HZ BOOKS
华章IT

NSFOCUS

信息安全
技术丛书

国内首部介绍SDN/NPV安全的书籍

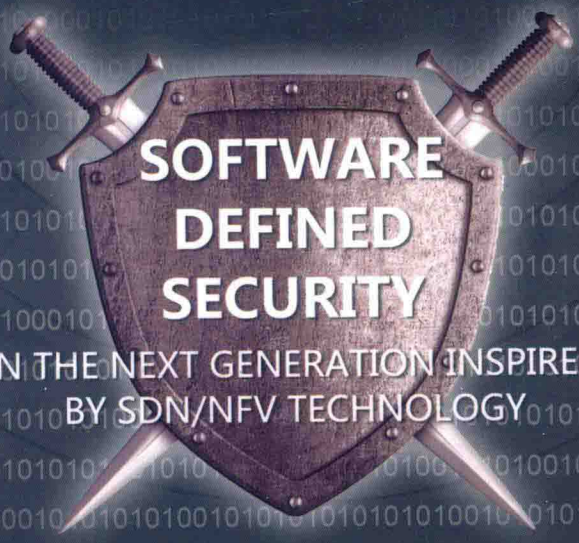
系统地介绍了基于软件定义思想重构安全体系的相关实践，为应对日益严峻的互联网安全挑战提供了很好的思路。

全面阐述了SDN/NFV原理、架构、组网，特别是SDN/NFV架构下的安全威胁分析，对SDN/NFV知识的普及、网络安全的研究和产业的发展有极大的促进作用。

软件定义安全

SDN/NFV新型网络的安全揭秘

刘文懋 裴晓峰 王翔 编著



机械工业出版社
China Machine Press

信息安全
技术丛书

软件定义安全

SDN/NFV新型网络的安全揭秘

刘文懋 裘晓峰 王翔 编著

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

软件定义安全：SDN/NFV 新型网络的安全揭秘 / 刘文懋，裘晓峰，王翔编著 . —北京：机械工业出版社，2016.9（2017.1 重印）
（信息安全技术丛书）

ISBN 978-7-111-54836-2

I. 软… II. ① 刘… ② 裘… ③ 王… III. 计算机网络 – 网络安全 IV. TP393.08

中国版本图书馆 CIP 数据核字（2016）第 218213 号

软件定义安全：SDN/NFV 新型网络的安全揭秘

出版发行：机械工业出版社（北京市西城区百万庄大街 22 号　邮政编码：100037）
责任编辑：余　洁　　责任校对：董纪丽
印　　刷：北京诚信伟业印刷有限公司　　版　　次：2017 年 1 月第 1 版第 2 次印刷
开　　本：186mm × 240mm　1/16　　印　　张：12
书　　号：ISBN 978-7-111-54836-2　　定　　价：59.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：（010）88379426　88361066　　投稿热线：（010）88379604
购书热线：（010）68326294　88379649　68995259　　读者信箱：hzit@hzbook.com

华章IT
HZBOOKS | Information Technology

Preface 序

软件定义网络（SDN）的发展之迅猛，超出所有人的预料。从 2007 年斯坦福大学的 Ethane 项目和普林斯顿大学的 4D 架构，到如今数十亿美元并持续快速增长的市场规模，SDN 冲破网络界长期以来愈发烦冗、日趋垄断的藩篱，为技术创新和产业发展打开了一片新天地。SDN 从象牙塔到投资潮前所未有的推进速度，也及时响应了云计算的呼唤。然而，正如互联网在成熟过程中所揭示的那样，网络连通技术的每一次阶跃都需要网络安全技术的伴随。反之，用户采纳新技术时对安全性的疑虑，会使其普及遭遇瓶颈。

SDN 安全因而成为近年来学术研究和产业开发的热点。软件定义网络的安全性有什么特点？如何构建相应能力保护 SDN 安全？如何利用 SDN 的优势提升网络的安全性？这些都成为 SDN 安全的研发内容，包括 SDN 的安全（Secure SDN 或 Security for SDN）和软件定义的网络安全（SDN Security 或 Security by SDN）。我国 SDN 学术研究开展得较晚，2011 年才在 INFOCOM 上有所展示，但产业开发的进展很快，2012 年就召开了“中国开放网络高峰会议”。尽管近几年国内已经出版了一些关于 SDN 的书籍，但关于 SDN 安全较为全面的总结和介绍尚不多见。本书填补了这方面的空白，从学术前沿到实用案例，做了一番综合梳理的可贵尝试，也凝结了作者的研发成果。

SDN 从技术到市场仍处于成熟期的“前夜”，而 SDN 安全的研究和开发更是处于茁壮成长的婴儿期，在很多方面尚未达成共识，标准化和商业化也还比较薄弱。然而，SDN 引领未来网络发展的势头毋庸置疑，SDN 安全更是面临着各种新兴网络的安全挑战。网络的虚拟化与隔离、入侵与泄露的防范、攻击的抵御与缓解，特

别是安全策略的动态有效管理，从架构到算法、从理论到实践、从学术到产业，都还有很大的研发空间。虽然本书只是SDN安全技术的一个阶段性总结，但我相信它会成为业界向新的技术前沿发起冲击的“加油站”，为SDN安全的蓬勃发展起到推动作用。

李军

清华大学研究员，博士生导师

清华大学信息科学技术学院常务副院长兼信息技术研究院院长

清华信息科学技术国家实验室副主任

Preface 前言

光阴荏苒，SDN 和 NFV 等新的网络技术提出也不过短短数年。在这数年中，笔者见证了网络和安全圈的很多变化：从勒索软件肆虐、DDoS 产业化到网络保险初露端倪，从 Target 丑闻到数据泄露天天见，从 Hacking Team 武器库曝光到各种安全事件层出不穷，从 APT 关注回落到威胁情报满天飞，从网信办成立、“三法”推出[⊖]到网络安全上升到国家战略，似乎每天都有“好戏”出台。可以说，这是一个最坏的时代，也是一个最好的时代。信息安全从业者如果不能适应这些矛盾、拥抱这种变化，迟早会被淘汰。

不仅安全业务日新月异，攻击手段也层出不穷，就连人们所依赖的基础设施也都在发生翻天覆地的变革。如果 5 年前人们对云计算还尚存疑虑，那么现在人们使用手机享受云端服务时，似乎早已理所当然。而支撑这些 SaaS 应用的计算、存储和网络很可能是虚拟形态的。Gartner 公司的成熟度曲线早已指出，在不久的未来，SDN、NFV 等新技术会重构现有的网络基础设施。那么如何认识这些新技术，如何在这些新型网络环境中部署安全防护机制，能否利用软件定义的思想重构防护体系，都给我们提出了现实的问题。本书从以下方面解答上述三个问题。

本书第 1 章介绍了 SDN 和 NFV 技术的基本概念和发展方向，这些技术无论从技术还是理念角度，给安全防护带来的影响是深远的。

其一，新技术带来了新的挑战，第 2 章从架构、协议、资源、应用和系统实现等方面阐述了 SDN 和 NFV 面临的风险和解决方法，可为广大网络和安全架构设计者提供思路。

⊖ “三法”是指《中华人民共和国刑法修正案（九）》《网络安全法（草案）》和《国家安全法》。

其二，由 SDN 引入的软件定义理念，为抵御日益复杂的网络攻击提供了新的思路，即本书重点介绍的“软件定义安全”；从第 3 到第 5 章依次介绍了软件定义安全的背景、概念和架构。

其三，新技术可实现敏捷的资源池化和网络流量调度，极大提高了该安全防护体系的效率，第 6 章从原理上介绍了使用 SDN 和 NFV 技术实现一些安全防护的功能，这些功能都可被软件定义的安全架构所用，以加快安全响应的速度，以快制快，及时检测并阻断攻击链。第 7 章介绍了业内利用 SDN 和 NFV 技术和理念所提出的安全产品、解决方案和标准。

第 8 章偏重在软件定义安全架构本身，介绍国内外成熟企业的解决方案和初创公司所做的实践。

需要特别指出的是，本书分别介绍了 SDN/NFV 安全和软件定义安全，但请读者不要将两者混为一谈，前者是新的网络技术的自身安全问题，利用新的网络技术实现更多的防护功能，如自动化调度流量、安全服务链；而后者其实并非是一种技术，而是一种思想，强调通过软件化的安全应用和安全控制平台，集中控制、智能决策和敏捷响应，以解决以往安全设备简单堆叠不能抵御频复杂、高级的安全威胁的难题。当然两者也是有联系的，正文会详细介绍，此处不再赘述。

限于编写时间以及笔者水平，书中难免会有错误或表达不当之处，希望读者、专家指出，便于笔者修正，在此衷心感谢！

行文至此，非常感谢赵粮、黄晟等业内专家的指导，感谢你们专业、富有启发性的建议；也感谢如 SDNLAB、SDNAP 和云头条等技术社区的朋友们，给我们带来了非常有用的业界动态；最后感谢我们的家人，允许我们利用本应与你们在一起的时间完成此书。

Contents 目 录

第 1 章 Chapter 1

SDN 和 NFV：下一代网络的变革

1.1 什么是 SDN 和 NFV

1.1.1 SDN/NFV 诞生的背景

计算机网络的高速发展催生了海量的网络应用，而以 TCP/IP 协议为核心的互联网早已渗透到人们工作、生活的各个领域，如信息化系统、搜索引擎、电子商务和社交网络等。随着网络用户数量的急剧增加，网络规模不断扩大，网络设备承载了过多复杂的网络协议。由于传统网络设备大都以封闭硬件的形态交付和部署，网络中充斥着烟囱式产品形态的网络设备。因此，网络设备的封闭性增加了网络定制与优化的难度，使得现有的计算机网络在丰富的网络应用面前，越来越突显其架构演进的局限性。

近年来，虚拟化与云计算技术的兴起给网络动态性提出了更高的要求。随着云计算和移动互联网技术的飞速发展，越来越多的网络业务逐渐向云数据中心迁移，而网络流量也随之呈爆发式增长。根据思科《全球云指数（2013—2018）》[1] 的预测：全球数据中心的网络流量在 2018 年将达 8.6ZB（1ZB = 2^{20}PB）；相较于传统数据中心，云数据中心的网络流量占比将从 2013 年的 54% 提升至 2018 年的 76%；

从流量类型上看，74.5%的网络流量发生在数据中心内部。网络业务和流量的快速增长极大地提高了云服务商对云数据中心网络，尤其是云数据中心内部网络的管理难度。另一方面，云计算以“租用”的方式改变了IT资源的交付手段。租户对资源“按需申请”和“按使用付费”，使得部署在云数据中心网络中的各种资源处于持续改变的状态。网络拓扑的动态性给网络运维人员带来了前所未有的管理挑战。

众多网络领域的学者认为，以TCP/IP为基础的传统自治的网络架构的弊端在多年的发展演进中逐渐显露，这些问题难以通过打补丁的方式从根本上得到解决。因此，网络架构的重构势在必行。重构的新的网络体系架构一方面能够尽可能地考虑当前的各种需求，另一方面能够尽可能地满足未来可能的需求。这种架构重构的方案在学术界被称为“Clean Slate”方案[2]，其中代表性的工作有：美国的GENI、欧盟的FIRE、中国的CENI，以及日本的AKARI。在这些工作中，斯坦福大学Nick Mckeown教授的博士生Martin Casado领导的一个关于网络安全的子项目Ethane[3]获得了广泛的关注。该项目利用集中的网络控制器，定义基于网流粒度的全网安全策略，并将这些策略动态部署到所控制的交换机上，从而实现对安全的管控。通过在Ethane工作的基础上进行抽象，Nick Mckeown研究组提出将传统网络设备的控制平面与数据平面在物理上进行分离，构建全网范围内集中的控制平面，同时标准化网络设备的编程接口，进而实现网络行为的可定制性。这些创新型的网络架构理念，在2008年发表的“OpenFlow: Enabling Innovation in Campus Networks”一文[4]中得到了系统的阐释，SDN（软件定义网络，Software Defined Network）架构和OpenFlow标准接口就此形成。SDN技术[5]提出了交换设备数据平面和控制平面相分离的网络体系架构。通过逻辑上集中的控制器和开放、标准的交换设备编程接口，网络的转发行为可以灵活、快速地由控制器上根据业务逻辑编写的应用程序来定制，从而极大地方便了网络管理，促进了网络领域的研究创新。SDN的提出在网络领域迅速掀起了研究与应用的热潮。为了进一步推进SDN的标准化，加快SDN应用的落地，非营利性组织性质的开放网络基金会（Open Networking Foundation, ONF）⊖于2011年成立。它每年举办的开放网络峰会（Open Networking Summit, ONS）⊜汇聚了

⊖ https://www.opennetworking.org/。

⊜ http://events.linuxfoundation.org/events/open-networking-summit。

全球工业界最前沿的SDN技术和应用案例；同时，该峰会还专门设立了研究通道，供学术界和工业界就SDN的发展前沿进行沟通。由于能够对网络设备实施更有效的控制，SDN技术在校园网、企业网、无线网和数据中心网络等多种环境下获得了广泛的实验部署。SDN最成功的实际应用当属在数据中心网络环境下。对于数据中心的内部网络，SDN/OpenFlow的创始团队成立了网络初创公司Nicira，瞄准云数据中心的网络虚拟化需求，提出了基于OpenFlow软件交换机的SDN解决方案[6]，得到了虚拟化领域的巨头VMware公司的重视，并被后者以12.6亿美元收购。对于数据中心之间的网络，互联网巨头Google公司利用OpenFlow硬件交换机和分布式控制器，在全球多个数据中心之间实施流量工程，将广域网的链路利用率从30% ~ 40%提升至接近100%，并且降低了交换机的网包缓存需求，使得网络状态变得更加稳定[7]。

与起源于学术界的SDN不同，网络领域最大的客户群体——运营商，对网络设备，尤其是网络服务设备，有着另一番认识。由于运营商所提供业务的多样性，其网络中部署了大量的专用硬件设备。而运营商每开通一项新业务，往往难以对已有的硬件资源进行重新利用，必须采购新的网络硬件设备才能实现对新业务的支持。这些新增的硬件设备消耗了机房和电力资源，增加了运营商的资本性支出（Capital Expenditure，CAPEX）；同时，不同类型、不同厂商设备的管理接口和功能特性通常存在差异，运营商在进行系统集成和运营维护时面临着较高的复杂性，增加了运营商的运营成本（Operating Expense，OPEX）。更为严重的是，随着技术进步速度的逐步加快，网络设备的产品生命周期逐渐缩短，从而加快了产品的更新换代，影响了运营商利润的增长。

随着x86服务器性能的不断提升，网络中间设备平台逐渐进入网络设备厂商和运营商的视野，成为网络服务设备实现的备选平台。网络中间设备又称中间设备（Middlebox，MB），它能为网络流量提供安全增强、性能提升和带宽优化等多种监控功能。中间设备主要包括防火墙、入侵检测/防御系统、负载均衡器，以及虚拟专用网和广域网代理等多种服务型网关[8]。运营商希望利用通用硬件来减少对特定硬件平台的依赖，将网络功能从专用硬件设备中解耦出来，各自独立进行演进，从而实现根据需要动态灵活部署网络功能。2012年10月，AT&T、BT、DT、

Orange 等 7 家运营商在欧洲电信标准协会（European Telecommunications Standards Institute，ETSI）下发起成立了一个新的标准工作组——网络功能虚拟化（Network Function Virtualization，NFV）工作组[⊖]，并发布了 NFV 技术白皮书 [9]。该工作组的主要目标是希望基于虚拟化技术，采用通用的计算、存储和网络硬件，承载各种类型的网络功能，实现在网络各个节点灵活部署配置，从而降低业务部署的复杂度，最终降低网络的 CAPEX 和 OPEX。

自 2012 年该概念提出之后，NFV 技术不仅在标准化方面推进迅速，在实现方案上也快速成熟。2012 年，网络领域的顶级国际会议 SIGCOMM 上有一篇文章对中间设备在实际网络中的部署情况进行了调查，调查样本包括 19 个小型网络（终端数量少于 1000）、18 个中型网络（终端数量为 1000 ~ 10 000）、11 个大型网络（终端数量为 10 000 ~ 100 000）和 7 个超大型网络（终端数量大于 100 000），共 55 个实际网络环境 [8]。如图 1-1 所示，在以上各种规模的网络环境下，中间设备的总量和交换设备的总量相当。例如，在超大型网络中，路由器的平均数量为 2850 台，而中间设备的平均数量为 1946 台；在小型网络中，上述两个数据分别为 7.3 台和 10.2 台，中间设备总数甚至超过了路由器总数。此外，在所有中间设备类型中，网络安全设备占了绝大多数，而防火墙和入侵检测 / 防御系统也分列平均部署总量的前两位。

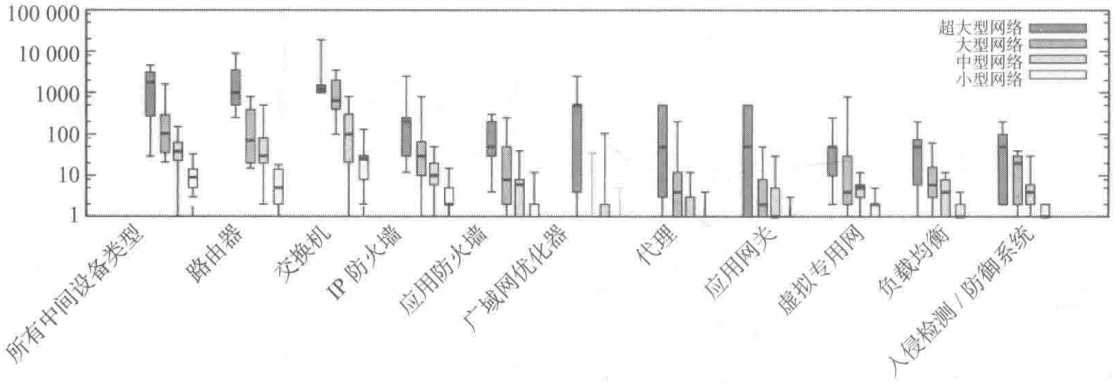


图 1-1 网络中间设备部署数量

⊖ http://portal.etsi.org。

SDN 和 NFV 一起成为了下一代网络变革的核心技术。作为全球领先的运营商，AT&T 公司在 2013 年 9 月发布的 Domain 2.0 网络变革计划中[10]，旗帜鲜明地将 SDN 和 NFV 作为其下一代网络架构的关键技术；同时宣称到 2020 年，会将基于 SDN 和 NFV 的新架构运用到超过 75% 的对外电信网络服务中，并彻底转型为一家软件公司。

1.1.2　SDN/NFV 的体系结构

根据 ONF 制定的 SDN 白皮书，SDN 的体系结构可以分为 3 层：基础设施层、控制层和应用层[5]，如图 1-2 所示。基础设施层与控制层之间通过控制数据平面接口（也称为南向接口）进行交互，控制层与应用层之间通过应用程序编程接口（也称为北向接口）进行交互。基础设施层由经过资源抽象的网络设备组成，这些网络设备仅实现网络转发等数据平面的功能，不包含或仅包含有限的控制平面的功能。控制层利用南向接口控制基础设施层的网络设备，构建并维护全局的网络视图，实现传统网络设备中控制平面的功能。应用层基于北向接口和控制层提供的网络视图进行编程，实现各种不同的网络应用，使得网络的转发行为能够通过软件进行定义，实现网络智能化。

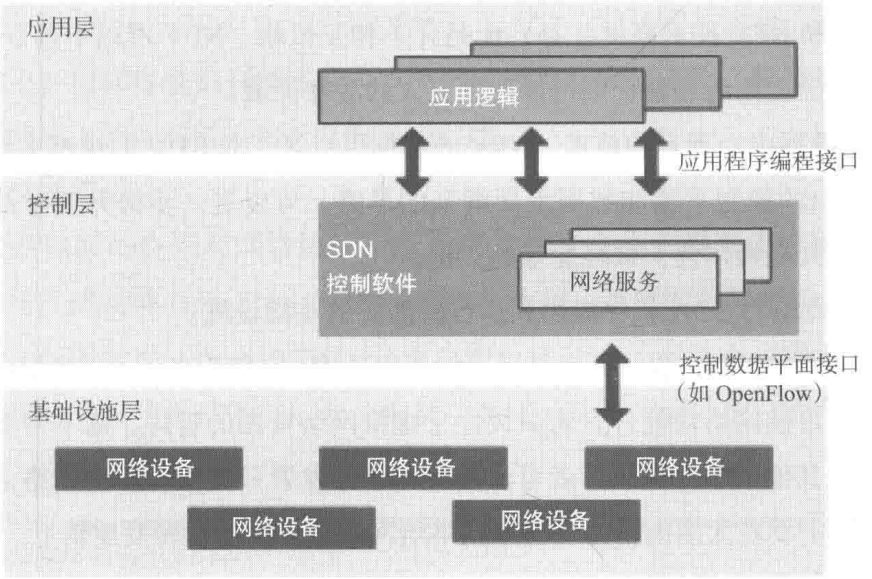


图 1-2　SDN 架构概览