(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 111447176 A
(43)申请公布日 2020.07.24

(21)申请号 202010119557.2

(22)申请日 2020.02.26

(71)申请人 中国平安人寿保险股份有限公司
地址 518000 广东省深圳市福田区益田路5033号平安金融中心14、15、16、37、41、44、45、46层

(72)发明人 马昱忻

(74)专利代理机构 深圳市世联合知识产权代理有限公司 44385
代理人 汪琳琳

(51)Int.Cl.
H04L 29/06(2006.01)
G06F 21/74(2013.01)

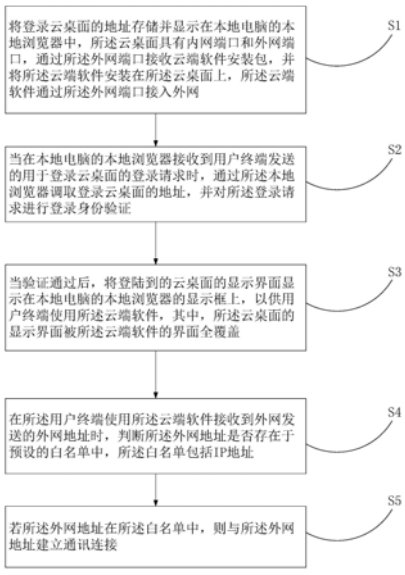
权利要求书3页 说明书11页 附图6页

(54)发明名称

内网安全访问外网的方法、装置、计算机设备及存储介质

(57)摘要

本申请属于信息安全技术领域，涉及一种内网安全访问外网的方法，包括：将登录云桌面的地址存储并显示在本地浏览器中，云桌面具有内、外网端口，通过外网端口接收云端软件安装包并安装，云端软件通过外网端口接入外网；当验证云桌面的登录身份通过后，将登陆到的云桌面的显示界面显示本地浏览器的显示框上，云桌面的显示界面被云端软件的界面全覆盖；在用户终端使用云端软件接收外网发送的外网地址时，判断外网地址是否存在于预设的白名单中；若外网地址在白名单中，与外网地址建立通讯连接。本申请还提供一种内网安全访问外网的装置、计算机设备及存储介质。本申请实现用户可以同时使用本地电脑和云桌面，有效隔离内外网，维护网络和信息安全。



CN 111447176 A

1.一种内网安全访问外网的方法,其特征在于,包括下述步骤:

将登录云桌面的地址存储并显示在本地电脑的本地浏览器中,所述云桌面具有内网端口和外网端口,通过所述外网端口接收云端软件安装包,并将所述云端软件安装在所述云桌面上,所述云端软件通过所述外网端口接入外网;

当在本地电脑的本地浏览器接收到用户终端发送的用于登录云桌面的登录请求时,通过所述本地浏览器调取登录云桌面的地址,并对所述登录请求进行登录身份验证;

当验证通过后,将登陆到的云桌面的显示界面显示在本地电脑的本地浏览器的显示框上,以供用户终端使用所述云端软件,其中,所述云桌面的显示界面被所述云端软件的界面全覆盖;

在所述用户终端使用所述云端软件接收到外网发送的外网地址时,判断所述外网地址是否存在于预设的白名单中,所述白名单包括IP地址;

若所述外网地址在所述白名单中,则与所述外网地址建立通讯连接。

2.根据权利要求1所述的内网安全访问外网的方法,其特征在于,所述对所述登录请求进行登录身份验证的步骤包括:

识别所述登录请求的网络来源;

若所述登录请求通过内网发送,则验证所述登录请求是否携带预设的登陆码;

若所述登录请求携带有登陆码,则确认所述登录请求的身份验证通过。

3.根据权利要求1所述的内网安全访问外网的方法,其特征在于,所述若所述外网地址在所述白名单中,则与所述外网地址建立通讯连接的步骤之后,还包括:

当接收到用户终端退出云端软件或关闭本地浏览器的指令时,同步停止对应所述云桌面的运行,关闭云桌面。

4.根据权利要求1至3任意一项所述的内网安全访问外网的方法,其特征在于,在所述若所述外网地址在所述白名单中,则与所述外网地址建立通讯连接的步骤之后,还包括:

根据所述白名单中的IP地址创建小程序,并将所创建的小程序与所述白名单中的IP地址进行关联;

将创建的小程序显示在所述云端软件中,以供用户终端访问对应IP地址。

5.根据权利要求4所述的内网安全访问外网的方法,其特征在于,所述白名单中的IP地址包括内网IP地址和外网IP地址;所述判断所述外网地址是否存在于预设的白名单中的步骤包括:

识别所述外网地址的IP地址;

若所述外网地址的IP地址在所述白名单的外网IP地址中,则确认所述外网地址在所述白名单中;

若所述外网地址的IP地址不存在于所述白名单中,则禁止与所述外网地址建立通讯连接;

所述在根据白名单中的IP地址创建小程序,并将所创建的小程序与所述白名单中的IP地址进行关联的步骤包括:

根据白名单中内网IP地址或外网IP地址创建小程序,并将所述创建的小程序与所述白名单中的内网IP地址或外网IP地址进行关联。

6.根据权利要求1所述的内网安全访问外网的方法,其特征在于,所述云端软件包括第

一软件、第二软件和第三软件;所述登录云桌面的地址包括第一地址、第二地址和第三地址;所述将登录云桌面的地址存储并显示在本地电脑的本地浏览器中,所述云桌面具有内网端口和外网端口,通过所述外网端口接收云端软件安装包,并将所述云端软件安装在所述云桌面上,所述云端软件通过所述外网端口接入外网的步骤,包括:

将登录云桌面的所述第一地址、第二地址和第三地址均存储并显示在本地电脑的本地浏览器中,所述云桌面具有内网端口和外网端口,通过所述外网端口接收第一软件的安装包、第二软件的安装包或第三软件的安装包,并将所述第一软件、第二软件或第三软件安装在所述云桌面上,其中,所述第一软件和所述第二软件为需要外网服务的软件,所述第三软件为不具有与外网用户进行消息传输功能的软件,所述第一软件或第二软件通过所述外网端口接入外网;

所述当在本地电脑的本地浏览器接收到用户终端发送的用于登录云桌面的登录请求时,通过所述本地浏览器调取登录云桌面的地址,并对所述登录请求进行登录身份验证的步骤包括:

当在本地电脑的本地浏览器接收到用户终端发送的用于登录云桌面的登录请求时,根据用户的选择,通过所述浏览器调取登录云桌面的第一地址、第二地址或第三地址,并对所述登录请求进行登录身份验证;

所述当验证通过后,将登陆到的云桌面的显示界面显示在本地电脑的本地浏览器的显示框上,以供用户终端使用所述云端软件,其中,所述云桌面的显示界面被所述云端软件的界面全覆盖的步骤包括:

当验证通过后,将登陆到的云桌面的显示界面显示在本地电脑的本地浏览器的显示框上,以供用户终端使用所述云端软件;

若所述用户通过所述第一地址登录云桌面,则所述云桌面的显示界面为所述第一软件所覆盖;或

若所述用户通过所述第二地址登录云桌面,则所述云桌面的显示界面为所述第二软件所覆盖;或

若所述用户通过第三地址登录云桌面,则所述云桌面的显示界面为第三软件所覆盖。

7.根据权利要求1所述的内网安全访问外网的方法,其特征在于,所述所述云桌面的显示界面被所述云端软件的界面全覆盖的步骤包括:

确定并存储所述云端软件的初始化尺寸;

根据所述云端软件的初始化尺寸,将云桌面的显示尺寸适配为所述云端软件的显示尺寸。

8.一种内网安全访问外网的装置,其特征在于,包括:

装载模块,用于将登录云桌面的地址存储并显示在本地电脑的本地浏览器中,所述云桌面具有内网端口和外网端口,通过所述外网端口接收云端软件安装包,并将所述云端软件安装在所述云桌面上,所述云端软件通过所述外网端口接入外网;

验证模块,用于当在本地电脑的本地浏览器接收到用户终端发送的用于登录云桌面的登录请求时,通过所述本地浏览器调取登录云桌面的地址,并对所述登录请求进行登录身份验证;

显示模块,用于当验证通过后,将登陆到的云桌面的显示界面显示在本地电脑的本地

浏览器的显示框上，以供用户终端使用所述云端软件，其中，所述云桌面的显示界面被所述云端软件的界面全覆盖；以及

判断模块，用于在所述用户终端使用所述云端软件接收到外网发送的外网地址时，判断所述外网地址是否存在于预设的白名单中，所述白名单包括IP地址；

通讯模块，用于当所述外网地址在所述白名单中时，与所述外网地址建立通讯连接。

9.一种计算机设备，其特征在于，包括存储器和处理器，所述存储器中存储有计算机程序，所述处理器执行所述计算机程序时实现如权利要求1至7中任一项所述的内网安全访问外网的方法的步骤。

10.一种计算机可读存储介质，其特征在于，所述计算机可读存储介质上存储有计算机程序，所述计算机程序被处理器执行时实现如权利要求1至7中任一项所述的内网安全访问外网的方法的步骤。

内网安全访问外网的方法、装置、计算机设备及存储介质

技术领域

[0001] 本申请涉及信息安全技术领域，尤其涉及一种内网安全访问外网的方法、装置、计算机设备及存储介质。

背景技术

[0002] 随着移动互联网的广度和深度不断发展，移动互联作为沟通渠道的作用也愈发凸显。随着科技的进步与发展，云桌面应运而生，云桌面可以把数据空间、管理服务，提供桌面化的方式发布给操作者，将传统PC升级为网络操作。基于数据空间的云桌面，主要通过虚拟化应用，将云端资源发布给各操作终端，仍属于数据平台云操作系统。

[0003] 然而，云桌面连接外网，且安装多种软件，不利于管理和控制；且云桌面覆盖PC桌面，用户无法实现同时使用本地电脑和云桌面，同时直接通过软件与外网用户交流时，存在无法有效隔离内外网，不能有效维护网络和信息安全的问题。

发明内容

[0004] 本申请实施例的目的在于提出一种内网安全访问外网的方法、装置、计算机设备及存储介质，实现用户可以同时使用本地电脑和云桌面，有效隔离内外网，维护网络和信息安全。

[0005] 为了解决上述技术问题，本申请实施例提供一种内网安全访问外网的方法，采用了如下所述的技术方案：

[0006] 一种内网安全访问外网的方法，包括下述步骤：

[0007] 将登录云桌面的地址存储并显示在本地电脑的本地浏览器中，所述云桌面具有内网端口和外网端口，通过所述外网端口接收云端软件安装包，并将所述云端软件安装在所述云桌面上，所述云端软件通过所述外网端口接入外网；

[0008] 当在本地电脑的本地浏览器接收到用户终端发送的用于登录云桌面的登录请求时，通过所述本地浏览器调取登录云桌面的地址，并对所述登录请求进行登录身份验证；

[0009] 当验证通过后，将登陆到的云桌面的显示界面显示在本地电脑的本地浏览器的显示框上，以供用户终端使用所述云端软件，其中，所述云桌面的显示界面被所述云端软件的界面全覆盖；

[0010] 在所述用户终端使用所述云端软件接收到外网发送的外网地址时，判断所述外网地址是否存在于预设的白名单中，所述白名单包括IP地址；

[0011] 若所述外网地址在所述白名单中，则与所述外网地址建立通讯连接。

[0012] 进一步的，所述对所述登录请求进行登录身份验证的步骤包括：

[0013] 识别所述登录请求的网络来源；

[0014] 若所述登录请求通过内网发送，则验证所述登录请求是否携带预设的登陆码；

[0015] 若所述登录请求携带有登陆码，则确认所述登录请求的身份验证通过。

[0016] 进一步的，所述若所述外网地址在所述白名单中，则与所述外网地址建立通讯连

接的步骤之后，还包括：

[0017] 当接收到用户终端退出云端软件或关闭本地浏览器的指令时，同步停止对应所述云桌面的运行，关闭云桌面。

[0018] 进一步的，在所述若所述外网地址在所述白名单中，则与所述外网地址建立通讯连接的步骤之后，还包括：

[0019] 根据白名单中的IP地址创建小程序，并将所创建的小程序与所述白名单中的IP地址进行关联；

[0020] 将创建的小程序显示在所述云端软件中，以供用户终端访问对应IP地址。

[0021] 进一步的，所述白名单中的IP地址包括内网IP地址和外网IP地址；所述判断所述外网地址是否存在于预设的白名单中的步骤包括：

[0022] 识别所述外网地址的IP地址；

[0023] 若所述外网地址的IP地址在所述白名单的外网IP地址中，则确认所述外网地址在所述白名单中；

[0024] 若所述外网地址的IP地址不存在于所述白名单中，则禁止与所述外网地址建立通讯连接；

[0025] 所述在根据白名单中的IP地址创建小程序，并将所创建的小程序与所述白名单中的IP地址进行关联的步骤包括：

[0026] 根据白名单中内网IP地址或外网IP地址创建小程序，并将所述创建的小程序与所述白名单中的内网IP地址或外网IP地址进行关联。

[0027] 进一步的，所述云端软件包括第一软件、第二软件和第三软件；所述登录云桌面的地址包括第一地址、第二地址和第三地址；所述将登录云桌面的地址存储并显示在本地电脑的本地浏览器中，所述云桌面具有内网端口和外网端口，通过所述外网端口接收云端软件安装包，并将所述云端软件安装在所述云桌面上，所述云端软件通过所述外网端口接入外网的步骤包括：

[0028] 将登录云桌面的所述第一地址、第二地址和第三地址均存储并显示在本地电脑的本地浏览器中，所述云桌面具有内网端口和外网端口，通过所述外网端口接收第一软件的安装包、第二软件的安装包或第三软件的安装包，并将所述第一软件、第二软件或第三软件安装在所述云桌面上，其中，所述第一软件和所述第二软件为需要外网服务的软件，所述第三软件为不具有与外网用户进行消息传输功能的软件，所述第一软件或第二软件通过所述外网端口接入外网；

[0029] 所述当在本地电脑的本地浏览器接收到用户终端发送的用于登录云桌面的登录请求时，通过所述本地浏览器调取登录云桌面的地址，并对所述登录请求进行登录身份验证的步骤包括：

[0030] 当在本地电脑的本地浏览器接收到用户终端发送的用于登录云桌面的登录请求时，根据用户的选择，通过所述浏览器调取登录云桌面的第一地址、第二地址或第三地址，并对所述登录请求进行登录身份验证；

[0031] 所述当验证通过后，将登陆到的云桌面的显示界面显示在本地电脑的本地浏览器的显示框上，以供用户终端使用所述云端软件，其中，所述云桌面的显示界面被所述云端软件的界面全覆盖的步骤包括：

[0032] 当验证通过后,将登陆到的云桌面的显示界面显示在本地电脑的本地浏览器的显示框上,以供用户终端使用所述云端软件;

[0033] 若所述用户通过所述第一地址登录云桌面,则所述云桌面的显示界面为所述第一软件所覆盖;或

[0034] 若所述用户通过所述第二地址登录云桌面,则所述云桌面的显示界面为所述第二软件所覆盖;或

[0035] 若所述用户通过第三地址登录云桌面,则所述云桌面的显示界面为第三软件所覆盖。

[0036] 进一步的,所述所述云桌面的显示界面被所述云端软件的界面全覆盖的步骤包括:

[0037] 确定并存储所述云端软件的初始化尺寸;

[0038] 根据所述云端软件的初始化尺寸,将云桌面的显示尺寸适配为所述云端软件的显示尺寸。

[0039] 为了解决上述技术问题,本申请实施例还提供一种内网安全访问外网的装置,采用了如下所述的技术方案:

[0040] 一种内网安全访问外网的装置,包括:

[0041] 装载模块,用于将登录云桌面的地址存储并显示在本地电脑的本地浏览器中,所述云桌面具有内网端口和外网端口,通过所述外网端口接收云端软件安装包,并将所述云端软件安装在所述云桌面上,所述云端软件通过所述外网端口接入外网;

[0042] 验证模块,用于当在本地电脑的本地浏览器接收到用户终端发送的用于登录云桌面的登录请求时,通过所述本地浏览器调取登录云桌面的地址,并对所述登录请求进行登录身份验证;

[0043] 显示模块,用于当验证通过后,将登陆到的云桌面的显示界面显示在本地电脑的本地浏览器的显示框上,以供用户终端使用所述云端软件,其中,所述云桌面的显示界面被所述云端软件的界面全覆盖;以及

[0044] 判断模块,用于在所述用户终端使用所述云端软件接收到外网发送的外网地址时,判断所述外网地址是否存在于预设的白名单中,所述白名单包括IP地址;

[0045] 通讯模块,用于当所述外网地址在所述白名单中时,与所述外网地址建立通讯连接。

[0046] 为了解决上述技术问题,本申请实施例还提供一种计算机设备,采用了如下所述的技术方案:

[0047] 一种计算机设备,包括存储器和处理器,所述存储器中存储有计算机程序,所述处理器执行所述计算机程序时实现上述的内网安全访问外网的方法的步骤。

[0048] 为了解决上述技术问题,本申请实施例还提供一种计算机可读存储介质,采用了如下所述的技术方案:

[0049] 一种计算机可读存储介质,所述计算机可读存储介质上存储有计算机程序,所述计算机程序被处理器执行时实现上述的内网安全访问外网的方法的步骤。

[0050] 与现有技术相比,本申请实施例主要有以下有益效果:用户可以通过本地浏览器存储的登录云桌面的地址登录云桌面,实现可以同时使用本地电脑与云桌面,且,本申请将

云端软件安装在同时连接内外网的云桌面上，所述云桌面的显示界面为所述云端软件的界面所覆盖，通过设置白名单，从而限制用户对IP地址的访问；并将允许访问的IP地址以小程序的方式在云端软件中提供，以此来保障内网与外围安全机制的维持；且对云端软件的更新升级都可以在云端进行，有效的统一管理升级的问题，避免了用户本地硬件和环境差异带来的本地升级的多样性和复杂性。

附图说明

[0051] 为了更清楚地说明本申请中的方案，下面将对本申请实施例描述中所需要使用的附图作一个简单介绍，显而易见地，下面描述中的附图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。

[0052] 图1是本申请可以应用于其中的示例性系统架构图；

[0053] 图2是根据本申请的内网安全访问外网的方法的一个实施例的流程图；

[0054] 图3是根据本申请的内网安全访问外网的方法的另一实施例的流程图；

[0055] 图4是根据本申请的内网安全访问外网的方法的另一实施例的流程图；

[0056] 图5是根据本申请的内网安全访问外网的装置的一个实施例的结构示意图；

[0057] 图6是根据本申请的计算机设备的一个实施例的结构示意图。

[0058] 附图标记：200、计算机设备；201、存储器；202、处理器；203、网络接口；300、内网安全访问外网的装置；301、装载模块；302、验证模块；303、显示模块；304、判断模块；305、通讯模块。

具体实施方式

[0059] 除非另有定义，本文所使用的所有的技术和科学术语与属于本申请的技术领域的技术人员通常理解的含义相同；本文中在申请的说明书中所使用的术语只是为了描述具体的实施例的目的，不是旨在于限制本申请；本申请的说明书和权利要求书及上述附图说明中的术语“包括”和“具有”以及它们的任何变形，意图在于覆盖不排他的包含。本申请的说明书和权利要求书或上述附图中的术语“第一”、“第二”等是用于区别不同对象，而不是用于描述特定顺序。

[0060] 在本文中提及“实施例”意味着，结合实施例描述的特定特征、结构或特性可以包含在本申请的至少一个实施例中。在说明书中的各个位置出现该短语并不一定均是指相同的实施例，也不是与其它实施例互斥的独立的或备选的实施例。本领域技术人员显式地和隐式地理解的是，本文所描述的实施例可以与其它实施例相结合。

[0061] 为了使本技术领域的人员更好地理解本申请方案，下面将结合附图，对本申请实施例中的技术方案进行清楚、完整地描述。

[0062] 如图1所示，系统架构100可以包括终端设备101、102、103，网络104和服务器105。网络104用以在终端设备101、102、103和服务器105之间提供通信链路的介质。网络104可以包括各种连接类型，例如有线、无线通信链路或者光纤电缆等等。

[0063] 用户可以使用终端设备101、102、103通过网络104与服务器105交互，以接收或发送消息等。终端设备101、102、103上可以安装有各种通讯客户端应用，例如网页浏览器应用、购物类应用、搜索类应用、即时通信工具、邮箱客户端、社交平台软件等。

[0064] 终端设备101、102、103可以是具有显示屏并且支持网页浏览的各种电子设备，包括但不限于智能手机、平板电脑、电子书阅读器、MP3播放器(Moving Picture Experts Group Audio Layer III，动态影像专家压缩标准音频层面3)、MP4(Moving Picture Experts Group Audio Layer IV，动态影像专家压缩标准音频层面4)播放器、膝上型便携计算机和台式计算机等等。

[0065] 服务器105可以是提供各种服务的服务器，例如对终端设备101、102、103上显示的页面提供支持的后台服务器。

[0066] 需要说明的是，本申请实施例所提供的内网安全访问外网的方法一般由服务器/终端设备执行，相应地，内网安全访问外网的装置一般设置于服务器/终端设备中。

[0067] 应该理解，图1中的终端设备、网络和服务器的数目仅仅是示意性的。根据实现需要，可以具有任意数目的终端设备、网络和服务器。

[0068] 继续参考图2，示出了根据本申请的内网安全访问外网的方法的一个实施例的流程图。所述的内网安全访问外网的方法，包括以下步骤：

[0069] S1：将登录云桌面的地址存储并显示在本地电脑的本地浏览器中，所述云桌面具有内网端口和外网端口，通过所述外网端口接收云端软件安装包，并将所述云端软件安装在所述云桌面上，所述云端软件通过所述外网端口接入外网。

[0070] 在本实施例中，本地电脑全部接入内网，通过将本地浏览器与登录云桌面的地址相关联，使得用户既可以使用接入内网的本地电脑进行工作、学习和娱乐，又可以通过登录云桌面使用云桌面上安装的云端软件进行工作、学习和娱乐；在用户登录云桌面后，用户相当于拥有两台电脑：本地电脑和远程的云桌面；所述本地浏览器用于通过云桌面的内网端口接入云桌面；通过本地浏览器远程接入云桌面，再通过云桌面的外网端口访问外网，保证内外网安全的同时，提供了可以外网访问的云端软件供内网用户使用。

[0071] 进一步的，当检测到云端软件存在更新包时，下载所述更新包，统一更新所述云端软件。

[0072] 对云端软件的更新和升级在云端集中管理，避免了用户本地硬件和环境差异导致的问题，比如有的用户升级，有的用户没有升级，导致软件的安装版本不同；或者因为硬件和环境上的差异，导致某些插件未安装，以及安装速度不同等问题；统一管理客户端升级的问题，避免本地升级的多样性和带来的复杂性。

[0073] 例如：云端软件包括企业微信、CAD制图、Solidwork、Office等软件，当这些软件安装在本地时，会产生许多的问题，包括每一个用户的安装版本不同，即点即用版或者专业版，导致将文件发送给其他版本不同的用户时，对方因为版本过低等原因无法打开文件；或者本地用户安装了专业版的Office，因为程序无法并行的问题，就无法再安装即点即用版的Visio，对于那些对互联网知之甚少的使用者来说，造成了极大的不便；本申请将软件安装在云桌面，升级和安装都在云桌面进行控制，保证了软件的一致性，且可以通过接收正版的云端软件，控制每一个云桌面的云端软件都是统一版本，解决了本地用户安装软件不兼容的不便。

[0074] S2：当在本地电脑的本地浏览器接收到用户终端发送的用于登录云桌面的登录请求时，通过所述本地浏览器调取登录云桌面的地址，并对所述登录请求进行登录身份验证。预先验证登录的用户的身份，以保护信息的安全性。

[0075] 具体的，在步骤S2中，即所述所述登录请求进行登录身份验证的步骤包括：

[0076] 识别所述登录请求的网络来源；

[0077] 若所述登录请求通过内网发送，则验证所述登录请求是否携带预设的登陆码；

[0078] 若所述登录请求携带有登陆码，则确认所述登录请求的身份验证通过。

[0079] 在本实施例中，当在本地浏览器接收到用户终端发送的用于登录云桌面的登录请求时，通过所述本地浏览器调取登录云桌面的地址，并验证所述登录请求的网络来源以及是否携带有登录码。在本申请中，用户需要在内网用登陆码(UM)才能够登录云桌面，进而才能够使用云端软件客户端。登录码为预设的可登录码，由用户的名字拼音加数字组成，预先存储在数据库中；若登录请求携带登陆码，验证登陆码是否与数据库中存储的登陆码一致，若一致，认为登陆码具有登录权限，确定验证通过。限制用户仅能通过内网登录云桌面，以确保是内网用户在公司登录使用云桌面；每位用户都有自己的登陆码，通过登陆码可以确定登录云桌面的用户，同时保障云桌面的信息安全确保网路安全。

[0080] 其中，若所述登录请求通过内网发送，但未携带预设的登录码，则拒绝登录；若所述登录请求通过外网发送，则直接拒绝登录，不需要验证是否携带有登陆码。其中，内网和外网通过IP地址进行分辨和确认。

[0081] 在本实施例中，若登录请求的网络来源为外网，那么认为是不安全网络，直接拒绝登录。若登录请求的网络来源为内网，但未携带登录码，无法验证登陆者身份，也不具有登录权限，拒绝登录。

[0082] S3：当验证通过后，将登陆到的云桌面的显示界面显示在本地电脑的本地浏览器的显示框上，以供用户终端使用所述云端软件，其中，所述云桌面的显示界面被所述云端软件的界面全覆盖。

[0083] 本申请的全覆盖指云端软件的界面完全覆盖住云桌面的显示界面；换而言之，云桌面的显示界面即为云端软件的界面，全覆盖的实现方便用户使用可以提供的最大窗口，提高用户体验，同时防止用户在云桌面上，但是是该云端软件以外的位置进行其他操作。

[0084] 具体的，在步骤S3中，即所述所述云桌面的显示界面被所述云端软件的界面全覆盖的步骤包括：

[0085] 确定并存储所述云端软件的初始化尺寸；

[0086] 根据所述云端软件的初始化尺寸，将云桌面的显示尺寸适配为所述云端软件的显示尺寸。

[0087] 在本实施例中，当验证通过后，确定所述用户终端登录所述云桌面，允许所述用户终端通过本地浏览器登录所述云桌面，以使用所述云端软件；所述云桌面的显示界面为所述云端软件的界面所覆盖，则云桌面的显示界面与所述云端软件显示的界面相同；根据不同的云端软件的初始化大小，将云桌面的尺寸与所述云端软件适配，以使得所述云桌面的显示尺寸与所述云端软件的显示尺寸一致，保证云桌面的整体显示界面为所述云端软件的界面。用户通过用户终端登录云桌面，进而使用云端软件与外部沟通。所述云桌面只显示云端软件的界面，不显示其他界面，用户通过云桌面仅可以直接操作云端软件。

[0088] S4：在所述用户终端使用所述云端软件接收到外网发送的外网地址时，判断所述外网地址是否存在于预设的白名单中，所述白名单包括IP地址。通过判断外网地址是否存在于预设的白名单中，来确定是否与所述外网地址建立通讯连接，从而保证内网的安全。

[0089] S5:若所述外网地址在所述白名单中,则与所述外网地址建立通讯连接。

[0090] 进一步的,若所述外网地址的IP地址不存在于所述白名单中,则禁止与所述外网地址建立通讯连接。

[0091] 在本实施例中,在内网白名单上的IP地址,是同意访问的地址,以此来保障访问的地址的安全性,控制用户的行为,使得用户仅访问提供的IP地址。通过创建白名单的方式,来保证云桌面和本地电脑中的信息安全;防止有害数据入侵。相对于通过本地电脑来控制外网访问具有的复杂性,和本地环境带来的差异问题,及更新换代电脑时,需要重新在本地电脑部署内外网访问控制来说,本申请将白名单的控制设置在云桌面中,在更换本地电脑后,也无需重新部署内外网访问控制,节约了成本,节省了时间,提高了效率。

[0092] 其中,在步骤S5之后,在所述若所述外网地址在所述白名单中,则与所述外网地址建立通讯连接的步骤之后,还包括:

[0093] 根据所述白名单中的IP地址创建小程序,并将所创建的小程序与所述白名单中的IP地址进行关联;

[0094] 将创建的小程序显示在所述云端软件中,以供用户终端访问对应IP地址。

[0095] 具体的,所述白名单中的IP地址包括内网IP地址和外网IP地址;在步骤S4中,即所述判断所述外网地址是否存在于预设的白名单中的步骤包括:

[0096] 识别所述外网地址的IP地址;

[0097] 若所述外网地址的IP地址在所述白名单的外网IP地址中,则确认所述外网地址在所述白名单中;

[0098] 若所述外网地址的IP地址不存在于所述白名单中,则禁止与所述外网地址建立通讯连接;

[0099] 所述在根据白名单中的IP地址创建小程序,并将所创建的小程序与所述白名单中的IP地址进行关联的步骤包括:

[0100] 根据白名单中内网IP地址或外网IP地址创建小程序,并将所述创建的小程序与所述白名单中的内网IP地址或外网IP地址进行关联。

[0101] 在本实施例中,小程序与内网IP地址连接,则提供服务的一方来自内网;小程序与外网IP地址连接,则提供服务的一方来自外网。比如:提供翻译服务,当小程序与提供翻译服务的内网IP地址连接,则确认提供翻译服务的一方来自内网,这个翻译服务可以是内网用户自己开发的,可以个性化定制,在翻译服务中提供内网用户常用的技术术语或者惯用交流词汇;当小程序与提供翻译服务的内网IP地址连接,则确认提供翻译服务的一方来自外网,翻译的词汇更加全面和多样化;每一个小程序可以都与外网IP地址连接,每一个小程序也可以分别与内网IP地址和外网IP地址连接,在实际应用中,可以根据实际情况进行多样化选择。

[0102] 当然,本申请还可以将用户访问的所述IP地址进行记录存储。在本实施例中,记录用户的访问历史并存储,以便后续对用户的访问记录合规质检。

[0103] 图3是根据本申请的内网安全访问外网的装置方法的另一实施例的流程图;如图3所示,在本申请的实施例的一些可选的实现方式中,在步骤S5之后,即所述若所述外网地址在所述白名单中,则与所述外网地址建立通讯连接的步骤之后;上述电子设备还可以执行以下步骤:

[0104] S6:当接收到用户终端退出云端软件或关闭本地浏览器的指令时,同步停止对应所述云桌面的运行,关闭云桌面。

[0105] 在本实施例中,云桌面的生命周期与云端软件保持一致。一旦关闭、退出或卸载云端软件,同步退出云桌面的登录,关闭云桌面;云桌面为内网用户提供了外网访问的渠道,内网用户通过云桌面上的云端软件实现外网访问,当用户关闭云端软件,则同时关闭云桌面,停止提供外网访问渠道,以保证内网的安全。

[0106] S7:当接收到用户终端最小化本地浏览器的指令时,在本地电脑上显示本地界面,提供本地软件供用户使用。在本申请中,用户可以灵活选择使用云桌面的软件或者本地软件。

[0107] 图4是根据本申请的内网安全访问外网的装置方法的另一实施例的流程图;如图4所示,在本申请的一些可选的实现方式中,所述云端软件包括第一软件、第二软件和第三软件;所述登录云桌面的地址包括第一地址、第二地址和第三地址;在所述步骤S1中,即将登录云桌面的地址存储并显示在本地电脑的本地浏览器中,所述云桌面具有内网端口和外网端口,通过所述外网端口接收云端软件安装包,并将所述云端软件安装在所述云桌面上,所述云端软件通过所述外网端口接入外网的步骤,包括:

[0108] S11:将登录云桌面的所述第一地址、第二地址和第三地址均存储并显示在本地电脑的本地浏览器中,所述云桌面具有内网端口和外网端口,通过所述外网端口接收第一软件的安装包、第二软件的安装包或第三软件的安装包,并将所述第一软件、第二软件或第三软件安装在所述云桌面上,其中,所述第一软件和所述第二软件为需要外网服务的软件,所述第三软件为不具有与外网用户进行消息传输功能的软件,所述第一软件或第二软件通过所述外网端口接入外网;

[0109] 在所述步骤S2中,即所述在本地电脑的本地浏览器当接收到用户终端发送的用于登录云桌面的登录请求时,通过所述本地浏览器调取登录云桌面的地址,并对所述登录请求进行登录身份验证包括:

[0110] S21:当在本地电脑的本地浏览器接收到用户终端发送的用于登录云桌面的登录请求时,根据用户的选择,通过所述浏览器调取登录云桌面的第一地址、第二地址或第三地址,并对所述登录请求进行登录身份验证。

[0111] 在所述步骤S3中,即所述将登陆到的云桌面的显示界面显示在本地电脑的本地浏览器的显示框上,以供用户终端使用所述云端软件,其中,所述云桌面的显示界面被所述云端软件的界面全覆盖的步骤包括:

[0112] S31:当验证通过后,将登陆到的云桌面的显示界面显示在本地电脑的本地浏览器的显示框上,以供用户终端使用所述云端软件;

[0113] 若所述用户通过所述第一地址登录云桌面,则所述云桌面的显示界面为所述第一软件所覆盖;或

[0114] 若所述用户通过所述第二地址登录云桌面,则所述云桌面的显示界面为所述第二软件所覆盖;或

[0115] 若所述用户通过第三地址登录云桌面,则所述云桌面的显示界面为第三软件所覆盖。

[0116] 在本实施例中,预设通过第一地址登录云桌面显示界面为所述第一软件所覆盖即

为:通过第一地址登录云桌面显示的界面与所述第一软件显示的界面相同。所述第一软件为需要外网服务且具有部署小程序功能的软件,如:个人微信、企业微信等;所述第二软件为需要外网服务但不具有部署小程序功能的软件,如:腾讯QQ、网易邮箱等;所述第三软件为不具有与外网用户进行消息传输的功能,同时不具有部署小程序功能的软件,如:CAD、Office、Photoshop等;用户可以根据实际需要打开不同的登录云桌面的地址来使用不同的软件。

[0117] 更进一步的,所述白名单中的IP地址包括内网IP地址和外网IP地址,在所述第一软件中创建小程序,每一个所述小程序分别与所述白名单中的内网IP地址和外网IP地址进行连接;其中,所述第一软件为具有部署小程序功能的软件。

[0118] 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程,是可以通过计算机程序来指令相关的硬件来完成,该计算机程序可存储于一计算机可读取存储介质中,该程序在执行时,可包括如上述各方法的实施例的流程。其中,前述的存储介质可为磁碟、光盘、只读存储记忆体(Read-Only Memory,ROM)等非易失性存储介质,或随机存储记忆体(Random Access Memory,RAM)等。

[0119] 应该理解的是,虽然附图的流程图中的各个步骤按照箭头的指示依次显示,但是这些步骤并不是必然按照箭头指示的顺序依次执行。除非本文中有明确的说明,这些步骤的执行并没有严格的顺序限制,其可以以其他的顺序执行。而且,附图的流程图中的至少一部分步骤可以包括多个子步骤或者多个阶段,这些子步骤或者阶段并不必然是在同一时刻执行完成,而是可以在不同的时刻执行,其执行顺序也不必然是依次进行,而是可以与其他步骤或者其他步骤的子步骤或者阶段的至少一部分轮流或者交替地执行。

[0120] 进一步参考图5,作为对上述图2所示方法的实现,本申请提供了一种内网安全访问外网的装置的一个实施例,该装置实施例与图2所示的方法实施例相对应,该装置具体可以应用于各种电子设备中。

[0121] 如图5所示,本实施例所述的内网安全访问外网的装置300包括:装载模块301、验证模块302、显示模块303、判断模块304以及通讯模块305,其中:

[0122] 装载模块301,用于将登录云桌面的地址存储并显示在本地电脑的本地浏览器中,所述云桌面具有内网端口和外网端口,通过所述外网端口接收云端软件安装包,并将所述云端软件安装在所述云桌面上,所述云端软件通过所述外网端口接入外网。

[0123] 验证模块302,用于当在本地电脑的本地浏览器接收到用户终端发送的用于登录云桌面的登录请求时,通过所述本地浏览器调取登录云桌面的地址,并对所述登录请求进行登录身份验证;

[0124] 显示模块303,用于当验证通过后,将登陆到的云桌面的显示界面显示在本地电脑的本地浏览器的显示框上,以供用户终端使用所述云端软件,其中,所述云桌面的显示界面被所述云端软件的界面全覆盖;以及

[0125] 判断模块304,用于在所述用户终端使用所述云端软件接收到外网发送的外网地址时,判断所述外网地址是否存在于预设的白名单中,所述白名单包括IP地址;

[0126] 通讯模块305,用于当所述外网地址在所述白名单中时,与所述外网地址建立通讯连接。

[0127] 在本实施例中,用户可以通过本地浏览器存储的登录云桌面的地址登录云桌面,

实现可以同时使用本地电脑与云桌面，且，本申请将云端软件安装在同时连接内外网的云桌面上，所述云桌面的显示界面为所述云端软件的界面所覆盖，通过设置白名单，从而限制用户对IP地址的访问；并将允许建立通讯连接的IP地址以小程序的方式在云端软件中提供，以此来保障内网与外围安全机制的维持；且对云端软件的更新升级都可以在云端进行，有效的统一管理升级的问题，避免了用户本地硬件和环境差异带来的本地升级的多样性和复杂性。

[0128] 所述验证模块301包括：识别单元、验证资格单元和确认单元；所述识别单元用于识别所述登录请求的网络来源；所述验证资格单元用于当所述登录请求通过内网发送时，验证所述登录请求是否携带预设的登陆码；所述确认单元用于当所述登录请求携带有登陆码时，确认所述登录请求的身份验证通过。

[0129] 所述内网安全访问外网的装置300还包括关闭单元、创建单元、显示单元。所述关闭单元用于当接收到用户终端退出云端软件或关闭本地浏览器的指令时，同步停止对应所述云桌面的运行，关闭云桌面。所述创建单元用于根据所述白名单中的IP地址创建小程序，并将所创建的小程序与所述白名单中的IP地址进行关联。所述显示单元用于将创建的小程序显示在所述云端软件中，以供用户终端访问对应IP地址。

[0130] 所述显示模块包括存储单元和适配单元，所述存储单元用于确定并存储所述云端软件的初始化尺寸；所述适配单元用于根据所述云端软件的初始化尺寸，将云桌面的显示尺寸适配为所述云端软件的显示尺寸。

[0131] 为解决上述技术问题，本申请实施例还提供计算机设备。具体请参阅图6，图6为本实施例计算机设备基本结构框图。

[0132] 所述计算机设备200包括通过系统总线相互通信连接存储器201、处理器202、网络接口203。需要指出的是，图中仅示出了具有组件201-203的计算机设备200，但是应理解的是，并不要求实施所有示出的组件，可以替代的实施更多或者更少的组件。其中，本技术领域技术人员可以理解，这里的计算机设备是一种能够按照事先设定或存储的指令，自动进行数值计算和/或信息处理的设备，其硬件包括但不限于微处理器、专用集成电路(Application Specific Integrated Circuit，ASIC)、可编程门阵列(Field－Programmable Gate Array，FPGA)、数字处理器(Digital Signal Processor，DSP)、嵌入式设备等。

[0133] 所述计算机设备可以是桌上型计算机、笔记本、掌上电脑及云端服务器等计算设备。所述计算机设备可以与用户通过键盘、鼠标、遥控器、触摸板或声控设备等方式进行人机交互。

[0134] 所述存储器201至少包括一种类型的可读存储介质，所述可读存储介质包括闪存、硬盘、多媒体卡、卡型存储器(例如，SD或DX存储器等)、随机访问存储器(RAM)、静态随机访问存储器(SRAM)、只读存储器(ROM)、电可擦除可编程只读存储器(EEPROM)、可编程只读存储器(PROM)、磁性存储器、磁盘、光盘等。在一些实施例中，所述存储器201可以是所述计算机设备200的内部存储单元，例如该计算机设备200的硬盘或内存。在另一些实施例中，所述存储器201也可以是所述计算机设备200的外部存储设备，例如该计算机设备200上配备的插接式硬盘，智能存储卡(Smart Media Card，SMC)，安全数字(Secure Digital，SD)卡，闪存卡(Flash Card)等。当然，所述存储器201还可以既包括所述计算机设备200的内部存储

单元也包括其外部存储设备。本实施例中，所述存储器201通常用于存储安装于所述计算机设备200的操作系统和各类应用软件，例如内网安全访问外网的方法的程序代码等。此外，所述存储器201还可以用于暂时地存储已经输出或者将要输出的各类数据。

[0135] 所述处理器202在一些实施例中可以是中央处理器(Central Processing Unit，CPU)、控制器、微控制器、微处理器、或其他数据处理芯片。该处理器202通常用于控制所述计算机设备200的总体操作。本实施例中，所述处理器202用于运行所述存储器201中存储的程序代码或者处理数据，例如运行所述内网安全访问外网的方法的程序代码。

[0136] 所述网络接口203可包括无线网络接口或有线网络接口，该网络接口203通常用于在所述计算机设备200与其他电子设备之间建立通信连接。

[0137] 本申请还提供了另一种实施方式，即提供一种计算机可读存储介质，所述计算机可读存储介质存储有内网安全访问外网的程序，所述内网安全访问外网的程序可被至少一个处理器执行，以使所述至少一个处理器执行如上述的内网安全访问外网的方法的步骤。

[0138] 通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到上述实施例方法可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质(如ROM/RAM、磁碟、光盘)中，包括若干指令用以使得一台终端设备(可以是手机，计算机，服务器，空调器，或者网络设备等)执行本申请各个实施例所述的方法。

[0139] 显然，以上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，附图中给出了本申请的较佳实施例，但并不限制本申请的专利范围。本申请可以以许多不同的形式来实现，相反地，提供这些实施例的目的是使对本申请的公开内容的理解更加透彻全面。尽管参照前述实施例对本申请进行了详细的说明，对于本领域的技术人员来而言，其依然可以对前述各具体实施方式所记载的技术方案进行修改，或者对其中部分技术特征进行等效替换。凡是利用本申请说明书及附图内容所做的等效结构，直接或间接运用在其他相关的技术领域，均同理在本申请专利保护范围之内。

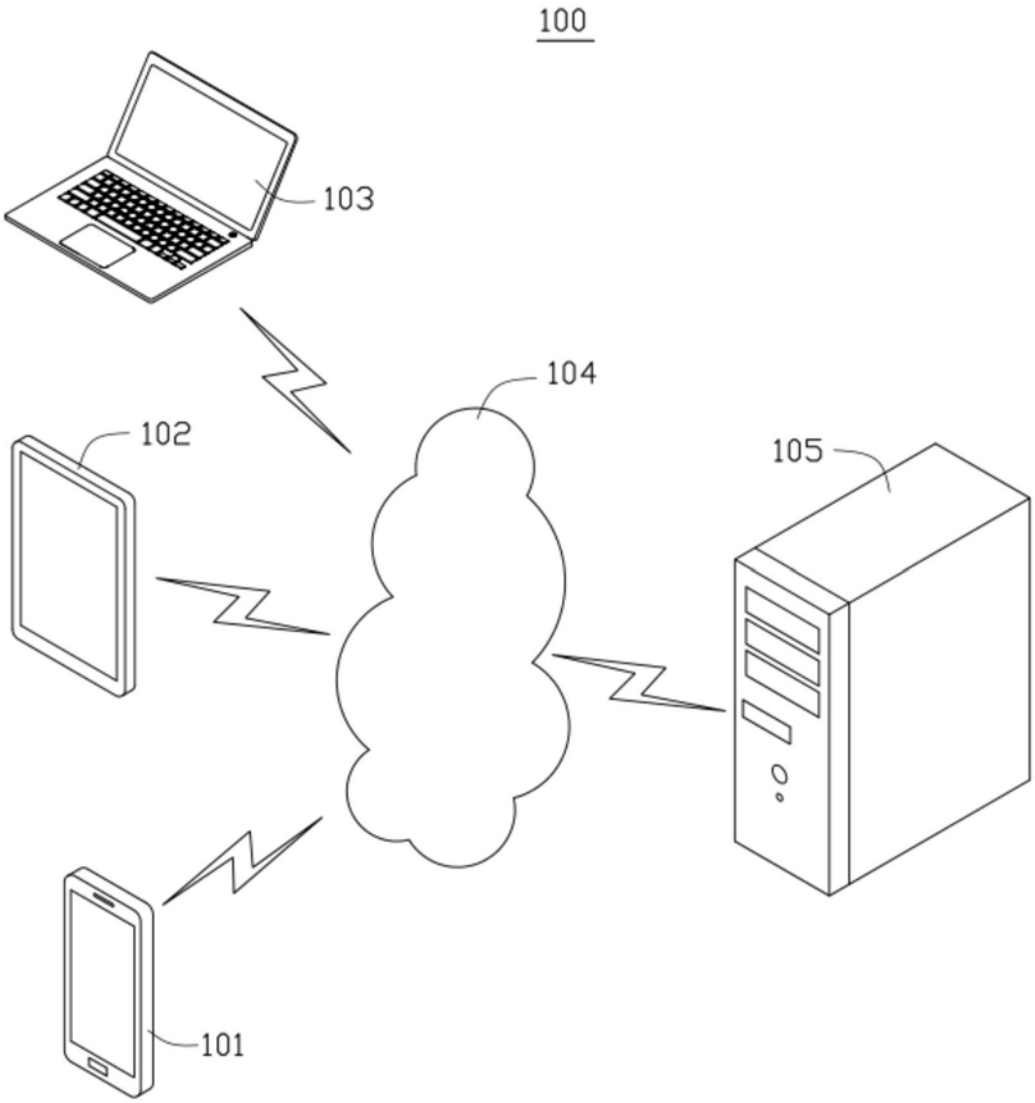


图1

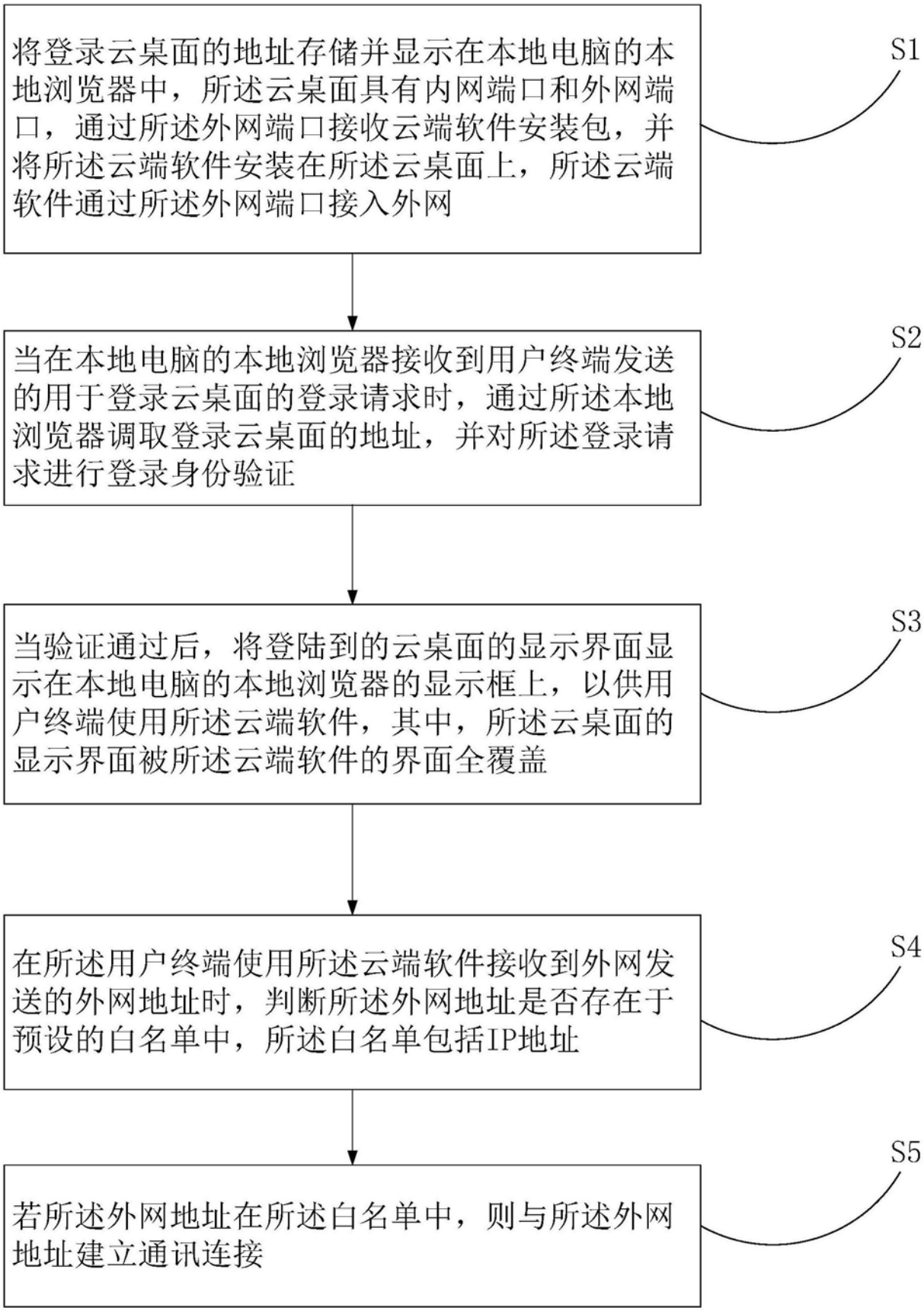

将登录云桌面的地址存储并显示在本地电脑的本地浏览器中，所述云桌面具有内网端口和外网端口，通过所述外网端口接收云端软件安装包，并将所述云端软件安装在所述云桌面上，所述云端软件通过所述外网端口接入外网
S1
当在本地电脑的本地浏览器接收到用户终端发送的用于登录云桌面的登录请求时，通过所述本地浏览器调取登录云桌面的地址，并对所述登录请求进行登录身份验证
S2
当验证通过后，将登陆到的云桌面的显示界面显示在本地电脑的本地浏览器的显示框上，以供用户终端使用所述云端软件，其中，所述云桌面的显示界面被所述云端软件的界面全覆盖
S3
在所述用户终端使用所述云端软件接收到外网发送的外网地址时，判断所述外网地址是否存在于预设的白名单中，所述白名单包括IP地址
S4
若所述外网地址在所述白名单中，则与所述外网地址建立通讯连接
S5

图2

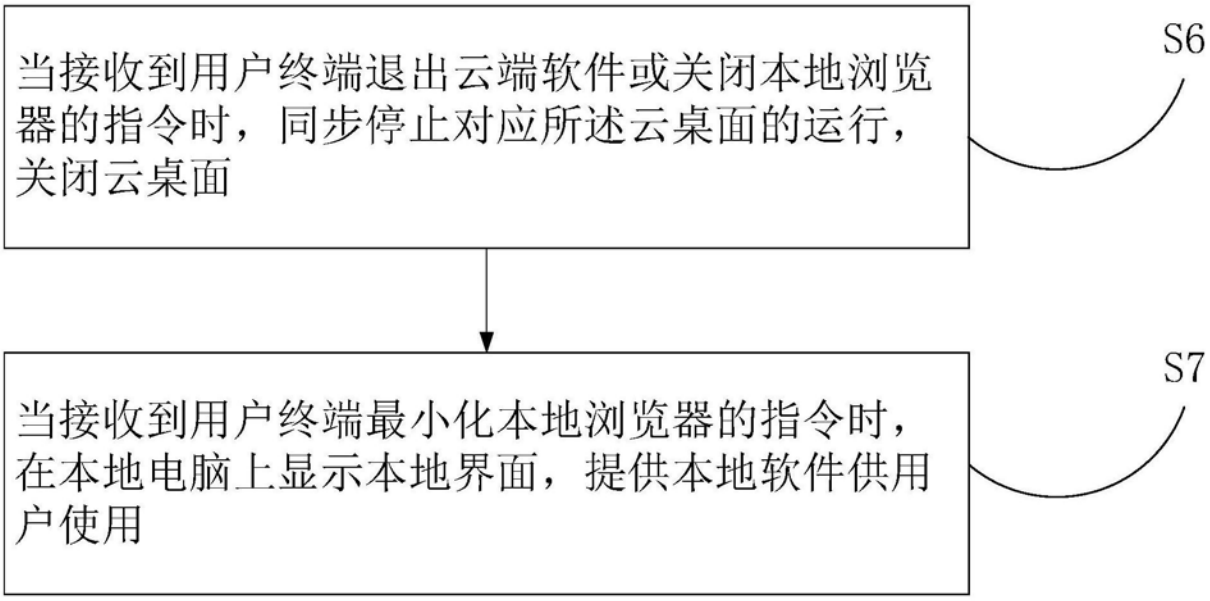

当接收到用户终端退出云端软件或关闭本地浏览器的指令时，同步停止对应所述云桌面的运行，关闭云桌面
S6
当接收到用户终端最小化本地浏览器的指令时，在本地电脑上显示本地界面，提供本地软件供用户使用
S7

图3

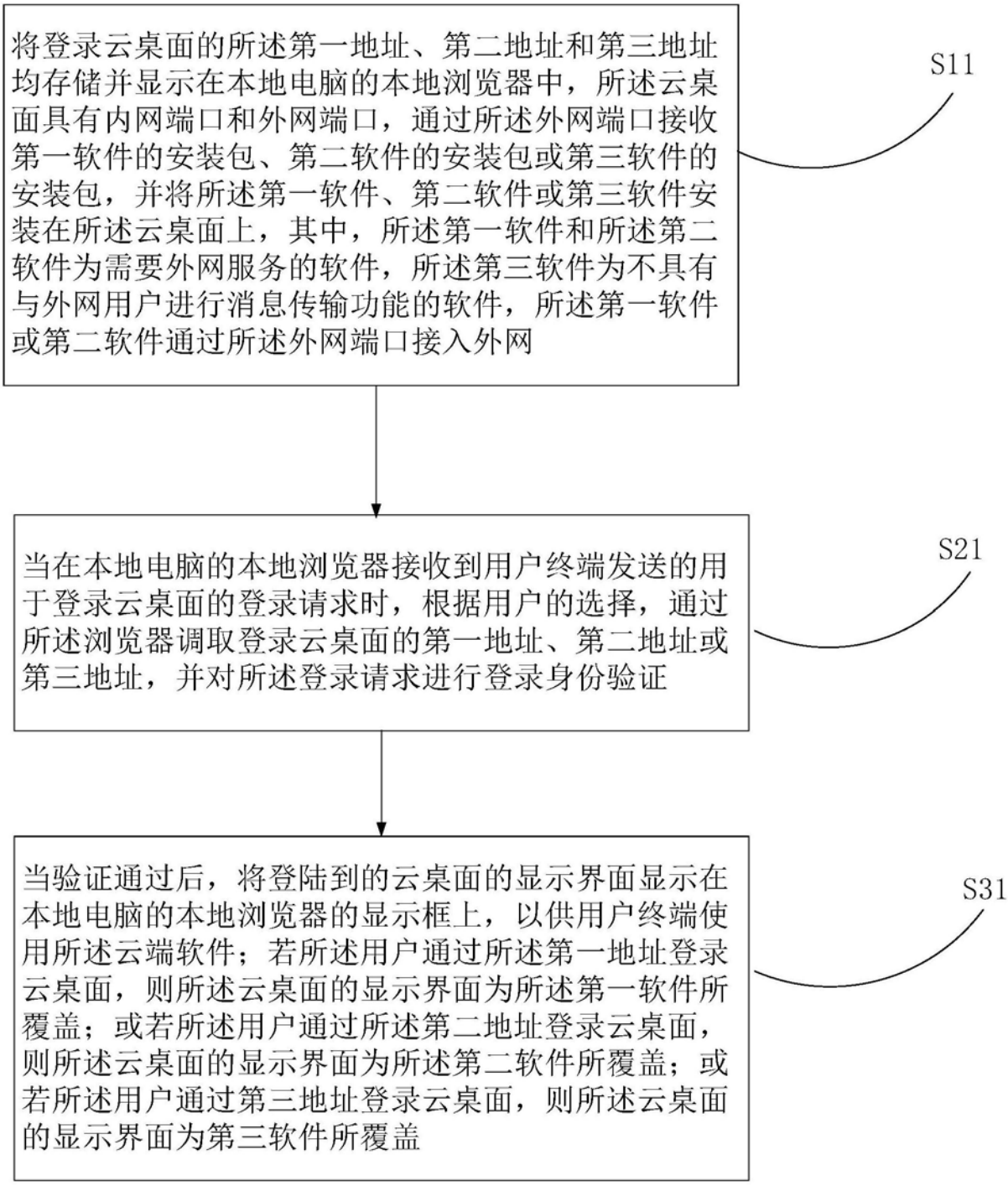

将登录云桌面的所述第一地址、第二地址和第三地址均存储并显示在本地电脑的本地浏览器中，所述云桌面具有内网端口和外网端口，通过所述外网端口接收第一软件的安装包、第二软件的安装包或第三软件的安装包，并将所述第一软件、第二软件或第三软件安装在所述云桌面上，其中，所述第一软件和所述第二软件为需要外网服务的软件，所述第三软件为不具有与外网用户进行消息传输功能的软件，所述第一软件或第二软件通过所述外网端口接入外网
S11
当在本地电脑的本地浏览器接收到用户终端发送的用于登录云桌面的登录请求时，根据用户的选择，通过所述浏览器调取登录云桌面的第一地址、第二地址或第三地址，并对所述登录请求进行登录身份验证
S21
当验证通过后，将登陆到的云桌面的显示界面显示在本地电脑的本地浏览器的显示框上，以供用户终端使用所述云端软件；若所述用户通过所述第一地址登录云桌面，则所述云桌面的显示界面为所述第一软件所覆盖；或若所述用户通过所述第二地址登录云桌面，则所述云桌面的显示界面为所述第二软件所覆盖；或若所述用户通过第三地址登录云桌面，则所述云桌面的显示界面为第三软件所覆盖
S31

图4

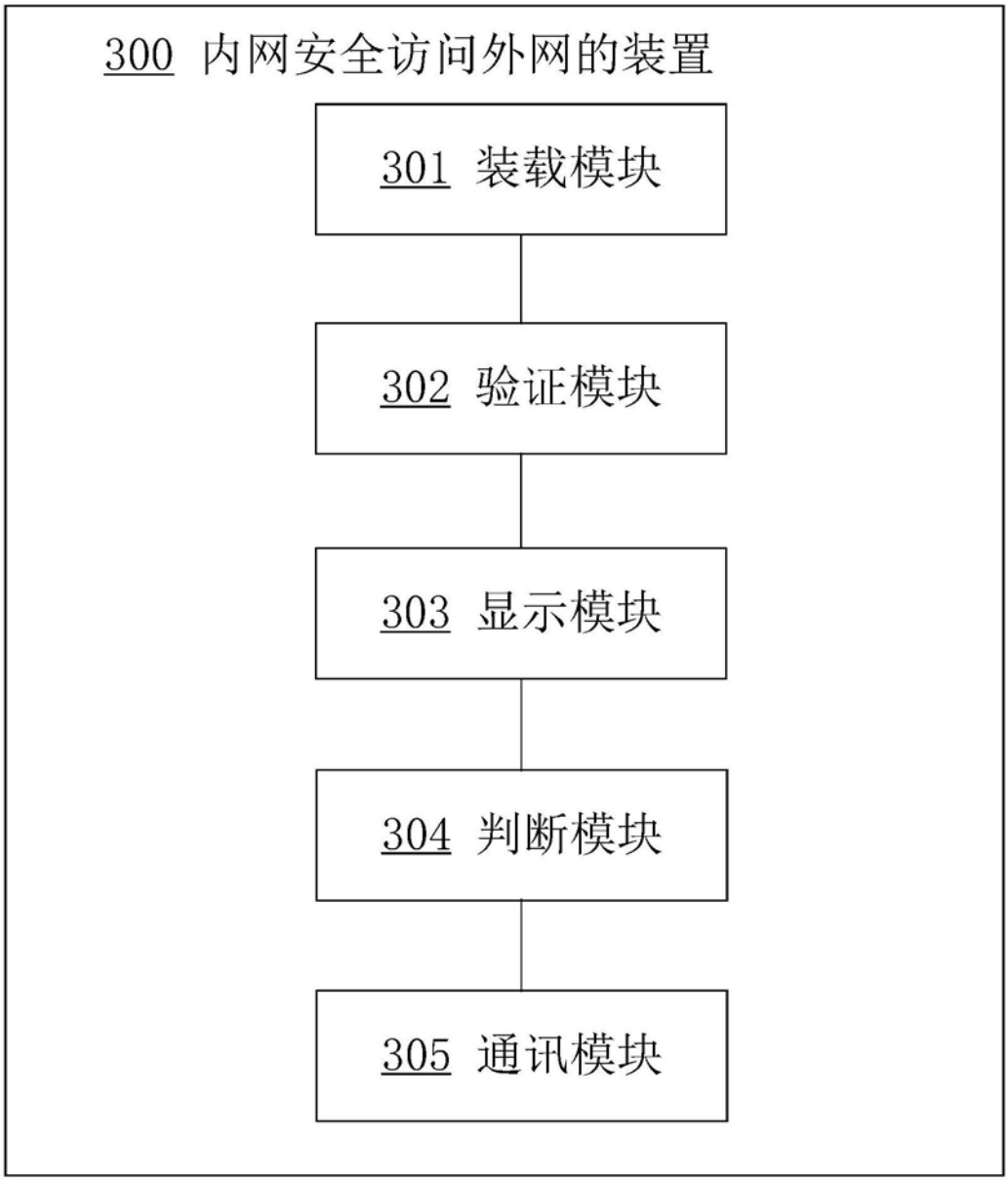


图5

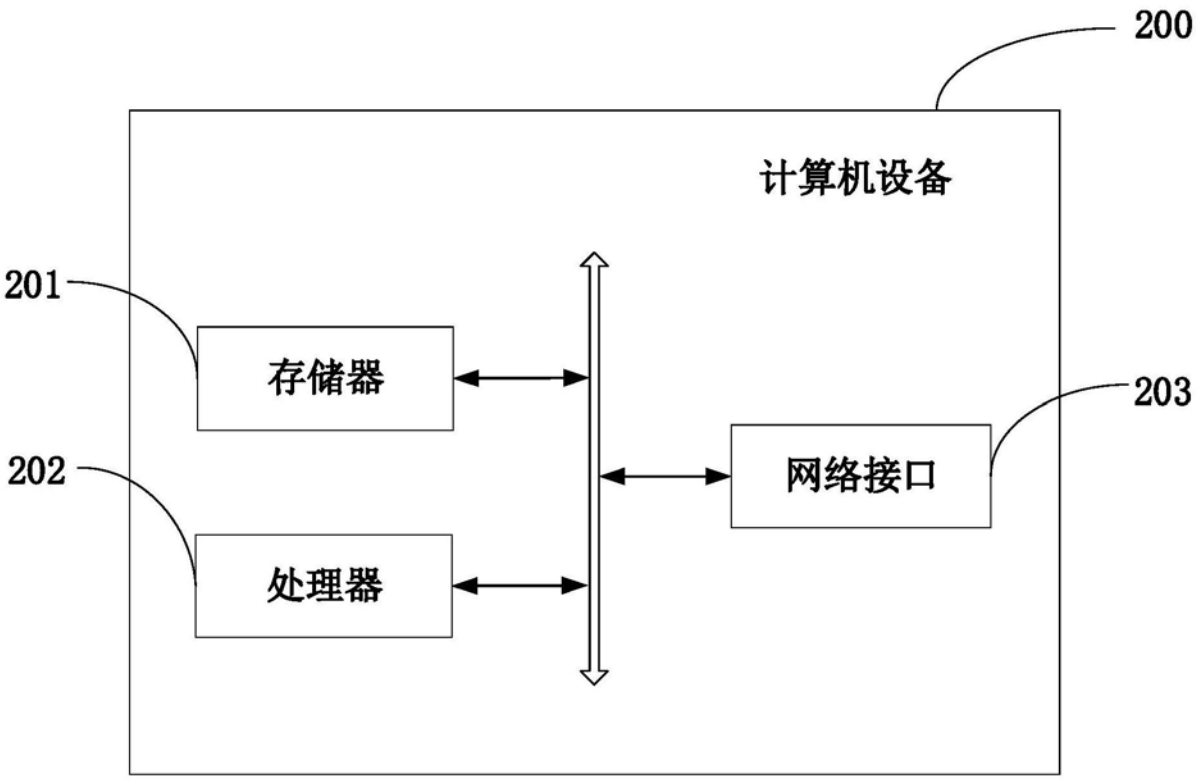


图6