利用网络微分段技术增强5G电信云安全性的研究

Research on Enhancing Security of 5G Telecom Cloud with Network Micro-Segmentation

曹　刚[1,2]，关先锋[1,2]（1. 中兴通讯股份有限公司，江苏 南京 210012；2. 移动网络和移动多媒体技术国家重点实验室，广东 深圳 518055）

Cao Gang[1,2]，Guan Xianfeng[1,2]（1. ZTE Corporation，Nanjing 210012，China；2. State Key Laboratory of Mobile Network and Mobile Multimedia Technology，Shenzhen 518055，China）

摘　要：

针对5G电信云面临的网络攻击威胁，提出了一种结合管理与编排（MANO）和软件定义网络（SDN）技术的微分段解决方案。通过在业务交换机上创建隔离区域，实现了对东西向流量的精细控制，显著增强了网络安全性。微分段技术不仅提升了5G电信云的防护能力，也给网络的扩展和维护带来了更大的灵活性，为电信行业提供了一种有效的安全防护手段，确保了5G网络的稳定运行和数据安全。

关键词：

微分段；5G电信云；MANO；SDN

doi：10.12045/j.issn.1007-3043.2025.05.011

文章编号：1007-3043（2025）05-0062-07

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：

It proposes a micro-segmentation solution that combines management and orchestration （MANO） and software-defined network （SDN） technology to address the cyber attack threats faced by 5G telecom clouds. By creating isolation areas on service switches，fine control of east-west traffic is achieved，significantly enhancing network security. Micro-segmentation technology not only improves the protection capabilities of 5G telecom cloud，but also brings greater flexibility to network scalability and maintenance，which provides an effective security protection method for telecom industry and ensures the stability operational and data security of 5G network.

Keywords：

Micro-segmentation；5G telecom cloud；MANO；SDN

引用格式：曹刚，关先锋. 利用网络微分段技术增强5G电信云安全性的研究[J]. 邮电设计技术，2025（5）：62-68.

0 引言

5G技术的快速发展和广泛应用，正在推动社会经济的数字化转型[1-2]。5G推动了产业升级和数字经济的增长，如助力智能工厂的建设。在行业领域，5G提升了智能化水平，如智能交通、智慧医疗；在日常生活中，5G带来了更丰富的体验，如高清视频、云游戏等。然而，5G技术的广泛应用也使电信行业成为网络攻击的主要目标。根据报告，有38%的云攻击针对电信公司[3]，攻击者可能会入侵电信云系统，进而在云内进行横向移动，获取敏感信息或扩大攻击范围，给经济和日常生活带来灾难。

为了应对这些安全挑战，业界提出了基于微分段（Micro-segmentation）的解决方案。微分段将网络划分为更小的、相互隔离的段来限制数据中心内部服务器、应用程序和工作负载之间的访问，从而增强网络的安全性[4]。尽管许多IT资源池已经实施了微分段以提高系统安全性，但该技术在电信云中的应用仍处于起步阶段。

本文提出一种结合MANO和SDN技术的网络微

收稿日期：2025-04-16

分段解决方案，强化电信云安全防护，精确控制网络流量，自动化部署安全策略，构建安全可靠的5G网络环境。

1 5G电信云安全威胁分析

电信云作为5G网络的关键组成部分，通过网络功能虚拟化（NFV）和SDN技术实现了资源的灵活调度和网络的自动化管理，提高了运营效率。此外，电信云支持云原生应用，具备微服务架构、容器化、动态编排等特点，使5G业务能够快速迭代和部署[6]。

电信云在安全方面面临着多重挑战。随着网络功能的开放，传统的网元边界防护策略不再适用；底层实现依赖开源软件，可能带来安全漏洞；采用通用协议开放网络功能及接口，电信云容易受到互联网攻击；离开封闭的物理环境，安全需求更加个性化，责任界定也更加困难[7]。

为了应对这些挑战，已采取以下措施：按网元类型划分资源池安全区域；在网络出口部署防火墙、IPS/IDS等设备，控制网络边界和管理流量；部署4A系统（认证、授权、审计、账号管理），提供远程安全接入和审计；定期或按需进行安全扫描；实施东西向流量隔离，按需划分VLAN和VRF进行网络隔离[8]。

然而，电信云面临的主要挑战是如何防止攻击者在突破安全防线后在数据中心内进行横向移动，从而导致数据泄露、服务中断和重大财务损失[9]。当前采用的东西向流量隔离措施可以在一定程度上阻止横向移动，但无法隔离同一子网内应用的互相访问。此外，当不同子网共用一个网关设备时，网关上的路由信息可能导致不同子网内的应用之间无法实现有效隔离。

访问控制列表（ACL）规则虽然可以实现应用隔离，但电信云中应用众多，需要配置大量ACL规则，这导致配置维护复杂且资源受限。在电信云的各个节点部署防火墙虽能实现内部隔离，但硬件投资和维护成本高。

因此，需采用更细粒度的控制方法，如先进的微分段技术。微分段技术可在工作负载级别创建隔离区域，实现精细流量控制，限制攻击者横向移动。

2 网络微分段的概念与原理

2.1 微分段的概念

微分段是一种网络安全技术，它通过将网络划分为更细粒度的子网络或安全区域，并基于策略控制流量，从而实现更高的安全性和网络性能。微分段的实现方式主要有3种：基于网络、基于Hypervisor和基于主机代理[10]。

a）基于网络。基于网络的实现方式依赖网络基础设施，利用物理和虚拟设备（如负载均衡器、交换机、SDN和Overlay网络）来实施策略[11]。Overlay网络通过封装协议，如虚拟扩展局域网（Virtual eXtensible Local Area Network，VxLAN）[12]，在物理基础设施上创建虚拟网络，实现东西向流量的检查。这种方式适合需要广泛覆盖和防护的场景。

b）基于Hypervisor。在虚拟化环境中，通过虚拟防火墙来监控和管理流量。这种方法控制粒度细，但不同Hypervisor平台之间可能不兼容[13]。

c）基于主机代理。在工作负载上部署软件代理，对单个主机和容器进行隔离。代理软件可以监测流量并根据安全规则进行处理。这种方法控制粒度细，但需要在每台主机上安装代理，可能会消耗额外资源[14]。

在IETF标准中，基于网络的微分段方案已经在VxLAN扩展的内容有所定义[15]，该方案相较于其他方案更为成熟。因此，本文主要介绍基于VxLAN的网络微分段方案。

2.2 基于VxLAN的网络微分段概念

基于VxLAN的网络微分段的基本概念如下。

a）EPG（End Point Group）。EPG是一种逻辑分组机制，将网络终结点（如虚拟机、容器或应用）按特定原则进行分类。分配到EPG的终结点为组内成员，未分配的则为未知成员。一个EPG可包含多个终结点。

b）GBP（Group Based Policy）。GBP是一种基于EPG的流量控制策略，它定义了EPG内部及EPG之间的流量规则，包括源/目的EPG、协议、端口与动作指令（如允许、禁止或默认策略）。

IETF定义了VxLAN-GBP标准，VxLAN-GBP通过扩展VxLAN报文格式来传递EPG信息，从而实现基于组策略的微分段。VxLAN与VxLAN-GBP报文的关系如图1所示。

VxLAN的报文格式主要包括外层以太网头部、外层IP头部、外层UDP头部、VxLAN头部和原始二层数据帧。VxLAN头部包含的字段如下。

a）VxLAN Flags。8比特，R位为0，I位为1，整体取值为00001000。

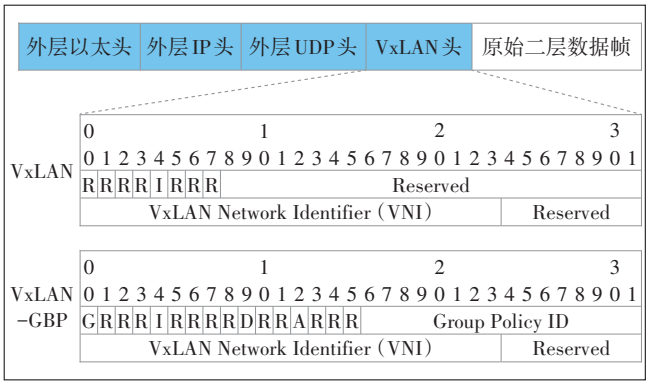

图1　VxLAN与VxLAN-GBP报文的关系

b）VxLAN Network Identifier（VNI）。24比特，用于区分不同的VxLAN网络段。

c）Reserved。24位和8比特，必须设置为0，保留以备将来使用。

VxLAN-GBP的报文格式在VxLAN头部报文格式的基础上增加了G标志位和Group Policy ID字段，用于传递源端的EPG组号，从而实现基于组策略的微分段。

a）G标志位。当此位置为1时，表示VxLAN报文头通过Group Policy ID字段携带源端终结点所属的EPG组号。

b）D与A的标志位。取值为0或1，指示报文的动态性或特定的处理要求，具体的含义可能依赖实现和上下文。

c）Group Policy ID字段。16比特，当G标志位为1时，表示该字段中的值为源终结点所属的EPG组号。

VTEP（VxLAN Tunnel Endpoint）是VxLAN网络中的隧道端点，负责封装和解封装VxLAN报文。VTEP通过G标志位和Group Policy ID字段向目的VTEP传递微分段信息。

2.3 网络微分段的工作机制

在VxLAN网络中，利用目标VTEP上的GBP策略来实现流量的精细化控制。以图2为例，说明通过启用微分段功能，并配置EPG和GBP来管理网络流量的步骤。

2.3.1 网络配置

a）VTEP1连接服务器Server A（IP：1.1.1.1）和Server B（IP：1.1.1.2）。

b）VTEP2连接服务器Server C（IP：1.1.1.3）。

c）Server A和Server B之间的通信在VTEP1上进行本地处理。

d）Server A和Server C之间的通信通过VxLAN隧道跨设备处理。

2.3.2 通信规则

a）Server A和Server B均能与Server C通信，使用UDP协议，源端口不限，目的端口范围为4 000~5 000。

b）Server A和Server B之间的TCP协议通信，源端口不限，目的端口为443，被禁止。

2.3.3 配置步骤

a）定义EPG。将Server A和Server B归入同一微分段；将Server C归入另一微分段。

b）定义GBP。根据通信规则配置相应的策略。

c）VTEP1与VTEP2上都需要配置EPG与GBP，EPG与GBP的配置具体如图2的样例所示。

2.3.4 工作流程

2.3.4.1 本地转发工作机制

a）VTEP1接收到Server A发送给Server B的TCP报文，源端口为1 000，目的端口为80。

b）VTEP1从报文中提取源IP地址（1.1.1.1）和目

EPG

IP address	Segment ID
1.1.1.1/32	101
1.1.1.2/32	101
1.1.1.3/32	102

GBP

Source EPG	Destination EPG	Protocol	Source Port	Destination Port	Policy
101	101	TCP	any	443	deny
101	102	UDP	any	4000~5000	permit

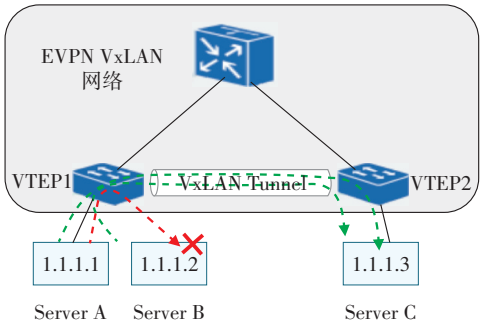

图2　VxLAN网络微分段示意

的IP地址（1.1.1.2），确定源端和目的端所属的EPG分段号均为101。

c）VTEP1根据源端和目的端的EPG分段号，查找GBP策略，并根据策略丢弃协议为TCP、目的端口为443的报文。

2.3.4.2 跨设备转发工作机制

a）VTEP1接收到Server A发送给Server C的UDP报文，其源端为1001，目的端口为23。

b）VTEP1从报文中提取源IP地址（1.1.1.1）和目的IP地址（1.1.1.3），确定源端口所属的EPG分段号为101。

c）VTEP1查找路由表信息并匹配目的地址的下一跳，为VTEP2，此时报文需通过VxLAN隧道转发。

d）VTEP1在VxLAN报文头中设置G标志位，将源端的EPG分段号（101）封装至Group Policy ID字段，发送给VTEP2。

e）VTEP2接收到VTEP1发送的VxLAN报文后进行解封装操作。由于报文的G标志位被设置，VTEP2从Group Policy ID字段中提取源端的EPG分段号（101）。

f）VTEP2根据目的IP地址（1.1.1.3）确定目的端所属的EPG分段号为102。

g）VTEP2查找源端与目的端之间的GBP策略，并根据策略允许协议为UDP、目的端口为4000的报文进行转发。

2.4 网络微分段与ACL比较

在网络配置和资源管理领域，与ACL相比，微分段技术展现出如下优势。

a）配置简化。GBP和ACL都控制IP五元组，但GBP通过EPG提升了管理效率。EPG可将有相似策略的IP进行归类，只需配置EPG间的交互，简化了配置。ACL则需逐个配置IP地址，并未利用IP间策略的关联性。以图3为例，8个IP地址，ACL需配置56条规则，GBP通过4个EPG，仅需16条规则，大幅减少了配置量。

b）策略灵活性。对于控制策略一致的IP地址，只需将它们分配到相应的EPG中，无需调整GBP配置。而ACL在添加新IP地址时，需要增加2×（N−1）条配置，这种方法不仅繁琐，而且在复杂业务场景下的适应性不足。

c）降低资源占用。在网络设备中，ACL需要匹配完整的IP地址，IPv4为32位，IPv6为128位，这会占用较多的硬件资源。相比之下，微分段技术通过使用16位或12位的微分段ID替代IP地址进行匹配，显著减少了硬件资源的占用，从而更高效地利用设备资源。

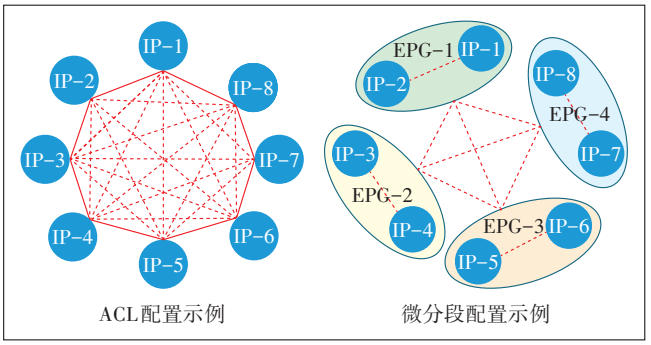

图3　微分段与ACL比较示意

综上所述，微分段技术在简化配置、提升灵活性和降低资源占用方面表现出色，可显著提高网络管理效率和适应性。

3 网络微分段在5G电信云的应用

3.1 电信云的安全隔离架构

按照层次和架构设计，电信云自下而上分为接入层、核心层、出口层，按Leaf—Spine—DCGW组网架构建设[16]，具体如图4所示。

a）接入层。部署Leaf交换机，连接各类服务器和存储设备，实现设备间的互通，并通过Spine设备实现不同Leaf间的互联。

b）核心层。部署业务Spine与存管Spine设备，这些设备汇聚接入层Leaf交换机，确保接入层设备间的高速交换；同时与DCGW互联，实现与外部网络的互联互通。

c）出口层。部署DCGW，作为电信云与外部网络的连接点，确保快速访问外部网络并管理内外网路由信息。DCGW连接核心层Spine设备，保证网络互通。旁侧部署外层防火墙和WAF设备，保护进出电信云的业务流量；同时部署网管防火墙，保护管理流量。

按照逻辑功能的不同，电信云可分为存储网络、存管网络和业务网络。

a）存储网络。连接存储节点，接收VNF/CNF请求，按需提供存储资源。

b）存管网络。连接管理节点，部署CISM/VIM等组件，管理资源池。

c）业务网络。业务网络包括业务Leaf和计算节点服务器。业务Leaf承载VNF/CNF业务流，Leaf设备

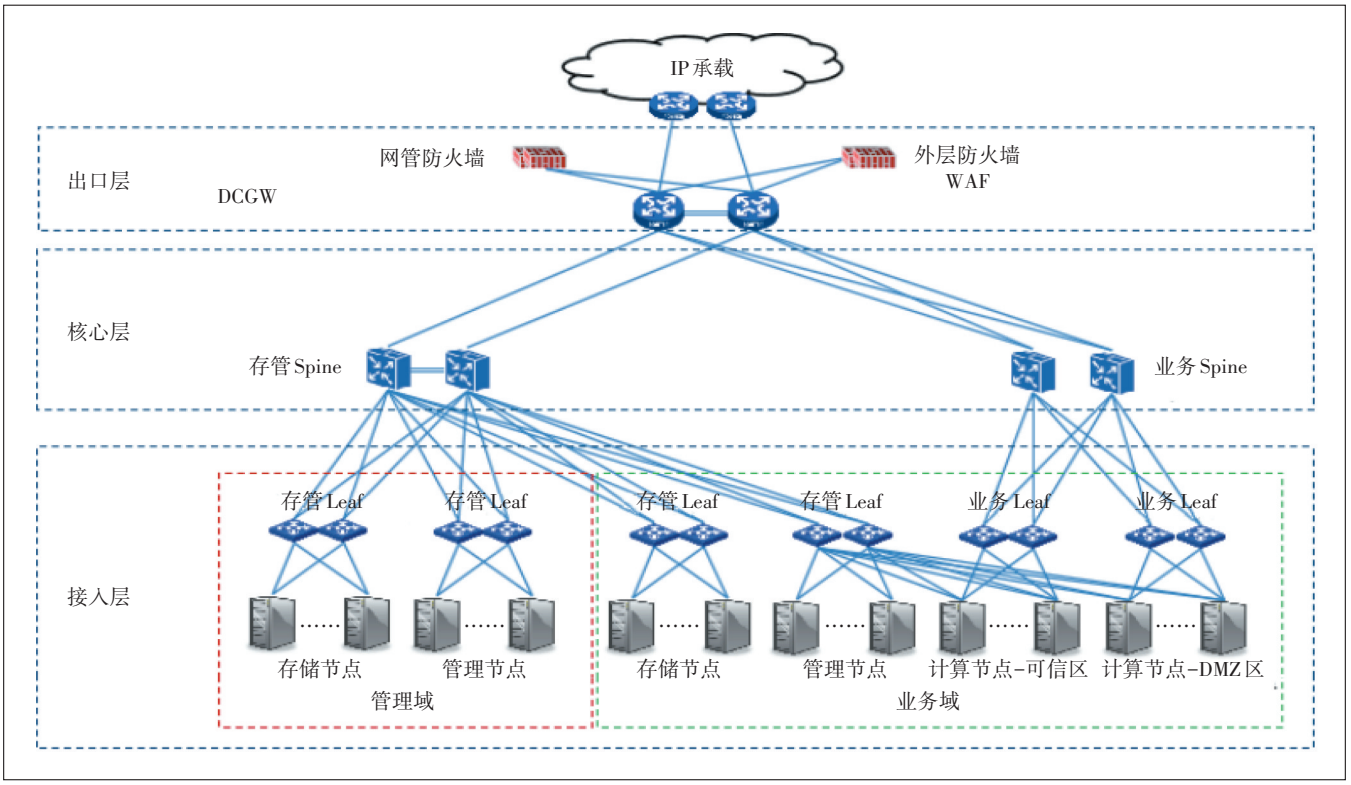

图4　电信云组网架构

与DCGW间运行BGP-EVPN/VxLAN协议，VNF/CNF间及与外网通过VxLAN互通。

为满足安全隔离需求，接入层又分为管理域和业务域。

a）管理域。管理业务域的软硬件设备，包括硬件管理、云管平台、SDN控制器、CNFM/VNFM、MANO和EMS等。

b）业务域。部署CNF/VNF实现业务功能，并根据5GC网元特点，划分为可信区与DMZ（Demilitarized Zone）区。其中，DMZ区部署用户面功能（UPF）、网络暴露功能（NEF）、安全边缘保护代理（SEPP）等网元，与外部网元通信时流量经外层防火墙保护，与可信区内网元通信时则无需防火墙。可信区内部署认证服务器（AUSF）、统一数据管理（UDM）、统一数据仓库（UDR）、接入和移动性功能（AMF）、会话管理功能（SMF）、策略控制功能（PCF）等关键网元，与外部网元通信时流量通过DMZ中的网元进行处理，确保网络安全性。

3.2 网络微分段方案

经过对电信云网络的深入分析发现，DMZ区的网元南北向流量已由防火墙进行有效保护。但是，可信区内的核心网元与DMZ区网元之间，以及这些网元内部的流量尚未采取适当的安全措施。为了提升网络安全，建议引入网络微分段技术，隔离并保护这些内部流量，确保网络各部分的安全，降低潜在风险，具体的微分段部署方案如图5所示。

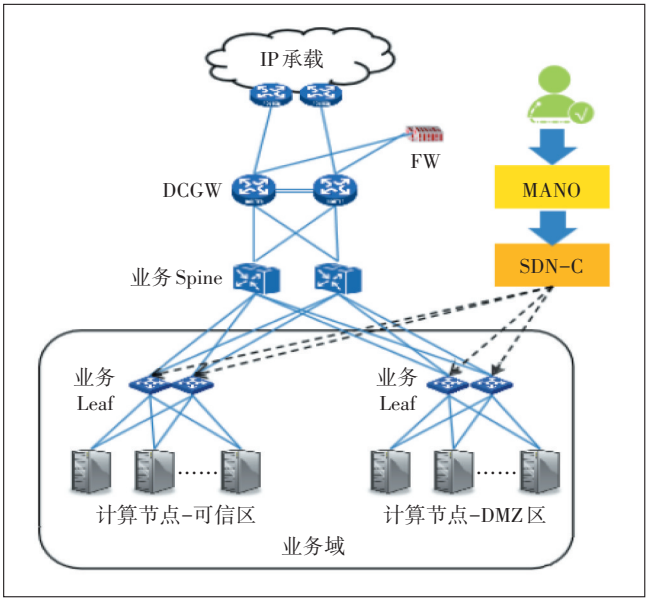

图5　微分段在电信云中的部署示意

微分段控制在业务Leaf上开启，由业务Leaf根据EPG/GBP策略，针对5GC网元的业务流量进行控制。由MANO与SDNC配合完成EPG/GBP配置自动下发的流程，自动部署的流程如下。

a）在MANO上配置EPG数据，包括5GC网元与EPG参数等内容；MANO查找5GC网元部署的节点服务器，形成节点服务器与EPG参数的数据，然后下发给SDNC。

b）SDNC查找节点服务器与业务Leaf的对应关系表格，将EPG参数下发给相应业务Leaf。

c）在MANO上配置GBP数据，然后下发给SDNC。

d）SDNC查找GBP中目的EPG的内容，然后查找EPG与业务Leaf的关系表，找到对应的业务Leaf；SDNC将GBP发送给相应业务Leaf。

当EPG/GBP在业务Leaf上配置完成后，就可以启用微分段功能。5GC网元发送IP报文到业务Leaf，业务Leaf根据第2.3节描述机制进行报文控制。

3.3 EPG/GBP配置策略

在部署网络微分段之前，精确配置EPG和GBP是确保网络安全的关键。本研究遵循“永不信任，始终验证”的零信任原则[17]，任何未在EPG/GBP通信矩阵中明确定义的流量都应自动拒绝。在配置过程中，实施精细的流量控制对于减少潜在安全风险至关重要。

在电信云环境中，可以通过网元类型来配置EPG。当新增的网元属于已有网元类型时，只需修改EPG而无需修改GBP，这降低了配置的复杂性并便于后续的网络维护。

微分段控制提供了比VRF/VLAN更细粒度的控制。因此，EPG的划分应基于每个网元的VRF进行，包括操作维护面、控制面、用户面和计费。这种划分方法有助于GBP根据明确的流量配置控制策略。

在电信云环境中，部署防火墙主要保护南北向流量，而微分段技术则专注于东西向流量的安全。电信云的通信需求可以主要分为2个类别。

a）电信云内部的东西向通信。针对电信云内部网元间和同一个网元内部的东西向通信，需要建立一个白名单，明确允许通信的源/目的EPG、协议和源/目的端口。

b）出电信云的南北向通信。针对不同电信云间的网元以及电信云与外部网络的南北向通信，需要结合防火墙和微分段技术来实现防护。在GBP上要明确电信云内部的EPG组，对于本电信云外部网元，采用“unknown”来配置。由防火墙负责做详细的控制，确保只有经过验证的流量能够通过。

通过这种综合的策略，可以确保网络中流动的流量都经过了严格的验证，从而显著提升整个网络环境的安全性。

3.4 网络微分段配置示例

在图5的基础上，通过配置示例来说明根据上述原则实施微分段EPG/GBP的配置。

3.4.1 组网假设

a）电信云可信区包含SMF01/SMF02网元，DMZ区包含UPF01/UPF02网元。

b）每个网元内部存在VM/POD间的通信需求。

c）SMF通过N4接口与UPF进行通信。

d）UPF通过N3接口与无线RAN进行通信。

e）UPF通过N4接口与SMF行通信。

f）UPF上用户通过N6接口与Internet通信。

3.4.2 全局GBP缺省配置

确保只有明确定义的数据流能够进行通信，具体配置如下。

a）已知到未知。已配置EPG与未配置在EPG中的IP之间的通信被明确禁止。

b）未知到未知。未配置在任何EPG中的IP地址之间不允许相互通信。

c）同一EPG内。同一EPG组内不允许通信。

3.4.3 EPG配置

首先，根据每类网元的网络平面/VRF配置EPG（端点组）。然后，通过通信矩阵管理网元之间的通信需求（见图6）。通信矩阵中的行和列表示EPG ID，相

EPG ID			101	102	201	202	203	301
	业务Leaf	unknown	SMF-Inner	SMF-N4	UPF-Inner	UPF-N3	UPF-N4	UPF-N6
	unknown					1		1
101	SMF-Inner		1					
102	SMF-N4						1	
201	UPF-Inner			1	1			
202	UPF-N3	1						
203	UPF-N4			1				
301	UPF-N6	1						

1 Permit　Deny

图6　EPG通信矩阵

交部分中，“1”表示允许通信，其他情况为拒绝通信。通过此矩阵，可以清晰地列出电信云中所有可能的通信关系，便于管理和优化网络策略。

3.4.4 GBP配置

在进行GBP配置时，本研究遵循精细流量控制原则，对通信矩阵进行了详尽的细化，包括协议和端口等具体细节。

优化后通信矩阵确保了允许通信的关系能够被精确定义，并明确列出了所使用的协议和端口。在此过程中，特别关注了主要通信协议以及网络保障协议，如ICMP，以增强网络的稳定性和可靠性。

用户与Internet之间的流量有防火墙进行保护，因此在配置微分段时，允许使用“any”来表示协议和端口，以提高通信的灵活性。对于其他类型的流量，要求明确指定协议和端口的范围，以确保网络的安全性和效率。

4 结束语

本研究针对电信云面临的安全威胁，提出集成MANO和SDN技术的网络微分段方案。该方案通过在业务交换机上创建隔离区域，实现对东西向流量的精细控制，显著提升了网络安全性与防护能力，增强了网络的扩展性和维护性，为电信行业提供了有效的安全防护手段，可保障5G网络得稳定运行和数据安全。

然而，网络安全是一个多技术协同的复杂系统。微分段技术虽在业务交换机层面细化了网络隔离，但并不能解决所有的安全问题。由于交换机资源的限制，微分段不能替代防火墙的功能，尤其是在处理大量GBP规则时。因此，在实施微分段策略时需考虑GBP规则数量的限制，并与其他安全措施如防火墙、入侵检测系统等结合，构建全面多层次的网络安全防护体系。

参考文献：

[1] 张阳. 记者手记：商用五周年，数说5G高质量发展[EB/OL]. [2024-06-06]. https://tech.huanqiu.com/article/4I6K34AfasW.

[2] 央视新闻客户端. 5G目前布局如何？多家运营商公布新进展[EB/OL]. [2024-05-18]. https://news.cnr.cn/native/gd/20240518/t20240518_526709225.shtml.

[3] Sysdig. Twenty 23: global cloud threat report[EB/OL]. [2024-05-18]. https://sysdig.com/content/c/pf-2023-global-cloud-threat-report?x=u_wfri.

[4] TechTarget中国. 使用微分段减少横向攻击[EB/OL]. [2024-03-14]. https://searchsecurity.techtarget.com.cn/11-26505/.

[5] ETSI. Network functions virtualisation (NFV) release 3; virtualised network function; specification of the classification of cloud native VNF implementationss: ETSI GS NFV-EVE 011[S/OL]. [2024-08-26]. https://standards.globalspec.com/std/13103182/gs-nfv-eve-011.

[6] 王卫斌. 5G商用将推动NFV进入新阶段[J]. 邮电设计技术，2018(11)：35-40.

[7] 王瀚洲，周洺宇，刘建伟，等. 5G网络安全威胁发现及解决方法综述[J]. 信息安全研究，2024，10(4)：340-346.

[8] 张世华，文湘江，张奎，等. 电信云安全方案研究[J]. 邮电设计技术，2023(4)：24-28.

[9] 央视网. 西北工业大学遭美国NSA网络攻击：美方逐步渗透，长期窃密[EB/OL]. [2024-09-21]. https://news.cctv.com/2022/09/27/ARTI1YjUCAzciKAsNQsy1Rxd220927.shtml.

[10] CyberGlossary. What is Microsegmentation? [EB/OL]. [2024-09-20]. https://www.fortinet.com/resources/cyberglossary/microsegmentation?utm_source=blog&utm_campaign=microsegmentation.

[11] CISCO. Cisco nexus 9000 series NX-OS VxLAN configuration guide, release 10.4(x)[EB/OL]. [2024-08-26]. https://www.cisco.com/c/en/us/td/docs/dcn/nx-os/nexus9000/104x/configuration/VxLAN/cisco-nexus-9000-series-nx-os-VxLAN-configuration-guide-release-104x/m_configuring_VxLAN_93x.html.

[12] MAHALINGAM M, DUTT D, DUDA K, et al. Virtual eXtensible local area network (VxLAN): a framework for overlaying virtualized layer 2 networks over layer 3 networks: RFC 7348[S/OL]. [2024-11-18]. https://datatracker.ietf.org/doc/rfc7348/.

[13] 为VLAN和覆盖网络微分段准备集群[EB/OL]. [2024-09-21]. https://docs.vmware.com/cn/VMware-NSX-T-Data-Center/3.1/installation/GUID-A0FED4E8-ADAE-466F-9840-BFCA8A43FB68.html.

[14] Akamai. 重磅丨Akamai被Forrester评为微分段领域领导者![EB/OL]. [2024-09-23]. https://zhuanlan.zhihu.com/p/482955868.

[15] SMITH M, KREEGER L. VxLAN group policy option: draft-smith-VxLAN-group-policy-05 [R/OL]. [2024-08-26]. https://datatracker.ietf.org/doc/html/draft-smith-VxLAN-group-policy.

[16] 张世华，胡祎，张奎，等. 面向5G的通信云部署方案[J]. 邮电设计技术，2020(9)：70-74.

[17] Department of Defense. Department of Defense (DOD) Zero Trust Reference Architecture[R]. 2021.

作者简介：

曹刚，毕业于东南大学，中兴通讯股份有限公司CCN产品规划总工，工程师，硕士，主要研究方向为电信云及核心网组网与关键技术；关先锋，毕业于华中科技大学，安全系统架构师，主要从事移动通信核心网的产品架构设计和产品安全治理工作。