基于路径可查的真实源地址验证在园区网中的实现

王宇亮[1],周 耐[1],李宗鹏[1,2],国兴昌[1],李 康[1]
(1. 泉城实验室,山东 济南 250100;
2. 清华大学 网络科学与网络空间研究院,北京 100084)

摘 要:随着通信技术和新一代网络的发展,园区网在诸多现实场景中得到了越来越广泛的应用,其安全问题也引来诸多研究者的关注和研究。缺乏对带有安全威胁的源地址进行检测和追溯,很容易使得网络主机设备遭受攻击,引发一系列网络安全问题。为此,该文提出了基于路径可查的园区网络真实源地址验证框架。该框架首先建立对主机粒度源地址验证的嗅探,然后通过最短路径优先协议实现园区网内路由和交换机设备之间的信息同步,同时告知并记录主机流量数据路径传播信息,根据不同的接口类型构建黑白名单并生成信息表项和过滤查找表。此外,基于以上验证框架设计逻辑,设计了路由器原型样机,并在公开的网络设备测试基准 RFC2544 上进行实验测试,实验结果均表明该验证框架具有较显著的性能。该验证框架通过路径可查的报文信息动态同步名单过滤查询表,有效地解决了源地址的验证和溯源问题,避免了无源头安全威胁,实现了低时延、多协议可支持的园区网真实源地址验证。

关键词:园区网安全;源地址验证;源地址追溯;路径可查;动态同步
中图分类号:TP18 **文献标识码**:A **文章编号**:1673-629X(2025)04-0073-07
doi:10.20165/j.cnki.ISSN1673-629X.2024.0375

Realization of Source Address Validation Based on Path Queryability in Campus Networks

WANG Yu-liang[1], ZHOU Nai[1], LI Zong-peng[1,2], GUO Xing-chang[1], LI Kang[1]
(1. Quan Cheng Laboratory, Jinan 250100, China;
2. Institute for Network Science and Cyberspace, Tsinghua University, Beijing 100084, China)

Abstract: As the development of communication technology and new generation network, campus network has been more and more widely used in many real-life scenarios, and its security problems have attracted the attention and research of many researchers. Without detecting and tracking the source address with security threats, it is easy to make the network host devices suffer from attacks, which triggers a series of network security problems. To address that, we propose a source address validation architecture framework for campus network based on path queryability, which firstly needs to establish the sniffing for host granularity source address verification, and then realizes the information synchronization between the route and switch devices in the campus network through the Open Shortest Path First protocol, meanwhile, informs and records the information about the host traffic data path propagation, constructs the black and white lists according to different interface types and generates the information table entries and the filtering. In addition, based on the above design logic of the verification framework, we design a prototype router and conducts experimental tests on the publicly available network equipment test benchmark RFC2544, and the experimental results show that the proposed verification framework has a more significant performance. The authentication framework effectively solves the problem of authentication and traceability of the source address by dynamically synchronizing the list filtering lookup table with the path-queryable message information, avoids the source-less security threat, and achieves the low-latency, multi-protocol-supportable authentication of the real source address of the campus network.

Key words: campus network security; source address verification; source address traceability; path traceability; dynamic synchronization

收稿日期:2024-08-14 **修回日期**:2024-12-17
基金项目:泉城省实验室重点项目(QCLZD202304);山东省实验室项目(SYS202201)
作者简介:王宇亮(1980-),男,高级工程师,硕士,研究方向为网络空间安全、下一代互联网研究;通信作者:周 耐(1992-),男,助理研究员,博士,研究方向为网络空间安全、自然语言处理;李宗鹏(1977-),男,教授,博士,研究方向为计算机网络、网络算法、网络编码。

0 引 言

引言园区网是互联网体系结构中的重要一环,也是主机设备接入到骨干互联网中十分重要的部分,其广泛应用于校园、大型商城和企业园区等多个现实场景中。主机设备的软硬件和系统在设计阶段,总会因为一些人为因素不可避免地出现设计缺陷,很容易被利用作为导致安全问题的漏洞。由于接入园区网的主机设备复杂多样,安全风险也随之增加,发送端设备在发送数据信息时很有可能伪造其真实的源地址,即源地址欺骗。近些年来,因为缺乏对源地址的检测和追溯,导致以分布拒绝服务(DDoS)、木蠕僵、恶意程序等网络攻击严重危害网络安全。据中国国家信息安全漏洞共享平台(CNVD)统计(https://www. cnnvd. org. cn/home/childHome),国内每月遭受的安全漏洞高达 2 000 余个。攻击者利用源地址欺骗可以成功地隐藏自己行为与信息,并将安全事故的责任转嫁给其他网络目标。在园区网中,通常花费大量的人力和物力识别攻击问题,也很难成功完成对攻击者的真实源地址进行追踪溯源。

为了解决源地址验证问题,近些年来,学术界在真实源地址验证方案的设计方面展开了大量的研究工作和工程实现[1-4]。SAVA(Source Address Validation Architecture)和 SAVI(Source Address Validation Implement)[1]是清华大学提出的一套真实源地址验证体系架构。基于以上体系架构,同时为了解决园区网中真实源地址的检测和溯源问题,该文提出了一种基于路径可查的真实源地址验证方案(Source Address Validation Based on Path Queryability,SAVPQ),并在园区网的内生安全机制中成功实现。SAVPQ 部署在园区网内的路由器上,首先通过源地址合法验证实现主机粒度源地址验证的嗅探,然后在边界路由协议中嵌入数据流路径传播信息,生成路径信息可查的 SAVPQ 表项,并且在路由器之间分布式动态同步并管理可信前缀信息。SAVPQ 在可编程交换芯片上实现,在保障表项同步和表项安全的同时,具有低时延、低丢包率以及低资源等优势。路由和交换机设备可以根据本地路由和远端同步路由生成全局视角下的动态认证规则,高效准确地检测和溯源园区网中的源地址。

1 相关工作

近年来,随着“下一代互联网”的研究发展,网络安全得到越来越多的重视,有关源地址验证的研究工作不断涌现[5-16]。早期重要的源地址验证方案主要包括基于加密认证、基于报文过滤和基于事后追溯的验证类型[17-22]。Kent 等[18]提出了一种主机粒度的端到端认证通信协议,利用封装安全载荷协议对传输数据的分组报文封装,然后采用私钥签名得到封装后报文的 Tag 值并标记到认证头内,最后通过校验目的端认证头保障数据传输安全性,但是该方案计算开销庞大,很难得到广泛应用。Bremler 等[19]提出了基于密钥认证的源地址验证方案,该方案通过建立安全联盟体系对发送的合法数据添加其与目的端预先商定的密钥标签 Tag,然后利用目的网络的边界路由器进行验证,该方案虽然部署简单,但是联盟成员无法区分外向内的反射式攻击。Jin 等[20]提出一种基于报文过滤的源地址验证方案,利用报文传输路径长度实现被动端的系统防御,通过建立 IP 地址与路径跳数的映射表和 IP 报文中的生存时间值判断合法报文的真伪性,保障传输数据的真实性。PPM[21]和 DPM[22]都是基于时序追溯的验证方案,前者 Savage 等将部分路径信息概率写入报文首部,通过重构攻击路径实现溯源定位;后者 Belenky 等则对传输的 IP 报文进行包标记,受攻击端通过维护源 IP 地址索引的入口表抉择是否转发接受数据。

针对以上早期的验证方案的不足,很多研究工作进行了改进[23-27]。Duan 等[23]提出了基于数据隐私验证框架的方案,该方案利用边界路由协议通过交换方式通告邻居路由信息的改变,并根据更新的路由信息鉴别传输数据的合法性。Li 等[26]则提出路由通信协议,该协议首先在路由器上建立源地址和入接口的映射关系,然后通过周期性地更新边界路由设备的映射关系变化,利用动态的路由映射表验证并过滤路由信息的匿名包。为了减小储存开销,Lee 等[27]对 SAVE 方案进行了改进,利用源地址与标记值的映射关系表来过滤伪造报文。此外,还有 RPF[28]、uRPF[29]等一系列源地址验证原理方案的改革研究工作。然而,以上方案大多数都是针对域间网络进行源地址验证,且普遍存在部署难度较大、实施复杂度较高、计算开销较大等问题。

针对以上问题,同时便于在园区网中部署,该文提出了基于路径可查的源地址验证方案。与现有工作相比,SAVPQ 方案在边界路由协议中嵌入数据流路径传播信息,利用合法用户前缀、前缀长度、绑定的接口和路径信息共同生成 SAVPQ 表项,并在可编程交换芯片上实现。该方案在实现源地址验证的同时,有效保障了表项同步和表项安全,还确保了低丢包率和转发时延,在资源占用较少和丢包率极低的情况下,实现了高吞吐量。在园区内网络拓扑结构中,边界路由器通过边界路由协议更新生成携带路径传播信息的全局状态下的表项,保证流出该园区网络内的流量数据采用的是真实的源地址,同时确保园区网内各个管理域之间互相访问,针对各个主机设备的源地址信息验证可

以共享,确保对园区网内所有主机设备的源地址可以有效地验证和溯源。

2　方　法

2.1　SAVA 技术

SAVA(源地址验证框架)是清华大学在 2008 年提出的一套真实源地址验证体系架构,该架构按照验证粒度从粗到细分为域间、域内和接入网等三个层次。SAVA 部署在骨干网络和接入网络之间的边界设备上,提供 IPv6 前缀粒度的保护能力,为主机设备的安全提供保障,其在域内网络上的拓扑结构示意图如图 1 所示。接入网络的用户通过设备 A 接入到边界设备 B 和 C。边界设备 C 依次经过设备 D、边界设备 B、设备 A 路径到接入网络;接入网络则经过设备 A 路径到边界设备 C。图中黑色实心圆表示部署 SAVA 功能的接口,开启 SAVA 功能后,接入网中所有合法前缀的用户报文均可以在任意边界设备上,通过源地址验证进行数据接受和转发。

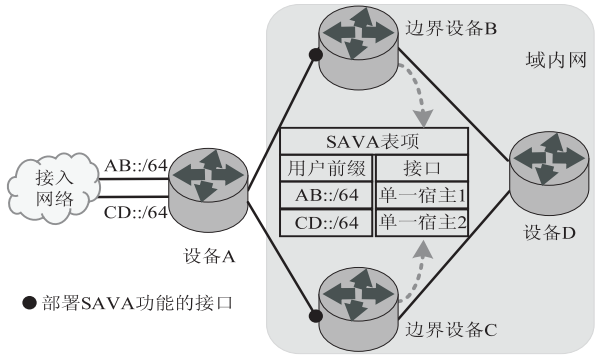

图 1　SAVA 在域内网络上的拓扑结构示意图

在园区网网络中,真实源地址验证虽然可以提供主机粒度的源地址验证,可以确保核心设备避免遭受网络攻击,但是当可信任主机出现安全问题时,真实源地址的追踪溯源仍然是值得关注的问题。SAVA 的出现为园区网 IPv6 源地址的追踪溯源提供了坚实的基础。在此基础之上,该文提出了基于路径可查的真实源地址验证方案,并在园区网中成功实现。

2.2　基于路径可查的真实源地址验证方案

基于路径可查的真实源地址验证方案是一种基于 SAVA 的安全验证框架,主要部署在园区网络拓扑中的核心交换机上。以校园网络为例,对于宿舍区、办公区、教学区、业务资源区以及安全管理区的接入交换机,还包括与校区专线互联网、互联网区连接部分的核心交换机,在以上交换机上加入本文提出的源地址验证框架。在校园各个区域网络中,每个主机设备都需要通过接入交换机实现双向流量的交互访问。其中,复杂多样的接入设备无形中对网络安全带来了严峻的挑战。当携带安全隐患的主机设备接入网络时,会对其他设备造成损害。即时有效地检测出携带安全隐患的流量信息接入网络,可以阻止网络攻击的传播。同时,追溯该流量信息的始发主机,可以从源头上对安全隐患进行处理。

2.3　方案设计

为了验证和追溯真实源地址,要基于源地址都是真实,即所有的网络成员都是真实可信的。在接入交换机上部署 SAVI 真实源地址验证,确保用户接入层源地址的有效性。在此基础之上,该文设计了基于路径可查的真实源地址验证方案,通过查询信息传输路径使得交换机或路由器能够识别园区内网络中所有主机的传输信息。以校园网场景为例,在各个功能区域内的所有接入交换机上部署 SAVI 功能,以及在所有的路由器和边界网关设备上部署 SAVPQ 功能,并通过可信前缀学习体系结构、SPA 报文等生成带路径信息的 SAVPQ 表项。

SAVPQ 方案的具体流程如图 2 所示,在所有接入交换机 A 和 B 上部署 SAVI 功能,针对连接的主机通过手工配置、DHCPv6 方式或者无状态自动配置方式动态分配地址。接入交换机的 SAVI 功能通过对报文源 IPv6 地址的合法性审查实现主机粒度源地址验证。该验证过程如下:

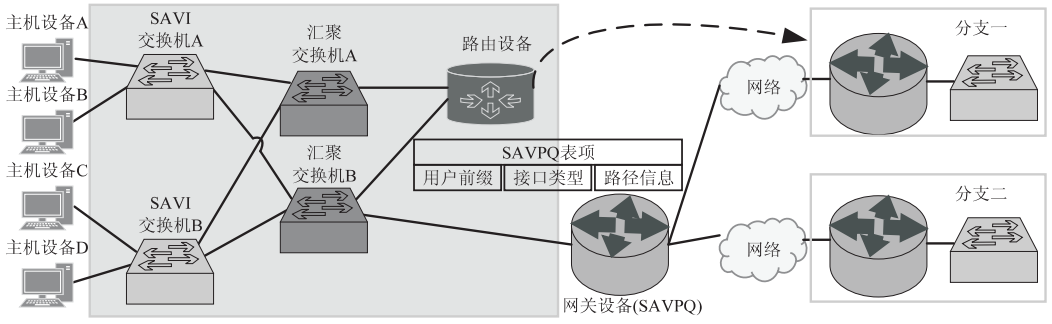

图 2　SAVPQ 方案具体流程

(1)在接入交换机 A 和 B 上配置 DHCPv6 Snooping 功能,在连接 DHCPv6 客户端接口上开启 DHCPv6 Snooping 地址表项记录功能,并通过该功能生成 DHCPv6 Snooping 表项。

(2)在接入交换机 A 和 B 上配置 ND Snooping 功能,并通过该功能生成 ND Snooping 表项。

(3)在接入交换机 A 和 B 上开启 SAVI 功能,使得该交换机利用生成的安全表项对 DHCPv6 协议报文、ND 协议报文和 IPv6 数据报文进行源地址合法性检验,过滤非法的报文,从而实现主机粒度源地址验证的嗅探。

在完成主机粒度的源地址验证后,通过 OSPFv3 协议将合法的主机信息报文同步给园区网内其他交换机和路由设备,同时记录主机流量传播路径信息。在网关和路由设备上部署 SAVPQ 功能,通过 VXL-AN 等技术实现跨园区网通信,同时部署支持在基于 BGP4+协议扩展的 SAVPQ 功能路由器,实现跨园区网的真实源地址验证。园区网内部署 SAVPQ 功能的路由器,按接口类型生成 SAVPQ 表项。

(1)针对单一宿主接口,本地路由表中以本接口为出接口的前缀进行构建,生成 SAVPQ 白名单。

(2)针对完全的多宿主接口,本地路由表中以本接口为出接口的前缀、SPA 报文中相同接口类型的前缀和本路由器上其它相同类型接口下的前缀进行构建,生成 SAVPQ 白名单。

(3)针对非完全的多宿主接口,本地路由器对接收到的 SPA 报文内的以上两种类型接口下的 SAVPQ 白名单中的前缀进行构建,转换并生成本接口下的黑名单。

(4)互联网接口设计与非完全多宿主接口相同。

根据以上接口类型生成 SAVPQ 表项的过程如下:边界网关设备分别从到达网络的路由信息和本地学习的信息中获取主机设备报文的前缀,以及传输路径信息。路由设备为到达接入网络的主机设备的路由信息打上特定的 Tag,并相互交换信息,同时利用 BGP4+将该路由信息引入到园区网络的动态路由协议中。边界网关设备通过动态路由协议学习到边缘路由器发布的带有特定 Tag 的路由信息。边界网关设备根据通过动态路由协议学习到的路由信息携带的 Tag 值和边界路由上配置的同步远端路由条目中的 Tag 值是否相同,生成具有白名单的 SAVPQ 表项,该表项信息包含合法用户前缀、前缀长度、绑定的接口和路径信息。

黑白名单使用数据包的源地址和入接口号进行表项匹配,其中源地址使用最长前缀匹配、入接口号使用精确匹配的方式,由于该方案使用的是可编程交换芯片,在数据平面上使用 TCAM 进行匹配。该名单保存在控制平面和数据平面中,在控制平面上使用 BGP、SAVPQ 和本地的路由信息进行表项的添加、删除、更新。BGP 利用 MD5 身份验证、BGPsec 等机制保障源地址表项的安全传递,控制平面仅使用直连路由生成源地址验证表项,数据平面和控制平面使用背板通信,背板不转发入站和出站流量,可以有效保障表项同步和表项安全。SAVPQ 表项生成过程中,在路由之间建立的可信前缀学习体系结构如图 3 所示。部署 SAVPQ 代理的源实体路由器 A 和 B 之间的通信,在路由器 A 的信息发送端发送携带源地址验证特殊信息,并通过信道传送给路由器 B 的接收端。然后路由器 B 根据路由表/转发表通过 SAVPQ 代理对源地址进行验证,完成两个源实体之间的通信。

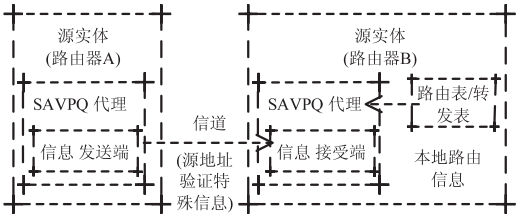

图 3 可信前缀学习体系结构

2.4 SAVPQ 路由器原型样机设计与实现

通过以上方案设计,该文开发了基于路径可查的真实源地址验证路由器原型样机,并在园区网中进行了实际的应用和验证,该设备软硬件体系结构如图 4 所示。

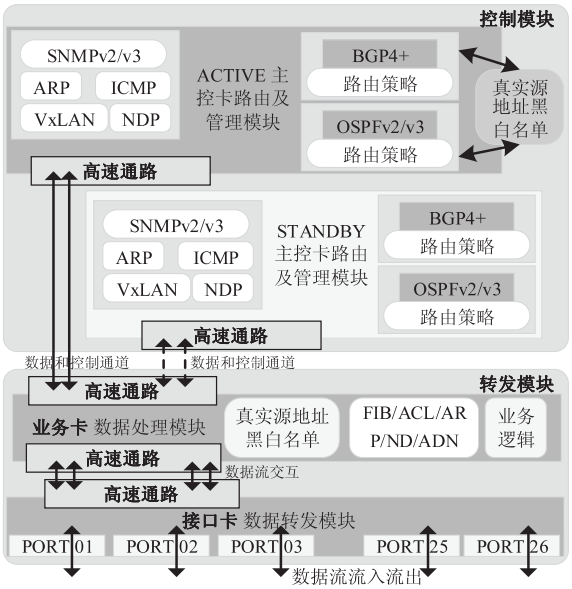

图 4 SAVPQ 设备软硬件体系结构

在图 4 中,带有 SAVPQ 功能的设备体系结构主要包括控制模块和转发模块,两个模块通过高速通路实现数据流的传输和相互控制的实现。在控制模块中,ACTIVE 主控卡路由及管理模块嵌入 BGP4+和 OSPFv2/v3 协议,该协议包括路由策略、路径可查信息以及真实源地址的黑白名单;此外还包括网络管理标准协议(SNMP)、地址解析协议(ARP)、网络控制报文协议(ICMP)、虚拟扩展局域网(VxLAN)和邻居发现协议(NDP)等一系列网络协议。STANDBY 主控卡路由及管理模块与 ACTIVE 主控卡路由及管理模块的结构基本类似,主要用于数据备份。在转发模块中,业务卡

数据处理模块包括真实源地址黑白名单、FIB/ACL/ARP/ND/ADN 和业务逻辑等功能协议。接口卡数据转发模块通过高速通路与业务卡数据处理模块实现数据流交互,并通过多个端口与外部设备实现数据流的流入流出功能。

3　实验及分析

实验以 Linux 系统作为开发平台,包括 2 个主控卡、2 个数据卡和 4 个接口卡。其中,主控卡配置为主频 2.7 GHz 6 核的 CPU、DDR4 32 GB 内存、SSD 500 GB 硬盘和 2 个 10 GE 带宽的网卡;数据卡配置为主频 2.2 GHz 4 核的 CPU、DDR4 16 GB 内存、SSD 128 GB 硬盘、10 GE 带宽的网卡和 SDE 服务器处理程序。实验采用的测试仪型号为 Spirent M1-KIT-23 -START.

3.1　生成的本地 SAVPQ 表项

本地 SAVPQ 表项的生成主要包括静态表项和本地路由转化两个部分,其各自的实现如图 5 所示。在图 5 左侧部分,在配置静态表项中,在 ipv6 地址 2100::/64 上,首先在 port4-1 接口添加静态白名单表项,并用类型 S 表示为静态表项。同时生成的黑名单表项,并用类型 X 表示黑名单条目,例如 port4-13 的类型为 X,表明 port4-13 是黑名单条目,禁止流量信息传输。

配置静态表项	本地路由转化
#ipv6 savpq 2100::/64 port4-1	# ipv6 savpq enable & int port4-1 & no shutdown
# do sh sav al	# ipv6 address 2001::1/64 & ipv6 savnet miig single_homing & do sh sav int
---LOCAL SAVNET ALLOW TABLE--- Codes: K-kernel route gen, C-Connected route gen, S-static entry, G-static route gen, O-OSPF gen, I- IS-IS gen, B-BGP gen, P-savnet spa, A-Babel gen, > - Selected entry, *-P4 Entry Prefix Allow Interfaces Lock C>* 2001::/64 port4-1 1 S>* 2100::/64 port4-1 1	Interface Miig-Type Miig_tag Status port4-1 single_homing NULL Link up
# do sh sav bl	# do sh sav al
---LOCAL SAVNET BLOCK TABLE--- Codes: X - blcok entry, >-selected entry, * - P4 Entry Prefix Block Interfaces X>* 2001::/64 port4-13 X>* 2100::/64 port4-13	Prefix Allow Interfaces Lock C>* 2001::/64 port4-1 1
	# int port4-13 & no shutdown & ipv6 address 2013::1/64
	# ipv6 savpq miig internet & do sh sav int
	Interface Miig-Type Miig_tag Status port4-1 single_homing NULL Link up port4-13 internet NULL Link up
	# do sh sav al
	-LOCAL SAVNET BLOCK TABLE- Codes: X-blcok entry, >-selected entry, * - P4 Entry Prefix Block Interfaces X>* 2001::/64 port4-13

图 5　静态表项配置和本地路由转化实现

在图 5 右侧部分,在本地路由转化中,在 ipv6 地址 2001::/64 上,单归属接口转换过程首先启动 SAVPQ 功能,并将 port4-1 接口设置为单归属接口,Miig-type 类型为 single_homing,在生成的白名单中类型为 C,表示该接口是由直连路由转换生成。互联网接口转换过程,在 ipv6 地址 2013::1/64 上,首先将 port4-13 接口设置为互联网接口,Miig-type 类型为 internet,同时生成黑名单表项,例如 ipv6 地址 2001::/64 的 port4-13 黑名单条目,并设置类型为 X.

3.2　BGP 中的 SAVPQ 表项信息

以 BGP4+协议为例,宣告本地 SAVPQ 表项过程如下:路由器 A 将两条白名单表项下发至 BGP 的 SAVPQ 信息表,然后通过携带 SPA 消息的 BGP UPDATAE 报文的 MP_REACH_NLRI 发送给路由器 B。学习邻居 SAVPQ 表项的过程为:路由器 B 的 SAVPQ 管理模块配置一个互联网接口,该路由器先解析 SPA 报文,然后将报文保存到 BGP 的 SAVPQ 信息表中。路由器 B 将两条通过 SPA 报文生成的 SAVPQ 信息下发至 SAVPQ 管理模块,生成两条黑名单。以上运行结果如图 6 所示。

```
----------BGP SAVPQ TABLE----------
Codes: C - connected route gen, S - static entry, G - static route gen,
       O- OSPF gen, I - IS-IS gen, B - BGP gen,
       P - savnet spa, > - selected entry,
Prefix          Allow Interfaces  Miig Type  Miig Tag  Origin  Origin Route ID
C>* 2001::/64   port4-1           1          0         S       10.0.0.17
S>* 2100::/64   port4-1           1          0         S       10.0.0.17
==========
----------BGP SAVPQ TABLE----------
Codes: C - connected route gen, S - static entry, G - static route gen,
       O- OSPF gen, I - IS-IS gen, B - BGP gen,
       P - savnet spa, > - selected entry,
Prefix          Allow Interfaces  Miig Type  Miig Tag  Origin  Origin Route ID
P>* 2060::/64   0                 1          0         P       10.0.0.17
P>* 2070::/64   0                 1          0         P       10.0.0.17
==========
----------LOCAL SAVPQ BLOCK TABLE----------
Codes: X - blcok entry, > - selected entry, * - P4 Entry
Prefix          Block Interfaces
X>* 2060::/64   port4-13
X>* 2070::/64   port4-13
```

图 6　学习邻居 SAVPQ 表项

3.3　性能测试以及表容量测试

在园区网的关键路由设备上部署 SAVPQ 框架功能后,该文采用公开的网络设备测试基准 RFC2544(Benchmarking Methodology for Network Interconnect Devices),设置一系列不同的帧长(86,128,256,512,1 024,1 280,1 518),分别对背靠背帧测试、时延测试、吞吐量测试以及资源占用等方面对 SAVPQ 框架的性能进行测试。背靠背帧测试结果如表 1 所示。在所有不同帧长情况下,设置发送时间为 30 秒,当突发流量为 10 G 时,均未发生丢包。以上结果表明部署 SAVPQ 功能的网络框架存储转发能力可以达到 10 G。

表 1　背靠背帧测试结果

Frame Size/bytes	Back-to-Back Burst/frames	Back-to-Back Time/s	Average Frame Rate/fps	Average Lost Frames
86	707547170	30	23584905	0
128	506756758	30	16891891	0
256	271739132	30	9057971	0

续表 1

Frame Size/ bytes	Back-to-Back Burst/frames	Back-to-Back Time/s	Average Frame Rate/fps	Average Lost Frames
512	140977444	30	4699248	0
1 024	71839082	30	2394636	0
1 280	57692308	30	1923076	0
1 518	48764630	30	1625487	0

时延测试结果如表 2 所示。在 10 G 流量传输情况下,随着帧长增加,时延时间略微有点增加。但是,在不同的帧长情况下,均未发生较大的时延,这也表明该文设计的方案在实际中具有较好的时延性能。

表 2 时延测试结果

Frame Size/ bytes	Load /%	Frame Loss /%	Min Latency /μs	Avg Latency /μs	Max Latency /μs
86	100	0	6.235	6.318	6.612
128	100	0	6.365	6.436	6.7
256	100	0	6.572	6.685	6.957
512	100	0	7.053	7.148	7.402
1 024	100	0	8.063	8.129	8.345
1 280	100	0	8.475	8.598	8.832
1 518	100	0	8.943	9.014	9.26

吞吐量的测试结果如表 3 所示。该文设计了 10 G 流量的转发,在所有帧长情况下,流量转发通过率均为 100%,同时帧丢失均为 0。以上结果表明,部署 SAVPQ 功能的设备在保证不丢包的情况下,数据流量传输量可达到 10 G。

表 3 吞吐量测试结果

Frame Size/ bytes	Load /%	Throughput /%	Max Latency Threshold Exceeded	Out of Seq Threshold Exceeded	Frame Loss	Forwarding Rate/fps
86	Passed	100	False	False	0	23584906
128	Passed	100	False	False	0	16891892
256	Passed	100	False	False	0	9057971
512	Passed	100	False	False	0	4699248
1 024	Passed	100	False	False	0	2394636
1 280	Passed	100	False	False	0	1923077
1 518	Passed	100	False	False	0	1574691

为了测试 SAVPQ 功能对数据转发时延的影响,在 SAVPQ 路由原型机上进行实验,第一次不开启 SAVPQ 功能,不对流量进行源地址认证,第二次启动 SAVPQ 源地址验证功能。该文设置添加 6 000 条表项,转发的流量随机命中 6 000 条表项中的 10 条,使用 RFC2544 的测试标准对帧长 86 ~ 1 518 的数据包在 1 Gbps 至 10 Gbps 的速率下进行转发时延测试。实验结果如表 4 所示。在绝大多数情况下,硬件设备开启 SAVPQ 功能的转发时延比未开启 SAVPQ 功能时增加了 0.05 ~ 0.06 微秒。在数据包速率为 7 Gbps,帧长为 1 024 时,开启 SAVPQ 功能的时延增加最大,为 0.08 微秒。以上实验结果表明,硬件开启 SAVPQ 功能的转发时延几乎可以忽略,即对数据包的转发时延几乎没有影响。

表 4 是否开启 SAVPQ 功能在硬件上的时延对比 μs

数据包速率\帧长 /Gbps	未开启 SAVPQ 功能							开启 SAVPQ 功能						
	86	128	256	512	1 024	1 280	1 518	86	128	256	512	1 024	1 280	1 518
1	5.153	5.175	5.278	5.374	5.485	5.549	5.627	5.159	5.181	5.284	5.38	5.491	5.556	5.632
2	5.153	5.176	5.279	5.374	5.485	5.549	5.627	5.159	5.182	5.284	5.38	5.491	5.556	5.633
3	5.153	5.176	5.279	5.374	5.485	5.549	5.627	5.159	5.182	5.284	5.38	5.491	5.556	5.633
4	5.153	5.176	5.279	5.374	5.485	5.549	5.627	5.160	5.182	5.284	5.38	5.491	5.556	5.633
5	5.153	5.175	5.278	5.374	5.485	5.549	5.626	5.160	5.182	5.284	5.38	5.491	5.556	5.633
6	5.153	5.176	5.279	5.374	5.485	5.549	5.627	5.159	5.183	5.284	5.38	5.491	5.556	5.633
7	5.153	5.176	5.279	5.374	5.485	5.549	5.627	5.159	5.182	5.284	5.38	5.493	5.556	5.633
8	5.153	5.176	5.279	5.374	5.485	5.549	5.627	5.160	5.182	5.284	5.38	5.491	5.556	5.633
9	5.154	5.176	5.279	5.374	5.485	5.549	5.627	5.159	5.183	5.286	5.38	5.491	5.556	5.633
10	5.153	5.176	5.279	5.374	5.485	5.549	5.628	5.160	5.183	5.284	5.38	5.491	5.555	5.632

4 结束语

针对园区网络安全,提出基于路径可查地源地址验证方案。在 SAVA 基础上,首先引入路径传播信息,构建可信前缀学习体系;接着扩展边界路由协议,分布式动态同步并管理园区内网络的前缀信息;然后综合本地路由和远端同步路由获取带路径传播信息 Tag 的路由信息,并生成过滤表项。在该方案中,黑白名单需要根据不同的接口类型和传播路径信息进行构建。并且,路径信息写在边界路由协议中,可以随路由协议全局动态更新过滤表项,同时避免占用多余的存储资源。实际部署后,多项指标的实验结果均表明该

验证方案具有低时延、高存储转发、高吞吐量的优点,在保证精确过滤的同时资源占用没有增加,避免了网络资源的额外负担。

参考文献:

[1] WU J P,BI J,LI X,et al. A source address validation architecture (SAVA) testbed and deployment experience[S]. RFC5210,2008.

[2] 吴建平,任　罡,李　星. 构建基于真实 IPv6 源地址验证体系结构的下一代互联网[J]. 中国科学:技术科学,2008,38(10):1583-1593.

[3] 毕　军,吴建平,程祥斌. 下一代互联网真实地址寻址技术实现及试验情况[J]. 电信科学,2008,24(1):11-18.

[4] 李　丹,秦澜城,吴建平,等. 基于边界路由动态同步的互联网地址域内真实源地址验证方法[J]. 电信科学,2020,36(10):21-28.

[5] 吴建平,吴　茜,徐　恪. 下一代互联网体系结构基础研究及探索[J]. 计算机学报,2008,31(9):1536-1548.

[6] WU J P,BI J,BAGNULO M,et al. Source address validation improvement (SAVA) framework[S]. RFC7039,2013.

[7] BI J,WU J P,YAO G,et al. Source address validation improvement (SAVI) solution for DHCP[S]. RFC7513,2015.

[8] BI J,YAO G,HALPERN J,et al. Source address validation improvement (SAVI) for mixed address assignent method sscenario[S]. RFC8074,2017.

[9] VIJAYALAKSHMI M,NITHYA N,SHALINIE S M. A novel algorithm on IP traceback to find the real source of spoofed IP packets[C]//Artificial intelligence and evolutionary algorithms in engineering systems. Kumaracoil:Springer,2015:79-87.

[10] SURESH S,RAM N S. Feasible DDoS attack source traceback scheme by deterministic multiple packet marking mechanism[J]. The Journal of Supercomputing,2020,76(6):4232-4246.

[11] YU S,ZHOU W L,GUO S,et al. A feasible IP traceback framework through dynamic deterministic packet marking[J]. IEEE Transactions on Computers,2015,65(5):1418-1427.

[12] CHEN G L,HU G W,JIANG Y,et al. SAVSH:IP source address validation for SDN hybrid networks[C]//IEEE symposium on computers and communication (ISCC). Messina:IEEE,2016:409-414.

[13] ALSABEH A. A survey on security applications of P4 programmable switches and a STRIDE-based vulnerability assessment[J]. Computer Networks,2022,207:108800.

[14] ZHANG Zhiyi. Revealing protocol architecture's design patterns in the volumetric DDoS defense design space[J]. IEEE Communications Surveys & Tutorials,2024.

[15] LIU Yihe,SHUANG Zhang. Information security and storage of Internet of Things based on block chains[J]. Future Generation Computer Systems,2020,106:296-303.

[16] ROTHENBERGER B. PISKES:pragmatic internet-scale key-establishment system[C]//Proceedings of the 15th ACM Asia conference on computer and communications security. New York:Association for Computing Machinery,2020:73-86.

[17] CHEN Y H,CHEN X,TIAN H,et al. A blind detection method for tracing the real source of DDoS attack packets by cluster matching[C]//Proceeding of the 8th IEEE international conference on communication software and networks. Beijing:IEEE,2016:551-555.

[18] KENT S,SEO K. Security architecture for the internet protocol[S]. RFC4301,2005.

[19] BREMLER-BARR A,LEVY H. Spoofing prevention method[C]//Proceeding of the 24th annual joint conference of the IEEE computer and communications societies. Miami:IEEE,2005,536-547.

[20] JIN C,WANG H N,SHIN K G. Hop-count filtering:an effective defense against spoofed DDoS traffic[C]//Proceedings of the 10th ACM conference on computer and communications security. Washington,DC:ACM,2003:30-41.

[21] SAVAGE S,WETHERALL D,KARLIN A,et al. Network support for IP traceback[J]. IEEE/ACM Transactions on Networking,2001,9(3):226-237.

[22] BELENKY A,ANSARI N. IP traceback with deterministic packet marking[J]. IEEE Communications Letters,2003,7(4):162-164.

[23] DUAN Z,YUAN X,CHANDRASHEKAR J. Constructing inter domain packet filters to control IP spoofing based on BGP updates[C]//25th IEEE international conference on computer communications. Barcelona:IEEE,2007:1-12.

[24] ALSULAMI H. Implementation analysis of reliable unmanned aerial vehicles models for security against cyber-crimes:attacks,tracebacks,forensics and solutions[J]. Computers and Electrical Engineering,2022,100:107870.

[25] PATIL R. A hybrid traceback based network forensic technique to identifying origin of cybercrime[J]. Journal of Engineering Science & Technology Review,2022,15(6):28-34.

[26] LI J,MIRKOVIC J,WANG M Q,et al. SAVE:source address validity enforcement protocol[C]//Annual joint conference of the IEEE computer and communications societies. New York:IEEE,2002:1557-1566.

[27] LEE H,KWON M,HASKER G,et al. BASE:an incrementally deployable mechanism for viable IP spoofing prevention[C]//ACM symposium on information,computer and communications security. Singapore:ACM,2007:20-31.

[28] WIJNANDS I J,BOERS A,ROSEN E. The reverse path forwarding (RPF) vector TLV[S]. RFC5496,2009.

[29] BAKER F,SAVOLA P. Ingress filtering for multihomed networks[S]. RFC3704,2004.