳；同时，威胁溯源较困难，难以精确溯源威胁的发生位置。市场上缺乏满足政企客户，特别是在总部-支部网络场景下，快速精准溯源威胁、及时阻断安全威胁需求的产品，因此本文基于APN6技术的网安联动提出了新的解决思路。

2 相关技术

2.1 APN6

APN6是一种新的网络架构，它利用IPv6报文自带的可编程空间，将应用信息（标识和/或网络性能需求）携带进入网络，使能网络感知应用及其需求，进而为其提供精细的网络服务和精准的网络运维。APN6共包含3个关键要素[4]，具体如下。

a）开放的应用信息。APN6通过Native IPv6报文自带的编程空间携带应用信息，包括标识信息（APN ID）和应用对网络的需求信息（APN Parameters），可针对不同应用（类/组）流量进行精细化区分和网络内调度。封装和携带应用信息的权利是面向应用开放的，应用可以根据需要自主选择。

b）丰富的网络服务。近年来，随着网络技术的不断发展，为应用提供的网络服务越来越丰富，包括SRv6 TE Policy、网络切片、SFC等，能够保障不同应用的各种差异化需求。APN6可以和这些网络新型技术结合，使能更加精细化的网络服务。例如，APN6结合网络切片技术，可以精细地为某个/组关键应用和用户提供专属网络切片，划分专属资源，提供差异化的SLA和可靠性保障。

c）准确的网络测量。网络测量技术不断丰富，APN6可以和网络测量技术相结合，提供应用级精细化可视、实时性能测量和快速故障定界等能力，使能网络精准运维。

2.2 APN ID标识技术

APN6通过扩展IPv6数据平面，携带APN Attribute（APN报文所携带的应用信息）。APN Attribute被携带在IPv6的目的选项报文头（Destination Options Header，DOH）中[5]（见图1）。DOH的报文头类型值为60，它通过Option Type标识APN6选项类型来携带APN Attribute，Option区块字段解释如表1所示。

IETF定义了APN Header的格式，如图2所示。其中，APN ID用于精细标识关键的应用或用户，引导进

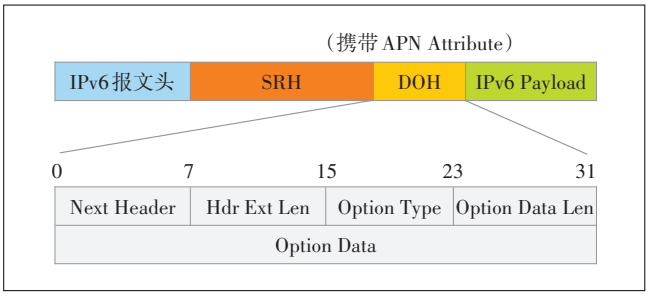

图1　APN标识位置示意

表1　Option区块字段解释

字段名	长度	含义
Option Type	8 bit	指明当前选项的类型，选项类型不同时，Data区域的数据格式也不同
Option Data Len	8 bit	指明当前选项Data区域的长度，单位为字节
Option Data	长度可变	当前选项的数据内容。此字段需使整个目的选项报文头的长度为8 B的整数倍，当数据长度不足时，可以使用填充选项

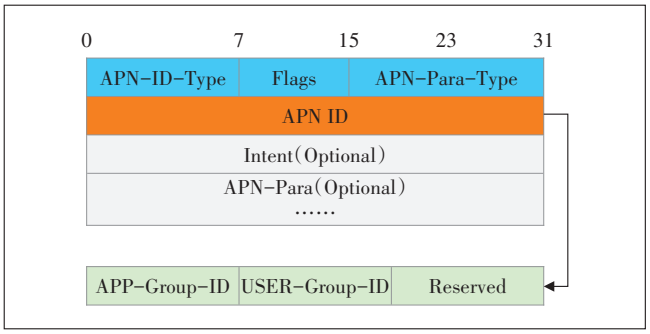

图2　APN Header的格式

入相应的SRv6 Policy隧道、网络切片、确定性网络（Deterministic Networking，DetNet）路径或业务功能链（Service Function Chain，SFC）路径等，实现应用分流和灵活选路。APN Header各字段的含义如表2所示。

表2　APN Header各字段的含义[6]

字段	含义
APN-ID-Type	1 B，APN ID的类型
Flags	1 B，当前未定义
APN-Para-Type	2 B，APN-Para的类型，描述了APN-Para里包含的网络性能的需求参数，可包括带宽、时延、抖动、丢包率。此字段暂未使用，填充保留值
APN ID	应用唯一对应的APN标识信息编号，由以下3部分组成： a）APP-Group-ID：应用组的标识信息，长度可变，由配置决定 b）USER-Group-ID：用户组的标识信息，长度可变，由配置决定 c）Reserved：预留字段
Intent(Optional)	可选，4 B，描述向网络提出的一组意图需求
APN-Para (Optional)	可选，网络性能需求参数的具体内容信息，每个参数使用4 B，包含哪些参数由APN-Para-Type决定

3 技术框架与关键技术

本项目利用APN ID全网唯一性（最大64 bit）、不随转发路径和跳数而变的独有特点，创造性地实现以APN ID、SDN控制器为核心的网安联动威胁溯源及处置（见图3）。

a）在接入侧，按照用户溯源表分配的唯一APN ID，随流添加，并随业务流量封装到IPv6头部。

b）在网络侧，通过部署支持APN6流量解析的探针、SDN控制器和安全态势感知平台实现威胁检测和威胁分析。通过APN6标识精准识别威胁源的位置，通过SDN控制器联动网络边缘设备（如路由器等）实现近源自动处置威胁，避免威胁扩散到网络的其他位

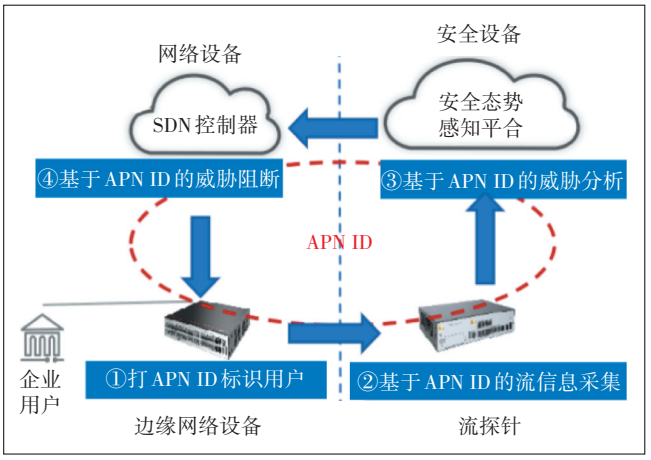

图3　网安联动威胁溯源及处置示意

置，实现全网安全监测和联动处置，构建主动纵深防护体系。

通过网络+安全设备协同联动形成存量升级易部署、自动化处置易运维、精准易溯源的网络安全防护技术方案。

3.1 APN6网安联动精准溯源架构

APN6网安联动精准溯源由智能分析层（APN态势感知平台）、管控层（网络控制器）和执行层（路由器、探针设备）3层组成（见图4）。

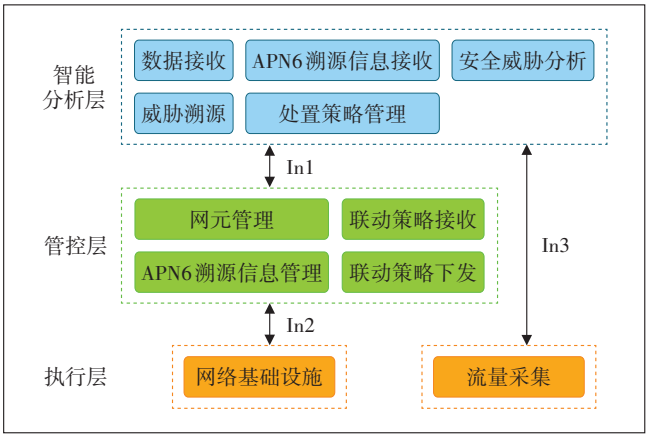

图4　APN6网安联动精准溯源方案架构

a）执行层。该层由网络基础设施和流量采集探针2个部分组成。其中，网络基础设施负责按照溯源规划表的APN ID设计（对应接入单位的接入位置信息/服务器/应用信息等）给用户流量打上标识；流量采集探针则支持APN6协议报文解析及入侵检测等能力，通过采集网络流量，将MetaData数据与威胁日志发送给智能分析层。

b）管控层。管控层是网络设备的控制大脑，同时与智能分析层进行协同。该层一方面按照溯源表规划完成相应网络边缘设备的APN ID标识，另一方面接收智能分析层下发的联动策略，并根据APN ID动态溯源到合适的威胁阻断点，向执行层的网络基础设施下发、撤销联动策略。

c）智能分析层。智能分析层实现威胁分析，并协同管控层实现自动近源处置。该层南向对接流量探针，接收流量探针的APN ID+流信息，并进行大数据关联威胁分析，通过APN ID关联威胁接入单位，实现基于APN ID的高级威胁分析能力，如IPS引擎、信息泄露、凭证窃取、注入检测、网站后门、拒绝服务等Web攻击检测能力，渗透、C&C通信、利用隐蔽通道进行数据外发等威胁。同时，对接管控层，实现威胁事件发生时，向管控层下发基于APN ID的联动策略威胁事件。

3.2 关键技术要求

3.2.1 APN标识技术要求

在APN6网安联动中，APN标识代表流量接入网络的位置，能明确标识流量的接入位置和接入单位。APN标识的技术要点如下。

a）APN标识在APN6网络域内全网唯一。

b）APN6网安联动的APN标识被携带在User-Group中，包含Device ID、Interface ID和VPN ID 3个字段（见图5），3个字段组合可以唯一确定流量的接入位置。

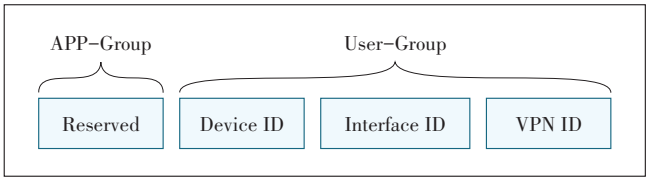

图5　APN标识

（a）Device ID：用于标识设备，每个网元分配全网唯一的ID，可基于Device ID获取对应的网元。

（b）Interface ID：用于标识接入接口，表示网元接入VPN的接口信息。

（c）VPN ID：用于标识VPN，每个VPN分配一个ID，不同网元相同的VPN使用相同的ID值。

c）APN标识模板在APN6网络域内全网唯一。

d）APN6网安联动的APN标识的3个字段可以灵活调整，但总长度不能超过APN标识的总长度，本文规定的APN标识模板示意如图6所示。

字段定义	字段1	字段2	字段3
字段类型	Device ID	Interface ID	VPN ID
字段长度/B	9	12	8

图6　APN标识模板示意

3.2.2 APN6溯源表技术要求

APN6溯源表用于承载网元、接口、VPN信息和APN标识的对应关系，基于APN标识能唯一查询到一条流量的接入位置，用于溯源威胁事件的接入单位和指导控制器下发联动处置策略。

APN6溯源表格式如图7所示。

网元描述			APN标识（APN ID）			APN ID描述（description）
网元名称	VPN名称	接口名称	Device ID	Interface ID	VPN ID	

图7　APN溯源表格式

a）网元描述中的网元名称、VPN名称、接口名称字段为字符串格式，各字段定义如下。

（a）网元名称：接入设备名称，即管控层纳管设备的设备名称，通过该名称管控层可管理和控制该网元。

（b）VPN名称：VPN名称与网络规划保持一致，智能分析层根据VPN名称创建一级租户。

（c）接口名称：VPN接入的接口名称，联动策略下发的接口。

b）APN标识（APN ID）中的Device ID、Interface ID、VPN ID字段为整数值格式，最大值转化为二进制串后的长度不超过各字段定义的长度（具体如图6所示）。

c）APN ID描述为字符串格式，代表接入单位名称。智能分析层基于该字段创建二级租户，实现威胁事件的接入单位级溯源

4 现网部署方案

基于运营商城域网实现基于APN6的安全威胁联动网络边缘设备（比如路由器等）精准溯源及近源自动处置。如图8所示，态势感知平台接收探针解析的APN ID以及安全事件，并结合溯源表分析威胁流量客户归属，判断大网威胁阻断点，生成联动阻断策略，调

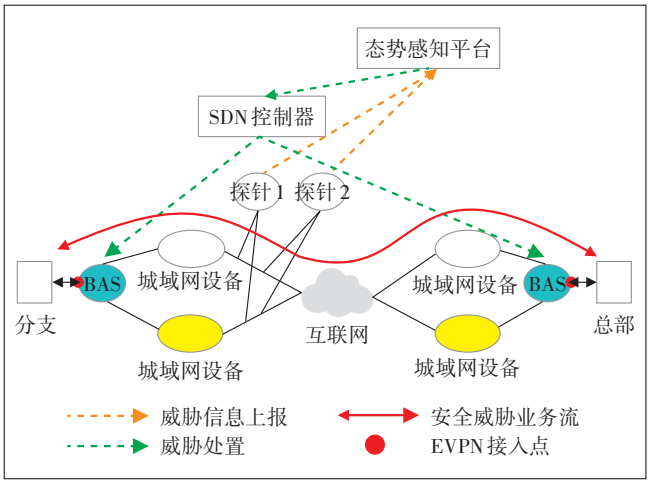

图8　APN6网安联动威胁溯源及处置部署拓扑

度网络控制器在大网相应的网络设备下发执行。

APN6网安联动威胁溯源及处置业务流程如图9所示，关键实施步骤如下。

a）运营人员规划生成溯源表（APN ID、设备、VPN、接口等），导入到网络控制器。

b）网络控制器通知态势感知平台溯源表有更新后，由态势感知平台查询全量溯源表信息。

c）运营人员根据溯源表规划向路由器配置APN ID。

d）路由器将APN ID封装到报文中，支持基于VPN封装APN ID并随流转发。

e）探针部署点镜像流量到探针，探针解析SRv6报文，获取流信息和APN ID信息并上报态势感知平台。

f）态势感知平台根据APN ID查询威胁流量所属的接入单位名称。

g）态势感知平台通过大数据关联分析发现威胁，自动向网络控制器下发联动策略（APN ID、流信息、阻断动作）。

h）网络控制器根据APN ID和流信息查询溯源表，获取威胁阻断点位置（接入接口），向网络设备下发策略阻断威胁。

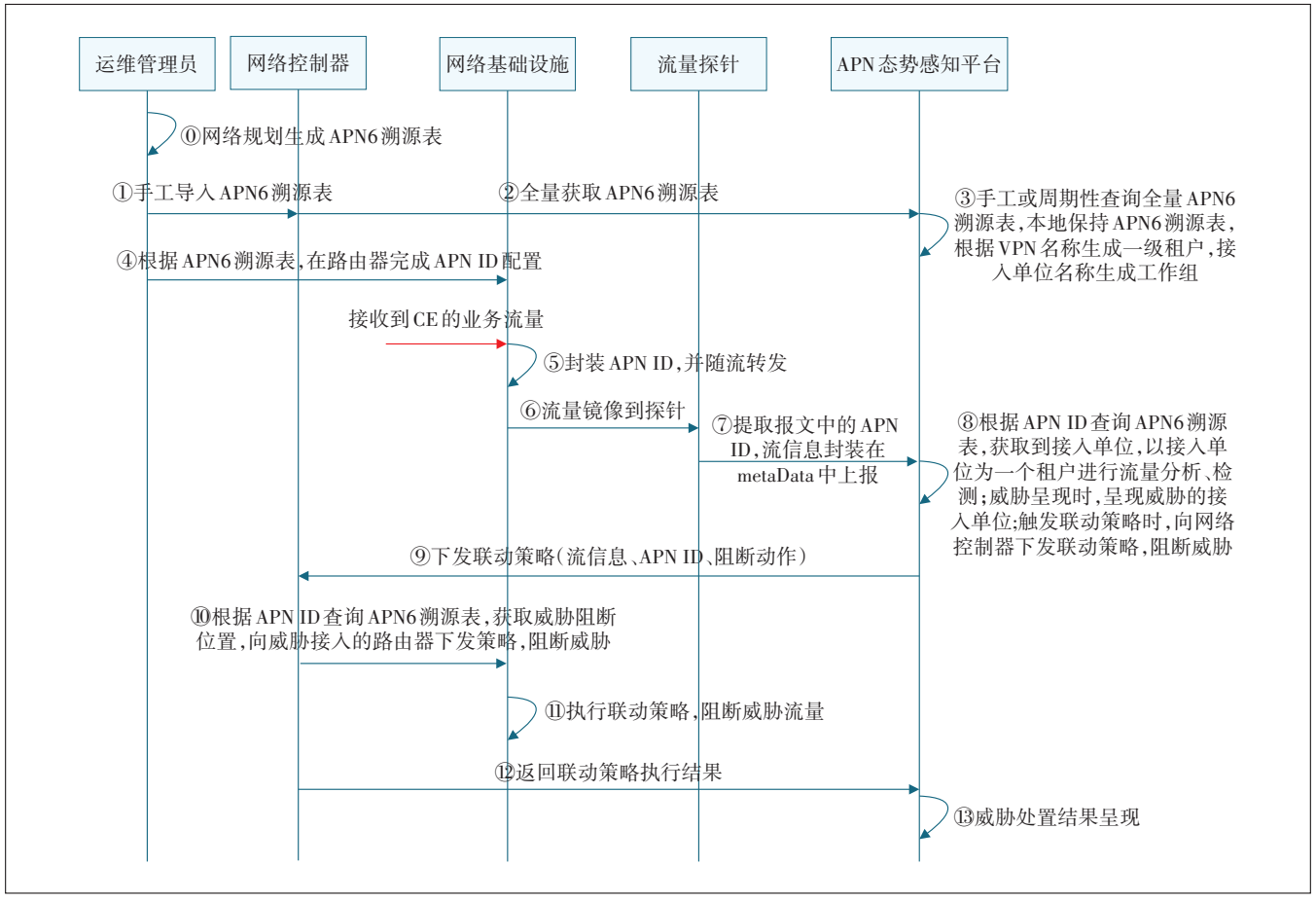

图9　APN6网安联动威胁溯源及处置业务流程

i）网络设备执行阻断策略，阻断威胁流。

j）根据APN ID查询APN6溯源表，获取威胁阻断位置，向威胁接入的路由器下发策略，阻断威胁。

k）执行联动策略，阻断威胁流量。

l）返回联动策略执行结果。

m）威胁处置结果呈现。

5 业务场景及成效说明

本文提出的“基于APN6威胁溯源与网安联动的网络安全防护技术”主要用于企业专线（典型用户为医共体、K12校园、政务外网等行业威胁检测、威胁阻断）、互联网专线（典型用户为金融、高新技术等总部—分支企业的威胁检测、威胁阻断）上的安全能力叠加，可在用户侧无需任何部署的前提下，提供精准快速溯源、阻断安全威胁的增值服务。

2024年，在某两家企业开展了基于APN6网安联动的创新技术试点验证，并于2024年8月完成业界首个APN6网安联动试点，实现总部—分部互联安全防护（见图10）。该试点在运营商网络集中进行威胁检测，精准溯源并近源阻断，单条威胁事件处置效率由小时级提升至分钟级。

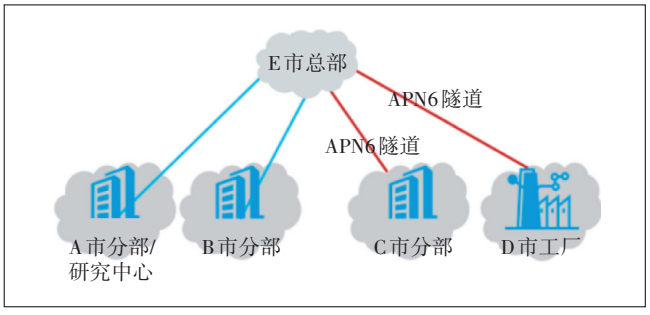

图10　企业总部—分支示意

6 结束语

本文提出的基于APN6威胁溯源与网安联动的网络安全防护方案在技术设计上充分考虑了IPv6网络的安全特性，并结合SDN架构和威胁溯源技术，实现了对网络威胁的高效感知与快速响应。通过实际案例分析，验证了该方案在实际应用中的可行性和有效性，并取得以下创新。

6.1 技术创新

业界首创将IPv6+网络技术与安全检测、威胁处置能力相结合，基于APN ID实现网安联动、精准溯源、自动处置。

a）APN ID作为关键key，串接网络与安全处理全流程，实现协同联动。通过APN ID将边缘接入、流量采集、威胁分析、威胁通告、阻断策略全流程进行串接，实现网安联动。

b）基于APN ID的整网唯一性，实现威胁事件精准溯源。APN ID与用户信息建立唯一映射关系，全局携带，不随转发处理而变化。威胁事件精准溯源接入单位，显著提升安全运营效率，有效解决了“虽然感知到威胁，但是无法快速溯源”的痛点问题，威胁检出率达96%以上，溯源率为100%。

c）安全威胁通告携带APN ID，与控制器对接实现分钟级自动威胁处置。安全态势感知平台识别到威胁后，通告给控制器指示边缘网络设备自动阻断威胁流量，实现自动近源处置，端到端可实现分钟级处置。

6.2 产品及商业模式创新

通过APN6流量标识能力实现网络能力与安全能力的无缝对接，解决了传统安全局限性、安全和网络无法协同等难题，实现大网集约化感知威胁，自动编排网络及安全策略，并精准溯源、及时阻断用户安全威胁的创新管理模式。

参考文献：

[1] 赵云龙，杨继，于运涛，等. 基于威胁情报关联的APT攻击识别与溯源技术[J]. 网络安全与数据治理，2024，43(8)：15-21，27.

[2] 唐晓萌，任凯，滕俐军，等. IPv6网络攻击事件溯源中的攻击树节点特征定位[J]. 计算技术与自动化，2024，43(2)：145-150.

[3] 北京瑞星网安技术股份有限公司. 2023年中国网络安全报告[R/OL]. 北京：北京瑞星网安技术股份有限公司，2023.

[4] 何林，况鹏，王士诚，等. 基于“IPv6+”的应用感知网络（APN6）[J]. 电信科学，2020，36(8)：36-42.

[5] 李振斌，赵锋. “IPv6+”技术标准体系[J]. 电信科学，2020，36(8)：11-21.

[6] 华为. IP网络系列丛书[EB/OL]. [2026-01-26]. https://e.huawei.com/cn/topic/enterprise-network/ip-ebook.

作者简介：
黎宇，正高级工程师，硕士，主要从事云计算技术、IP网、网络安全技术研究和应用工作；周婧莹，高级工程师，硕士，主要从事运营商云网安全防护及安全能力价值输出等工作；梁洪智，工程师，学士，主要从事网络信息安全、云网安全以及云网运营等工作；彭紫璇，工程师，学士，主要从事运营商云计算、云安全相关咨询设计工作。