(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 106789945 A
(43)申请公布日 2017.05.31

(21)申请号 201611079368.7

(22)申请日 2016.11.30

(71)申请人 上海斐讯数据通信技术有限公司
地址 201616 上海市松江区思贤路3666号

(72)发明人 刘玉敏

(74)专利代理机构 上海硕力知识产权代理事务所 31251
代理人 郭桂峰

(51)Int.Cl.
H04L 29/06(2006.01)

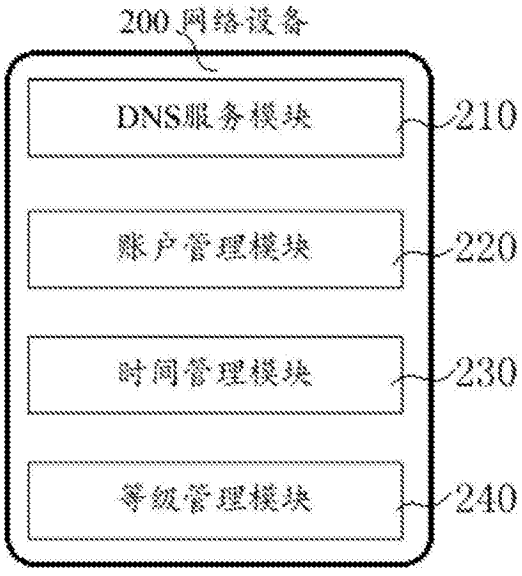
权利要求书2页 说明书8页 附图3页

(54)发明名称

一种网络设备以及上网行为管理方法

(57)摘要

本专利申请为网络设备以及上网行为管理方法，涉及网络通信领域，尤其涉及上网行为管理的技术。公开了一种上网行为管理的网络设备，包括DNS服务模块、账户管理模块、时间管理模块和访问等级管理模块，所述DNS服务模块，用于将被访问的域名转换成目标IP地址；所述账户管理模块，用于建立不同使用身份；所述时间管理模块，用于限制上网的时间权限；所述等级管理模块，用于限制上网的访问范围权限。



CN 106789945 A

1.一种上网行为管理方法，其特征在于，所述方法步骤包括：

设定网络设备的上网访问的账户；

给所述账户设定上网访问的时间限制；

给所述账户设定上网访问的范围限制；

给所述账户设定上网访问的等级限制。

2.根据权利要求1所述的上网行为管理方法，其特征在于，在所述设定网络设备的上网访问的账户步骤中还包括如下步骤：

给同一人在不同场合设定上网访问的所述账户；

给同一场合的不同人设定上网访问的所述账户；

给同类的所述账户设定至少一个同类管理员；给所述网络设备设定至少一个总管理员。

3.根据权利要求1所述的上网行为管理方法，其特征在于，在所述给所述账户设定上网访问的时间限制步骤中还包括如下步骤：

当符合所述时间限制的时候，所述账户可以通过所述网络设备进行上网访问；

当不符合所述时间限制的时候，所述账户被禁止继续进行所述上网访问。

4.根据权利要求1所述的上网行为管理方法，其特征在于，在所述给所述账户设定上网访问的范围限制步骤中还包括如下步骤：

当符合所述范围限制的时候，所述账户可以通过所述网络设备进行上网访问；

当不符合所述范围限制的时候，所述账户被禁止进行逾制的所述上网访问。

5.根据权利要求1所述的上网行为管理方法，其特征在于，在所述给所述账户设定上网访问的等级限制步骤中还包括如下步骤：

当符合所述等级限制的时候，所述账户可以通过所述网络设备进行上网访问；

当不符合所述等级限制的时候，所述账户被禁止进行僭越的所述上网访问。

6.根据权利要求3或4或5所述的上网行为管理方法，其特征在于，所述方法步骤还包括如下步骤：

当发生超时访问、逾制访问或者僭越访问的情况时，给相关管理员发送报警提醒；

广告拦截模块拦截所述目标IP地址中的弹窗广告；

病毒识别模块扫描所述目标IP地址中的病毒程序或者木马程序。

7.一种上网行为管理的网络设备，包括DNS服务模块、账户管理模块、时间管理模块和访问等级管理模块，其特征在于，

所述DNS服务模块，用于将被访问的域名转换成目标IP地址；

所述账户管理模块，用于建立不同使用身份；

所述时间管理模块，用于限制上网的时间权限；

所述等级管理模块，用于限制上网的访问范围权限。

8.根据权利要求7所述的上网行为管理的网络设备，其特征在于，所述网络设备还包括广告拦截模块，

所述广告拦截模块，用于拦截所述目标IP地址中的弹窗广告。

9.根据权利要求7所述的上网行为管理的网络设备，其特征在于，所述网络设备还包括病毒识别模块，

所述病毒识别模块，用于扫描所述目标IP地址中的病毒程序或者木马程序。

10.根据权利要求7或8或9所述的上网行为管理的网络设备，其特征在于，所述网络设备还包括报警模块，

所述报警模块，用于在发生超时访问、逾制访问、僭越访问、广告弹窗或者病毒程序启动的情况时，给相关管理员发送报警提醒。

一种网络设备以及上网行为管理方法

技术领域

[0001] 本专利申请涉及网络通信领域，尤其涉及上网行为管理的技术。

背景技术

[0002] 路由器(Router，又称路径器)是一种计算机网络设备，它能将数据通过打包一个个网络传送至目的地(选择数据的传输路径)，这个过程称为路由。路由器就是连接两个以上各别网络的设备，路由工作在OSI模型的第三层——即网络层。

[0003] 路由器(Router)，是连接因特网中各局域网、广域网的设备，它会根据信道的情况自动选择和设定路由，以最佳路径，按前后顺序发送信号。路由器是互联网络的枢纽，"交通警察"。目前路由器已经广泛应用于各行各业，各种不同档次的产品已成为实现各种骨干网内部连接、骨干网间互联和骨干网与互联网互联互通业务的主力军。路由和交换机之间的主要区别就是交换机发生在OSI参考模型第二层(数据链路层)，而路由发生在第三层，即网络层。这一区别决定了路由和交换机在移动信息的过程中需使用不同的控制信息，所以两者实现各自功能的方式是不同的。

[0004] AP是(Wireless)Access Point的缩写，即(无线)访问接入点。如果无线网卡可比作有线网络中的以太网卡，那么AP就是传统有线网络中的HUB，也是目前组建小型无线局域网时最常用的设备。AP相当于一个连接有线网和无线网的桥梁，其主要作用是将各个无线网络客户端连接到一起，然后将无线网络接入以太网。

[0005] DNS是计算机域名系统(Domain Name System或Domain Name Service)的缩写，它是由域名解析器和域名服务器组成的。域名服务器是指保存有该网络中所有主机的域名和对应IP地址，并具有将域名转换为IP地址功能的服务器。其中域名必须对应一个IP地址，而IP地址不一定有域名。域名系统采用类似目录树的等级结构。域名服务器为客户机/服务器模式中的服务器方，它主要有两种形式:主服务器和转发服务器。将域名映射为IP地址的过程就称为"域名解析"。在Internet上域名与IP地址之间是一对一(或者多对一)的，也可采用DNS轮循实现一对多，域名虽然便于人们记忆，但机器之间只认IP地址，它们之间的转换工作称为域名解析，域名解析需要由专门的域名解析服务器来完成，DNS就是进行域名解析的服务器。DNS命名用于Internet等TCP/IP网络中，通过用户友好的名称查找计算机和服务。当用户在应用程序中输入DNS名称时，DNS服务可以将此名称解析为与之相关的其他信息，如IP地址。因为，你在上网时输入的网址，是通过域名解析系统解析找到了相对应的IP地址，这样才能上网。其实，域名的最终指向是IP。

[0006] OpenDNS为个人和商业用户提供DNS方案。用户可以自行选择使用OpenDNS的服务或者使用当地ISP提供的DNS服务。将服务器组放置在具有战略意义的地方和使用大量的域名缓存可以使DNS查询进度更快，从而加快页面的检索速度。DNS的查询结果有时被本地的操作系统或应用程序缓存下来，所以速度的增加也许不能在每次查询中体现出来，但本地缓存里没有的结果其查询速度的增加则显而易见。其他特征包括一个反钓鱼过滤器和输入纠正(typo correction)。通过收集恶意网站列表，当用户通过他们的服务来访问这些恶意

网站时，OpenDNS将封锁这些恶意网站。OpenDNS最近启动了反钓鱼服务(PhishTank)，这样全球的用户就可以报告和察看不可信的钓鱼网站。

[0007] 中国专利申请号为CN201410004945.0，本发明的目的是提供一种用于实现访问控制的方法、设备与系统。第一网络设备端根据第二网络设备所对应的域名及第一访问控制信息，生成与第一访问控制信息相对应的第二访问控制信息，并将其作为域名发送至DNS设备；然后在第二网络设备端根据对第二网络设备端的应用访问请求信息，以及第二网络设备端所对应的域名，生成与应用访问请求信息相对应的域名查询信息，将域名查询信息在与第二网络设备端相对应的DNS设备中进行查询，以确定与应用访问请求信息相对应的访问控制信息。与现有技术相比，本发明基于DNS协议的简单性、时效性、可靠性、安全性以及支持的广泛性，实现了对访问控制信息的动态调整与统一管理，提高了对访问控制信息的管理效率。

[0008] 中国专利申请号为CN201410552834.3，一种上网行为管理系统，它涉及网络系统技术领域，网络信号源的输出端与卫星的输入端连接，卫星的输出端与用户终端装置的输出端连接，数据修改装置的输出端分别与数据粉碎装置和用户POST接受装置的输入端连接，数据粉碎装置的输出端与报警装置的输入端连接。本发明结构简单、设计合理，网络原始数据通过卫星传输到用户客户端处，并对原始数据进行存储，同时利用敏感内容检测装置对原始数据进行检测，当信息没有被病毒污染时，用户可直接接受并打开，当原始数据检测到有问题时，先通过数据修改器进行修改，再次发送给客户，当无法修改时则直接通过数据粉碎装置对数据进行粉碎，并同时报警，很好的提高数据使用的安全性。

[0009] 现有技术中，并没有给到路由器做到上网行为的有效管理，包括基于时间的管理、基于权限的管理、基于访问范围的管理等。

发明内容

[0010] 本发明在于提供一种内置OpenDNS的上网行为控制的路由器产品，能做到上网的时间管控、上网的访问范围管控、上网的访问内容级别管控，还可以设置多种使用者身份，方便因人而异进行上网行为管理。

[0011] 本发明是通过以下技术方案实现的：

[0012] 一种上网行为管理方法，所述方法步骤包括：

[0013] 设定网络设备的上网访问的账户；

[0014] 给所述账户设定上网访问的时间限制；

[0015] 给所述账户设定上网访问的范围限制；

[0016] 给所述账户设定上网访问的等级限制。

[0017] 进一步，所述的上网行为管理方法，在所述设定网络设备的上网访问的账户步骤中还包括如下步骤：

[0018] 给同一人在不同场合设定上网访问的所述账户；

[0019] 给同一场合的不同人设定上网访问的所述账户；

[0020] 给同类的所述账户设定至少一个同类管理员；比如组管理员、多组的上级管理员等；

[0021] 给所述网络设备设定至少一个总管理员。

[0022] 总管理员管辖多组的上级管理员，多组的上级管理员管辖其下级的多个组管理员，组管理员管辖组成员(普通用户)。根据情形需要，可以只设两级管理，比如家庭环境下只设有总管理员和普通用户，也可以设多级管理，比如大规模的公司，总管理员下分别设有部门级管理员、科室级管理员、小组级管理员和普通用户。

[0023] 在公司的公共区域，可以设置该区域的管理员，任何进入该区域的普通用户受制于该区域的管理员和该管理员设定的上网行为管理策略。

[0024] 进一步，所述的上网行为管理方法，在所述给所述账户设定上网访问的时间限制步骤中还包括如下步骤：

[0025] 当符合所述时间限制的时候，所述账户可以通过所述网络设备进行上网访问；

[0026] 当不符合所述时间限制的时候，所述账户被禁止继续进行所述上网访问。

[0027] 进一步，所述的上网行为管理方法，在所述给所述账户设定上网访问的范围限制步骤中还包括如下步骤：

[0028] 当符合所述范围限制的时候，所述账户可以通过所述网络设备进行上网访问；

[0029] 当不符合所述范围限制的时候，所述账户被禁止进行逾制的所述上网访问。

[0030] 进一步，所述的上网行为管理方法，在所述给所述账户设定上网访问的等级限制步骤中还包括如下步骤：

[0031] 当符合所述等级限制的时候，所述账户可以通过所述网络设备进行上网访问；

[0032] 当不符合所述等级限制的时候，所述账户被禁止进行僭越的所述上网访问。

[0033] 进一步，所述的上网行为管理方法，所述方法还包括如下步骤：

[0034] 当发生超时访问、逾制访问或者僭越访问的情况时，给相关管理员发送报警提醒。

[0035] 广告拦截模块拦截所述目标IP地址中的弹窗广告；

[0036] 病毒识别模块扫描所述目标IP地址中的病毒程序或者木马程序；上述2种情况下，也给相关管理员发送报警提醒。

[0037] 比如某用户发生上述情况，其组管理员和网络设备的总管理员将收到报警提醒。报警提醒可根据设置，发送到相关人员的手机短信、邮箱或者QQ等通信软件中，也可接通相关人员的电话，并播放预设的语音提醒。

[0038] 本发明还提供了一种可以用于管理上网行为的网络设备：

[0039] 一种上网行为管理的网络设备，包括DNS服务模块、账户管理模块、时间管理模块和访问等级管理模块，

[0040] 所述DNS服务模块，用于将被访问的域名转换成目标IP地址；

[0041] 所述账户管理模块，用于建立不同使用身份；比如总管理员，有权为每个访问成员设定登陆账户，对每个账户设定上网权限。而身份包括总管理员、管理员组管理员、用户组管理员和普通用户等；

[0042] 所述时间管理模块，用于限制上网的时间权限；

[0043] 所述等级管理模块，用于限制上网的访问范围权限。

[0044] 进一步，所述的上网行为管理的网络设备，所述网络设备还包括广告拦截模块，所述广告拦截模块，用于拦截所述目标IP地址中的弹窗广告。

[0045] 进一步，所述的上网行为管理的网络设备，所述网络设备还包括病毒识别模块，所述病毒识别模块，用于扫描所述目标IP地址中的病毒程序或者木马程序。

[0046] 进一步，所述的上网行为管理的网络设备，所述网络设备还包括报警模块，

[0047] 所述报警模块，用于在发生超时访问、逾制访问、僭越访问、广告弹窗或者病毒程序启动的情况时，给相关管理员发送报警提醒。比如向设定终端发出报警提示和报警内容，短信、微信或者电话语音。

[0048] 本发明至少具有以下有益效果之一：

[0049] 1.本发明克服了原先单一的上网控制的技术问题——要么全放开，要么不放开，上网行为管理效果差，适应性不强；

[0050] 2.本发明赋予网络设备可以进行具体的上网干预，包括上网的时间管控、上网的访问范围管控、上网的访问内容级别管控等；

[0051] 3.本发明赋予网络设备可以设置多种使用者身份，方便因人而异进行上网行为管理，还可以设置各级管理员，实现多级管控；

[0052] 4.本发明提供的网络设备不仅可以在家庭用于管控未成年的孩子随时上网，也能管控他们的访问限制；还可以在企业用于管控员工的上网行为，阻止他们在工作时间访问与工作无关的网址；

[0053] 5、本发明提供的网络设备还可以进行报警提醒，通知相关管理人员实时掌握普通用户的违规操作情况；

[0054] 6、本发明提供的网络设备，智能化程度强、可靠性高，同时执行效率高、应用范围广。

附图说明

[0055] 下面结合附图和具体实施方式对本发明作进一步详细说明：

[0056] 图1为本发明第一实施例流程示意图；

[0057] 图2为本发明第一实施例模块示意图；

[0058] 图3为本发明第二实施例流程示意图；

[0059] 图4为本发明第二实施例模块示意图；

[0060] 图5为本发明第四实施例网络连接示意图。

[0061] 附图标记说明

[0062] 网络设备-200、DNS服务模块-210、账户管理模块-220、时间管理模块-230、等级管理模块-240、广告拦截模块-250、病毒识别模块-260、报警模块-270。

具体实施方式

[0063] 为了更清楚地说明本发明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，以下说明和附图对于本发明是示例性的，并且不应被理解为限制本发明。以下说明描述了众多具体细节以方便对本发明理解。然而，在某些实例中，熟知的或常规的细节并未说明，以满足说明书简洁的要求。

[0064] 在本申请一个典型的计算硬件配置中，客户端/终端、网络设备和可信方均包括一个或多个处理器(CPU)、输入/输出接口、网络接口和内存。

[0065] 本发明中的客户端、移动终端或网络设备包括处理器，含单核处理器或多核处理器。处理器也可称为一个或多个微处理器、中央处理单元(CPU)等等。更具体地，处理器可为

复杂的指令集计算(CISC)微处理器、精简指令集计算(RISC)微处理器、超长指令字(VLIW)微处理器、实现其他指令集的处理器，或实现指令集组合的处理器。处理器还可为一个或多个专用处理器，诸如专用集成电路(ASIC)、现场可编程门阵列(FPGA)、数字信号处理器(DSP)、网络处理器、图形处理器、网络处理器、通信处理器、密码处理器、协处理器、嵌入式处理器、或能够处理指令的任何其他类型的逻辑部件。处理器用于执行本发明所讨论的操作和步骤的指令。

[0066] 本发明中的客户端、移动终端或网络设备包括存储器，用于存储大数据，可包括一个或多个易失性存储设备，如随机存取存储器(RAM)、动态RAM(DRAM)、同步DRAM(SDRAM)、静态RAM(SRAM)或其他类型的存储设备。存储器可存储包括由处理器或任何其他设备执行的指令序列的信息。例如，多种操作系统、设备驱动程序、固件(例如，输入输出基本系统或BIOS)和/或应用程序的可执行代码和/或数据可被加载在存储器中并且由处理器执行。

[0067] 本发明中的客户端、移动终端或网络设备的操作系统可为任何类型的操作系统，例如微软公司的Windows、Windows Phone，苹果公司IOS，谷歌公司的Android，以及Linux、Unix操作系统或其他实时或嵌入式操作系统诸如VxWorks等。

[0068] 为了更清楚地说明本发明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，以下说明和附图对于本发明是示例性的，并且不应被理解为限制本发明。以下说明描述了众多具体细节以方便对本发明理解。然而，在某些实例中，熟知的或常规的细节并未说明，以满足说明书简洁的要求。本发明的设备/系统及方法参见下述实施例：

[0069] 第一实施例

[0070] 如图1本发明第一实施例流程示意图所示：

[0071] 一种上网行为管理方法，所述方法步骤包括：

[0072] S100：设定网络设备的上网访问的账户；

[0073] S200：给所述账户设定上网访问的时间限制；

[0074] S300：给所述账户设定上网访问的范围限制；

[0075] S400：给所述账户设定上网访问的等级限制。

[0076] 优选地，所述的上网行为管理方法，在所述S100步骤中还包括如下步骤：

[0077] S110：给同一人在不同场合设定上网访问的所述账户；

[0078] S120：给同一场合的不同人设定上网访问的所述账户；

[0079] S130：给同类的所述账户设定至少一个同类管理员；比如组管理员、多组的上级管理员等；

[0080] S140：给所述网络设备设定至少一个总管理员。

[0081] 总管理员管辖多组的上级管理员，多组的上级管理员管辖其下级的多个组管理员，组管理员管辖组成员(普通用户)。根据情形需要，可以只设两级管理，比如家庭环境下只设有总管理员和普通用户，也可以设多级管理，比如大规模的公司，总管理员下分别设有部门级管理员、科室级管理员、小组级管理员和普通用户。

[0082] 在公司的公共区域，可以设置该区域的管理员，任何进入该区域的普通用户受制于该区域的管理员和该管理员设定的上网行为管理策略。

[0083] 优选地，所述的上网行为管理方法，在所述S200步骤中还包括如下步骤：

[0084] S210：当符合所述时间限制的时候，所述账户可以通过所述网络设备进行上网访问；

[0085] S220：当不符合所述时间限制的时候，所述账户被禁止继续进行所述上网访问。

[0086] 优选地，所述的上网行为管理方法，在所述S300步骤中还包括如下步骤：

[0087] S310：当符合所述范围限制的时候，所述账户可以通过所述网络设备进行上网访问；

[0088] S320：当不符合所述范围限制的时候，所述账户被禁止进行逾制的所述上网访问。

[0089] 优选地，所述的上网行为管理方法，在所述S400步骤中还包括如下步骤：

[0090] S410：当符合所述等级限制的时候，所述账户可以通过所述网络设备进行上网访问；

[0091] S420：当不符合所述等级限制的时候，所述账户被禁止进行僭越的所述上网访问。

[0092] 本实施例提供了一种可以用于管理上网行为的网络设备，如图2为本发明第一实施例模块示意图所示：

[0093] 一种上网行为管理的网络设备200，包括DNS服务模块210、账户管理模块220、时间管理模块230和访问等级管理模块240，

[0094] 所述DNS服务模块210，用于将被访问的域名转换成目标IP地址；包括域名解析器和域名服务器，前者后者

[0095] 所述账户管理模块220，用于建立不同使用身份；比如总管理员，有权为每个访问成员设定登陆账户，对每个账户设定上网权限。而身份包括总管理员、管理员组管理员、用户组管理员和普通用户等；

[0096] 所述时间管理模块230，用于限制上网的时间权限；

[0097] 所述等级管理模块240，用于限制上网的访问范围权限。

[0098] 账户管理模块，可以制作成类似OpenDNS的功能，也可以将OpenDNS功能内置于网络设备中，保持网络设备中的设置/功能与远端OpenDNS的设置/功能保持同步，定期更新，方便使用和管理。

[0099] 账户管理可以与访问范围管理、访问时间管理和访问等级管理等进行叠加组合，使上网行为管控策略更加灵活多样，适应各种场合和用户管理的需求。

[0100] 第二实施例

[0101] 在实施例一的基础上，本实施例还提供了上网行为管理方法，如图3为本发明第二实施例流程示意图所示，优选地，在所述S400步骤之后还包括如下步骤：

[0102] S500：当发生超时访问、逾制访问或者僭越访问的情况时，给相关管理员发送报警提醒。

[0103] S600：广告拦截模块拦截所述目标IP地址中的弹窗广告；

[0104] S700：病毒识别模块扫描所述目标IP地址中的病毒程序或者木马程序；上述2种情况下，也给相关管理员发送报警提醒。

[0105] 比如某用户发生上述情况，其组管理员和网络设备的总管理员将收到报警提醒。报警提醒可根据设置，发送到相关人员的手机短信、邮箱或者QQ等通信软件中，也可接通相关人员的电话，并播放预设的语音提醒。

[0106] 本实施例还提供了一种可以用于管理上网行为的网络设备，如图4为本发明第一

实施例模块示意图所示：

[0107] 在实施例一的基础上，优选地，所述的上网行为管理的网络设备，所述网络设备还包括广告拦截模块250，所述广告拦截模块250，用于拦截所述目标IP地址中的弹窗广告。

[0108] 优选地，所述的上网行为管理的网络设备，所述网络设备还包括病毒识别模块260，所述病毒识别模块260，用于扫描所述目标IP地址中的病毒程序或者木马程序。

[0109] 优选地，所述的上网行为管理的网络设备，所述网络设备还包括报警模块270，所述报警模块270，用于在发生超时访问、逾制访问、僭越访问、广告弹窗或者病毒程序启动的情况时，给相关管理员发送报警提醒。比如向设定终端发出报警提示和报警内容，短信、微信或者电话语音，比如“某某用户，正在访问含病毒程序的网站”、“某某用户，试图访问其未授权许可的网站”等等。方便相关管理员第一时间知晓危险情形，或者便于第一时间进行远程介入干预。

[0110] 第三实施例

[0111] 现在是网络世界，青少年和儿童接触网络的机会很大。对父母而言，这是个很可拍的想法。如何限制他们上网时间，如聊天、游戏、社交网络、购物和观看视频?如何在不需要24小时监视的情况下保护他们免受潜在伤害并且避免浏览不合适内容?

[0112] 现有具有家长控制功能的路由器采用的是控制设备的上网时间段。在允许的时间段对网络内容没有做相应过滤，即使可以做到添加URL过滤，这种方式也只能屏蔽少量网站，起不到网络保护的作用；在不允许访问网络的时间段，也没法去获取学习资料。这种控制方式不够灵活、人性化。

[0113] 本实施例涉及的一款内置OpenDNS家长控制服务的路由器产品。可以阻止不合适和危险网站，按时间(例如，在做家庭作业时不得访问facebook)和类别(成人、游戏、社交媒体等)限制访问，同时通过一个中心控制点(内置OpenDNS家长控制服务的路由器)保护家庭网络上每台设备免受恶意软件和钓鱼网站的侵害。为用户提供个性化和灵活性的需要。对于提供免费WiFi的小型企业、学校和其他设施，家长控制还能提供智能保护，通过简便的方式监控和保护您的客户、学生或员工免受不良的互联网内容和潜在黑客的侵害。家长控制可阻止多达50种类别的互联网内容，比如，社交、成人、暴力等网站内容，防止身份盗用和诈骗。

[0114] 内置OpenDNS家长控制服务的路由器产品。可以阻止不合适和危险网站，按时间(例如，在做家庭作业时不得访问facebook)和类别(成人、游戏、社交媒体等)限制访问，根据OpenDNS中的不同模式自动封杀家长不希望让孩子看到的内容，只要是经过这个路由器传送的数据将全部被控制，父母不但可以控制网站的访问，还可以对所有连接的设备执行网页过滤。

[0115] 本实施例提供了一个免费的家长控制软件，该软件能够以灵活的方式来监视和限制访问互联网上的不良内容。家长控制功能是由OpenDNS支持的，OpenDNS是在安全和基础设施服务领域领先的供应商，通过集成的Web内容过滤、防钓鱼网站和DNS安全等功能让互联网更安全。

[0116] 内置OpenDNS家长控制服务其实就是限制访问由路由器所定义的网站。定义了5个等级，从不限制到最高等级，由等级管理模块240进行设定控制：

[0117] (1).内置OpenDNS家长控制服务的路由器过滤级别分为：无(不阻止)、最小(仅阻

止网络钓鱼)、低(阻止情色网站和网络钓鱼)、中等(阻止所有与成人有关的网站、非法活动和网络钓鱼)、高(阻止所有与成人有关的网站、非法活动、社交网站、共享视屏网站、钓鱼网站和浪费时间的内容)五个等级;

[0118] (2).创建一个OPENDNS免费账号,登录后针对某一时间段,特定设备,设置过滤等级;

[0119] (3).在远程访问路由器家长控制中心,用已有的OPENDNS账号登录,可以控制家用路由器的过滤等级。

[0120] 至此,家长控制功能基本介绍。从注册使用和拦截结果来看,简单易用,而且效果明显。

[0121] 第四实施例

[0122] 如图5为本发明第四实施例网络连接示意图所示,本实施例涉及的“管理员实时控制”是家庭、小型企业及拥有免费Wi-Fi的地方如图书馆、咖啡馆这样的公共设施的福音——任何人基本上都想从充斥着不适宜内容的互联网中得到一个额外的保护,都会需要“管理员实时控制”。它拥有功能完整的设置,是其他“监控”解决方案不具备的;它使用户能够通过设置过滤器来阻止50多个类别不同的内容涵盖,其中包括社交、色情、暴力等网站。此外,这些设置可以具体指定每个用户每次上网。这就是说,某些网站或内容可以在特定用户上网的时候被拦截。

[0123] 本发明的好处还在于:

[0124] 一来可以避免孩子错误点击病毒网站而造成电脑中毒;二来从此可以培养对孩子的良好的上网行为;三来这个功能也可以使用在小企业上,避免员工在工作时间访问一些娱乐网站。

[0125] 对于本领域技术人员而言,显然本发明不限于上述示范性实施例的细节,而且在不背离本发明的精神或基本特征的情况下,能够以其他的具体形式实现本发明。因此,无论从哪一点来看,均应将实施例看作是示范性的,而且是非限制性的,本发明的范围由所附权利要求而不是上述说明限定,因此旨在将落在权利要求的等同要件的含义和范围内的所有变化涵括在本发明内。不应将权利要求中的任何附图标记视为限制所涉及的权利要求。此外,显然“包括”一词不排除其他单元或步骤,单数不排除复数。装置权利要求中陈述的多个单元或装置也可以由一个单元或装置通过软件或者硬件来实现。第一,第二等词语用来表示名称,而并不表示任何特定的顺序。

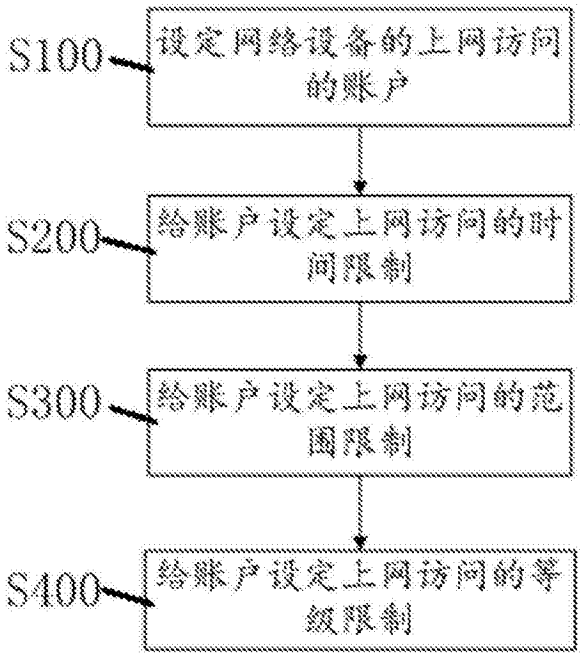

S100
设定网络设备的上网访问的账户
S200
给账户设定上网访问的时间限制
S300
给账户设定上网访问的范围限制
S400
给账户设定上网访问的等级限制

图1

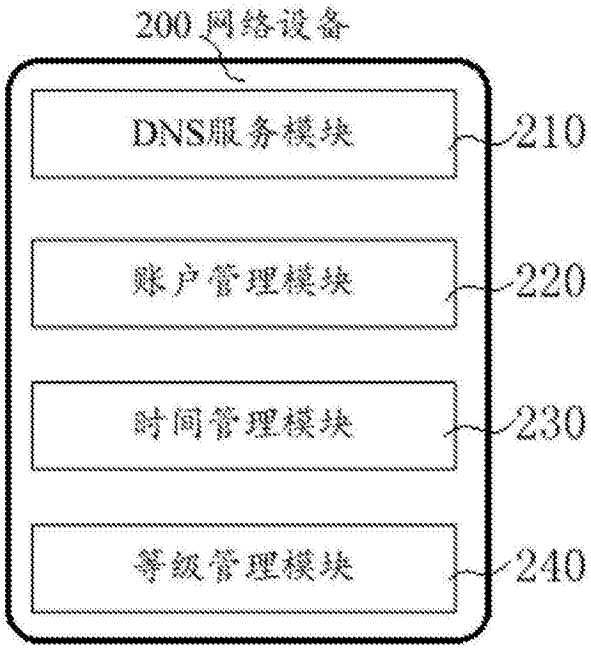

200 网络设备
DNS服务模块
210
账户管理模块
220
时间管理模块
230
等级管理模块
240

图2

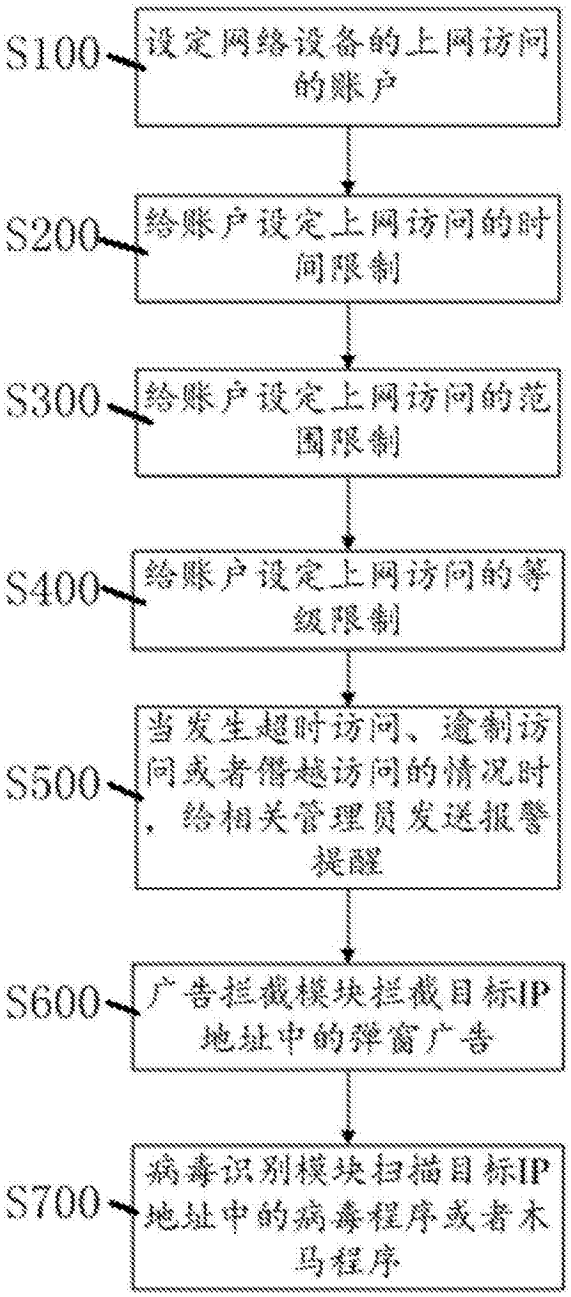

S100
设定网络设备的上网访问的账户
S200
给账户设定上网访问的时间限制
S300
给账户设定上网访问的范围限制
S400
给账户设定上网访问的等级限制
S500
当发生超时访问、违制访问或者僭越访问的情况时，给相关管理员发送报警提醒
S600
广告拦截模块拦截目标IP地址中的弹窗广告
S700
病毒识别模块扫描目标IP地址中的病毒程序或者木马程序

图3

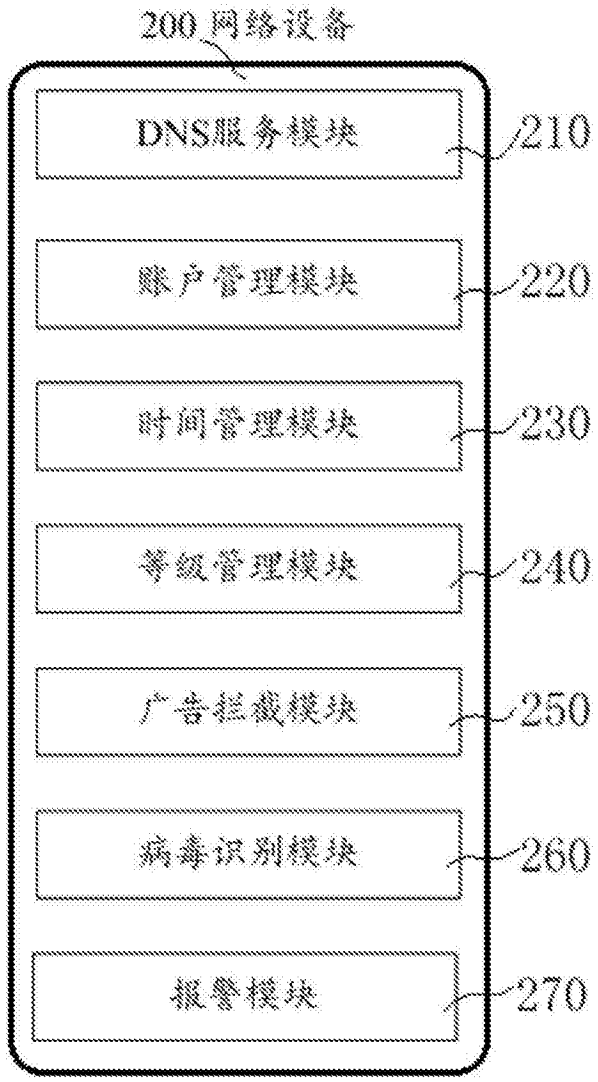

200 网络设备
DNS服务模块
210
账户管理模块
220
时间管理模块
230
等级管理模块
240
广告拦截模块
250
病毒识别模块
260
报警模块
270

图4

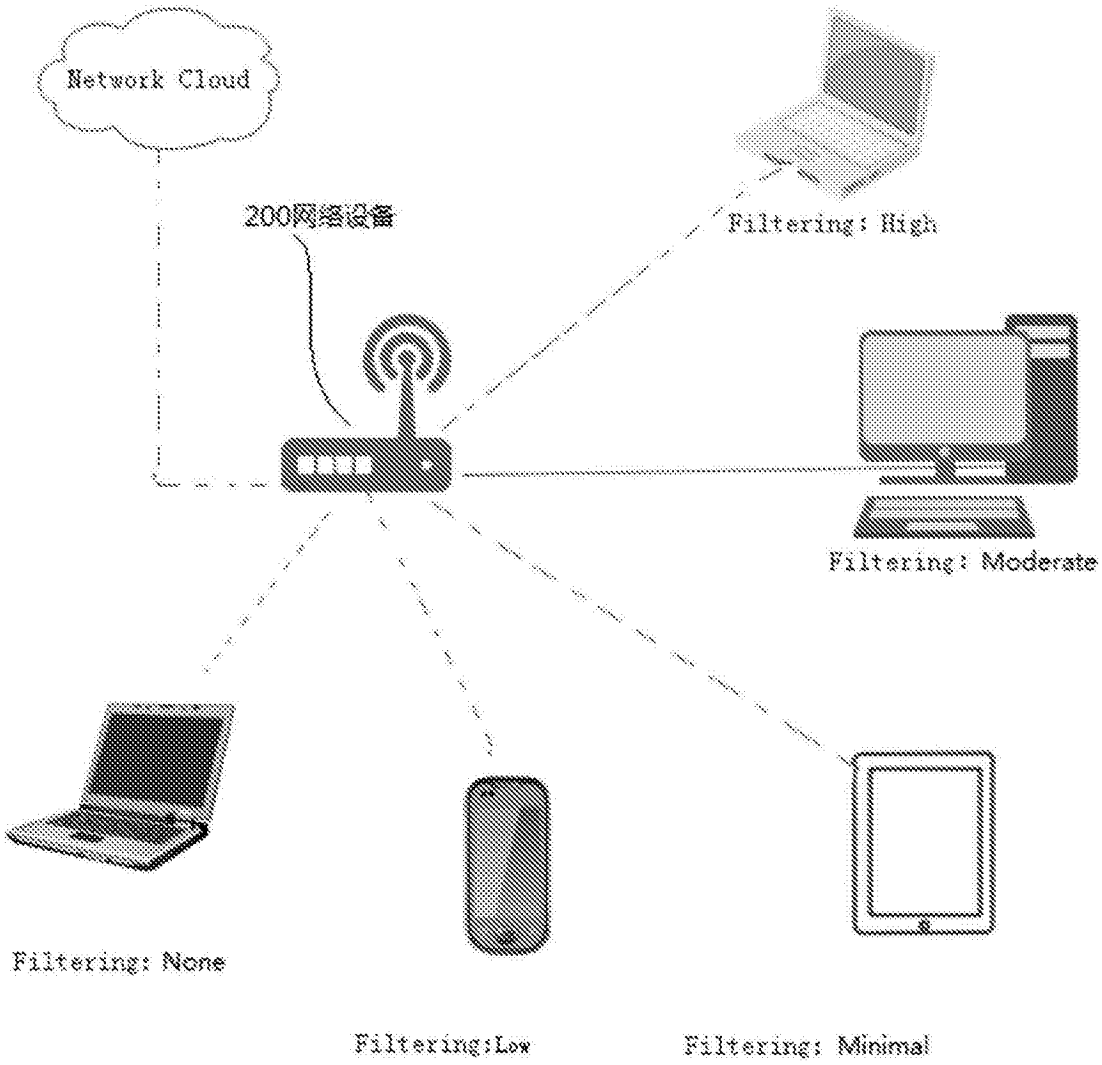

Network Cloud
200网络设备
Filtering: High
Filtering: Moderate
Filtering: None
Filtering:Low
Filtering: Minimal

图5