基于 SDN 的网络安全防火墙设计与实现

唐海洋 郭晓丹

四川大学锦城学院 计算机与软件学院 四川 成都 611731

【摘 要】：软件定义网络（softwaredefinednetworking，SDN）技术是将传统网络架构进行解耦，使得网络设备中的控制平面集中收发到控制器中，网络设备只保留转发平面，以此通过软件实现灵活的控制面功能，满足用户多元化需求，从而为未来互联网技术的改革提供一种新的解决方案。但随着与 SDN 相关的网络设备的研发与使用，网络安全隐患也相应产生。本文首先在介绍了网络安全中的主要问题后，在研究 SDN 网络架构基础上，系统的将 SDN 网络架构理念与传统防火墙结合起来，给出的一种加强型的 SDN 网络安全防御机制,希望能在未来有效地为各行业网络安全提供强有力的保障。

【关键词】：SDN；网络安全；防火墙

引言

SDN（softwaredefinednetworking）所提出的网络架构理念，通过逻辑上集中的控制平面，实现网络管理以及控制集中化、自动化。它通过解耦控制层和数据层,从基础的网络设备中抽离控制层，并将控制层的工作移交给一个集中式、可编程的软件控制器（SDN Control Software），从而简化了底层硬件的复杂度。SDN 定义了统一的控制层面与数据层面之间的接口（Control Data PlaneInterface）抽象了底层硬件，从而屏蔽了底层硬件的区别。但 SDN 控制能力的集中使得控制器的安全性和性能成为整个网络的瓶颈。相对于传统网络设备的封闭特性，SDN 的开放接口这一特性，从而引起的网络攻击导致 SDN 在安全方面的薄弱性，这一问题不容小视。因此本文在研究 SDN 控制器的基础上，相对系统地梳理了 SDN 技术目前所面对的主要安全问题，给出了一种增强 SDN 安全的改进型 SDN 网络安全防御机制，以便对未来 SDN 网络安全的发展提供一种解决方案。

1 SDN 网络安全威胁

目前，虽然 SDN 为传统网络分离了控制层面和数据层面、简化了底层硬件，实现并简化了整个网络的配置过程，以及向上层应用提供网络的全局视图等优点。但是，作为一个尚在起步阶段的体系结构，在简化网络管理、缩短创新周期的同时，也引入了不可低估的安全威胁。

1.1 控制层安全威胁

SDN 由于管理的集中性，从而使得网络配置、网络服务访问控制、网络安全服务部署等一系列功能都集中于 SDN 这一台控制器上。SDN 的集中式控制方式使得控制器存在单点失效的风险。首先，控制器的集中控制的方式会使得控制器容易成为攻击目标，攻击者一旦成功实施了对控制器的攻击，将造成网络服务的大面积瘫痪，影响控制器覆盖的整个网络范围。其次，集中控制的方式，使得控制器容易受到资源耗尽型攻击，如 DoS、DDoS 等，被攻击的主机会出现目标主机有大量无法处理的 TCP 连接的现象，网络中出现大量虚假源地址的垃圾数据包，造成网络堵塞，使受害主机无法与外界通讯，还会利用目标主机提供的服务和传输协议上的缺陷，反复高效的发出特定的服务请求使受害主机无法处理合法请求等现象；同时，开放性使得 SDN 控制器需要谨慎评估开放的接口，以防止攻击者利用某些接口进行网络监听、网络攻击等非法行为。此外，控制器的自身安全性、可靠性也尤为关键。

由于 SDN 的控制器通常部署在通用计算机或服务器上，打破了传统的封闭运行环境，因此，SDN 控制器面临与操作系统相同的风险，且也无法防护攻击者针对计算机本身发起的攻击，如数据溢出型攻击。

1.2 应用层安全威胁

SDN 架构通过 SDN 控制器给应用层提供大量的可编程接口，这个层面上的开放性可能会带来接口的滥用，由于现有的对应用的授权机制不完善，用户极易安装恶意应用或安装易受攻击的应用，使得攻击者利用开放接口实施对网络控制器的攻击；其次，由于缺乏对各种应用的策略冲突检测机制，OpenFlow 应用程序之间下发的流量策略可以互相影响，从而导致恶意应用对已有的安全防护策略产生影响。

1.3 数据平面安全威胁

SDN 定义了控制层面和数据层面的标准接口协议 OpenFlow，也可能会受到攻击者发起的协议攻击；同时，由于 OpenFlow 协议中安全传输方式为可选项，在普通的传输模式下，攻击者能够伪造控制器或者篡改策略信息，向交换机发送虚假的流命令。

1.4 南向接口安全威胁

这主要是指由 OpenFlow 协议的脆弱性而引发的安全性威胁。OpenFlow 安全通道采用 SSL/TLS 对数据进行加密，但由于 SSL/TLS 协议本身并不安全，再加上 OpenFlow1.3.0 版本之后的规范均将 TLS 设为可选的选项，允许控制通道不采取任何安全措施，因而南向接口面临着窃听、控制器假冒等安全威胁。

1.5 北向接口安全威胁

北向应用程序接口(northbound application programming interface，简称 Northbound API)的标准化问题已成为 SDN 讨论的热点。由于应用程序种类繁多且不断更新，目前北向接口对应用程序的认证方法和认证力度尚没有统一的规定。此外，相对于控制层和基础设施层之间的南向接口，北向接口在控制器和应用程序之间所建立的信赖关系更加脆弱，攻击者可利用北向接口的开放性和可编程性，对控制器中的某些重要资源进行访问。因此，对攻击者而言，攻击北向接口的门槛更低。目前，北向接口面临的安全问题主要包括非法访问、数据泄露、消息篡改、身份假冒、应用程序自身的漏洞以及不同应用程序在合作时引入的新漏洞等。各个不同的平面或接口都涉及不同的安全威胁，其中网络攻击威胁等级以及主要方式，如表 1 及表 2 所示。

表 1 网络攻击威胁等级

表 2 网络攻击的主要方式以及防护措施

序号	类型	致命	高	中	低	信息	总数
1	DoS	-	0	5834	0	-	5834
2	漏洞攻击防护	2	49	17	0	0	68
3	WEB应用防护	-	0	0	0	-	0
4	病毒查杀	-	0	0	0	-	0
5	僵尸网络	-	795	0	0	-	795
6	总数	2	844	5851	0	0	6697

2 一种改进型的 SDN 网络安全防御机制

可见，要保障 SDN 的安全，必须探讨相关的安全认证机制和框架，当然也包括安全策略体系的构建。经上述分析，SDN 体系结构通过 SDN 控制器向业务应用层供给了开放的可编程接口。如果在 SDN 架构的基础上，增加一个包含应用层安全，北向通道安全，控制层安全，南向通道安全，数据层安全，东西通道安全和策略安全 SDN 的安全引擎构件，自动阻止接口滥用，可高效提升 SDN 安全性，如图 1 所示。

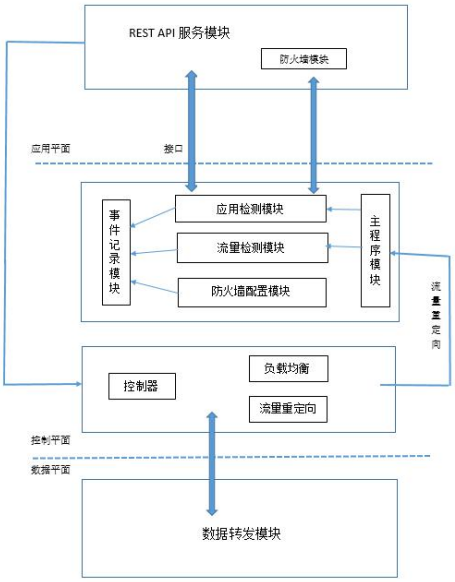

图 1:SDN 网络安全防火墙架构

2.1 REST API 服务模块

REST API 服务模块在应用平面的作用是实现与控制平面的对接，它通过 SDN 标准化开放的可编程接口完成与控制平面内模块间的交互。该模块中由控制层所提供的开放的可编程接的接口，即 REST API 形式，同时也遵循了网络中 HTTP 等相关协议。

2.2 防火墙模块

该模块属于应用层，可将其看作是一个应用程序，它可定期通过控制层来获取底层网络运行状态信息。例如，当底层交换机突然接收到大量恶意数据包，那么它便会阻挡这些不明来源的网络攻击，同时实时地评估当前网络的安全状态，并及时地通过控制器向数据转发层下发相应的包过滤规则等一系列有效措施，从而为网络安全提供有效地保障。

2.3 负载均衡模块

该模块是基于 NOX 控制器中的开源负载均衡组件改写后实现，该模块维护着一个循环链表，该链表记录了分布式应用防火墙系统中的每一个可对外提供服务的防火墙 IP 地址。当有新的任务或数据流到来时，负载均衡器会将任务或数据流轮流分配给各个防火墙，如此循环往复。

2.4 流量重定向模块

该模块通过接收负载均衡模块的分配信息，生成指定的防火墙的流条目，然后下发给 OpenFlow 交换机。此外，流量重定向模块也可接收控制器的配置信息，生成将内部流量转发至防火墙的流条目，并下发给 OpenFlow 交换机。

2.5 主程序模块

该模块是应用防火墙层面的主要模块，负责加载防火墙配置信息，将软件防火墙各模块实例化，并完成各模块实例的初始化。

2.6 防火墙配置模块

该模块用于提升对传统防火墙模块的配置。该模块通过将 iptables 防火墙的配置命令分解，定义地址对象、服务对象和时间对象，使防火墙实现可视化的过滤规则设置。

2.7 传统防火墙模块

该模块由 Linux 内核中的 netfilter 组件实现，netfilter 组件能够高效运行，且十分稳定，保证了传统数据包在过滤防火墙时，实现其对数据包的快速分析和过滤。

2.8 应用检测模块

该模块采用深度包检测技术，优化了开源项目 OpenDPI 的部分功能，实现了 URL 地址过滤、应用数据检测和过滤、应用层协议识别等一系列功能。

2.9 流量统计模块

该模块用于对途经防火墙系统的网络流量进行统计和汇总，可以从多个维度进行统计，比如针对各种应用协议流量的统计、流入流量的统计、流出流量的统计等。

2.10 事件记录模块

该模块的主要功能是用于对 REST API 服务模块中的安全审计规则和日志记录规则的配置，以及报警和日志事件的存储、检索。

2.11 数据转发模块

该模块主要是用来支持 OpenFlow 协议的网络设备，能够较好地完成对数据包的转发工作。同样存在于网络设备中的流表也是按照 OpenFlow 协议制定，我们知道流表项是由匹配域、计数器和动作三项组成。数据的转发是用于对交换机中的流表项进行优先级匹配，匹配成功的数据包便会直接执行流表项中的计数器功能和动作，如转发到交换机的某个端口，并在计数器中记录转发包的数量等。对于没有匹配成功的数据包将以 PACKET_IN 的形式发送到控制器进行处理。

3 实验环境展示及结果

该应用通过 SDN 网络实验平台搭建的一个实验环境来验证防火墙系统的有效性。实验环境部署和配置如图 2 所示。

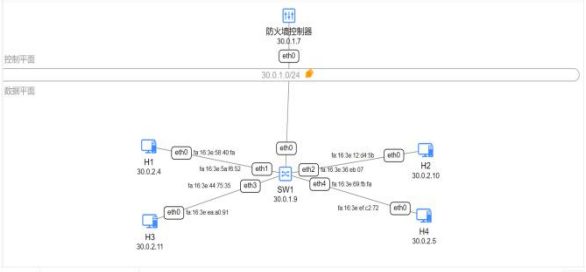

图 2 SDN 安全防御机制实验拓扑

该实验中，安装了一台 controller 防火墙控制器和 1 台 OpenvSwitch 交换机，并将交换机上物理端口 0、端口 1 和端口 2、端口 3、端口 4 分别划分到相应的主机上。并在交换机上设置了相应的访问控制策略。设置控制器 IP 地址为 30.0.1.0，交换机 IP 地址为 30.0.1.9，主机 1 的 IP 地址为 30.0.2.4，主机 2 的 IP 地址为 30.0.2.10，主机 3 的 IP 地址为 30.0.2.11，主机 4 的 IP 地址为 30.0.2.5，3.2 实验结果实验采用 ping 命令和流量发生器发送网络流量，并使用工具查看每个端口的流量情况。主机 1 向主机 3，主机 4 发送相应 ICMP 报文，操作指令为 ping 30.0.2.11 和 ping 30.0.2.5。

3.1 实验场景 1

在 mininet 中验证内网的连通性，即 host1 对 host2 进行 ping 操作。指令：h1 ping -c1 h2 。mininet 中可以直接观察到结果，如果成功则说明内网的 L2-learning 交换机工作正常，且内网络主机之间可以连通，同时我们也可以通过 ping 指令完成主机与服务器之间的连通性。

3.2 实验场景 2

在 mininet 中验证内网与外网的连通性，即 host4 对 host3 进行 ping 操作。指令：h4 ping -c1 h3 。同上在 mininet 中直接观察结果，在状态防火墙机制中，我们设定外网主机可以直接 ping 内网服务器，即外网主机 h4 随时可 ping 通 host3 运行 HTTP 服务。

3.3 实验场景 3

在 mininet 中验证内网与外网的隔离性，即 host4 对 host1 进行 ping 操作，指令：h4 ping -c1 h1。在 mininet 中直接观察结果，此项实验同时也能体现状态防火墙具备的普通防火墙的网络间访问控制特性，只有内网主机 h1 先行 ping 主机

h4 并且在 t 时间内才能成功，外网主机不能直接访问内网主机（host1 和 host2）。

结语

本文提出的一种基于 SDN 的网络安全防御机制，已通过实验方案并且验证了其可行性。实验结果表明。SDN 网络架构下的可编程管理方式具有高度的灵活性，在对防火墙进行功能的升级或应用进行增删改时无需过度依靠硬件与专业系统的开发，可以模块或应用程序的方式加入 SDN 网络架构中。同时 SDN 作为一种全新的未来网络管理架构，SDN 网络防火墙具有高效性，灵活性等特点，在未来的网络安全领域可以发挥巨大的作用，极大地体现了 SDN 与网络安全领域技术之间的融合性。

参考文献：

[1] 唐国纯.SDN 网络安全架构的研究[J].软件,2020,41(08):10-13.

[2] 费宁,刘春秋.基于 OpenDaylight 防火墙的研究与实现[J].计算机技术与发展,2019,29(06):112-115.

[3] 陈铭.网络与信息安全问题分析与防控[J].中国新通信,2020,22(10):143.

[4] 刘琦,陈云芳,张伟.软件定义网络下状态防火墙的设计与实现[J].信息网络安全,2015(11):47-52.