SDN安全防护技术研究

陶 冶[1] 张 尼[1] 张云勇[1] 王肖梅[2]
1.中国联合网络通信有限公司研究院
2.联通宽带在线有限公司

1 引言

在互联网设计初期，为实现不同设备的互联与数据通信需求，传统网络协议架构一直采用“漏斗式”设计原则，然而，随着近20年互联网用户呈现爆炸性增长，新型的网络应用如社交网络、在线大流量视频以及创新的服务模式如云计算、大数据的出现，对网络提出了新的要求。传统的网络架构逐渐在可控性、拓展性、安全性等方面出现瓶颈。

随着软件定义网络（SDN）、网络功能虚拟化（NFV）等新技术的出现，互联网的现有问题正在得以解决，但由于SDN等技术尚处于发展初期，安全方面的设计并不完善，且其架构本身对于传统网络结构冲击巨大，如果不对其进行相应的安全加固方案，而盲目代替现有网络设备及部署结构，SDN的引入将同样为网络安全带来挑战。下面从SDN为网络安全带来的机遇与挑战两方面，探讨安全平滑引入SDN技术的方案，为现有网络安全保驾护航。

2 SDN为网络安全带来的机遇与挑战

2.1 SDN技术完善网络安全体系

随着互联网应用的飞速发展与大规模普及，网络安全成为了一个不得不重视的重要挑战。由于互联网最初设计的主要目标是实现鲁棒性互联和资源共享，并未充分考虑网络的安全需求，虽然陆续有IPSec、DNSSec、RADIUS等技术被提出以加强网络安全性，但整个互联网的安全保障仍处于被动应对状态，网络的安全性问题缺乏系统性的解决方案。随着数据中心网络与云计算的日益兴起以及各式各样新兴网络应用的不断涌现，网络拥塞、黑客攻击、路由体系臃肿以及网络地址缺乏等问题越来越尖锐，这些问题都指向互联网最关键的软肋——可控性。

SDN的出现，使得上述网络安全难题出现解决的可能。SDN是一种新型网络架构，其具备两个主要特点：控制平面与转发平面分离；使用软件控制器对网络转发规则进行集中管理。SDN管控技术旨在通过构建网络虚拟化层和智能化网络操作系统，在一张物理网络拓扑的情况下合理划分虚网，并采用有效的隔离机制，进而实现高效的网络管控与资源调度。此外，SDN还能够通过网络操作系统将预先制定的机制策略添加到网络以达到预期管控目的。

2.2 引入SDN技术存在安全风险

新网络架构与技术的引入也给网络安全带来冲击。理解SDN架构与NFV技术的脆弱性对新型网络技术的落地有着重要意义。

由于SDN尚处于发展初期，业界各方也主要针对SDN的转发、控制等核心功能进行研究、开发与测试，而对于SDN架构与技术的安全性问题却尚无系统性的考虑。SDN相较于传统的网络架构，主要有两大创新点：数据转发平面与控制平面分离；控制平面采用软件形式的控制器集中管理。这其中，SDN控制器作为网络设备（交换机、路由器等）的集中管理软件，具备改变、下发流量报文转发规则等关键功能。软件控制器是整个SDN体系“大脑”，

所以保护控制器安全是SDN安全的重中之重。SDN的控制器安全防护主要包括以下几方面：软件控制器自身安全、控制器网络安全、控制器的高可用性、控制器的审计。

总之，软件定义网络是一种新型的网络架构，它可以通过集中管理的特性提供网络的完整拓扑与集中控制，形成更加细粒度的安全防护。然而，鉴于SDN控制器能够集中管理网络节点以向这些系统下发各类命令，围绕该系统的安全性开展工作是SDN技术落地的重要前提。控制器是SDN的大脑，如果没有部署适当的安全措施，网络可能遭到恶意攻击或者意外更改，这两者都会使网络崩溃。现在企业应该确保在SDN的设计、部署和管理过程中，其安全性是首要考虑因素。

3 SDN安全弱点与加固方案分析

3.1 SDN架构安全威胁分析

SDN的集中控制特性可以为网络的管理与运维带来巨大变革，上文也提到利用SDN控制器集中管理网络设备实现数据中心网络安全防护的方案，但由于控制器在SDN架构中的位置过于重要，一旦遭受恶意攻击，整个网络的安全性将受到严重威胁。特别是SDN技术还处于起步阶段，许多企业在引入SDN的同时，并没有在安全性上做出相应的防护措施，这也导致SDN控制器一旦遭受到恶意攻击，整个数据中心的网络将面临瘫痪威胁。

目前，针对SDN控制器的攻击方式主要有以下几类。

远程控制：由于SDN控制器管理数据中心内部几乎所有路由设备、交换设备以及其他网络功能设备，通过植入恶意软件远程控制控制器就意味着可以控制整个数据中心的网络流量。这种恶意攻击往往来自数据中心外部，一旦攻击成功，整个数据中心内的重要数据与资源将面临严重威胁。

数据中心内部的恶意用户：SDN通常被部署在云计算环境中，由于云平台的多租户特性，租户属性可能十分复杂且不易管控。由于租户使用的虚拟交换、路由设备可能与SDN控制器直接连接，内部的恶意租户将很容易直接对控制器发起攻击或向控制器植入恶意应用。另外，数据中心内部的恶意攻击往往比较隐蔽，可能采用心跳等方式对控制器进行持续攻击与控制，使得这种攻击可能很难被识别。

对控制器南向接口的恶意攻击与劫持：由于SDN控制器与数据中心内网络设备采用软件接口的方式连接，如果对控制器与网络设备的会话进行劫持，攻击者将能对数据中心的网络设备转发规则进行恶意篡改，以达到对隐私数据窃取等目的。许多传统的会话劫持方法如重放攻击就可以实现对控制器的南向接口的会话劫持。

伪造的SDN控制器：SDN控制器的软件属性意味着攻击者可能会通过伪造控制器以实现对数据中心内部资源的攻击与控制。由于SDN的自动化优势，人工检测往往被忽视，这也导致伪造的SDN控制器一旦成功与网络设备建立连接，将很难被识别。

恶意转发策略：SDN控制器可以对网络的交换以及路由规则进行控制与组合，实现对流量的转发、拒绝或修改等操作，但这也意味着攻击者可以对底层的转发规则进行恶意组合，形成恶意转发策略。由于这些恶意策略均由正常转发规则组合而成，这类攻击将很难被发现。

3.2 SDN安全加固方案建议

综上所述，目前针对SDN的攻击主要集中在对控制器的攻击。下面将对SDN控制器的防护与加固方案提出以下可行性建议。

利用传统网络安全设备：将传统硬件防火墙分别部署在SDN控制器的

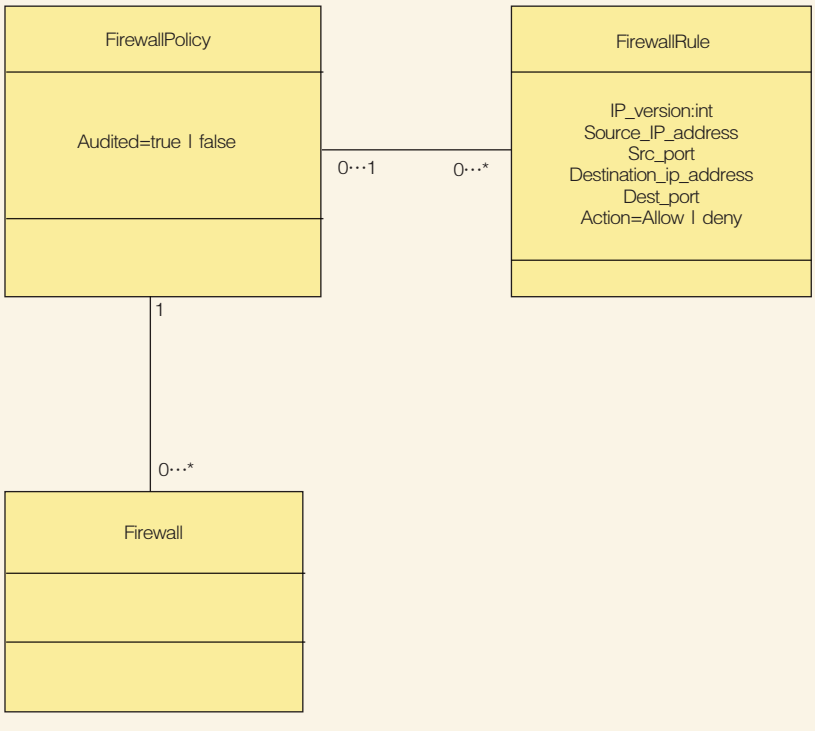

图1　Neutron防火墙服务的数据模型

北向与南向接口处，既可以有效防止来自数据中心外部的攻击，也可以组织内部恶意租户对控制器产生威胁。

部署安全代理：SDN控制器技术采用软件实现，对软件本身进行安全加固以及漏洞更新可以在一定程度解决控制器的安全问题。

控制器的高可用方案：为了防止控制器由于被攻击或自身原因导致的瘫痪情况，对控制器所在的服务器进行高可用备份十分重要。

控制器的分布式部署方案：由于SDN集中化管理的设计理念，控制器往往承担管理数据中心大部分网络设备的职责。如果所有网络设备的管理功能都集中在单一控制器上，一旦遭受攻击，后果将不可想象。采用分布式架构，多个控制器分别控制部分网络设备，所有控制器互为备份，可以有效解决网络安全风险。

4 SDN技术在安全领域的应用实践

4.1 OpenStack中的虚拟网络安全应用

OpenStack是目前业界关注度最高的开源云计算平台管理项目之一，许多知名的公有云平台与大型企业的私有云平台都是基于OpenStack搭建的。作为OpenStack内的重要核心项目，Neutron项目为用户提供端口、路由器、子网等各类虚拟网络服务，是NFV技术的最有代表性的落地实现。在基础网络功能日益完善后，Neutron也将发展重点放在网络安全服务上，其中负载均衡、VPN和防火墙都是Neutron项目中正在重点开发的功能。

在2013年10月18日发布的OpenStack Havana版本中，Neutron的防火墙功能完成了第一次迭代开发，实现对外软件接口以及基于IPTables的参考实现开发。在Havana版本中，整体网络安全服务链（包括VPN、负载均衡以及完整的防火墙功能等服务的服务链条）还没有搭建完成，但基础的防火墙功能已基本实现独立工作。未来随着整个链条的健全，每个网络服务可以作为节点被任意创建，引入到虚拟机以及网络流量路径上，形成真正的私有虚拟环境。

目前，Neutron防火墙服务的底层数据模型由防火墙策略（FirewallPolicy）、防火墙规则（FirewallRule）与虚拟防火墙（Firewall）三个模块组成。三个模块的数据模型如图1所示。

防火墙规则：防火墙规则模块是Neutron防火墙服务的最基础类，定义了包过滤所需要的一切信息以及匹配规则后对象需要执行的动作。

防火墙策略：防火墙规则定义了最底层的数据包过滤规则以及执行动作，而防火墙策略则是若干个防火墙规则类的集合。

虚拟防火墙：此数据类是OpenStack平台最终要实现的虚拟防火墙。通过与定义好的防火墙策略匹配，实现防火墙功能。

在上述三个数据类中，都包括“租户ID”这个属性。通过绑定租户ID，Neutron可以实现为每个租户提供个性化的虚拟防火墙服务。这样，整个云平台内各租户的防火墙信息以及数据流量就实现隔离。未来Neutron防火墙服务还将支持为一个租户创建多个虚拟防火墙实体，从而允许租户内部再分割成若干个相互隔离的虚拟网络环境。

4.2 巧用Openflow交换机防护DDoS攻击

如前文所述，SDN作为新网络架构，凭借其可控性强的特点，可以有效解决现有网络安全问题。目前，日本在SDN领域的研究与技术落地处于世界前列，如日本最大的电信运营商NTT公司早在2012年就利用SDN对其部分数据中心网络进行了革新，解决了传统数据中心网络部署繁琐、网元繁多、不易管理、易被攻击等问题，同时大大降低了网络部署成本。下面是日本某公司的一个实际案例，巧妙利用OpenFlow交换机搭配现有的流量清洗设备（IPS）进行针对数据中心的DDoS（分布式拒绝服务）攻击防护。

首先，该方案需要在数据中心的总入口路由器以及每个子数据中心的入口路由器均旁挂一台OpenFlow交换机，而入侵检测设备部署在数据中心的总入口处。SDN控制器利用软件接口方式与路由器及IPS相连。当IPS检测到DDoS恶意攻击流量时会通过接口发送通知给SDN控制器，控制器自动更改入口路由器的路由协议配置，将发送到目标服务器的全部流量引至OpenFlow交换机。然后，控制器会自动配置OpenFlow交换机处理这些攻击流量：首先根据源IP、目标IP、端口号等信息，区分正常报文与DDoS恶意攻击报文；然后将恶意报文删除，实现流量清洗，将正常报文的目标IP地址还原，防止形成路由环路；最后将正常报文送回总入口路由器，再转发至目标子数据中心的入口路由器处。同时，如果子数据中心需要对此流量进行再清洗，还可以再通过子数据中心入口处旁挂的OpenFlow交换机，利用如上步骤进行二次清洗。

相比传统方案，利用SDN技术实现的数据中心DDoS攻击防护有以下优势。

高可控性：SDN控制器可以通过软件接口的方式，统一管理所有路由器以及流量清洗设备。

低成本：无需使用厂商定制化方案，利用标准化的OpenFlow协议与开源的SDN控制器，即可有效实现DDoS攻击防护。

自动化：传统方案往往需要大量人工来24h监视入侵检测设备的报警情况，如发现攻击行为，需要人工修改路由器规则。利用SDN的软件定义特性，所有防护流程均可实现自动化（通过软件接口自动触发）。

灵活性：OpenFlow交换机可以根据不同规则识别攻击流量，在恶意流量清洗后可自动修改报文的目标IP地址，防止形成环路。传统设备则需要复杂的定制化程序或借用ACL策略等方式达到相同的效果。

通用性：由于OpenFlow协议为标准协议，对数据中心内网络架构以及设备无需进行大规模修改。

5 结束语

综上所述，随着SDN、NFV等下一代网络技术的日益成熟，互联网环境正在进行一场革命。随着物联网、社交网络等新型网络应用越来越普及，网络对可控性、安全性等功能的强烈需求也在加速这场变革。很多企业已经在下一代网络技术的探索上走在了前列，SDN与NFV等技术已经开始在某些环境，特别是在云数据中心商用落地。目前，世界上最大的公有云平台之一亚马逊云正是凭借引入SDN概念与虚拟防火墙、交换机技术，为用户提供了最新的虚拟私有云环境服务，这种全新服务可以在网络的数据链路层（Layer 2）实现不同租户的资源以及数据隔离，形成真正安全可信的私有云环境。

随着下一代网络技术的快速成熟与应用，这些新型网络架构与技术的安全隐患也逐渐浮出水面。高度集中的管理，过于依赖软件等特性，既为用户带来便捷，也带来很多安全问题，如何平滑、安全引入新网络技术，是这场网络革命能否成功的关键。

参考文献

[1] 刘诚明,陈赤航,张云勇,等.软件定义网络技术及应用.人民邮电出版社,2013(10)

[2] 张卫峰.深度解析SDN.电子工业出版社,2014(1)

如对本文内容有任何观点或评论，请发E-mail至ttm@bjxintong.com.cn。

作者简介

陶冶

硕士，现就职于中国联合网络通信有限公司研究院，工程师，主要从事信息安全、物联网安全技术、云运营等领域的开发与研究工作。

张尼

博士，现任中国联合网络通信有限公司研究院平台与云计算中心安全运营团队主任，高级工程师，主要从事信息安全、物联网安全、网络安全等领域的咨询与研究工作。

张云勇

博士，现任中国联合网络通信有限公司研究院平台与云计算中心主任，高级工程师，主要从事下一代开放网络、固定移动融合核心网、移动互联网及业务、公共运算等领域的咨询与研究工作。

王肖梅

现任职于联通宽带在线有限公司，工程师，主要从事数据仓库技术、信息安全技术及移动增值业务支撑系统的规划、建设与技术支撑工作。

高通为中小企业和小区接入点推出高性能、低成本小型基站系统级芯片

近日，美国高通公司子公司美国高通技术公司为小区和中小企业（SMB）小型基站推出Qualcomm FSM90xx系统级芯片（SoC）。从初期研发到实现，FSM90xx的设计与优化可满足小区和中小企业对于成本目标及性能的需求。FSM90xx的设计可提供特定功能，原始设备制造商可针对目标用户案例提供适合的产品外型和应用程序。FSM90xx充分运用2013年推出并已经在市场销售的FSM99xx的LTE功能。通过这款以全新小型基站系统级芯片为基础的接入点，移动运营商、有线多重系统运营商及企业将可扩充网络容量，并以极具成本效益的方法确保终端用户获得优异的移动体验。

FSM90xx的设计可帮助网络运营商增强其现有基站网络，同时提供基站和Wi-Fi连接支持。为了提升家庭和中小企业的连接体验，FSM90xx充分运用Qualcomm互联网处理器的功能，让LTE和Wi-Fi更加紧密结合，因为它具备强大的分包处理引擎，可扩充处理各种网络功能，包括Wi-Fi和LTE。其芯片组已经内建硬件加速器，以加快这两种无线电技术的数据处理速度，如此将可节省大量材料成本，包括硬件方面以及缩短系统整合所需的整体开发时间。

FSM90xx采用28nm技术的小区和中小企业产品，可提供极佳的耗电量，并可为极大量的应用减少整体解决方案成本。该产品的设计可轻松整合现有的产品，包括住宅宽带网关和中小企业Wi-Fi路由器，因此软件应用程序可同时运用基站和Wi-Fi无线电以提供更好的终端用户体验。

FSM90xx的软件与FSM99xx兼容，可让OEM充分运用FSM99xx的软件投资以扩大产品组合。FSM90xx同样获益于成熟的LTE PHY、数字预失真、低功耗及FSM99xx的其他差异化功能。

为了在密集的中小企业和小区小型基站部署环境中降低干扰并维持高服务质量，FSM90xx通过UltraSON软件整合先进的自组网络技术。FSM90xx可搭配美国高通技术公司的RFIC(FTR8xxx)，支持全球所有LTE频段，并保持与FSM99xx的兼容性，进一步简化并加快OEM跨产品线的开发速度。