www.secdoctor.com《安全周报》2012 年 11 月第 2 期

# “软件定义网络”的安全

李军　清华大学信息技术研究院

2012 年 4 月开放网络峰会（Open Network Summit,即 ONS）以来，软件定义网络(Software-Defined Networking，即 SDN)迅速窜红，终于真正闯出学术界的象牙塔，带动了产业界风起云涌的“变革”激情。尽管如此，从目前已经公开的资料看，SDN 的实际部署至今仍多数局限于私有云的数据中心之间或私有云的内部网络之中。然而，SDN 公认的巨大市场空间却存在于对网络安全有更高要求的多租户（或用户，即 tenant）公有云，以致企业网。

那么，以建设基于公有云的虚拟私有云为例，SDN 的安全架构应该如何设计呢？

## 软件定义网络安全的特点

有人半开玩笑地说，对于网络管理人员来说，有无 SDN 相当于计算机与计算器的区别，前者可以通过编程较为灵活地实现自己的应用，而后者只能完成厂家规定的功能。SDN 将分立设备中的控制机制抽取出来，由控制器对其所管控的网络进行相对集中的全局流量调度，构成具有全局知识的控制平面（Control Plane)，从而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。

研究云数据中心可以有多种角度,较为流行的有美国 NIST 提出的 IAAS、PAAS、SAAS 以及公有云、私有云、混合云等不同分类，也有计算、网络、存储的系统角度或使用（in use)、存档（at rest)、传输（in motion）的数据角度。具体到云网络，又有云端（终端接入)、云内、云间网络的不同特点。例如，在业界引起巨大反响的 Google 应用案例,就是利用 OpenFlow 协议将其所有云数据中心之间的互联全部用 SDN 实现了。而 VMware 斥资 12.6 亿美元收购 SDN 领军企业 Nicira，据信是瞄准云数据中心内部网络虚拟化，以期巩固其服务器虚拟化产业龙头地位，成就虚拟数据中心的完整蓝图。

从虚拟私有云租户的实际需求出发研究 SDN 的安全，比较企业内网与虚拟私有云的异同，则不难看到，用户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）与外部网络（非可信网络或称公有网络）的安全连接、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、以及网络流量的安全处理。SDN 带来的最大挑战，就是与虚拟化所提供的网络拓扑灵活性“孪生”的网络边界动态性，换言之，原来静态、自然的内部网络物理边界，被 SDN 动态、虚拟的逻辑边界替代，因而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。

**软件定义网络安全的构架**

以基于 OpenFlow 的 SDN 为例，与原有网络相比，核心的变化是将交换机、路由器等转发设备中的控制机制，包括信息采集、策略比对、决策编译（生成转发表或路由表）等统统剔出，使转发设备自身仅按控制器下达的流表（flow table）转发，从而变得效率更高、成本更低。另一方面，控制器统一收集网络状态信息，发现网络拓扑关系，检查网络转发策略，并生成和下达流表。

由此可见，根据一个网流的首个网包（first packet，即首包）的包头（header）所进行的安全处理，不应再发生在网关（gateway）处，而是在控制器上。那么，传统的 ACL（Access Control List，接入控制表）或网包过滤防火墙（packet filtering firewall），就应该部署在控制器处。然而，控制器通常只能收到首包的包头，无法进行状态检测（stateful inspection），所以状态防火墙和需要过滤网包载荷（payload）的深度检测（deep inspection）防火墙，还应部署在数据平面（data plane）上或数据平面与控制平面的交汇处，既可以是交换机、Hypervisor 上，也可以是虚拟机、服务器上。因此，传统上部署在物理网关处的网络接入控制（通用防火墙）依然要在安排到“逻辑”网关处。利用 SDN 调度网流的便利，这个逻辑网关可远可近，可分可合，可软可硬。

所谓远近，是指离防护对象的距离远近。安全机制可以和虚拟机结合在一起（接在 vSwitch 上），这样会适应动态性强的特点，在虚拟机迁移时只需 SDN 调整流表，安全策略的实施受到的影响相对较小，安全管理可以相对独立。例如，VMware 的 vSheild 很大程度上就是以此为基础的解决方案。这种做法实际上延续了传统做法，将一般只在 2 层（或 3 层）的网络交换与通常在 4 层（或 3 层）

以上的网络安全相对独立地处理。安全机制也可以建立在稍远的数据中心 fabric 上，或者说相关流量的中继节点处，由控制器根据物理网络与逻辑网络的映射关系变化统一更新转发和安全策略。这是因为 SDN（以 OpenFlow 为例）对网流的处理是可以贯穿 2 层至 4 层的。这样做的另外一个好处是可以借助硬件设备满足对安全机制的性能要求。例如，专注 SDN 安全的硅谷创业公司 vArmour 在今年春季 ONS 上展示的似乎就是这样一种方案，集成了网络智能与应用安全，并与 OpenFlow 控制器一起，支撑动态网络拓扑。

所谓分合，是指安全机制的分布与集中，既可以是安全防护部署像前文所述一样分布在逻辑网络的不同位置，也可以是安全能力的分享与聚合。面向多租户以及一个租户的多安全域的情况，可以将一个高端硬件防火墙根据各个租户或安全域不同的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 IDS/IPS、DLP/ILP 或防病毒等安全能力不够时，可以使用“多虚一”的手段，利用多个安全设备通过负载均衡或协调工作组成的集群系统，灵活增减、调配安全处理能力。

所谓软硬，其实前文都已经涉及到，就是硬件设备和软件实现的选择和结合。有些安全机制是需要或者适用专用硬件加速的，例如 VPN 需要对大流量进行加解密操作，大规模网络中防火墙、防攻击的状态自动机也需要硬件加速，而真正突破入侵、泄露、病毒等各类特征匹配瓶颈，也许最终要仰仗专用硬件（ASIC、FPGA 或众核处理器），而非通用服务器所能承担。当然，考虑到目前数据中心中服务器的实际计算容量使用率较低，如果能调度机架内闲置的 CPU 时间去做安全处理，潜力也是巨大的。

**软件定义网络安全的技术**

基于 SDN 的云数据中心网络安全，特别是以虚拟私有云为例，涉及很多关键技术，难以全面综述。但最核心的至少应该包括以下几项。

虚拟网络需保证租户或安全域具有完整的、隔离的网络边界。这并不是单纯的网络安全技术，而是对虚拟网络本身服务于多租户或提供虚拟私有云服务的基本要求，在网络设计和实施中必须加以保证。当然，由于不同租户的虚拟机共享相同的物理资源，防止虚拟机逃逸等系统安全保证也是网络安全的基础。

另外，控制器上对多域包头的策略匹配，与传统 ACL、防火墙技术所用算法本质上是相通的，但转发与安全的协同调度，尚无成熟技术。在转发与安全策略耦合而控制分离的情况下，转发是虚拟网络配置的，安全则由租户各自设定，从逻辑网络到物理网络的安全策略映射及其正确性和一致性需要由自动化工具来完成和保证。

保障虚拟网络的边界安全，要求防火墙、IDS/IPS 等能够与控制器对流量的调度相配合，适应虚拟机迁移（migration）引起的安全边界动态变化，以及虚拟机增减（scale in/out）对安全能力的动态需求。保障虚拟网络的数据安全，对 DLP/ILP、防病毒等的要求类似，但相对于传统产品形态，策略配置上的变化应该会小些，主要挑战在于能力配置上。而保障虚拟网络的互连安全，因为接入点有时会随着逻辑网络边界的变化而变动，也需要相应地增加灵活性。

在上述对虚拟化和动态性的适应基础上，SDN 安全可以发挥更大功效。譬如，SDN 掌握完整的云数据中心网络拓扑，实时监测全局网络流量，因此可以与全局安全管理中心协同，根据网络拓扑、拥塞状况和安全事件及时做出判断，缓和（mitigate）安全压力、避免安全事故。SDN 也使得利用分布式安全能力构造成逻辑资源池成为可能，从而使安全的形态成为另一种 SaaS（Security as a Service，即作为服务的安全或“安全即服务”）。另外，需要研究的还包括提升控制器性能和抗攻击能力的技术，在分布式安全资源的情况下 SDN 安全机制的热备份（HA，High Availability，即高可用性）技术，SDN 安全资源的自身安全证明与测试验证技术，但远远不只这些方面。

SDN 以其开放的力量极大地震撼了网络工业。有人说，SDN 是自 1983 年 TCP/IP 应用和 1997 年 MPLS 滥觞之后，两个 14 年后网络界的又一重大热点；也有人说，SDN 有可能给网络界带来的是一场革命，其意义不下于当年 Wintel 和 IBM 兼容机对 PC 行业的解放。云数据中心的安全是信息产业真正进入云计算时代的关键， 而 SDN 安全将是对其实力和潜能的终极考验。