



软件定义的企业级数据中心网络安全研究 *

刘文懋^{1,2}

(1.北京神州绿盟信息安全科技股份有限公司 北京 100089;2.清华大学信息技术研究院 北京 100084)

摘要:新型数据中心引入 SDN(软件定义网络)和虚拟化网络后面临诸多新型安全威胁,针对 3 类主要的安全威胁提出了安全防护的 3 个阶段,有效解决了新型网络的特有问题和现有安全产品缺陷,并针对目前安全难以适应的业务需求,给出了一种软件定义安全架构,可有效抵御各类快速和深度的攻击。

关键词:网络虚拟化;安全;软件定义网络

doi: 10.3969/j.issn.1000-0801.2014.11.024

Security Study of Software-Defined Enterprise Data Center Network

Liu Wenmao^{1,2}

(1. NSFOCUS Information Technology Co., Ltd., Beijing 100089, China;

2. Research Institute of Information Technology, Tsinghua University, Beijing 100084, China)

Abstract: Security threats of novel data center using software-defined networking were analyzed, and then three protection phases for defending were proposed, which solved unique problems and overcame current security product defects, and finally a software-defined security architecture to defend various quick and advanced attacks was designed.

Key words: network virtualization, security, software-defined networking

1 引言

经过多年的技术准备和商业模式探索,云计算已然进入快速发展阶段。当前有不少大型数据中心和企业 IT 系统可为云计算提供设施级别的强大支撑平台,然而业务快速增加给数据中心和大型企业的复杂网络管理带来了极大的挑战。网络虚拟化组件可对物理和虚拟主机所在的网络进行生成删除、拓扑调整和流量动态分配。在结合软件定义网络 (software-defined networking, SDN) 后,迁移虚拟机、动态组网,可以大大加快变更网络拓扑的进度。网络虚拟化和 SDN 的结合从很大程度上解决了上述问题,然而这类新型网络给安全防护带来了极大的挑战,现有安全架构既不能理解网络流量、防护网络资源,也不能满足网络

变更带来的更多防护需求。本文主要探讨新场景中传统安全面临的挑战以及可能的安全解决技术。

2 相关研究工作

参考文献[1]详细介绍了基于 OpenFlow 的 SDN 技术的背景和架构以及在系统高性能、一致性和可靠性方面的重要工作,但缺少安全方面挑战的介绍和分析,只提到 OpenFlow 协议设计中对安全性问题考虑不够。事实上,在 SDN 和虚拟化的新网络环境中的安全防护机制与传统网络存在很大差异。

SDN 和虚拟化的变革对安全防护提出了诸多挑战,为了兼容当前的安全设备,Zafar^[2]等人使用 SDN 控制器引导网络设备,将流量引导到实体安全设备中,但这种方案可

* 国家科技重大专项 03 专项基金资助项目 (No. 2012ZX03002011-003, No. 2012ZX03002002-003)

能会造成环路,虽然改写了 OpenFlow 的某些字段,但可能破坏协议兼容性。更好的办法是将安全设备虚拟化,融入整个设施虚拟化的体系内,将以往的安全边界从网络出入口移到虚拟网络设备中。虽然有一些新型网络的安全机制的探索,但总体而言还处于起始阶段,可实用的安全体系设计尚需大量的工作。

3 新型网络环境面临的安全挑战

部署虚拟化和 SDN 的新型网络带来了新的问题和挑战。一方面,传统的安全产品和安全解决方案无法解决新的网络安全问题;另一方面,网络虚拟化自身也面临一些安全问题,主要分为以下几类。

3.1 网络控制失效

新型网络虽然有相对传统网络的优势,但 SDN 本身也存在漏洞,特别是复杂的 SDN 控制器。数据平面和控制平面的分离主要是由控制器实现的,控制器是网络虚拟化最重要的设施。

(1) SDN 控制器被拒绝服务

攻击者可以通过发送大量数据分组进行拒绝服务攻击,使得控制器疲于分析数据分组而不能进行正常的网络管理;此外在一个大二层的 SDN 中,不正确的网络设置(如多个交换机成环后的网络风暴)也会造成控制器不可用。此时整个 SDN 就会崩溃,造成非常严重的后果。可见,保证控制器的可用性和安全性将是 SDN 安全中非常重要的一个环节。

(2) 应用策略不一致绕过

控制器控制整个网络的拓扑,并处理几百个甚至上千个应用的路由策略,每个应用的路由路径可能不同,如果这些不同应用产生的路由项之间存在不一致,就可能会出现非法路径。参考文献[3]提出一种攻击场景,系统根据安全策略应禁止主机 A 与主机 B 通信,但如果存在多个应用下发策略,使得从 A 传输到 B 的数据分组在中间交换机依次做了 SNAT 和 DNAT,最终被允许转发。攻击者可以攻破若干应用,从而绕过控制器实施进一步攻击。

3.2 传统安全设备失效

虚拟化环境中的数据流量一般可分为两类,但现有安全设备无法直接监控和防护这些数据:一类是跨物理主机的虚拟机数据流,一般通过隧道或 VLAN 等模式进行传输,如参考文献[4]所述云环境中存在多租户隔离的各种机制,现有的安全设备无法理解这些经过封装或加入 VLAN

tag 的数据分组,也无法部署在所有的传输路径上进行监控;另一类是同一物理主机内部的虚拟机数据流,只存在于虚拟交换机和虚拟网卡上,无法被实体的安全设备监控到。

总之,虚拟化改变了数据的流向,增大了大量物理设备不可见的区域,增加了整个虚拟化网络的安全管理难度。

3.3 难以适应网络变革

当 SDN 技术将网络更新缩短到分钟级或秒级时,安全防护的响应速度还停留在周级别甚至月级别。安全解决方案面临与传统网络一样的困境:封闭、视野受限和厂商锁定,难以适应网络变革。新环境中安全面临的挑战主要有以下两方面。

一方面,安全策略难以迁移。当虚拟机迁移时,网络管理系统可快速调整网络拓扑,在旧物理节点中删除虚拟网络资源(地址、路由策略等),并在新的物理节点中分配资源。但现有安全产品缺乏对安全策略迁移的支持,原网络设备和安全设备的安全控制不能按需变化。

另一方面,安全设备的设计往往与传统网络设备类似,将安全应用、操作系统和数据分组处理硬件全部封闭在一个硬件设备中,设备只处理经过的数据分组,视野受限;配置依赖管理员操作,异常繁琐;安全规则内置不易更新,恶意行为从检测到防护的周期很长。

4 新型网络环境下的安全对策

针对第 3 节中涉及的安全问题,提出一些可行的安全对策。

4.1 设计安全可靠的网络控制架构

在新的网络环境中,控制平面上移,且控制机制趋于集中化。网络控制器是 SDN 的中心,也是其前置的安全保证,需设计一个高可信、安全和顽健的网络控制器。

首先,控制器需要加入访问控制和审计机制,检查访问控制器的用户,保证是合法可信的,避免恶意攻击者发动各类攻击;并记录原始日志,做到事后或定时检测异常行为。其次,保证控制器和交换设备的通信安全,如 OpenFlow 协议就要求两者通信必须存在一个加密通道,以防止中间人攻击。最后,针对安全应用攻击或管理员不正确的配置,控制器的策略管理可检测下发的路由规则是否兼容并满足安全需求。

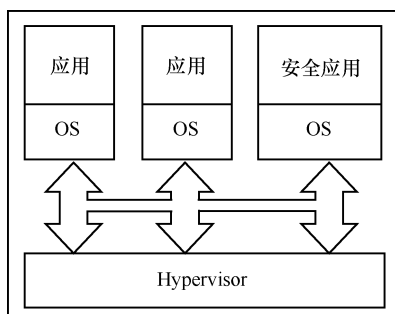
4.2 支持虚拟化的安全解决方案

针对传统安全产品对内部网络不可见的缺点,安全厂商推出支持虚拟化的安全产品,通常有如下 3 类。

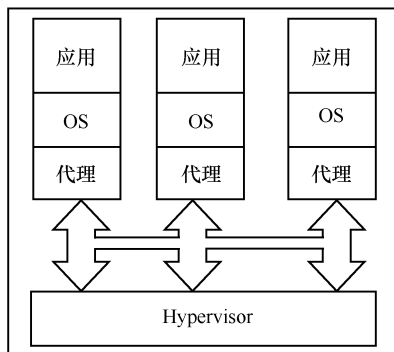


(1) 虚拟机形态

安全设备可以置于一台虚拟机中,并部署到虚拟化环境中,如图 1(a)所示。这种方式较方便,可不改动任何网络拓扑和计算节点,缺点是安全产品性能较低,容易遭到被感染的虚拟机的攻击,配置也比较复杂,需要随着虚拟网络的变动重新配置。



(a) 虚拟机形态



(b) 代理形态

图 1 支持虚拟化的安全解决方案

(2) agent(代理)形态

安全产品以代理的形式部署在各个虚拟机的操作系统中,并利用 Hypervisor 的应用接口,监控虚拟机的流量,如图 1(b)所示,该类产品已有一些案例,如 Trendmicro 的

Deep Security^[5]。这种方式可感知虚拟机和网络变化并采取应用策略,减少了对安全产品的攻击,没有过多带宽要求。缺点是功能受限于 Hypervisor 所提供的接口,在一些封闭的虚拟化实现中,开发较为困难,此外需要对 guest OS(子操作系统)进行修改,且整体防护方案限制在原宿主机内,复杂的安全联动方案不易部署。

(3) 实体形态加 SDN

虽然软件形态可以方便地监控虚拟环境中的内部流量,但限于现有条件,也可借助 SDN 的技术实现实体安全设备监控内部流量。如图 2 所示,假定检测虚拟机 VM1 到 VM2 的流量,SDN 控制器向 VM1 所在的交换机下发流表,除正常转发外,另将流量输出到与物理交换机相连的虚拟端口,并加上 VLAN 标记,数据分组经过物理交换机后到达安全设备;如果要对两台虚拟机间的流量进行防护,SDN 控制器可计算出源 VM 到安全设备的路径,向路径上的交换机下发流表,指定流量经过计算的路径到达安全设备,清洗后的流量到达某网络设备,SDN 控制器再计算该设备到目的 VM 的路径。这样,内部流量可以方便地牵引到实体设备中,后者只需要实现租户隔离即可适用于新型网络。

这种方案最大的优点是无需使用虚拟化的安全产品,最大程度地节省了短期开发成本;硬件安全产品不易受到恶意虚拟机攻击,自身安全性较高。其劣势是所有流量都要复制一份,较占物理网络带宽,并且需要修改每个交换机的流表,安全产品自动化和可扩展性较差。

从长远看,VM 形态比代理形态更开放,比实体形态更容易部署,如 Trendmicro 在参考文献 [6] 中也提出了 agentless(无代理)的方案,使用安全虚拟设备(security virtual appliance)。安全 VM 与安全控制器协同,实现安全设备动态部署和流量动态牵引,可实现快速安全响应。

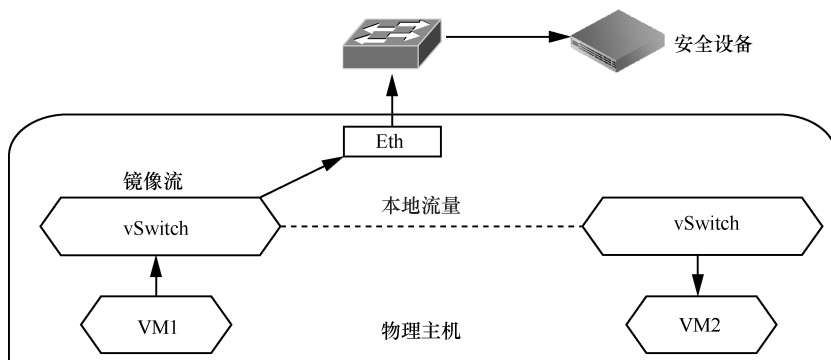


图 2 交换机将流量重定向到实体 IDS 设备

4.3 设计软件定义的安全架构

针对安全难以适应网络变化产生的挑战,需对安全架构进行重构,实现快速响应和联动防护,实现软件定义安全(software-defined security,SDSec)。本节介绍将安全的数据平面和控制平面分离,设计网络控制器和安全控制器联动的安全机制。

4.3.1 设计独立的安全控制体系

当前很多 SDN 下的安全设计是在 SDN 控制器中加入安全模块,如 FRESKO^[2]在 SDN 控制器中加入一个安全模块,可使用用户脚本检测 SDN 流信息,具有开放特性。但其应用没有与底层安全设备交互,无法做到深度防护;此外 FRESKO 与 SDN 控制器深度整合,过多脚本容易使其成为 SDN 系统的瓶颈。此外,如参考文献[6]提出了一种检测分布式拒绝服务攻击的方法,定时获取并分析流统计信息;参考文献[7]提出了一个 OpenFlow 扩展 FleXam,可对每条流进行采样,使 SDN 控制器访问部分数据分组以判断是否有攻击。这些架构只聚焦于局部安全功能,仅为 SDN 控制器的一个安全组件;且没有考虑安全应用和安全模块与安全设备的交互需求,作为网络应用与安全设备进行交互从架构上是不清晰的。在真实的 SDN 安全解决方案中,应该设计独立于 SDN 的安全控制体系,包括安全应用、安全控制器(SC)和安全设备。其中安全设备用于监控和处理 VM 的数据流,将处理过程中得到的安全告警信息上传到安全控制器上;安全应用对异常的安全事件进行细粒度的分析和检测,并做进一步决策;安全控制器掌握全局安全

状态,筛选可疑数据和事件,解析和执行应用下发的策略,并调度各安全模块。

在这种架构中,南北向控制器和底层设备是松耦合的,东西向数据流交换设备也是松耦合的,数据可以依次串行通过若干个安全设备,如防火墙、IPS 或 ADS 等,即使单个设备出现故障,也可以通过控制器及时调整路径避免单点失效。软件定义的安全架构如图 3 所示。

4.3.2 建立流、数据分组和深度行为结合的协同防护机制

SDN 环境中,网络控制器(NC)可分析全局流量,使得检测范围大大增加,并通过统计特征分析出一些异常通信,但无法确认攻击;传统安全检测设备可以对数据分组进行分析、管理和控制,但其分析内容颗粒较细,负载较重,且误报率较高;另外针对 APT 攻击出现很多新型的检测方法,如文件静态深度分析和文件动态行为检测,准确率较高,但涉及分组重组和深度分析,资源消耗非常高。深度安全监测和防护则需建立流、数据分组和文件层面结合的安全控制器——安全设备联动防护机制,如图 4 所示。

安全控制器通过 SDN 控制器建立全局流表,当出现异常的数据流(连接非常用端口、流量异常大)时,则将其牵引到 IDS 等安全设备,并将数据流标记为异常;当安全控制器收到安全设备上报的告警时,则进一步将数据流牵引到深度分析设备,并将数据流标记为可疑;当安全控制器收到深度分析设备的日志后,将数据分组标记为恶意,并将流量牵引到如 IPS 或防火墙设备进行防护。

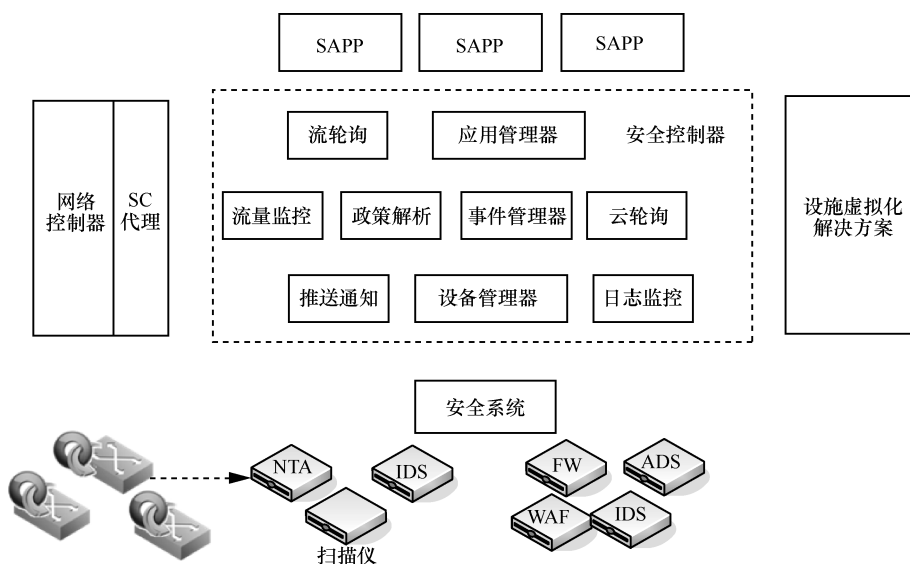


图 3 软件定义的安全架构

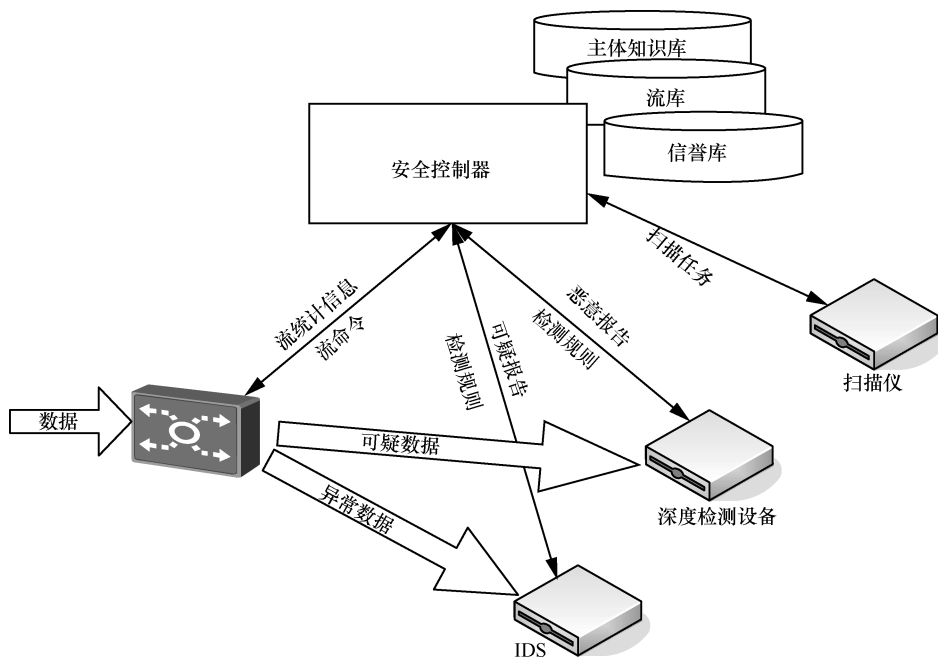


图4 面向流的安全设备联动机制

5 结束语

SDN 和虚拟化构建了下一代新型网络,SDN 在带来巨大便利的同时,引入了大量尚未解决的安全问题。本文分析了 SDN 的安全挑战,如对传统网络的攻击和对网络控制器的攻击,随后针对这两类攻击提出网络虚拟化的安全对策。针对安全策略难以迁移和网络流量不可见的问题,安全厂商需对自己的安全产品进行扩展,使之能与控制器联动,或者控制业务流程,并及时根据网络拓扑和网络流量变化调整安全策略。在此基础上,实现“底层安全监控保护产品—安全控制器—网络控制器”相互协作的安全解决方案,使用业务和安全松耦合,可防护传统手段难以抵御的各种攻击。

参考文献

- 1 左青云,陈鸣,赵广松等. 基于 OpenFlow 的 SDN 技术研究. 软件学报, 2013, 24(5)
- 2 Ayyub Q Z, Tu C C, Luis C, *et al.* SIMPLE-fying middlebox policy enforcement using SDN. Proceedings of SIGCOM, HongKong, China, 2013
- 3 Randell R. How the software defined datacenter is turning security on its head. Proceedings of RSA Conference, SanFrancisco, USA, 2013
- 4 沈余锋,余小军. 云计算环境下虚拟化安全探讨. 电力信息与

通信技术, 2013, 11(11)

- 5 Trendmicro. Changing the game with agentless security for the virtual datacenter. <http://www.vmware.com/files/pdf/partners/trendmicro/vmware-trendmicro-anti-virus-virtual-datacenter-sb-en.pdf>, 2012
- 6 Shin S, Porras P, Yegneswaran V, *et al.* FRESCO: modular composable security services for software-defined networks. Proceedings of Network and Distributed Security Symposium, SanDiego, California, USA, 2013
- 7 Braga R, Mota E, Passito A. Lightweight DDoS flooding attack detection using NOX/OpenFlow. Proceedings of IEEE 35th Conference on Local Computer Networks(LCN), Edmonton, Canada, 2010
- 8 Shirali-Shahreza S, Ganjali Y. Empowering software defined network controller with packet-level information. Proceedings of Communications Workshops (ICC), Atlanta, 2013

[作者简介]



刘文懋,男,博士,北京神州绿盟信息安全科技股份有限公司研究员,主要研究方向为 SDN 安全。

(收稿日期:2014-08-06)