(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 117220969 A
(43)申请公布日 2023.12.12

(21)申请号 202311234772.7

(22)申请日 2023.09.21

(71)申请人 武汉思普崚技术有限公司
地址 430070 湖北省武汉市武汉东湖新技术开发区光谷大道308号光谷动力节能环保科技企业孵化器(加速器)一期11栋3层01室

(72)发明人 宋晓勇

(74)专利代理机构 北京弘权知识产权代理有限公司 11363
专利代理师 朱紫晓 孙亚芹

(51)Int.Cl.
H04L 9/40(2022.01)
H04L 61/4511(2022.01)

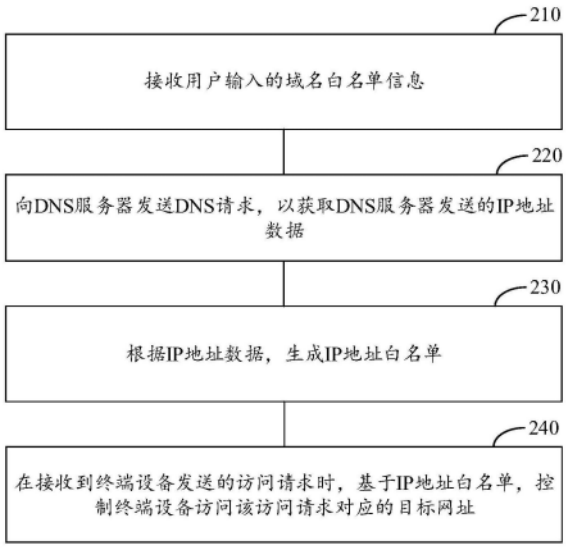
权利要求书2页 说明书10页 附图6页

(54)发明名称

访问控制方法、装置、网关设备及存储介质

(57)摘要

本发明实施例涉及网络安全技术领域,公开了一种访问控制方法、装置、网关设备及存储介质,该方法应用于网关设备,包括:接收用户输入的域名白名单;向DNS服务器发送DNS请求,以获取所述DNS服务器发送的IP地址数据,所述IP地址数据包括所述域名白名单中各域名对应的IP地址;根据所述IP地址数据,生成IP地址白名单;在接收到终端设备发送的访问请求时,基于所述IP地址白名单,控制所述终端设备访问所述访问请求对应的目标网址。应用本发明的技术方案,能够提高网络系统的安全性。



CN 117220969 A

1.一种访问控制方法,其特征在于,应用于网关设备,所述方法包括:

接收用户输入的域名白名单信息;

向DNS服务器发送DNS请求,以获取所述DNS服务器发送的IP地址数据,所述IP地址数据包括所述域名白名单信息中各域名对应的IP地址;

根据所述IP地址数据,生成IP地址白名单;

在接收到终端设备发送的访问请求时,基于所述IP地址白名单,控制所述终端设备访问所述访问请求对应的目标网址。

2.根据权利要求1所述的方法,其特征在于,所述向DNS服务器发送DNS请求,以获取所述DNS服务器发送的IP地址数据,包括:

按照预设时间间隔向所述DNS服务器发送所述DNS请求,直至获取到所述DNS服务器发送的所述IP地址数据。

3.根据权利要求1所述的方法,其特征在于,所述IP地址数据还包括所述域名白名单信息中各域名对应的IP地址的有效期,所述根据所述IP地址数据,生成IP地址白名单,包括:

基于所述IP地址数据,确定所述IP地址数据中各个IP地址的有效期;

将所述IP地址数据中的各个IP地址和各所述IP地址的有效期添加至所述IP地址白名单。

4.根据权利要求3所述的方法,其特征在于,所述在接收到终端设备发送的访问请求时,基于所述IP地址白名单,控制所述终端设备访问所述访问请求对应的目标网址,包括:

根据所述访问请求,确定所述目标网址和所述目标网址的目标IP地址;

将所述目标IP地址与所述IP地址白名单中的IP地址进行匹配;

在确定所述目标IP地址与所述IP地址白名单中的任一IP地址匹配的情况下,允许所述终端设备访问所述目标网址;

在确定所述目标IP地址与所述IP地址白名单中的各个IP地址不匹配的情况下,禁止所述终端设备访问所述目标网址。

5.根据权利要求3所述的方法,其特征在于,所述将所述IP地址数据中的各个IP地址和各所述IP地址的有效期添加至所述IP地址白名单,包括:

在所述IP地址白名单中查找所述IP地址数据中的各个IP地址;

若所述IP地址白名单中存在所述IP地址数据中的任一IP地址,则停止将所述任一IP地址添加至所述IP地址白名单;

若所述IP地址白名单中不存在所述IP地址数据中的任一IP地址,则将所述任一IP地址添加至所述IP地址白名单。

6.根据权利要求3所述的方法,其特征在于,所述方法还包括:

记录所述IP地址数据中各所述IP地址在所述IP地址白名单中的存活时间,以在所述IP地址数据中任一IP地址的存活时间大于存活时间阈值时,向所述DNS服务器发送地址更新请求,以获取所述DNS服务器发送的更新后的IP地址数据。

7.根据权利要求4所述的方法,其特征在于,所述目标IP地址是由所述DNS服务器响应于所述终端设备发送的IP地址获取请求,发送给所述终端设备的。

8.一种访问控制装置,其特征在于,应用于网关设备,所述装置包括:

接收模块,用于接收用户输入的域名白名单信息;

获取模块,用于向DNS服务器发送DNS请求,以获取所述DNS服务器发送的IP地址数据,所述IP地址数据包括所述域名白名单信息中各域名对应的IP地址;

生成模块,用于根据所述IP地址数据,生成IP地址白名单;

控制模块,用于在接收到终端设备发送的访问请求时,基于所述IP地址白名单,控制所述终端设备访问所述访问请求对应的目标网址。

9.一种网关设备,其特征在于,包括:

处理器;以及

存储器,用于存储所述处理器的可执行指令;

其中,所述处理器配置为经由执行所述可执行指令来执行如权利要求1-7任意一项所述的访问控制方法的操作。

10.一种计算机可读存储介质,其特征在于,所述存储介质中存储有至少一可执行指令,所述可执行指令在网关设备上运行时,使得网关设备执行如权利要求1-7任意一项所述的访问控制方法的操作。

访问控制方法、装置、网关设备及存储介质

技术领域

[0001] 本发明实施例涉及网络安全技术领域,具体涉及一种访问控制方法、装置、网关设备及存储介质。

背景技术

[0002] 互联网技术的发展为人们的工作带来了极大的便利。例如,企业员工可以使用互联网访问网站,以获取其需要的信息。

[0003] 在用户通过终端访问网站时,终端会通过网关设备向DNS(Domain Name System,域名系统)服务器发送DNS请求,使得DNS服务器通过网关设备将网站对应的IP地址返回给终端,这样在终端访问网站时,便可以直接使用该网站的IP地址访问网站的网络资源。在这个过程中,为了确保安全性,网关设备可以利用黑白名单对终端的DNS请求和DNS服务器的回应报文进行安全校验,实现安全控制。

[0004] 然而,一些安全性要求比较高的企业往往会配置专用的DNS服务器,以便处理终端访问网站时的DNS请求,此时终端的DNS请求和DNS服务器的回应报文均不需要经过网关设备,所以网关设备配置的黑白名单便无法生效,也无法对终端的DNS请求和DNS服务器的回应报文进行安全校验,因此,终端访问网站的过程存在安全隐患。

发明内容

[0005] 鉴于上述问题,本发明实施例提供了一种访问控制方法、装置、网关设备及存储介质,用于解决现有技术中存在的数据报文的协议解析效率较低问题。

[0006] 根据本发明实施例的一个方面,提供了一种访问控制方法,应用于网关设备,所述方法包括:接收用户输入的域名白名单信息;向DNS服务器发送DNS请求,以获取所述DNS服务器发送的IP地址数据,所述IP地址数据包括所述域名白名单信息中各域名对应的IP地址;根据所述IP地址数据,生成IP地址白名单;在接收到终端设备发送的访问请求时,基于所述IP地址白名单,控制所述终端设备访问所述访问请求对应的目标网址。

[0007] 在一些实施例中,所述向DNS服务器发送DNS请求,以获取所述DNS服务器发送的IP地址数据,包括:按照预设时间间隔向所述DNS服务器发送所述DNS请求,直至获取到所述DNS服务器发送的所述IP地址数据。

[0008] 在一些实施例中,所述IP地址数据还包括所述域名白名单信息中各域名对应的IP地址的有效期,所述根据所述IP地址数据,生成IP地址白名单,包括:基于所述IP地址数据,确定所述IP地址数据中各个IP地址的有效期;将所述IP地址数据中的各个IP地址和各所述IP地址的有效期添加至所述IP地址白名单。

[0009] 在一些实施例中,所述在接收到终端设备发送的访问请求时,基于所述IP地址白名单,控制所述终端设备访问所述访问请求对应的目标网址,包括:根据所述访问请求,确定所述目标网址和所述目标网址的目标IP地址;将所述目标IP地址与所述IP地址白名单中的IP地址进行匹配;在确定所述目标IP地址与所述IP地址白名单中的任一IP地址匹配的情

况下,允许所述终端设备访问所述目标网址;在确定所述目标IP地址与所述IP地址白名单中的各个IP地址不匹配的情况下,禁止所述终端设备访问所述目标网址。

[0010] 在一些实施例中,所述将所述IP地址数据中的各个IP地址和各所述IP地址的有效期添加至所述IP地址白名单,包括:在所述IP地址白名单中查找所述IP地址数据中的各个IP地址;若所述IP地址白名单中存在所述IP地址数据中的任一IP地址,则停止将所述任一IP地址添加至所述IP地址白名单;若所述IP地址白名单中不存在所述IP地址数据中的任一IP地址,则将所述任一IP地址添加至所述IP地址白名单。

[0011] 在一些实施例中,所述方法还包括:记录所述IP地址数据中各所述IP地址在所述IP地址白名单中的存活时间,以在所述IP地址数据中任一IP地址的存活时间大于存活时间阈值时,向所述DNS服务器发送地址更新请求,以获取所述DNS服务器发送的更新后的IP地址数据。

[0012] 在一些实施例中,所述目标IP地址是由所述DNS服务器响应于所述终端设备发送的IP地址获取请求,发送给所述终端设备的。

[0013] 根据本发明实施例的另一方面,提供了一种访问控制装置,应用于网关设备,包括:接收模块,用于接收用户输入的域名白名单信息;获取模块,用于向DNS服务器发送DNS请求,以获取所述DNS服务器发送的IP地址数据,所述IP地址数据包括所述域名白名单信息中各域名对应的IP地址;生成模块,用于根据所述IP地址数据,生成IP地址白名单;控制模块,用于在接收到终端设备发送的访问请求时,基于所述IP地址白名单,控制所述终端设备访问所述访问请求对应的目标网址。

[0014] 在一些实施例中,所述获取模块用于按照预设时间间隔向所述DNS服务器发送所述DNS请求,直至获取到所述DNS服务器发送的所述IP地址数据。

[0015] 在一些实施例中,所述IP地址数据还包括所述域名白名单信息中各域名对应的IP地址的有效期,所述生成模块用于基于所述IP地址数据,确定所述IP地址数据中各个IP地址的有效期;将所述IP地址数据中的各个IP地址和各所述IP地址的有效期添加至所述IP地址白名单。

[0016] 在一些实施例中,所述控制模块用于根据所述访问请求,确定所述目标网址和所述目标网址的目标IP地址;将所述目标IP地址与所述IP地址白名单中的IP地址进行匹配;在确定所述目标IP地址与所述IP地址白名单中的任一IP地址匹配的情况下,允许所述终端设备访问所述目标网址;在确定所述目标IP地址与所述IP地址白名单中的各个IP地址不匹配的情况下,禁止所述终端设备访问所述目标网址。

[0017] 在一些实施例中,所述生成模块用于在所述IP地址白名单中查找所述IP地址数据中的各个IP地址;若所述IP地址白名单中存在所述IP地址数据中的任一IP地址,则停止将所述任一IP地址添加至所述IP地址白名单;若所述IP地址白名单中不存在所述IP地址数据中的任一IP地址,则将所述任一IP地址添加至所述IP地址白名单。

[0018] 在一些实施例中,所述获取模块还用于记录所述IP地址数据中各所述IP地址在所述IP地址白名单中的存活时间,以在所述IP地址数据中任一IP地址的存活时间大于存活时间阈值时,向所述DNS服务器发送地址更新请求,以获取所述DNS服务器发送的更新后的IP地址数据。

[0019] 在一些实施例中,所述目标IP地址是由所述DNS服务器响应于所述终端设备发送

的IP地址获取请求,发送给所述终端设备的。

[0020] 根据本发明实施例的另一方面,提供了一种网关设备,包括:处理器;以及存储器,用于存储所述处理器的可执行指令;其中,所述处理器配置为经由执行所述可执行指令来执行如上任意一项所述的访问控制方法的操作。

[0021] 根据本发明实施例的又一方面,提供了一种计算机可读存储介质,所述存储介质中存储有至少一可执行指令,所述可执行指令在网关设备上运行时,使得网关设备执行如上任意一项所述的访问控制方法的操作。

[0022] 综上,根据本发明实施例提供的访问控制方法、装置、网关设备及存储介质,能够接收用户输入的域名白名单信息,向DNS服务器发送DNS请求,以获取DNS服务器发送的IP地址数据,根据IP地址数据,生成IP地址白名单,从而在接收到终端设备发送的访问请求时,基于IP地址白名单,控制终端设备访问访问请求对应的目标网址。

[0023] 通过该方法,网关设备可以主动获取域名白名单信息对应的IP地址数据,并根据IP地址数据实现对终端设备的访问请求的安全控制,能够提高网络系统的安全性。

[0024] 上述说明仅是本发明实施例技术方案的概述,为了能够更清楚了解本发明实施例的技术手段,而可依照说明书的内容予以实施,并且为了让本发明实施例的上述和其它目的、特征和优点能够更明显易懂,以下特举本发明的具体实施方式。

附图说明

[0025] 附图仅用于示出实施方式,而并不认为是对本发明的限制。而且在整个附图中,用相同的参考符号表示相同的部件。在附图中:

[0026] 图1示出了相关技术中一种网络架构的示意图;

[0027] 图2示出了本发明实施例提供的一种访问控制方法的流程图;

[0028] 图3示出了本发明实施例提供的一种配置界面的示意图;

[0029] 图4示出了本发明实施例提供的一种访问控制的系统架构示意图;

[0030] 图5示出了本发明实施例提供的一种访问控制方法的子流程图;

[0031] 图6示出了本发明实施例提供的一种IP地址数据的处理方法的流程图;

[0032] 图7示出了本发明实施例提供的一种指令界面的示意图;

[0033] 图8示出了本发明实施例提供的另一种配置界面的示意图;

[0034] 图9示出了本发明实施例提供的另一种访问控制方法的子流程图;

[0035] 图10示出了本发明实施例提供的一种访问控制装置的结构示意图;

[0036] 图11示出了本发明实施例提供的一种网关设备的结构示意图。

具体实施方式

[0037] 下面将参照附图更详细地描述本发明的示例性实施例。虽然附图中显示了本发明的示例性实施例,然而应当理解,可以以各种形式实现本发明而不应被这里阐述的实施例所限制。

[0038] 为了确保网络安全,用户通过终端访问互联网可以通过网关设备完成,图1示出了相关技术中一种网络架构的示意图,如图1所示,当用户在终端的浏览器中输入网址A的地址时,即触发对网址A的访问,此时终端可以向公共DNS服务器发送DNS请求,使得公共DNS服

务器可以将携带网址A的IP地址的回应报文返回给终端,然后终端便可以直接向网址A的IP地址,即网址A的服务器发送访问请求,以获取网址A的网络资源。这个过程中,DNS请求和回应报文均是通过网关设备转发的,所以网关设备可以基于自身的安全机制,如黑白名单对终端发送的访问请求进行安全校验。

[0039] 但是,在一些情况下,企业内部使用的内部网站不需要企业外的人访问,所以一些企业会在企业内部配置专用的DNS服务器,这样终端的DNS请求和DNS服务器的回应报文均不会经过网关设备,所以网关设备配置的黑白名单便无法生效,也无法对终端的DNS请求和DNS服务器的回应报文进行安全校验,因此,会导致网络系统存在安全风险。

[0040] 鉴于前述的一个或多个问题,图2示出了本发明实施例提供的一种访问控制方法的流程图,该方法可以由网关设备执行。其中,网关设备是连接不同网络的关键组件,它可以实现网络间的数据转发和协议转换。如图2所示,该方法包括以下步骤:

[0041] 步骤210:接收用户输入的域名白名单信息。

[0042] 其中,域名白名单信息是用于控制访问权限的工具,可以包括一个或多个域名的域名地址。域名是用于在互联网上标识和定位特定网站或网络资源的字符串,如可以是网站的网址,如www.123456.com就是一个网址,当用户想要访问该网址时,可以在浏览器中输入www.123456.com这个域名,便可以访问这个网址。

[0043] 域名白名单信息是指一份允许访问的域名列表,当使用域名白名单信息时,只有列表中列出的域名才能被访问或允许进行某种操作,其他域名将被阻止或限制访问。

[0044] 示例性的,用户可以通过如图3所示的配置界面在网关设备上配置域名白名单信息,如设置一个或多个域名的域名地址。

[0045] 步骤220:向DNS服务器发送DNS请求,以获取DNS服务器发送的IP地址数据。

[0046] 其中,IP地址数据包括域名白名单信息中各域名对应的IP地址。例如,假设域名白名单信息中配置了m个域名,则这m个域名对应的IP地址即构成IP地址数据,m为正整数。本实施例中,一个域名可以对应一个IP地址,也可以对应多个IP地址。

[0047] DNS服务器是提供域名服务的服务器,可以是企业内部配置的专门用于处理内部访问请求的DNS服务器。域名服务是运行域名系统的互联网工具,为互联网上的主机分配域名地址和IP地址,在使用域名地址时,域名系统会将域名地址转换为IP地址。DNS请求是指在计算机网络中向DNS服务器发送查询信息以获取域名对应的IP地址的请求。DNS请求包含要查询的域名信息,通常是一个域名解析的请求类型。

[0048] 在网关设备接收到用户输入的域名白名单信息时,会向DNS服务器发送DNS请求,使得DNS服务器根据DNS请求所请求查询的域名进行查找,并返回相应的IP地址数据。通过这种方式,网关设备可以在接收到用户输入的域名白名单信息时,主动获取域名白名单信息对应的IP地址数据,不会产生因DNS服务器部署在内部网络,DNS请求和回应报文不经过网关设备,而导致网关设备无法获取IP地址数据的问题。

[0049] 图4示出了本发明实施例提供的一种访问控制的系统架构示意图,如图4所示,当用户在网关设备上配置域名白名单信息时,假设该域名白名单信息中添加了“www.123456.com”这个域名,并且网关设备中配置有DNS服务器的IP地址,为10.1.0.3,网关设备可以开启DNS学习状态,如由用户或自动运行指令“private-dns-request enable”,向10.1.0.3这一IP地址发送DNS请求,该DNS请求经过内网交换机被转发至DNS服务器,DNS

服务器在接收到DNS请求时,会根据DNS请求查找“www.123456.com”这一域名对应的IP地址,然后将“www.123456.com”的IP地址封装在回应报文中,通过内网交换机返回给网关设备。

[0050] 与此同时,如图4所示,终端设备为了访问“www.123456.com”这一域名对应的网址,也会通过内网交换机向DNS服务器发送终端DNS请求,来获取“www.123456.com”这一域名对应的IP地址。可以看出,终端设备向DNS服务器发送终端DNS请求的流量不经过网关设备。

[0051] 在一些实施例中,为了确保网关设备能够获取到域名白名单信息对应的IP地址数据,网关设备可以按照预设时间间隔向DNS服务器发送DNS请求,直至获取到DNS服务器发送的IP地址数据。其中,预设时间间隔可以由操作人员自行定义,或者也可以设置为默认值,如可以设置为3秒、5秒等。

[0052] 例如,在用户在网关设备上将“www.123456.com”这一域名配置为域名白名单信息中的一个域名时,网关设备可以立即开始向DNS服务器发送DNS请求,之后每间隔5秒主动向DNS服务器发送一次DNS请求,使得DNS服务器可以响应于接收到的DNS请求,返回域名白名单信息对应的IP地址数据。在接收到DNS服务器返回的IP地址数据时,停止向DNS服务器发送DNS请求。

[0053] 由于DNS服务器获取到的域名与IP地址的数据可能随时会被更新,所以通过上述方法,网关设备可以在未获取到域名白名单信息对应的IP地址数据时,持续请求DNS服务器返回IP地址数据,这样当DNS服务器获取到域名白名单信息对应的IP地址数据,便可以返回给网关设备,故能够提高IP地址数据的获取成功率。

[0054] 在一些实施例中,为了减少网关设备持续向DNS服务器发送DNS请求所造成的流量消耗,避免网关设备发生故障,在网关设备按照预设时间间隔向DNS服务器发送DNS请求时,网关设备连续发送DNS请求的次数可以小于预设次数,即网关设备可以按照预设时间间隔向DNS服务器连续发送预设次数次DNS请求,如果在连续发送预设次数DNS请求仍未接收到DNS服务器返回的IP地址数据,则停止此次发送。其中,预设次数可以由操作人员自定义,如可以设置为10次、15次等。

[0055] 在某一次发送DNS请求后,如果网关设备接收到DNS服务器返回的IP地址数据,则停止向DNS服务器发送DNS请求。

[0056] 步骤230:根据IP地址数据,生成IP地址白名单。

[0057] IP地址白名单是用于进行访问控制的IP地址工具。

[0058] 在得到IP地址数据后,网关设备可以基于IP地址数据,生成用于进行访问控制的IP地址白名单。例如,可以将IP地址数据中的IP地址确定为IP地址白名单中的IP地址。

[0059] 在一些实施例中,IP地址数据中还可以包括域名白名单信息中各域名对应的IP地址的有效期,该有效期可以表示IP地址的最大可用时间。同时,在获取到IP地址数据后,由于IP地址白名单可以在之前的配置中已经生成,针对这种情况,为了生成IP地址白名单,如图5所示,网关设备可以执行以下步骤:

[0060] 步骤510:基于IP地址数据,确定IP地址数据中各个IP地址的有效期。

[0061] 例如,网关设备可以根据IP地址数据,在其中查找每个IP地址和每个IP地址对应的有效期。

[0062] 步骤520:将IP地址数据中的各个IP地址和各IP地址的有效期添加至IP地址白名单。

[0063] 由于IP地址数据是域名白名单信息对应的各个域名的IP地址,所以为了使用户能够正常访问域名白名单信息中的各个域名,在得到IP地址数据后,可以将IP地址数据中的各个IP地址和各IP地址的有效期添加至IP地址白名单。

[0064] 通过记录各IP地址和各IP地址的有效期,网关设备可以获取DNS服务器返回的域名与IP地址的映射关系,在记录各IP地址的有效期后,可以根据该有效期确定IP地址的可用时间,一旦确定某个IP地址到期,便可以重新向DNS服务器发送DNS请求,来更新这一IP地址。

[0065] 在一些实施例中,如果IP地址白名单中已经存在IP地址数据中的某个IP地址,则可以取消将该IP地址添加至IP地址白名单。也就是说,可以执行以下方法:

[0066] 在IP地址白名单中查找IP地址数据中的各个IP地址。

[0067] 若IP地址白名单中存在IP地址数据中的任一IP地址,则停止将上述任一IP地址添加至IP地址白名单。

[0068] 若IP地址白名单中不存在IP地址数据中的任一IP地址,则将上述任一IP地址添加至IP地址白名单。

[0069] 例如,可以将IP地址数据中的每个IP地址与IP地址白名单中的每个IP地址进行比较,确定IP地址白名单中是否存在与IP地址数据中任一IP地址相同的IP地址,如果存在,则为了避免重复,可以停止将IP地址数据中上述任一IP地址添加至IP地址白名单。如果IP地址白名单中不存在与IP地址数据中的任一IP地址相同的IP地址,则说明该任一IP地址未添加至IP地址白名单,所以可以将该任一IP地址添加至IP地址白名单。

[0070] 通过这种方式,可以将IP地址数据中的IP地址添加至IP地址白名单,并且确保IP地址白名单中不存在重复的IP地址。

[0071] 实际上,通过上述步骤510～520,可以根据获取得到的IP地址数据,生成IP地址白名单,这样在后续用户通过终端设备访问网站时,网关设备便可以根据IP地址白名单进行访问控制,确保终端设备的安全性。

[0072] 为了说明网关设备对IP地址数据的处理方法,图6示出了本发明实施例提供的一种IP地址数据的处理方法的流程图,如图6所示,网关设备可以执行以下方法:

[0073] 步骤610:开启DNS主动探测模式。

[0074] 例如,用户可以通过如图7所示的指令界面输入“private-dns-request enable”,以开启网关设备的DNS主动探测模式。

[0075] 步骤620:用户输入域名白名单信息。

[0076] 步骤630:在接收到用户输入的域名白名单信息时,创建定时器。

[0077] 步骤640:按照预设时间间隔向DNS服务器发送DNS请求,以获取DNS服务器返回的IP地址数据。

[0078] 例如,用户可以预先通过如图8所示的配置界面在网关设备上配置DNS服务器的IP地址,这样,在接收到用户输入的域名白名单信息时,网关设备可以每间隔5秒主动向DNS服务器的IP地址发送一次DNS请求,使DNS服务器向自己返回域名白名单信息对应的IP地址数据。

[0079] 步骤650:确定是否获取到域名白名单信息对应的IP地址数据。如果是,则执行步骤660,如果否,则继续执行步骤640,以继续按照预设时间间隔向DNS服务器发送DNS请求,获取DNS服务器返回的IP地址数据。

[0080] 步骤660:确定IP地址白名单中是否存在IP地址数据中的IP地址。如果不存在,则执行步骤670,将IP地址数据中的IP地址存储在IP地址白名单中,如果存在,则执行步骤680,删除定时器,并丢弃域名白名单信息对应的IP地址数据。

[0081] 步骤670,将IP地址数据中的IP地址存储在IP地址白名单中。

[0082] 步骤680,删除定时器,并丢弃域名白名单信息对应的IP地址数据。

[0083] 通过这种方法,网关设备可以获取域名白名单信息对应的IP地址数据,并基于IP地址数据中的IP地址是否已存储在IP地址白名单中,对IP地址白名单进行更新,确保IP地址白名单中存储IP地址数据中的IP地址,且无重复的IP地址。

[0084] 进一步的,为了使IP地址白名单中的IP地址持续保持最新状态,在一些实施例中,网关设备还可以执行以下方法:

[0085] 记录IP地址数据中各IP地址在IP地址白名单中的存活时间,以在IP地址数据中任一IP地址的存活时间大于存活时间阈值时,向DNS服务器发送地址更新请求,以获取DNS服务器发送的更新后的IP地址数据。

[0086] 其中,IP地址数据中各IP地址在IP地址白名单中的存活时间可以从IP地址被添加至IP地址白名单的时刻开始记起。存活时间阈值是指IP地址在IP地址白名单中的最大存活时间,可以由操作人员根据IP地址的有效期等进行设置,或者也可以设置为默认值,如3天、7天等。地址更新请求是指网关设备发送的获取IP地址数据中一个或多个IP地址的更新后的地址数据的请求。

[0087] 示例性的,在将IP地址数据中的某个IP地址添加到IP地址白名单中时,可以开始计时,确定该IP地址的存活时间,然后,在该存活时间大于存活时间阈值时,可以向DNS服务器发送地址更新请求,以获取DNS服务器发送的更新后的IP地址数据。更新后的IP地址数据可以包括存活时间大于存活时间阈值的所有IP地址的更新后的IP地址。

[0088] 通过上述方法,可以保持IP地址白名单的IP地址处于最新状态,而不会产生因IP地址未更新而导致无法进行安全控制的问题。

[0089] 步骤240:在接收到终端设备发送的访问请求时,基于IP地址白名单,控制终端设备访问该访问请求对应的目标网址。

[0090] 访问请求是指终端设备发送的访问目标网址的请求。

[0091] 当用户在终端设备的浏览器应用程序中输入目标网址时,终端设备触发对目标网址的访问请求,网关设备可以接收该访问请求,并利用IP地址白名单,对访问请求进行安全校验,以实现对终端设备访问目标网址的访问请求进行安全控制。

[0092] 具体的,在一些实施例中,如图9所示,步骤240可以通过以下方法实现:

[0093] 步骤910:根据访问请求,确定目标网址和目标网址的目标IP地址。

[0094] 其中,目标IP地址是由DNS服务器响应于终端设备发送的IP地址获取请求,发送给终端设备的。示例性的,在用户通过终端设备触发对目标网址的访问请求时,终端设备可以首先向DNS服务器发送IP地址获取请求,来获取DNS服务器返回的目标网址的目标IP地址。

[0095] 在网关设备接收到终端设备的访问请求时,可以对访问请求进行解析,确定终端

设备所请求访问的目标网址,并在自己存储的域名与IP地址的映射表中查找目标网址的目标IP地址。

[0096] 步骤920:将目标IP地址与IP地址白名单中的IP地址进行匹配。

[0097] 例如,可以将目标IP地址与IP地址白名单中的每个IP地址进行比较,确定IP地址白名单中是否存在与目标IP地址匹配的IP地址。

[0098] 步骤930:在确定目标IP地址与IP地址白名单中的任一IP地址匹配的情况下,允许终端设备访问目标网址。

[0099] 在确定目标IP地址与IP地址白名单中的任一IP地址匹配时,说明目标IP地址为IP地址白名单中的IP地址,则确定允许终端设备访问目标网址,网关设备放通终端设备访问目标网址的流量。

[0100] 与此同时,在网关设备将目标IP地址与IP地址白名单中的IP地址进行匹配时,为了确定目标IP地址是否为非法地址,网关设备还可以将目标IP地址与预先配置的黑名单中的IP地址进行匹配,如果确定目标IP地址为预先配置的黑名单中的任一IP地址时,说明目标IP地址为非法地址,可直接终止访问。

[0101] 步骤940:在确定目标IP地址与IP地址白名单中的各个IP地址不匹配的情况下,禁止终端设备访问目标网址。

[0102] 在确定目标IP地址与IP地址白名单中的各个IP地址均不匹配时,说明目标IP地址为非法IP地址,则确定禁止终端设备访问目标网址,网关设备拒绝终端设备访问目标网址的流量。

[0103] 通过上述方法,可以实现基于IP地址白名单的访问控制,使得终端设备访问目标网址的流量被网关设备进行全放通,而不需要经过认证策略、安全策略等。

[0104] 综上,根据本实施例中的访问控制方法,可以接收用户输入的域名白名单信息,向DNS服务器发送DNS请求,以获取DNS服务器发送的IP地址数据,根据IP地址数据,生成IP地址白名单,在接收到终端设备发送的访问请求时,基于IP地址白名单,控制终端设备访问访问请求对应的目标网址。

[0105] 通过该方法,网关设备可以主动获取域名白名单信息对应的IP地址数据,并根据IP地址数据实现对终端设备的访问请求的安全控制,能够提高网络系统的安全性。

[0106] 此外,由于本实施例中,DNS服务器被配置为内网专用的DNS服务器,所以用户通过内部网络中的终端设备访问网站时,均可以通过内网专用的DNS服务器获取IP地址数据,这样,内网DNS服务器获取的IP地址数据只需要从公共DNS服务器获取一次,一部分网络流量就可以被拦截在内网,故也可以节省网络资源。

[0107] 图10示出了本发明实施例提供的一种访问控制装置的结构示意图,该访问控制装置可以应用于网关设备。如图10所示,该访问控制装置1000包括:接收模块1010,用于接收用户输入的域名白名单信息;获取模块1020,用于向DNS服务器发送DNS请求,以获取DNS服务器发送的IP地址数据,IP地址数据包括域名白名单信息中各域名对应的IP地址;生成模块1030,用于根据IP地址数据,生成IP地址白名单;控制模块1040,用于在接收到终端设备发送的访问请求时,基于IP地址白名单,控制终端设备访问访问请求对应的目标网址。

[0108] 在一些实施例中,获取模块1020用于按照预设时间间隔向DNS服务器发送DNS请求,直至获取到DNS服务器发送的IP地址数据。

[0109] 在一些实施例中,IP地址数据还包括域名白名单信息中各域名对应的IP地址的有效期,生成模块1030用于基于IP地址数据,确定IP地址数据中各个IP地址的有效期;将IP地址数据中的各个IP地址和各IP地址的有效期添加至IP地址白名单。

[0110] 在一些实施例中,控制模块1040用于根据访问请求,确定目标网址和目标网址的目标IP地址;将目标IP地址与IP地址白名单中的IP地址进行匹配;在确定目标IP地址与IP地址白名单中的任一IP地址匹配的情况下,允许终端设备访问目标网址;在确定目标IP地址与IP地址白名单中的各个IP地址不匹配的情况下,禁止终端设备访问目标网址。

[0111] 在一些实施例中,生成模块1030用于在IP地址白名单中查找IP地址数据中的各个IP地址;若IP地址白名单中存在IP地址数据中的任一IP地址,则停止将任一IP地址添加至IP地址白名单;若IP地址白名单中不存在IP地址数据中的任一IP地址,则将任一IP地址添加至IP地址白名单。

[0112] 在一些实施例中,获取模块1020还用于记录IP地址数据中各IP地址在IP地址白名单中的存活时间,以在IP地址数据中任一IP地址的存活时间大于存活时间阈值时,向DNS服务器发送地址更新请求,以获取DNS服务器发送的更新后的IP地址数据。

[0113] 在一些实施例中,目标IP地址是由DNS服务器响应于终端设备发送的IP地址获取请求,发送给终端设备的。

[0114] 上述装置中各模块的具体细节在方法部分实施方式中已经详细说明,未披露的方案细节内容可以参见方法部分的实施方式内容,因而不再赘述。

[0115] 图11示出了本发明实施例提供的一种网关设备的结构示意图,本发明具体实施例并不对网关设备的具体实现做限定。

[0116] 如图11所示,该网关设备可以包括:处理器(processor)1102、通信接口(Communications Interface)1104、存储器(memory)1106、以及通信总线1108。

[0117] 其中:处理器1102、通信接口1104、以及存储器1106通过通信总线1108完成相互间的通信。通信接口1104,用于与其它设备比如客户端或其它服务器等的网元通信。处理器1102,用于执行程序1110,具体可以执行上述用于访问控制方法实施例中的相关步骤。

[0118] 具体地,程序1110可以包括程序代码,该程序代码包括计算机可执行指令。

[0119] 处理器1102可能是中央处理器CPU,或者是特定集成电路ASIC(Application Specific Integrated Circuit),或者是被配置成实施本发明实施例的一个或多个集成电路。网关设备包括的一个或多个处理器,可以是同一类型的处理器,如一个或多个CPU;也可以是不同类型的处理器,如一个或多个CPU以及一个或多个ASIC。

[0120] 存储器1106,用于存放程序1110。存储器1106可能包含高速RAM存储器,也可能还包括非易失性存储器(non-volatile memory),例如至少一个磁盘存储器。

[0121] 程序1110具体可以被处理器1102调用使网关设备执行上述访问控制方法。

[0122] 本发明实施例提供了一种计算机可读存储介质,所述存储介质存储有至少一可执行指令,该可执行指令在网关设备/访问控制装置上运行时,使得所述网关设备/访问控制装置执行上述任意方法实施例中的访问控制方法。

[0123] 可执行指令具体可以用于使得网关设备/访问控制装置执行以下操作:接收用户输入的域名白名单信息;向DNS服务器发送DNS请求,以获取DNS服务器发送的IP地址数据,IP地址数据包括域名白名单信息中各域名对应的IP地址;根据IP地址数据,生成IP地址白

名单;在接收到终端设备发送的访问请求时,基于IP地址白名单,控制终端设备访问访问请求对应的目标网址。

[0124] 在此提供的算法或显示不与任何特定计算机、虚拟系统或者其它设备固有相关。此外,本发明实施例也不针对任何特定编程语言。

[0125] 在此处所提供的说明书中,说明了大量具体细节。然而能够理解,本发明的实施例可以在没有这些具体细节的情况下实践。类似地,为了精简本发明并帮助理解各个发明方面中的一个或多个,在上面对本发明的示例性实施例的描述中,本发明实施例的各个特征有时被一起分组到单个实施例、图、或者对其的描述中。其中,遵循具体实施方式的权利要求书由此明确地并入该具体实施方式,其中每个权利要求本身都作为本发明的单独实施例。

[0126] 本领域技术人员可以理解,可以对实施例中的设备中的模块进行自适应性地改变并且把它们设置在与该实施例不同的一个或多个设备中。可以把实施例中的模块或单元或组件组合成一个模块或单元或组件,以及此外可以把它们分成多个子模块或子单元或子组件。除了这样的特征和/或过程或者单元中的至少一些是相互排斥之外。

[0127] 应该注意的是上述实施例对本发明进行说明而不是对本发明进行限制,并且本领域技术人员在不脱离所附权利要求的范围的情况下可设计出替换实施例。在权利要求中,不应将位于括号之间的任何参考符号构造成对权利要求的限制。单词“包含”不排除存在未列在权利要求中的元件或步骤。位于元件之前的单词“一”或“一个”不排除存在多个这样的元件。本发明可以借助于包括有若干不同元件的硬件以及借助于适当编程的计算机来实现。在列举了若干装置的单元权利要求中,这些装置中的若干个可以是通过同一个硬件项来具体体现。单词第一、第二、以及第三等的使用不表示任何顺序。可将这些单词解释为名称。上述实施例中的步骤,除有特殊说明外,不应理解为对执行顺序的限定。

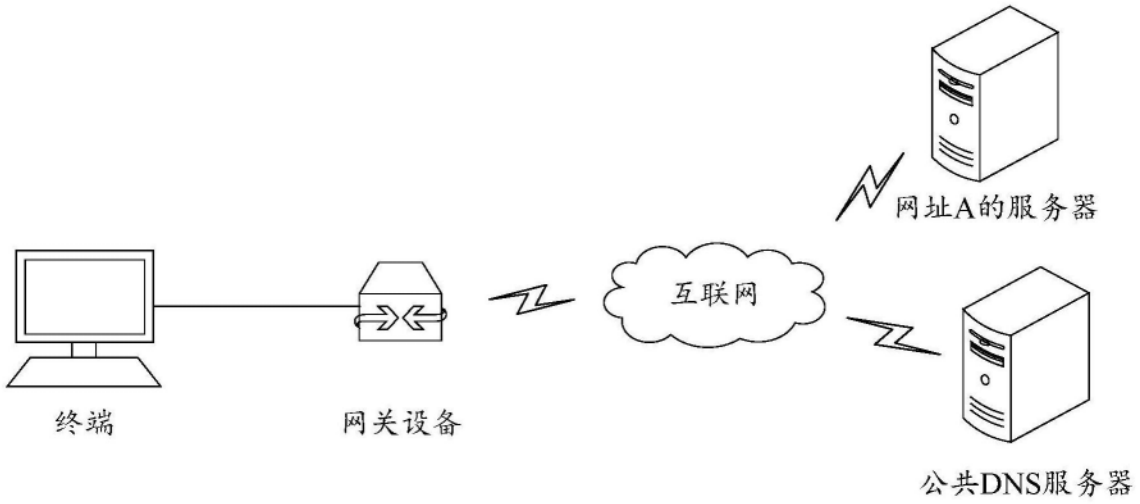

网址A的服务器
互联网
终端
网关设备
公共DNS服务器

图1

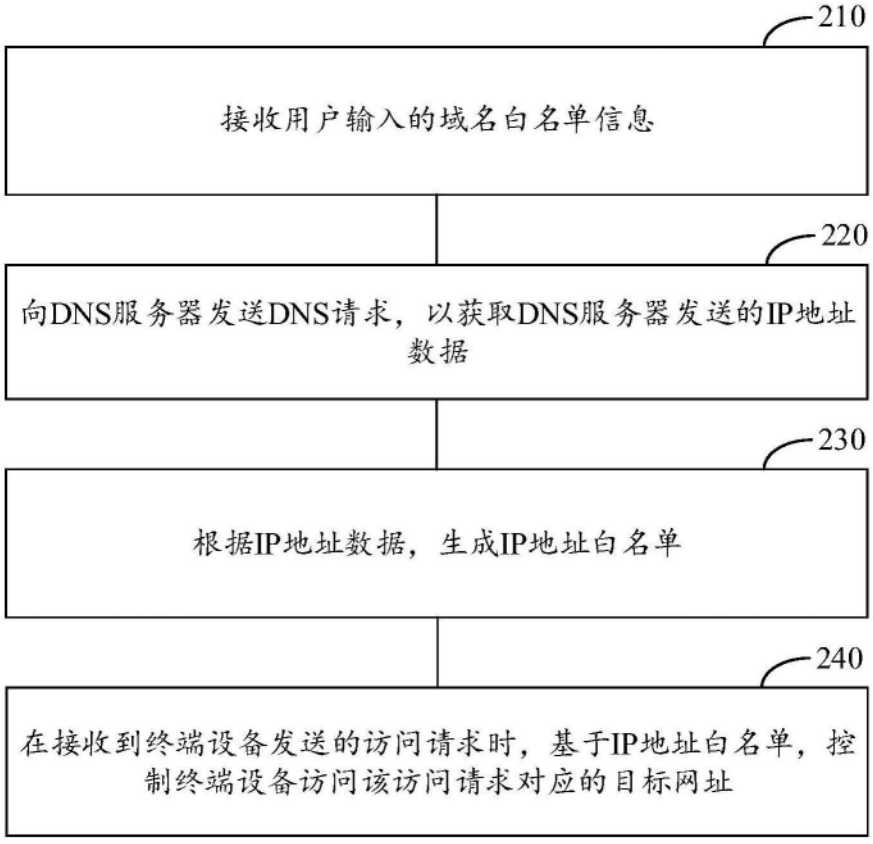

210
接收用户输入的域名白名单信息
220
向DNS服务器发送DNS请求，以获取DNS服务器发送的IP地址数据
230
根据IP地址数据，生成IP地址白名单
240
在接收到终端设备发送的访问请求时，基于IP地址白名单，控制终端设备访问该访问请求对应的目标网址

图2

策略配置 / 全局白名单
全局白名单
新建
删除
启用
禁用
名称
地址
描述
状态
1
域名白名单
www.people.com.cn

图3

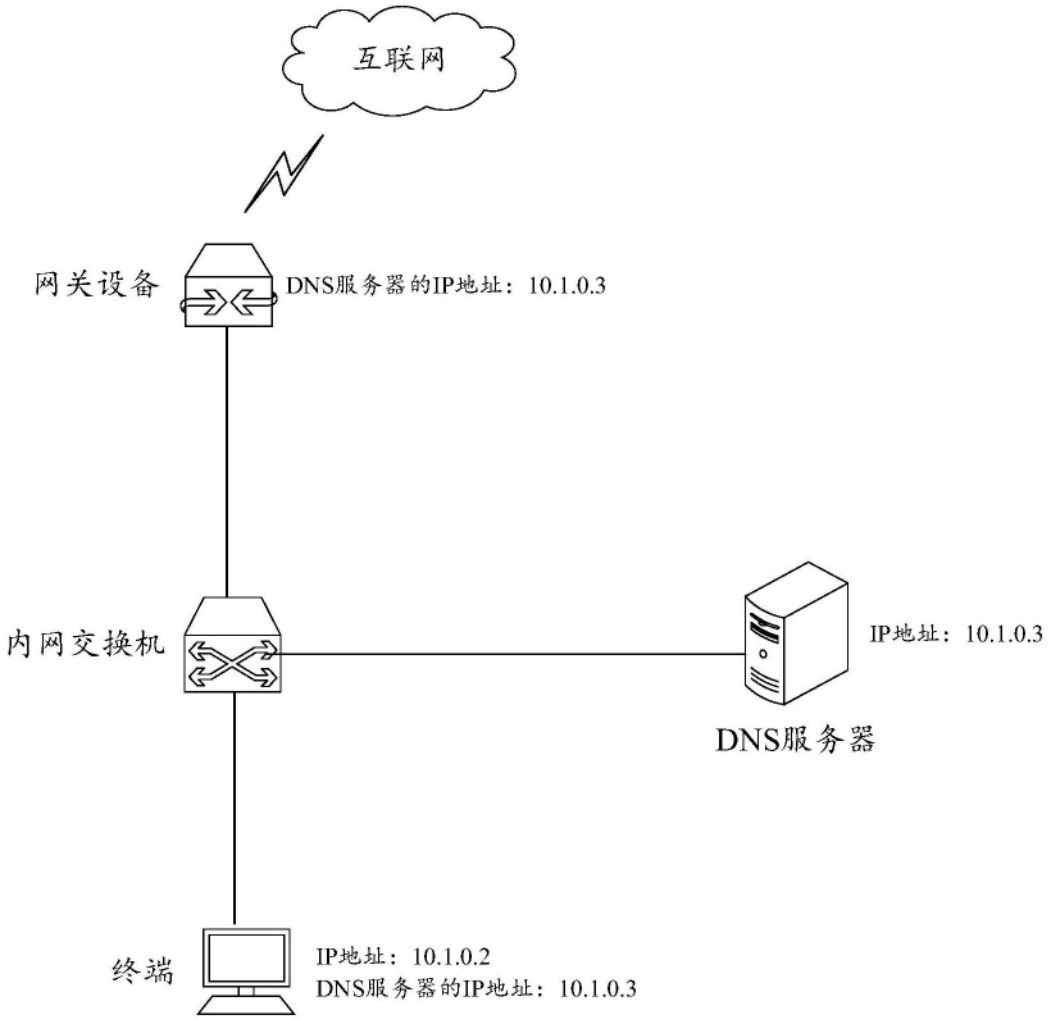

互联网
网关设备
DNS服务器的IP地址：10.1.0.3
内网交换机
IP地址：10.1.0.3
DNS服务器
终端
IP地址：10.1.0.2
DNS服务器的IP地址：10.1.0.3

图4

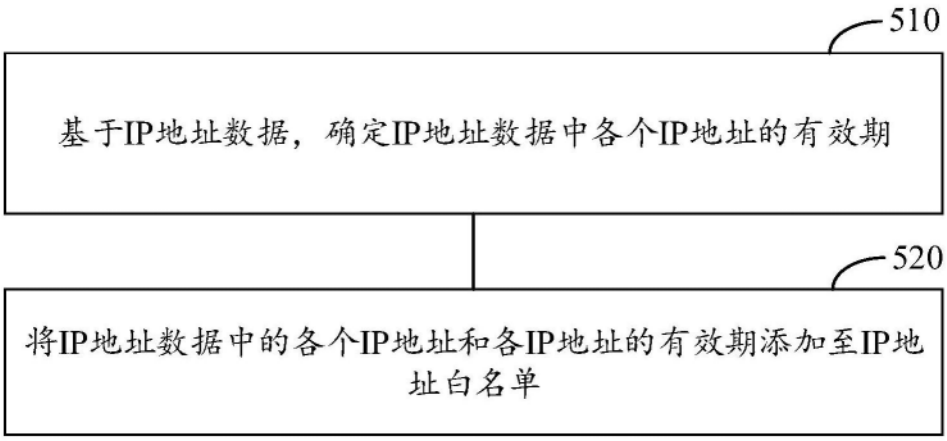

510
基于IP地址数据，确定IP地址数据中各个IP地址的有效期
520
将IP地址数据中的各个IP地址和各IP地址的有效期添加至IP地址白名单

图5

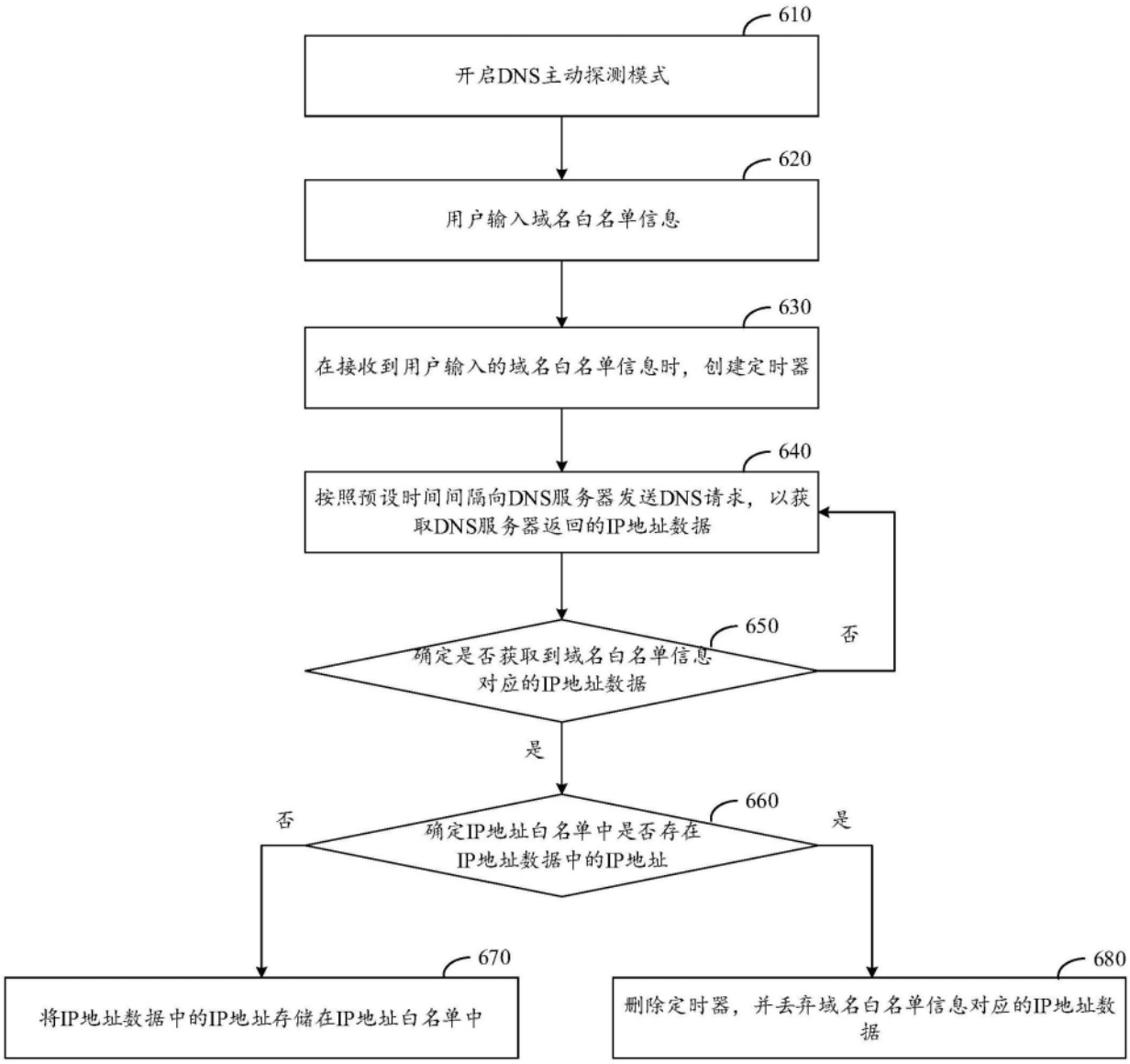


图6

```
AAA:WD-D#
AAA:WD-D# configure terminal
AAA:WD-D(config)# private-dns-request enable
AAA:WD-D(config)#
```

图7

基础网络 / DNS服务
域名管理
动态缓存
特定域名解析
DNS透明代理
DNS 服务器
启用DNS全局代理
DNS 服务器1
10.1.0.3
DNS 服务器2
例如：192.168.1.1或2000::1
DNS 服务器3
例如：192.168.1.1或2000::1
DNS 服务器4
例如：192.168.1.1或2000::1
提交
取消

图8

910
根据访问请求，确定目标网址和目标网址的目标IP地址
920
将目标IP地址与IP地址白名单中的IP地址进行匹配
930
在确定目标IP地址与IP地址白名单中的任一IP地址匹配的情况下，允许终端设备访问目标网址
940
在确定目标IP地址与IP地址白名单中的各个IP地址不匹配的情况下，禁止终端设备访问目标网址

图9

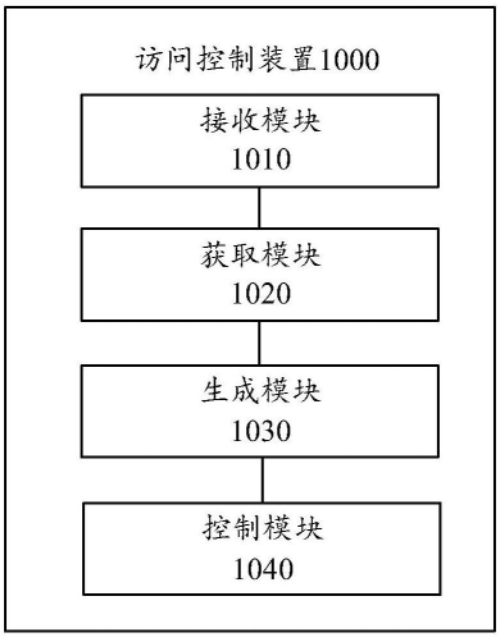

访问控制装置1000
接收模块
1010
获取模块
1020
生成模块
1030
控制模块
1040

图10

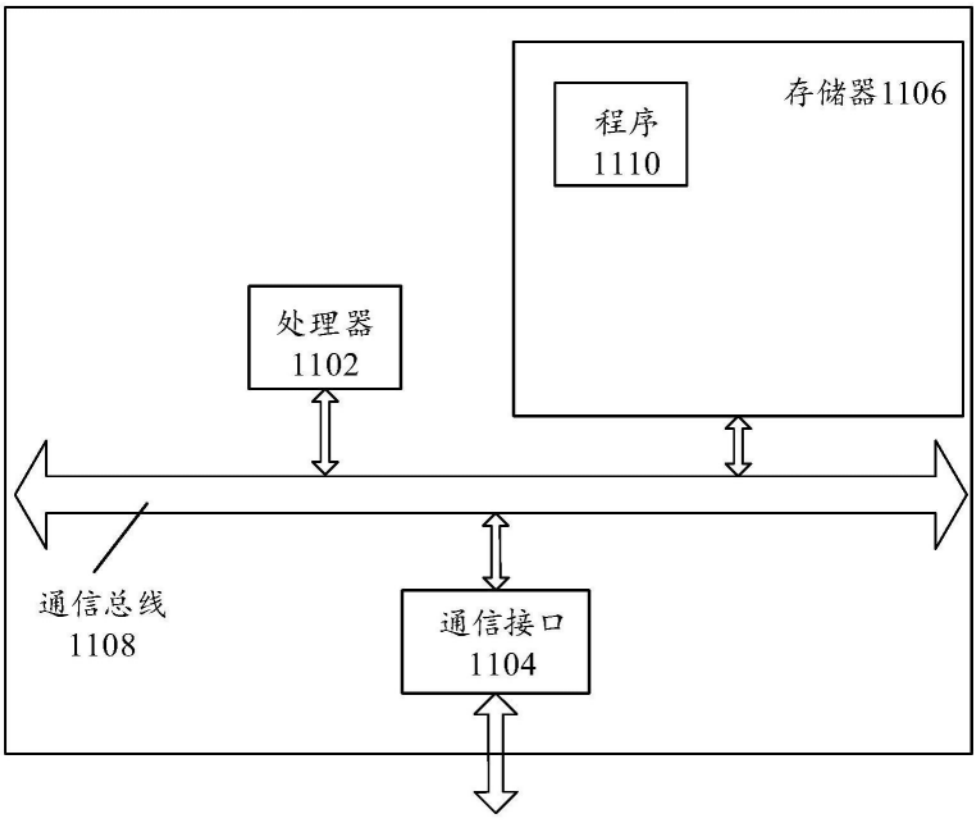

存储器1106
程序
1110
处理器
1102
通信总线
1108
通信接口
1104

图11