(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 105516981 A
(43)申请公布日 2016.04.20

(21)申请号 201510960146.5

(22)申请日 2015.12.21

(71)申请人 深圳维盟科技有限公司
地址 广东省深圳市龙华新区龙华街道油松商务大厦1801－1805（办公场所）

(72)发明人 蹇浩林 符常勇

(74)专利代理机构 北京风雅颂专利代理有限公司 11403
代理人 陈宙 于晓霞

(51)Int.Cl.
H04W 12/06(2009.01)
H04L 29/06(2006.01)

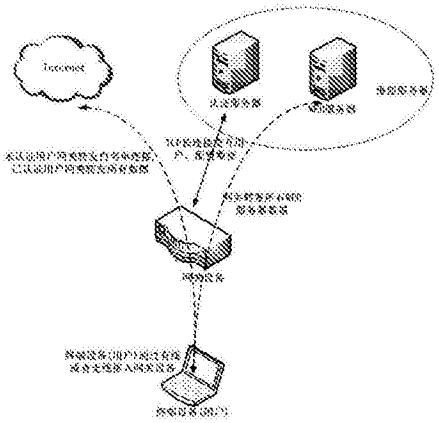
权利要求书1页 说明书3页 附图2页

(54)发明名称

智慧WiFi认证系统

(57)摘要

本发明公开了一种智慧WiFi认证系统，包括网关设备、认证服务器和WEB服务器；所述网关设备为终端用户提供网络接入入口；所述认证服务器对网关设备提交过来的终端用户身份进行认证处理；所述WEB服务器为用户提供认证页面支持。本发明的认证方法通过强制portal认证技术，验证用户身份信息后，开通其访问网络权限的一种业务技术。该技术通过在网关设备处对用户的网络访问连接信息进行拦截跳转到指定认证页面后，验证用户身份信息。解决了传统的WEB认证技术认证页面只有简单的账号、密码输入框；用户存储只能在网关设备中，存储量不足；以及只有账号密码一种认证方式的不足之处。



CN 105516981 A

1.一种智慧WiFi认证系统,其特征在于:包括网关设备、认证服务器和WEB服务器;

所述网关设备为终端用户提供网络接入入口;

所述认证服务器对网关设备提交过来的终端用户身份进行认证处理;

所述WEB服务器为用户提供认证页面支持;

所述网关设备接入因特网后,与认证服务器建立TCP长连接;网关设备将连接网关的终端用户信息发送给认证服务器;认证服务器对终端用户进行认证处理后,回复网关设备用户控制状态和Portal地址,Portal地址指向WEB服务器;所述网关设备根据认证服务器回复的控制状态对用户进行管控。

2.根据权利要求1所述的一种智慧WiFi认证系统,其特征在于:所述系统对数据连接分类为:白名单、非白名单和DNS报文;其中,白名单:用户配置的域名、目的IP所属的链接;非白名单:非白名单的链接;DNS报文:路由器放行所有的DNS报文。

3.根据权利要求1所述的一种智慧WiFi认证系统,其特征在于:所述系统对用户控制状态的分类包括以下几种:

(1)Pass:放行所有数据连接,针对已通过认证或者在不需要认证的用户;

(2)Block:阻止所有数据连接,针对非白名单用户;

(3)Block&Redirect:放行所有白名单链接,阻止其它非HTTP协议连接,对HTTP协议进行重定向到Portal页面;

(4)Pass&Redirect:放行所有白名单链接,放行所有非白名单连接,对HTTP协议进行重定向到Portal页面。

4.根据权利要求1所述的一种智慧WiFi认证系统的认证方法,其特征在于:包括以下步骤:

(1)终端设备通过有线或无线的方式连接网关,或者到IP;

(2)网关设备将终端设备IP/MAC发送到认证服务器;

(3)认证服务器判断此终端设备的控制状态及Portal页面地址,并回复给网关设备;

(4)网关设备根据认证服务器返回的控制状态对终端设备进行控制,并保存Portal页面地址;

(5)用户打开浏览器,输入地址或点击链接产生HTTP连接;

(6)设备网关对此连接进行业务分析,判断是否为白名单连接,若非白名单连接则将此连接重定向到Portal页面地址,并在Portal页面地址后追加终端用户参数:IP/MAC/Device_SN。

(7)用户打开Portal页面完成认证流程,Portal页面由WEB服务器提供;

(8)WEB服务器通知认证服务器,认证服务器再通知网关设备放行此终端;

(9)网关设备放行此终端设备,控制状态Pass,完成整个认证过程。

智慧WiFi认证系统

技术领域

[0001] 本发明涉及网络认证技术，尤其涉及一种智慧WiFi认证系统。

背景技术

[0002] 传统的WEB认证技术的不足之处在于：认证页面只有简单的账号、密码输入框；用户存储只能在网关设备中，存储量不足；只有账号密码一种认证方式。为解决以上不足之处，将认证页面放在云端WEB服务器上，由数据库来保存用户信息和日志等，增加多种方认证方式。

发明内容

[0003] 本发明是为了解决上述不足，提供了一种智慧WiFi认证系统。

[0004] 本发明的上述目的通过以下的技术方案来实现：一种智慧WiFi认证系统，其特征在于：包括网关设备、认证服务器和WEB服务器；

[0005] 所述网关设备为终端用户提供网络接入入口；

[0006] 所述认证服务器对网关设备提交过来的终端用户身份进行认证处理；

[0007] 所述WEB服务器为用户提供认证页面支持；

[0008] 所述网关设备接入因特网后，与认证服务器建立TCP长连接；网关设备将连接网关的终端用户信息发送给认证服务器；认证服务器对终端用户进行认证处理(处理无需认证业务、白名单用户、非白名单用户等)后，回复网关设备用户控制状态和Portal地址，Portal地址指向WEB服务器；所述网关设备根据认证服务器回复的控制状态对用户进行管控。

[0009] 所述认证服务器同时也可以下发其它功能、参数控制，如：白名单，无线参数等。

[0010] 所述系统对数据连接分类为：白名单、非白名单和DNS报文。其中，白名单：用户配置的域名、目的IP所属的链接；非白名单：非白名单的链接；DNS报文：路由器放行所有的DNS报文。

[0011] 所述系统对用户控制状态的分类包括以下几种：

[0012] (1)Pass：放行所有数据连接，针对已通过认证或者在不需要认证的用户。

[0013] (2)Block：阻止所有数据连接，针对非白名单用户。

[0014] (3)Block&Redirect：放行所有白名单链接，阻止其它非HTTP协议连接，对HTTP协议进行重定向到Portal页面。

[0015] (4)Pass&Redirect：放行所有白名单链接，放行所有非白名单连接，对HTTP协议进行重定向到Portal页面。

[0016] 一种智慧WiFi认证系统的认证方法，其特征在于：包括以下步骤：

[0017] (1)终端设备通过有线或无线的方式连接网关，或者到IP；

[0018] (2)网关设备将终端设备IP/MAC发送到认证服务器；

[0019] (3)认证服务器判断此终端设备的控制状态及Portal页面地址，并回复给网关设备；

[0020] (4)网关设备根据认证服务器返回的控制状态对终端设备进行控制，并保存Portal页面地址；

[0021] (5)用户打开浏览器，输入地址或点击链接产生HTTP连接；

[0022] (6)设备网关对此连接进行业务分析，判断是否为白名单连接，若非白名单连接则将此连接重定向到Portal页面地址，并在Portal页面地址后追加终端用户参数：IP/MAC/Device_SN(网终设备唯一序列号)。

[0023] (7)用户打开Portal页面完成认证流程，Portal页面由WEB服务器提供；

[0024] (8)WEB服务器通知认证服务器，认证服务器再通知网关设备放行此终端；

[0025] (9)网关设备放行此终端设备，控制状态Pass，完成整个认证过程。

[0026] 本发明是利用HTTP协议返回状态“302”(定向连接)来实现强制用户进行身份验证上网。

[0027] 本发明不单用于常见的Portal WEB认证，还可用于目前流行的第三方认证，如微信认证、QQ认证、新浪微博认证等。

[0028] 由于Portal认证页面或者第三方认证页面的目的地址(服务器)都是在外网，用户在认证前都需要访问这些页面，并且认证页面上的某些元素可能会在其它地址的服务器上。所以本发明增加了域名、目的IP白名单功能，将Portal页面地址所在域名以及第三方认证资源相关域名或用户自定义域名全部放入到白名单中。网关设备会对目的IP属于白名单内的连接进行直接转发放行，这样用户在登录之前只能访问白名单中的目标地址。而且为了加快域名解析速度，本发明将所有域名解析到的IP地址全部缓存起来，以便下次有相同域名解析报文请求时，直接由网关设备回复，无需再到外网域名服务器处解析。

[0029] Portal认证页面的内容全部放在云端的服务器中，这样可以在portal页面中放入更加生动美丽的内容，甚至可以放入富媒体内容。

[0030] 网关设备对用户的状态操作，只负责上报终端用户的上下线状态及接收和处理服务器下发的指令。所有耗时、消耗资源的操作全都由认证服务器处理，这样可以最大限度的减少网关设备的处理压力，提升网关设备的数据处理能力和终端上网体验满意度。

[0031] 网关设备不存储任何用户信息，所有用户信息均存放在服务器数据库中，这样就完全取消了网关设备对用户存储所造成的存储开销。

[0032] 本发明与现有技术相比的优点是：本发明通过强制portal认证技术，验证用户身份信息后，开通其访问网络权限的一种业务技术。该技术通过在网关设备处对用户的网络访问连接信息进行拦截跳转到指定认证页面后，验证用户身份信息。解决了传统的WEB认证技术认证页面只有简单的账号、密码输入框；用户存储只能在网关设备中，存储量不足；以及只有账号密码一种认证方式的不足之处。

附图说明

[0033] 图1是本发明的系统结构示意图。

[0034] 图2是本发明的认证流程示意图。

具体实施方式

[0035] 下面结合附图对本发明进一步详述。

[0036] 如图1所示，一种智慧WiFi认证系统，包括网关设备、认证服务器和WEB服务器；

[0037] 所述网关设备为终端用户提供网络接入入口；

[0038] 所述认证服务器对网关设备提交过来的终端用户身份进行认证处理；

[0039] 所述WEB服务器为用户提供认证页面支持；

[0040] 所述网关设备接入因特网后，与认证服务器建立TCP长连接；网关设备将连接网关的终端用户信息发送给认证服务器；认证服务器对终端用户进行认证处理(处理无需认证业务、白名单用户、非白名单用户等)后，回复网关设备用户控制状态和Portal地址，Portal地址指向WEB服务器；所述网关设备根据认证服务器回复的控制状态对用户进行管控。

[0041] 所述认证服务器同时也可以下发其它功能、参数控制，如：白名单，无线参数等。

[0042] 所述系统对数据连接分类为：白名单、非白名单和DNS报文；其中，白名单：用户配置的域名、目的IP所属的链接；非白名单：非白名单的链接；DNS报文：路由器放行所有的DNS报文。

[0043] 所述系统对用户控制状态的分类包括以下几种：

[0044] (1)Pass：放行所有数据连接，针对已通过认证或者在不需要认证的用户。

[0045] (2)Block：阻止所有数据连接，针对非白名单用户。

[0046] (3)Block&Redirect：放行所有白名单链接，阻止其它非HTTP协议连接，对HTTP协议进行重定向到Portal页面。

[0047] (4)Pass&Redirect：放行所有白名单链接，放行所有非白名单连接，对HTTP协议进行重定向到Portal页面。

[0048] 如图2所示，一种智慧WiFi认证系统，包括以下步骤：

[0049] (1)终端设备通过有线或无线的方式连接网关，或者到IP；

[0050] (2)网关设备将终端设备IP/MAC发送到认证服务器；

[0051] (3)认证服务器判断此终端设备的控制状态及Portal页面地址，并回复给网关设备；

[0052] (4)网关设备根据认证服务器返回的控制状态对终端设备进行控制，并保存Portal页面地址；

[0053] (5)用户打开浏览器，输入地址或点击链接产生HTTP连接；

[0054] (6)设备网关对此连接进行业务分析，判断是否为白名单连接，若非白名单连接则将此连接重定向到Portal页面地址，并在Portal页面地址后追加终端用户参数：IP/MAC/Device_SN(网终设备唯一序列号)。

[0055] (7)用户打开Portal页面完成认证流程，Portal页面由WEB服务器提供；

[0056] (8)WEB服务器通知认证服务器，认证服务器再通知网关设备放行此终端；

[0057] (9)网关设备放行此终端设备，控制状态Pass，完成整个认证过程。

[0058] 以上所述仅为本发明的实施例，并非因此限制本发明的专利范围，凡是利用本发明说明书及实施例内容所作的等效结构或等效流程变换，或直接或间接运用在其他相关的技术领域，均同理包括在本发明的专利保护范围内。

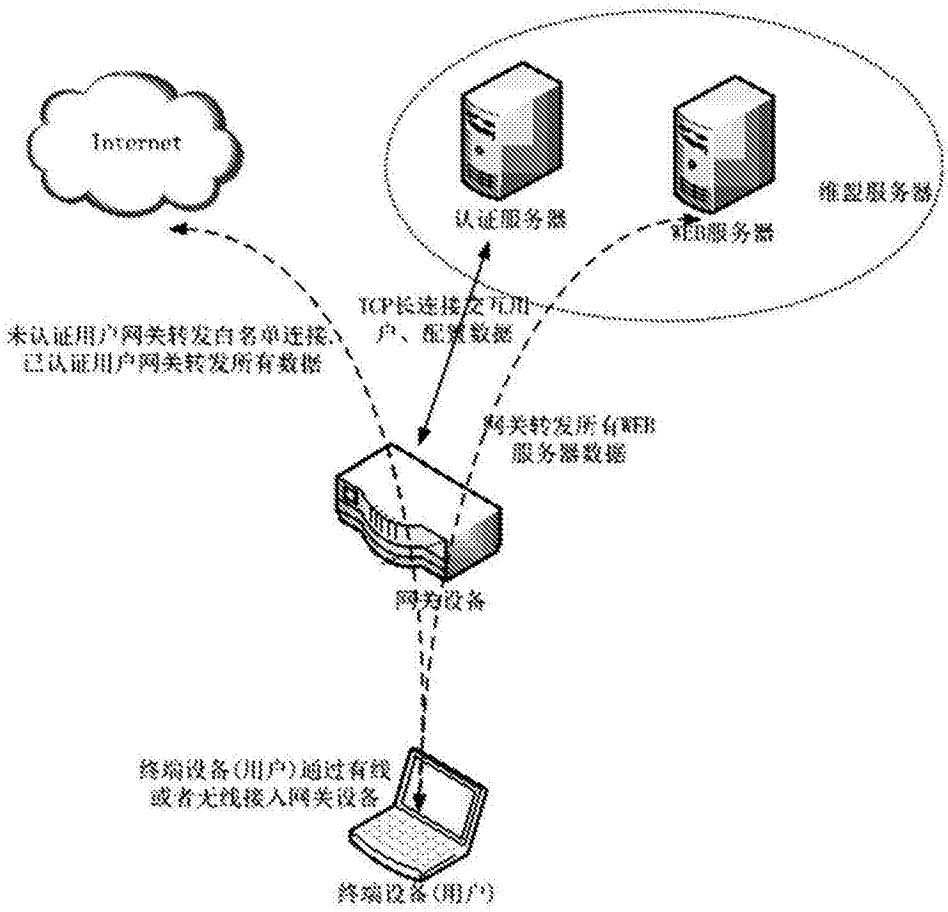

Internet
认证服务器
WEB服务器
维护服务器
TCP长连接交互用户、配置数据
未认证用户网关转发白名单连接、已认证用户网关转发所有数据
网关转发所有WEB服务器数据
网关设备
终端设备(用户)通过有线或者无线接入网关设备
终端设备(用户)

图1

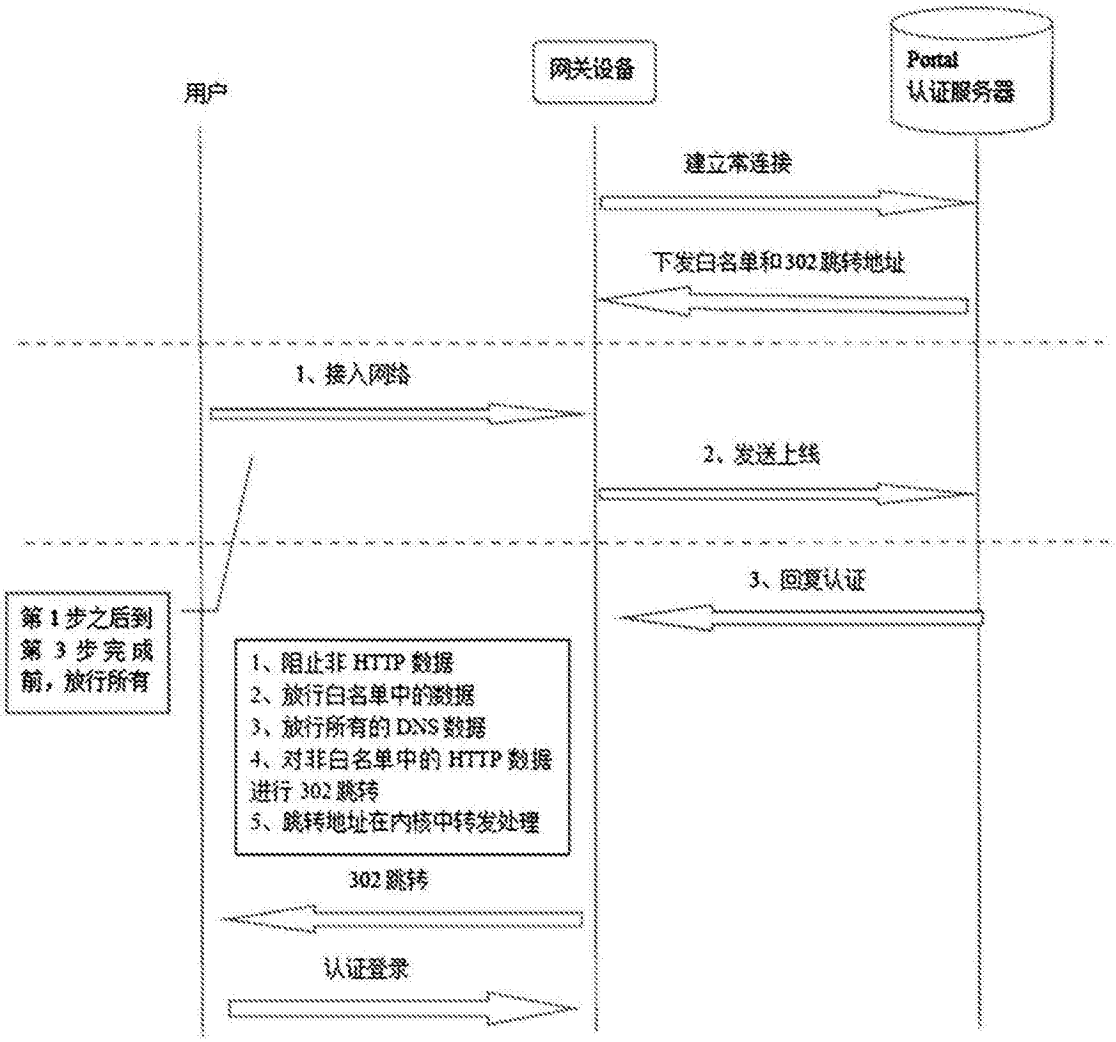

用户
网关设备
Portal
认证服务器
建立常连接
下发白名单和302跳转地址
1、接入网络
2、发送上线
3、回复认证
第1步之后到第3步完成前，放行所有
1、阻止非HTTP数据
2、放行白名单中的数据
3、放行所有的DNS数据
4、对非白名单中的HTTP数据进行302跳转
5、跳转地址在内核中转发处理
302跳转
认证登录

图2