(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 114531270 A
(43)申请公布日 2022.05.24

(21)申请号 202111671863.8

(22)申请日 2021.12.31

(71)申请人 网络通信与安全紫金山实验室
地址 211100 江苏省南京市江宁区秣周东路9号
申请人 国家数字交换系统工程技术研究中心

(72)发明人 荆文韬 江逸茗 张进 唐寅

(74)专利代理机构 江苏圣典律师事务所 32237
专利代理师 梅学兵

(51)Int.Cl.
H04L 9/40(2022.01)
H04L 45/00(2022.01)

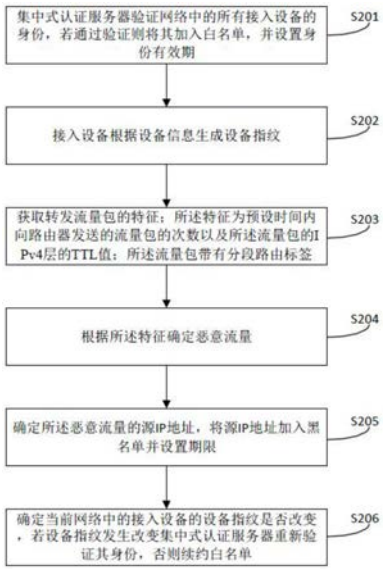
权利要求书2页 说明书8页 附图4页

(54)发明名称

针对分段路由标签探测的防御方法及装置

(57)摘要

本发明公开了一种针对分段路由标签探测的防御方法及装置，其中防御方法包括：集中式认证服务器验证网络中的所有接入设备的身份；接入设备根据设备信息生成设备指纹；获取转发流量包的特征；所述特征为预设时间内向路由器发送的流量包的次数以及所述流量包的IPv4层的TTL值；根据所述特征确定恶意流量；确定所述恶意流量的源IP地址，将源IP地址加入黑名单并设置期限；确定当前网络中的接入设备的设备指纹是否改变；本发明通过获取转发流量的频率以及数据包中IPv4层的TTL值来判断恶意流量，从而对其进行防御，这样可以精确防御分段路由标签探测的攻击，可以提高目标网络的安全性，减少了网络被破坏的可能。



CN 114531270 A

1.一种针对分段路由标签探测的防御方法,其特征在于,包括:

集中式认证服务器验证网络中的所有接入设备的身份,若通过验证则将其加入白名单,并设置身份有效期;

接入设备根据设备信息生成设备指纹;

获取转发流量包的特征;所述特征为预设时间内向路由器发送的流量包的次数以及所述流量包的IPv4层的TTL值;所述流量包带有分段路由标签;

根据所述特征确定恶意流量;

确定所述恶意流量的源IP地址,将源IP地址加入黑名单并设置期限;

确定当前网络中的接入设备的设备指纹是否改变,若设备指纹发生改变集中式认证服务器重新验证其身份,否则续约白名单。

2.根据权利要求1所述的防御方法,其特征在于,接入设备根据设备信息生成设备指纹,进一步包括:

接入设备利用设备信息做哈希;所述设备信息包括系统的进程、开放的端口、开启的服务、依赖库、硬件版本、系统版本、软件版本和设备配置中的一项或多项;

根据哈希生成设备指纹。

3.根据权利要求1所述的防御方法,其特征在于,在获取转发流量包的特征,之前还包括:确定当前网络是否拥塞,若拥塞,则镜像通过路由器的流量,优先让流量拥塞的路由器快速转发流量。

4.根据权利要求1所述的防御方法,其特征在于:所述恶意流量包的特征为预设时间内多次向路由器发送的流量包且该流量包的IPv4层的TTL值为1。

5.根据权利要求1所述的防御方法,其特征在于,集中式认证服务器验证网络中的所有接入设备的身份,进一步包括:

集中式认证服务器通过密码验证网络中的所有接入设备的身份。

6.根据权利要求5所述的防御方法,其特征在于:身份验证在设备上进行认证或在控制器上统一认证。

7.一种针对分段路由标签探测的防御装置,其特征在于,包括:

验证单元,用于验证网络中的所有接入设备的身份;若通过验证则将其加入白名单,并设置身份有效期;

生成单元,用于根据设备信息生成设备指纹;

获取单元,用于获取转发流量包的特征;所述特征为预设时间内向路由器发送的流量包的次数以及所述流量包的IPv4层的TTL值;所述流量包带有分段路由标签;

第一确定单元,用于根据所述特征确定恶意流量;

第二确定单元,用于确定所述恶意流量的源IP地址,将源IP地址加入黑名单并设置期限;

第三确定单元,用于确定当前网络中的接入设备的设备指纹是否改变,若设备指纹发生改变集中式认证服务器重新验证其身份,否则续约白名单。

8.根据权利要求7所述的防御装置,其特征在于,所述生成单元包括:

哈希计算模块,用于利用设备信息做哈希;所述设备信息包括系统的进程、开放的端口、开启的服务、依赖库、硬件版本、系统版本、软件版本和设备配置中的一项或多项;

设备指纹生成模块，用于根据哈希生成设备指纹。

9.根据权利要求7所述的防御装置，其特征在于，还包括：

第四确定单元，用于确定当前网络是否拥塞，若拥塞，则镜像通过路由器的流量，优先让流量拥塞的路由器快速转发流量。

10.根据权利要求7所述的防御装置，其特征在于：所述恶意流量包的特征为预设时间内多次向路由器发送的流量包且该流量包的IPv4层的TTL值为1。

11.一种计算机可读存储介质，所述计算机可读存储介质存储有计算机程序，其特征在于，所述计算机程序被处理器执行时实现如权利要求1至6任一项所述的一种针对分段路由标签探测的防御方法的步骤。

针对分段路由标签探测的防御方法及装置

技术领域

[0001] 本发明涉及网络通信安全领域,特别涉及一种针对分段路由标签探测的防御方法及装置。

背景技术

[0002] 分段路由体系结构是不基于特定的控制平面实现的。尽管理论上讲,在网络节点上静态地配置Segment指令是可能的,但是通常使用路由协议在网络中分发Segment信息。SR控制平面当前支持链路状态IGP、ISIS/OSPF以及BGP。有IGP分发的Segment称为“IGP Segment”,由BGP分发的Segment称为“BGP Segment”。分段路由可以通过PCEP协议,实施集中控制方案,通过PCE来为流量根据需求计算路径,然后下发到PCC来引导流量路径。

[0003] SID有很多类型,有Node SID,Prefix SID,Adjacency SID,此场景下使用的是Prefix SID。SR域中的每个节点为其接收到的每个Prefix Segment安装转发条目。节点学习到IP前缀P,以及与此前缀相关联的用于算法A的Prefix-SID S。N是采用算法A计算出的去往前缀P路径的下一跳。该节点及其下一跳N都支持算法A。如果存在多条去往前缀P的等价路径,则存在多个下一跳(N1,N2,N3……),并且流量在这些等价路径上负载均衡。节点为此Prefix Segment安装以下SR转发条目,图1展示了Prefix-SID的转发行为。图1中,入向活动Segment:S;出接口:去往下一跳N的接口;下一跳:N;Segment列表操作:如果下一跳N是P的发起者,且N指示删除活动Segment,则执行“NEXT”操作。否则,执行“CONTINUE”操作。

[0004] 参照图1,节点11到节点12有两条等价路径:经由节点1和经由节点3。节点11使用常规的哈希计算,来实现流量在两条路径上的负载均衡。例如,节点1收到携带Prefix-SID 16012的数据包,将其沿着去往节点12的最短路径转发:经由节点2。然后节点2将该数据包转发到节点12。

[0005] 节点11使用节点4的Prefix Segment 16004将数据包引导到节点4。去往节点4的最短路径经由节点3,然后节点3将该数据包转发到节点4。

[0006] 在SR域中,SR通过Prefix Segment来进行数据包转发,当Prefix Segment被攻击者知道,攻击者可以通过构造包来为数据包添加Prefix Segment,从而达到恶意引流的目的。恶意引流可以造成网络整体的拥挤和堵塞从而瘫痪网络,可以造成某条链路的拥挤和堵塞从而使服务器拒绝服务,可以使恶意包发送的目标设备上从而探测目标设备的信息为后续攻击做准备,可以发送恶意包到目标设备上从而触发漏洞利用。

发明内容

[0007] 为了解决上述问题,本发明提供一种能够有效抑制针对分段路由标签探测的攻击的防御方法及装置。

[0008] 为了实现上述目的,本发明一方面提供一种针对分段路由标签探测的防御方法,包括:

[0009] 集中式认证服务器验证网络中的所有接入设备的身份;若通过验证则将其加入白

名单,并设置身份有效期;

[0010] 接入设备根据设备信息生成设备指纹;

[0011] 获取转发流量包的特征;所述特征为预设时间内向路由器发送的流量包的次数以及所述流量包的IPv4层的TTL值;所述流量包带有分段路由标签;

[0012] 根据所述特征确定恶意流量;

[0013] 确定所述恶意流量的源IP地址,将源IP地址加入黑名单并设置期限;

[0014] 确定当前网络中的接入设备的设备指纹是否改变,若设备指纹发生改变集中式认证服务器重新验证其身份,否则续约白名单。

[0015] 作为优选的一种技术方案,接入设备根据设备信息生成设备指纹,进一步包括:

[0016] 接入设备利用设备信息做哈希;所述设备信息包括系统的进程、开放的端口、开启的服务、依赖库、硬件版本、系统版本、软件版本和设备配置中的一项或多项;

[0017] 根据哈希生成设备指纹。

[0018] 作为优选的一种技术方案,在获取转发流量包的特征,之前还包括:

[0019] 确定当前网络是否拥塞,若拥塞,则镜像通过路由器的流量,优先让流量拥塞的路由器快速转发流量。

[0020] 作为优选的一种技术方案,所述恶意流量包的特征为预设时间内多次向路由器发送的流量包且该流量包的IPv4层的TTL值为1。

[0021] 作为优选的一种技术方案,集中式认证服务器验证网络中的所有接入设备的身份,进一步包括:

[0022] 集中式认证服务器通过密码验证网络中的所有接入设备的身份。

[0023] 作为优选的一种技术方案,身份验证在设备上进行认证或在控制器上统一认证。

[0024] 另一方面,本发明还提供一种针对分段路由标签探测的防御装置,包括:

[0025] 验证单元,用于验证网络中的所有接入设备的身份;若通过验证则将其加入白名单,并设置身份有效期;

[0026] 生成单元,用于根据设备信息生成设备指纹;

[0027] 获取单元,用于获取转发流量包的特征;所述特征为预设时间内向路由器发送的流量包的次数以及所述流量包的IPv4层的TTL值;所述流量包带有分段路由标签;

[0028] 第一确定单元,用于根据所述特征确定恶意流量;

[0029] 第二确定单元,用于确定所述恶意流量的源IP地址,将源IP地址加入黑名单并设置期限;

[0030] 第三确定单元,用于确定当前网络中的接入设备的设备指纹是否改变,若设备指纹发生改变集中式认证服务器重新验证其身份,否则续约白名单。

[0031] 本发明相对于现有技术的有益效果是:本发明通过获取转发流量的频率以及数据包中IPv4层的TTL值来判断恶意流量,从而对其进行防御,这样可以精确防御分段路由标签探测的攻击,对于开启了SR域的网络来说,可以提高目标网络的安全性,减少了网络被破坏的可能。由于数据包的特征比较特殊,误报率也极低,实施防御后也不会影响目标网络的稳定性和可用性。

附图说明

[0032] 图1是本发明提供的现有技术中Prefix-SID的转发行为的示意图；

[0033] 图2是本发明提供的攻击者通过分段路由标签探测方法攻击网络的示意图；

[0034] 图3是本发明提供的攻击者发送恶意数据包的转发路线图；

[0035] 图4是本发明提供的攻击者探测出路由器的SR标签值后的转发路线图；

[0036] 图5是本发明提供的针对分段路由标签探测的防御方法的流程图；

[0037] 图6是本发明提供的含有集中式的认证设备的拓扑图；

[0038] 图7是本发明提供的针对分段路由标签探测的防御装置的结构图。

具体实施方式

[0039] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅是本发明的一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0040] 为了更加清楚的阐述本发明的技术方案，现对攻击者对网络进行攻击以及如何进行分段路由标签探测的过程做具体解释。

[0041] 参照图2，攻击者连接到路由器1，所有路由器开启了OSPF协议来保证设备之间的通信。此外，路由器1、2、3、4都开启了Segment Routing且标签分别为16001、16002、16003、16004。攻击者可以通过分段路由标签探测方法来探测到16002，16003，16004这些标签及路由器，然后利用这些标签可以构造恶意的流量包进行针对任意目标的攻击，包括路由器1、2、3、4。下面对攻击者如何进行分段路由标签探测的流程进行介绍。

[0042] 步骤101，攻击者构造恶意的数据包，此数据包要确保能与路由器进行二层通信，所以在Ethernet层中写入MAC地址，源地址为本机的出口接口MAC地址，目的地址为到目标网络的下一跳的入接口的MAC地址。

[0043] 为了能支持数据包携带MPLS标签，将下一层Type设置为MPLS-Unicast。

[0044] 对MPLS层的构造在步骤102中操作，因为SR标签值是流程图中唯一的变量，需要单独在一个步骤中操作才方便通过流程图进行整个流程描述。

[0045] 将MPLS层的下一层设置成IPv4层，此时需要设置DSCP字段，定位为高位字段，设置IPv4层的ID，定位为低位字段，因为SID的长度为20位，IPv4的ID长度为16位，所以需要DSCP字段的4位来补充。例如，当DSCP为0且IPv4ID为16002时，SID为16002；当DSCP为1且IPv4为16002时，SID为81,538。IPv4的ID值设置的意义就是为了可以在收到回包的时候通过ID值来得到SR标签值，因为ID值与SR标签值是同步进行遍历的。此外，还要设置TTL为1，使到达目的地时的TTL为0，触发分段路由回一个ICMP包的机制。

[0046] 在IPv4层中，需要设置源地址为本地出接口地址，目的地址为任意的地址，为了可以让目标设备回包的时候有一个发回包的目的地址。然后将下一层设置为ICMP层。

[0047] 将ICMP层的ICMP类型设置为8，Echo Request，为了触发TTL＝0的回包。将下一层设置为data层，不需要添加任何数据。

[0048] 步骤102，在构造的数据包的MPLS层推入一个SR标签，起始值为0。攻击者也可以根据经验来设置其他起始值。同时，将DSCP与IPv4ID的组合设置为与新添加的SR标签值同步。

[0049] 步骤103,判断攻击者有无收到ICMP的回包,如果有收到回包则进入步骤104,如果没有收到回包则进入步骤106.

[0050] 步骤104,记录下SR标签的标签值

[0051] 步骤105,将记录下的SR标签保存在构造包的标签栈中,然后步骤105进入步骤102,在保存的SR标签下面再添加一个新的SR标签。举例,在只有一层标签且标签值为16002时,攻击者收到了回包,那么攻击者会在16002标签的下面在打上新的标签0,此时标签栈为16002,0。当新的标签遍历到目标中存在的标签时,标签栈结果将更新为16002,16004。通过标签栈,攻击者就可以进行网络空间绘制了。

[0052] 步骤106,在步骤105判断攻击者没有收到ICMP回包才会进入步骤106,意味着添加的标签没有击中目标设备的标签值,所以将步骤102添加的标签值加一。此时如果标签栈存在多个标签值,说明前面几次遍历中成功找到了网络中的SR标签值,而步骤106的操作只针对步骤102新添加进来的SR标签。

[0053] 步骤107,判断SR标签值是否遍历穷尽,如果没有穷尽则进入步骤103判断是否收到ICMP回包,如果穷尽了则进入步骤108。

[0054] 步骤108,此时SR标签值已经遍历穷尽,意味着目标网络中已经没有设置了SR标签值的设备可以再被发现了,所以攻击者进行SR标签栈的整理。

[0055] 步骤109,对之前进行的探测行为所收集的数据进行整理,例如标签栈中的标签值和标签值的位置,从而进行目标网络空间的绘制及SR标签的分布。

[0056] 步骤1010,分段路由标签探测方法的输出结果,即为含有各个设备SR标签的网络空间绘制图,方便攻击者进行下一步的攻击,包括SR标签利用方面的攻击,也包括得知网络空间情况之后的攻击。

[0057] 参照图3,攻击者发送恶意数据包的转发路线,从攻击者到达路由器1,再到路由器2,然后发现TTL为0,路由器3发送ICMP TTL＝0的消息经由路由器1到达攻击者。此时,攻击者尝试的SR标签为正确的标签,路由器3才会发送ICMP TTL＝0的消息给攻击者。

[0058] 默认情况下,攻击者携带的第一个标签为路由器3的标签,不为路由器1的标签,因为路由器1与攻击者直连。

[0059] 表1

[0060]

阶段	层次	字段
①	Ethernet	Destination MAC Source MAC Ethernet II
②	MPLS	Label Payload type
③	IPv4	DSCP ID TTL Source address
③	ICMP	Comman header
无	DATA	any

[0061] 表1和图3结合起来，图3中的数据包转发流程的1，2，3分别需要用到表1中的标注了1，2，3的信息，分别为Ethernet层，MPLS层，和IPv4及ICMP层。

[0062] 表1中显示IPv4需要用到DSCP与ID来定位SR的标签值，是因为IPv4的ID长度为16位，DSCP的长度位4位，而SR标签的长度为20位，所以需要DSCP与ID结合起来定位SR的标签值以达到覆盖。

[0063] 如图4，攻击者探测出路由器3的SR标签值，进而在标签栈中再遍历路由器4的标签值，直到找到路由器4的标签值，从而使发过去的恶意数据包触发回复ICMP TTL＝0的回复消息。

[0064] 当找出几个标签值后，攻击者可以使用推测的方法推理出目标SR域内的标签值范围，例如本案例中的16000左右为SR域内的标签值使用范围，大概率后面几个设备是16005、16006、16007……。

[0065] 详细地描述了分段路由标签探测的方法之后，可以得出分段路由标签探测的特征是攻击者持续且频繁发送的报文中的IPv4层中的TTL值为1在探测攻击刚开始时。针对这个特征，被攻击路由器上可以通过防火墙的规则设置来拦截此类的恶意报文。

[0066] 防火墙的规则原理是匹配短时间内路由器多次收到的MPLS包中IPv4层的TTL值为1的数据包，并将源地址加入黑名单设置一个期限。例如，5秒内收到同一个IP地址的MPLS包中IPv4层的TTL值为1的数据包5次，则将此IP地址加入黑名单封禁1天。

[0067] 下面具体解释本发明的技术方案。

[0068] 参照图5，本实施例提供一种针对分段路由标签探测的防御方法，包括以下步骤：

[0069] S201:集中式认证服务器验证网络中的所有接入设备的身份;若通过验证则将其加入白名单,并设置身份有效期;

[0070] 应当说明的是,如图6所示,图6是含有集中式的认证设备的拓扑图,集中式设备为节点1,与其他节点连接且保持与其他节点的通信,节点之间的连线具有冗余性。节点7为准备接入的节点设备,当节点7接入目标网络中,需要经过节点1,即集中式认证设备的身份验证。设备之间的连接具有冗余性的目的是防止节点间通信断开的可能,因为通过验证的设备在后续的再次验证中检测出威胁并断开,由此会导致与之相连的设备无法与集中式认证设备通信。

[0071] 在本实施例中,集中式认证服务器对目标网络中的所有接入设备进行身份验证并加入白名单,同时设置一个有效期限。一旦到了期限,需要接入设备重新进行验证。身份验证可以在设备上进行认证,也可以在控制器上统一进行认证。同时,续约也是如此,可以在设备上或者控制器上进行。

[0072] 应当说明的是,验证的方式通过传统的密码验证并要求安全姓高的密码规范,例如密码需要符合字母大小写加数字的格式。

[0073] S202:接入设备根据设备信息生成设备指纹;

[0074] 具体的,接入设备需要对系统的进程、开放的端口、开启的服务、依赖库、硬件版本、系统版本、软件版本和设备配置做一个哈希,生成一个设备指纹并上报集中式认证服务器。因为网络中长期接入设备是不经常做改动的,所以设备指纹应该长时间保持不变。

[0075] 当攻击者攻破目标网络中的设备,并上传恶意脚本,运行恶意脚本时或进行一些恶意行为时,设备指纹将会改变,同时集中式认证服务器将会检测到设备指纹改变,要求设备进行重新验证,否则踢出白名单,不准此设备进入网络。

[0076] S203:获取转发流量包的特征;所述特征为预设时间内向路由器发送的流量包的次数以及所述流量包的IPv4层的TTL值;所述流量包带有分段路由标签;

[0077] 具体的,当网络开始运行时,获取转发流量的MPLS包的IPv4层的TTL值,以及流量包的发送次数,通过IPv4层的TTL值以及发送次数来判断该流量包是否为恶意流量。

[0078] S204:根据所述特征确定恶意流量;

[0079] 通过上述说明可知,若一定时间内多次发送同样的流量包,例如5秒内发送同样的数据包10,且该流量包的IPv4层的TTL值为1。

[0080] 在此需要说明的是,本发明对上述的时间以及次数不做具体限定,这个可以根据需要进行调整,例如1秒3次,2秒10次等等。

[0081] 在另外一实施例中,为了可以在不影响流量正常转发导致流量拥塞,在步骤S40之前可以先判断网络状况是否堵塞,如果不堵塞则进入步骤S40,如果堵塞,镜像通过路由器的流量,优先让流量拥塞的路由器快速转发流量,同时防火墙对路由器的镜像流量进行特征匹配,这样虽然导致了对恶意流量的匹配具有了延迟性,但是降低了防御方法带来的副作用,保证了目标网络的可靠性和可用性。

[0082] S205:确定所述恶意流量的源IP地址,将源IP地址加入黑名单并设置期限;

[0083] 具体的,当确定了恶意流量之后,根据流量包的内容就能够找到对应的源IP地址,将该源IP地址加入黑名单并根据需要设置期限,这样可以精确防御分段路由标签探测的攻击,对于开启了SR域的网络来说,可以提高目标网络的安全性,减少了网络被破坏的可能。

[0084] 应当理解的是，由于数据包特征比较特殊，一般普通流量都不会同时拥有这些特征，所以在实施防御方法后，防御方法也不会影响目标网络的稳定性和可用性，正常业务流量仍然可以在网络中正常转发。

[0085] S206：确定当前网络中的接入设备的设备指纹是否改变，若设备指纹发生改变集中式认证服务器重新验证其身份，否则续约白名单。

[0086] 为了进一步保障接入设备不被误封，会在发现了攻击者之后对网络设备的设备指纹重新验证，如果设备指纹发生变更就需要集中式认证服务器重新验证其身份，否则续约白名单。

[0087] 通过集中式认证服务器认证，可以确保接入设备的安全性、可靠性和可信性，从而减少攻击者攻击目标网络的可能性。集中式的认证就是在目标网络中设立一个集中式的认证服务器，所有要接入目标网络中的设备都需要通过认证服务器进行身份的验证，只有身份验证成功之后，才可以接入目标网络，否则将会被目标网络断开或隔离。认证服务器可以将身份仓库作为身份数据中心，来实现多种多样的认证和授权服务。此外，集中管理确保了数据的安全性，只要确保集中式服务器的数据安全，就可以抑制敏感数据的泄露。

[0088] 参照图6，本实施例还提供一种针对分段路由标签探测的防御装置，包括：验证单元100，用于验证网络中的所有接入设备的身份；若通过验证则将其加入白名单，并设置身份有效期；在此需要说的是，由于具体的验证方式以及过程在上述实施例中所记载的针对分段路由标签探测的防御方法的步骤S201中已经详细阐述，故在此不再赘述。

[0089] 生成单元200，用于根据设备信息生成设备指纹；在此需要说的是，由于具体的生成方式以及过程在上述实施例中所记载的针对分段路由标签探测的防御方法的步骤S202中已经详细阐述，故在此不再赘述。

[0090] 获取单元300，用于获取转发流量包的特征；所述特征为预设时间内向路由器发送的流量包的次数以及所述流量包的IPv4层的TTL值；在此需要说的是，由于具体的获取方式以及过程在上述实施例中所记载的针对分段路由标签探测的防御方法的步骤S203中已经详细阐述，故在此不再赘述。

[0091] 第一确定单元400，用于根据所述特征确定恶意流量；在此需要说的是，由于具体的确定方式以及过程在上述实施例中所记载的针对分段路由标签探测的防御方法的步骤S204中已经详细阐述，故在此不再赘述。

[0092] 第二确定单元500，用于确定所述恶意流量的源IP地址，将源IP地址加入黑名单并设置期限；在此需要说的是，由于具体的确定方式以及过程在上述实施例中所记载的针对分段路由标签探测的防御方法的步骤S205中已经详细阐述，故在此不再赘述。

[0093] 第三确定单元600，用于确定当前网络中的接入设备的设备指纹是否改变，若设备指纹发生改变集中式认证服务器重新验证其身份，否则续约白名单；在此需要说的是，由于具体的确定方式以及过程在上述实施例中所记载的针对分段路由标签探测的防御方法的步骤S206中已经详细阐述，故在此不再赘述。

[0094] 在另外一实施例中，本发明还提供一种计算机可读存储介质，其中，该计算机可读存储介质可存储有程序，该程序执行时包括上述方法实施例中记载的任何一种针对分段路由标签探测的防御方法的部分或全部步骤。

[0095] 另外，在本发明各个实施例中的各功能单元可以集成在一个处理单元中，也可以

是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。

[0096] 所述集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储器中。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的全部或部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储器中，包括若干指令用以使得一台计算机设备(可为个人计算机、服务器或者网络设备等)执行本发明各个实施例所述方法的全部或部分步骤。而前述的存储器包括：U盘、只读存储器(ROM，Read-Only Memory)、随机存取存储器(RAM，Random Access Memory)、移动硬盘、磁碟或者光盘等各种可以存储程序代码的介质。

[0097] 本领域普通技术人员可以理解上述实施例的各种方法中的全部或部分步骤是可以通过程序来指令相关的硬件来完成，该程序可以存储于一计算机可读存储器中，存储器可以包括：闪存盘、只读存储器(英文：Read-Only Memory，简称：ROM)、随机存取器(英文：Random Access Memory，简称：RAM)、磁盘或光盘等。

[0098] 以上参照附图描述了根据本发明的实施例的用于对针对分段路由标签探测的防御方法的示例性流程图。应指出的是，以上描述中包括的大量细节仅是对本发明的示例性说明，而不是对本发明的限制。在本发明的其他实施例中，该方法可具有更多、更少或不同的步骤，且各步骤之间的顺序、包含、功能等关系可以与所描述和图示的不同。

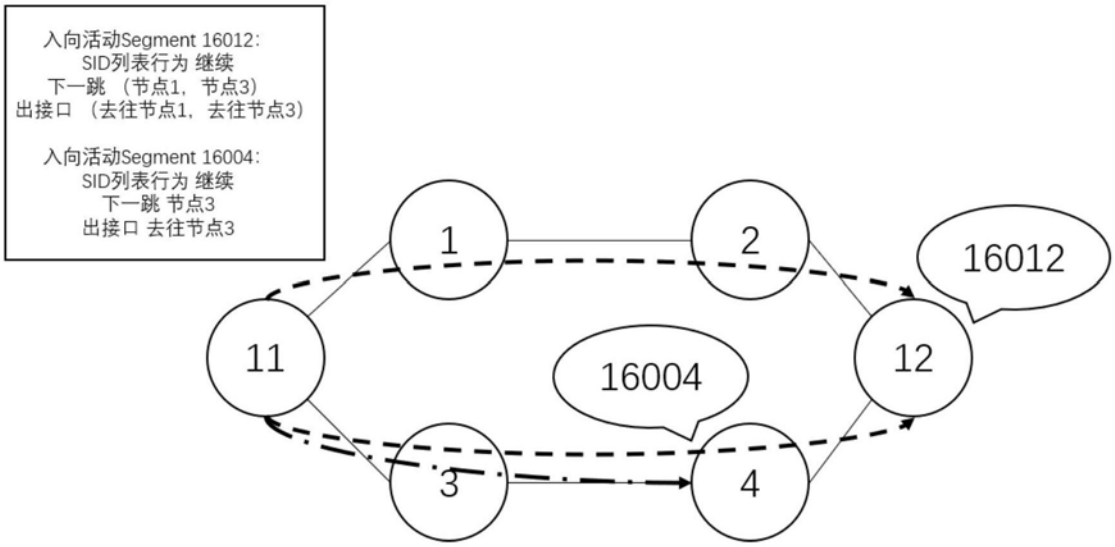

入向活动Segment 16012:
SID列表行为 继续
下一跳 （节点1，节点3）
出接口 （去往节点1，去往节点3）
入向活动Segment 16004:
SID列表行为 继续
下一跳 节点3
出接口 去往节点3
1
2
16012
11
12
16004
3
4

图1

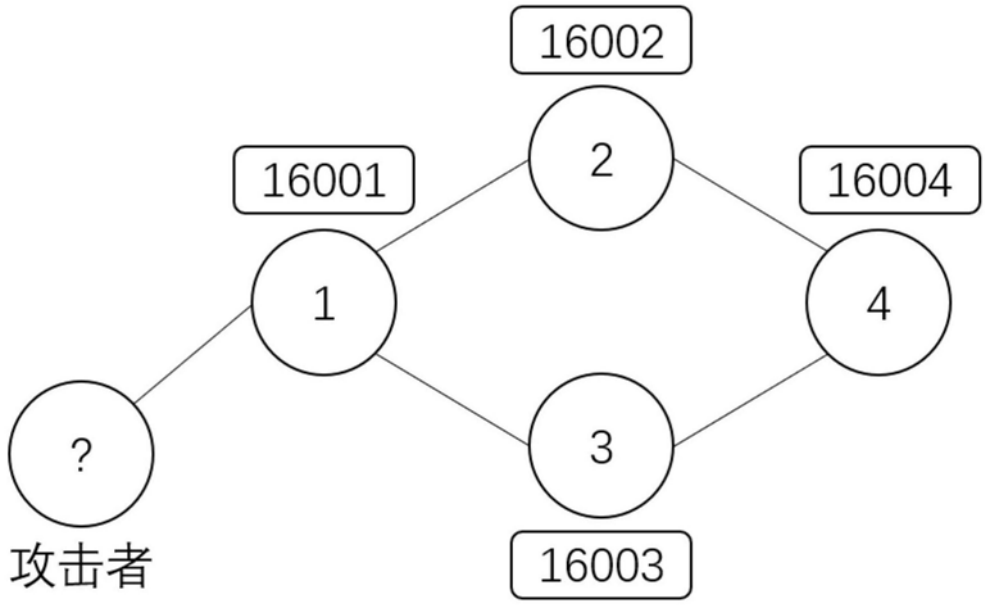

16002
2
16001
16004
1
4
?
3
攻击者
16003

图2

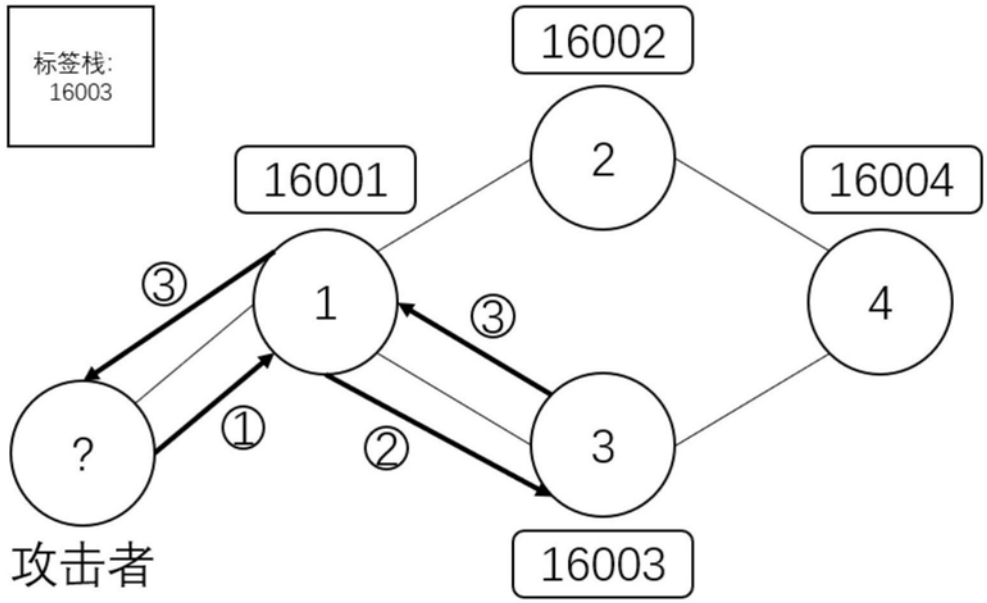

标签栈:
16003
16002
16001
2
16004
③
1
③
4
?
①
②
3
攻击者
16003

图3

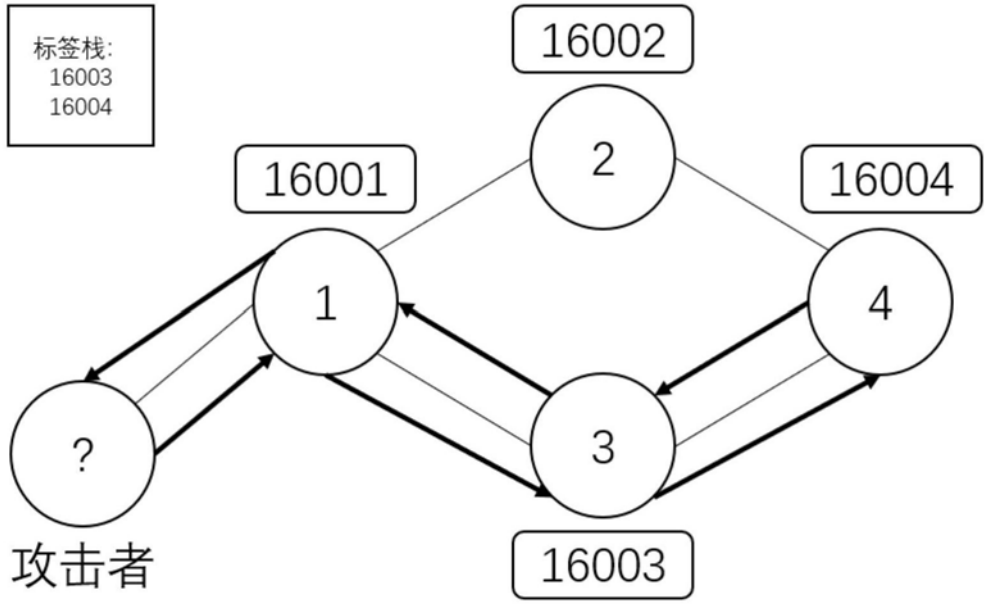

标签栈:
16003
16004
16002
16001
2
16004
1
4
?
3
攻击者
16003

图4

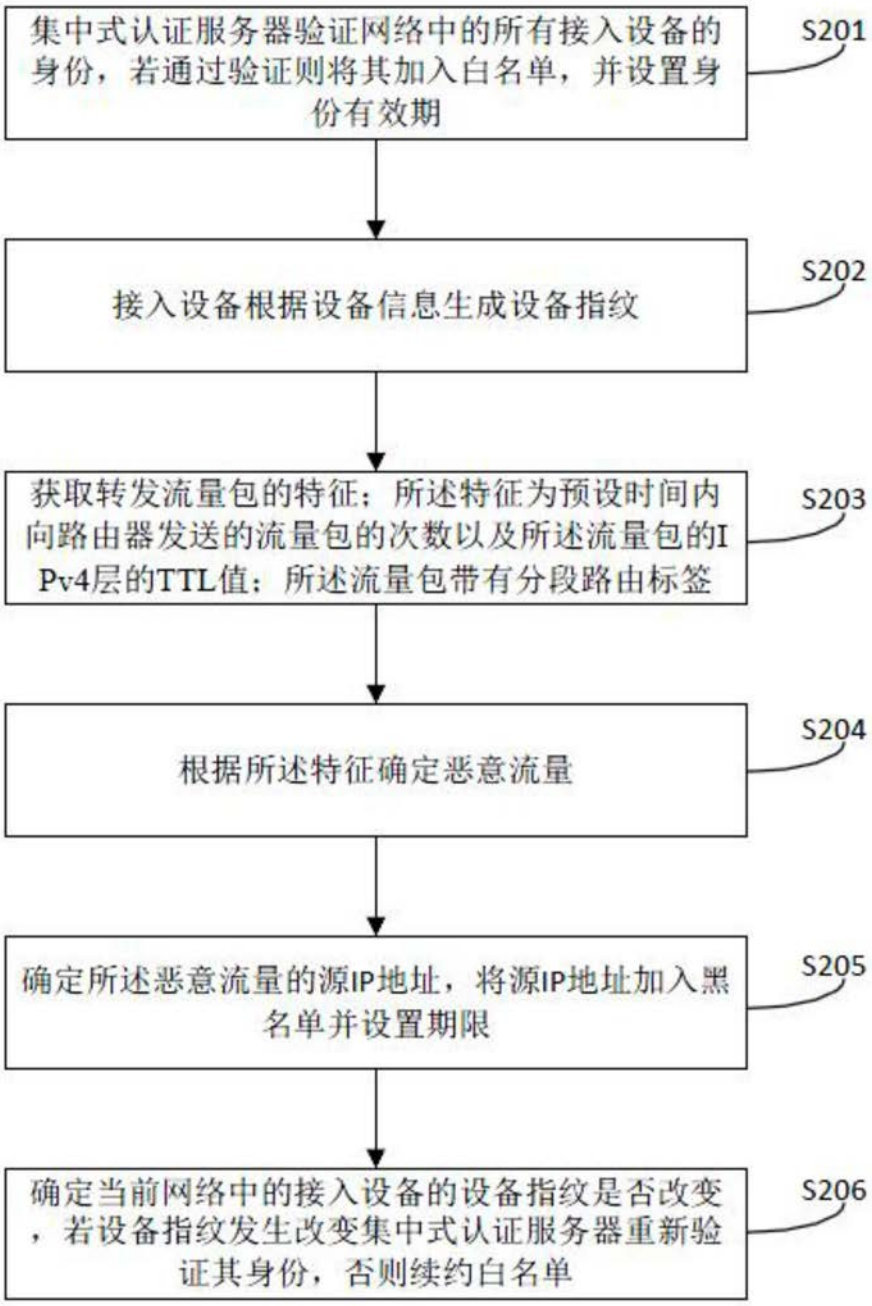

集中式认证服务器验证网络中的所有接入设备的身份，若通过验证则将其加入白名单，并设置身份有效期
S201
接入设备根据设备信息生成设备指纹
S202
获取转发流量包的特征；所述特征为预设时间内向路由器发送的流量包的次数以及所述流量包的IPv4层的TTL值；所述流量包带有分段路由标签
S203
根据所述特征确定恶意流量
S204
确定所述恶意流量的源IP地址，将源IP地址加入黑名单并设置期限
S205
确定当前网络中的接入设备的设备指纹是否改变，若设备指纹发生改变集中式认证服务器重新验证其身份，否则续约白名单
S206

图5

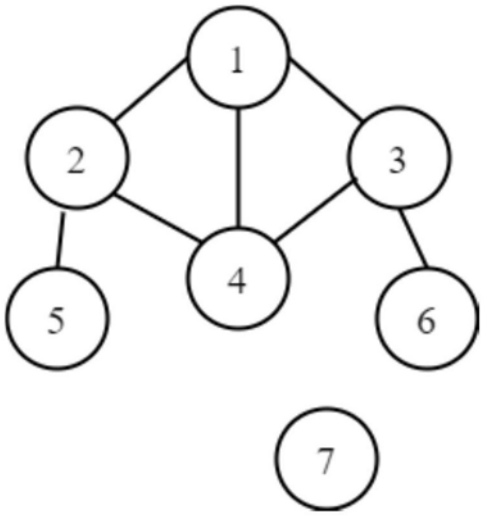

1
2
3
4
5
6
7

图6


100
验证单元
生成单元
200
300
获取单元
第一确定单元
400
500
第二确定单元
第三确定单元
600
针对分段路由标签探测的防御装置

图7