

基于 SDN 的智能安全接入平台研究

李鹏, 杨跃平, 杨扬

(国网浙江省电力有限公司宁波供电公司, 浙江 宁波 315010)

摘 要: 针对传统的安全服务设备安全服务升级难、扩展难的问题, 首先, 提出一种智能安全接入平台的设计方案; 然后, 阐述智能安全接入平台的研发思路及其技术路线, 并进行硬件设计和软件设计; 最后, 进行平台成果测试及部署建设。

关键词: 安全服务; SDN; 智能安全接入平台

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-8930.2023036

Research on Intelligent Security Access Platform Based on SDN

LI Peng, YANG Yueping, YANG Yang

State Grid Zhejiang Electric Power Co., Ltd., Ningbo Power Supply Company, Ningbo 315010, China

Abstract: Firstly, the difficulty of upgrading and expanding the traditional security service equipment were analyzed, and a design of an intelligent security access platform was proposed. Then, the research and development ideas and technical routes of the intelligent security access platform were explained, and hardware and software were designed. Finally, the platform achievement test and application deployment construction were carried out to verify the value of the platform.

Keywords: security service, SDN, intelligent security access platform

0 引言

传统通信网络是一个按需建设、静止且封闭的网络, 随着承载业务的多样化, 网络也越来越复杂, 随着云计算、物联网等新兴业务的出现和发展, 传统网络模式已经难以为继, 并严重阻碍了网络技术的发展和革新。转发面开放协议 (OpenFlow) 的出现, 打破了传统网络以硬件为主的发展模式, 软件开始成为了网络发展的主要驱动力, 软件定义网络 (Software Defined Network, SDN) 的概念开始在运营商、设备商、互联网厂商之间广为传播, 并掀起了一股研究和应用热潮。

随着对 SDN 研究的不断深入, SDN 技术已经延伸到了卫星互联网领域, 有效提高了卫星运营商的资源利用效率和业务响应速度, 可以为用户提供更多更好的服务, 并进一步发挥卫星网络在通信领域的优势。在当今瞬息万变的信息时代, 许多行业越来越依赖日益互联的各种网络,

企业和用户的重要信息都存储在数据中心, 这将带来网络安全严峻挑战。

内部攻击成为了内部安全最大的风险。在大数据、物联网技术、人工智能应用的推动下, 边缘计算的应用场景越来越多, 在靠近数据源或用户的地方提供计算、存储等基础设施, 并为边缘应用提供云服务和 IT 环境服务。相比于集中部署的云计算服务, 边缘计算解决了时延过高、汇聚流量过大等问题, 为实时性和带宽密集型业务提供了更好的支持。随着 5G 和工业互联网的快速发展, 新兴业务对边缘计算的需求十分迫切。在众多垂直行业新兴业务中, 对边缘计算的需求主要体现在时延、带宽和安全 3 个方面。在工业互联网、物联网、泛在电力物联网、综合能源站的接入端, 都需要更加灵活的网络接入设备。

安全是边缘计算的关键要素。首先, 有效的安全机制才能避免引入边缘计算应用对服务的影响; 其次, 只有从

技术和管理上切实保障边缘计算本身的安全,才能扫除第三方应用入驻边缘计算平台的顾虑;此外,入驻边缘计算平台的第三方应用通常需要通用的安全能力(如防火墙、IDS/IPS、WAP等)。完善的网络和信息安全机制,是边缘计算产业和生态健康发展的前提。

接入网关需要融合 ICT 技术、互联网技术,需要对各接入成分进行实时监测和分析,包括安全防御等。本文定义了一个基于 SDN 的工业级安全路由网关平台,硬件上采用“CPU+路由交换芯片”异构的网络架构,硬件全部采用国产化芯片,实现了安全及自主可控;功能上实现了网络安全入侵检测、防火墙、负载均衡、数据流分析和内容可视化监控。针对云时代的工业融合和工业 4.0 时代的网络需求,实现 SDN 管理和网络低时延,同时支持 IPv4 和 IPv6 网络协议。本文所提出的硬件成果可以应用于工业互联网、物联网、泛在电力物联网、综合能源站等场景。

1 智能安全接入平台研发思路及技术路线

1.1 研发思路

传统的安全服务设备与网络拓扑紧密耦合,需串联在网络拓扑中,配置复杂,且存在严重的单点故障,无法随业务安全需求的变更而变化,安全服务升级难、扩展难。本文所提方案采用 SDN 交换架构,实现了安全服务链,可实现基于用户身份、业务应用类型的网络流量按需防护,支持硬件安全服务和虚拟安全服务,用户可根据不同业务需求部署不同的硬件服务或网络功能虚拟化(Network Function Virtualization, NFV)节点(如虚拟防火墙、入侵检测、虚拟负载均衡等),按需编排服务节点形成安全服务链,在应用生命周期内为应用提供安全服务。

同时,本文所提方案支持安全服务弹性扩展,安全服务链支持网络功能服务类型智能感知,允许客户根据不同的业务需求,动态增删服务节点,高弹性服务链满足业务扩容、升级,同时解耦网络设备之间的关联。

在动态网络功能服务池,SDN 安全服务链支持 NFV 节点或硬件服务节点资源池化,客户可根据业务需求动态扩展资源池。业务流量大时,增加服务节点;业务流量小时,释放服务节点。这使得服务资源得到更合理的利用,极大降低网络投入和运维成本。

1.2 技术路线

本文所提方案在技术上采用了全部国产化硬件,包括国产 CPU 平台,CPU 负责计算、安全防范、信息分析和

识别,网络芯片支持路由交换,聚焦于下一代城域网、物联网等以太网的多业务融合应用,能够完美支持多种城域以太网业务,同时可满足园区网和企业网汇聚、数据中心千兆接入。对 IPv4/IPv6、多协议标记交换(Multi-Protocol Label Switching, MPLS)、多种隧道和多播协议的支持可以保证各种业务的灵活部署,而特有的低时延、低抖动特性则能够全面保证各种业务的服务质量。国产交换芯片具有千兆汇聚和万兆汇聚交换能力,可以提供多层交换能力和线速的路由转发能力。它除具有多层路由器的容量大、高速转发性能优点外,还进一步将 IP 网络安全机制等策略融合到整个路由器系统中,设备具有更多的智能安全特性,充分满足构建安全可控的 IP 网络的需求。

在当前的网络环境中分布式拒绝服务(Distributed Denial of Service, DDoS)攻击已经非常普遍,攻击流量能在几秒钟之内达到 Gbit 量级或者更大,要防御这些攻击比较困难。本文设计了一种有 SDN 参与的 DDoS 防护方案。检测服务器检测到攻击后,通过边界网关协议(Border Gateway Protocol, BGP)将报文牵引到旁挂的 OpenFlow 交换机,利用 OpenFlow 交换机修改合法报文的 IPDA(受 DDoS 攻击的 IPDA),将报文原路返回,修改 IPDA 的目的是防止发回到核心路由器后形成环路。

随着 Web 应用的兴起,负载均衡的应用需求得到了广泛关注。负载均衡不仅适用于 Web 需求,也越来越多地应用于其他场景中,成为 SDN 的重要应用。本文采用的国产 CPU 主控芯片,将从外部进来的报文负载均衡到旁路的安全设备上,进行其他应用处理。

2 智能安全接入平台硬件建设

智能安全接入平台硬件建设方案如下。

- 硬件平台主处理芯片采用国产 CPU 龙芯 3A4000 四核处理器,工作频率 1.5~2.0 GHz,设计功耗 60 W。
- 芯片组采用自主龙芯 7A1000 系列,支持双路 DIMM4-2400 内存,最大可支持 32 GB,支持差错校验(Error Checking and Correction, ECC)功能。
- 系统支持双路 SATA2.0,并支持 CF 卡读写。
- 双路 PCIeX8, 内置扩展槽,支持加密卡扩展。
- 多种输入电压方式:AC 220 V、DC 240 V、DC 48 V 可选。
- 电源支持 AT/ATX 触发。
- 平台集成 10 个千兆网口,采用 RJ45 电口+光口 SFP 混合配置。
- 硬件平台支持网络扩展模块。

3 智能安全接入平台软件建设

智能安全接入平台软件采用可信交换防御技术路线,自主建立网络访问流量模型并识别可信和非可信主客体,对普通区域、重点区域等各种逻辑网络进行分级划分和方位隔离,识别访问类型并对访问攻击进行拦截。

3.1 识别可信/非可信主客体

可信交换防御系统自动获取网络中的流量信息,判断各类网络资产之间的业务数据流量关系。通过一个阶段的东西向流量的自学习,并将这些信息汇总后,由策略计算绘制出一个完整的业务流模型图,辅助管理者对整个内网进行管理。

在自学习过程中,智能安全接入平台会根据识别策略列出相应的访问源IP/目的IP、端口号、数据流向;管理者通过该模型便可快速掌握网络中整个信息资产的逻辑应用关系图,该模型会将可信访问的主客体全部展现在管理者面前。

可信交换防御系统采用独有的专利技术——全息诱捕技术,可以在4层网络中虚拟出大量的虚拟IP和端口,从而形成海量高密度的陷阱主机,当攻击者访问陷阱主机的次数超过设定的次数时,将该IP认为非可信客体。

3.2 可信访问控制

可信交换防御系统通过自主流量建模后,会根据可信访问列表建立基于白名单的访问控制策略,把普通区域、重点区域等各种逻辑网络进行隔离,避免了不安全因素的扩散,只有合理地划分了网络区域,安全策略才可以更有效地实施。具体技术细节包括以下两点。

(1) 访问控制策略基于五元组的白名单模式,只允许某IP访问某IP的某个端口,其他皆不允许。

(2) 管理员可对策略进行自定义调整:添加,开启,关闭,对五元组进行调整、重构。

3.3 非可信主客体拦截

可信交换防御系统通过全息诱捕技术将非可信IP捕获后,有以下3种可能。

(1) 可信交换防御系统会立即拦截全息捕获的非可信IP,阻止其访问真实主机。

(2) 可信交换防御系统不会拦截非可信IP继续访问陷阱主机,继续让非可信IP对陷阱主机进行各种操作,不让非可信IP有所察觉,留存更多痕迹以便进一步观察和判断。

(3) 可信交换防御系统通过旁路方式部署时,可以与第三方主流交换机进行联动,当诱捕到非可信IP后,主动推送ALC到第三方交换机进行拦截、阻断。

3.4 攻击防御

可信交换防御系统内置了完善的2~7层攻击防御模块,基于攻击特征的检测技术对经过系统的流量进行过滤,实时发现并拦截各种已知的攻击,如系统漏洞利用、Web应用攻击、蠕虫木马等。

可信交换防御系统为客户定位各种网络威胁,以及违反安全策略的流量,并提供详实、有效的指导措施,进而实现防护—检测—响应一体化的解决方案。

3.5 引流功能

通过可信交换防御系统可以将来自内网和外网的流量引流至第三方交互式蜜罐或其他安全检测设备,以便进一步分析可疑流量。通过此种方法,无须用户在网络中部署大量的交互式蜜罐,可以大大降低部署交互式蜜罐的人力、物力和财力成本。

4 平台成果测试及部署建设

本文采用SDN交换架构实现了安全服务链,可实现基于用户身份、业务应用类型的网络流量进行按需防护,支持硬件安全服务和虚拟安全服务,用户可根据不同业务需求部署不同的硬件服务或NFV节点(如虚拟防火墙、入侵检测、虚拟负载均衡等),按需编排服务节点形成安全服务链,在应用生命周期内为应用提供安全服务。

同时,支持安全服务弹性扩展,安全服务链支持网络功能服务类型智能感知,允许客户根据不同业务需求,动态增删服务节点,高弹性服务链满足业务扩容、升级,同时解耦网络设备之间的关联。

在动态网络功能服务池,软件定义安全服务链支持虚拟化节点或硬件服务节点资源池化,客户可根据业务需求动态扩展资源池,业务流量大时,增加服务节点;业务流量小时,释放服务节点,使得服务资源得到更合理的利用,极大降低网络投入和运维成本。本接入平台有两种推荐部署及建设方式,分别对应不同的网络环境。

(1) 接入层分布式部署

对于新建网络环境,推荐采用接入层分布式部署,最大限度地保护内网安全。在此建设方案下,智能安全接入系统以接入层交换机的角色接入网络,交换口接入真实服务器或终端,将控制节点下沉到各服务器的接入端口,实现端到端级别的微隔离功能、全息诱捕功能,多个智能安全接入系统可以通过集群方式进行统一管控。

(2) 旁路部署

对于原有网络环境,采用旁路部署,大大加强现有网

络环境的安全防护。智能安全接入系统旁路部署方式,可通过开启全息诱捕功能,在所有网段部署陷阱主机进行诱捕,可将内网流量镜像至智能安全接入系统的镜像口,通过自学习功能可对内网的应用关系进行可视化展示,用作维护依据。

5 结束语

本文提出的基于 SDN 的智能安全接入平台,解决了传统的安全服务设备与网络拓扑紧密耦合,需串联在网络拓扑中,配置复杂,且存在严重的单点故障,无法随业务安全需求的变更而变化,安全服务升级难、扩展难的问题。经过平台成果测试及部署建设,验证了该平台可以为应用提供安全服务,在卫星互联网、工业互联网、物联网、泛在电力物联网、综合能源站等领域,具有一定的应用价值。

参考文献:

- [1] 周光涛, 郭爱鹏, 唐雄燕. SDN/NFV 技术在宽带 IP 城域网中的应用[J]. 信息技术, 2015, 9(2): 12-15.
- [2] 刁澜炯. 固网引入 SDN 助力运营商构建弹性、敏捷的宽带网络[J]. 通信世界, 2015(23): 37-38.
- [3] DIAO Y J. The introduction of SDN into fixed network helps operators to build flexible and agile broadband networks[J]. Communications World, 2015(23): 37-38.
- [4] 张朝昆, 崔勇, 唐嵩嵩, 等. 软件定义网络(SDN)研究进展[J]. 软件学报, 2015, 26(1): 62-81.
- [5] ZHANG C K, CUI Y, TANG H H, et al. State-of-the-art survey on software-defined networking (SDN)[J]. Journal of Software, 2015, 26(1): 62-81.
- [6] LEE S S W, LI K Y, WU M S. Design and implementation of a GPON-based virtual Open Flow-enabled SDN switch[J]. Journal of Lightwave Technology, 2016, 34(10): 2552-2561.
- [7] LEE S S W, LI K Y, LIU W K, et al. Embedding bandwidth-guaranteed network-based virtual Ethernet switches in SDN networks[J]. Journal of Lightwave Technology, 2017, 35(23): 5041-5055.