(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 114448734 A
(43)申请公布日 2022.05.06

(21)申请号 202210371211.0

(22)申请日 2022.04.11

(71)申请人 北京指掌易科技有限公司
地址 100085 北京市海淀区创业路8号3号楼-1层3-10A42号

(72)发明人 王家荣 王伟

(74)专利代理机构 北京品源专利代理有限公司 11332
专利代理师 倪焱

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

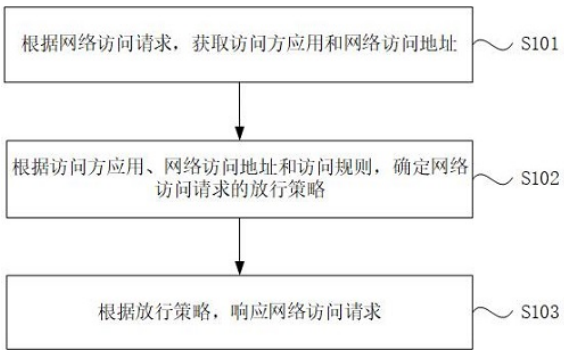
权利要求书2页 说明书11页 附图4页

(54)发明名称

一种网络访问方法、装置、设备以及存储介质

(57)摘要

本发明公开了一种网络访问方法、装置、设备以及存储介质。该方法包括:根据网络访问请求,获取访问方应用和网络访问地址;根据所述访问方应用、网络访问地址和访问规则,确定所述网络访问请求的放行策略;其中,所述访问规则包括应用访问规则和网络访问规则;根据所述放行策略,响应所述网络访问请求。本发明提供的方案,通过根据应用访问规则和网络访问规则来确定网络访问请求的放行策略,进而对网络访问请求做出响应,能够实现在不同应用访问不同网络时,基于应用访问规则和网络访问规则,给出针对性的响应,有效地对网络访问请求进行局部拦截或放行。



CN 114448734 A

1.一种网络访问方法,其特征在于,所述方法包括:

根据网络访问请求,获取访问方应用和网络访问地址;

根据所述访问方应用、网络访问地址和访问规则,确定所述网络访问请求的放行策略;其中,所述访问规则包括应用访问规则和网络访问规则;

根据所述放行策略,响应所述网络访问请求。

2.根据权利要求1所述的方法,其特征在于,所述根据网络访问请求,获取访问方应用和网络访问地址,包括:

调用微软网络过滤平台WFP驱动,基于域名系统DNS协议,解析网络访问请求对应的网络访问地址;

在访问方应用基于所述网络访问地址建立网络访问连接的过程中,调用WFP驱动,获取访问方应用。

3.根据权利要求2所述的方法,其特征在于,在访问方应用基于所述网络访问地址建立网络访问连接的过程中,调用WFP驱动,获取访问方应用,包括:

在访问方应用基于所述网络访问地址建立网络访问连接的过程中,根据网络访问地址的类型,调用WFP驱动,获取访问方应用。

4.根据权利要求1所述的方法,其特征在于,所述根据所述访问方应用、网络访问地址和访问规则,确定所述网络访问请求的放行策略,包括:

调用WFP驱动,基于DNS协议,解析所述网络访问请求对应的目标域名地址关系;

根据所述目标域名地址关系和访问规则中的网络访问规则,更新本地域名地址关系集;

判断所述网络访问地址是否记录在所述本地域名地址关系集中,且所述访问方应用是否满足所述访问规则中的应用访问规则;

根据判断结果,确定网络访问请求的放行策略。

5.根据权利要求4所述的方法,其特征在于,所述根据所述目标域名地址关系和访问规则中的网络访问规则,更新本地域名地址关系集,包括:

若所述目标域名地址关系中的域名满足所述访问规则中的网络访问规则,则将所述目标域名地址关系,添加到本地域名地址关系集中。

6.根据权利要求1所述的方法,其特征在于,根据所述访问方应用、网络访问地址和访问规则,确定所述网络访问请求的放行策略,包括:

对访问规则中的应用访问规则进行合法性验证;

若验证通过,则根据所述访问方应用、网络访问地址和访问规则,确定所述网络访问请求的放行策略。

7.根据权利要求6所述的方法,其特征在于,对访问规则中的应用访问规则进行合法性验证,包括:

获取访问规则中的应用访问规则关联的应用程序数据;

确定所述应用程序数据的校验值;

根据所述校验值,对所述应用访问规则进行合法性验证。

8.一种网络访问装置,其特征在于,包括:

获取模块,用于根据网络访问请求,获取访问方应用和网络访问地址;

确定模块，用于根据所述访问方应用、网络访问地址和访问规则，确定所述网络访问请求的放行策略；其中，所述访问规则包括应用访问规则和网络访问规则；

响应模块，用于根据所述放行策略，响应所述网络访问请求。

9.一种电子设备，其特征在于，包括：

一个或多个处理器；

存储器，用于存储一个或多个程序；

当所述一个或多个程序被所述一个或多个处理器执行，使得所述一个或多个处理器实现如权利要求1-7中任一项所述的网络访问方法。

10.一种计算机可读存储介质，其上存储有计算机程序，其特征在于，该程序被处理器执行时实现如权利要求1-7中任一项所述的网络访问方法。

一种网络访问方法、装置、设备以及存储介质

技术领域

[0001] 本发明实施例涉及计算机技术，尤其涉及一种网络访问方法、装置、设备以及存储介质。

背景技术

[0002] 目前很多企业拥有自己内部的软件，出于安全的考虑，企业希望自己某些特定的网络资源只能被特定的应用访问，但现有的网络拦截方式往往都是全局拦截或放行。

[0003] 因此，如何在用户从不同的应用端访问不同的网络地址时，给出针对性的响应，实现网络访问请求的局部拦截，是目前亟待解决的问题。

发明内容

[0004] 本发明提供一种网络访问方法、装置、设备以及存储介质，能够实现在不同应用访问不同网络时，基于应用访问规则和网络访问规则，给出针对性的响应，有效地对网络访问请求进行局部拦截或放行。

[0005] 第一方面，本发明实施例提供了一种网络访问方法，该方法包括：

根据网络访问请求，获取访问方应用和网络访问地址；

根据所述访问方应用、网络访问地址和访问规则，确定所述网络访问请求的放行策略；其中，所述访问规则包括应用访问规则和网络访问规则；

根据所述放行策略，响应所述网络访问请求。

[0006] 第二方面，本发明实施例还提供了一种网络访问装置，包括：

获取模块，用于根据网络访问请求，获取访问方应用和网络访问地址；

确定模块，用于根据所述访问方应用、网络访问地址和访问规则，确定所述网络访问请求的放行策略；其中，所述访问规则包括应用访问规则和网络访问规则；

响应模块，用于根据所述放行策略，响应所述网络访问请求。

[0007] 第三方面，本发明实施例还提供了一种电子设备，该电子设备包括：

一个或多个处理器；

存储器，用于存储一个或多个程序；

当所述一个或多个程序被所述一个或多个处理器执行，使得所述一个或多个处理器实现如本发明任意实施例所提供的网络访问方法。

[0008] 第六方面，本发明实施例还提供了一种计算机可读存储介质，其上存储有计算机程序。其中，该程序被处理器执行时实现如本发明任意实施例所提供的网络访问方法。

[0009] 本发明实施例根据网络访问请求，获取访问方应用和网络访问地址之后，根据访问方应用、网络访问地址、应用访问规则和网络访问规则，确定网络访问请求的放行策略，最后根据放行策略，响应网络访问请求。通过基于应用访问规则和网络访问规则来确定网络访问请求的放行策略，进而对网络访问请求做出响应，能够实现在不同应用访问不同网络时，基于应用访问规则和网络访问规则，给出针对性的响应，有效地对网络访问请求进行

局部拦截或放行。

附图说明

[0010] 图1为本发明实施例一提供的一种网络访问方法的流程图；
图2为本发明实施例二提供的一种网络访问方法的流程图；
图3为本发明实施例三提供的一种网络访问方法的流程图；
图4为本发明实施例四提供的一种网络访问方法的流程图；
图5A为本发明实施例五提供的一种网络访问方法的流程图；
图5B为本发明实施例五提供的服务器的结构框图；
图6为本发明实施例六提供的一种网络访问装置的结构框图；
图7为本发明实施例七提供的一种电子设备的结构示意图。

具体实施方式

[0011] 下面结合附图和实施例对本发明作进一步的详细说明。可以理解的是，此处所描述的具体实施例仅仅用于解释本发明，而非对本发明的限定。另外还需要说明的是，为了便于描述，附图中仅示出了与本发明相关的部分而非全部结构。

[0012] 实施例一

图1为本发明实施例一提供的一种网络访问方法的流程图，本实施例可适用于服务器如何对网络请求进行响应的情况，具体的，可适用于服务器如何确定网络请求的放行策略并根据放行策略给出响应的情况，该方法可以由网络访问装置来执行，该装置可以采用软件和/或硬件的方式实现，并可集成于具有网络访问功能的电子设备中，由电子设备中对网络访问请求进行响应的服务器执行。如图1所示，本实施例提供的网络访问方法具体包括：

S101、根据网络访问请求，获取访问方应用和网络访问地址。

[0013] 其中，网络访问请求是指访问方应用向服务器发送的访问指定网络的请求。访问方应用是指发出网络访问请求的应用。网络访问地址是指访问方应用目标访问的网络地址。

[0014] 可选的，用户可以在访问方应用的客户端，如windows电脑上的软件客户端，主动通过点击等激活方式，向服务器发出网络访问请求，也可以是在访问方应用的客户端自动登录时，自动向服务器发出访问特定网址的网络访问请求。

[0015] 可选的，服务器检测到访问方应用发送的网络访问请求之后，可以根据网络访问请求，对请求的内容进行解析，直接获取网络访问请求中访问方应用的相关信息(如应用名称或代号等标识信息)以及访问方应用目标访问的域名地址，即获取访问方应用和网络访问地址；也可以先利用常用的网络过滤框架，对网络访问请求进行解析，确定网络访问地址，进一步基于网络访问地址，确定访问方应用的相关信息，即获取访问方应用和网络访问地址。

[0016] S102、根据访问方应用、网络访问地址和访问规则，确定网络访问请求的放行策略。

[0017] 其中，访问规则是指是否许可预设的应用访问预设网络的规则。访问规则包括应

用访问规则和网络访问规则。应用访问规则包含至少一个预设的网址以及对应的该网址限制或允许访问的应用的信息。网络访问规则包含至少一个预设的应用，以及限制或允许应用访问的网址的信息。例如，某网址只允许QQ应用访问为应用访问规则，某应用只允许访问百度网址为网络访问规则。放行策略是指决策是否放行网络访问请求访问对应网址的策略。放行策略可以包括允许放行策略和拒绝放行策略。

[0018] 可选的，获取访问方应用和网络访问地址之后，可以进一步基于应用访问规则，判断该网络访问地址对应的网络是否允许该访问方应用访问，同时，基于网络访问规则，判断该访问方应用是否被允许访问该网络访问地址对应的网络，若访问网络允许访问方应用访问，且访问方应用被允许访问对应网络，即同时满足应用访问规则和网络访问规则，则确定网络访问请求的放行策略为允许放行策略，否则，确定网络访问请求的放行策略为拒绝放行策略，即确定网络访问请求的放行策略；也可以在获取访问方应用和网络访问地址之后，将获取的访问方应用、网络访问地址以及预存的访问规则，输入预先训练好的策略确定模型，输出放行策略结果，即确定网络访问请求的放行策略。

[0019] S103、根据放行策略，响应网络访问请求。

[0020] 可选的，确定放行策略之后，可以根据放行策略的内容，生成对应的响应结果，根据响应结果，响应网络访问请求。具体的，若放行策略为拒绝放行策略，则可以生成相应的跳转网页或提示窗口，提醒用户访问失败以及提示用户可能的访问失败原因。若放行策略为允许放行策略，则不进行拦截，允许访问方应用与网络访问地址对应网络之间的通信连接。

[0021] 在本发明实施例中，服务器根据网络访问请求，获取访问方应用和网络访问地址之后，进一步根据访问方应用、网络访问地址、应用访问规则和网络访问规则，确定网络访问请求的放行策略，最后根据放行策略，响应网络访问请求。通过根据应用访问规则和网络访问规则来确定网络访问请求的放行策略，进而对网络访问请求做出响应，能够实现在不同应用访问不同网络时，基于应用访问规则和网络访问规则，给出针对性的响应，有效地对网络访问请求进行局部拦截或放行。

[0022] 实施例二

图2为本发明实施例二提供的一种网络访问方法的流程图，本实施例在上述实施例的基础上，进一步对“根据网络访问请求，获取访问方应用和网络访问地址”进行详细解释说明，如图2所示，本实施例提供的网络访问方法具体包括：

S201、调用微软网络过滤平台WFP驱动，基于域名系统DNS协议，解析网络访问请求对应的网络访问地址。

[0023] 其中，微软网络过滤平台(Windows Filtering Platform，WFP)是一种新的网络过滤框架，其主要工作在内核的TCP/IP(Transmission Control Protocol，传输控制协议)/(Internet Protocol，网际互连协议))协议栈的四层协议栈中，可以对TCP/IP协议栈进行拦截和过滤。域名系统(Domain Name System，DNS)是可以将域名和IP地址(Internet Protocol Address，互联网协议地址)相互映射的一个分布式数据库。

[0024] 可选的，服务器在检测到应用发出的网络访问请求之前，可以接收由相关人员如管理员下发的访问规则，此时操作系统处于用户态。

[0025] 可选的，服务器检测到访问方应用发出网络访问请求时，可以调用WFP的内核驱

动,此时操作系统的状态由原来的用户态转换为内核态,进一步利用WFP内核态下的域名解析模块,基于域名系统DNS协议,将网络访问请求中包含的访问网络的域名转换为IP地址,并将该IP地址作为网络访问请求对应的网络访问地址,即解析网络访问请求对应的网络访问地址。

[0026] S202、在访问方应用基于网络访问地址建立网络访问连接的过程中,调用WFP驱动,获取访问方应用。

[0027] 可选的,服务器解析网络访问请求对应的网络访问地址,获取到访问的IP地址,即网络访问地址之后,可以将解析的IP地址反馈至访问方应用,使得访问方应用基于解析的IP地址,与网络访问地址对应的网络建立socket(套接字)连接,同时,服务器在访问方应用基于网络访问地址建立网络访问连接的过程中,调用WFP驱动,获取访问方应用相关信息,如访问方应用的程序路径,即获取访问方应用。

[0028] 可选的,服务器调用WFP驱动之前,可以先判断网络访问地址的类型,进一步获取访问方应用,相应的,在基于网络访问地址,建立网络访问连接的过程中,调用WFP驱动,获取访问方应用,包括:在访问方应用基于网络访问地址建立网络访问连接的过程中,根据网络访问地址的类型,调用WFP驱动,获取访问方应用。

[0029] 可选的,服务器在访问方应用基于网络访问地址建立网络访问连接的过程中,可以先根据网络访问地址即IP地址的地址编号,确定网络访问地址的类型属于常用的IPV6(Internet Protocol Version 6,互联网协议第6版)还是IPV4(Internet Protocol version 4,互联网通信协议第4版)类型,进一步的,WFP驱动根据IP类型,确定需要进入的驱动层,具体的,若IP类型为IPV6,则会进入FWPM_LAYER_ALE_AUTH_CONNECT_V6(IPV6)层,若IP类型为IPV4,则会进入FWPM_LAYER_ALE_AUTH_CONNECT_V4(IPV4)层,WFP驱动进入对应的驱动层之后,可以获取访问方应用相关信息,如访问方应用的程序路径,即获取访问方应用。

[0030] S203、根据访问方应用、网络访问地址和访问规则,确定网络访问请求的放行策略。

[0031] S204、根据放行策略,响应网络访问请求。

[0032] 在本发明实施例中,服务器在检测到网络访问请求之后,调用微软网络过滤平台WFP驱动,基于域名系统DNS协议,解析网络访问请求对应的网络访问地址,进一步在访问方应用基于网络访问地址建立网络访问连接的过程中,调用WFP驱动,获取访问方应用,从而确定网络访问请求的放行策略,响应网络访问请求。通过这样的方式,给出了一种获取访问方应用的实施方式,能够有效的获取访问方应用的相关信息,便于后续确定放行策略并对网络访问请求进行针对性的响应。

[0033] 实施例三

图3为本发明实施例三提供的一种网络访问方法的流程图,本实施例在上述实施例的基础上,进一步对“根据访问方应用、网络访问地址和访问规则,确定网络访问请求的放行策略”进行详细解释说明,如图3所示,本实施例提供的网络访问方法具体包括:

S301、根据网络访问请求,获取访问方应用和网络访问地址。

[0034] S302、调用WFP驱动,基于DNS协议,解析网络访问请求对应的目标域名地址关系。

[0035] 其中,目标域名地址关系是指网络访问请求目标访问的域名地址(目标域名)与其

对应的IP地址的对应关系。

[0036] 具体的，服务器检测到访问方应用发出网络访问请求时，可以调用WFP的内核驱动，此时操作系统的状态由原来的用户态转换为内核态，进一步利用WFP内核态下的域名解析模块，基于域名系统DNS协议，将网络访问请求中包含的访问网络的域名转换为IP地址，将访问网络的域名与转换出的IP地址的一一对应关系，作为网络访问请求对应的目标域名地址关系，即解析网络访问请求对应的目标域名地址关系。

[0037] S303、根据目标域名地址关系和访问规则中的网络访问规则，更新本地域名地址关系集。

[0038] 其中，本地域名地址关系集是指存储于本地的地址关系集。本地域名地址关系集包含至少一组域名与IP地址的对应关系。

[0039] 可选的，确定目标域名地址关系之后，可以将目标域名地址关系中的目标域名和/或IP地址以及访问规则中的网络访问规则输入预先训练好的匹配模型，确定匹配结果，也可以根据预设的条件，判断本地域名地址关系集中是否未存储有目标域名地址关系，若否，则不进行本地域名地址关系集更新，若是，则基于目标域名地址关系中的目标域名和/或IP地址，以及访问规则中的网络访问规则，更新本地域名地址关系集，具体的，根据目标域名地址关系和访问规则中的网络访问规则，更新本地域名地址关系集，包括：若目标域名地址关系中的域名满足访问规则中的网络访问规则，则将目标域名地址关系，添加到本地域名地址关系集中。

[0040] 可选的，可以将目标域名地址关系中的域名与访问规则中的网络访问规则进行匹配，判断网络访问规则中是否包含该域名，若是，则认为匹配成功，进一步将该域名与其对应IP地址的一一对应关系添加到本地域名地址关系集中，即将目标域名地址关系，添加到本地域名地址关系集中。

[0041] 可选的，服务器可以包括DNS解析模块和ALE(Application Link and Enabling，应用连接使能)控制模块，S302-S303的操作可以是通过服务器中的DNS解析模块来执行。

[0042] S304、判断网络访问地址是否记录在本地域名地址关系集中，且访问方应用是否满足访问规则中的应用访问规则。

[0043] 可选的，服务器中的ALE控制模块可以获取访问方应用的程序路径(即应用在磁盘的存储路径)和网络访问地址对应的IP地址，将网络访问地址以及本地存储的本地域名地址关系集进行匹配，判断网络访问地址是否记录在本地域名地址关系集中，若是，则认为目标访问地址满足网络访问规则，进一步的，根据获取的访问方应用的程序路径(即应用在磁盘的存储路径)，确定访问方应用的标识信息，判断访问方应用是否为被允许访问的应用，即判断访问方应用是否满足访问规则中的应用访问规则。

[0044] S305、根据判断结果，确定网络访问请求的放行策略。

[0045] 可选的，若网络访问地址记录在本地域名地址关系集中，且访问方应用满足访问规则中的应用访问规则，则可以确定网络访问请求的放行策略为允许放行策略；若网络访问地址未记录在本地域名地址关系集中，或访问方应用不满足访问规则中的应用访问规则，则可以确定网络访问请求的放行策略为拒绝放行策略。

[0046] S306、根据放行策略，响应网络访问请求。

[0047] 可选的，若确定网络访问请求的放行策略为允许放行策略，则可以根据访问方应

用与网络访问地址的访问端口，对相应的访问端口进行放行，使得访问方应用与目标网络保持连接。

[0048] 在本发明实施例中，服务器调用WFP驱动，基于DNS协议，解析网络访问请求对应的目标域名地址关系，并根据目标域名地址关系与网络访问规则，更新本地域名地址关系集，进一步判断网络访问地址是否记录在关系集中，且访问方应用是否满足应用访问规则，最后根据判断结果，确定网络访问请求的放行策略并进行响应，通过这样的方式，给出了一种确定放行策略的可实施方式，能够实现在不同应用访问不同网络时，基于应用访问规则和网络访问规则，确定出准确的放行策略，给出针对性的响应，有效地对网络访问请求进行局部拦截或放行。

[0049] 实施例四

图4为本发明实施例四提供的一种网络访问方法的流程图，本实施例在上述实施例的基础上，进一步对“根据访问方应用、网络访问地址和访问规则，确定网络访问请求的放行策略”之前的步骤进行详细的解释说明，如图4所示，本实施例提供的网络访问方法具体包括：

S401、根据网络访问请求，获取访问方应用和网络访问地址。

[0050] S402、对访问规则中的应用访问规则进行合法性验证。

[0051] 其中，合法性验证是指对应用是否为合法应用的验证。

[0052] 可选的，可以通过预设的规则，基于应用访问规则中包含的应用的相关信息，以及预存的该应用准确相关信息，进行合法性验证，即对访问规则中的应用访问规则进行合法性验证；也可以应用访问规则中关联应用的相关信息输入预先训练好的模型中，输出合法性验证的验证结果，即对访问规则中的应用访问规则进行合法性验证。

[0053] 可选的，可以对应用访问规则中关联应用的应用程序进行校验，来验证应用访问规则，相应的，对访问规则中的应用访问规则进行合法性验证，包括：获取访问规则中的应用访问规则关联的应用程序数据；确定应用程序数据的校验值；根据校验值，对应用访问规则进行合法性验证。

[0054] 其中，应用程序数据是指生成应用或可以表征应用身份的程序数据，如应用安装程序代码。校验值是指对应用程序数据进行处理之后获得的校验数值，例如，校验值可以是应用程序数据的MD5值，其中MD5值是利用一种被广泛使用的密码散列函数产生出的一个128位(16字节)的散列值，所谓密码散列函数是利用MD5信息摘要算法(MD5 Message-Digest Algorithm)得到的。校验值也可以是通过其他的加密算法对应用程序数据进行处理之后获得，本发明对此不做限制。

[0055] 具体的，服务器可以获取应用访问规则关联的应用的程序安装包等相关程序代码，利用MD5信息摘要算法，确定该程序代码的MD5值，同时获取预存的该程序代码以及程序代码对应的真实MD5值，将确定的程序代码的MD5值与预存的真实MD5值进行一致性比较，若一致，则表明验证通过，应用访问规则中该应用的信息是合法的，若不一致，则表明验证未通过，认为应用访问规则关联的应用是冒充的。

[0056] S403、若验证通过，则根据访问方应用、网络访问地址和访问规则，确定网络访问请求的放行策略。

[0057] 可选的，若验证通过，则可以认为访问规则中的应用访问规则是合法的，此时根据

访问方应用、网络访问地址和访问规则，确定网络访问请求的放行策略的过程在S102中已经给出了详细解释，此处不进行赘述。

[0058] 可选的，若验证未通过，则服务器可以确定放行策略为拒绝放行策略，不对该应用发出的网络访问请求进行放行。

[0059] S404、根据放行策略，响应网络访问请求。

[0060] 在本发明实施例中，服务器在确定放行策略之前，先对访问规则中的应用访问规则进行合法性验证，在验证通过的情况下，进一步确定放行策略并进行响应，通过这样的方式，校验了应用规则中应用的真实性，可以避免其他应用冒充某些应用，访问指定网络的情况，从而有效地对网络访问请求进行局部拦截或放行，提高了网络访问过程的安全性。

[0061] 实施例五

图5A为本发明实施例五提供的一种网络访问方法的流程图，图5B为本发明实施例五提供的服务器的结构框图，本实施例在上述实施例的基础上，给出了服务器根据管理员下发的访问规则，对网络访问请求进行局部拦截或放行的优选实例。

[0062] 如图5A所示，本实施例提供的网络访问方法具体包括：

S501、接收管理员向服务器下发的访问规则。

[0063] 可选的，S501是在操作系统的用户态下执行的。

[0064] 需要说明的是，访问方应用所处的本地机启动时，会自动加载并启动WFP驱动。示例性的，在驱动启动时，该驱动会在DATAGRAM_DATA_V4，ALE_AUTH_CONNECT_V4，ALE_AUTH_CONNECT_V6网络层上，设置访问允许授权或拦截。

[0065] 如图5B所示，本实施例中的服务器可以包括策略分发模块、DNS解析模块和ALE控制模块。操作系统可以包括用户态和内核态。操作系统处于用户态时，服务器可以接收管理员在操作系统用户态下向策略分发模块下发的访问规则。具体的，策略分发模块用于接收用户态传递的应用规则和网络规则，即应用策略，先检测应用规则的合法性，如果校验成功，则调用WFP内核驱动，此时操作系统的状态变为内核态，同时，把应用规则下发到WFP内核态下的DNS解析模块，把网络规则下发到WFP内核态下的DNS解析模块和ALE控制模块。

[0066] DNS解析模块具体用于：解析应用发出的DNS域名解析请求，获取域名和IP的对应关系，根据设置的网络规则做匹配，如果该域名在域名规则中，则把域名/IP对应关系保存起来。

[0067] ALE控制模块具体用于：当应用开始网络请求时，根据请求的IP地址，端口，应用路径配合网络规则和应用规则做匹配，如果匹配成功，则放行，不匹配，则拦截这个网络请求。

[0068] S502、检测应用访问规则合法性，若合法，则执行S504，若不合法，则执行S503。

[0069] 具体的，服务器的策略分发模块获取到访问规则之后，可以先把网络访问规则下发至驱动中，然后校验应用访问规则的合法性，如果合法，则将应用访问规则下发到WFP驱动中。

[0070] S503、若不合法，则拦截网络，不设置访问规则至WFP驱动。

[0071] S504、下发访问规则至WFP驱动。

[0072] 示例性的，以谷歌浏览器访问www.baidu.com(用户打开谷歌浏览器，输入www.baidu.com并回车)为例，当策略分发模块下发访问规则至WFP驱动完毕以后，操作系统处于内核态。

[0073] S505、根据访问规则，判断是否匹配，若是，则执行S507，若否，则执行S506。

[0074] 示例性的，谷歌浏览器发送DNS请求获取www.baidu.com对应的IP地址，此时会进入WFP FWPM_LAYER_DATAGRAM_DATA_V4层回调(解析模块通过回调找对应关系)，服务器可以通过DNS解析模块，按照DNS协议，解析出域名和IP对应关系，并将域名和网络访问规则进行匹配，如果域名是www.baidu.com，则将域名/IP对应关系保存起来

示例性的，谷歌浏览器获取DNS请求成功时，谷歌浏览器会开始基于IP与百度服务器连接，具体的，对目的IP做套接字(socket)连接，WFP驱动会根据IP地址类型，选择进入FWPM_LAYER_ALE_AUTH_CONNECT_V6(IPV6)或FWPM_LAYER_ALE_AUTH_CONNECT_V4(IPV4)层，服务器中的ALE控制模块可以获取到网络访问请求的程序路径(即谷歌应用在磁盘的路径)、目的IP(百度IP)和端口，来判断目的IP是否存储于域名/IP对应关系表(即本地域名地址关系集)中，若是，则进一步判断程序路径满足应用访问规则，在网络访问规则和应用访问规则都满足时，放行网络，否则，拦截网络请求。

[0075] S506、若不匹配，则拦截网络，不设置访问规则至WFP驱动。

[0076] 示例性的，若访问规则为只允许谷歌浏览器访问www.baidu.com，谷歌浏览器访问www.qq.com时，服务器中的DNS解析模块解析到www.qq.com和IP的对应关系之后，发现域名www.qq.com未存储在网络访问规则中，即不满足网络访问规则，因此不保存对应关系，此时驱动在ALE_AUTH_CONNECT_V6或ALE_AUTH_CONNECT_V4层中，因为没有在域名/IP对应表中查到IP，所以访问www.qq.com失败。

[0077] 示例性的，若访问规则为只允许谷歌浏览器访问www.baidu.com，IE浏览器访问www.baidu.com时，DNS解析模块解析到www.baidu.com域名和IP的对应关系并保存，虽然域名/IP对应表中查到了IP，即满足了网络访问规则，但是在应用访问规则中没有找到IE浏览器这个应用，所以IE浏览器访问www.baidu.com失败。

[0078] S507、放行网络。

[0079] 在本发明实施例中，服务器接收管理员下发的访问规则后，先检测应用访问规则的合法性，在应用访问规则合法的情况下，下发访问规则到WFP驱动，服务器进一步基于DNS解析模块和ALE模块，判断访问方应用及网络访问地址是否与访问规则匹配，在匹配的情况下，放行网络，在不匹配的情况下，拦截网络，给出了一种服务器在检测到网络访问请求时，如何对网络访问请求进行局部拦截或放行的可实施方式，可以有效的实现在不同应用访问不同网络时，基于应用访问规则和网络访问规则，给出针对性的响应，对网络访问请求进行局部拦截或放行。

[0080] 实施例六

图6为本发明实施例六提供的一种网络访问装置的结构框图，本发明实施例所提供的一种网络访问装置可执行本发明任一实施例所提供的网络访问方法，具备执行方法相应的功能模块和有益效果。

[0081] 该网络访问装置可以包括：获取模块601、确定模块602和响应模块603。

[0082] 其中，获取模块601，用于根据网络访问请求，获取访问方应用和网络访问地址；

确定模块602，用于根据所述访问方应用、网络访问地址和访问规则，确定所述网络访问请求的放行策略；其中，所述访问规则包括应用访问规则和网络访问规则；

响应模块603，用于根据所述放行策略，响应所述网络访问请求。

[0083] 在本发明实施例中，服务器根据网络访问请求，获取访问方应用和网络访问地址之后，根据访问方应用、网络访问地址、应用访问规则和网络访问规则，确定网络访问请求的放行策略，最后根据放行策略，响应网络访问请求。通过根据应用访问规则和网络访问规则来确定网络访问请求的放行策略，进而对网络访问请求做出响应，能够实现在不同应用访问不同网络时，基于应用访问规则和网络访问规则，给出针对性的响应，有效地对网络访问请求进行局部拦截或放行。

[0084] 进一步的，获取模块601可以包括：

解析单元，用于调用微软网络过滤平台WFP驱动，基于域名系统DNS协议，解析网络访问请求对应的网络访问地址；

获取单元，用于在访问方应用基于所述网络访问地址建立网络访问连接的过程中，调用WFP驱动，获取访问方应用。

[0085] 进一步的，获取单元具体用于：

在访问方应用基于所述网络访问地址建立网络访问连接的过程中，根据网络访问地址的类型，调用WFP驱动，获取访问方应用。

[0086] 进一步的，确定模块602可以包括：

关系解析单元，用于调用WFP驱动，基于DNS协议，解析所述网络访问请求对应的目标域名地址关系；

更新单元，用于根据所述目标域名地址关系和访问规则中的网络访问规则，更新本地域名地址关系集；

判断单元，用于判断所述网络访问地址是否记录在所述本地域名地址关系集中，且所述访问方应用是否满足所述访问规则中的应用访问规则；

确定单元，用于根据判断结果，确定网络访问请求的放行策略。

[0087] 进一步的，更新单元具体用于：

若所述目标域名地址关系中的域名满足所述访问规则中的网络访问规则，则将所述目标域名地址关系，添加到本地域名地址关系集中。

[0088] 进一步的，确定模块602还可以包括：

验证单元，用于对访问规则中的应用访问规则进行合法性验证；

策略确定单元，用于若验证通过，则根据所述访问方应用、网络访问地址和访问规则，确定所述网络访问请求的放行策略。

[0089] 进一步的，验证单元具体用于：

获取访问规则中的应用访问规则关联的应用程序数据；

确定所述应用程序数据的校验值；

根据所述校验值，对所述应用访问规则进行合法性验证。

[0090] 实施例七

图7为本发明实施例七提供的一种电子设备的结构示意图。图7示出了适于用来实现本发明实施例实施方式的示例性设备的框图。图7显示的设备仅仅是一个示例，不应对本发明实施例的功能和使用范围带来任何限制。

[0091] 如图7所示，电子设备12以通用计算设备的形式表现。电子设备12的组件可以包括但不限于：一个或者多个处理器或者处理单元16，系统存储器28，连接不同系统组件(包括

系统存储器28和处理单元16)的总线18。

[0092] 总线18表示几类总线结构中的一种或多种,包括存储器总线或者存储器控制器,外围总线,图形加速端口,处理器或者使用多种总线结构中的任意总线结构的局域总线。举例来说,这些体系结构包括但不限于工业标准体系结构(ISA)总线,微通道体系结构(MAC)总线,增强型ISA总线、视频电子标准协会(VESA)局域总线以及外围组件互连(PCI)总线。

[0093] 电子设备12典型地包括多种计算机系统可读介质。这些介质可以是任何能够被电子设备12访问的可用介质,包括易失性和非易失性介质,可移动的和不可移动的介质。

[0094] 系统存储器28可以包括易失性存储器形式的计算机系统可读介质,例如随机存取存储器(RAM)30和/或高速缓存存储器(高速缓存32)。电子设备12可以进一步包括其它可移动/不可移动的、易失性/非易失性计算机系统存储介质。仅作为举例,存储系统34可以用于读写不可移动的、非易失性磁介质(图7未显示,通常称为“硬盘驱动器”)。尽管图7中未示出,可以提供用于对可移动非易失性磁盘(例如“软盘”)读写的磁盘驱动器,以及对可移动非易失性光盘(例如CD-ROM, DVD-ROM或者其它光介质)读写的光盘驱动器。在这些情况下,每个驱动器可以通过一个或者多个数据介质接口与总线18相连。系统存储器28可以包括至少一个程序产品,该程序产品具有一组(例如至少一个)程序模块,这些程序模块被配置以执行本发明实施例各实施例的功能。

[0095] 具有一组(至少一个)程序模块42的程序/实用工具40,可以存储在例如系统存储器28中,这样的程序模块42包括但不限于操作系统、一个或者多个应用程序、其它程序模块以及程序数据,这些示例中的每一个或某种组合中可能包括网络环境的实现。程序模块42通常执行本发明实施例所描述的实施例中的功能和/或方法。

[0096] 电子设备12也可以与一个或多个外部设备14(例如键盘、指向设备、显示器24等)通信,还可与一个或者多个使得用户能与该电子设备12交互的设备通信,和/或与使得该电子设备12能与一个或多个其它计算设备进行通信的任何设备(例如网卡,调制解调器等等)通信。这种通信可以通过输入/输出(I/O)接口22进行。并且,电子设备12还可以通过网络适配器20与一个或者多个网络(例如局域网(LAN),广域网(WAN)和/或公共网络,例如因特网)通信。如图所示,网络适配器20通过总线18与电子设备12的其它模块通信。应当明白,尽管图7中未示出,可以结合电子设备12使用其它硬件和/或软件模块,包括但不限于:微代码、设备驱动器、冗余处理单元、外部磁盘驱动阵列、RAID系统、磁带驱动器以及数据备份存储系统等。

[0097] 处理单元16通过运行存储在系统存储器28中的程序,从而执行各种功能应用以及数据处理,例如实现本发明实施例所提供的网络访问方法。

[0098] 实施例八

本发明实施例八还提供一种计算机可读存储介质,其上存储有计算机程序(或称为计算机可执行指令),该程序被处理器执行时用于执行本发明实施例所提供的网络访问方法。

[0099] 本发明实施例的计算机存储介质,可以采用一个或多个计算机可读的介质的任意组合。计算机可读介质可以是计算机可读信号介质或者计算机可读存储介质。计算机可读存储介质例如可以是但不限于电、磁、光、电磁、红外线、或半导体的系统、装置或器件,或者任意以上的组合。计算机可读存储介质的更具体的例子(非穷举的列表)包括:具有一个或

多个导线的电连接、便携式计算机磁盘、硬盘、随机存取存储器(RAM)、只读存储器(ROM)、可擦式可编程只读存储器(EPROM或闪存)、光纤、便携式紧凑磁盘只读存储器(CD-ROM)、光存储器件、磁存储器件、或者上述的任意合适的组合。在本文件中,计算机可读存储介质可以是任何包含或存储程序的有形介质,该程序可以被指令执行系统、装置或者器件使用或者与其结合使用。

[0100] 计算机可读的信号介质可以包括在基带中或者作为载波一部分传播的数据信号,其中承载了计算机可读的程序代码。这种传播的数据信号可以采用多种形式,包括但不限于电磁信号、光信号或上述的任意合适的组合。计算机可读的信号介质还可以是计算机可读存储介质以外的任何计算机可读介质,该计算机可读介质可以发送、传播或者传输用于由指令执行系统、装置或者器件使用或者与其结合使用的程序。

[0101] 计算机可读介质上包含的程序代码可以用任何适当的介质传输,包括但不限于无线、电线、光缆、RF等等,或者上述的任意合适的组合。

[0102] 可以以一种或多种程序设计语言或其组合来编写用于执行本发明实施例操作的计算机程序代码,所述程序设计语言包括面向对象的程序设计语言—诸如Java、Smalltalk、C++,还包括常规的过程式程序设计语言诸如“C”语言或类似的程序设计语言。程序代码可以完全地在用户计算机上执行、部分地在用户计算机上执行、作为一个独立的软件包执行、部分在用户计算机上部分在远程计算机上执行、或者完全在远程计算机或服务器上执行。在涉及远程计算机的情形中,远程计算机可以通过任意种类的网络包括局域网(LAN)或广域网(WAN)连接到用户计算机,或者,可以连接到外部计算机(例如利用因特网服务提供商来通过因特网连接)。

[0103] 注意,上述仅为本发明的较佳实施例及所运用技术原理。本领域技术人员会理解,本发明不限于这里所述的特定实施例,对本领域技术人员来说能够进行各种明显的变化、重新调整和替代而不会脱离本发明的保护范围。因此,虽然通过以上实施例对本发明实施例进行了较为详细的说明,但是本发明实施例不仅仅限于以上实施例,在不脱离本发明构思的情况下,还可以包括更多其他等效实施例,而本发明的范围由所附的权利要求范围决定。

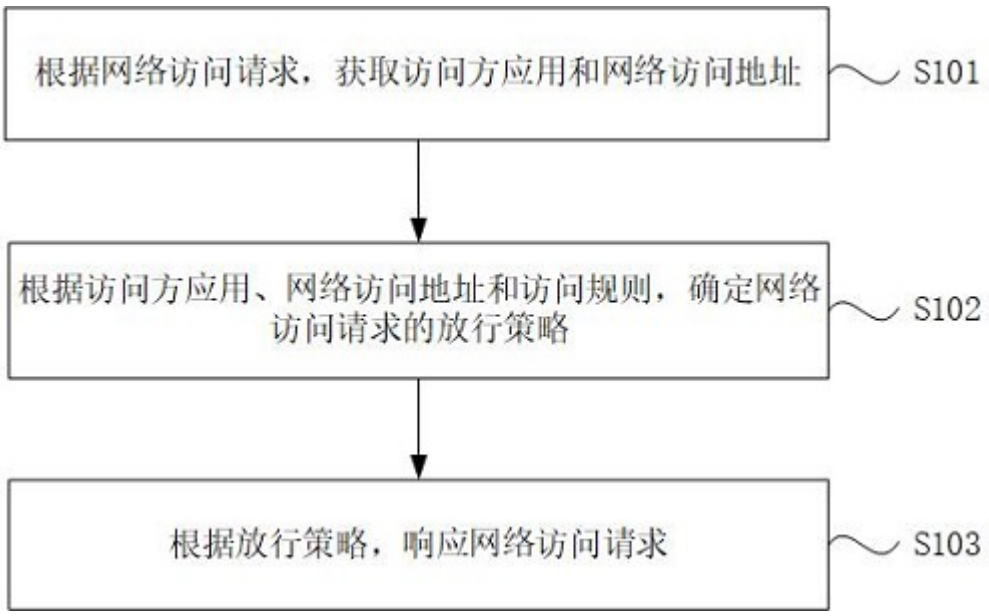

根据网络访问请求，获取访问方应用和网络访问地址
S101
根据访问方应用、网络访问地址和访问规则，确定网络访问请求的放行策略
S102
根据放行策略，响应网络访问请求
S103

图1

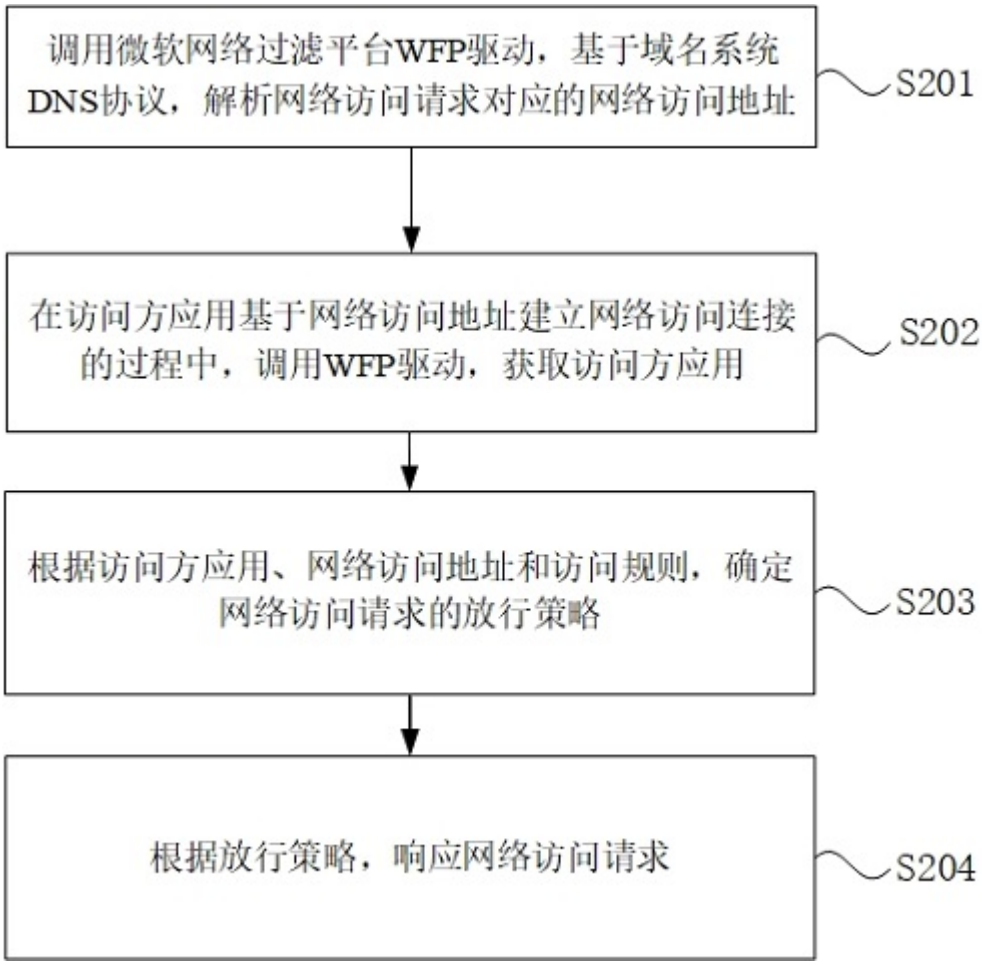

调用微软网络过滤平台WFP驱动，基于域名系统DNS协议，解析网络访问请求对应的网络访问地址
S201
在访问方应用基于网络访问地址建立网络访问连接的过程中，调用WFP驱动，获取访问方应用
S202
根据访问方应用、网络访问地址和访问规则，确定网络访问请求的放行策略
S203
根据放行策略，响应网络访问请求
S204

图2

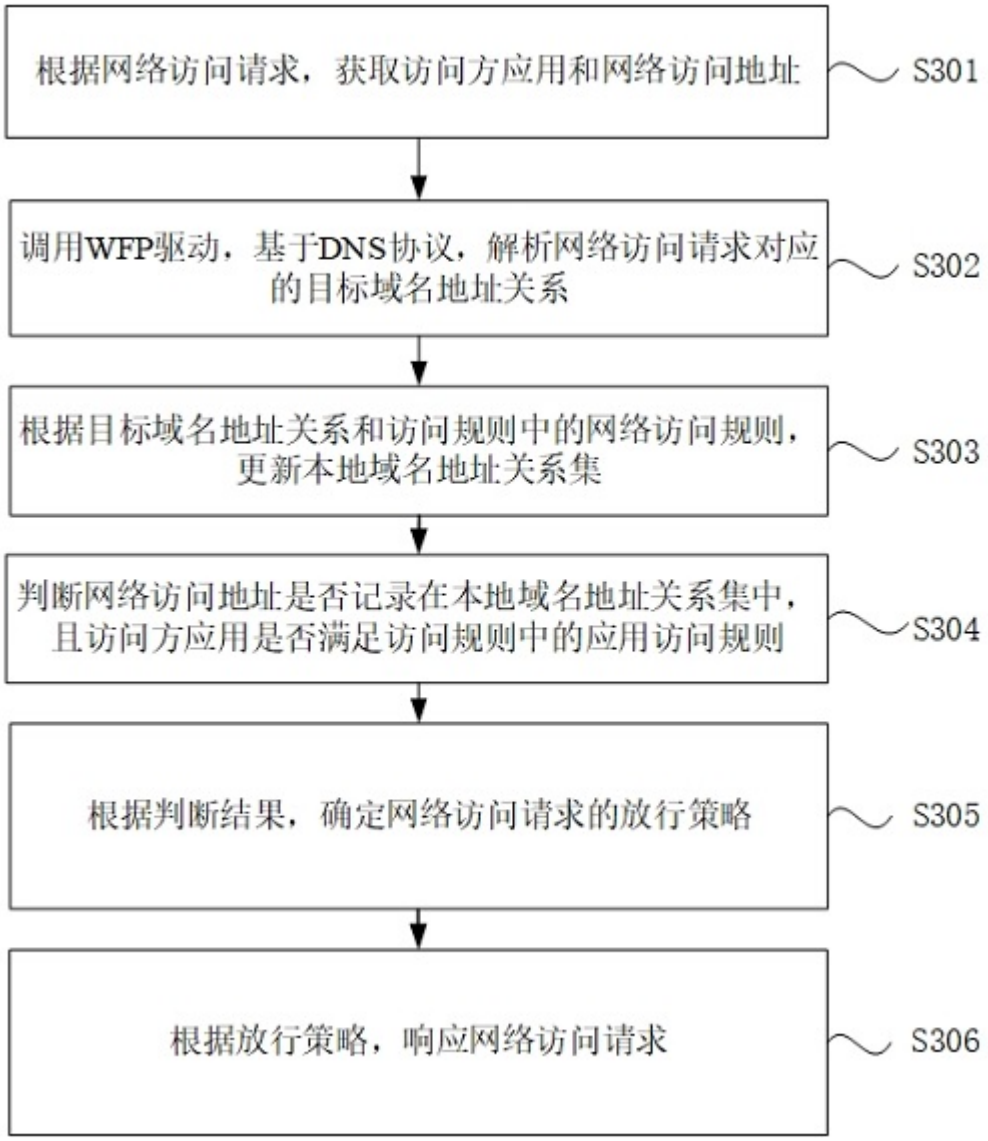

根据网络访问请求，获取访问方应用和网络访问地址
S301
调用WFP驱动，基于DNS协议，解析网络访问请求对应的目标域名地址关系
S302
根据目标域名地址关系和访问规则中的网络访问规则，更新本地域名地址关系集
S303
判断网络访问地址是否记录在本地域名地址关系集中，且访问方应用是否满足访问规则中的应用访问规则
S304
根据判断结果，确定网络访问请求的放行策略
S305
根据放行策略，响应网络访问请求
S306

图3

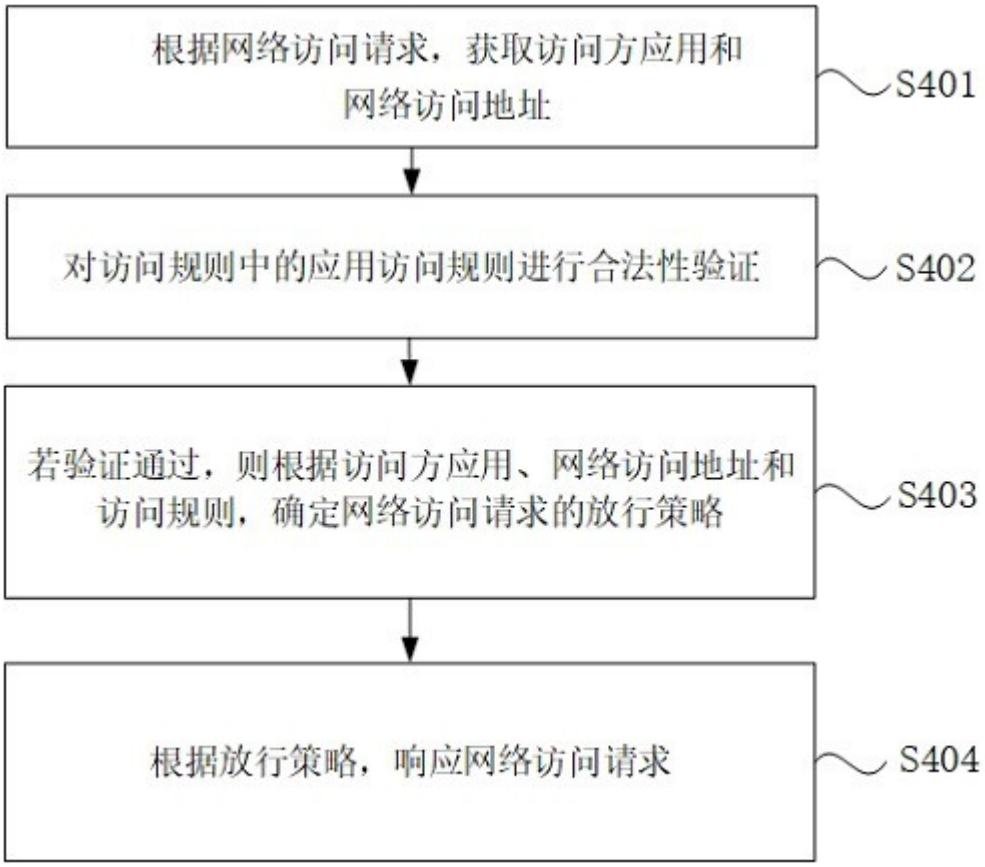

根据网络访问请求，获取访问方应用和网络访问地址
S401
对访问规则中的应用访问规则进行合法性验证
S402
若验证通过，则根据访问方应用、网络访问地址和访问规则，确定网络访问请求的放行策略
S403
根据放行策略，响应网络访问请求
S404

图4

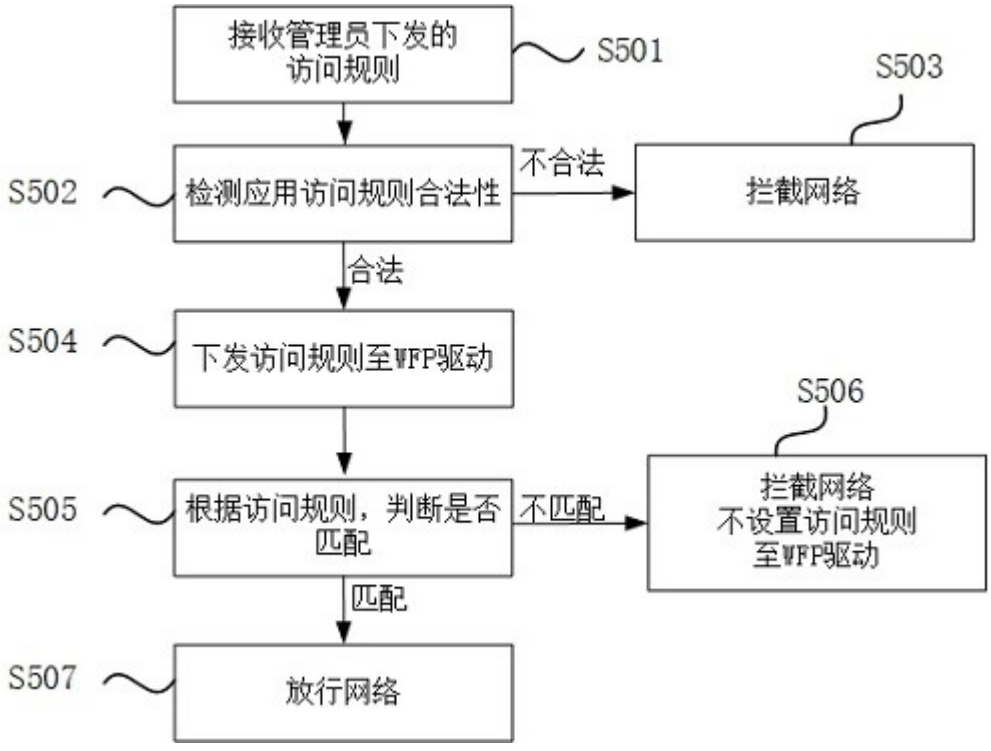

接收管理员下发的访问规则
S501
S502
检测应用访问规则合法性
不合法
S503
拦截网络
合法
S504
下发访问规则至WFP驱动
S505
根据访问规则，判断是否匹配
不匹配
S506
拦截网络
不设置访问规则
至WFP驱动
匹配
S507
放行网络

图5A


用户态
策略分发模块
内核态
DNS解析模块
ALE控制模块

图5B

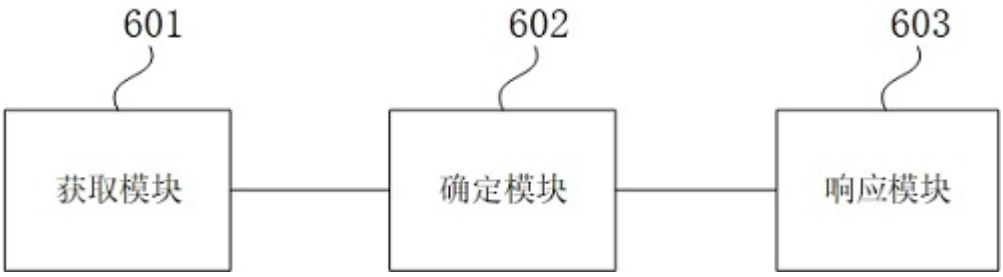

601
602
603
获取模块
确定模块
响应模块

图6

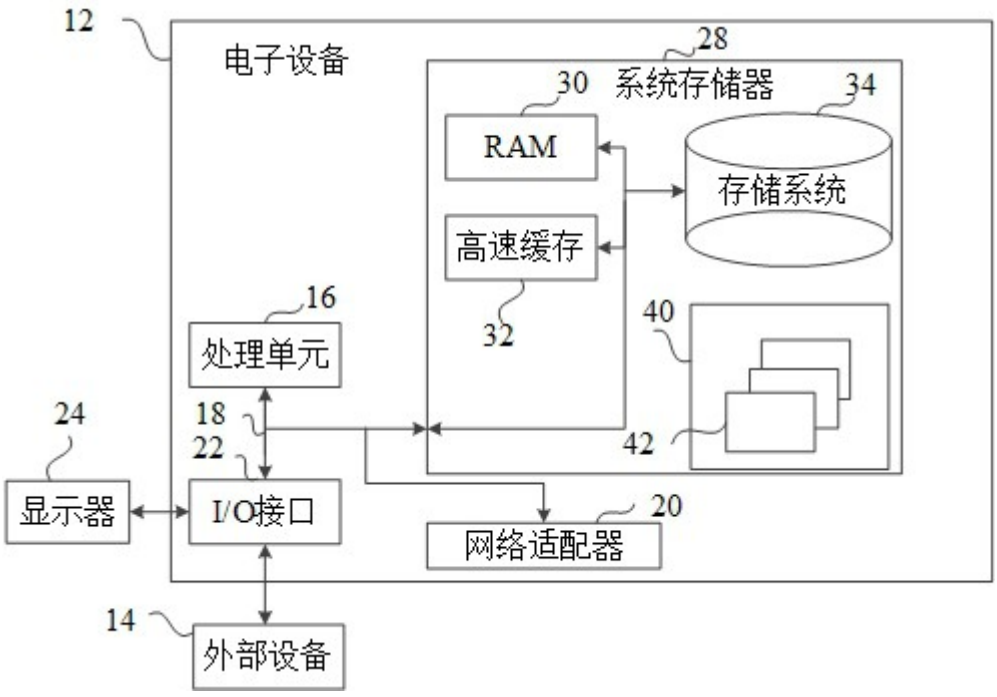

12
电子设备
28
30
系统存储器
34
RAM
存储系统
高速缓存
32
16
处理单元
40
24
18
22
42
显示器
I/O接口
20
网络适配器
14
外部设备

图7