(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2017 年 2 月 16 日 (16.02.2017)

WIPO | PCT

(10) 国际公布号
WO 2017/024977 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2016/093186

(22) 国际申请日: 2016 年 8 月 4 日 (04.08.2016)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201510497226.1 2015 年 8 月 13 日 (13.08.2015) CN

(71) 申请人: **阿里巴巴集团控股有限公司 (ALIBABA GROUP HOLDING LIMITED)** [—/CN]; 英属开曼群岛大开曼资本大厦一座四层 847 号邮箱, Grand Cayman (KY)。

(72) 发明人: **肖洪亮 (XIAO, Hongliang)**; 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。 **张大成 (ZHANG, Dacheng)**; 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。

(74) 代理人: **北京三友知识产权代理有限公司 (BEIJING SANYOU INTELLECTUAL PROPERTY AGENCY LTD.)**; 中国北京市金融街 35 号国际企业大厦 A 座 16 层, Beijing 100033 (CN)。

(81) 指定国 (除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明，要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:
— 包括国际检索报告(条约第 21 条(3))。

(54) **Title**: NETWORK ATTACK PREVENTION METHOD, APPARATUS AND SYSTEM

(54) **发明名称** : 一种网络攻击的防御方法、装置及系统

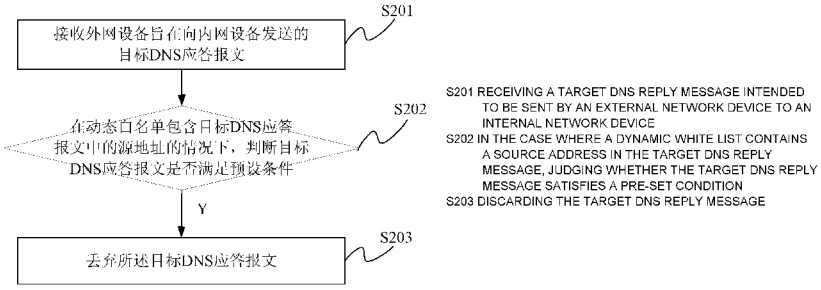

图 2

(57) **Abstract**: Provided are a network attack prevention method, apparatus and system. The method comprises: receiving a target DNS reply message intended to be sent by an external network device to an internal network device; in the case where a dynamic white list contains a source address in the target DNS reply message, judging whether the target DNS reply message satisfies a pre-set condition; and if the target DNS reply message satisfies the pre-set condition, discarding the target DNS reply message, wherein the pre-set condition at least comprises that: a target domain name in the target DNS reply message is not contained in a history domain name record, and each history domain name in the history domain name record is extracted from a history DNS reply message sent from the external network device. The present application can filter out a DNS reply message in the case of a real source attacking an internal network device by means of different domain names, thereby alleviating an impact on a service and a network, caused by a DNS reply attack.

(57) **摘要**: 本申请提供了一种网络攻击的防御方法、装置及系统，其中方法包括：接收外网设备旨在向内网设备发送的目标 DNS 应答报文；在动态白名单包含所述目标 DNS 应答报文中的源地址的情况下，判断所述目标 DNS 应答报文是否满足预设条件；若所述目标 DNS 应答报文满足预设条件，则丢弃所述目标 DNS 应答报文；其中，所述预设条件至少包括：所述目标 DNS 应答报文中的目标域名不包含在历史域名记录中，所述历史域名记录中的每个历史域名均从所述外网设备所发送的历史 DNS 应答报文中提取。本申请可以过滤掉真实源以不同域名的方式来攻击内网设备的 DNS 应答报文，从而缓解 DNS 应答攻击对业务和网络造成的冲击。

WO 2017/024977 A1

一种网络攻击的防御方法、装置及系统

本申请要求 2015 年 08 月 14 日递交的申请号为 201510497226.1、发明名称为“一种网络攻击的防御方法、装置及系统”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本申请涉及网络技术领域，尤其涉及一种网络攻击的防御方法、装置及系统。

背景技术

随着网络技术的不断进步，网络领域中的网络攻击也越来越多。目前，在众多网络攻击中分布式拒绝服务攻击（Distributed Denial of Service，DDoS）已经成为较为严重的攻击手段。在 DDOS 攻击中 DNS 应答攻击已成为主流攻击类型，DNS 应答攻击又可以称为域名解析系统（DNS，Domain Name System）应答攻击。

为了防范 DNS 应答攻击，可以在原有系统中加入清洗设备进而形成防御系统。参见图 1 为一种防御系统结构示意图，在图示中可以看出清洗设备旁路设置在路由设备的一侧。

在清洗设备旁路设置的情况下，可以使用源探测的方式来清洗外网设备向内网设备发送的具有攻击性的 DNS 应答报文。具体清洗过程可以为：清洗设备接收外网设备向内网设备发送的 DNS 应答报文后，提取其中的源地址，并判断源地址是否包含在动态白名单中。如果源地址没有包含在动态白名单中，则向外网设备发送一个 DNS Request 报文作为探测报文，如果未接收到外网设备反馈的 DNS 应答报文，则确定外网设备为虚假源，丢弃 DNS 应答报文；如果接收到外网设备反馈的 DNS 应答报文，且 DNS 应答报文中的域名满足一定条件，则确定外网设备为真实源，将外网设备的 IP 地址加入至动态白名单中。如果源地址包含在动态白名单中，即外网设备为真实源，则转发 DNS 应答报文。

DNS 应答攻击按攻击类型又可以分为：真实源攻击和虚假源攻击。由于动态白名单中仅包含真实源的 IP 地址，不包含虚假源的 IP 地址，所以源探测方式仅能够清洗虚假源发起的 DNS 应答攻击，而不能够清洗掉真实源发起的 DNS 应答攻击。

鉴于此，现在需要一种方法来清洗真实源发起的 DNS 应答攻击，以缓解 DNS 应答攻击对业务和网络造成的冲击。

发明内容

本申请提供了一种网络攻击的防御方法、装置及系统，清洗真实源发起的DNS应答攻击，以缓解DNS应答攻击对业务和网络造成的冲击。

为了实现上述目的，本申请提供了以下技术手段：

一种网络攻击的防御方法，包括：

接收外网设备旨在向内网设备发送的目标DNS应答报文；

在动态白名单包含所述目标DNS应答报文中的源地址的情况下，判断所述目标DNS应答报文是否满足预设条件；

若所述目标DNS应答报文满足预设条件，则丢弃所述目标DNS应答报文；

其中，所述预设条件至少包括：所述目标DNS应答报文中的目标域名不包含在历史域名记录中，所述历史域名记录中的每个历史域名均从所述外网设备所发送的历史DNS应答报文中提取。

优选的，所述预设条件还包括：

所述外网设备发起访问所述目标域名的第一发送时间与第二发送时间的时间间隔小于预设时间间隔；

其中，所述第一发送时间为所述目标DNS应答报文的发送时间，所述第二发送时间为所述外网设备在所述第一发送时间之前最近一次发送包含所述目标域名的DNS应答报文的时间。

优选的，还包括：

在所述时间间隔不小于预设时间间隔情况下，将所述目标DNS应答报文转发给所述内网设备。

优选的，还包括：

若所述目标DNS应答报文中的目标域名不包含在历史域名记录中，则将所述目标域名和所述目标DNS应答报文的发送时间，存储在所述历史域名记录中。

优选的，还包括：

依据与所述外网设备的源地址对应的所述历史域名记录，计算命中次数超过预设次数的域名数量与所有域名数量的比值；其中，所述历史域名记录中包含所述外网设备所发送的历史DNS应答报文中所有域名以及每个域名的命中次数；所述预设次数为不小于3的自然数；

若所述比值大于预设比值，则删除所述动态白名单中的所述外网设备的源地址；

将所述外网设备的源地址添加至动态黑名单中。

优选的，所述历史域名记录中每个域名的命中次数的计算方式包括：

在接收一个 DNS 应答报文之后，在所述历史域名记录中查找该 DNS 应答报文中的域名；

将所述域名的命中次数增加 1；其中，每个域名的命中次数的初始值为零。

优选的，所述预设条件还包括：

所述目标 DNS 应答报文的流量值及历史 DNS 应答报文的流量值的总和流量值大于所述预设流量值；

其中，所述历史 DNS 应答报文为所述外网设备在发送目标 DNS 应答报文之前所发送的所有 DNS 应答报文。

优选的，还包括：

在所述总和流量值大于所述预设流量值的情况下，删除所述动态白名单中的所述源地址；

将所述源地址加入至动态黑名单中。

优选的，所述历史 DNS 应答报文的流量值计算过程包括：

在所述外网设备的源地址发送一个 DNS 应答报文之后，在所述历史 DNS 应答报文的流量值上叠加该 DNS 应答报文的流量值；所述历史 DNS 应答报文的流量值的初始值为零。

优选的，还包括：

在动态黑名单中包含所述目标 DNS 应答报文中的源地址的情况下，丢弃所述目标 DNS 应答报文。

一种网络攻击的防御装置，包括：

接收单元，用于接收外网设备旨在向内网设备发送的目标 DNS 应答报文；

判断单元，用于在动态白名单包含所述目标 DNS 应答报文中的源地址的情况下，判断所述目标 DNS 应答报文是否满足预设条件；

第一丢弃单元，用于若所述目标 DNS 应答报文满足预设条件，则丢弃所述目标 DNS 应答报文；

其中，所述预设条件至少包括：所述目标 DNS 应答报文中的目标域名不包含在历史域名记录中，所述历史域名记录中的每个历史域名均从所述外网设备所发送的历史 DNS 应答报文中提取。

优选的，所述预设条件还包括：

所述外网设备发起访问所述目标域名的第一发送时间与第二发送时间的时间间隔小于预设时间间隔；

其中，所述第一发送时间为所述目标 DNS 应答报文的发送时间，所述第二发送时间为所述外网设备在所述第一发送时间之前最近一次发送包含所述目标域名的 DNS 应答报文的时间。

优选的，还包括：

转发单元，用于在所述时间间隔不小于预设时间间隔情况下，将所述目标 DNS 应答报文转发给所述内网设备。

优选的，还包括：

存储单元，用于若所述目标 DNS 应答报文中的目标域名不包含在历史域名记录中，则将所述目标域名和所述目标 DNS 应答报文的发送时间，存储在所述历史域名记录中。

优选的，还包括：

比值计算单元，用于依据与所述外网设备的源地址对应的所述历史域名记录，计算命中次数超过预设次数的域名数量与所有域名数量的比值；其中，所述历史域名记录中包含所述外网设备所发送的历史 DNS 应答报文中所有域名以及每个域名的命中次数；所述预设次数为不小于 3 的自然数；

第一删除单元，用于若所述比值大于预设比值，则删除所述动态白名单中的所述外网设备的源地址；

第一添加单元，用于将所述外网设备的源地址添加至动态黑名单中。

优选的，还包括：

命中次数计算单元，用于在接收一个 DNS 应答报文之后，在所述历史域名记录中查找该 DNS 应答报文中的域名；将所述域名的命中次数增加 1；其中，每个域名的命中次数的初始值为零。

优选的，所述预设条件还包括：

所述目标 DNS 应答报文的流量值及历史 DNS 应答报文的流量值的总和流量值大于所述预设流量值；

其中，所述历史 DNS 应答报文为所述外网设备在发送目标 DNS 应答报文之前所发送的所有 DNS 应答报文。

优选的，还包括：

第二删除单元，用于在所述总和流量值大于所述预设流量值的情况下，删除所述动态白名单中的所述源地址；

第二添加单元，用于将所述源地址加入至动态黑名单中。

优选的，还包括：

流量计算单元，用于在所述外网设备的源地址发送一个 DNS 应答报文之后，在所述历史 DNS 应答报文的流量值上叠加该 DNS 应答报文的流量值；所述历史 DNS 应答报文的流量值的初始值为零。

优选的，还包括：

第二丢弃单元，用于在动态黑名单中包含所述目标 DNS 应答报文中的源地址的情况下，丢弃所述目标 DNS 应答报文。

一种网络攻击的防御系统，包括：外网设备、清洗设备和内网设备；

所述外网设备，用于向清洗设备发送旨在向内网设备发送的目标 DNS 应答报文；

所述清洗设备，用于接收外网设备旨在向内网设备发送的目标 DNS 应答报文；在动态白名单包含所述目标 DNS 应答报文中的源地址的情况下，判断所述目标 DNS 应答报文是否满足预设条件；若所述目标 DNS 应答报文满足预设条件，则丢弃所述目标 DNS 应答报文；其中，所述预设条件至少包括：所述目标 DNS 应答报文中的目标域名不包含在历史域名记录中，所述历史域名记录中的每个历史域名均从所述外网设备所发送的历史 DNS 应答报文中提取；

内网设备，用于接收清洗设备清洗后的 DNS 应答报文。

从以上技术内容可以看出本申请具有以下有益效果：

本申请实施例在确认目标 DNS 应答报文中源地址在动态白名单内后，即可确认发起目标 DNS 应答报文的外网设备非虚假源而是真实源。真实源发起 DNS 应答攻击的一种方式为，频繁发送包含不同域名的 DNS 应答报文来攻击内网设备。因此本申请中设有一个历史域名记录，其中记录有外网设备所发送的所有域名。

当目标 DNS 应答报文中的目标域名不包含在历史域名记录中时，则表明外网设备为首次发送包含目标域名的 DNS 应答报文。在此情况下，目标 DNS 应答报文可能是由外网设备以不同域名方式发起 DNS 应答攻击，为了避免内网设备遭受攻击，此时丢弃所述目标 DNS 应答报文。

由于正常的外网设备具有自动重发机制，如果正常的外网设备发送的 DNS 应答报文被丢弃之后，正常的外网设备会在接收到内网设备重发的 DNS Request 报文之后，重新

发送目标 DNS 应答报文，因此本申请不会影响正常的 DNS 应答报文发送至内网设备。而具有攻击性的外网设备则不具有重发机制，所以本申请可以过滤掉真实源以不同域名的方式来攻击内网设备的 DNS 应答报文，从而缓解 DNS 应答攻击对业务和网络造成的冲击。

附图说明

为了更清楚地说明本申请实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本申请的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

图 1 为一种防御系统的结构示意图；

图 2 为本申请实施例公开的一种网络攻击的防御方法的流程图；

图 3 为本申请实施例公开的又一种网络攻击的防御方法的流程图；

图 4 为本申请实施例公开的一种网络攻击的防御方法中更改动态白名单的流程图；

图 5 为本申请实施例公开的又一种网络攻击的防御方法的流程图；

图 6 为本申请实施例公开的一种网络攻击的防御装置的结构示意图；

图 7 为本申请实施例公开的又一种网络攻击的防御装置的结构示意图；

图 8 为本申请实施例公开的又一种网络攻击的防御装置的结构示意图。

具体实施方式

下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，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，都属于本申请保护的范围。

为了清楚介绍本申请的应用场景，参见图 1，为一种网络攻击的防御系统，所述系统具体包括外网设备 100、路由设备 200、内网设备 300 和与路由设备 200 旁路设置的清洗设备 400。

其中，外网设备 100 用于向清洗设备 400 发送旨在向内网设备 300 发送的 DNS 应答报文；外网设备所发送的 DNS 应答报文中可能在正常的 DNS 应答报文中加杂有攻击的 DNS 应答报文。因此清洗设备 400 用于清洗掉外网设备正常的 DNS 应答报文中具有攻

击性的 DNS 应答报文，然后将清洗掉具有攻击性的 DNS 应答报文之后的正常的 DNS 应答报文，转发至内网设备 300。

在图 1 所示的网络攻击的防御系统的基础上，本申请提供了一种网络攻击的防御方法。本申请中仅针对一个外网设备和该外网设备所要访问的一个内网设备进行详细说明，可以理解的是，其它外网设备和内网设备的实施方式与本申请提供的方法一致。

如图 2 所示，本申请提供一种网络攻击的防御方法，应用于清洗设备，所述方法具体以下步骤 S201~S203：

步骤 S201：接收外网设备旨在向内网设备发送的目标 DNS 应答报文。

外网设备在接收到目标 DNS 应答报文发送指令后，会向清洗设备发送旨在向内网设备发送的目标 DNS 应答报文。目标 DNS 应答报文中包括：发送目标 DNS 应答报文的外网设备的源地址（IP 地址），以及，外网设备需要访问内网设备的目标域名。清洗设备在接收目标 DNS 应答报文后，可以对目标 DNS 应答报文进行判断，以确定目标 DNS 应答报文是否为具有攻击性的 DNS 应答报文。

步骤 S202：在动态白名单包含所述目标 DNS 应答报文中的源地址的情况下，判断所述目标 DNS 应答报文是否满足预设条件。

清洗设备中设有一个动态白名单，该动态白名单中存储有暂时不具有攻击性的真实源的 IP 地址。动态白名单中不具有攻击性的 IP 地址是暂时的，当某一个 IP 地址随着本申请的判断条件已经改变为具有攻击性的 IP 地址时，则将该 IP 地址在动态白名单中删除。即本申请中的动态白名单中的 IP 地址不是固定的，而是动态变化的，所以称为动态白名单。清洗设备在接收目标 DNS 应答报文之后，在目标 DNS 应答报文中提取外网设备的源地址，然后判断动态白名单中是否包含有外网设备的源地址。

如果动态白名单中不包含有外网设备的源地址，则使用源探测方式来确定源地址对应的外网设备是否为虚假源；如果外网设备为虚假源则目标 DNS 应答报文为虚假源发送的具有攻击性的 DNS 应答报文，此时丢弃目标 DNS 应答报文。

如果动态白名单中包含有外网设备的源地址，则表示外网设备为真实源；目标 DNS 应答报文为真实源发送的 DNS 应答报文。随着攻击技术的发展，真实源也可以被攻击人员作为攻击源，所以在确定外网设备为真实源后需要采取进一步判断，来确定目标 DNS 应答报文是否为具有攻击性的报文。

由于真实源发起 DNS 应答攻击的方式一为，频繁发送包含不同域名的 DNS 应答报

文来攻击内网设备，因此本申请中清洗设备为动态白名单中的每一个 IP 地址构建一个历史域名记录。历史域名记录用于记录每个 IP 地址所发送的 DNS 应答报文中所包含的域名。可见，本实施例中在清洗设备也存在一个与外网设备对应历史域名记录，其中记录有外网设备所发送的历史 DNS 应答报文中所出现过的域名。

为了进一步确定目标 DNS 应答报文是否为具有攻击性的报文，本实施例预先设定预设条件。预设条件至少包括：所述目标 DNS 应答报文中的目标域名不包含在历史域名记录中，所述历史域名记录中的每个历史域名均从所述外网设备所发送的历史 DNS 应答报文中提取。

在确定动态白名单中包含有目标 DNS 应答报文的源地址之后，提取目标 DNS 应答报文中的目标域名，然后进一步判断与源地址对应的历史域名记录中是否包含目标域名，即判断目标 DNS 应答报文是否满足预设条件。

步骤 S203：若所述目标 DNS 应答报文满足预设条件，则丢弃所述目标 DNS 应答报文。若所述目标 DNS 应答报文不满足预设条件，则执行其它处理。

如果历史域名记录中不包含目标域名，则表明外网设备首次发送包含目标域名的 DNS 应答报文。在此情况下，目标 DNS 应答报文可能是由外网设备以不同域名方式发起 DNS 应答攻击，所以，历史域名记录中不存在目标域名。在此情况下，为了避免内网设备遭受攻击，此时丢弃目标 DNS 应答报文。此过程可称为“首包丢弃机制”。

可以理解的是，目标 DNS 应答报文还可能是正常的外网设备发起的（外网设备第一次访问目标域名对应的内网设备），在本申请假设目标 DNS 应答报文是正常，在本步骤中也会被丢弃。鉴于此，在丢弃目标 DNS 应答报文之后，将目标域名存储在历史域名记录中，以便正常的外网设备在重发机制下再次发送的包含目标 DNS 应答报文中的目标域名会包含在历史域名记录中，即历史域名记录中的目标域名被命中，从而保证正常的 DNS 报文不会因为“首包丢弃机制”被丢弃。

由于正常的外网设备具有重发机制，即内网设备在向外网设备发送 DNS 请求之后，没有接收到外网设备发送的 DNS 应答报文，内网设备会向外网发送 DNS Request 报文，在 DNS Request 报文的触发下，正常的外网设备会重新发送目标 DNS 应答报文。当清洗设备再次接收到目标域名时，由于历史域名记录中已有目标域名，所以不会再次因为“首包丢弃机制”的原因被再次丢弃，从而保证正常 DNS 应答报文不受影响。

具有攻击性的外网设备不具有重发机制，所以针对真实源以不同域名的方式来攻击内网设备的 DNS 应答报文，本申请可以准确的清洗掉，从而缓解 DNS 应答攻击对业务

和网络造成的冲击。

下面介绍本申请提供一种网络攻击的防御方法的实施例二。如图 3 所示，所述方法包括步骤 S301~S304：

步骤 S301：接收外网设备旨在向内网设备发送的目标 DNS 应答报文。

步骤 S302：在动态白名单包含所述目标 DNS 应答报文中的源地址的情况下，判断所述目标 DNS 应答报文是否满足第一预设条件；所述第一预设条件为所述目标 DNS 应答报文中的目标域名不包含在历史域名记录中。若不满足第一预设条件，则进入步骤 S303；若满足第一预设条件，则进入步骤 S304。

本步骤的具体执行过程已在图 2 所示的实施例中进行详细说明，在此不再赘述。

步骤 S303：判断所述目标 DNS 应答报文是否满足第二预设条件；所述第二预设条件为：外网设备发起访问所述目标域名的第一发送时间与第二发送时间的时间间隔小于预设时间间隔。其中，所述第一发送时间为所述目标 DNS 应答报文的发送时间，所述第二发送时间为所述外网设备在所述第一发送时间之前最近一次发送包含所述目标域名的 DNS 应答报文的时间。若满足第二预设条件则进入步骤 S304。若不满足第二预设条件，则进入步骤 S305。

真实源发起 DNS 应答攻击的方式二为，以有限个域名或者相同域名频繁发送 DNS 应答报文。由于真实源发送 DNS 应答报文的频率较高，所以在此情况下，包含相同域名的 DNS 应答报文的间隔时间会非常短。因此本申请设定一个预设时间间隔，例如 1S。预设时间间隔为正常的外网设备相邻两次发送相同域名的 DNS 应答报文时，所应该具有的时间间隔。

在历史域名记录中包含目标域名的情况下，判定目标 DNS 应答报文的预设条件还包括：所述外网设备发起访问所述目标域名的第一发送时间与第二发送时间的时间间隔小于预设时间间隔。

清洗设备在接收目标 DNS 应答报文时，将当前时间作为目标 DNS 应答报文的发送时间，即第一发送时间。清洗设备的历史域名记录中会记录有包含目标域名的 DNS 应答报文最近一次的发送时间，即第二发送时间。

如果第一发送时间和第二发送时间的时间间隔小于预设时间间隔，则说明外网设备频繁发送包含相同域名的 DNS 应答报文，也就是，外网设备发送相同域名的 DNS 应答报文的频率过高，此时可能是外网设备以有限个域名或者相同域名频繁发送 DNS 应答报

文的攻击方式来攻击内网设备。因此，清洗设备丢弃目标 DNS 应答报文，以保护内网设备免受攻击。

步骤 S304：丢弃所述目标 DNS 应答报文。

步骤 S305：将所述目标 DNS 应答报文转发至内网设备。

如果第一发送时间和第二发送时间的时间间隔不小于预设时间间隔，则说明目标 DNS 应答报文暂且为正常外网设备发送的 DNS 应答报文，因此转发 DNS 应答报文至内网设备。

在上述图 2 和图 3 的实施例中所使用的动态白名单中的 IP 地址仅是暂时不具有攻击性的设备，所以，需要定期检测动态白名单中的 IP 地址是否已经转换为攻击性的设备，以便更新动态白名单。具体的可以采用以下方式：

在动态白名单中的真实源可以发起 DNS 应答攻击的方式三：发送的 DNS 应答报文中的域名比较多但是周期性变化，并且相同域名攻击报文之间的间隔大于 1 秒。在此情况下，上述两个预设条件均不能清洗掉此种具有攻击性 DNS 应答报文。因此采用下述方式来解决方式三的攻击：

在图 2 或 3 所示的实施例的基础上，本申请的提供的实施例还包括：针对外网设备所发送的 DNS 应答报文，清洗设备在接收一个 DNS 应答报文之后，在所述历史域名记录中查找该 DNS 应答报文中的域名；如果在历史域名中查找到 DNS 应答报文中域名，则说明该域名被命中，因此将所述域名的命中次数增加 1；其中，每个域名的命中次数的初始值为零。所以，历史域名记录中记录有外网设备所发送的所有域名，以及每个域名被命中的总次数。

本申请设定一个预设命中次数，该命中次数至少为 3 次。因为一般情况下，正常的 DNS 应答报文最多发送 2 两次包含相同域名的 DNS 应答报文。当一个域名对应的 DNS 应答报文的命中次数超过预设命中次数之后，则说明该域名被频繁用于向内网设备发送 DNS 应答报文，所以可以认为该域名被作为攻击域名来攻击内网设备。

如图 4 所示，在图 2 或图 3 所示的实施例的基础上，清洗设备会定期执行以下步骤：

步骤 S401：依据与所述外网设备的源地址对应的所述历史域名记录，计算命中次数超过预设次数的域名数量与所有域名数量的比值；其中，所述历史域名记录中包含所述外网设备所发送的历史 DNS 应答报文中所有域名以及每个域名的命中次数。

在历史域名记录中统计命中次数超过预设次数的域名数量（第一数量），这样做的

目的是统计外网设备所发送的攻击域名的数量；然后再统计外网设备所发送的所有域名的数量（第二数量）；计算第一数量和第二数量的比值，以确定外网设备中发送攻击域名与所有域名的比值。

步骤 S402：判断所述比值是否大于预设比值，若是，则进入步骤 S403，否则执行其它处理。

本申请可以设定一个预设比值，例如 0.5，用于表示正常情况下攻击域名在所有域名中占有的比值。

步骤 S403：删除所述动态白名单中的所述外网设备的源地址。

当 S401 中计算得到的比值大于预设比值时，则说明外网设备频繁发送包含攻击域名的 DNS 应答报文，即外网设备现在已转换为具有攻击性的外网设备，所以将外网设备的源地址在动态白名单中删除。

步骤 S404：将所述外网设备的源地址添加至动态黑名单中。

定期将动态白名单中的具有攻击性的外网设备的源地址添加至动态黑名单中，以便外网设备再次发送 DNS 应答报文时，丢弃外网设备所发送的 DNS 应答报文，从而保护内网设备免受攻击。

图 4 所示的实施例以目标 DNS 应答报文中的目标域名为出发点，来确定外网设备发送的目标 DNS 应答报文是否为具有攻击性，从而实现更新动态白名单的目的。除了采用域名的方式，本申请还提供了采用流量的方式，来更新动态白名单。

具体的可以为：外网设备的源地址发送一个 DNS 应答报文且源地址包含在动态白名单中，在历史 DNS 应答报文的流量值上叠加该 DNS 应答报文的流量值；所述历史 DNS 应答报文的流量值的初始值为零。即这样做的目的为不断统计外网设备发送 DNS 应答报文的流量值。

在此情况下，所述预设条件还包括：所述目标 DNS 应答报文的流量值及历史 DNS 应答报文的流量值的总和流量值大于所述预设流量值；其中，所述历史 DNS 应答报文为所述外网设备在发送目标 DNS 应答报文之前所发送的所有 DNS 应答报文。

本申请设定一个预设流量值，用于表示正常外网设备在一段时间内所发送的流量值总和。当一段时间内，外网设备所发送的 DNS 应答报文的流量值超过预设流量值，则说明该外网设备频繁发送 DNS 应答报文。在此情况下，表明动态白名单中的外网设备已经转换为具有攻击性外网设备，因此在所述总和流量值大于所述预设流量值的情况下，删

除所述动态白名单中的所述源地址；将所述源地址加入至动态黑名单中。

针对真实源发起 DNS 应答攻击的方式三（发送的 DNS 应答报文中的域名比较多但是周期性变化，并且相同域名攻击报文之间的间隔大于 1 秒），尽管在图 2 或图 3 所示的实施例中没有办法及时清除，但是通过定期查看外网设备所发送的流量值总和的方式，或者，采用攻击域名的命中次数超过预设比值的方式，便能够确定外网设备是否为具有攻击性的设备。如果是具有攻击性的设备，则将外网设备对应的源地址加入至动态黑名单中，以便下次外网设备再发送 DNS 应答报文时，则可以立即丢弃报文。

下面介绍本申请提供一种网络攻击的防御方法的实施例三。如图 5 所示，所述方法包括步骤 S501~S504：

步骤 S501：接收外网设备旨在向内网设备发送的目标 DNS 应答报文。

步骤 S502：判断动态黑名单中是否包含有所述目标 DNS 应答报文中的源地址；如果是，则进入步骤 S512；如果否，则进入步骤 S503。

清洗设备接收到一个外网设备发送的 DNS 应答报文之后，根据报文的目的地址（IP 地址）查询该目的地址对应的内网设备是否处于防御状态。如果，内网设备处于防御状态，则可以执行本实施例中的过程。

动态黑名单中存储的为具有攻击性的外网设备的源地址，所以当外网设备的源地址命中动态黑名单之后，则确定目标 DNS 应答报文为具有攻击性的报文，此时丢弃目标 DNS 应答报文。

步骤 S503：判断动态白名单是否包含所述目标 DNS 应答报文中的源地址；如果是，则进入步骤 S508 以及步骤 S514，否则进入步骤 S504。

步骤 S504：向外网设备发送一个包含特殊域名的 DNS Request 报文作为探测报文。

清洗设备会构造一个 DNS Request 报文作为探测报文发送给外网设备，其中，DNS Request 报文中的域名可由目标 DNS 应答报文中的五元组信息和域名信息通过一定哈希方式构造而来，并保证构造的域名是现网中不存在的域名。

步骤 S505：清洗设备判断是否接收到外网设备反馈的包含特殊域名的 DNS 应答报文；如果是，则进入步骤 S506，否则进入步骤 S507。

清洗设备再次接收该外网设备发送的 DNS 应答报文后，查看报文中域名是否是由步骤 S504 中的方式构造而来的。如果是正常的外网设备在接收 DNS Request 报文后，会将其中的域名加载在依据 DNS Request 报文所生成的 DNS 应答报文中。所以如果再次接收

到的 DNS 应答报文中包含特殊域名，则表示该外网设备是正常的外网设备，否则表示该外网设备是具有攻击性的外网设备。

步骤 S506：将外网设备的 IP 地址加入至动态白名单中，并为外网设备的 IP 地址构建历史域名记录，以及流量监控表。

步骤 S507：将外网设备对应的 IP 地址加入至动态黑名单中。

步骤 S508：判断所述目标 DNS 应答报文是否满足第一预设条件；所述第一预设条件为所述目标 DNS 应答报文中的目标域名不包含在历史域名记录中。若不满足第一预设条件，则进入步骤 S509；若满足第一预设条件，则进入步骤 S511。

步骤 S509：将历史域名记录中目标 DNS 应答报文中目标域名的命中次数加 1。

步骤 S510：判断所述目标 DNS 应答报文是否满足第二预设条件；所述第二预设条件为：外网设备发起访问所述目标域名的第一发送时间与第二发送时间的时间间隔小于预设时间间隔。若满足第二预设条件则进入步骤 S512。若不满足第二预设条件，则进入步骤 S513。

步骤 S511：将目标域名以及包含目标域名的发送时间，添加至外网设备的历史域名记录中，并设置目标域名的命中次数为 1。

步骤 S512：丢弃所述目标 DNS 应答报文。

步骤 S513：将目标 DNS 应答报文转发至内网设备。

步骤 S514：将目标 DNS 应答报文的流量值添加至流量监控表中。

步骤 S515：如果流量监控表中的流量值是否大于预设流量值，则在动态白名单中删除外网设备的源地址，并将外网设备的源地址加入至动态黑名单中。

步骤 S516：定期计算命中次数超过预设次数的域名数量与所有域名数量的比值。

步骤 S517：如果比值大于预设比值，则删除所述动态白名单中的所述外网设备的源地址，将所述外网设备的源地址添加至动态黑名单中。

通过图 5 所示的实施例，可以过滤所有类型的 DNS 应答攻击：

针对虚假源类型的 DNS 应答攻击：通过步骤 S503 动态白名单的方式即可过滤掉；针对真实源的 DNS 应答攻击方式一（攻击报文中的域名随机变化），采用步骤 S508 的方式（域名首包丢弃机制）即可过滤掉；针对真实源的 DNS 应答攻击的方式二（攻击报文中的域名个数有限或不变，相同域名攻击报文之间的间隔小于 1 秒），通过步骤 S510 的判断即可过滤掉；针对真实源的 DNS 应答攻击的方式三（攻击报文中的域名比较多但是周期性变化，相同域名攻击报文之间的间隔大于 1 秒），通过步骤 S515-S517 即可

过滤掉。

因此本申请可以过滤所有类型的 DNS 应答攻击，从而缓解 DNS 应答攻击对业务和网络造成的冲击。

与本申请提供的一种网络攻击的防御方法相对应，本申请还提供了一种网络攻击的防御装置。如图 6 所示，本装置包括：

接收单元 61，用于接收外网设备旨在向内网设备发送的目标 DNS 应答报文；

判断单元 62，用于在动态白名单包含所述目标 DNS 应答报文中的源地址的情况下，判断所述目标 DNS 应答报文是否满足预设条件；

第一丢弃单元 63，用于若所述目标 DNS 应答报文满足预设条件，则丢弃所述目标 DNS 应答报文；

其中，所述预设条件至少包括：所述目标 DNS 应答报文中的目标域名不包含在历史域名记录中，所述历史域名记录中的每个历史域名均从所述外网设备所发送的历史 DNS 应答报文中提取。

所述预设条件还包括：所述外网设备发起访问所述目标域名的第一发送时间与第二发送时间的时间间隔小于预设时间间隔。其中，所述第一发送时间为所述目标 DNS 应答报文的发送时间，所述第二发送时间为所述外网设备在所述第一发送时间之前最近一次发送包含所述目标域名的 DNS 应答报文的时间。

所述预设条件还包括：所述目标 DNS 应答报文的流量值及历史 DNS 应答报文的流量值的总和流量值大于所述预设流量值；其中，所述历史 DNS 应答报文为所述外网设备在发送目标 DNS 应答报文之前所发送的所有 DNS 应答报文。

如图 7 所示，本申请还提供的一种网络攻击的防御装置，还包括：

转发单元 64，用于在所述时间间隔不小于预设时间间隔情况下，将所述目标 DNS 应答报文转发给所述内网设备。

存储单元 65，用于若所述目标 DNS 应答报文中的目标域名不包含在历史域名记录中，则将所述目标域名和所述目标 DNS 应答报文的发送时间，存储在所述历史域名记录中。

比值计算单元 66，用于依据与所述外网设备的源地址对应的所述历史域名记录，计算命中次数超过预设次数的域名数量与所有域名数量的比值；其中，所述历史域名记录

中包含所述外网设备所发送的历史 DNS 应答报文中所有域名以及每个域名的命中次数；

第一删除单元 67，用于若所述比值大于预设比值，则删除所述动态白名单中的所述外网设备的源地址；

第一添加单元 68，用于将所述外网设备的源地址添加至动态黑名单中。

命中次数计算单元 69，用于在一个 DNS 应答报文被丢弃之后，在所述历史域名记录中查找该 DNS 应答报文中的域名；将所述域名的命中次数增加 1；其中，每个域名的命中次数的初始值为零。

由以上内容可以看出，本申请具有以下有益效果：

本申请实施例在确认目标 DNS 应答报文中源地址在动态白名单内后，即可确认发起目标 DNS 应答报文的外网设备非虚假源而是真实源。真实源发起 DNS 应答攻击的一种方式为，频繁发送包含不同域名的 DNS 应答报文来攻击内网设备。因此本申请中设有一个历史域名记录，其中记录有外网设备所发送的所有域名。

当目标 DNS 应答报文中的目标域名不包含在历史域名记录中时，则表明外网设备为首次发送包含目标域名的 DNS 应答报文。在此情况下，目标 DNS 应答报文可能是由外网设备以不同域名方式发起 DNS 应答攻击，为了避免内网设备遭受攻击，此时丢弃所述目标 DNS 应答报文。

由于正常的外网设备具有自动重发机制，如果正常的外网设备发送的 DNS 应答报文被丢弃之后，正常的外网设备会重新发送目标 DNS 应答报文，从而不影响正常的 DNS 应答报文发送至内网设备。而具有攻击性的外网设备则不具有自动重发机制，所以本申请可以过滤掉真实源以不同域名的方式来攻击内网设备的 DNS 应答报文，从而缓解 DNS 应答攻击对业务和网络造成的冲击。

如图 8 所示，本申请还提供的一种网络攻击的防御装置，还包括：

流量计算单元 71，用于在所述外网设备的源地址发送一个 DNS 应答报文之后，在所述历史 DNS 应答报文的流量值上叠加该 DNS 应答报文的流量值；所述历史 DNS 应答报文的流量值的初始值为零。

第二删除单元 72，用于在所述总和流量值大于所述预设流量值的情况下，删除所述动态白名单中的所述源地址；

第二添加单元 73，用于将所述源地址加入至动态黑名单中。

第二丢弃单元 74，用于在动态黑名单中包含所述目标 DNS 应答报文中的源地址的

情况下，丢弃所述目标 DNS 应答报文。

参见图 1，本申请提供了一种网络攻击的防御系统，包括：外网设备 100、路由设备 200，清洗设备 400 和内网设备 300；

所述外网设备 100，用于向清洗设备 400 发送旨在向内网设备 300 发送的目标 DNS 应答报文。

所述清洗设备 400，用于接收外网设备旨在向内网设备发送的目标 DNS 应答报文；在动态白名单包含所述目标 DNS 应答报文中的源地址的情况下，判断所述目标 DNS 应答报文是否满足预设条件；若所述目标 DNS 应答报文满足预设条件，则丢弃所述目标 DNS 应答报文；其中，所述预设条件至少包括：所述目标 DNS 应答报文中的目标域名不包含在历史域名记录中，所述历史域名记录中的每个历史域名均从所述外网设备所发送的历史 DNS 应答报文中提取；

内网设备 300，用于接收清洗设备清洗后的 DNS 应答报文。

本系统具有以下有益效果：

本申请实施例在确认目标 DNS 应答报文中源地址在动态白名单内后，即可确认发起目标 DNS 应答报文的外网设备非虚假源而是真实源。真实源发起 DNS 应答攻击的一种方式为，频繁发送包含不同域名的 DNS 应答报文来攻击内网设备。因此本申请中设有一个历史域名记录，其中记录有外网设备所发送的所有域名。

当目标 DNS 应答报文中的目标域名不包含在历史域名记录中时，则表明外网设备为首次发送包含目标域名的 DNS 应答报文。在此情况下，目标 DNS 应答报文可能是由外网设备以不同域名方式发起 DNS 应答攻击，为了避免内网设备遭受攻击，此时丢弃所述目标 DNS 应答报文。

由于正常的外网设备具有自动重发机制，如果正常的外网设备发送的 DNS 应答报文被丢弃之后，正常的外网设备会重新发送目标 DNS 应答报文，从而不影响正常的 DNS 应答报文发送至内网设备。而具有攻击性的外网设备则不具有自动重发机制，所以本申请可以过滤掉真实源以不同域名的方式来攻击内网设备的 DNS 应答报文，从而缓解 DNS 应答攻击对业务和网络造成的冲击。

本实施例方法所述的功能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设备可读取存储介质中。基于这样的理解，本申请实施例

对现有技术做出贡献的部分或者该技术方案的部分可以以软件产品的形式体现出来，该软件产品存储在一个存储介质中，包括若干指令用以使得一台计算设备（可以是个人计算机，服务器，移动计算设备或者网络设备等）执行本申请各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U 盘、移动硬盘、只读存储器（ROM，Read-Only Memory）、随机存取存储器（RAM，Random Access Memory）、磁碟或者光盘等各种可以存储程序代码的介质。

本说明书中各个实施例采用递进的方式描述，每个实施例重点说明的都是与其它实施例的不同之处，各个实施例之间相同或相似部分互相参见即可。

对所公开的实施例的上述说明，使本领域专业技术人员能够实现或使用本申请。对这些实施例的多种修改对本领域的专业技术人员来说将是显而易见的，本文中所定义的一般原理可以在不脱离本申请的精神或范围的情况下，在其它实施例中实现。因此，本申请将不会被限制于本文所示的这些实施例，而是要符合与本文所公开的原理和新颖特点相一致的最宽的范围。

权 利 要 求 书

1、一种网络攻击的防御方法，其特征在于，包括：

接收外网设备旨在向内网设备发送的目标DNS应答报文；

在动态白名单包含所述目标 DNS 应答报文中的源地址的情况下，判断所述目标DNS应答报文是否满足预设条件；

若所述目标DNS应答报文满足预设条件，则丢弃所述目标DNS应答报文；

其中，所述预设条件至少包括：所述目标 DNS 应答报文中的目标域名不包含在历史域名记录中，所述历史域名记录中的每个历史域名均从所述外网设备所发送的历史DNS应答报文中提取。

2、如权利要求1所述的方法，其特征在于，所述预设条件还包括：

所述外网设备发起访问所述目标域名的第一发送时间与第二发送时间的时间间隔小于预设时间间隔；

其中，所述第一发送时间为所述目标 DNS 应答报文的发送时间，所述第二发送时间为所述外网设备在所述第一发送时间之前最近一次发送包含所述目标域名的 DNS 应答报文的时间。

3、如权利要求2所述的方法，其特征在于，还包括：

在所述时间间隔不小于预设时间间隔情况下，将所述目标 DNS 应答报文转发给所述内网设备。

4、如权利要求1所述的方法，其特征在于，还包括：

若所述目标 DNS 应答报文中的目标域名不包含在历史域名记录中，则将所述目标域名和所述目标DNS应答报文的发送时间，存储在所述历史域名记录中。

5、如权利要求4所述的方法，其特征在于，还包括：

依据与所述外网设备的源地址对应的所述历史域名记录，计算命中次数超过预设次数的域名数量与所有域名数量的比值；其中，所述历史域名记录中包含所述外网设备所发送的历史 DNS 应答报文中所有域名以及每个域名的命中次数；所述预设次数为不小于3的自然数；

若所述比值大于预设比值，则删除所述动态白名单中的所述外网设备的源地址；

将所述外网设备的源地址添加至动态黑名单中。

6、如权利要求 5 所述的方法，其特征在于，所述历史域名记录中每个域名的命中次数的计算方式包括：

在接收一个 DNS 应答报文之后，在所述历史域名记录中查找该 DNS 应答报文中的域名；

将所述域名的命中次数增加 1；其中，每个域名的命中次数的初始值为零。

7、如权利要求 1 所述的方法，其特征在于，所述预设条件还包括：

所述目标 DNS 应答报文的流量值及历史 DNS 应答报文的流量值的总和流量值大于所述预设流量值；

其中，所述历史 DNS 应答报文为所述外网设备在发送目标 DNS 应答报文之前所发送的所有 DNS 应答报文。

8、如权利要求 7 所述的方法，其特征在于，还包括：

在所述总和流量值大于所述预设流量值的情况下，删除所述动态白名单中的所述源地址；

将所述源地址加入至动态黑名单中。

9、如权利要求 8 所述的方法，其特征在于，所述历史 DNS 应答报文的流量值计算过程包括：

在所述外网设备的源地址发送一个 DNS 应答报文之后，在所述历史 DNS 应答报文的流量值上叠加该 DNS 应答报文的流量值；所述历史 DNS 应答报文的流量值的初始值为零。

10、如权利要求 1-8 任一项所述的方法，其特征在于，还包括：

在动态黑名单中包含所述目标 DNS 应答报文中的源地址的情况下，丢弃所述目标 DNS 应答报文。

11、一种网络攻击的防御装置，其特征在于，包括：

接收单元，用于接收外网设备旨在向内网设备发送的目标 DNS 应答报文；

判断单元，用于在动态白名单包含所述目标 DNS 应答报文中的源地址的情况下，判断所述目标 DNS 应答报文是否满足预设条件；

第一丢弃单元，用于若所述目标 DNS 应答报文满足预设条件，则丢弃所述目标 DNS 应答报文；

其中，所述预设条件至少包括：所述目标 DNS 应答报文中的目标域名不包含在历史域名记录中，所述历史域名记录中的每个历史域名均从所述外网设备所发送的历史 DNS 应答报文中提取。

12、如权利要求 11 所述的装置，其特征在于，所述预设条件还包括：

所述外网设备发起访问所述目标域名的第一发送时间与第二发送时间的时间间隔小于预设时间间隔；

其中，所述第一发送时间为所述目标 DNS 应答报文的发送时间，所述第二发送时间为所述外网设备在所述第一发送时间之前最近一次发送包含所述目标域名的 DNS 应答报文的时间。

13、如权利要求 12 所述的装置，其特征在于，还包括：

转发单元，用于在所述时间间隔不小于预设时间间隔情况下，将所述目标 DNS 应答报文转发给所述内网设备。

14、如权利要求 11 所述的装置，其特征在于，还包括：

存储单元，用于若所述目标 DNS 应答报文中的目标域名不包含在历史域名记录中，则将所述目标域名和所述目标 DNS 应答报文的发送时间，存储在所述历史域名记录中。

15、如权利要求 14 所述的装置，其特征在于，还包括：

比值计算单元，用于依据与所述外网设备的源地址对应的所述历史域名记录，计算命中次数超过预设次数的域名数量与所有域名数量的比值；其中，所述历史域名记录中包含所述外网设备所发送的历史 DNS 应答报文中所有域名以及每个域名的命中次数；所述预设次数为不小于 3 的自然数；

第一删除单元，用于若所述比值大于预设比值，则删除所述动态白名单中的所述外网设备的源地址；

第一添加单元，用于将所述外网设备的源地址添加至动态黑名单中。

16、如权利要求 15 所述的装置，其特征在于，还包括：

命中次数计算单元，用于在接收一个 DNS 应答报文之后，在所述历史域名记录中查找该 DNS 应答报文中的域名；将所述域名的命中次数增加 1；其中，每个域名的命中次数的初始值为零。

17、如权利要求 11 所述的装置，其特征在于，所述预设条件还包括：

所述目标 DNS 应答报文的流量值及历史 DNS 应答报文的流量值的总和流量值大于所述预设流量值；

其中，所述历史 DNS 应答报文为所述外网设备在发送目标 DNS 应答报文之前所发送的所有 DNS 应答报文。

18、如权利要求 17 所述的装置，其特征在于，还包括：

第二删除单元，用于在所述总和流量值大于所述预设流量值的情况下，删除所述动态白名单中的所述源地址；

第二添加单元，用于将所述源地址加入至动态黑名单中。

19、如权利要求 18 所述的装置，其特征在于，还包括：

流量计算单元，用于在所述外网设备的源地址发送一个 DNS 应答报文之后，在所述历史 DNS 应答报文的流量值上叠加该 DNS 应答报文的流量值；所述历史 DNS 应答报文的流量值的初始值为零。

20、如权利要求 11-18 任一项所述的装置，其特征在于，还包括：

第二丢弃单元，用于在动态黑名单中包含所述目标 DNS 应答报文中的源地址的情况下，丢弃所述目标 DNS 应答报文。

21、一种网络攻击的防御系统，其特征在于，包括：外网设备、清洗设备和内网设备；

所述外网设备，用于向清洗设备发送旨在向内网设备发送的目标 DNS 应答报文；

所述清洗设备，用于接收外网设备旨在向内网设备发送的目标 DNS 应答报文；在动态白名单包含所述目标 DNS 应答报文中的源地址的情况下，判断所述目标 DNS 应答报文是否满足预设条件；若所述目标 DNS 应答报文满足预设条件，则丢弃所述目标 DNS 应答报文；其中，所述预设条件至少包括：所述目标 DNS 应答报文中的目标域名不包含在历史域名记录中，所述历史域名记录中的每个历史域名均从所述外网设备所发送的历史 DNS 应答报文中提取；

内网设备，用于接收清洗设备清洗后的 DNS 应答报文。

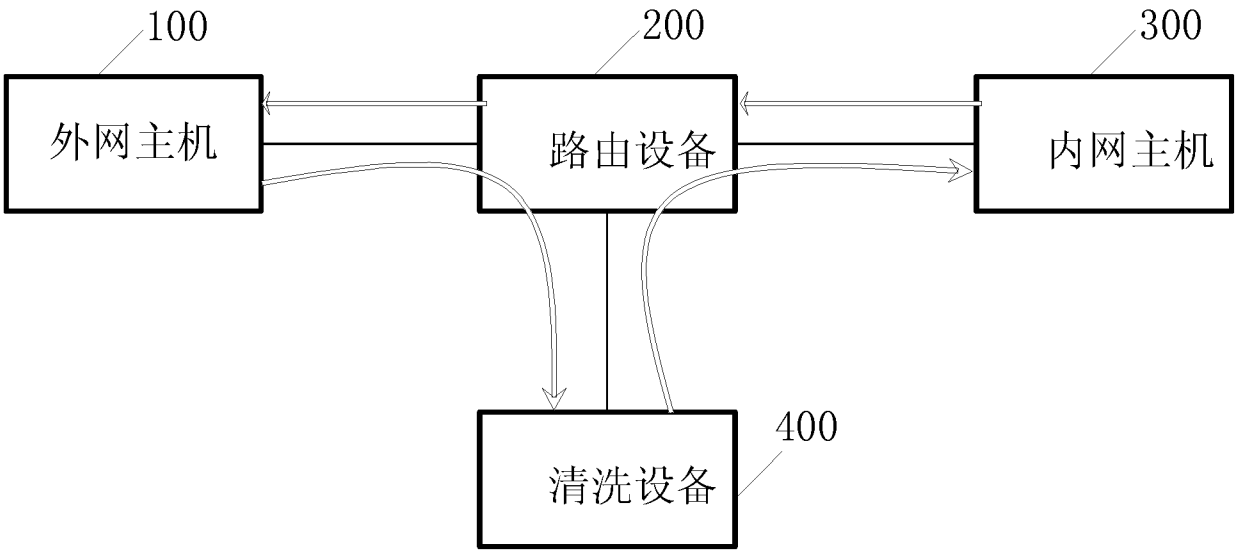
100
200
300
外网主机
路由设备
内网主机
400
清洗设备

图 1

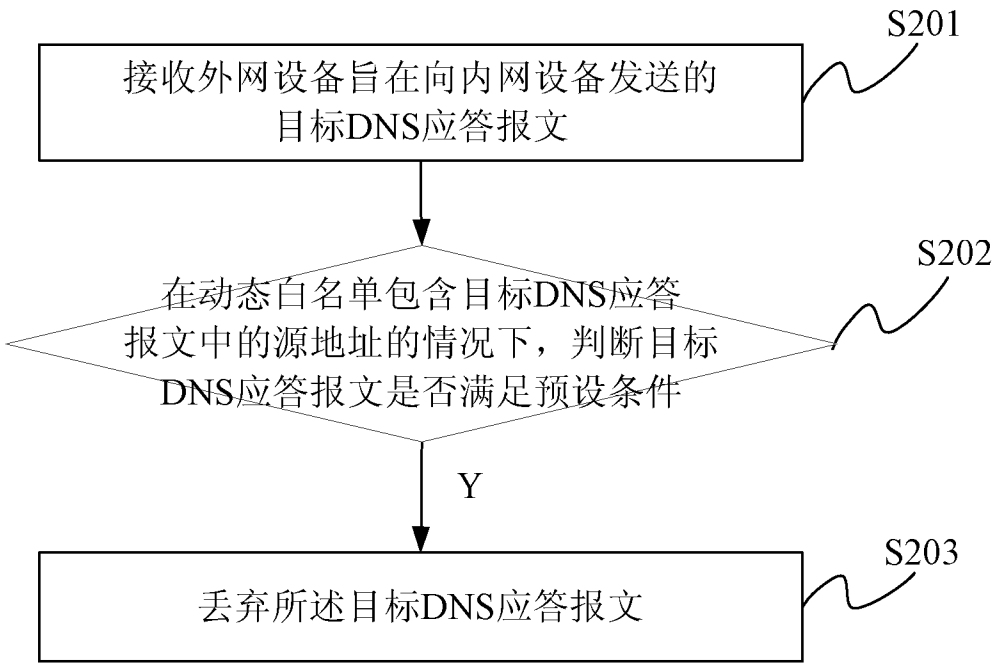
S201
接收外网设备旨在向内网设备发送的目标DNS应答报文
S202
在动态白名单包含目标DNS应答报文中的源地址的情况下，判断目标DNS应答报文是否满足预设条件
Y
S203
丢弃所述目标DNS应答报文

图 2

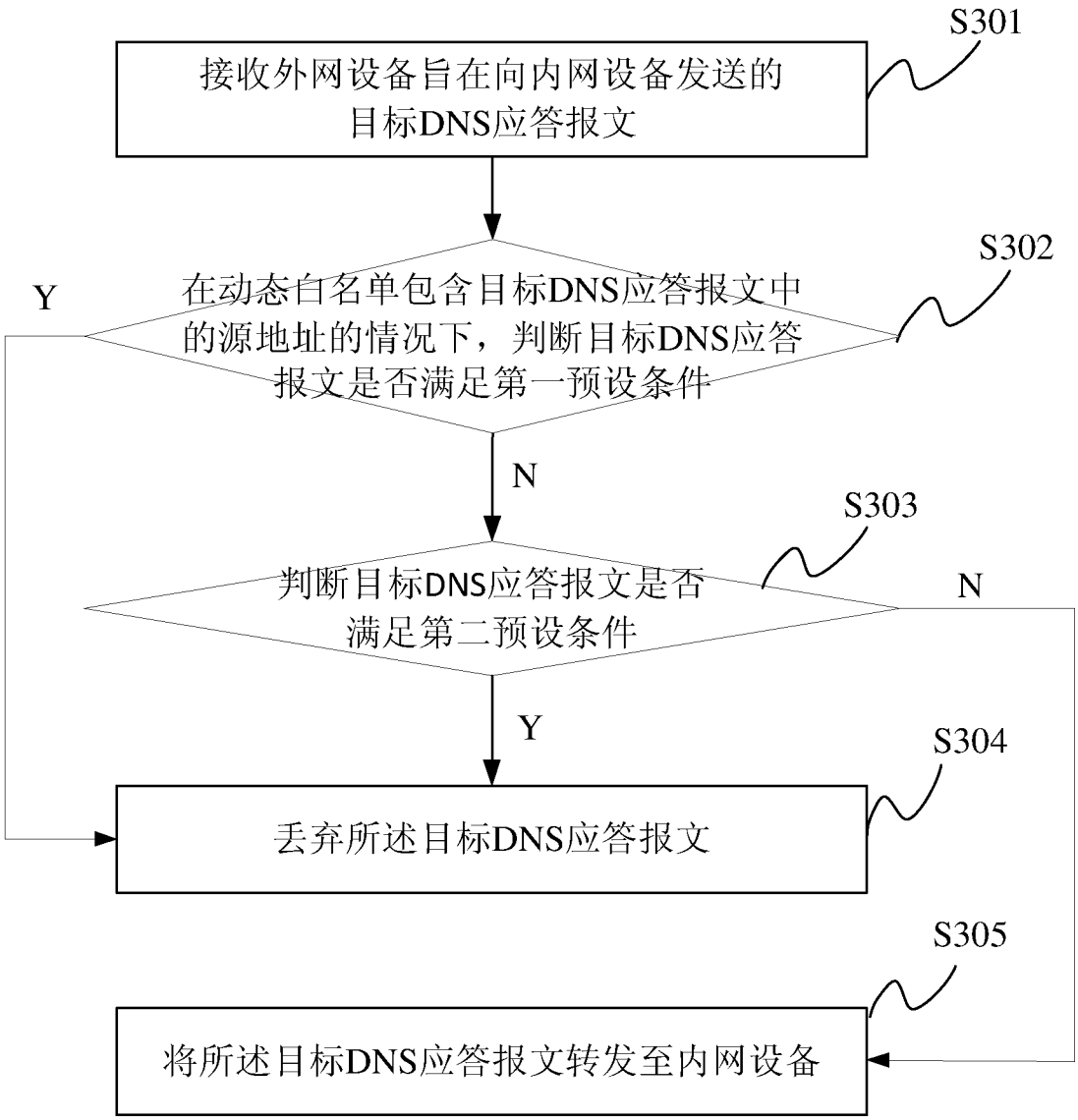
S301
接收外网设备旨在向内网设备发送的目标DNS应答报文
S302
在动态白名单包含目标DNS应答报文中的源地址的情况下，判断目标DNS应答报文是否满足第一预设条件
Y
N
S303
判断目标DNS应答报文是否满足第二预设条件
N
Y
S304
丢弃所述目标DNS应答报文
S305
将所述目标DNS应答报文转发至内网设备

图 3

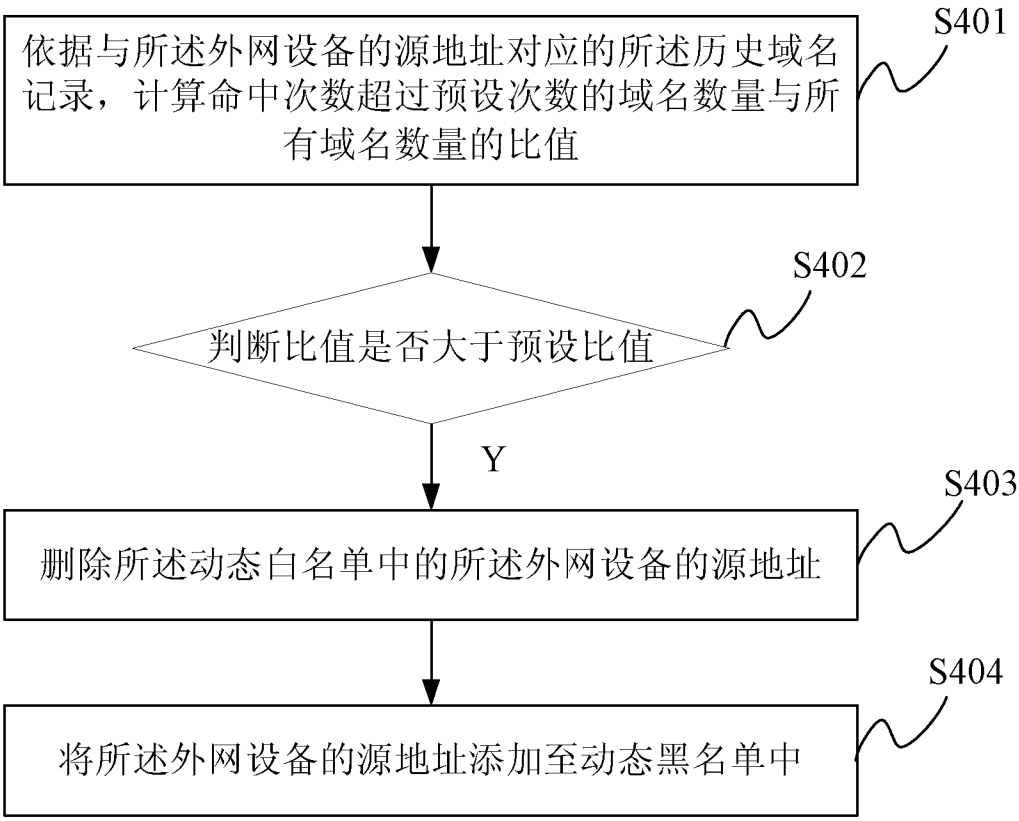
依据与所述外网设备的源地址对应的所述历史域名记录，计算命中次数超过预设次数的域名数量与所有域名数量的比值
S401
判断比值是否大于预设比值
S402
Y
删除所述动态白名单中的所述外网设备的源地址
S403
将所述外网设备的源地址添加至动态黑名单中
S404

图 4

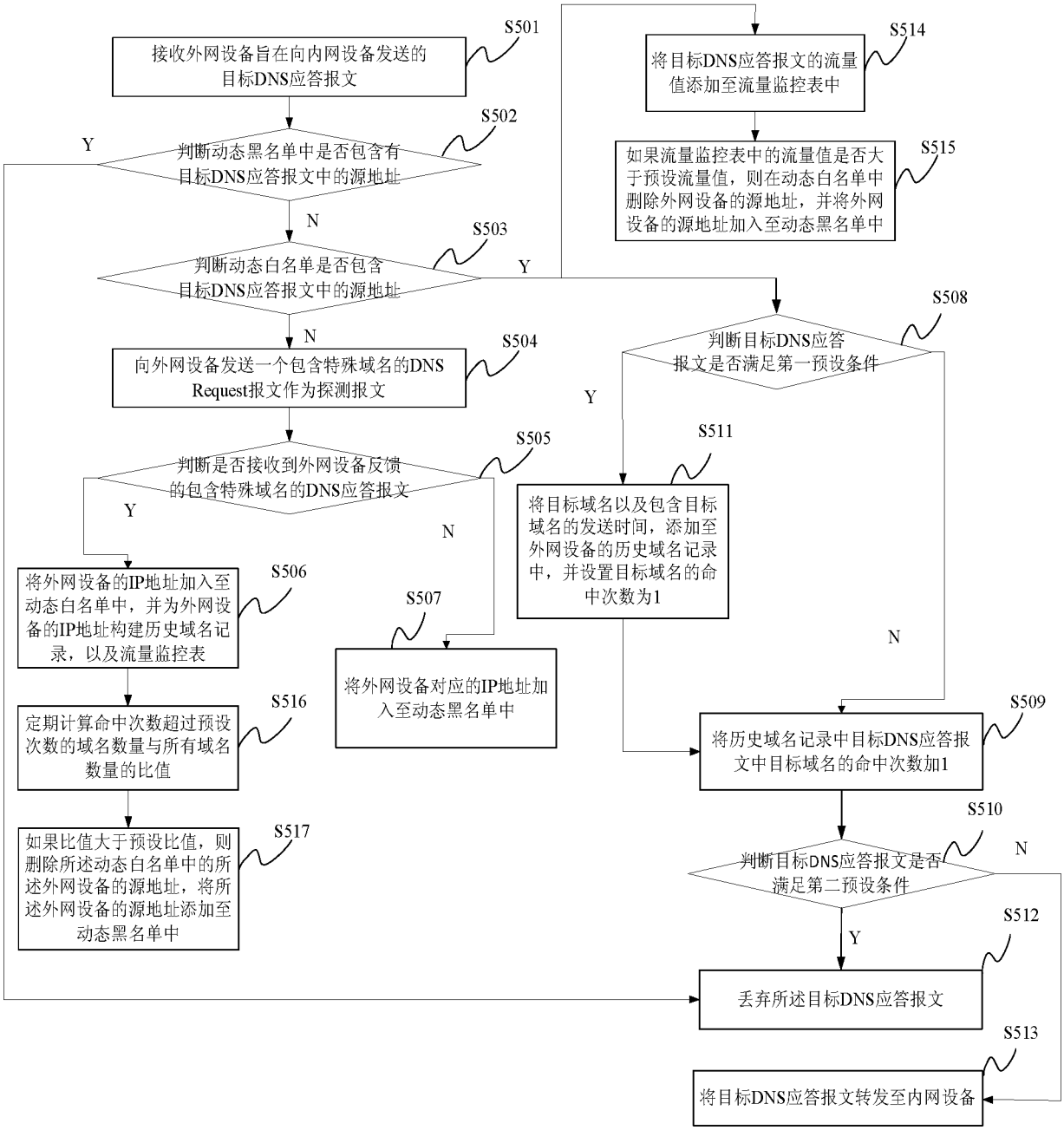
S501
接收外网设备旨在向内网设备发送的目标DNS应答报文
S502
判断动态黑名单中是否包含有目标DNS应答报文中的源地址
Y
N
S503
判断动态白名单是否包含目标DNS应答报文中的源地址
Y
N
S504
向外网设备发送一个包含特殊域名的DNS Request报文作为探测报文
S505
判断是否接收到外网设备反馈的包含特殊域名的DNS应答报文
Y
N
S506
将外网设备的IP地址加入至动态白名单中，并为外网设备的IP地址构建历史域名记录，以及流量监控表
S507
将外网设备对应的IP地址加入至动态黑名单中
S516
定期计算命中次数超过预设次数的域名数量与所有域名数量的比值
S517
如果比值大于预设比值，则删除所述动态白名单中的所述外网设备的源地址，将所述外网设备的源地址添加至动态黑名单中
S514
将目标DNS应答报文的流量值添加至流量监控表中
S515
如果流量监控表中的流量值是否大于预设流量值，则在动态白名单中删除外网设备的源地址，并将外网设备的源地址加入至动态黑名单中
S508
判断目标DNS应答报文是否满足第一预设条件
Y
N
S511
将目标域名以及包含目标域名的发送时间，添加至外网设备的历史域名记录中，并设置目标域名的命中次数为1
S509
将历史域名记录中目标DNS应答报文中目标域名的命中次数加1
S510
判断目标DNS应答报文是否满足第二预设条件
N
Y
S512
丢弃所述目标DNS应答报文
S513
将目标DNS应答报文转发至内网设备

图 5

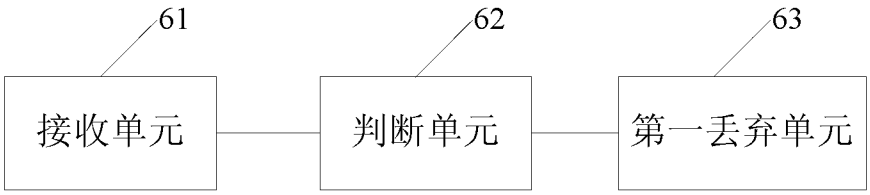
61
62
63
接收单元
判断单元
第一丢弃单元

图 6

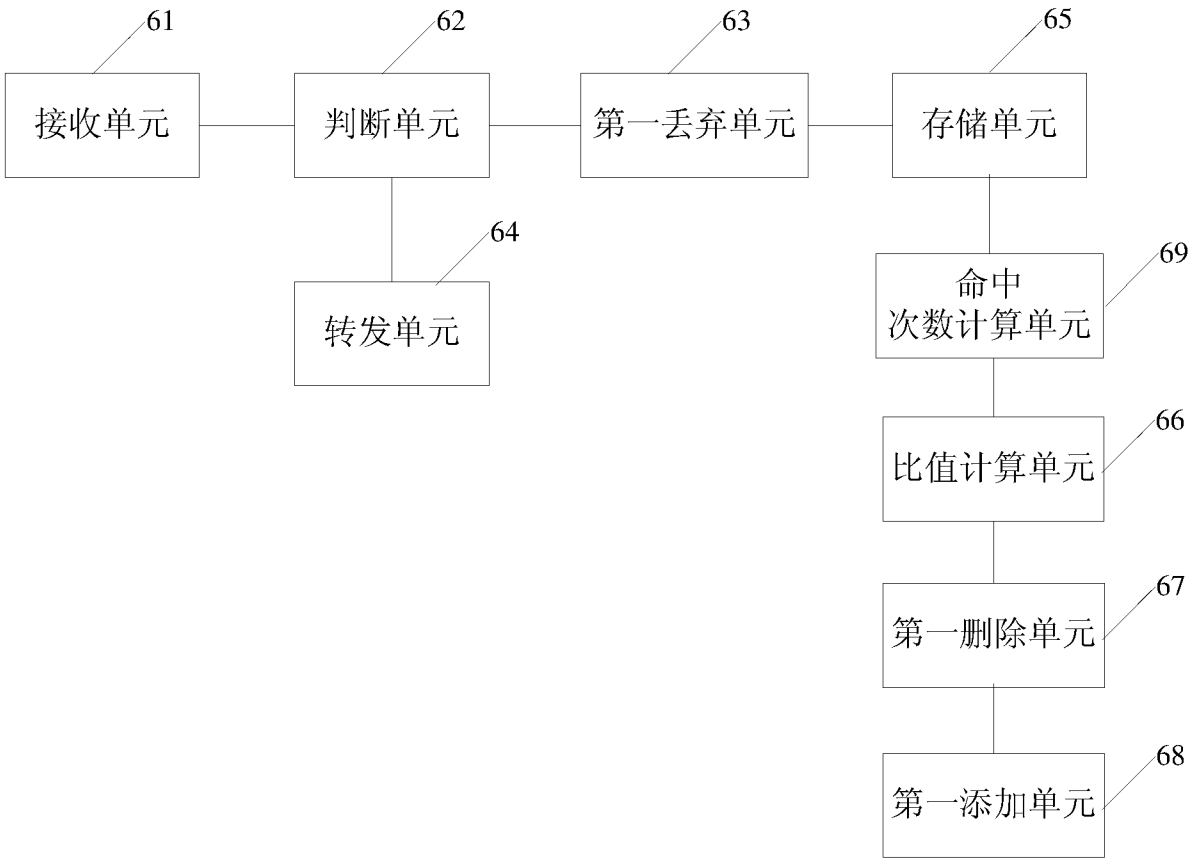
61
62
63
65
接收单元
判断单元
第一丢弃单元
存储单元
64
转发单元
69
命中
次数计算单元
66
比值计算单元
67
第一删除单元
68
第一添加单元

图 7

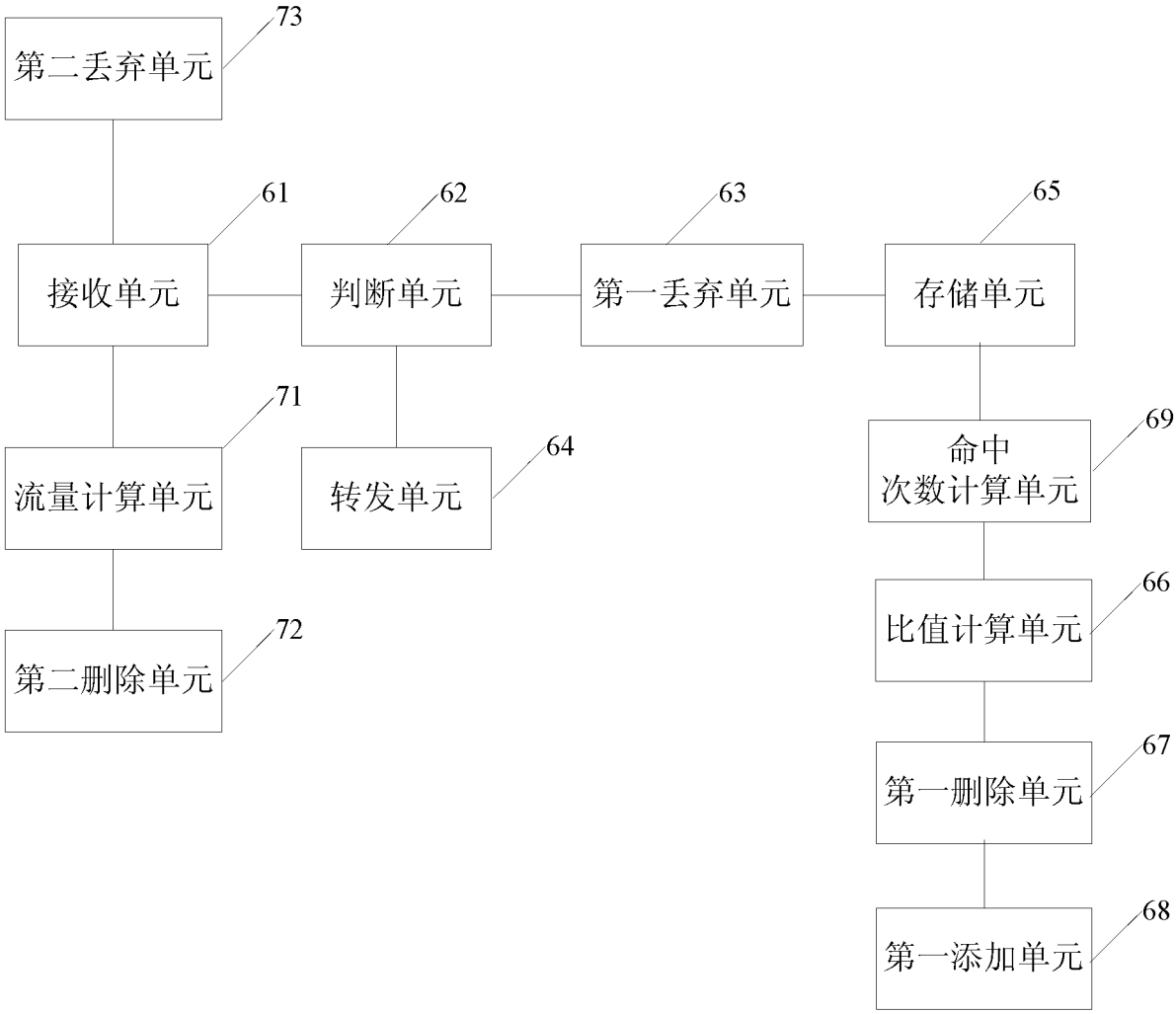
第二丢弃单元
73
61
62
63
65
接收单元
判断单元
第一丢弃单元
存储单元
71
64
69
流量计算单元
转发单元
命中
次数计算单元
66
比值计算单元
72
第二删除单元
67
第一删除单元
68
第一添加单元

图 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/093186

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L; H04Q; H04W

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI; EPODOC; CNPAT; CNKI: domain name system, domain name resolution, distributed denial of service, DNS, attack+, source, target, white list, history, response, DDoS, retrans+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 103856487 A (OPZOON TECHNOLOGY CO., LTD.), 11 June 2014 (11.06.2014), description, paragraph [0006]	1-21
A	CN 102075592 A (LV, Xiaowen et al.), 25 May 2011 (25.05.2011), the whole document	1-21
A	CN 104125242 A (BEIJING UNIONREAD INFORMATION TECHNOLOGY LTD.), 29 October 2014 (29.10.2014), the whole document	1-21
A	CN 103391272 A (TENCENT INC.), 13 November 2013 (13.11.2013), the whole document	1-21
A	US 2013232574 A1 (COX COMMUNICATIONS, INC.), 05 September 2013 (05.09.2013), the whole document	1-21

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
08 October 2016 (08.10.2016)	**26 October 2016 (26.10.2016)**
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer **NIU, Xiangchao** Telephone No.: (86-10) **010-62413421**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2016/093186

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 103856487 A	11 June 2014	None	
CN 102075592 A	25 May 2011	None	
CN 104125242 A	29 October 2014	None	
CN 103391272 A	13 November 2013	None	
US 2013232574 A1	05 September 2013	None	

国际检索报告

国际申请号
PCT/CN2016/093186

A. 主题的分类

H04L 29/06(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L; H04Q; H04W

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)

WPI;EPODOC;CNPAT;CNKI:域名系统，域名解析，攻击，源，目标，白名单，历史，应答，响应，分布式拒绝服务，重发，重新发送，DNS，attack+，source，target，white list，history，response，DDoS，retrans+

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
A	CN 103856487 A (汉柏科技有限公司) 2014年 6月 11日 (2014-06-11) 说明书第[0006]段	1-21
A	CN 102075592 A (吕晓雯等) 2011年 5月 25日 (2011-05-25) 全文	1-21
A	CN 104125242 A (北京阅联信息技术有限公司) 2014年 10月 29日 (2014-10-29) 全文	1-21
A	CN 103391272 A (深圳市腾讯计算机系统有限公司) 2013年 11月 13日 (2013-11-13) 全文	1-21
A	US 2013232574 A1 (COX COMMUNICATIONS, INC.) 2013年 9月 5日 (2013-09-05) 全文	1-21

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2016年 10月 8日	2016年 10月 26日

ISA/CN的名称和邮寄地址	受权官员
中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088	牛相潮
传真号 (86-10)62019451	电话号码 (86-10)010-62413421

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2016/093186

检索报告引用的专利文件			公布日 (年/月/日)	同族专利	公布日 (年/月/日)
CN	103856487	A	2014年 6月 11日	无	
CN	102075592	A	2011年 5月 25日	无	
CN	104125242	A	2014年 10月 29日	无	
CN	103391272	A	2013年 11月 13日	无	
US	2013232574	A1	2013年 9月 5日	无	