基于SASE架构的主动免疫安全威胁防御机制研究

Research on Dynamic Immune Security Threat Defense Mechanism Based on SASE Architecture

杨丽丽[1]，张小梅[2]，由志远[1]，刘　果[1]，戚大强[1]（1. 中讯邮电咨询设计院有限公司，北京 100048；2. 中国联合网络通信集团有限公司，北京 100033）

Yang Lili[1], Zhang Xiaomei[2], You Zhiyuan[1], Liu Guo[1], Qi Daqiang[1] (1. China Information Technology Designing & Consulting Institute Co., Ltd., Beijing 100048, China; 2. China United Network Communications Group Co., Ltd., Beijing 100033, China)

摘　要：

针对传统SASE“静态规则库依赖”和“协同缺失”对未知威胁适应性不足的核心问题，提出动态免疫的启发式SASE防御框架。基于云网边端协同架构构建仿生免疫系统，实现“态势感知—智能决策—动态响应—自主进化”的闭环自适应机制。重点论证了基于ATT&CK战术的威胁基因编码技术、基于边缘—云跨层检测与深度分析的决策协同机制和基于联邦进化模型驱动的动态策略进化模型3个核心方法论，为构建“主动免疫型”网络安全体系提供理论支撑。

关键词：

SASE架构；威胁建模；协同决策；动态免疫

doi：10.12045/j.issn.1007-3043.2025.09.002

文章编号：1007-3043（2025）09-0009-05

中图分类号：TN915.08

文献标识码：A

开放科学（资源服务）标识码（OSID）：

Abstract：

Addressing the core issue of insufficient adaptability to unknown threats in traditional SASE due to “static rule library dependence” and “lack of collaboration” by proposing a heuristic SASE defense framework based on dynamic immunity. By constructing a bio—inspired immune system based on a cloud—edge—end collaborative architecture, a closed-loop adaptive mechanism encompassing “situational awareness—intelligent decision making—dynamic response—autonomous evolution” is achieved. The framework focuses on three core methodologies: threat gene encoding technology based on ATT&CK tactics, decision-making collaboration mechanism based on cross-layer detection and deep analysis at the edge-cloud, dynamic strategy evolution model driven by federated evolution model, providing theoretical support for building an “active immunity type” network security system.

Keywords：

SASE architecture; Threat modeling; Collaborative decision-making; Dynamic immunity

引用格式：杨丽丽，张小梅，由志远，等. 基于SASE架构的主动免疫安全威胁防御机制研究[J]. 邮电设计技术，2025（9）：9-13.

1 概述

1.1 研究背景与挑战

随着企业数字化转型进程加速，网络架构正经历根本性变革。一方面，远程办公模式的常态化与IoT设备的大规模接入彻底瓦解了传统网络边界。另一方面，云计算与5G边缘计算的普及推动业务负载向“云—边—端”分布式架构迁移。这种变革在提升业务灵活性的同时，也使得攻击面呈现爆炸性增长，传统基于边界防护的安全模型彻底失效。

在此背景下，SASE（Secure Access Service Edge）作为融合网络与安全的云原生架构，成为应对边界消失的主流解决方案。然而，当前SASE实践暴露三大关键挑战：其一，跨层级数据孤岛阻碍全局防护视野。终端行为日志、边缘流量数据、云端威胁情报分散于独立系统，传统IOC（Indicators of Compromise）难以描述攻击的战术意图关联性。例如，某次勒索攻击可能从终端漏洞利用开始，经边缘节点横向移动，最终在

收稿日期：2025-07-07

云端实施加密，但碎片化数据导致防御体系无法构建完整的攻击链视角，大幅降低主动拦截能力。其二，边缘与云端能力割裂引发协同困境。当前SASE架构中，边缘节点（MEC）侧重实时流量处理，云端专注深度分析，二者缺乏有效的协同决策机制。例如，边缘检测到低置信度威胁时，需全量上传数据至云端验证，导致关键响应延迟。而在5G场景下，工业控制、自动驾驶等业务要求威胁处置延迟低至毫秒，现有架构难以兼顾检测精度与实时性。其三，静态防御机制难以应对动态威胁演化。现有SASE方案依赖预定义规则库与签名检测技术，面对APT攻击的持续变异显得力不从心。MITRE ATT&CK统计显示，2023年新型攻击技术增长率达42%，攻击者通过组合多战术形成复杂攻击链，而静态规则更新周期通常滞后24 h以上，导致防御窗口失效[1]。

这些挑战本质上是安全范式与架构变革脱节的结果，在边界消失、威胁动态化的新环境中，传统SASE仍延续中心化、静态化的防御思维。因此，亟需构建一种具备系统适应性的动态协同防御理论，实现从“被动响应”到“主动免疫”的范式跃迁。

1.2 研究目标与创新

本研究旨在构建一种具有系统适应性的动态防御理论模型，以解决传统SASE架构在边界瓦解、威胁动态化环境中的根本性局限。核心目标包含如下3个维度。

a）威胁基因编码技术。设计基于ATT&CK战术链的“威胁基因”表达体系，突破传统IOC的碎片化局限，为攻击行为提供结构化、可演化的描述框架。

b）跨层联动机制。提出边缘—云跨层联动机制，在保障隐私的前提下实现全局策略生成与边缘执行的动态协同，平衡实时性与检测精度的矛盾。

c）动态策略进化模型。通过边缘和云端策略智能计算分流机制和动态参数调整机制实现防御自适应调整，确保防御体系始终处于最优状态。

该模型致力于为下一代SASE架构提供可证明、可扩展的理论基石，推动安全防御从“规则驱动”升级为“意图驱动”。

2 系统主动免疫防御模型设计

2.1 系统主动免疫核心组件

基于运营商边缘—云网协同基础设施，构建系统化的主动免疫安全威胁防御体系具备完备的物理基础。零信任、安全网关等终端具备终端固有免疫层能力，终端代理提供非特异性基础防御，通过动态认证与环境感知实现即时威胁阻断（如未授权设备拦截），无需依赖特定威胁特征。MEC轻量化安全引擎提供边缘局部免疫能力，对于5G用户的边缘侧实现精准化局部防御，通过行为特征识别潜在威胁并限制其影响范围。云网协同具备适应性免疫能力，进行高智能特异性响应，基于深度学习的攻击链解析生成定制化防御策略。威胁基因库具备全局免疫记忆能力，持久化存储威胁特征与应对经验，使系统再次遭遇同类攻击时快速响应，系统主动免疫涉及核心组件如表1所示。

表1　主动免疫涉及核心组件

传统SASE	主动免疫概念	系统主动免疫组件	安全功能
终端策略执行	皮肤屏障	零信任、安全网关等终端代理	设备认证与环境合规性检查以及动态访问控制策略执行
边缘流量中转	巨噬细胞	MEC轻量防护引擎	实时阻断已知威胁（如恶意IP、签名病毒）
云端集中管控中心	淋巴细胞	云端AI分析中心	深度威胁识别，整合多源数据构建攻击知识图谱
网络策略访问控制	抗体	动态微隔离策略	生成定制化“抗体”（微隔离策略、WAF规则等），对攻击进程隔离与阻断
IOC知识库	免疫记忆	威胁基因库	结构化记录ATT&CK战术序列，存储战术-防御策略映射关系

2.2 4个阶段自适应闭环架构

该架构通过4个阶段闭环设计，将主动免疫系统的分布式感知、特异性识别、协同清除、记忆进化四大核心机制转化为可工程实现的网络安全范式，为构建具备自主演进能力的动态防御体系奠定理论基础。感知层通过终端代理实时捕获设备行为、网络流量、环境状态等原始信号，边缘节点提取ATT&CK战术序列，压缩为轻量基因编码。决策层通过MEC轻量模型对基因片段进行置信度评估，低置信度事件上传云端，通过知识图谱推理攻击意图[2]。响应层下发微隔离策略至边缘节点，隔离受感染终端，网络层同步清洗恶意流量，终端代理终止恶意进程。进化层将新型攻击特征（如0day漏洞利用）结构化存储为战术基因，基于边缘节点本地数据的联邦学习，动态调整基因特征权重，利用损失函数优化检测模型[3]。4个阶段的闭环架构如图1所示，其核心创新在于建立威胁处置与能力进化的正反馈循环，使系统防御效能随时间呈指数增长，而非传统架构的线性衰减。

2.3 核心方法论

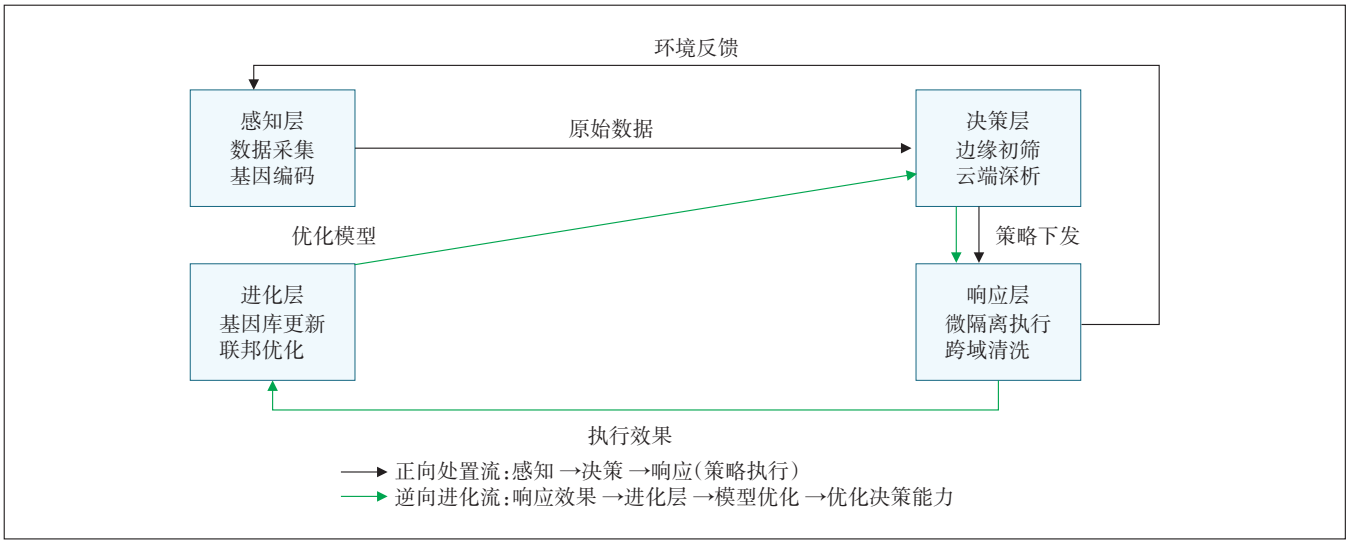

图1　4个阶段自适应闭环逻辑图

2.3.1 威胁基因编码理论

威胁基因编码理论通过将碎片化IOC与ATT&CK战术意图融合为结构化基因向量，从根本上解决传统威胁情报的高碎片化问题，并基于基因编辑距离量化攻击家族的同源性（如勒索软件变种从v1到v2的演化追踪），为构建具备血缘感知能力的动态防御体系提供理论基石[4]。其基本步骤如下。

步骤1：原始数据采集。数据来源为终端日志、网络流量、边缘节点检测日志、云端审计记录等，采集内容包括行为数据（进程创建、文件操作、网络连接等）、流量数据（五元组、载荷特征、协议行为）和环境数据（设备指纹、用户身份、地理位置）。

步骤2：战术特征提取。包括T_i和P_i，其中T_i表示第i个ATT&CK战术的置信度得分，取值[0,1]，使用预训练的ATT&CK分类器（如LSTM或Transformer）从采集的原始数据中识别战术；P_i表示第i个ATT&CK战术的权重，由现有威胁情报平台及APT攻击检测系统统计该种攻击出现的频率，并把它作为ATT&CK战术的权重依据。

步骤3：IOC特征压缩。

a）聚类。将相似IOC聚类（如同一C2家族的IP归为同一类），原始威胁指标集合（IP、域名、文件哈希等）生成节点node。

b）嵌入。使用图神经网络将聚类后的每个IOC节点嵌入为向量，从粗粒度IOC数据堆砌升级为高价值威胁信号。即：

$$u_k=\mathrm{GNN}(\mathrm{node}_j,\mathrm{ATT\&CK知识图谱})$$

c）聚合。对同一事件的多个IOC向量求均值：

$$\Psi(\mathrm{IOC})=\mathrm{mean}(\{u_1,u_2,\ldots,u_k\})$$

步骤4：融合计算。将异构的战术和IOC特征映射到同质基因空间，实现威胁事件的“语义聚合”，将同一攻击团伙的分散IOC聚合为单一向量。

$$\mathrm{Gene}_j=(\sum P_i\delta(T_i),\Psi(\mathrm{IOC}))\in R^d$$

步骤5：威胁基因变种分析。威胁基因变种分析主要通过向量距离来计算变种演化关系，如威胁事件A和事件B的基因变种距离可用于攻击血缘分析和动态防御进化的核心指标[5]。

$$\text{变种距离}=1-\frac{\mathrm{Gene}_A\times\mathrm{Gene}_B}{\|\mathrm{Gene}_A\|\|\mathrm{Gene}_B\|}$$

2.3.2 边缘—云跨层联动机制

在边缘侧的安全防护体系中，边缘—云跨层联动机制通过多组件协同实现高效威胁阻断。零信任网关作为第1道防线，基于SDP架构实施动态身份验证，持续评估设备、用户及环境风险，对未授权访问实时拦截[6]。轻量级AI检测引擎以极低延迟分析流量与行为，通过微型CNN模型识别异常模式（如可疑加密行为），当置信度超过阈值时立即触发处置流程。微隔离模块则根据策略自动执行精细化隔离，将受感染终端划入安全域，阻断横向移动路径（如RDP爆破、PsExec攻击），同时保留关键业务通信。边缘节点通过加密通道与云端中枢保持实时同步，动态加载云端下发的基因化威胁指标（如勒索软件战术指纹），将其转化为本地拦截规则，确保防御策略与最新威胁态势同步，跨层联动示意如图2所示。

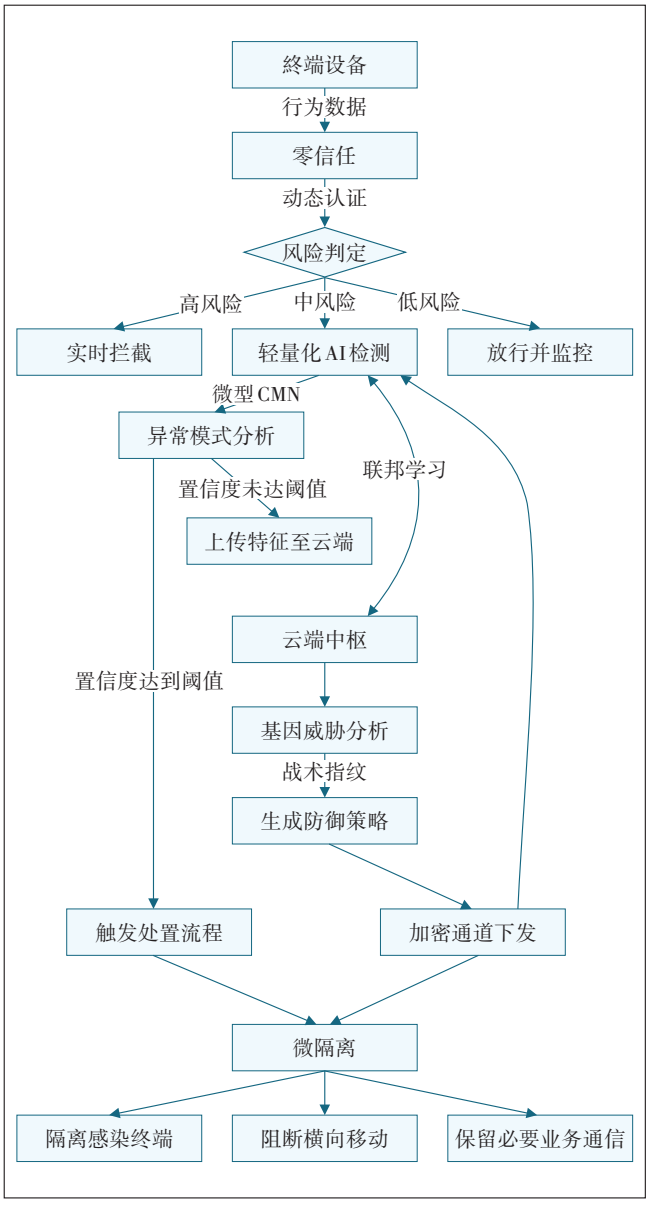

图2　边缘—云跨层联动示意

这种分层协作机制既保障了边缘侧的实时响应能力，又通过云端情报赋能弥补本地检测视野的局限性，形成兼具敏捷性与全局观的防御体系[7]。

2.3.3 动态策略进化模型

边缘—云跨层协同运作实现了威胁的即时处置，防御体系具备真正的进化能力，更依赖于持续的知识积累和策略优化。

边缘节点动态策略进化采用动态调节的检测阈值，初始值设定为行业安全标准，当感知到攻击频率上升时自动进入超敏感模式，威胁平息后则恢复基准状态，这种弹性机制有效解决了检测精度与误报率的矛盾。同时，边缘侧对明确的高危威胁实施毫秒级阻断，而对可疑行为则触发深度分析，形成分级响应体系[8]。

云端中枢通过隐私保护的方式聚合全局威胁情报。边缘节点仅上传最具价值的模型参数变化，并添加符合严格标准的保护性噪声，确保知识共享过程的安全合规。云端对这些信息进行深度关联分析，识别跨区域的攻击模式，将碎片化威胁情报转化为可执行的防御策略。这种机制既保留了边缘侧的敏捷性，又赋予系统持续进化的认知能力。

为实现资源高效利用，系统需要建立智能计算分流机制。边缘设备处理高置信度威胁，而将中低置信度事件交由云端研判，通过动态卸载使边缘计算负载降低。系统还采用自适应资源管理策略，根据威胁态势和组件效能动态调整资源分配，确保防御体系始终处于最优状态。

3 可行性分析

3.1 理论可行性分析

本研究在理论层面具有多维度的可行性支撑。首先，传统SASE架构依赖静态规则库，防御更新滞后于攻击演化，而动态基因库的自主演化机制能够实现实时威胁适应，确保防御策略的动态调整与攻击演化同步。其次，传统方案因云端集中分析引入高延迟，而主动免疫防御机制采用边缘实时阻断与云端异步优化的协同机制，在理论上兼顾了响应速度与检测精度，符合低延迟高可靠的安全需求。此外，面对未知威胁时，传统SASE依赖人工介入导致分析效率低下，而通过威胁基因编码技术沉淀战术链特征，使系统具备自主识别和处置新型攻击的能力，提升了智能化水平[9]。

3.2 技术可行性分析

本研究的技术实现分为3层：基因编码层、协同决策层和进化层，形成端到端的智能威胁检测进化框架。

在基因编码层，采用Node2Vec图嵌入算法对攻击行为序列建模，构建行为特征图（节点=攻击实体，边=依赖关系），并通过Skip-gram训练生成低维向量（如128维），保留攻击链的上下文语义。同时，结合MITRE ATT&CK官方威胁评分（如CAPEC Meta-Attributes或ATT&CK评估数据），采用层次分析法（AHP）动态分配战术权重（如Initial Access权重高于

Discovery），确保特征编码贴合实际威胁优先级[10]。

协同决策层采用边缘—云协同架构。边缘侧部署轻量化MobileNetV3-Small（<5 MB），通过量化感知训练（QAT）压缩至INT8精度，输入基因编码向量后输出实时威胁分类（如恶意/可疑）。云端基于Transformer构建基因关联分析引擎，利用多头注意力机制解析跨边缘节点的行为序列，识别高阶攻击模式（如APT组织战术关联），并通过位置编码保留时序依赖性[11]。

进化层依托FATE联邦学习平台实现模型持续优化。边缘节点本地训练MobileNetV3后，通过Paillier同态加密梯度参数并上传至云端聚合，避免原始数据泄露。云端采用差分隐私（DP）注入高斯噪声，进一步防御成员推断攻击，最终生成全局模型并下发至边缘端，形成闭环进化[12]。

验证阶段，通过MITRE Caldera模拟多战术攻击链，测试基因编码层对TTPs的召回率，并评估边缘端推理延迟。联邦学习收敛效率对比显示，加密传输仅增加较小幅度的通信开销，但保障了数据隐私性。系统实现了威胁检测的轻量化、关联分析与隐私安全的平衡，适用于物联网等分布式场景[13]。

4 结论与未来方向

4.1 方法论价值

本研究的理论创新在于基于免疫启发的SASE动态防御模型，通过模拟生物免疫系统的自适应机制，使网络安全防御具备动态演化能力，提升了对抗高级持续性威胁（APT）的智能化水平[14]。提出的“威胁基因”概念，将离散的攻击行为特征统一为可计算、可关联的编码形式，为威胁检测提供了标准化表达框架，增强了跨平台分析的兼容性。

在工程指导层面，给出了边缘—云协同的联邦学习实现路径，使分布式节点能在隐私保护前提下共享威胁情报，优化全局检测效率。同时，设计的零信任终端与MEC安全接口规范，为下一代网络架构提供了可落地的安全接入方案，确保动态防御策略在边缘计算环境中的可靠执行[6]。

4.2 挑战与展望

基因编码的标准化问题，当前“威胁基因”的编码方式缺乏统一规范，不同厂商的图嵌入算法和特征提取方法存在差异，导致数据互操作性受限。需联合MITRE、NIST等权威机构制定标准化编码协议，确保行为特征表达的一致性和可扩展性[15]。

跨运营商情报共享的信任机制，在联邦学习框架下，运营商间的威胁情报共享面临信任缺失和合规风险。需设计基于区块链或安全多方计算（SMPC）的分布式信任机制，平衡数据隐私与协同防御需求，同时满足GDPR等数据监管要求。

参考文献：

[1] 魏小强. 基于Gartner SASE思想构建多云环境安全防御框架研究[J]. 信息网络安全，2021(S01)：222-226.
[2] 张俊杰，张春明，陈海强. 基于SASE架构的企业组网设计与应用[J]. 网络安全技术与应用，2024(9)：126-128.
[3] 胡建强. 基于SD-SEC的云安全资源池设计与实现[J]. 信息与电脑，2020，32(11)：213-216.
[4] 李安. 基因武器：人类安全的新威胁[J]. 国家安全通讯，2002(1)：3.
[5] 元栋. 面向威胁情报的知识图谱构建关键技术研究[D]. 佛山：佛山科学技术学院，2024.
[6] 中国通信协会. 安全访问服务边缘（SASE）整体方案技术要求：T/ZGTXXH 026-2022[S]. 北京：中国通信协会，2022.
[7] 贺译册，余思阳，曹京卫，等. 云原生架构与SASE安全融合实践[J]. 邮电设计技术，2024(8)：73-77.
[8] 刘素平. 基于智能策略的网络自管理模型及应用研究[D]. 上海：东华大学，2008.
[9] 叶朝阳，王欣，张士聪，等. SASE云安全研究与实践[J]. 电信科学，2022，38(1)：10.
[10] 杭州安恒信息技术股份有限公司. 基于MITRE ATT&CK创建安全闭环过程的方法：CN201911401807. 5[P]. 2022-10-21.
[11] 付钰，李洪成，吴晓平，等. 基于大数据分析的APT攻击检测研究综述[J]. 通信学报，2015，36(11)：14.
[12] 关泽宇. 基于FATE实现的联邦学习在大数据环境下的隐私应用[D]. 西安：西北大学，2022.
[13] 刘辉. 搜索引擎联邦算法设计与系统实现[D]. 北京：清华大学，2004.
[14] 杨秀璋，彭国军，刘思德，等. 面向APT攻击的溯源和推理研究综述[J]. 软件学报，2025，36(1)：203-252.
[15] 梁晴. 基于MITRE Engage模型的网络安全能力建设思路[J]. 信息安全与通信保密，2024(9)：63-70.

作者简介：
杨丽丽，毕业于合肥工业大学，学士，主要从事网络安全技术方向的研究工作；张小梅，高级工程师，硕士，主要从事网络安全技术研究工作；由志远，毕业于西安电子科技大学，高级工程师，硕士，主要从事网络软件研发工作；刘果，毕业于武汉理工大学，学士，主要从事网络安全技术的研究工作；戚大强，毕业于中国药科大学，学士，主要从事网络安全技术的研究工作。