



软件定义安全模型与架构浅析

郭春梅¹, 马骏¹, 郭昊², 毕学尧¹, 张如辉¹, 朱少敏¹, 杨聪毅¹

(1. 北京启明星辰信息安全技术有限公司, 北京 100193; 2. 全球能源互联网研究院, 北京 102209)

摘要: 目前大多数企业已经部署了基于策略访问控制的信息安全防御体系, 但是随着云计算环境部署和网络攻击技术的发展, 安全正成为云计算环境下亟待解决的重要问题, 诸如能轻而易举地绕过传统防火墙、突破基于黑/白名单与特征匹配的安全防御机制等高级持续性攻击, 给传统安全体系带来了新的挑战。分析了传统紧耦合安全防御体系在虚实结合网络环境下面临的问题, 提出了软件定义安全的模型及其框架下的关键技术, 实现了虚拟的和物理的网络安全设备与它们的接入模式、部署位置解耦合, 为企业云计算环境下自适应的主动安全防护提供了有益的探索。

关键词: 访问控制; 云计算; 高级持续性攻击; 软件定义安全; 解耦合

中图分类号: TP309

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2017074

Analysis of software defined security model and architecture

GUO Chunmei¹, MA Jun¹, GUO Hao², BI Xueyao¹, ZHANG Ruhui¹, ZHU Shaomin¹, YANG Congyi¹

1. Beijing Venus Information Security Technology Incorporated Company, Beijing 100193, China

2. State Grid Smart Grid Research Institute, Beijing 102209, China

Abstract: Currently, most enterprises have deployed information security defense system based on policy access control. With cloud computing environment deployment and network attacking technology development, security has been regarded as one of the greatest problems in the cloud computing environment. The advanced persistent attacks including of bypassing the traditional firewall easily, breaking through the black and white list and feature matching of the security defense mechanism have included to the traditional security system new challenges. The problem in the traditional tightly coupled security defense system of combining the virtual with the true for construction of network environments was described, and a software defined security model and framework was provided. The decoupling scheme of access patterns and deployment position in combining the virtual with the true for construction of network environments was realized, which provided a beneficial exploration in the field of the adaptive active safety for enterprise cloud computing environment.

Key words: access control, cloud computing, advanced persistent threat, software defined security, decoupled

1 引言

传统的网络安全防护方法通常是根据网络的拓扑情况, 以手动方式在安全域边界串联 (例如

UTM、IPS) 或旁路部署 (例如 IDS、Audit) 安全设备, 对进出安全域的流量进行监控。如果将这种与接入模式、部署位置紧密耦合的防护方法沿用到物理与虚拟网络共存的数据中心环境中,

会存在诸多不适应性。

(1) 安全设备部署过程繁复

传统安全设备部署过程通常依赖手动的方式,各种设备依次接入,过程繁复,对网络运行影响大,并且后期改动、调整起来也不灵活,扩展性差。对于虚拟计算环境而言,还会造成系统管理员与网络安全管理员职责界限模糊,出现问题后难于追责。

(2) 不能区别处理流经的流量

传统的在安全域边界连接一套安全设备的方法处理所有流经的流量,通常不能满足各细分用户/租户的定制化需求,而在边界连接多套安全设备的方法也是不现实的,因此带来了不灵活性和资源浪费问题。

(3) 安全防护范围僵化

安全设备防护范围就是整个安全域。在物理环境中不会经常变动硬件机器部署,因此安全域边界较为固定。对于虚拟计算环境而言,由于虚拟机迁移过程简单,虚拟机迁入、迁出情况会更频繁,从而导致相应的安全域边界发生改变。如果安全设备不能随之调整安全防护范围,就会带来安全隐患。

(4) 安全设备成为单一故障点

采用串联模式接入网络的安全设备(例如UTM、IPS),在完成安全防护的同时,也起到了网络连接的作用。如果安全设备出现故障,就会导致网络连接的中断。在这种情况下,通常会采用双机热备份的部署方式来提高可用性,但在一些情况下(如软件错误、攻击发生),仍然存在双设备故障的可能性。对于虚拟计算环境而言,双机热备份意味着更多地占用虚拟计算平台资源,安全风险加大。

从上述问题可以看出,传统的网络安全防护方法不能完全满足未来数据中心网络安全防护需求,因此,一种更为适用的防护方法——软件定义安全(software defined security, SDS)应运而生。SDS是从软件定义网络(software defined networking, SDN)引申而来,它的核心思想是将虚拟的、物理的网络

安全设备与它们的接入模式、部署位置解耦,抽象为安全资源池里的资源,统一通过软件编程的方式进行智能化、自动化管理和使用,安全资源、网络流量、安全模型间通过开放的接口定义,灵活地实现了安全功能部署和安全能力的提供,从而完成虚拟和物理网络的整体安全防护。

2 工作模型

就工作机制而言,SDS可以分解为软件定义安全资源、软件定义流量、软件定义高级威胁模型,3个举措环环相扣,形成一个动态的、闭环的工作模型。

(1) 软件定义安全资源(安全资源池)

配备安全资源是实现网络安全防护的第一步。在软件定义安全模式下,安全资源的配备是由软件编程的方式来管理的。由管理中心对安全资源进行统一注册、管理后,才能够实现后续的灵活使用。在虚拟计算环境下,管理中心还需支持虚拟安全设备模板分发和设备的创建。

(2) 软件定义流量(流安全平台)

由软件编程的方式实现网络流量的转发控制,通过将目标网络流量转发到安全设备上实现安全设备的逻辑部署和使用。

(3) 软件定义高级威胁模型(安全大数据、安全管理平台)

安全运营中心从各种设备上收集安全相关的事件、信息,通过预定义的算法进行自动化的整理和挖掘,实现对高级安全威胁甚至未知威胁的实时分析和建模,之后自动地将分析结果通过调用流安全平台和安全资源池的相关接口再次应用于安全防护,从而实现一种动态的、自动的、快速的安全防护。

3 整体框架

就具体实现而言,SDS框架可以划分为4个层次,由底至顶分别为安全资源层、转发层、控制层、管理编排层,如图1所示。以一个数据中心为例,SDS框架的各个层次详细介绍如下。

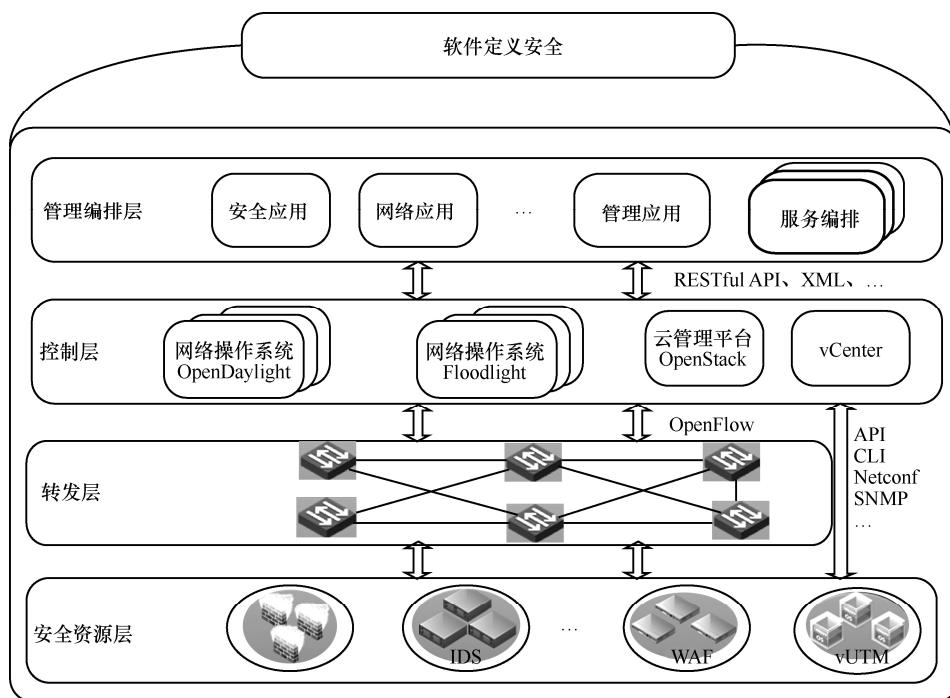


图1 软件定义安全整体框架

(1) 安全资源层

由数据中心内的各种物理形态或虚拟形态的网络安全设备组成，兼容各厂商的产品。这些安全设备不再采用单独部署、各自为政的工作模式，而是由管理中心统一部署、管理、调度，以实现相应的安全功能。安全资源可以按需取用，支持高扩展性、高弹性，就像一个资源池一样。

(2) 转发层

即 SDN 中的转发层，是指一类仅支持根据控制器指令进行数据分组转发，而不再自主进行地址学习和选路的网络交换设备。将网络安全设备接入转发层，通过将数据分组导入或绕过安全设备，即可实现安全设备的部署和撤销。

(3) 控制层

能够从全局的角度进行网络构建、管理，并提供开放 API 的网络控制器。这里既包括进行逻辑网络构建的控制器（例如 SDN 的网络控制器，通过给已有的下辖交换机下发转发表来实现网络构建），也包括进行实际网络构建的控制器（例如虚拟计算平台的管理中心，通过创建虚拟交换机并连线来实现网络构建）。

(4) 管理编排层

由侧重于安全方面的应用组成，包含用户交互界面，将用户配置或运行中实时产生的安全功能需求转化为具体的安全资源调度策略，并基于控制层提供的 API 予以实现，做到安全防护的智能化、自动化、服务化。

4 系统实现

4.1 关键技术

SDS 实现的关键在于如何使用安全资源池里的资源来实现相应的安全功能，要全面覆盖现有的数据中心网络情况，需要采用以下两类关键技术。

(1) 基于 SDN/OpenFlow 技术

SDN 思想将传统网络设备自带的控制功能和转发功能分离，其中网络设备仅保留转发功能，构成转发层；引入全局网络控制器提供控制功能，构成控制层；并且应用程序可以调用控制器提供的 API 构建网络，构成应用层。OpenFlow 协议被认为是 SDN 架构控制层和转发层间的第一个标准通信接口^[3]。将安全设备接入 SDN 的转发层，由应用层

程序调用控制层 API 设置转发层的转发表, 基于这种流量转发的可定义性实现灵活的逻辑部署。目前, SDN/OpenFlow 已被多款流行的开源虚拟计算平台 (例如 KVM、Xen) 采纳为虚拟网络的实现技术, 并且已有多家厂商的硬件交换机产品支持 SDN/OpenFlow, 也已有多款开源控制器可供选择 (例如 Floodlight、OpenDaylight、Ryu)。因此, 基于 SDN/OpenFlow 实现的 SDS, 能够适用于开源虚拟计算平台上的虚拟网络以及部分物理网络的安全防护。

(2) 调用虚拟计算平台提供的 API

适用于闭源虚拟计算平台上的虚拟网络防护。这类平台上的虚拟网络设备通常采用传统的自主工作模式, 不能通过设置转发表实现安全设备的部署和撤销。这里可以调用平台提供的 API, 通过将虚拟安全设备接入或断出虚拟交换机的方法, 实现安全设备的灵活使用。目前, 主流的闭源虚拟计算平台均有 API 满足上述需求。

4.2 系统实现

4.2.1 安全资源池

安全资源池由各种物理形态或虚拟形态的网络安全设备组成, 兼容各厂商的产品。这些安全设备不再采用单独部署、各自为政的工作模式, 而是由管理中心统一部署、管理、调度, 以实现相应的安全功能。安全资源可以按需取用, 支持高扩展性、高弹性, 就像一个资源池一样, 核心技术之一是安全产品虚拟化。

安全产品虚拟化就是使软件和硬件相互分离, 把软件从传统安全设备的硬件中分离出来, 使得安全产品的系统可以直接运行在通用服务器的虚拟环境中, 可允许多个安全产品同时运行在一个或多个服务器之上, 形成安全资源池, 对外提供各项安全服务。安全资源池系统架构如图 2 所示。

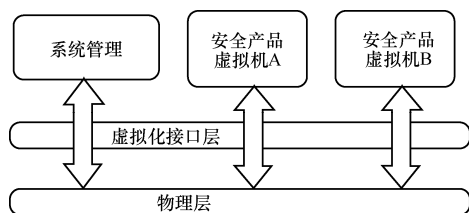


图2 安全资源池系统架构

4.2.2 虚拟网络监控系统

网络安全产品通常部署在网络边界。传统网络环境下安全域的边界就是安全域所在交换机的上行链路。对该链路上的网络流量进行监控, 就可以对安全域的边界进行防护。而在虚拟网络环境中, 同一个安全域内的虚拟机可能分布在不同的虚拟化服务器中, 并不能通过一条物理的或虚拟的链路监听到安全域中的所有边界流量, 即通常所说的“网络边界消失”了。“网络边界消失”后, 基于网络边界进行防护的网络安全产品就无法部署到虚拟化环境中。

解决上述问题的方法之一是构建虚拟网络监控系统, 对虚拟化计算环境的虚拟安全域进行防护。对虚拟网络监控系统而言, 虚拟化管理中心和虚拟化服务器是被保护的对象。虚拟网络监控系统对被保护的对象不做调整。在虚拟化计算环境的网络可达位置, 需要部署一个策略控制中心, 对虚拟化网络监控系统进行管理。策略控制中心是虚拟网络导流转发机制的管理控制中心。通过策略控制中心可以划分和管理安全域, 下发和管理安全域的安全防护策略, 控制导流虚拟机的行为, 查看导流虚拟机的工作状态和统计信息。

通过虚拟网络监控系统梳理出虚拟网络的边界, 使得利用物理网络安全产品对虚拟网络进行防护成为可能。实现虚拟网络的边界梳理和防护, 需要在每个虚拟化服务器中部署一个导流虚拟机 (AGT)。AGT 本质上是一个虚拟机, 它的主要功能是将虚拟交换机上的网络报文按照策略要求引导到指定的位置。在 AGT 的辅助下, 可以将分散在多个虚拟化服务器安全域 (边界或内部) 中的网络流量分流汇聚到指定的物理交换机端口或物理设备上^[4], 从而构造出了虚拟安全域中的网络流量汇聚点。基于这个汇聚点, 就可以通过物理网络安全设备对虚拟网络安全域进行安全防护。

以虚拟网络监控系统在 VMware 上的具体实现为例, 如图 3 所示。虚拟网络监控系统需要在

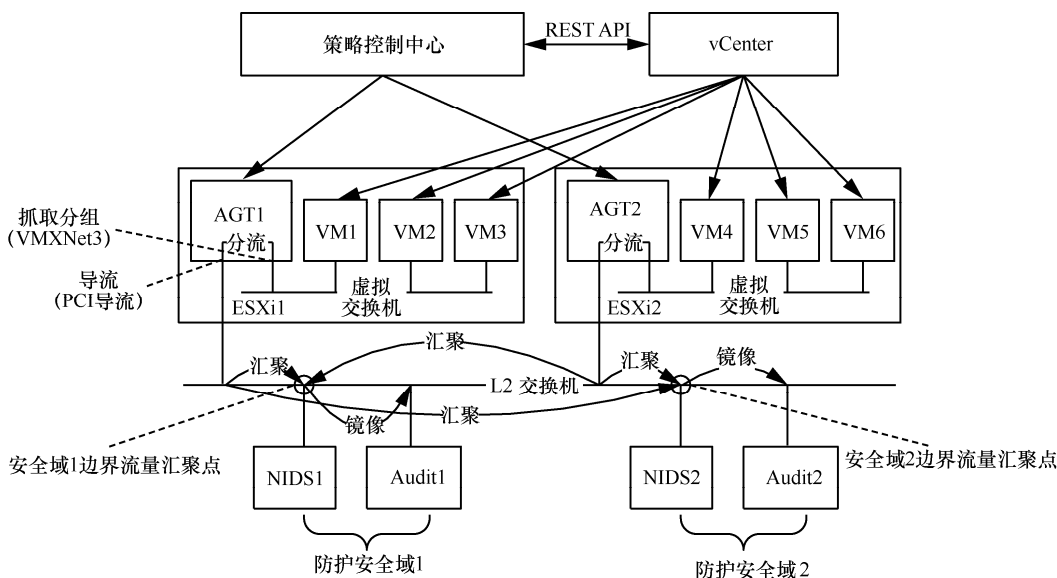


图3 虚拟网络监控系统原理

每一台虚拟化服务器中都部署一个导流虚拟机。导流虚拟机的抓取分组网卡需要连接到虚拟交换机的混杂端口组。每个需要被监控的虚拟机所在的虚拟交换机上都需要配置混杂端口组，并将导流虚拟机的一个抓取分组网卡连接到这个端口组中，用于抓取网络报文。导流虚拟机的转发网卡可以是物理网卡通过PCI导流技术直接赋给导流虚拟机使用，也可以是虚拟网卡。导流虚拟机导流出来的网络报文，可以导流到业务网络所在的物理交换机（带内方式），也可以导流到专用的物理交换机（带外方式）。

4.2.3 自适应控制

SDS系统为实现自适应控制，硬件方面采用具有SDN功能的硬件交换机，软件方面采用联动相关API实现。控制器向上层安全应用开放接口，通过接口安全应用能以软件编程的形式调用各种安全资源，全局把控整个网络的安全资源状态，实现对安全资源的统一调度和自适应控制。因为接口是直接为安全应用服务的，因此其设计需要密切联系安全应用需求，具有多样化的特征。

SDS自适应安全流程如图4所示。由图4可知，利用高层数据平台从外部获取威胁情报，结

合本地资产和漏洞的态势信息以及防护范围，判断出本地部分资源缺少相关防护，利用接口来调用SDS对从外到内的Web流量重新编排，同时调用对应的虚拟Web应用防护（virtual Web application firewall, vWAF）安全资源进行对应和防护，vWAF生成事件再提交给高层数据平台进行基于源IP地址的汇总分析，生成IP地址黑名单，同步给网络层防火墙进行阻断，从而实现网络层和应用层的两层防护，同时缓解应用层的性能压力。

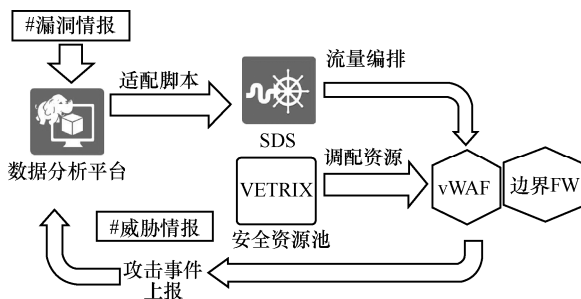


图4 SDS自适应安全流程

4.3 特点分析

通过编程的方式调用安全设备资源，SDS实现了一种灵活的网络安全防护，更加适用于情况复杂的数据中心网络。与传统的网络安全防护方

法相比, SDS 有如下特点。

(1) 安全功能部署灵活简单

管理员可以随时、随地采用多种设备对应用层软件(例如管理中心)进行访问,通过简单的界面点击操作实现安全功能的自动化部署。由于不再需要复杂的手动操作部署每台安全设备,提高了可扩展性。

(2) 细粒度区分流量

通过转发层对流经同一网络的流量做细粒度区分,支持不同流量采用不同的安全策略,因此适用于多租户环境。各个租户可以按需进行个性化安全服务定制,具备高弹性、可计量性。

(3) 安全防护范围动态调整

集中化的管理方式使得控制层能够快速感知虚拟机的动态迁移事件,该事件被上送到应用层,应用层随之下发策略来改变安全资源的部署,最终实现安全防护范围的动态调整。

(4) 维护网络高可靠性

安全功能的部署和撤销均采用自动化的方式进行。当检测到某个安全设备发生故障后,可以实时地将基于该安全设备的应用撤销;当安全设备故障解除后,又可以实时地将基于该安全设备的应用恢复。这期间维持网络不间断,确保了网络的可靠性。

(5) 安全功能易于创新

基于软件的安全功能编排、与硬件安全设备的解耦使得安全功能的创新不再依赖硬件安全设备的升级。并且,控制层全局化的视角使得安全功能更容易根据实时运行情况做出调整,更具智能性。

5 结束语

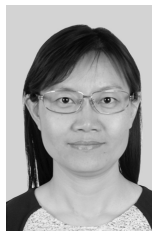
随着虚拟化技术和 SDN 在企业数据中心的快速应用与部署,网络边界逐渐淡化,传统紧耦合的安全防护机制已不能满足新形势下的安全要求。SDS 框架能够支持物理与虚拟网络并存、多租户、易迁移、高弹性、自动化等特性

需求,极大地减小了安全产品和虚拟化平台耦合度,将成为未来数据中心网络安全防护的有力支撑。同时,SDS 架构具备平滑升级能力,当网络层升级到 SDN 时,该方案能够结合 SDN 控制机制,实现安全能力的自适应业务编排,有力保障了用户虚实结合网络环境下的安全防护要求。

参考文献:

- [1] 刘文懋, 裴晓峰, 陈鹏程, 等. 面向 SDN 环境的软件定义安全架构[J]. 计算机科学与探索, 2015, 9(1): 63-70.
LIU W M, QIU X F, CHEN P C, et al. SDN oriented software-defined security architecture[J]. Journal of Frontiers of Computer Science and Technology, 2015, 9(1): 63-70.
- [2] 裴晓峰, 赵粮, 高腾. VSA 和 SDS: 两种 SDN 网络安全架构的研究[J]. 小型微型计算机系统, 2013, 34(10): 2299-2303.
QIU X F, ZHAO L, GAO T. VSA and SDS: two security architectures in SDN[J]. Journal of Chinese Computer Systems, 2013, 34(10): 2299-2303.
- [3] 左青云, 陈鸣, 赵广松, 等. 基于 OpenFlow 的 SDN 技术研究[J]. 软件学报, 2013, 24(5): 1078-1097.
ZUO Q Y, CHEN M, ZHAO G S, et al. Research on OpenFlow-based SDN technologies[J]. Journal of Software, 2013, 24(5): 1078-1097.
- [4] 李陟, 李小康. 通过虚拟分流突破云环境安全部署问题[J]. 邮电设计技术, 2016, 10(1): 45-49.
LI Z, LI X S. Through the virtual diversion to break through the cloud environment safety deployment issues[J]. Designing Techniques of Posts and Telecommunications, 2016, 10(1): 45-49.
- [5] 林萍萍, 毕军, 胡虹雨, 等. 一种面向 SDN 域内控制平面可扩展性的机制[J]. 小型微型计算机系统, 2013, 34(9): 1980-1983.
LIN P P, BI J, HU H Y, et al. MSDN: a mechanism for scalable intra-domain control plane in SDN[J]. Journal of Chinese Computer Systems, 2013, 34(9): 1980-1983.

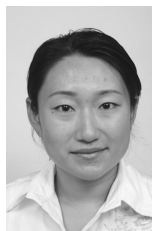
[作者简介]



郭春梅(1979-),女,北京启明星辰信息安全技术有限公司资深研究员,主要从事信息安全前沿技术研究工作,主要研究方向为网络安全、云计算/虚拟化技术及安全、物联网安全等。



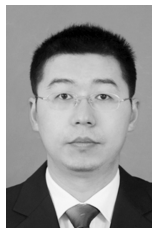
马骏（1976-），男，北京启明星辰信息安全技术有限公司检查本部副总经理，主要从事高级威胁检测、大数据审计、云安全、软件定义安全等研究工作，主要研究方向为网络安全、高级持续性威胁检测技术及云安全等。



张如辉（1978-），女，北京启明星辰信息安全技术有限公司资深研究员，主要研究方向为云计算/虚拟化技术及安全、安全标准等。



郭昊（1981-），男，全球能源互联网研究院工程师，主要研究方向为电力信息安全、攻防对抗技术、物联网安全等。



朱少敏（1983-），男，北京启明星辰信息安全技术有限公司行业专家，主要从事电力系统网络与信息安全技术研究工作，主要研究方向为电力二次系统安全防护、信息隐藏与大数据分析等。



毕学尧（1974-），男，北京启明星辰信息安全技术有限公司高级工程师，主要研究方向为云计算安全、网络安全防护体系等。



杨聪毅（1976-），男，北京启明星辰信息安全技术有限公司检测本部技术总监，主要研究方向为云计算/虚拟化技术及安全、网络入侵检测与防御体系等。