云网融合下的安全能力池关键技术与应用

Key Technologies and Application of Security Capability Pool for Cloud-Network Convergence

余启明/YU Qiming，吴爽/WU Shuang，黄帅/HUANG Shuai，刘紫千/LIU Ziqian

（天翼安全科技有限公司，中国 北京 100020）
(China Telecom Cybersecurity Technology Co., Ltd., Beijing 100020, China)

DOI：10.12142/ZTETJ.202301005
网络出版地址：https://kns.cnki.net/kcms/detail//34.1228.TN.20230224.1459.006.html
网络出版日期：2023-02-24
收稿日期：2022-12-15

摘要：设计并实现了云网安一体化的安全能力池系统。该系统将重要的网络安全能力虚拟化、原子化后沉入边缘云节点进行部署，支持多种流量型与非流量型的安全服务场景。系统基于IPv6的段路由（SRv6）与Flowspec技术实现了安全服务链编排与流量调度，配置简单，灵活高效，并通过标准化接口实现了跨厂商安全能力统一纳管。系统通过工程方法解决了生产运行过程中存在的运行速度慢、业务中断等问题，实现了安全能力的集中管理与智能调度。目前，安全能力池已进入商用阶段，服务客户上千家，累计防御次数达到百万级。

关键词：云网融合；安全能力池；近源防护；弹性扩展；按需组合

Abstract: A security capability resource pool system that integrates cloud, network, and security is proposed. The system deploys major security capabilities at the edge cloud nodes and supports a variety of traffic-mode and non-traffic-mode service scenarios. Based on Segment Routing IPv6 (SRv6) and Flowspec technology, the resource pool achieves service chain orchestration and flow scheduling with simple configuration and high efficiency. Meanwhile, the system manages cross-vendor security capabilities through standardized interfaces. In addition, the whole system solves the problems such as slow running speed and service interruption in operation and achieves unified management and intelligent scheduling of security capabilities. At present, with the commercial use of the security capability resource pool, thousands of customers have been successfully protected from millions of cyber-attacks.

Keywords: cloud-network convergence; security capability resource pool; near-source protection; elastic expansion; integration by requirements

互联网信息技术发展日新月异，大数据、云计算等新兴技术加快了进入政务、金融、医疗、教育等行业的步伐[1-2]。与此同时，网络安全问题也日渐凸显，如何高效满足各行业企业对网络安全防护的多种需求成为产业界亟待解决的问题。传统企业具有相对固定的网络安全边界，因此安全厂商常采用串接或者并接硬件设备的方式为用户提供安全解决方案。此种方式的弊端日益凸显，例如：部署繁琐，功能单一，可维护性差等[3-4]。随着网络安全威胁的持续变化和企业自身数字化转型的深入，企业对安全防护手段的多样化需求与日俱增，对各种手段的综合防护能力和效果的要求也不断提高。传统的依靠堆叠安全硬件的方法已经无法满足用户对安全能力按需快速组合和防护能力弹性扩容的需求。因此，通过可运营升级的云化软件即服务（SaaS）安全防护方案来解决各类网络安全问题已经成为了行业新的重要趋势[5-6]。

为满足企业用户对安全防护能力多层次可定制的需求，在运营商云网融合的技术驱动下，云资源池应运而生[7-10]。本文提出了一种云网安一体化的安全能力池技术方案，提高了网络安全防护的灵活定制和可编排能力，满足网络安全能力的可快速扩展的要求。安全能力池技术方案主要基于边缘云技术、自动化云端部署安全防护能力，通过软件化、服务化的安全能力为用户提供实时安全保障，并可直接借助安全管理平台对所需安全能力进行统一管理与配置，极大地提升了安全能力的使用效率，降低了使用成本。

1 系统整体设计方案

根据中国电信网络安全统一规划，安全能力池计划覆盖中国电信所有主要的城域网，为客户提供复合安全防护能力。这些安全能力可分为流量型和非流量型两类：流量型指基于业务流量行为进行实时检测阻断的安全能力，这类能力

往往需要在业务流量流经路径中进行干预才能起到效果，例如：防火墙、入侵检测和Web应用防护等；非流量型指不依赖业务流量路径干预也能发挥作用的安全能力，例如：漏洞扫描、日志审计等。安全能力池系统需要解决复杂流量调度、多业务场景编排、跨厂商应用维护等技术问题。此外，安全能力池需要作为多生态能力的承载平台，与上层应用低耦合，并具备高扩展能力。安全能力池分为上、中、下3层架构，如图1所示，分别为安全能力管理平台层、安全业务中台层和资源池层。

上层安全能力管理平台（后文简称为安管平台）在多租户场景中为角色和权限各异的用户提供统一的管理访问入口；中间层为安全业务中台，主要实现对资源池的纳管、原子能力的适配和服务之间的安全认证。从图1中可以看到，业务中台将安管平台与底层资源池分割开来，并将复杂的安全业务场景逐步拆分，这样降低了系统耦合度，同时提高了系统的高扩展性。最下层为资源池层，具备多种安全原子能力、流量调度与服务链编排能力和大规模数据存储能力，解决了核心的安全防护和大规模流量安全调度问题。资源池层的流量调度与服务编排技术解决大流量传输效率和自动化编排问题。业务中台层的原子能力统一纳管解决多厂商原子能力适配问题，以及整体的系统性能优化升级。

安全能力池的系统架构具有集中、近源、共享等特点：

1）集中。安全能力池通过安管平台对所有线上资源池集中统一纳管，提供SaaS化服务，提高运维效率。

2）近源。资源池结合边缘云技术与电信运营商的大网优势实现了近源流量安全防护，将需要防护的业务流量引导到距离防护目标最近的资源池内，经过多种安全防护能力检测、网络安全威胁清除后将流量回注给被防护对象。此种方式为用户提供更加实时、高效的防护。

3）共享。SaaS化的原子能力的共享模式实现了同一服务点下多租户共享虚拟机（VM）集群。每个VM集群部署一类服务，不同租户间通过逻辑隔离，共享模式具有成本低、效率高和资源利用最大化等优势。

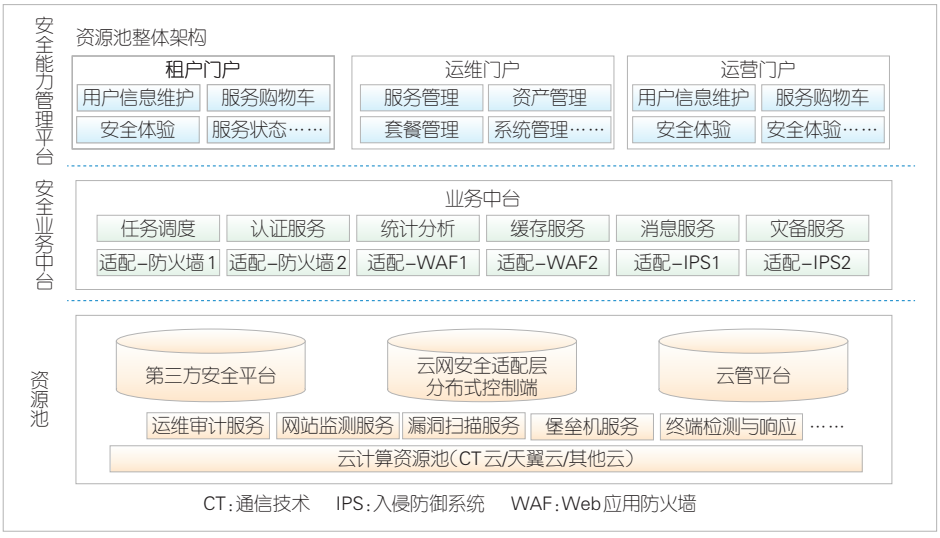
1.1 管理平台层设计

安管平台层重点解决资源池分布广、管理难度大、运维难度高等问题。作为整个系统架构的最顶层，安管平台为租户门户、运维门户、运营门户提供三位一体的管理功能，其整体结构如图2所示。

安全原子能力服务管理模块提供原子能力的统一配置、管理及安全策略下发服务，通过原子能力编排服务，实现资源池内安全原子能力的整合与联动。订单管理服务组、用户/租户管理服务组、主机管理服务组等为租户提供了良好的用户体验。告警监控服务组可以实时查看资源池健康状态、内存使用率，提升了系统整体透明度，增强了网络故障定位能力。安管平台作为资源池的集中管理入口，通过三大门户实现资源集中配置，从而降低产品集成风险，提升工作效率。管理层平台三大门户的具体功能如下：

1）租户门户系统主要为租户提供安全服务订阅功能；

2）运维门户系统采用自动一体化形式，可自动部署、启动安全原子能力服务并完成资源池内服务自动化编排；



▲图1 安全能力池整体架构图

▲图2 安全能力管理平台整体结构图

3）运营门户系统负责自定义安全服务策略、资源池运营等服务。

1.2 业务中台层设计

业务中台层重点解决两大问题：适配性问题和安全性问题。适配性问题聚焦于如何纳管各种厂商的多种安全原子能力，如何适配不同的云上资源池；安全型问题重点考虑平台直接调用底层原子能力对资源池的较高侵入性，以及未经监管的流量所带来的安全隐患。能力池系统在安全能力管理平台与底层资源池之间引入了安全业务中台层，功能如图3所示。

安全业务中台主要具备4个方面能力：1）通过制定安全组件接口规范，实现对多云底座的纳管和对多个厂家异构资源的统一纳管，并对第三方安全平台中间件、云管中间件进行统一管理；2）作为南北向通信的桥梁，将南北向解耦；3）作为业务信息、运维、运营信息的管控入口，承担着应用程序编程接口（API）统一管理的职责，通过一套标准化的接口规范，支持多种业务的水平扩展，提高了系统的可用性；4）承担整个系统架构的安全访问认证职责，实现整个系统的自主可控，提升了云网安全运营的自动化、智能化。

1.3 资源池层设计

安全能力池底层是基于轻量化边缘云技术的资源池底座实现的，其结构如图4所示。资源池封装了多厂商优势产品的安全能力，极大地提升了安全防护能力的多样性，而且安全场景覆盖性高，已覆盖10多类共计30项安全原子能力。资源池中的物理设备资源主要为安全能力提供底层的路由交换、流量调用以及数据存储。其中，安全流量调度网关具有虚拟化管理和网络流量编排功能，承担整体调度职责，分别和新型城域网控制器、安全能力池控制器对接，完成用户流量的路径编排。目前，资源池的部署方式有两种：一是采用安全能力集中部署的方法，同时在云平台核心网络设备上部署近源安全能力，主辅双线并行共同满足用户需求；二是在专线用户网络中部署近源安全能力，满足专线用户需求，充分利用运营商大网优势，将集中能力复用给专线客户，减少专线用户安全能力的部署工作。

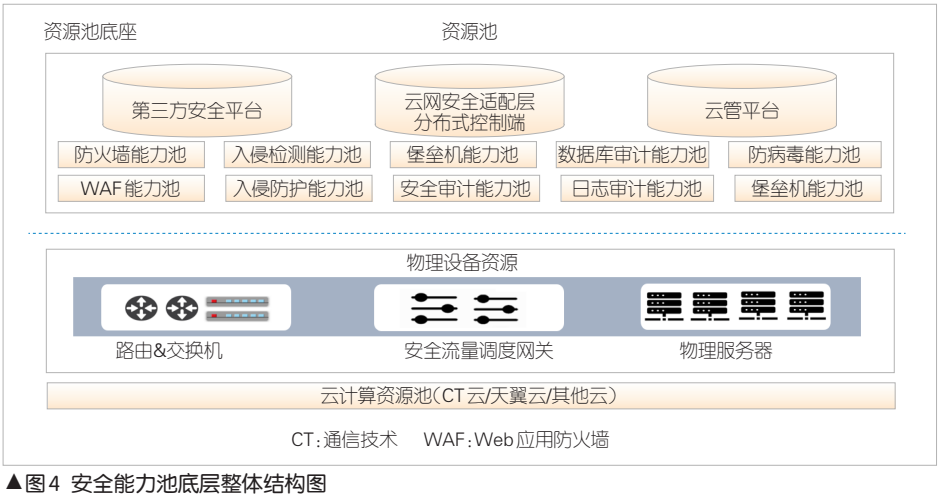
安全能力池采用统一的SaaS化架构来提供安全服务，具有按需组合、弹性扩张的特点。用户在使用安全服务时，在租户平台输入所需的安全能力和需防护的目标资产。根据运营人员的配置情况，资源池会通过Flowspec控制器将流量从IP承载网核心路由器（CR）牵引至离用户最近的资源池，在资源池内为用户流量进行安全防护，之后会将处理后的流量通过路由原址送回给用户。用户可以实时自主选择所需的安全能力。这种方式更加灵活、方便。

2 关键问题与技术

2.1 流量调度与服务编排

传统资源池使用基于策略的路由（PBR）进行流量调度。针对运营商级别的大网流量牵引调度，该方式会占用路由条目项，配置繁琐，速度慢，规模部署将难以维护。为使网络与云池有机融合和统一调度，安全能力池采用了一种新颖的流量调度与服务链编排技术。在系统需要流量调度的情况下，资源池通过自主研发的Flowspec控制器来修改路由的下一跳地址，从而将流量牵引至距用户最近的池子，进而提供安全防护。流量进入云池后，针对云资源池内的原子能力编排，安全能力池使用基于IPv6的段路由（SRv6）的端到

▲图3 安全业务中台功能图



▲图4 安全能力池底层整体结构图

端引流方案。资源池将原子能力所在虚拟机的IPv6地址定义成实例化的段标识（SID），通过操作不同的SID，实现路径规划。SRv6将128 bit的IPv6地址作为SID。如果段路由扩展报文头（SRH）封装较多的SID，则会造成SRv6报文头开销过大、传输效率低。针对该问题，资源池利用SID包头压缩技术，在保持对128 bit SID兼容的同时，删除SID的冗余信息并将其压缩为32 bit。压缩后的方案中引入了SI字段来控制32 bit SID的目的地址更新。32 bit的压缩方案在支持原有硬件设备的同时具有更高的传输效率和转发性能。基于SRv6的服务链动态编排技术效率是传统编排方式的3倍。在传递相同大小的数据块时，优化后的编排相比于原SRv6，流量传输效率能提高约30%。

安全能力池通过实验验证了SRv6端到端引流方案的有效性。在城域网某支持SRv6的多服务边缘设备（MSE）的节点上部署了1台服务器并将其作为靶机。另外，在云安全池内部署了2台服务器，每台服务器各虚拟化部署2台虚机、1台防火墙（FW）和1台入侵防御系统（IPS）。每台服务器宿主机系统采用开源虚拟化路由器（VR），并接入所有虚拟FW和IPS。VR作为池内与池外流量的锚点，也是SRv6路由调度策略的实施点。靶机与互联网的流量交互通过MSE与VR之间规划的SRv6策略实现引流，实验环境如图5所示。

实验首先对SRv6 SID进行规划，每一个SID代表一个引流行为，如表1所示。由于SRv6的流量策略在头端生效，因此将靶机的流量引入FW1时，只需头端多服务边缘（MSE）设备通过SRv6策略将流量引入靶机，并将上行流量segment list设置为A::1__C::1，下行流量segment list设置为A::1__B::1。如需将流量引入IPS1，上行segment list则设置为A::2__C::1，下行segment list设置为A::2__B::1；如需将流量依次引入FW1、IPS1，上行segment list则设置为A::1__A::2__C::1，下行segment list设置为A::2__A::1__B::1。

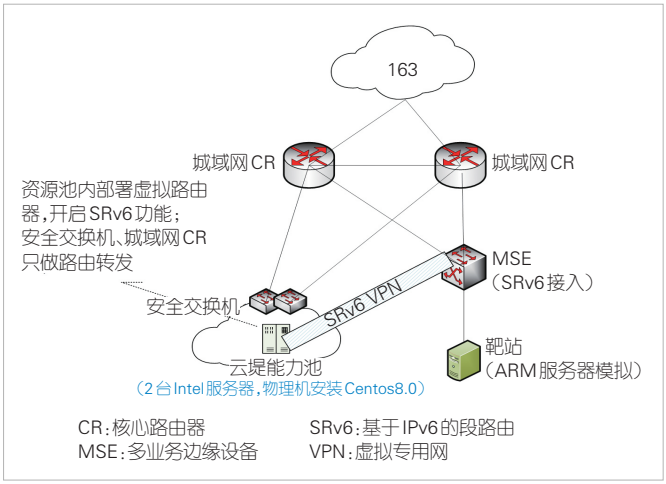
实验测试了流量编排能否按需穿过不同安全网元以及安全网元功能是否正常的情况。通过在FW1、IPS1处进行抓包，我们发现本方案可以实现基于SRv6的云网融合的流量编排。通过防火墙访问控制技术（ACL）功能测试，我们发现安全网元可以在该场景下正常工作。

2.2 系统性能优化升级

安全能力池将10余款安全能力的核心引擎、平台管理、数据分析进行解耦，融合微服务化、容器化等云原生技术，实现了从威胁监测、威胁分析到威胁处置，以及威胁审计等全流程自动化秒级联动。基于Lambda大数据技术架构，建立了统一的安全数据采集、分析、存储、查询和可视化能力，在保障平台健壮性、易于水平扩展等特性的同时，又满足查询的便利性，以及海量数据查询的低时延。

另外，针对实际的业务中断、运行速度慢等问题，本文给出以下两个典型解决方案：

1）在对资源池进行多线程压力测试时，我们发现程序运行速度远低于单线程。该问题导致系统无法满足实时性需求，用户体验下降。通过分析发现，流量型原子能力存在内存消耗大且访问具有随机性的问题。为了保证资源池系统稳定同时提升用户整体体验，方案引入大页内存技术。原始的小页内存通过页表来定位真实的物理内存空间，这使得中央处理器（CPU）在存取一个数据时，需要2次访问内存空间：第1次访问页表，然后根据页表计算出物理内存地址；第2次访问物理内存地址。为了提高地址变换速度，操作系统会在高速缓冲存储器中增设一个快表，来缓存部分经常使用的页表。这样通过访问一次高速缓冲存储器和一次内存就可以完成地址映射，实现速度的提升。但对于资源池来说，快表通常只能缓存几百页。如果页很小而程序占用内存很大，那么快表无法命中某页表的概率很大，缓存功能就失去



▲图5 引流测试环境

▼表1 SID规划

配置点	引流目标	SID	作用
VR1	FW1	A::1	将流量引入FW1
VR1	IPS1	A::2	将流量引入IPS1
VR2	FW2	A::3	将流量引入FW2
VR2	IPS2	A::4	将流量引入IPS2
MSE	靶机	B::1	将流量引入靶机
VR1 VR2	CR	C::1	将SRv6流量解封装将IPv4流量回送CR

CR：核心路由器　IPv4：互联网通信协议第4版　SRv6：基于
FW：防火墙　MSE：多服务边缘设备　IPv6的段路由
IPS：入侵防御系统　SID：段标识　VR：虚拟路由器

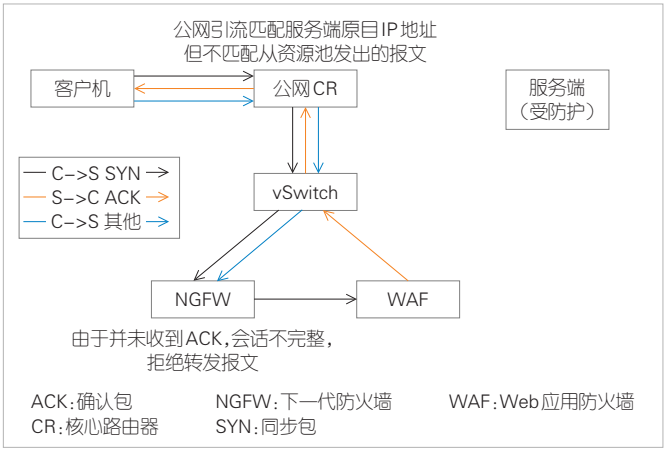
了效果。因此，资源池根据实际运行情况，调整了页的大小从而减少页表项，这使得快表尽可能完全缓存页表，从而提高程序性能。实验测得，大页内存在配置时采用对半配置原则效果较好。如果总内存为512 GB，则分配256 GB的大页内存。而当每一页大小为1 GB时，系统性能最佳。经过测试，当安全能力池配置16核32 GB内存的Web应用防火墙（WAF）时，大页技术可将程序性能提升50%左右。

2）在安全能力池多类型防护网元编排测试过程中，会出现某些业务中断的现象。例如，下一代防火墙（NGFW）和WAF进行流量编排时，出现流量经过WAF后业务中断的情况，如图6所示。客户端将与传输控制协议（TCP）3次握手的1号包同步包（SYN）引流至NGFW，NGFW再将SYN包转发给WAF（如图6中黑色箭头），WAF接收到客户端的SYN后，直接向客户端响应同步包–确认包（SYN–ACK）（TCP握手2号包，如红色箭头所示），客户端接收到SYN–ACK后，发起ACK（TCP握手3号包）。当ACK数据转发到NGFW时，此前NGFW只转发了1号包SYN，而2号包即WAF代理响应客户端的ACK未经过NGFW转发，因此当客户端发起的3号包到NGFW后，NGFW默认不放行（如蓝色箭头所示）。这导致客户端与服务器3次握手无法建立，业务异常。因此，通过优化TCP握手的数据传输验证机制，解决了此业务中断问题。

针对某些安全原子能力，例如堡垒机只能单租户独享问题，安全能力池会深入其内部结构，实现了堡垒机SaaS化。

2.3 原子能力统一纳管

安全能力池通常涵盖大量资源池底座与多种原子能力。传统资源池每引入一种新型原子能力都需要大幅度改动系统，因此存在交付效率低、系统维护困难等问题。安全能力池有上百个资源池、数千台硬件服务器，原子化后的安全能力组合方式呈指数级增长，因此如何快速纳管安全原子能力以及不同云下的资源池成为系统能否高效运行的关键。



▲图6 多网元流量编排异常问题示意图

针对以上问题，安全能力池在安全能力管理平台和底层资源池之间引入分布式高可用的安全业务中台。中台通过统一规范的接口为上层平台侧的扩展提供便利，并面向多安全厂商异构设备提供标准化接口，例如：《中国电信原子能力组件接口规范》将私有协议解耦，对南北向接口进行标准化。建立这种网络安全产品互联互通的标准，使得安全能力池能够实现跨厂商安全原子能力的统一纳管。所有厂商安全原子能力只要符合该标准，均可接入安全业务中台。统一纳管使得用户无须关注底层架构，这提升了业务的灵活性和高效性，打破了各厂商间安全设备难以互通的孤岛形态，建立了可信任的安全联动体系。标准化接口规范的推进和安全能力的适配，为云上安全可信生态的构建奠定了基础。接口规范目前已迭代至第5版。

3 安全能力池应用

3.1 典型应用场景

1）等级保护二级、三级认证应用场景

《中华人民共和国网络安全法》明确规定，网络运营者应当按照网络安全等级保护（后简称为等保）制度的要求，履行相应的安全保护义务。中国各行业大量重要信息系统已经或正在按照规定进行等保定级备案并定期接受测评，等保合规应用场景的需求不断增多。针对上述情况，安全能力池通过提供“等保二级套餐”“等保三级套餐”等产品解决方案，为各个政企用户提供安全咨询、定级、备案、建设、测评和监督检查。例如：通过安全管理中心和NGFW、端点检测响应（EDR）、日志审计、堡垒机等安全原子能力，满足用户等保二级认证的需求，并达到基础安全防护的效果；在上述基础上增加WAF、数据库审计、漏洞扫描3项原子能力可满足用户等保三级认证的需求。

2）用户增加内部安全防护能力场景

企业用户希望增强内部安全防护能力，保护内部系统正常安全运转。针对这一人群，可通过网络入侵防护、主机安全检测和综合审计这3类安全原子能力来满足用户需求。首先通过网络引流的方式将流量牵引至网络入侵防护平台，然后通过在主机上部署EDR客户端，进行漏洞扫描、基线检查以及病毒查杀，最后通过日志审计原子能力对各类设备的日志进行收集、解析和关联分析，从而达到全方位内部安全防护效果。

3.2 应用案例

目前，安全能力池已投入生产应用，为政府、金融机构和云服务提供商等政企用户提供了可定制、全面和深层次的安全防护服务，例如：某客户公司互联网出口使用简单堆叠式硬件安全防护，面临硬件设备升级困难、维护成本高等问题。另外，该客户在将本地业务系统迁移上云过程中也存在新的安全挑战。本文所提出的新型安全架构，通过安全管理平台调用了电信某省级安全能力池中的10余种能力。流量型原子能力通过Flowspec控制器将流量从客户公司网络出口牵引至资源池，流经池内安全检测和服务链自动化编排后，再次回注到该公司出口；非流量型原子能力则直接使用资源池内SaaS化能力提供安全检测或分析。最终，该安全能力池具备按需组合、流量编排等技术优势，为用户提供了全面、纵深的安全防护能力，实现其云上等保三级需求，现网安全攻击防护成功率高达99%。

4 结束语

本文提出了云网安一体化的安全能力池技术架构。该架构基于Flowspec控制器与SRv6技术实现了大网与资源池内部流量的牵引调度和服务链编排，增强了整体防护性能，提高了流量编排效率；基于多云底座、跨厂商安全能力统一纳管，实现了服务的按需组合，灵活扩张；基于大页内存等技术，实现了资源池系统的性能的优化。安全能力池为安全行业探索出一种高效、智能、稳定的云安全防护服务模式。

未来，安全能力池可在两个方向上进行升级和迭代：

1）动态授权访问与持续安全监测。当各个资源池内部网络安全边界防护逐渐模糊时，需要改变传统的边界防护模式。针对这一问题，可研究基于零信任的动态授权访问系统，确保安全能力的动态授权访问与持续安全监测，更好保证资源池内部的安全性[11-12]。

2）提出面向云网融合的新型城域网技术方案。通过SRv6、以太虚拟专用网络（EVPN）等新协议的支持能力，实现流量的自动化调度和网络的自动化配置，解决流量转发迟滞的问题。

参考文献

[1] ALLAM Z, DHUNNY Z. On big data, artificial intelligence and smart cities [J]. Cities, 2019, 89: 80-91. DOI: 10.1016/j.cities.2019.01.032

[2] TANG Y, DANANJAYAN S, HOU C, et al. A survey on the 5G network and its impact on agriculture: challenges and opportunities [J]. Computers and electronics in agriculture, 2021, 180: 105895. DOI: 10.1016/j.compag.2020.105895

[3] ARZIEVA J, NUKUSBAEV N. Network security issues and effective protection against network attacks [J]. Bulletin of science and practice, 2021, 7(9): 479-485. DOI: 10.33619/2414-2948/70/45

[4] SERROR M, HENZE M, HACK S, et al. Towards in-network security for smart homes [C]//Proceedings of the 13th International Conference on Availability, Reliability and Security. ACM, 2018: 1-8. DOI: 10.1145/3230833.3232802

[5] SUBRAMANIAN N, JEYARAJ A. Recent security challenges in cloud computing [J]. Computers & electrical engineering, 2018, 71: 28-42. DOI: 10.1016/j.compeleceng.2018.06.006

[6] HERARDIAN R. The soft underbelly of cloud security [J]. IEEE security & privacy, 2019, 17(3): 90-93

[7] 回红秀. W公司安全资源池项目风险管理研究 [D]. 北京: 北京邮电大学, 2021

[8] 吴晨花, 王瑶, 李映壮. 基于SDN安全云资源池提升中小企业安全防护能力 [J]. 科技创新导报, 2019, 16(5): 140-143. DOI: 10.16660/j.cnki.1674-098x.2019.05.140

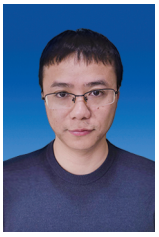
[9] 乔延臣, 张结辉, 陈晓帆. 基于安全资源池的云安全解决方案 [J]. 信息技术与标准化, 2018(9): 57-62

[10] 才宏. 云资源池网络安全策略的分析与设计研究 [J]. 网络安全技术与应用, 2021(6): 79-80. DOI: 10.3969/j.issn.1009-6833.2021.06.049

[11] WARD R, BEYER B. Beyondcorp: a new approach to enterprise security [J]. USENIX & SAGE, 2014, 39(6): 6-11

[12] BUCK C, OLENBERGER C, .SCHWEIZER A, et al. Never trust, always verify: a multivocal literature review on current knowledge and research gaps of zero-trust [J]. Computers & security, 2021, 110: 102436. DOI: 10.1016/j.cose.2021.102436

作 者 简 介



余启明，天翼安全科技有限公司开发工程师；负责安全能力池相关技术架构和开发工作，研究方向为安全服务SaaS化；已发表论文1篇。

吴爽，天翼安全科技有限公司研发工程师；现从事网络安全产品研发；已发表论文1篇，申请专利4项。

黄帅，天翼安全科技有限公司研发工程师；现从事网络安全产品研发和强化学习等；已发表论文4篇，拥有软著2项。

刘紫千，天翼安全科技有限公司总经理，正高级工程师；主要从事网络安全技术研究和安全产品研发运营工作；获得省部级科技进步奖4次；已发表论文10余篇，获发明专利10余项。