面向云网融合的网络安全互操作

Network Security Interoperability Towards Cloud-Network Convergence

魏亮/WEI Liang，查选/ZHA Xuan，戴方芳/DAI Fangfang

（中国信息通信研究院，中国 北京 100191）
(China Academy of Information and Communications Technology, Beijing 100191, China)

DOI：10.12142/ZTETJ.202301003
网络出版地址：https://kns.cnki.net/kcms/detail/34.1228.TN.20230222.1751.008.html
网络出版日期：2023-02-23
收稿日期：2022-12-18

摘要：云网融合通过网络与云的主动适配、协同和融合，为数字化应用提供灵活部署的云网资源。分析了云网时代的主要安全挑战，认为网络安全互操作是云网融合安全发展的重要路径。基于网络安全互操作发展现状分析，从标准规范、能力验证、行业示范3方面指出了云网安全互操作的重点发展方向。

关键词：云网融合；网络安全；安全互操作

Abstract: Cloud-network convergence provides flexible deployment of cloud network resources for digital applications through active adaptation, collaboration, and integration of information network and cloud environment. The main security challenges faced by cloud-network convergence are analyzed, and the security interoperability is proposed as an important way for the cloud-network convergence security development. With the development status analysis of security interoperability, the future development directions of security interoperability are pointed out from the aspects of standards, capability verification and industry demonstration.

Keywords: cloud-network convergence; network security; security interoperability

在数字时代，云网融合的智能化数字基础设施建设，打通了经济社会发展的信息“大动脉”，为数字产业化和产业数字化发展注入新动能。全方位、全链条的数字化升级加速传统行业转型。围绕新生产要素的攻击风险日益突出，传统网络安全威胁与新型网络安全威胁相互交织，保障融合领域安全的能力需求不断提高。网络安全已成为全球各国面临的共同挑战。

自党的十八大以来，以习近平同志为核心的党中央高度重视网络安全，从发展中国特色社会主义、实现中华民族伟大复兴中国梦的战略高度，统筹发展和安全两个大局，系统部署和全面推进网络安全工作。习近平总书记在《关于〈中共中央关于制定国民经济和社会发展第十四个五年规划和二〇三五年远景目标的建议〉的说明》中指出，“安全是发展的前提，发展是安全的保障”。习近平总书记还指出，“过去分散独立的网络变得高度关联、相互依赖，网络安全的威胁来源和攻击手段不断变化，那种依靠几个安全设备和安全软件就想永保安全的想法已不合时宜，需要树立动态、综合的防护理念”。在数字化发展新阶段下，要深刻落实习近平总书记讲话精神，通过打造网络安全互操作新体系，深度融合各领域安全能力，打破割裂的、静态的、封闭的安全，打造一体的、动态的、开放的网络安全屏障，推动网络安全综合保障能力再上新台阶，为加快建设网络强国提供有力支撑。

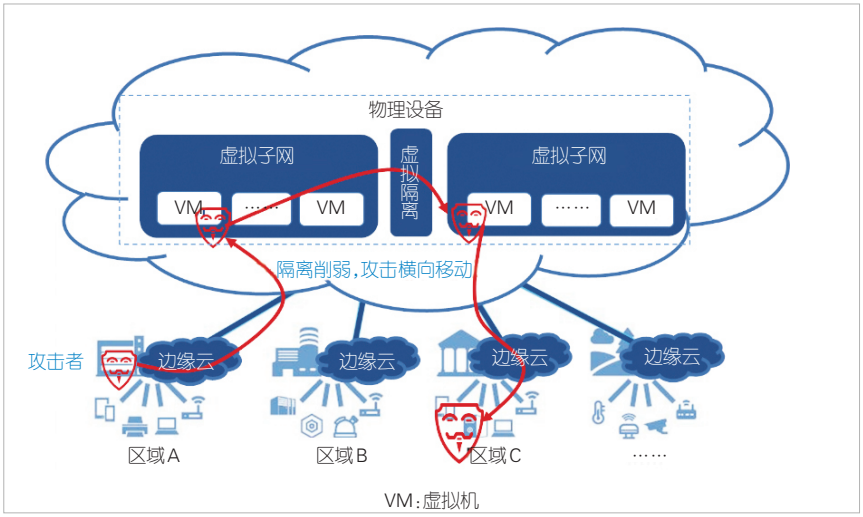
1 云网时代的安全新挑战

通过虚拟化、软件化、云化和人工智能（AI）等信息化技术，云网与通信技术深度融合。这将深刻变革信息基础设施的技术架构、业务形态和运营模式，有助于实现云网边端的智能互联、统一调度和智能化运维，打造新型信息基础设施底座[1-2]。与此同时，云网融合技术变革、融合应用、开放式生态新特性也引入了新的安全挑战[3]。

1）从技术变革看，虚拟化的架构给传统基于边界的防护带来挑战。

云网融合采用统一的虚拟化技术架构，将网络功能从硬件设备中分离，使网络架构从传统固态封闭向动态开放改变。网络的边界感和隔离感随之削弱。一方面，网络布局从传统的接入、汇聚、核心3层网络架构转向围绕数据中心的扁平部署，难以在分层架构的边界提供传统的物理安全隔离；另一方面，存储虚拟化、计算虚拟化、网络虚拟化打破设备单一物理机形态，通过池化的方式对外提供动态服务，不同业务可能共享相同的物理、计算、存储资源，传统的物理隔离保护在资源池内部失效。利用虚拟化网络架构下被削弱的网络隔离，威胁可在边界突破单点后向内扩散，引入内

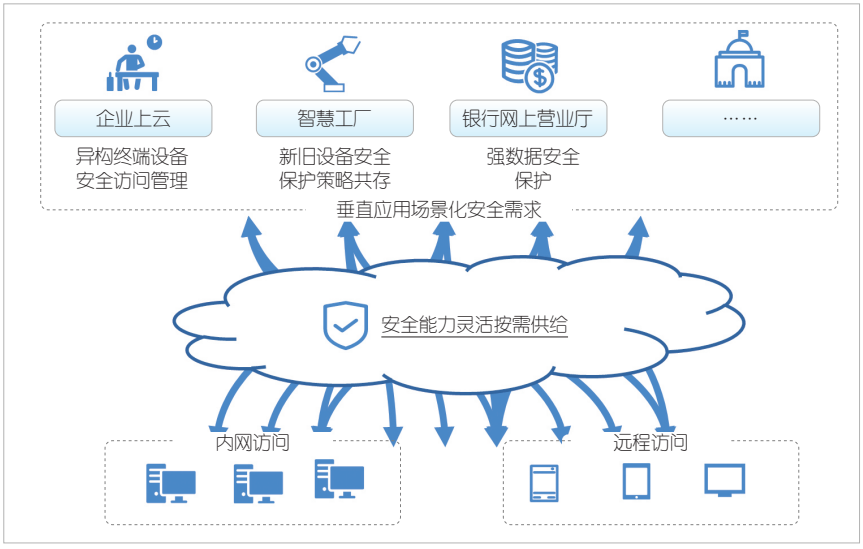
网横向移动攻击威胁，甚至潜藏或传播多处后形成攻击链，发动分布式拒绝服务（DDoS）、高级可持续威胁（APT）等更高级别的攻击，如图1所示。为应对攻击内部横向移动风险，需要从单点防御转向全网联防联动，实现全域安全能力的按需编排和弹性调度。



▲图1 虚拟化网络新架构引入攻击横向传播风险

2）从应用场景看，差异化的安全需求带来按需安全供给新挑战。

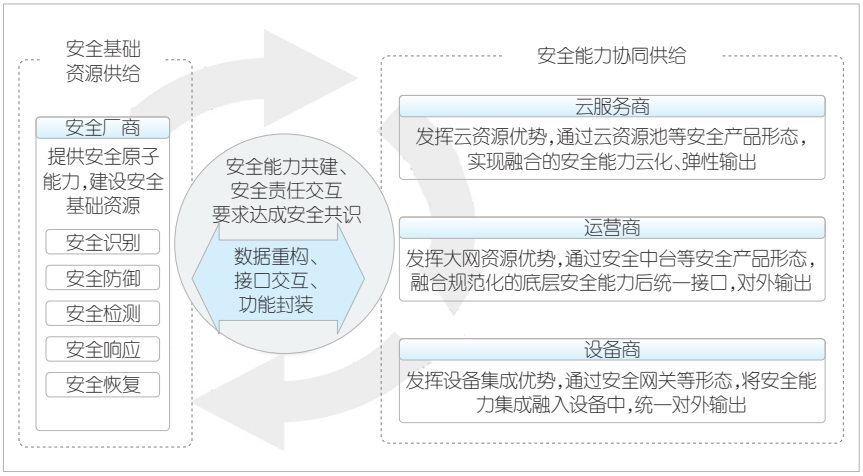
随着云网在数字化场景中的融合应用，云网上承载的垂直应用具有场景化安全需求。应用终端设备安全能力各异，组网架构更新迭代、周期各不相同，数据流量类型千差万别，网络性能要求高低不一，网络安全保障需求各不相同。垂直应用场景的差异化使安全特性从“通用安全”向“按需安全”转变，对安全能力的灵活性提出更高要求。例如：大型信息通信技术（ICT）企业上云存在多类不同终端异地安全接入的场景需求，要求基于身份与设备的分级别安全访问机制能够实现终端识别与安全防御，并具备对不同类终端的异常检测和响应能力，通过识别、防御、检测、响应能力联动实现对异构设备的全闭环安全管理，避免恶意终端对企业内部系统的破坏。智慧工厂中既有适用于早期封闭式生产环境的传统生产设备，又有新型的智能化生产设备。前者安全能力缺乏，需要部署外挂式安全设备来提供防御检测等安全能力，后者可与外部安全机制进行数据联动以实现安全保护。因此，我们需要多类不同的安全机制共存联动以满足新旧设备不同的安全需求。银行等金融系统对数据安全具有极高要求。银行有大量的分支机构和合作伙伴，要求基于业务、网络的分层分级逻辑隔离实现对数据的高效保护。如图2所示，为了满足不同应用场景差异化的安全需求，云网环境下的安全能力需要实现灵活编排重组，根据业务场景需求按需提供安全保障。



▲图2 满足差异化安全需求的安全能力

3）从产业生态看，纵向深度协同的新生态打开了云网安全协同新局面。

云网融合以运营商与云服务商主导的基础通信网络云化为核心，向下带动运营商与设备商开展云网一体硬件体系创新，向上为各类ICT数字化平台提供云网资源，推动产业生态融合发展。在云网上下协同产业的新生态下，安全角色也面临新变化，传统由安全厂商单一供给的状态发生变化，呈现出各方安全共建的网络安全协同新局面，如图3所示。安全厂商作为网络安全基础能力的建设者，由上至下提供安全能力供给；运营商与云服务商利用云网基础资源优势与入口优势，将安全厂商的成熟安全能力进行融合重组后赋能产业界。例如：运营商、云服务商等与安全厂商优势互补，合作推动安全访问服务边缘（SASE）等基于云网的安全能力供给服务，或在云网环境中融合抗DDoS、流量清洗等安全能力，通过安全即服务的方式，对外提供可按需订购的网络攻击防护服务；下游的设备商在云网融合硬件创新过程中，将安全能力封装在设备中，如通过安全网关等在硬件设备中融入安全能力。在各参与方深度参与云网安全的规划、建设和运营的过程中，安全责任界面需要各方共同构建。这不仅涉及安全厂商在供给安全原子能力时的安全责任，还涉及数据重构、接口调用、功能封装等环节引入的新安全责任，因此需



▲图3 云网安全协同新局面

要各参与主体在网络安全能力共建的不同环节（规划、建设、运营、使用等）达成共识，共担安全保护职责。

面对云网时代下的威胁横向移动风险、按需安全能力供给新要求以及云网安全协同新生态，单一的安全能力、单一的安全相关方无法适应云网融合新安全态势。技术发展、垂直应用以及产业生态3个层面都要求安全能力之间实现融合协同。打通网络安全能力间的互操作通道，可实现全域安全能力联动、安全能力灵活编排、安全能力高效集成。

2 网络安全互操作发展现状

2.1 标准化现状

1）国际标准化工作起步较早，多维度推动规范实践。

其他国家对安全互操作研究已久，政产学研高度协同：既有美国国土安全部（DHS）、美国国家安全局（NSA）等诸多国家部门引导，又有IBM、思科、戴尔、McAfee、Fortinet、Mandiant等各领域头部企业发力推进，同时还有国际电信联盟（ITU）、国际互联网工程任务组（IETF）等国际标准化组织推进标准规范研制。它们共同从安全协同顶层模型、基础类规范、语义类规范、接口类规范、数据类规范等诸多维度，推动安全互操作的研究应用[4]，如表1所示。

a）顶层模型。2014年，DHS、NSA等联合提出集成自适应网络防御框架（IACD），从顶层定义了安全协同参考架构、互操作规范草案、用例和实施案例，通过将安全产品抽象为“感觉–理解–决策–行动”工作流，共享威胁情报、编排协调响应和行动，实现采集、分析、决策、执行、恢复、信息共享的全自动化，提高了响应处理效率。根据金融服务信息共享和分析中心（FS–ISAC）的统计，基于IACD的系统将调查和响应事件的时间从11 h缩减至10 min，有效提高了安全效能。IACD已形成由FireEye、Splunks、Microsoft、VMware等主流安全厂商、机构、系统和产品构成的生态体系，被试用于美国FS–ISAC和美国能源部等多个部门。

b）基础类规范。安全能力作为安全互操作的基础元素，定义了为抵抗安全攻击所提供的能力。ITU–T、IETF等国际

▼表1 安全互操作国际标准化及应用情况

互操作层面		项目名称	提出年份	主导及参与方	应用情况
顶层模型		IACD	2014	DHS、NSA、约翰·霍普金斯大学应用物理实验室	试用于美国金融和能源等行业政府部门
基础规范		安全能力定义	2022	ITU–T SG17	—
		I2NSF工作组	2014	IETF	—
语义规范		OpenC2	2017	NSA、美国银行和奥斯陆大学等	多用于美国军方，未实现大规模商业应用
接口规范	威胁情报	TAXII	2012	DHS、OASIS网络威胁情报技术委员、MITRE等	被DHS、IBM、微软、惠普、思科、戴尔及大型金融机构等广泛应用
	通用安全	OpenDXL、OpenDXL Ontology	2016、2020	IBM、McAfee、Fortinet等	至2020年，OpenDXL已被4 000多个组织使用
数据规范		STIX	2012	DHS、OASIS网络威胁情报技术委员、MITRE、CTIN等	被DHS、IBM、微软、惠普、思科、戴尔及大型金融机构等广泛应用
		OpenIOC	2011	Mandiant	在威胁情报中心及相关产品有广泛应用，如启明星辰、安天等威胁情报中心，CounterCraft网络欺骗平台等

DHS：美国国土安全部
I2NSF：网络安全功能接口
IACD：集成自适应网络防御框架
IETF：国际互联网工程任务组
ITU–T SG17：国际电联安全研究组
NSA：美国国家安全局
OASIS：结构化信息标准促进组织
OpenIOC：开放威胁指标
OpenDXL：开放数据交换层
STIX：结构化威胁信息表达
TAXII：情报信息自动化交换

标准化组织启动了安全能力相关的标准化研究。2022年5月，ITU-T安全研究组SG17启动国际标准《X.secadef：安全能力定义》的制定，旨在为信息系统、网络、应用程序生命周期的每个阶段定义一组通用的安全能力。2014年，IETF成立网络安全功能接口（I2NSF）工作组，旨在通过提供架构、软件接口规范和数据模型，实现对物理和虚拟的网络安全能力的统一监控和管理。目前IETF已形成3个请求评论（RFC）、10余个工作组草案，包括《RFC8329: Framework for Interface to Network Security Functions》《RFC8129: Interface to Network Security Functions (I2NSF): Problem Statement and Use Cases》《RFC9061: A YANG Data Model for IPsec Flow Protection Based on Software-Defined Networking (SDN)》等。

c）语义类规范。2017年，NSA牵头形成了网络防御互操作性规范OpenC2，并制定了配套语言结构、配置文件、传输协议相关规范，通过将防火墙、沙箱等安全防御响应类产品间的交互抽象为“动作—目标”类标准化编排语言，以实现不同厂家和不同编程语言的安全产品间的自动化联动。受到各方保护自身威胁情报、漏洞库等安全信息商业价值的影响，OpenC2尚未实现大规模商业应用。中国奇安信、绿盟、启明星辰等在各自安全编排自动化与响应（SOAR）平台上提供相应适配和支持。

d）接口类规范。安全互操作接口类规范较为成熟，包括典型的情报信息自动化交换（TAXII）、开放数据交换层（OpenDXL）、OpenDXL Ontology等。基于指标信息的可信自动化交换TAXII是威胁信息共享领域的典型接口规范。该规范定义了网络威胁情报共享的协议、服务和信息格式，得到了美国国防部（DoD）、NSA等国家机构及IBM、思科、戴尔等的支持，具有成熟且广泛的应用。OpenDXL与OpenDXL Ontology是基于开源思路的通用型安全互操作接口通信类标准。2016年，McAfee发布了开源工具OpenDXL。OpenDXL通过提供软件开发工具包（SDK）来创建或连接基于数据交换层（DXL）的应用程序，协调不同供应商应用程序间的数据和操作，完成安全情报共享。截至2020年，OpenDXL已被4 000多个组织使用。2020年，在OpenDXL的基础上，由IBM、McAfee、Fortinet等联合成立的开放网络安全联盟（OCA）发布了开源的消息传递框架OpenDXL Ontology。该框架结合了OpenC2与结构化威胁信息表达（STIX）等通用消息内容开放标准，进一步定义了安全互操作消息格式。

e）数据类规范。典型的安全互操作数据类规范包括STIX、开放威胁指标（OpenIOC）等。STIX为威胁分析、威胁情报交换、检测和响应等安全行为提供描述威胁信息的语言和序列化格式，包括对威胁对象、威胁活动、威胁属性等威胁情报的多方面特征，被DHS、IBM、微软、惠普、思科、戴尔及大型金融机构等广泛使用。OpenIOC是Mandiant公司发布的情报共享规范。通过建立威胁指标（IOC）的逻辑分组，OpenIOC以可扩展标记语言（XML）文档类型描述捕获多种威胁的事件响应信息，包括病毒文件的属性、注册表改变的特征、虚拟内存等，在机器中以可读的格式进行通信，从而实现威胁情报的交流共享。该规范在威胁情报中心及相关产品中得到广泛支持。

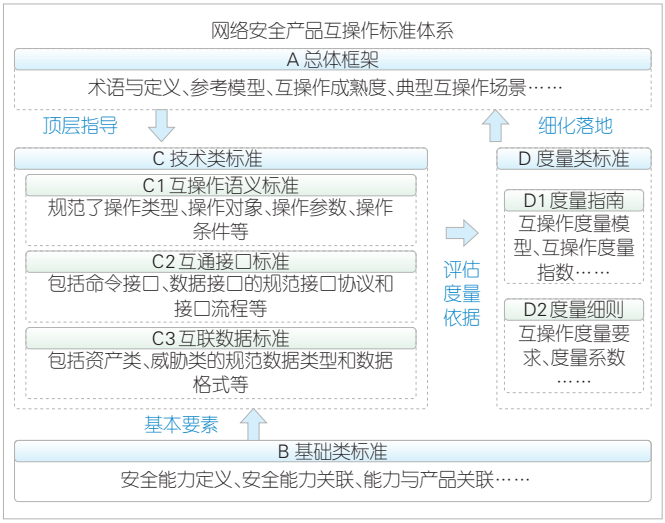
2）中国标准化工作发展不均衡，体系化标准建设迫在眉睫。

中国标准化工作起步较晚，各领域发展不均衡的特征较为明显。其中，整体框架和标准路线图研究初现成效，威胁领域互操作的数据规范化程度较高。安全日志、恶意程序等部分领域的网络安全互操作也形成了相关接口规范，但缺乏语义领域标准规范研究。

a）顶层框架。2022年3月，全国信息安全标准化技术委员会（TC260）发布网络安全国家标准需求，从国家标准层面提出网络安全产品互联互通框架、接口和数据格式等方面的标准制定的急迫性。2022年9月CCSA TC8 WG1（中国通信标准化协会工作组）结项的行业标准研究课题2022B72《网络安全产品互操作标准体系研究》，是中国首个通用的网络安全互操作标准项目。该项目解答了网络安全产品互操作发展现状、术语定义、参考模型、标准体系、标准路线等关键问题，为系统推动网络安全互操作系列标准研制提供顶层指导，如图4所示。2022年9月，CCSA TC8 WG1新立项的行业标准《网络安全产品互操作 第1部分：总体框架》，是安全产品互操作系列标准的首部标准，这标志着中国正式启动网络安全互操作标准体系化研制。

b）接口类规范。中国已在安全日志、恶意程序样本等信息互通方面发布了接口行业规范，如YD/T 3496-2019《Web安全日志格式及共享接口规范》、YD/T 2849-2015《移动互联网恶意程序疑似样本报送接口规范》等，定义了接口的名称、协议、流程、字段等信息。此外，中国通信标准化协会（CCSA）还启动了SOAR、SASE、安全中台等新安全技术产品与其他类安全功能间的接口规范化研制，使新技术在应用落地之初便具备与其他安全能力进行接口层面互操作的能力。

c）数据类规范。中国在网络安全互操作数据共享领域的标准化起步较早，已面向威胁情报、WEB漏洞、终端漏洞、源代码漏洞等形成了国家标准和行业标准，为安全产品间交互共享各类漏洞威胁信息提供了规范化格式。相关标准



▲图4 网络安全产品互操作标准体系结构图[4]

包括GB/T 28458–2012《信息安全技术 安全漏洞标识与描述规范》、GB/T 36643–2018《信息安全技术 网络安全威胁信息格式规范》、YD/T 3448–2019《联网软件源代码漏洞分类及等级划分规范》、YD/T 3667–2020《移动智能终端漏洞标识格式要求》、YD/T 3955–2021《WEB漏洞分类与定义指南》等。

2.2 行业应用现状

运营商、云服务商、安全厂商、设备商等发挥各自优势，以云安全资源池、安全中台、安全访问服务边缘等新网络安全产品为服务对象，打通网络安全能力互操作通道，向下对底层安全识别、分析、检测、响应等安全能力进行统一规范、编排、集成，向上通过云化方式、规范化接口等为上方数字化应用提供灵活、按需的安全能力，实现上层数字化应用需求与下层网络安全产品能力供给按需对接，如图5所示。

在云网环境下，运营商依托大网资源优势，通过实现多个安全厂商的抗DDoS安全产品互操作，以安全即服务等方式，为客户提供可定制、防护能力秒级生效、超大防护流量的抗DDoS服务。我们以此为例进行详细说明。

1）部署位置。运营商在城域网出口、IDC边界、骨干网络等重要位置部署多个安全厂商的抗DDoS检测设备和抗DDoS流量清洗设备，并集中部署抗DDoS管理平台，以管理全网抗DDoS检测设备和抗DDoS流量清洗设备。

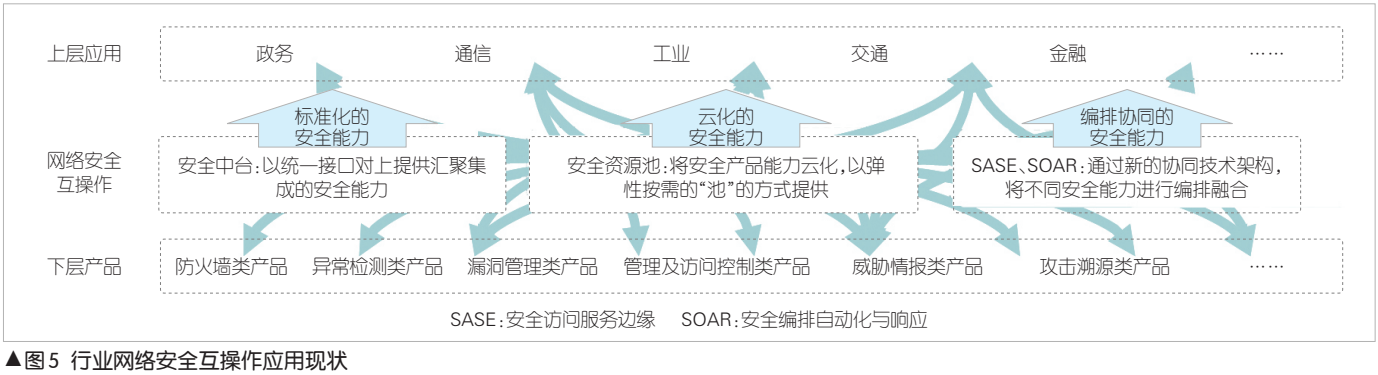
2）互操作过程。运营商统一规范各安全厂商的抗DDoS检测设备和流量清洗设备的DDoS攻击类型、异常流量信息、清洗策略等相关数据定义，并统一各安全厂商抗DDoS设备与平台间的接口，实现抗DDoS检测设备、流量清洗设备以及管理平台间的互操作，如图6所示。具体协同运作流程如下：

a）抗DDoS检测设备将检测出的异常流量信息上报给抗DDoS管理平台。上报信息包含异常流量攻击类型、异常流量攻击目标、异常流量五元组信息等。抗DDoS管理平台基于汇聚的异常流量信息，可形成对异常流量更加精准的判断，依此形成更精准的流量清洗策略。

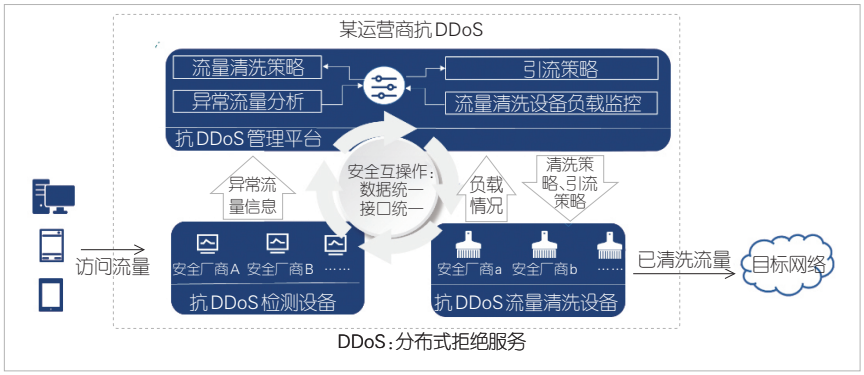
b）抗DDoS管理平台可监控抗DDoS流量清洗设备负载情况。根据汇聚的异常流量信息与抗DDoS流量清洗设备负载情况，遵循近源、流量均衡的原则，抗DDoS管理平台制定引流策略和流量清洗策略，并下发给相应的抗DDoS流量清洗设备，即引流至近源的抗DDoS流量清洗中心进行引流清洗，或在异常流量带宽过高时将流量牵引至多个抗DDoS流量清洗中心进行分级引流清洗，以此提升抗DDoS效能。

3 未来工作展望

网络安全互操作是云网时代下打造高效、灵活、全方位安全能力的技术基石。为实现高质量发展和高水平安全的良性互动，提升网络安全互操作实力，中国政府需发动产学研各界力量，开展标准规范、能力验证、行业示范3个方面工作。



▲图5 行业网络安全互操作应用现状



▲图6 抗DDoS网络安全互操作示例

1）规范先行，推动标准体系化建设。体系化的标准规范是推动网络安全互操作实践的前提。中国需要加快网络安全互操作标准体系化建设，梳理现有国家和行业标准，遵循急用先行、基础先行的原则，加快重点空白领域的网络安全互操作标准研究，如基础标准、语义类标准、评估类标准；鼓励运营商、云服务商、安全厂商、设备厂商等共同参与标准的研制与落地验证，确保标准的可操作性；推动在国际标准组织中牵头或参与网络安全互操作相关标准的立项研制，争取网络安全互操作领域的国际标准话语权。

2）能力验证，以实效评估推动能力提升。面向典型网络安全互操作场景、新型协同技术平台、典型安全产品等开展网络安全互操作评估验证，中国需要了解网络安全产业界的网络安全互操作现状，梳理网络安全互操作的优势领域与短板领域，形成未来网络安全互操作实践重点突破方向；推动网络安全互操作实验测试床建设，打造网络安全互操作能力验证硬能力，突破“现网级”安全实效验证。

3）打造标杆，遴选示范案例引领行业实践。依托网络安全试点示范等工作，遴选行业网络安全互操作优秀案例，打造单类网络安全产品、网络安全互操作平台类等不同类型的示范标杆，为威胁共享、身份验证、策略编排、运营管理等典型网络安全互操作场景下的互操作实践提供参考模板；通过网络安全互操作案例集等方式，引领行业开展网络安全互操作实践。

4 结束语

云网融合为数字化发展提供高性能网络连接、海量数据存储与多形态计算能力。为进一步夯实数字化中国发展的安全基础，本文从云网融合技术变革、融合应用、开放式生态3个方面梳理了安全新挑战，指出打通网络安全互操作通道是实现全域安全能力高效联动、提供灵活按需协同的安全能力的关键所在，可有效应对云网时代安全新挑战。未来，网络安全产业各方应携手并进，通过标准建设、能力验证、示范引领3个方面的工作，提升中国网络安全互操作水平，为云网时代打造扎实的安全基石。

参考文献

[1] DUAN Q, WANG S G, ANSARI N. Convergence of networking and cloud/edge computing: status, challenges, and opportunities [J]. IEEE network, 2020, 34(6): 148–155. DOI: 10.1109/MNET.011.2000089
[2] 柯瑞文. 立足科技自立自强全面推进云网融合 [J]. 人民论坛, 2021(36): 6–8. DOI: 10.3969/j.issn.1004–3381.2021.36.001
[3] 张鉴, 唐洪玉, 刘文韬, 等. 面向云网融合的电信网安全防护体系参考架构 [J]. 电信科学, 2020, 36(5): 10–15. DOI: 10.11959/j.issn.1000–0801.2020140
[4] CCSA. 网络安全产品互操作标准体系研究: 2022B72 [S]. 2022

作　者　简　介

魏亮，中国信息通信研究院副院长、ITU-T SG17副主席，教授级高级工程师；研究领域包括下一代电信网、网络架构、网络与信息安全等。

查选，中国信息通信研究院安全研究所高级工程师；研究领域包括无线网络安全、区块链安全等。

戴方芳，中国信息通信研究院安全研究所网络安全研究部副主任、ITU-T SG17 Q8报告人、CCSA TC8 WG1副组长、高级工程师；研究领域包括5G网络安全、云计算网络安全等。