云数据中心网络安全的新挑战

李 军 王 翔
清华大学

李 军 清华大学教授，博士生导师，信息技术研究院院长，清华信息科学与技术国家实验室常务副主任。主要从事网络安全、模式识别和图像处理领域的科研和教学工作。先后参加过CAFIS（中国指纹自动识别系统）、M-WIP（多波长红外二维测温系统）、10Gbps UTM（万兆统一威胁管理系统）等科研项目。曾主持模块化线速安全网关的研制，带动了统一威胁管理安全网关产品的形成和发展。著译教材3部，发表学术论文近百篇，获得美国专利1项，中国发明专利十余项，并担任中国电子学会计算机工程与应用分会副主任、工信部电子科技委委员等学术职务。

云计算技术极大地提高了IT资源的交付能力，是信息产业变革之路上的下一个制高点。数据中心为云计算的落地提供了强有力的支撑，而云数据中心网络安全问题已经成为当前影响企业对云计算接受程度的最重要因素之一，也直接影响着云计算未来的发展走势。

那么，云计算模式下的数据中心网络究竟与传统数据中心网络有何异同？这些变化对数据中心网络安全带来何种挑战？我们又应当如何应对这些挑战？

一、云数据中心网络变革

云计算的发展催化了数据中心的变革。传统的数据中心大多只是提供机房空间或计算设备的租用，即使提供增值服务，租户使用的物理资源也是独占的。云数据中心中的各种资源则往往采用了相应的虚拟化技术，以“按需申请，按用付费”的租用方式实现给租户的资源交付。

为了实现灵活有效的资源交付方式，在虚拟化的云数据中心中，租户的网络应用不再是直接运行在实际的物理网络之上，而是由云提供商按照多租用的需求，在物理网络之上通过虚拟化抽象出一层逻辑网络，根据不同租户的需求为其分配不同数量及拓扑的虚拟网络。该虚拟网络拓扑是租户业务处理和应用运行所依托的网络环境，一旦部署之后不会频繁进行变更。图1显示了在云数据中心中部署的两个不同租户的虚拟网络。租户1和租户2

分别构建了两个和一个虚拟二层网络，其中虚拟二层网络的行为等同于普通以太网的转发行为。虽然两个租户的虚拟机都接入到同一数据中心物理网络中，但由于网络虚拟化的存在，两个租户的流量以及租户1的两个虚拟二层网络的流量（除非经过三层网关）是完全相互隔离、互不可见的。为了保证数据中心资源的充分利用，云提供商会根据运维需要调整承载业务和应用的虚拟机资源，使得虚拟机处于不断的动态迁移中，而数据中心中的网络流量也会随之进行动态的导引。因此，虚拟网络拓扑到物理网络拓扑的映射处于不断的变化过程中，原来静态、自然的网络物理边界被动态、虚拟的逻辑边界所替代。

与此同时，数据中心网络的层级结构也随着云计算的到来，而悄然发生变化。在传统数据中心中，为网络提供业务增强服务的各种中间设备，例如防火墙、入侵检测与防御、负载均衡等，往往通过位于核心层与接入层之间的汇聚层接入到数据中心网络中，并且直接部署于数据中心南北流量所流经的关键路径上。而云数据中心的运营方式，促使网络扁平化构建，数据中心网络中东西向的流量可能大大超过南北向的流量。为了适应网络流量特性的变化，各种中间设备与提供计算、存储等服务的硬件资源一起部署在数据中心网络的边界处，并统一通过接入层接入到数据中心网络中。图2对比了上述传统数据中心与云数据中心网络层次结构与节点拓扑上的差异。

二、云数据中心网络安全挑战

对比企业内网与云数据中心网络的异同，则不难看出：网管人员对网络安全的要求依旧是可以通过灵活定制的策略，实现自身网络（可信网络或称内部网络）的内部互联（可简称云内网络）、自身网络与公共网络（非可信网络或称外部网络）的安全连接（可简称云端网络）、自身网络处于不同物理位置（甚至跨数据中心）的可信网段之间通过公有网络的安全连接（可简称云间网

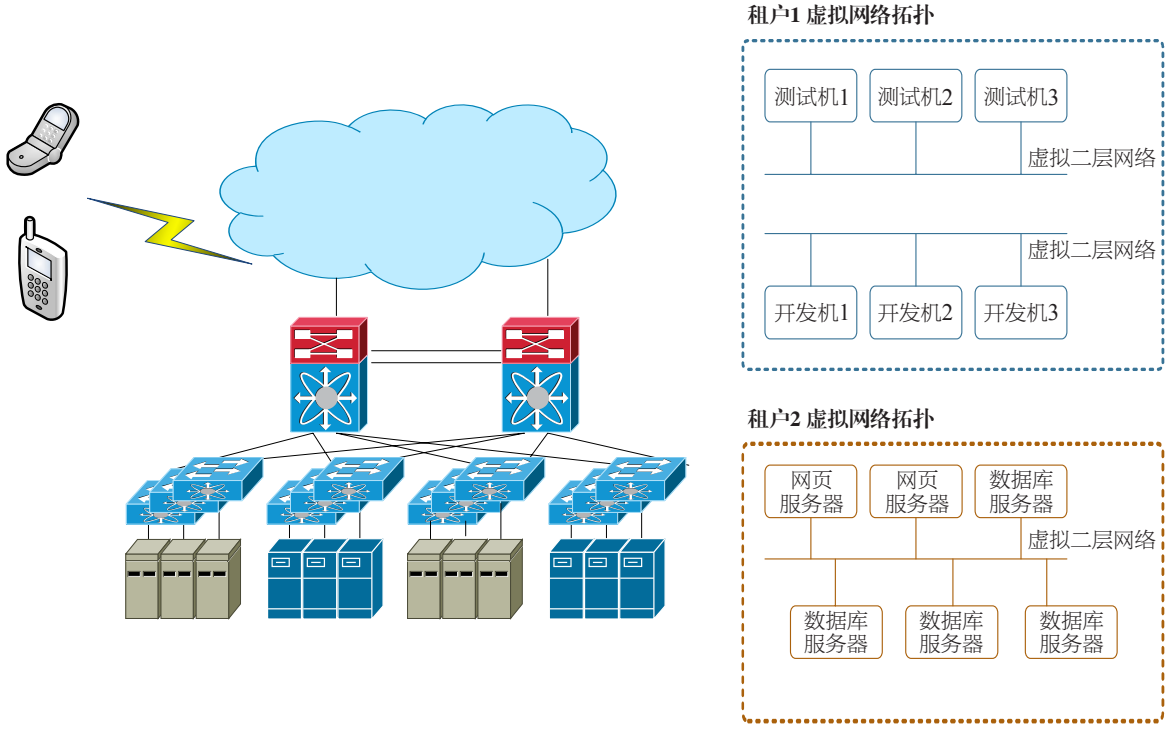

图1 云数据中心的多租用虚拟网络

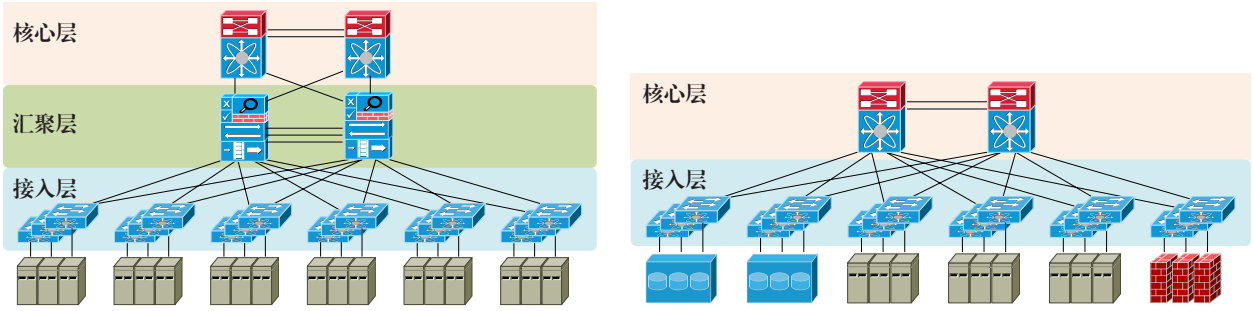

图2 传统数据中心与云数据中心网络拓扑对比

络），以及网络流量的安全处理。云数据中心网络虚拟化带来的网络边界动态性，使得数据中心网络特别是云内网络安全的保障将更加依赖于安全策略和安全构件的动态部署、配置和管理，更加依赖于网络安全系统对流量和业务的感知、决策与响应。

具体来说，云数据中心网络安全主要面临以下几个挑战：

（一）虚拟网络环境中安全策略的全局协同及动态映射

虚拟网络环境下的策略机制与单纯物理网络中的不同。

首先，虚拟网络策略的定义需要从多租用环境的拓扑结构出发，以所面向的具体应用为目标，在区分不同安全域的基础上，抽象安全策略的描述方式，简化安全策略的制定。

其次，针对云计算不同应用场景需要不同云安全策略的特点，安全策略的制订采用层次化、模块化的实现机制，一方面租户为自有业务所定制的安全策略必须与全网的安全策略协同；另一方面不同应用的安全策略之间必须协同，避免安全策略冲突（不一致）的情况。

再次，由于多台物理服务器上的虚拟机为提高资源利用不断地动态迁移，在虚拟网络拓扑不变的情况下，必须将基于逻辑拓扑定义的安全策略根据虚拟机的迁移状况，动态地、实时地映射到实际的物理设备和安全设备上，避免安全策略的实施在拓扑的动态变化过程中产生空窗期。

（二）虚拟网络环境中安全能力的高效实现和统一管理

在虚拟化的云数据中心中，安全能力目前大多以专有硬件的方式直接部署在数据中心的网络中。然而，虚拟化云数据中心的大规模、多租用的特点，使得传统的单点高性能硬件安全设备很难满足安全监测的需求。安全能力需要根据复杂多变的功能组合以及应用需求的差异，灵活地部署在实际网络中不同的层级和节点上。在图3所示的部署方式中，对于无流量状态的网包过滤（packet filtering）等简单访问控制策略，可分散在交换机上实施；而对于状态监测（stateful inspection）以及基于内容的深度监测（deep inspection）等网流安全监控，则需要由专有的硬件设备来保证性能。

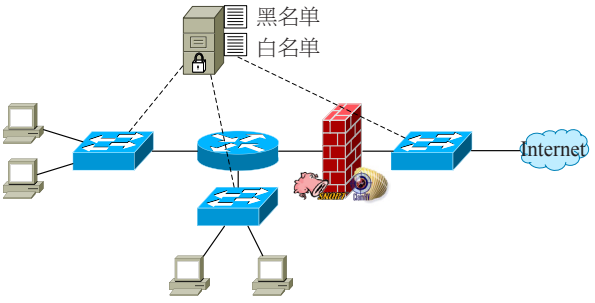

图3 云数据中心安全机制的实施节点

同时，面向多租户以及一个租户具有多个安全域的情况，需要将一个高端硬件防火墙根据各

个租户或安全域不同的功能和性能要求虚拟成多个逻辑防火墙，即所谓“一虚多”，各自执行相应的安全策略。而当安全监控能力不够时，需要使用“多虚一”的手段，将多个安全设备通过负载均衡或协同工作组成集群系统，提高整体的处理性能。图4显示了按照不同应用需求将防火墙进行“一虚多”，以及入侵检测设备的“多虚一”的能力聚合方式。

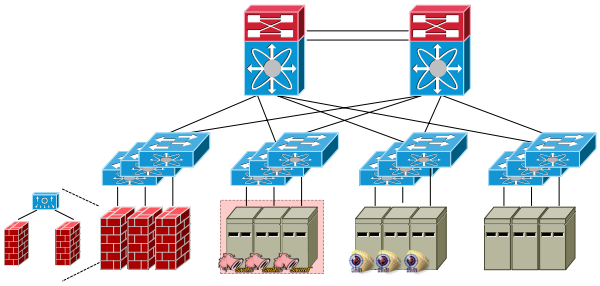

图4 云数据中心安全设备处理能力的聚合

除此之外，为了实现对同一网流的多项检测，传统上往往是将不同类型的安全设备或功能简单地加以堆叠。由于大多数设备对流量检测的前期处理相同或相似（如网包捕获、协议解析、状态维护和网流重组等），简单的堆叠导致硬件资源及能耗的浪费。安全设备提供商在设备管理模型和管理接口上的差异限制了安全资源的集中统一运维。这些都与云计算的节能和自动化管理的初衷相违背。

（三）虚拟网络环境中安全架构的分布式扩展

云数据中心分批建设、异地灾备、跨站点高速互联等内在需求，导致必须以物理上分布的形式实现对安全策略和安全能力逻辑上的集中管理和控制。首先，为同时满足云提供商和租户在云资源使用上不同的需求，需要对安全资源的分配、调度和控制予以全局优化；其次，为了降低流量监控对云数据中心网络的性能压力，提升安全服务的整体性能，需要根据安全资源的分布对流量进行负载均衡和智能调度；再次，由于数据中心庞大的规模、分批的部署方式、多站点和灾备等多方面需求，逻辑上全局集中的控制必须以分布式的形式实施，并且需要根据不同的应用场景，在数据的一致性、可用性和分区容错性三者之间做出相应的权衡。

三、云数据中心网络安全技术的核心——软件定义网络

软件定义网络（Software Defined Networking, SDN）概念由斯坦福大学和加州伯克利大学的学者提出，并很快为工业界所接受。图5显示了SDN的架构框图。SDN提出了网络控制平面与数据平面相解耦的架构，将控制平面的功能及数据统一抽取出来，形成全局网络拓扑并由逻辑上集中的控制器所管控。控制器根据当前网络状态与策略要求，确定所有转发节点的流表（flow table），并通过以OpenFlow等协议开放的转发设备流表控制接口下发到对应的物理交换机上。由此可以看出，SDN通过构建具有全局知识的控制平面，给予网络管理人员前所未有的控制能力，也使得更加智能的自动化网管成为可能。SDN技术本身源于企业内网中访问控制的网络安全应用背景，并在解决私有云数据中心网络的流量工程（traffic engineering）与公有云数据中心的多租用虚拟

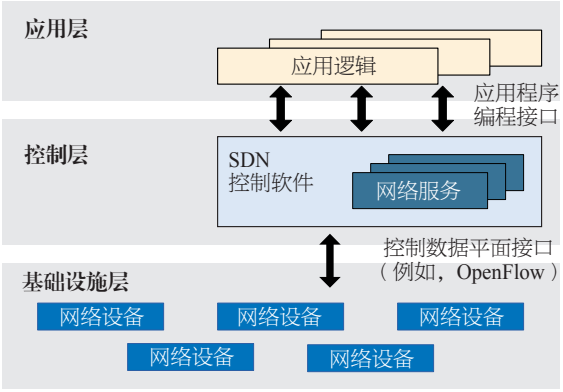

图5 SDN架构框图

网络等背景下进一步发展成熟。

针对云数据中心虚拟化、多租用及大规模所带来的安全边界模糊化、安全机制动态化、大规模资源管控集中化的问题，基于SDN技术，可以重新定义虚拟网络环境下安全策略和边界。通过SDN技术中网络控制器提供的全局网络视图和对网络设备的可编程控制，根据网流对应的终端节点在数据中心内部网络拓扑中的位置，动态调整交换设备上的转发流表和安全设备上的策略映射，并借助虚拟化技术优化安全设备的接入方式，将网流导入到分布式的安全设备中进行处理，并根据检测结果对网络中的非法流量进行实时阻断。同时，扩展网络控制器所管理的节点类型，使安全设备成为网络中的服务元素，将安全设备与云数据中心的其他资源一样，视为一种服务，在全网范围内进行资源的优化配备和调度。抽象不同种类安全设备的控制接口，构建同构的安全设备管理框架；将分布式安全能力经过量化，构造成逻辑资源池，从而使安全的形态成为另一种SaaS（Security as a Service，安全即服务）。

具体来说，基于SDN的云数据中心网络安全有以下几个关键点：

（一）多目标安全策略的制订与分发

安全策略通常是租户根据应用的安全等级及虚拟网络拓扑确定的，传统上并不考虑物理网络状态；而网络设备的处理规则往往仅考虑了在特定拓扑上的转发，而很少考虑安全的需求。在云数据中心网络的应用场景中，既要简化安全策略定义与实施，又需要达到与转发功能的协同。在图5所示的策略分发过程中，基于SDN控制平面提供的网络状态信息，控制器将转发策略与安全策略联合编译，并根据所需求的资源量与资源类型，分发到网络中的不同节点上。

因此，一方面需要针对不同应用的安全需求，设计适合该类应用的安全策略描述方式。这种描述方式仅和所使用的应用场景相关，属于上层应用级

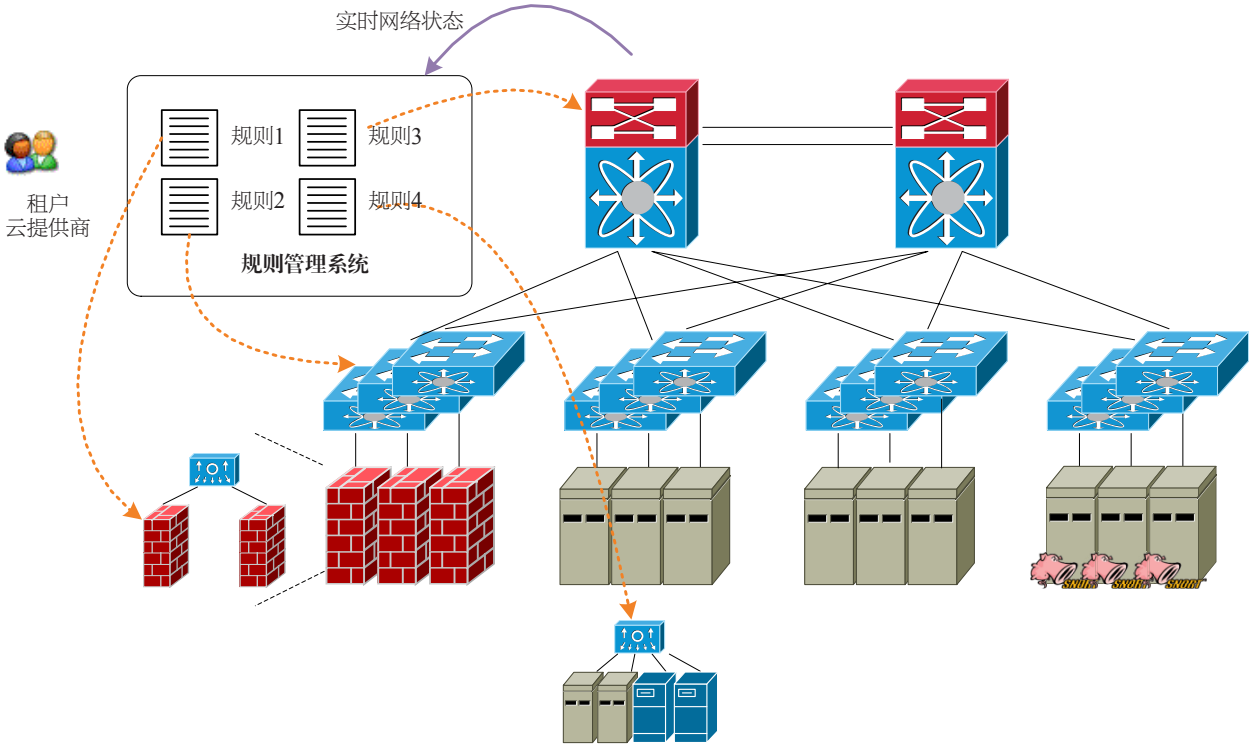

图6　转发策略与安全策略的协同部署

别的抽象定义，不涉及实现该策略所要求底层硬件支持的规则格式。这样的设计一来可降低租户安全资源管理的复杂度，减少运维费用的支出；再者可将安全策略的制订与安全策略的实施相隔离，既赋予租户宽松的安全策略制订方式，又可以通过策略映射灵活调整策略的实施方式。

另一方面，由于云数据中心网络的大规模和动态性，规则的部署方式及更新机制也是多目标安全策略实施的关键点。计算量小、动态性强、无状态、依赖全局网络视图的规则既可部署在网络的控制平面上，也可部署在网络的数据平面上，而计算量大、依赖网流状态信息的规则必须部署在网络的数据平面上。对于更新频繁、规模大、应用实时性强的规则，可在研究策略编译的过程中考虑引入动态增量更新算法；同时，在更新的过程中，需要尽可能地保证整个更新过程及所依赖的数据结构无锁，以免影响系统的整体处理性能。

（二）可重构复用的安全设备架构及抽象交互接口

将安全设备的软件功能与所依赖的硬件资源解耦，抽象并封装不同安全设备中对网包处理的软件功能模块，构建不同安全能力的逻辑处理框架。框架重构完毕后，提取并合并其中公共的处理模块，软硬件联合优化其中的性能关键点，统一网包处理的输入输出接口，为上层的安全处理提供可复用的、高性能的基础支撑；上层的安全处理模块基于统一定义的输入输出接口对网包进行处理，并可通过流水线的方式进行功能的组合拼接，实现不同监控功能的高效动态组合。

借鉴OpenFlow的标准和SDN的思想，提出不同类型安全能力的标准控制模型与接口，消除各种类型安全设备不同提供商之间的差异。定义安全资源与软件定义网络控制器之间的通用交互规范，其中包括网络参数的交互、安全策略的下发、安全事件的反馈、流量状态的反馈等。在此基础上搭建网络安全能力的集中管控平台，实现安全资源和功能的可编程性。

（三）安全资源的全局优化方法与高效流量调度

利用数据中心网络的全局特性，以网络为资源优化分配和调度的中心。通过将所有类型的资源视为网络端口上的属性，基于SDN控制平面提供的全局网络视图，以端口为粒度对资源进行精细化的调配和控制。

在单个监控节点上，按照不同安全功能对硬件资源需求的差异，分配最适合其实现的资源类型，实现单个节点上负载均衡和资源优化配置；在全网范围内，按照虚拟网络拓扑与物理网络拓扑之间的映射、物理服务器的负载情况以及流量的分布模型，选择最适合安全设备接入的位置，实现全网范围上资源的统筹。

此外，随着云数据中心承载业务的不断扩大，越来越多的设备需要加入到云管理平台中进行管理；同时，由于设备的升级和更新换代，新旧设备分散在数据中心机房中，造成处理能力的分布不均；再者，多个数据中心之间的业务交互以及灾备等需求，都需要借助SDN提供的全局网络视图来完成。

云计算的发展给数据中心网络安全带来了新的挑战，而软件定义网络技术的出现无疑是解决大规模、动态网络拓扑下安全问题的强有力手段之一。

然而，SDN仅仅开放了网络2~3层的可编程性，对于安全处理所依赖的网络4~7层并未提供易于编程控制的抽象。正因为如此，SDN需要通过流量牵引来协调虚拟网络与安全设备，但是不可避免地对数据中心核心网络带来了额外的带宽开销。伴随着数据中心所有资源虚拟化的进程逐步加快，安全设备的虚拟化和开放接口必将为云数据中心网络安全服务的提供带来更多的便利。而软件定义网络中“软件定义”的核心思想，必将为云数据中心网络安全问题的最终解决提供方向性的指引。END