

# 5G+时代的软件定义安全技术架构研究与实践

全硕，王旭亮，朱泽亚
（中国电信股份有限公司研究院，北京 102209）

**摘　要**：新基建和数字经济激发了云网安全的保障需求，云网融合安全也是未来的重要发展趋势。首先分析了面向 5G 专网用户提供整体安全服务面临的三大类问题，提出了在 5G+时代软件定义安全整体架构。其次基于该架构介绍了相应的原型系统的设计与实现。最后验证了基于云化构架的软件定义安全编排与调度体系有助于精确化地整体解决 5G+时代 5G 专网企业客户的业务安全威胁和隐患，为后续的研究提供了系统性的参考价值。

**关键词**：软件定义安全；服务功能链；网络功能虚拟化
**中图分类号**：TP393
**文献标识码**：A
**doi:** 10.11959/j.issn.1000−0801.2021277

# Research and practice of software-defined security technology architecture in the 5G+ era

QUAN Shuo, WANG Xuliang, ZHU Zeya
Research Institute of China Telecom Co., Ltd., Beijing 102209, China

**Abstract:** Cloud network security has become a strong need under the background of the new infrastructure and digital economy, while cloud network integration security has been defined as an ongoing trends. Initially, three major types of problems facing 5G private network users were presented in providing overall security services, and an overall software-defined security architecture in the 5G+ era was proposed. Furthermore, the corresponding prototype system design and implementation was discussed based on this architecture. At the end, the verification shows that the software-defined security orchestration and scheduling system based on the cloud-based architecture helps to accurately solve the overall business security threats and hidden dangers of 5G private network enterprise customers in the 5G+ era, providing systematic reference value for subsequent research.

**Key words:** software-defined security, service function chain, network function virtualization

## 1　引言

云网安融合基础设施作为新基建的重要组成部分，正在快速推动企业业务的数字化转型，在 Gartner 的《网络安全的未来在云端》报告阐明了在新的网络和安全模型的基础上进行云网络和安全转型的潜力，该模型称为安全访问服务边缘（secure access service edge，SASE）。随着符合零

收稿日期：2021−10−20；修回日期：2021−12−10

信任网络和SASE理念的云网安产品的不断成熟，才能在 5G+时代真正打消企业数字化转型中最大的疑虑，快速推动云网安基础设施+数字化应用的整体生态发展。

运营商作为新基建与数字经济的重要市场参与方，在 SASE 理念基础之上，提出了 5G 专网+云化安全服务的综合解决方案。5G 定制网业务基于 5G SA 2B 网络进行承载，采用大区集约管理、省级集中控制的方式，按需构建多级 2B 业务转发面，形成“2+31”5G 定制网框架结构，具体如图 1 所示，在全国，部署 2 个 5G 定制网集约节点，包括数据面网元 UDM 和部分信令面网元（PCF、NRF、SCP），满足用户数据、业务策略控制、计费的统一集约管理。在省层面，分省部署控制面网元 SMF 和用户面网元 UPF，用于实现全国各省份业务承载。基于上述网络框架，在全国开通 5G 定制网政企 2B 默认切片和定制网物联网默认切片，支持集约场景业务全国服务。

5G 专网虽然为企业提供组网与上网业务的便利性，但专线业务本身的安全隐患和防护问题依然没有得到充分解决。反而随着 5G 专网的推出，企业客户的业务和应用变得更加多样化，提供能够按需定义、快速开通、动态可重构的安全服务与产品是亟须解决的核心问题之一；如何基于 5G 专网面向客户业务提供按需、高效、精确以及整体化的安全防护服务面临如下 3 方面的问题：第一，云化部署的 5G 定制网本身带来的灵活定制组网的特点使网络的安全边界模糊，新一代安全威胁凸显，依靠相对独立、局部、烟囱式的安全能力无法满足防护需求；第二，用户业务的安全防护需求从客户侧延伸到云侧，需要整体安全能力解决方案，实现主动防御；第三，无法基于网络安全威胁分析数据的“头疼医头”式方案无法有效消除安全威胁，安全服务碎片化、防护手段数据采集离散且缺少关联协同以及缺乏多个安全服务能力的自动化调度能力。

针对上述存在的问题，本文提出一种基于云化部署的软件定义安全服务整体架构与方案，经

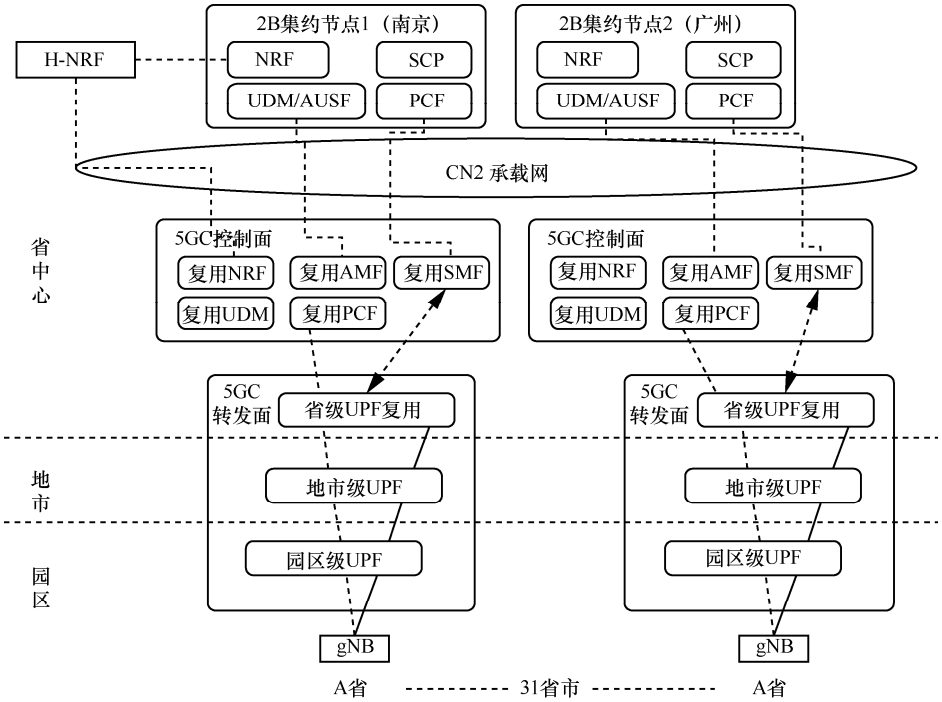


图 1　运营商 5G 定制网网络架构

过原型系统验证可以有效解决安全服务能力碎片化、安全能力部署分散造成的无法根据客户安全定制化需求进行高效自动化调度与部署的问题。

本文解决方案中大量采用云计算、NFV、SDN以及包括多种服务功能链（service function chain，SFC）实现技术等。根据 ETSI NFV 组在 2018 年发布标准 ETSI GS NFV-EVE 011[1]，NFV 技术旨在推动传统网络设备的云化，具体来说，是在标准 IT 服务器组成的云资源池上运行虚拟机，将网络设备的应用程序运行在这些虚拟机像传统物理网元一样向最终用户提供网元功能服务。通过标准服务器和虚拟机配合的方式承载传统网元服务实现了传统网元设备的软硬件解耦，从而获得网元应用的统一云化承载、弹性伸/缩、网络业务自动化编排等传统网络不具备的先天技术优势。NFV 最大的特色是它在传统云计算技术框架的基础之上定义了一整套管理编排框架——MANO[2]（management and network orchestration，MANO）。根据 ETSI NFV 组在 2020 年发布的标准 ETSI GR NFV-REL 011 [3]，它由 3 部分组成，包括网络服务编排器（network function virtualization orchestration，NFVO）、虚拟网元管理器（virtual network function，VNF）以及虚拟基础设施资源管理器（virtual infrastructure manager，VIM）。

SDN 技术从 2009 年被提出，一直被视为近 10 年网络能力开放和网络架构创新的核心基石性技术。主要包括 SDN 控制器和被控制器所管理的网络设备组成。SDN 控制器会根据上层业务的要求给其所管理的网元设备进行配置下发、网络流量调度、网络设备状态监控与收集以及相应的运维操作。本文在一套 SDN 控制器的基础之上，按需采用多种 SFC 技术对云资源池内的软件交换机、硬件交换机以及硬件路由器进行统一的管理和配置下发。

SDN 控制器对安全业务的引流方式逐渐丰富且可以按需采用。SDN overlay 虚拟网络提供了一种集中的管控网络，通过把传统网络设备的所有功能拆分为控制平面和转发平面并解耦，将控制逻辑集中控制到控制平面的 SDN 控制器中。通过标准化南向接口控制和管理数据平面的网元，与北向的开放接口和各种定制化的程序进行交互，以调用索取的各种网络资源，从而建立高度可编程、可拓展和自动化的网络，简化了网络的配置、管理和优化[2]。

SFC 技术的目的是动态建立服务功能链使不同租户的流量可以按照不同顺序导向不同的服务功能模块[4]。SFC 使网络报文流量走特定的路径，而不是通过 IP 目的地址查看路由表的最终目的地[4]。基于 SDN/NFV 的 SFC 可以有效灵活地调整到端的安全服务路径，达到安全服务资源的高效利用。本文提出的方案中基于一套 SDN 控制器实现 4 种安全业务引流方式，包括 PBR（policy based routing，PBR）、SRv6、VxLAN 以及 Networking-SFC 等，重点介绍其中 3 种。

- SRv6 由于具备很强的网络编程能力以及流量工程能力，契合了网络虚拟化思想，为服务功能链技术提供了新的实施思路。SRv6 基于 IPv6 协议栈，支持 SDN 集中控制方案，适应了当前网络虚拟化发展趋势和推进 IPv6 转发平面部署需求，SRv6 所具备的流量工程能力以更加简洁的方式实现了服务功能链路径 SFP 编排与转发过程，且无须大规模设备升级即可实现服务功能链功能，降低了服务功能链部署开销和运维成本[4]。
- VxLAN 作为过去十年来网络虚拟化最成功的实现方案之一，通常与 SDN 控制器配合实现对各类网络设备的 overlay 网络流量进行转发。其中，VxLAN 利用 network overlay 的理念，实现业务网络路径与真实网络设备解耦的做法，真正实现了上层多种业务网络与底层统一基础设施网络解

耦，大大解放了生产力，带动了网络生态近十年的大繁荣，催生了 SD-WAN、云网络以及 SASE 等一大批新型网络产品。本文中为了提升云网安产品能力的快速开通也遵循 SDN 的理念，且成功地在运营商安全资源池场景中实现了体系化的软件定义安全能力。

- Networking-SFC 主要应用于 SDN 技术中，根据不同的安全策略联同 NFV 提供安全 SFC。SFC 利用了 SDN/NFV 的优势，根据安全业务的需求可以个性化将一系列虚拟网络功能有序组合，形成若干个逻辑上的链式服务功能集，同时通过入口分类器的分类规则和逻辑集中的控制器制定的流量调度规则[5]。

## 2　相关研究

针对软件定义网络的管控引流和编排问题，从业者已经提出使用软件定义网络的思路构建云网协作整体架构解决安全设备资源的调度管理问题。本文选取文献[6-8]与本文的方案相比对。

文献[6]提出了 6G 可定义的 6G 安全架构模型，探讨了基于软件定义的理念实现 6G 安全架构、能力定制与协同。该研究力图基于软件定义的理念设计基础资源网络资源和安全资源之间的控制编排承载架构，但是缺少了对安全能力进一步的抽象，对安全能力的调度和基础能力。本文在安全能力的基础上对安全产品与应用抽象为安全可编排调度的内容，对安全服务功能链的引流和开通业务给出了解决方案。

文献[7]提出了一种基于软件定义的安全能力架构，该架构能够实现 5G 网络模块化的、可调用的、快速部署的内生安全能力，以满足 5G 业务多样化和 5G 系统架构变迁所带来的安全需求。该方案考虑的是 5G 时代的网络业务模式和针对业务的可能安全需求，然而网络架构设计没有全面完成全面解耦，物理设备管控面没有统一，不能按需、差异化地定义安全产品内容。本设计方案使用了基于 PBR、SRv6、SFC 等方式全面将安全能力云网资源统一编排。

文献[8]对软件定义网络平台实现安全设备资源池化进行了研究，通过 SDN 平台实现港口网络安全设备统一集中调配使用和安全设备重新整合。该研究着重于使用软件定义网络对硬件安全资源的部署和管控，但是没有考虑使用虚拟化网元对安全设备解耦的方式重新编排，无法自由管理和调度复杂多样的物理硬件资源。本方案使用 NFV 技术对硬件设备进行解耦，使用容器部署等方式可以同时对云网安资源统一管控和云化承载。

综上所述，本文遵循软件定义各类服务的理念，在运营商的云网安融合的基础设施上，提出了面向 5G 企业客户的安全产品编排、调度、承载以及管理等多维度的整体技术框架，根据原型系统的验证结论，本研究具备独创性和较高的研究价值。

## 3　设计与实现

针对 5G 专线业务安全产品服务迭代周期慢、用户差异化的安全需求无法满足、局部单一的安全防护体系无法应对新一代安全威胁、安全设备资源利用率低下等问题，本文通过借鉴云网融合、软件定义、服务建模等理念，提出了在 5G+时代软件定义安全体系架构的设计和实现方案。通过该方案可以实现安全产品服务的快速定制开通、安全能力的按需编排调度、网络控制与安全控制的联动协同、云网安资源的高效利用，构建云网安融合、协同、全面的安全能力服务体系。

### 3.1　软件定义安全总体架构

软件定义安全总体架构如图 2 所示，分为安全产品/应用、安全服务定义/设计、安全服务编排、SDN 控制器、基础设施、云网安资源统一管理 6 个模块。

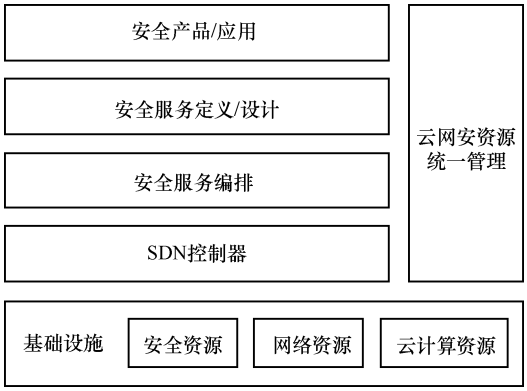


图 2　软件定义安全总体架构

- 安全产品/应用：包括各种各样的安全产品和应用。
- 安全服务定义/设计：将安全产品与应用自动转义为安全服务编排模块可编排调度的内容（编排包）。
- 安全服务编排：解析编排包，根据资源需求进行基础设施资源的编排调度；根据规则策略和动作，进行相应的引流控制。
- SDN 控制器：实现 5G 专线用户流量的引流控制。分为池内引流和大网引流两部分。池内引流根据用户购买的安全产品，将用户流量按需引流到各个安全原子能力（指安全特性组件，如 FW、IPS、WAF、主机漏扫、Web 漏洞扫描等）；大网引流则将用户的流量引流到安全资源池内。
- 基础设施：由安全资源、网络资源、云计算资源组成的安全资源池。其中安全资源包括各种硬件、软件形态的安全设备、安全原子能力等；网络资源包括物理网络设备、虚拟网元等；云计算资源包括承载安全能力、网元等组件的物理机、虚拟机和容器。
- 云网安资源的统一管理：云计算资源、网络资源、安全资源的统一管理，包括资源的生命周期管理、资源信息的实时采集与控制、镜像管理等功能。

#### 3.1.1　安全服务定义

安全服务定义与设计参考 PSR 服务建模体系，通过构建 PSR（product service resource）安全能力对象模型，进行产品－服务－资源的三层解耦，实现安全产品的灵活组装、快速加载和开通。

PSR 模型定义了产品与服务、服务与资源的映射关系，PSR 安全产品模型如图 3 所示。

定义一个新的安全产品时，根据安全产品的属性、服务动作等定义，自动生成 PST（product service template）。开通业务时，PST 能够将安全产品自动解析成对应的安全服务 CFS 组合，再根据预先定义的 CFS→RFS→RES 的映射关系，得到所需资源，再通过编排器完成相应资源的编排、调度与控制下发。

PSR 模型的引入，减少人工干预过程，实现安全产品的灵活组合和快速开通。当引入不同安全厂商、新的安全原子能力类型时，只需在安全服务和安全产品中进行定义，即可完成安全原子能力、服务的更新迭代，具有较高的灵活性和可扩展能力。

PSR 模型是安全服务编排的基石。通过产品到服务、服务到资源的拆分，可以实现更加灵活的编排调度；通过不同类型资源的解耦，编排器可以根据资源的需求、资源的特性进行自由组合，为实现网络控制和安全控制的联动协同、资源的高效利用提供了基础。

#### 3.1.2　安全服务编排

安全服务编排模块能够自动高效地完成资源分配、策略下发等，实现安全服务的快速开通。该模块包括业务的编排控制、资源的编排调度两部分。在进行编排时，具体步骤如下。

- 安全服务定义与设计模块通过 PST 模板将安全产品应用解析成资源需求、规则动作等信息，并将这些信息告知安全服务编排模块。

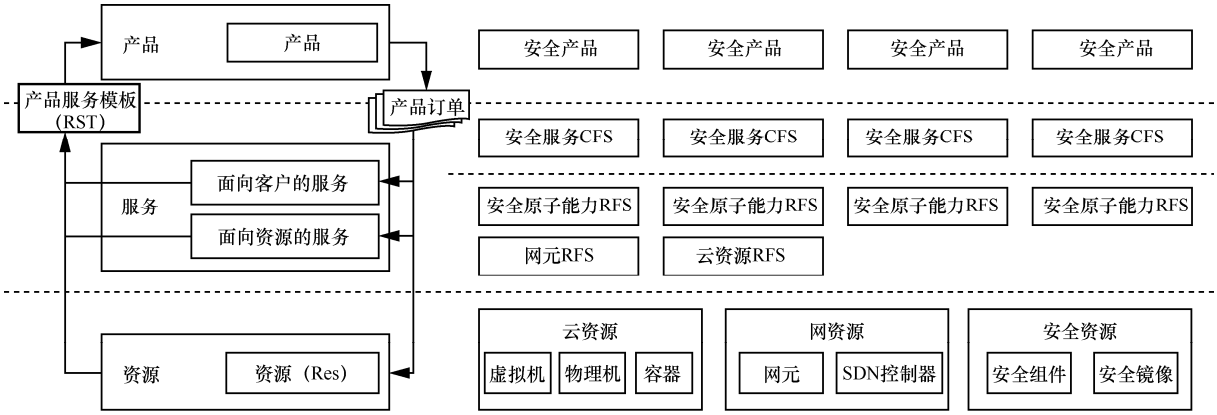


图 3　PSR 安全产品模型

- 安全服务编排模块根据产品信息、资源需求等内容，向云网安资源统一管理模块请求可用资源。如果现有资源满足需求，将信息返回给安全服务编排模块，如果现有资源不满足，则按需进行创建。安全服务编排模块接收到信息后，根据一定的策略：比如用户的地理位置（就近分配安全资源池，减少引流造成的网络资源损耗）、资源的剩余情况（优先分配资源使用率较低安全资源池，优化资源利用率）、网络组网情况（不同的组网情况，需要不同控制协议支持）等，进行资源的自动化编排调度，并通过云网安资源统一管理模块进行具体的配置策略下发。
- 在完成资源的编排调度后，需要按照产品需求进行业务的编排控制，分别调用大网控制器和安全资源池控制器向对应的设备下发大网业务配置信息。安全服务编排流程如图 4 所示。

通过上述架构，实现资源编排和业务编排的分离，增加了系统的灵活性；实现云网安资源的统一编排、网络控制和安全控制的联动协同，提高资源的整体利用效率。

### 3.1.3　SDN 控制器

SDN 控制器包括大网引流和池内引流两部分。

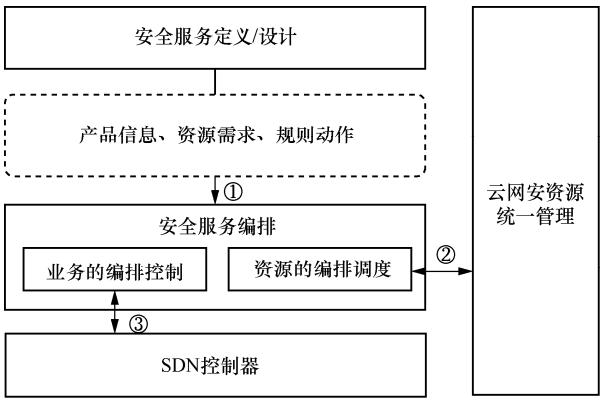


图 4　安全服务编排流程

通过控制器在相应网络设备、流分类器和 vRouter 等网元节点上下发引流控制信息，实现安全能力端到端的打通。

SDN 控制器北向对接安全服务编排模块，通过应用程序编程接口（API）接收编排信息，南向通过 OpenFlow、Netconf 等标准协议对接网络设备、虚拟网元。

（1）池内引流

池内引流要求用户的流量通过转发流经特定的安全原子能力，可以参考 SFC 架构。

SFC 服务功能链系统架构如图 5 所示，主要包含以下关键部分。

- SF（service function）提供特定网络服务的节点[4]。
- SFF（service function forwarder）支持 SFC

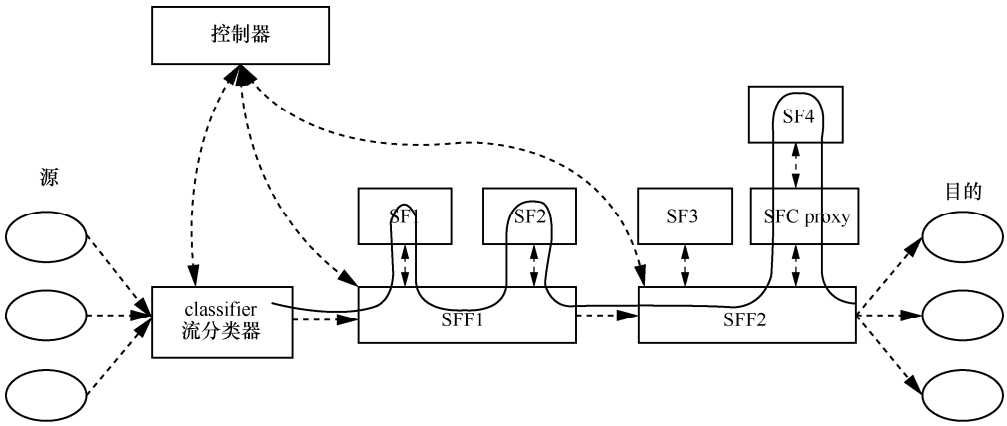


图 5　SFC 系统架构

的转发器，一般挂接 SF 节点，用于将报文转发到 SF 节点。

- SFP（service function path）是 SFC 对应的转发路径[9]。
- classifier 用于将数据流分类，并转发到对应的 SFP。
- SFC proxy：为不支持 SFC 的 SF 节点提供代理接入 SFC 的能力。
- SFC：服务功能链，指一组 SF（服务功能）节点组成的序列。

安全资源池内的引流方案中，SF 通常指的是安全原子能力，SFF 指的是 vRouter、vSwitch 等虚拟网元，classifier 指资源池的入口设备或流量经过的第一个虚拟网元。池内 SDN 控制器根据池内的网络设备能力、组网情况以及 SFC 架构，通过不同的协议框架（PBR、Networking-SFC、SRv6 等），向流分类器和业务功能转发器下发配置，实现用户安全业务的按需引流。

1）大网引流

大网引流目的是把用户的流量牵引到安全资源池内。大网引流模式如图 6 所示，安全服务编排器将安全资源池路由器作为流量的结束点，然后对流量经过的路径进行编排，到相应的网络控制器上下发引流策略。

大网引流还需要池内控制器和网络控制器之间的协同。以 SRv6 方案引流策略为例，企业客

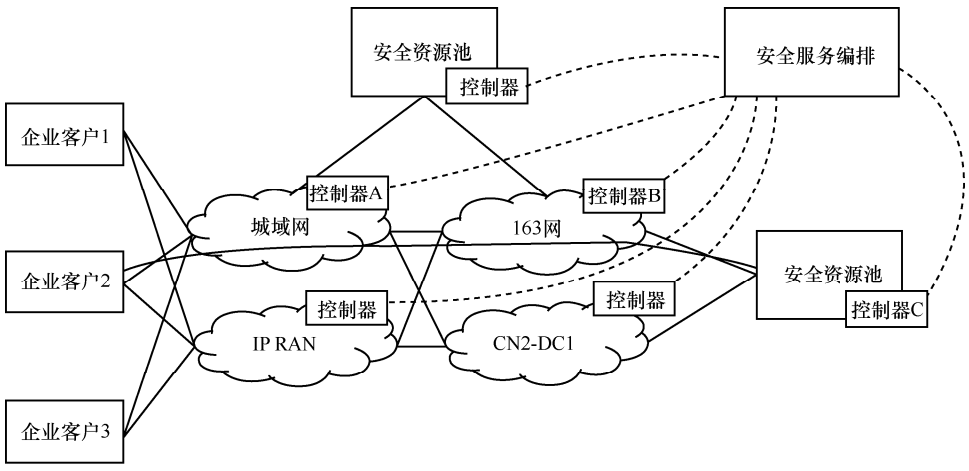


图 6　大网引流模式

户 2 经过城域网和 163 网络到达安全资源池，控制器 A 和控制器 B 分别创建 SRv6 policy 进行引流，池内的 SRv6 policy 绑定一个 binding SID 对外发布，作为大网 SRv6 policy 中 segment list 的一个 SID，完成整个流量端到端的控制。

#### 3.1.4　基础设施

基础设施主要包括安全资源、网络资源和云计算资源。

安全资源主要包括基于硬件的安全设备以及能够虚拟化部署的安全原子能力。随着安全设备运维复杂、利用率低下、网络稳定性差、投入成本较高等问题，安全能力也在逐步向虚拟化方向发展，因此安全资源池应该能同时兼顾不同形态的安全能力。同时，需要制定标准化和规范化的安全原子能力接口，屏蔽不同厂商不同安全原子能力在服务编排调度的差异性，实现安全产品服务的快速定制开通、安全能力的按需编排调度的基础。

网络资源主要分为网络设备和虚拟网元。网络设备指的是具有高性能转发的路由器、交换机，通常部署在大网和安全资源池的出入口。这部分设备需要保证流量的高效、稳定、可靠，因此采用物理设备。虚拟网元指的是池内的业务转发模块，采用 NFV（网络功能虚拟化）技术，实现软硬件解耦，使得网络服务可以快速迭代，以应对通信技术的升级换代并降低硬件成本[5]。

云计算资源是安全能力和网络功能云化承载的基础。主要包含物理机、虚拟机和容器，分别用于部署虚拟化网络和安全功能以及容器化的网络和安全功能。

#### 3.1.5　云网安资源统一管理

云网安资源的统一管理实现资源的生命周期管理、信息实时采集与控制、镜像管理、监控运维等功能。

资源的生命周期管理包括了虚拟机、容器、容器集群、网元、安全原子能力等资源的动态按需创建、删除、迁移、扩/缩容、灾备、状态管理等。

信息实时采集与控制包括将各类资源的使用情况、状态、运维信息等数据实时采集，辅助安全服务编排模块在进行编排时计算资源的调度情况；对于部分安全原子能力，能够根据用户的业务进行安全策略和配置的下发。

镜像管理包括了镜像的上传、分发、同步、检索、存储等功能。

监控运维模块能够及时地掌握各类资源的实际使用情况，在出现异常、告警时能够通过异常检查、根因分析等手段保障用户业务的正常运行。

云网安资源的统一控制是实现资源高效利用的基础，也是云网安深度融合的前提。

### 3.2　关键技术

#### 3.2.1　支持多种协议的池内引流控制

综合考虑网络设备能力、安全资源池内组网情况的差异性以及引流方案的完备性和可扩展能力，控制器支持多种协议的引流控制，在实际应用中按需采用。

以基于 PBR、Networking-SFC、SRv6 共 3 种框架协议的引流方案进行阐述。

（1）基于 PBR 的引流方案

池内引流将用户的流量按需引流到各个安全原子能力中，而安全原子能力本身所具备的转发能力是不确定的，例如是否支持 PBR、SRv6 等协议。因此，通过 vRouter 挂接安全原子能力的方式实现流量的高效转发。

基于策略路由（policy based routing，PBR）通过在流分类器和 vRouter 上面配置静态路由实现流量转发。PBR 策略路由流程如图 7 所示。

基于 PBR 的引流策略是一个通用的解决方案，通过静态路由实现，网络设备基本支持。其缺陷也比较明显：需要在路径上的各个节点都进行配置，开发运维复杂，特别是随着产品业务的复杂度提升，维护会变得更加困难；可扩展性受限不够灵活，安全产品服务的变动复杂；通过流

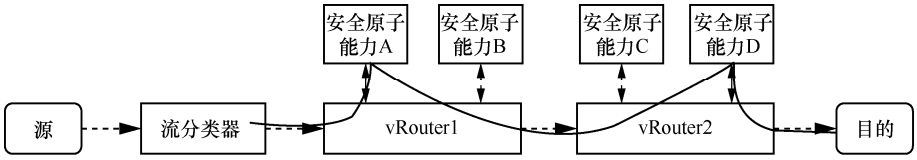


图 7　PBR 策略路由流程

量的源地址和目的地址进行分类，无法进行更细力度的流量控制，如区分上下行流量等。

（2）基于 Networking-SFC 的引流方案

Networking-SFC 服务功能链流程如图 8 所示，Networking-SFC 通过动态建立服务功能链使不同用户的流量可以按照不同顺序导向不同的安全原子能力[10]。在创建虚拟机时会创建多个网络端口（port），选择其中的两个 port 组成 port pair，一个作为流量入口（Ingress），一个作为流量出口（Engress）。将一连串的 port pair 组合形成一个 port chain 代表实际的安全服务功能链，通过 port chain 使用户流量走特定的路径。在实际使用中，port chain 数量较多较复杂，则可以把多个 port pair 定义为 port pair group，可以简化操作以及实现多条安全服务功能链的负载均衡。

Networking-SFC 依赖于 OVS，优点是不需要额外的转发模块，安全原子能力的端口在虚拟交换机上，可以很方便地进行引流。但是也受限于 OVS 的性能、稳定和可扩展性。例如当安全能力使用 SR-IOV、PCI Passthrough 等直通类型网卡，则需要物理交换机支持 OpenFlow 流表。

（3）基于 SRv6 的引流方案

SRv6 服务功能链流程如图 9 所示，分段路由支持在入节点显式的编程流量转发路径，通过构建分段列表使用户的流量按照 Sid 的组合依次流经各安全原子能力。考虑安全原子能力对 SRv6 协议的支持情况，引入 SR Proxy 组件。

通过 SRv6 的方式，只需要在安全服务功能链的入节点下发 SRv6 policy 即可，不需要在网络节点中维护逐流的转发状态，降低了控制平面的部署难度；与底层的物理组网解耦，可以进行灵活的扩展；通过 service type、traffic type 等信息进行细粒度的控制。同时，基于 SRv6 的引流方案也存

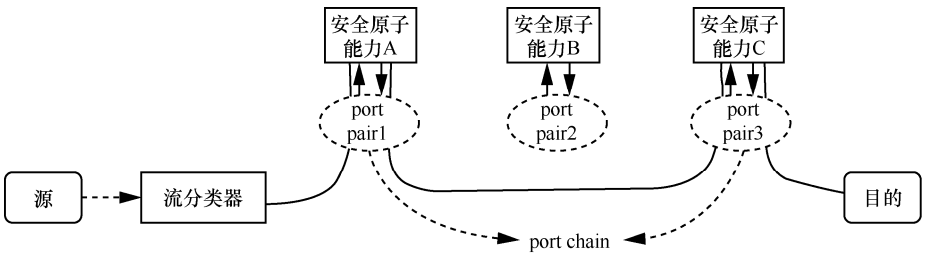


图 8　Networking-SFC 服务功能链流程

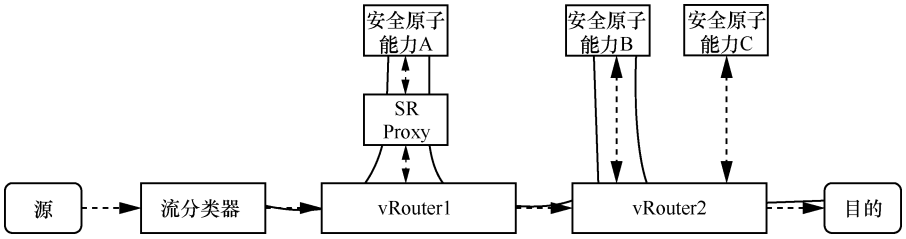


图 9　SRv6 服务功能链流程

在一定的问题：当安全原子能力数量过多时，分段列表中 SID 数量较多，SRv6 的报文开销相对较大；SR proxy 的引入增加了部署难度；支持 SRv6 协议的网络设备成本较高，现网不具备条件。

#### 3.2.2　安全原子能力的云化承载

为实现安全原子能力的灵活组合、安全产品的快速迭代，除了通过 PSR 模型构建映射关系，还需要底层能力支持。

安全原子能力随着网络攻击和安全防御手段快速变化呈现多样化的趋势；本文提出的软件定义安全体系架构也支持实现了标准化接口的安全原子能力灵活接入。可以想象，5G+时代不同安全设备厂商、不同种类的安全原子能力数量呈爆发式增长，但是安全资源池可能受资源限制无法部署所有类型的安全原子能力（特别是边缘资源池），导致部分用户无法按需定义安全产品。因此，本文提出了一种基于多容器集群的安全原子能力云化承载方案，实现安全原子能力跨集群、跨 DC、跨地域的灵活组合。

安全能力云化承载方案的整体架构如图 10 所示。

容器集群采用 K8S 作为编排管理工具。将可容器化部署的安全原子能力封装为 Pod，非容器化部署的安全能力使用代理网关的方式接入 K8S 进行统一管理调度。引流所需要的 vRouter 等网元和控制器进行按需部署。多个 K8S 集群通过多容器集群的管理、编排与调度模块拉通，实现不同容器集群内应用（安全原子能力）的夸集群访问。

通过上述方案，还可以将常用的安全原子能力进行集群化部署（一个容器集群只部署一类安全原子能力），便于维护和访问控制，实现安全原子能力的可靠性、稳定性以及负载均衡。

## 4　关键问题

通过软件定义安全整体架构的设计与关键技术实现，基本验证了本文方案的可行性。但是在实现的过程中，也碰到一些问题需要进一步讨论解决。

### 4.1　多厂商网络设备适配

SDN 控制器在网络设备上配置引流策略时，需要适配多个厂商的各类网络设备。虽然有标准的网络管理协议（例如 Netconf）和统一的数据建模语言规范（例如 YANG），但是在不同网络设备配置相同策略时，构建的数据模型仍然有较大的差异性，需要开发相应的适配器进行适配，这给底层网络设备的接入带来了极大的挑战。

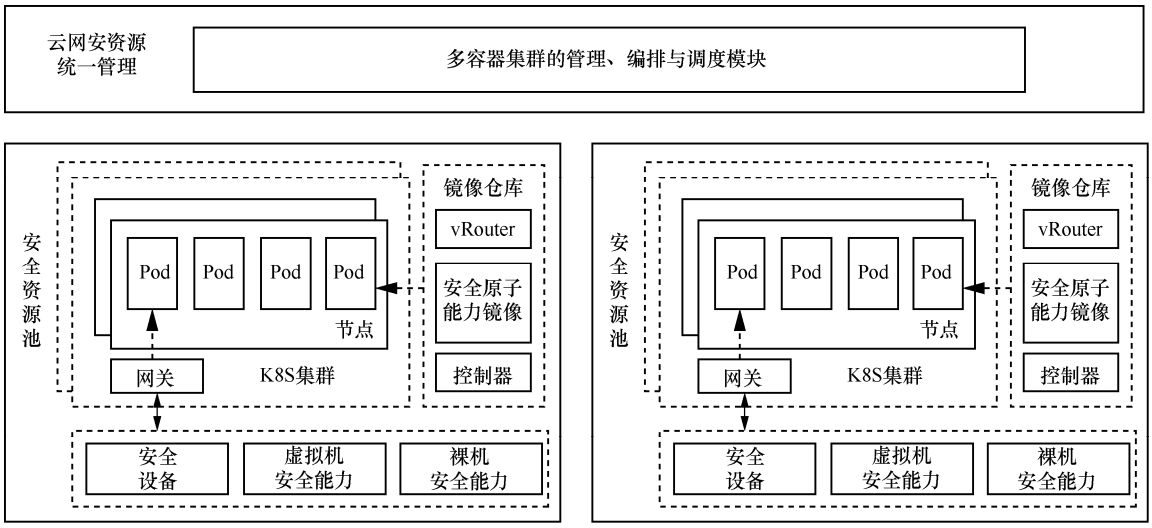


图 10　安全能力云化承载方案

现有方案采用 SDN 控制器的传统架构，在SDN控制器与网络设备的南向API中间加了SAL（service abstraction layer），通过抽象逻辑和接口在一定程度上简化了设备的适配难度，但是面对多厂商、多种类、多版本的海量设备接入，仍然没有从根本上解决问题。

针对该问题提出了两种思路。

- 不同网络设备通常会有相应的控制器，SDN 控制器通过调用设备控制器的北向接口，实现引流策略配置下发。优点是减少SDN 控制器适配设备的工作；缺点是需要厂商按照规范开放北向接口，增加了购买设备控制器成本。
- 在SAL层之上构建共享数据与结构模块。该模块通过使用标准数据结构和数据建模语言，定义标准化的数据模型，使其能在不同协议、不同厂商设备的应用程序中实现数据共享。设备进行接入时，根据共享数据自动组装成设备可识别的配置指令，实现引流配置下发。优点是进一步简化设备适配难度；限制是需要针对不同协议制定标准化的数据结构和数据模型。

### 4.2 避免 SRv6 环路

池内引流采用SRv6协议时，需要将流量引入SRv6 policy。流量的数据报文格式分为SRv6和非SRv6两种，对于SRv6格式的报文，通过匹配SRv6 policy的BSID直接引入；对于非SRv6格式的报文，则使用路由匹配的方式引入。

安全资源池的实际部署中，考虑网络设备成本通常使用一台物理路由器同时作为流量的出入口。对于非SRv6格式报文以路由匹配方式接入，存在环路问题。当流量进入路由器后，查表转发到 SFF 中，流经安全原子能力后回到路由器，查表会再次转发到 SFF 中，从而形成环路。

现有方案采取的策略是在路由器中通过 PBR 的方式将流量引入SRv6 policy，也引入了PBR的缺点，比如配置烦琐。针对该问题提出了另一种思路：将物理路由器虚拟成两个虚拟路由器，一个作为入口设备，一个作为出口设备。这种方案的优点是逻辑比较明确，无须额外配置，限制是需要物理设备支持，并且虚拟化后设备的性能有待验证。

## 5 结束语

本文从分析了 5G+时代专线业务所面临的安全隐患和防护问题。针对上述分析，提出了一种基于云化部署的软件定义安全服务整体架构与方案，通过引入 PBR 服务建模体系可以实现安全服务的按需定义与设计、安全产品的快速定制开通，满足专线用户多样化差异化的安全产品需求；同时基于安全能力、网络功能的云化承载、安全控制和网络控制的联动协同，云计算资源、网络资源、安全资源的统一编排调度与管理，实现了云网安能力的深度融合，为用户提供端到端的安全防护体系。经过系统原型验证表明基于云化构架的软件定义安全编排与调度体系有助于精确化的整体解决5G专网用户的业务安全威胁。

本文完成了 5G+时代软件定义安全的整体设计以及SDN控制器和云化承载等原型的实现，初步验证该方案可以有效地解决 5G 专网用户的安全问题。未来工作主要从以下两方面展开：继续完善整个系统的实现，包括安全服务定义与设计、安全服务编排等模块；结合区块链、AI、大数据等新技术，使安全架构向可信增强、自主防御、智能决策等方向演进。

## 参考文献：

[1] ETSI GS NFV-EVE 011-2018.Virtualised Network Function; Specification of the Classification of Cloud Native VNF implementations[S]. 2018.

[2] 王旭亮, 刘增义, 胡雅婕, 等. 基于NFV MANO的边缘计算多种智能化部署方案研究[J]. 电子技术应用, 2019, 45(10):

19-24, 28.
WANG X L, LIU Z Y, HU Y J, et al. Research of various intelligent multi-access edge computing deployment solutions based on NFV MAN Chinese Full Text[J]. Application of Electronic Technique, 2019, 45(10): 19-24, 28.

[3] ETSI GR NFV-REL 011-2020.Management and Orchestration; Report on NFV-MANO software modification[S]. 2020.

[4] 钱成功. 基于 SRv6 的服务功能链系统设计与实现[D]. 北京: 北京邮电大学, 2020.
QIAN C G. Design and implementation of service function chain system based on SRv6[D]. Beijing: Beijing University of Posts and Telecommunications, 2020.

[5] 徐玉伟, 赵宝康, 时向泉, 等. 容器化安全服务功能链低延迟优化编排研究[J]. 信息网络安全, 2020, 20(7): 11-18.
XU Y W, ZHAO B K, SHI X Q, et al. Low-latency optimal orchestration of containerized security service function Chain Chinese full text[J]. Netinfo Security, 2020, 20(7): 11-18.

[6] 刘国荣, 沈军, 白景鹏. 可定义的 6G 安全架构[J]. 移动通信, 2021, 45(4): 54-57.
LIU G R, SHEN J, BAI J P. A definable 6G security Architecture Chinese full text[J]. Mobile Communications, 2021, 45(4): 54-57.

[7] 张鉴, 唐洪玉, 侯云晓. 基于软件定义的 5G 网络安全能力架构[J]. 中兴通讯技术, 2019, 25(4): 25-29.
ZHANG J, TANG H Y, HOU Y X. Security capability architecture of software-defined 5G Network Chinese full text[J]. ZTE Technology Journal, 2019, 25(4): 25-29.

[8] 张华, 岳皓. 基于 SDN 的港口安全资源池建设[J]. 网络空间安全, 2020, 11(3): 39-43.
ZHANG H, YUE H. Construction of port security resource pool based on SDN Chinese Full Text[J]. Cyberspace Security, 2020, 11(3): 39-43.

[9] 李畅, 徐琪, 李光磊, 等. 基于服务功能链的多域安全服务按需适配方法[J]. 计算机工程与应用, 2018, 54(21): 56-64, 119.
LI C, XU Q, LI G L, et al. On-demand adaptation method for multi-domain security services based on service function chaining Chinese Full Text[J]. Computer Engineering and Applications, 2018, 54(21): 56-64, 119.

[10] 华彦裴. 智慧协同网络下基于流量感知的功能族群适配机制设计与实现[D]. 北京: 北京交通大学, 2020.
HUA Y P. Design and implementation of functional group adaptation mechanism based on traffic awareness in smart collaborative network[D]. Beijing: Beijing Jiaotong University, 2020.

[作者简介]

**全硕**（1991− ），男，中国电信股份有限公司研究院工程师，主要研究方向为云网融合、云计算与大数据和云网运营等。

**王旭亮**（1986− ），中国电信股份有限公司研究院高级工程师，主要研究方向为云网融合技术、云数据中心网络和边缘计算等。

**朱泽亚**（1995− ），男，中国电信股份有限公司研究院工程师，主要研究方向为云网融合技术、云网运营技术和大数据与云计算等。