(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2022 年 12 月 1 日 (01.12.2022)

WIPO | PCT

(10) 国际公布号
WO 2022/247751 A1

(51) 国际专利分类号:
G05B 19/042 (2006.01)

(21) 国际申请号: PCT/CN2022/094195

(22) 国际申请日: 2022 年 5 月 20 日 (20.05.2022)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202110595342.2 2021年5月28日 (28.05.2021) CN

(71) 申请人: 上海云盾信息技术有限公司 (**SHANGHAI YUNDUN INFORMATION TECHNOLOGY CO., LTD.**) [CN/CN]; 中国上海市闵行区中春路7001号2幢3楼C3058室, Shanghai 201108 (CN)。

(72) 发明人: 胡金涌(**HU, Jinyong**); 中国上海市闵行区中春路7001号2幢3楼C3058室, Shanghai 201108 (CN)。 刘贺(**LIU, He**); 中国上海市闵行区中春路7001号2幢3楼C3058室, Shanghai 201108 (CN)。

(74) 代理人: 北京名华博信知识产权代理有限公司 (**BOXIN CHINA INTELLECTUAL PROPERTY**); 中国北京市海淀区黑泉路8号1幢4层101-10号, Beijing 100192 (CN)。

(81) 指定国(除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU,

(54) **Title:** METHOD, SYSTEM AND APPARATUS FOR REMOTELY ACCESSING APPLICATION, DEVICE, AND STORAGE MEDIUM

(54) **发明名称**: 远程访问应用的方法、系统、装置、设备及存储介质

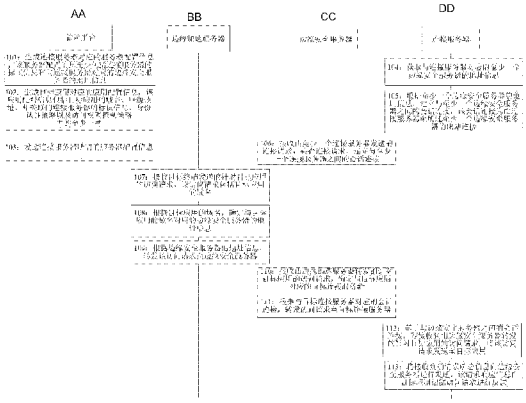

图 2

101 Generate server configuration information corresponding to a connection server, the server configuration information at least comprising identification information of the connection server and address information of an edge security server corresponding to the connection server
102 Generate application configuration information corresponding to a target application, the application configuration information comprising at least one of the domain name of the target application, a back-to-source address, the identification information of the associated connection server, an identity authentication policy, and an access permission control policy
103 Send the server configuration information required by the connection server
104 Acquire the address information of at least one edge security server corresponding to the connection server
105 According to the address information of the at least one edge security server, establish a session connection with the at least one edge security server, the session connection being an outbound connection from the connection server to the at least one edge security server
106 Receive a connection request sent by at least one connection server, and establish a session connection with the at least one connection server according to the connection request
107 Receive an access request, sent by a target terminal, for the target application, the access request comprising the domain name of the target application
108 According to the domain name of the target application, determine the address information of the edge security server corresponding to the domain name of the target application
109 Forward the access request to the edge security server according to the address information of the edge security server
110 Receive the access request, forwarded by an edge acceleration server, for the target application, and determine a target connection server corresponding to the target application
111 Forward the access request to the target connection server according to the session connection corresponding to the target connection server
112 On the basis of the session connection with the edge security server, if the access request, forwarded by the edge security server, for the target application is received, send the access request to the target application
113 Send received request response information to the edge security server, the request response information being fed back by the target application according to the access request
AA Management platform CC Edge security server
BB Edge acceleration server DD Connection server

(57) **Abstract:** The present disclosure provides a method, system and apparatus for remotely accessing an application, a device, and a storage medium. The method comprises: acquiring address information of at least one edge security server corresponding to a connection server; establishing a session connection with the at least one edge security server according to the acquired address information; on the basis of the session connection, if an access request, forwarded by the edge security server, for a target application is received, sending the access request to the target application; and sending, to the edge security server, received request response information fed back by the target application.

(57) **摘要**: 本公开提出一种远程访问应用的方法、系统、装置、设备及存储介质，该方法包括：获取与连接服务器对应的至少一个边缘安全服务器的地址信息；根据获取的地址信息，建立与至少一个边缘安全服务器之间的会话连接；基于会话连接，若接收到由边缘安全服务器转发的针对目标应用的访问请求，将访问请求发送至目标应用；将接收到的目标应用反馈的请求响应信息发送给边缘安全服务器。

WO 2022/247751 A1

[见续页]

CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。

(84) 指定国(除另有指明，要求每一种可提供的地区保护)：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布：

— 包括国际检索报告(条约第21条(3))。

远程访问应用的方法、系统、装置、设备及存储介质

本公开基于 2021 年 05 月 28 日提交中国专利局、申请号为 202110595342.2，发明名称为“远程访问应用的方法、系统、装置、设备及存储介质”的中国专利申请提出，并要求该中国专利申请的优先权，该中国专利申请的全部内容在此引入本公开作为参考。

技术领域

本公开实施例涉及但不限于一种远程访问应用的方法、系统、装置、设备及存储介质。

背景技术

过去企业员工访问企业应用时，大多需要使用 VPN（Virtual Private Network，虚拟专用网络）进行访问，其由安全部门为员工分配 VPN 凭证，员工登陆 VPN 并输入 VPN 凭证即可访问到应用。

而随着云计算技术的发展，企业的基础设施发生了重大变革，企业的应用可广泛分布于公有云、私有云和混合云中，随之改变的是，企业员工对企业应用的访问需求也呈现出新的变化，如移动化、远程办公、第三方合作伙伴的访问等等。企业需要为日益多样化、分布广泛的用户提供服务，也需要保证应用的安全性。

但基于传统的 VPN 方案难以胜任这种新的变化。首先，企业在多分支机构和多云环境下部署 VPN 面临着成本高、管理复杂的问题；其次，传统的 VPN 体验较差，因网络波动容易导致访问延迟或者服务不稳定等问题，影响工作效率；再者，传统 VPN 主要通过不受信任的网络连接企业的基础设施，本身就会在防火墙上形成漏洞。一旦 VPN 凭证被黑客利用，黑客即可通过 VPN 访问到企业网络并在内部横向移动以访问应用程序和数据，这给企业带来巨大的安全风险。

发明内容

以下是对本公开详细描述的主题的概述。本概述并非是为了限制权利要求的保护范围。

为克服相关技术中存在的问题，本公开提出一种远程访问应用的方法、系统、装置、设备及存储介质，进而至少可以在一定程度上既可以避免 VPN 不稳定且难以维护的问题，还可以保证目标应用的安全性。

根据本公开的第一方面，提供一种远程访问应用的方法，应用于连接服务器，所述连接服务器与至少一个目标应用相关联，包括：

获取与所述连接服务器对应的至少一个边缘安全服务器的地址信息；

根据所述至少一个边缘安全服务器的地址信息，建立与所述至少一个边缘安全服务器之间的会话连接，所述会话连接为由所述连接服务器至所述至少一个边缘安全服务器的出站连接；

基于所述会话连接，若接收到由边缘安全服务器转发的针对目标应用的访问请求，将所述访问请求发送至所述目标应用；

将接收到的请求响应信息向所述边缘安全服务器进行发送，所述请求响应信息由所述目标应用根据所述访问请求进行反馈。

根据本公开的第二方面，提供一种远程访问应用的方法，应用于边缘安全服务器，包括：

接收由至少一个连接服务器发送的连接请求；

根据所述连接请求，建立与所述至少一个连接服务器之间的会话连接；

接收由边缘加速服务器转发的针对目标应用的访问请求，确定与所述目标应用对应的目标连接服务器；

根据与所述目标连接服务器对应的会话连接，转发所述访问请求至所述目标连接服务器。

根据本公开的第三方面，提供一种远程访问应用的方法，应用于边缘加速服务器，包括：

接收由目标终端发送的针对目标应用的访问请求，所述访问请求包含所述目标应用的域名；

根据所述目标应用的域名，确定与所述目标应用的域名对应的边缘安全服务器的地址信息；

根据所述边缘安全服务器的地址信息，转发所述访问请求至所述边缘安全服务器。

根据本公开的第四方面，提供一种远程访问应用的方法，应用于管理平台，

包括：

生成连接服务器对应的服务器配置信息，所述服务器配置信息至少包括连接服务器的标识信息和与连接服务器对应的边缘安全服务器的地址信息；

生成目标应用对应的应用配置信息，所述应用配置信息包括目标应用的域名、回源地址、相关联的连接服务器的标识信息、身份认证策略以及访问权限控制策略中的至少一种；

发送所述连接服务器所需的服务器配置信息；

发送边缘加速服务器所需的所述目标应用的应用配置信息以及与所述目标应用相关联的连接服务器的服务器配置信息。

根据本公开的第五方面，提供一种远程访问应用的系统，包括：管理平台、边缘加速服务器、边缘安全服务器和连接服务器；

管理平台，设置为生成目标应用的应用配置信息，以及生成连接服务器对应的服务器配置信息；发送边缘加速服务器所需的所述目标应用的应用配置信息以及与所述目标应用相关联的连接服务器的服务器配置信息，并发送所述连接服务器所需的服务器配置信息；

边缘加速服务器，设置为接收目标终端发送的针对目标应用的访问请求；并根据所述访问请求包含的目标应用的域名，将所述访问请求向对应的边缘安全服务器进行发送；

边缘安全服务器，设置为接收所述边缘加速服务器发送的所述访问请求；根据在先建立的与连接服务器的会话连接，将所述访问请求转发至对应的连接服务器；

连接服务器，设置为接收所述边缘安全服务器发送的所述访问请求，并将所述访问请求转发至对应的目标应用。

根据本公开的第六方面，提供一种远程访问应用的装置，应用于连接服务器，包括：

获取模块，设置为获取与所述连接服务器对应的至少一个边缘安全服务器的地址信息；

建立会话模块，设置为根据所述至少一个边缘安全服务器的地址信息，建立与所述至少一个边缘安全服务器之间的会话连接，所述会话连接为由所述连接服务器至所述至少一个边缘安全服务器的出站连接；

发送模块，设置为基于所述会话连接，若接收到由边缘安全服务器转发的针对目标应用的访问请求，将所述访问请求发送至所述目标应用；将接收到的请求响应信息向所述边缘安全服务器进行发送，所述请求响应信息由所述目标应用根据所述访问请求进行反馈。

根据本公开的第七方面，提供一种远程访问应用的装置，应用于边缘安全服务器，包括：

接收模块，设置为接收由至少一个连接服务器发送的连接请求；

建立会话模块，设置为根据所述连接请求，建立与所述至少一个连接服务器之间的会话连接；

所述接收模块，还设置为接收由边缘加速服务器转发的针对目标应用的访问请求；

确定模块，设置为确定与所述目标应用对应的目标连接服务器；

发送模块，设置为根据与所述目标连接服务器对应的会话连接，转发所述访问请求至所述目标连接服务器。

根据本公开的第八方面，提供一种远程访问应用的装置，应用于边缘加速服务器，包括：

接收模块，设置为接收由目标终端发送的针对目标应用的访问请求，所述访问请求包含所述目标应用的域名；

确定模块，设置为根据所述目标应用的域名，确定与所述目标应用的域名对应的边缘安全服务器的地址信息；

发送模块，设置为根据所述边缘安全服务器的地址信息，转发所述访问请求至所述边缘安全服务器。

根据本公开的第九方面，提供一种远程访问应用的装置，应用于管理平台，包括：

生成模块，设置为生成连接服务器对应的服务器配置信息，所述服务器配置信息至少包括连接服务器的标识信息和与连接服务器对应的边缘安全服务器的地址信息；生成目标应用对应的应用配置信息，所述应用配置信息包括目标应用的域名、回源地址、相关联的连接服务器的标识信息、身份认证策略以及访问权限控制策略中的至少一种；

发送模块，设置为发送所述连接服务器所需的服务器配置信息；发送边缘加

速服务器所需的所述目标应用的应用配置信息以及与所述目标应用相关联的连接服务器的服务器配置信息。

根据本公开的第十方面，提供一种电子设备，包括存储器、处理器及存储在所述存储器上并可在所述处理器上运行的计算机程序，所述处理器运行所述计算机程序以实现上述第一至第四方面中任一方面所述的方法。

根据本公开的第十一方面，提供一种计算机可读存储介质，其上存储有计算机程序，所述程序被处理器执行实现上述第一至第四方面中任一方面所述的方法。

本公开实施例中提供的技术方案，至少具有如下技术效果或优点：

在本公开实施例中，通过连接服务器的设置并建立连接服务器与边缘安全服务器之间的会话连接，该会话连接为连接服务器至边缘安全服务器之间的出站连接，使得用户不需要使用 VPN 服务器即可实现目标终端远程访问目标应用，解决了 VPN 服务器不稳定且难以维护的问题。同时，基于该会话连接，接收由边缘安全服务器转发的针对目标应用的访问请求，可以避免由其他服务器主动向连接服务器发送信息或者建立连接的情况发生，降低了遭受恶意攻击的风险，保证了目标应用的安全性。

在阅读并理解了附图和详细描述后，可以明白其他方面。

附图说明

构成本公开的一部分的附图用来提供对本公开的进一步理解，本公开的示意性实施例及其说明用于解释本公开，并不构成对本公开的不当限定。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：

图 1 是根据一示例性实施例示出的可以应用本公开实施例的技术方案的示例性系统架构的示意图；

图 2 是根据一示例性实施例示出的一种远程访问应用的方法的信令交互图；

图 3 是根据一示例性实施例示出的目标应用的应用配置信息及连接器的模板参数信息的示意图；

图 4 是根据一示例性实施例示出的连接服务器与边缘安全服务器建立会话连接的过程示意图；

图 5 是根据一示例性实施例示出的边缘安全服务器建立连接服务器的标识信息与会话的映射关系的示意图；

图 6 是根据一示例性实施例示出的一种远程访问应用的方法的流程图；

图 7 是根据一示例性实施例示出的一种远程访问应用的方法的另一流程图；

图 8 是根据一示例性实施例示出的一种远程访问应用的方法中连接服务器的操作流程图；

图 9 是根据一示例性实施例示出的一种远程访问应用的方法中边缘安全服务器的操作流程图；

图 10 是根据一示例性实施例示出的一种远程访问应用的方法中边缘加速服务器的操作流程图；

图 11 是根据一示例性实施例示出的一种远程访问应用的方法中管理平台的操作流程图；

图 12 是根据一示例性实施例示出的一种应用于连接服务器的远程访问应用的装置的结构示意图；

图 13 是根据一示例性实施例示出的一种应用于边缘安全服务器的远程访问应用的装置的结构示意图；

图 14 是根据一示例性实施例示出的一种应用于边缘加速服务器的远程访问应用的装置的结构示意图；

图 15 是根据一示例性实施例示出的一种应用于管理平台的远程访问应用的装置的结构示意图；

图 16 是根据一示例性实施例示出的一种电子设备的结构示意图；

图 17 是根据一示例性实施例示出的一种存储介质的示意图。

具体实施方式

下面将参照附图更详细地描述本公开的示例性实施方式。虽然附图中显示了本公开的示例性实施方式，然而应当理解，可以以各种形式实现本公开而不应被这里阐述的实施方式所限制。相反，提供这些实施方式是为了能够更透彻地理解本公开，并且能够将本公开的范围完整的传达给本领域的技术人员。

需要注意的是，除非另有说明，本公开使用的技术术语或者科学术语应当为本公开所属领域技术人员所理解的通常意义。

下面结合附图来描述根据本公开实施例提出的一种远程访问应用的方法、系统、装置、设备及存储介质。

本公开实施例提供了一种远程访问应用的方法，参见图 1，该方法所基于的网

络系统架构包括连接服务器、边缘安全服务器、边缘加速服务器、管理平台和目标终端。其中，连接服务器可以采用 VPC（Virtual Private Cloud，专有网络）/NAT（Network Address Translation，网络地址转换），配置有一个或多个连接器的服务器称为连接服务器，连接器可以为用于进行网络通信的软件程序，连接服务器可以通过其自身所配置的连接器与至少一个目标应用相关联。具体地，连接服务器中的每个连接器均可以与一个或多个目标应用通信连接，目标应用可以为内网中的内部应用，也可以为公网中的应用，例如源站等。

图 1 中仅示意性地画出了连接服务器包括一个连接器，该连接器与内网中的一个目标应用通信连接。连接服务器通过连接器与边缘安全服务器建立会话连接，该会话连接为出向的通信连接，该会话连接可以为 TCP（Transmission Control Protocol，传输控制协议）连接或 HTTPS（Hyper Text Transfer Protocol over Secure Socket Layer，超文本传输安全协议）连接或 SSL/TLS 连接等。边缘加速服务器与边缘安全服务器和目标终端通信，管理平台与边缘加速服务器通信连接。

如图 1 所示，该网络系统架构中还可以通过边缘加速节点对目标终端的用户执行认证策略，以保证只有通过该认证策略的目标终端才可以进行目标应用的访问，保证目标应用的安全性。在一示例中，边缘加速节点可以通过认证中心获取目标用户的身份信息，以针对该身份信息执行认证策略。其中，该认证中心可以为设置于边缘加速服务器中的认证组件或者为独立于边缘加速服务器的认证设备，该认证中心与边缘加速服务器相连接。在一示例中，该认证中心可以与第三方身份认证系统相连接，以从第三方身份认证系统中获取目标用户的身份信息；在另一示例中，该认证中心也可以通过边缘加速服务器、边缘安全服务器和连接服务器从内部身份认证系统中获取目标用户的身份信息。由此，认证中心可以根据用户所选择的认证方式，从第三方身份认证系统或内部身份认证系统中获取目标用户的身份信息，等等。本领域技术人员可以根据实际实现需要，确定对应的身份信息获取方式，本公开对此不作特殊限定。

需要说明的是，当无需第三方身份认证系统提供身份信息或者进行身份信息的验证时，边缘加速服务器也可以通过边缘安全服务器和连接服务器从内部身份认证系统中获取身份信息或者进行身份信息验证，而无需认证中心的参与，即在该网络系统架构中，认证中心并不是一定存在的，本领域技术人员可以根据实际实现需要进行配置，本公开对此不作特殊限定。

需要说明的，该目标终端可以包括智能手机、平板电脑、便携式电脑或者台式计算机中的一种或者多种。可以理解的，图 1 中的目标终端、边缘加速服务器、认证中心、管理平台、边缘安全服务器以及连接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目标终端、边缘加速服务器、认证中心、管理平台、边缘安全服务器以及连接服务器。例如，该网络架构中可以包括一个或多个边缘加速服务器以及一个或多个边缘安全服务器，图 1 中仅示意性地画出了一个边缘加速服务器和一个边缘安全服务器。

值得注意的是，本公开实施例提到的边缘加速服务器和边缘安全服务器，是两个逻辑概念，分开提出来是为了帮助理解，实践中可以分开部署，也可以部署在同一台服务器设备上，本公开对此不作特殊限定。

基于上述网络架构，不需要使用 VPN 服务器即可实现目标终端访问内网中的目标应用，解决了 VPN 服务器不稳定且难以维护的问题。直接将内网的目标应用发布到公网上，由边缘加速服务器对用户身份及访问权限进行认证，消除了恶意攻击的风险。不需要对原有的网络拓扑进行修改即可将内网中的目标应用 SaaS（Software-as-a-Service，软件即服务）化。且通过增加边缘加速服务器和边缘安全服务器的数量，能够很方便地进行扩容，能够适应目标用户数量很大的应用场景。

以下对本公开实施例的技术方案的实现细节进行详细阐述：

图 2 示出了本公开一实施例所提供的的一种远程访问应用的方法的信令交互图。参照图 2 所示，该方法至少包括步骤 101 至步骤 113，详细介绍如下：

步骤 101：管理平台生成连接服务器对应的服务器配置信息，该服务器配置信息至少包括连接服务器的标识信息和与连接服务器对应的边缘安全服务器的地址信息。

其中，管理平台可以为云计算平台，如私有云或公有云等。该管理平台可以为企事业单位或社会组织等团体的连接服务器提供服务器配置信息。该服务器配置信息至少包括连接服务器的标识信息和与连接服务器对应的边缘安全服务器的地址信息。其中，标识信息可以用于唯一标识连接服务器，可以为连接服务器的 IP 地址、MAC（Media Access Control Address，硬件地址）地址或人为设定或自动生成的能够唯一标识该连接服务器的字符序列等。

连接服务器可以是安装有连接器的服务器，连接器为用于进行网络通信的软件程序，将连接器安装在企事业单位或社会组织等团体的连接服务器上，使得连接服务器能够通过连接器与外部网络建立会话连接，通过建立的会话连接实现内

部网络的远程访问。

边缘安全服务器可以是能够与连接服务器进行通信的服务器，其可以与连接服务器之间建立用以传输信息的会话连接。可以理解的，边缘安全服务器的地址信息可以包括域名和/IP 地址，若为域名，则根据该域名可以解析到一个或多个边缘安全服务器的 IP 地址。需要说明的是，一个边缘安全服务器可以与一个或者多个连接服务器进行通信，一个连接服务器也可以与一个或者多个边缘安全服务器进行连接，本公开对此不作特殊限定。

在本公开一示例性实施例中，在通过连接服务器实现远程访问前，首先在管理平台上生成连接服务器对应的服务器配置信息，该服务器配置信息可以作为连接服务器对应的启动参数，以在根据该服务器配置信息对连接服务器进行配置之后启用该连接服务器。

作为一种实现方式，客户可以自行配置该服务器配置信息，具体地，管理平台可以支持客户的配置操作，接收客户配置的服务器配置信息。其也可以由客户将应用服务器的相关配置信息提供给服务提供方，再由服务提供方在管理平台上配置该客户的应用服务器对应的服务器配置信息。

作为另一种实现方式，管理平台也可以自动生成连接服务器对应的服务器配置信息，具体地，管理平台可以为连接服务器分配用于唯一标识该连接服务器的标识信息，以及根据整个网络系统架构中包括的所有边缘安全服务器的配置信息，分配与该连接服务器对应的边缘安全服务器。其中，边缘安全服务器的配置信息中可以包括但不限于边缘安全服务器的地址信息、已关联的连接器的数目、能关联的连接器数目的上限值等。管理平台为该连接服务器分配标识信息及相关联的边缘安全服务器后，将该标识信息及该连接服务器对应的边缘安全服务器的地址信息等确定为该连接服务器对应的服务器配置信息。

在本公开一示例性实施例中，连接器可以是在管理平台上创建的，管理平台可以为服务提供方提供用于创建连接器的接口。连接器可以运行在多种平台上，如 VMware 的虚拟机、Docker（应用容器引擎）、公有云云主机等。服务提供方利用管理平台提供的接口创建运行在不同平台上的连接器。在创建出连接器后，还生成连接器对应的安装包和配置信息，该配置信息中包括连接器的唯一标识、连接器对应的边缘安全服务器的地址信息等，该边缘安全服务器的地址信息可以包括边缘安全服务器的域名和/或 IP 地址。

需要说明的，管理平台上可以创建一个连接器，也可以创建多个连接器，且在各连接器对应的配置信息中可以包括该连接器所对应的一个或多个边缘安全服务器的地址信息，以便连接服务器安装并启动连接器之后，该连接器可以与图 1 所示系统架构中的一个或多个边缘安全服务器建立会话连接。

例如，图 3 中示出了一个连接器的配置信息，该配置信息中包括连接器的唯一标识“连接器 id:12345”，以及连接器对应的边缘安全服务器的域名“companyA.connector.com”。

另外，在一示例性实施例中，为了实现访问的高可用，边缘安全服务器的地址信息包括的域名至少会解析到两个边缘安全服务器的 IP 地址。由此，连接服务器可以根据解析到的多个边缘安全服务器的 IP 地址，分别建立与多个边缘安全服务器之间的会话连接，从而在某一会话连接失效或者故障时，可以通过其他的会话连接进行信息传输。可以理解的，根据该多个边缘安全服务器所建立的会话连接可以是用于传输相同信息的会话连接，换言之，多个会话连接中有的可以作为主会话连接，其他的作为副会话连接，以在主会话连接失效时，可以通过副会话连接所传输的信息进行处理，以保证访问的稳定性。

步骤 102：管理平台生成目标应用对应的应用配置信息，该应用配置信息包括目标应用的域名、回源地址、相关联的连接服务器的标识信息、身份认证策略以及访问权限控制策略中的至少一种。

其中，目标应用可以为企事业单位或社会组织等团体的内网中的应用，如 OA 系统、Web（网站）、SSH（Secure Shell，安全外壳协议）、VNC（Virtual Network Console，虚拟网络控制台）、RDP（Remote Desktop Protocol，远程桌面协议）、内部 IAM（Identity and Access Management，身份识别与访问管理）等。目标应用也可以为公网中的应用程序。

在本公开一示例性实施例中，在访问目标应用之前，由管理平台生成目标应用对应的应用配置信息。具体地，管理平台可以支持用户的配置操作，用户依据自身需求确定允许远程访问的目标应用，然后在管理平台上配置这些目标应用对应的应用配置信息，管理平台可以接收并存储用户所配置的应用配置信息，并将该应用配置信息与对应的目标应用相关联。

在一示例性实施例中，该应用配置信息可以包括回源地址、目标应用的域名、身份认证策略、访问权限控制策略以及与该目标应用相关联的连接服务器的标识信息等多种信息中的一种或多种的组合。其中，回源地址可以包括目标应用所在

设备的IP地址及目标应用所在设备对外开放的端口号等。身份认证策略用于规定目标用户的身份认证方式，访问权限控制策略用于规定对该目标应用具有访问权限的用户身份。

例如，图3中示出的目标应用对应的应用配置信息中的回源地址为172.16.1.100:433，其中172.16.1.100为目标应用所在设备的IP地址，433表示目标应用所在设备对外开放的端口仅为433端口（即网页浏览端口）。图3中应用配置信息包括的目标应用的域名为“oa.companyA.com”，回源负载均衡策略为“轮询”，身份认证方式为“企业微信”，访问权限控制策略为“允许财务人员访问”，与该目标应用相关联的连接服务器的唯一标识为“绑定连接器：12345”。

通过步骤101和102的操作，在管理平台上生成连接服务器对应的服务器配置信息及目标应用对应的应用配置信息，通过在应用配置信息中设置相关联的连接服务器的标识信息将该目标应用与连接服务器关联起来。

需要说明的，目标应用与连接服务器可以处于同一网络，例如均属于内部网络、均属于公共网络或者属于同一C段网络等，目标应用与连接服务器也可以处于不同网络，例如一个在公网、另一个在内部网络等，本公开对此不作特殊限定，只需目标应用与连接服务器之间可以通信即可。

步骤103：管理平台发送连接服务器所需的服务器配置信息。

在本公开一示例性实施例中，连接服务器可以直接从管理平台中下载连接器的安装包，依据下载的安装包在连接服务器本地安装连接器。具体地，连接服务器发送连接器获取请求给管理平台，管理平台根据接收到的连接服务器的连接器获取请求，将连接器的安装包发送给该连接服务器。连接服务器从管理平台下载连接器的安装包后，根据该安装包在连接服务器中安装该连接器。

或者，连接服务器的云主机中可以预先安装有连接器。或者，还可以是连接服务器从管理平台中下载完整的连接器镜像文件进行安装，等等。本公开实施例对连接服务器如何安装连接器的方式不作特殊限定。

在连接服务器安装连接器后，可以从管理平台请求服务器配置信息。管理平台响应连接服务器的请求，发送服务器配置信息给连接服务器。连接服务器安装连接器并从管理平台获得服务器配置信息后，以服务器配置信息来启动此连接器。在一示例中，连接服务器向管理平台请求服务器发送配置信息获取请求，该配置信息获取请求中可以包含该连接服务器的标识信息（即连接器的标识信息），管理平台可以根据该标识信息，将对应的服务器配置信息向连接服务器进行反馈。

在本公开实施例中，同一连接服务器可以部署一个或多个连接器。在部署多个连接器的应用场景中，多个连接器可以与相同的目标应用关联，对于该相同的目标应用来说，其关联的多个连接器可以划分为主用连接器和备用连接器，以便在主用连接器故障时采用备用连接器进行通信，提高远程访问应用的网络稳定性。

需要说明的，当一个连接服务器中部署多个连接器时，多个连接器的标识信息均可以作为该连接服务器的标识信息，例如在连接服务器 A 中包含两个连接器，两个连接器的标识信息分别为 123456 和 234567，那么，该连接服务器 A 的标识信息可以为两个即 123456 和 234567，等等。又或者，当一个连接服务器中部署多个连接器时，可以为该连接服务器配置一个标识信息，该标识信息则可以与多个连接器的标识信息存在映射关系。本领域技术人员可以根据实际实现需要确定对应的实现方式，本公开对此不作特殊限定。

步骤 104：连接服务器获取与连接服务器对应的至少一个边缘安全服务器的地址信息。

在本公开一示例性实施例中，连接服务器由管理平台中获取连接服务器对应的服务器配置信息。可选的，连接服务器可以直接从管理平台中获取服务器配置信息。或者，连接服务器也可以通过中间媒介间接从管理平台获取服务器配置信息，例如管理平台将该连接服务器的服务器配置信息下发至配置中心，连接服务器再从配置中心获取该服务器配置信息。连接服务器在获得服务器配置信息后，从该服务器配置信息中获取与连接服务器对应的至少一个边缘安全服务器的地址信息。该地址信息包括边缘安全服务器的 IP 地址和/或域名。

步骤 105：连接服务器根据至少一个边缘安全服务器的地址信息，建立与至少一个边缘安全服务器之间的会话连接，该会话连接为由连接服务器至所述至少一个边缘安全服务器的出站连接。

在本公开一示例性实施例中，在连接服务器中安装连接器，且连接器运行正常之后，连接服务器需要通过连接器建立与该连接服务器对应的至少一个边缘安全服务器之间的会话连接。若至少一个边缘安全服务器的地址信息中包括边缘安全服务器的 IP 地址，则根据至少一个边缘安全服务器的 IP 地址，直接建立该连接服务器与至少一个边缘安全服务器之间的会话连接。

若至少一个边缘安全服务器的地址信息中仅包括边缘安全服务器的域名，则连接服务器发送该至少一个边缘安全服务器的域名解析请求给域名服务器。域名

服务器对每个域名进行域名解析，得到每个域名对应的 IP 地址，然后将每个域名对应的 IP 地址发送给连接服务器。连接服务器接收域名服务器返回的每个域名对应的 IP 地址，根据每个 IP 地址，分别发送连接请求给每个 IP 地址对应的边缘安全服务器，该连接请求包括该连接服务器的标识信息，以建立并唯一标识该连接服务器与其对应的至少一个边缘安全服务器之间的会话连接。

在本公开实施例中，该会话连接为由连接服务器至所述至少一个边缘安全服务器的出站连接，这些会话连接是连接服务器主动向外的通信连接。连接服务器禁止入向的连接，具体地，可以在连接服务器的防火墙中配置禁止入向的连接请求，从而使连接服务器能够通过防火墙禁止除上述建立的会话连接以外的所有入向请求。如此能够确保连接服务器只能通过建立的会话连接接收入向的信息，通过建立的会话连接实现对目标应用程序的远程访问，同时能够避免其他入向访问，确保目标应用程序的安全性。在目标应用为内网的应用时，能够极大地提高内网的安全性。

步骤 106：边缘安全服务器接收由至少一个连接服务器发送的连接请求，根据连接请求，建立与至少一个连接服务器之间的会话连接。

步骤 105 中连接服务器建立与边缘安全服务器之间的会话连接之前，发送连接请求给边缘安全服务器，该连接请求中包括该连接服务器的标识信息。由于一个边缘安全服务器可以与至少一个连接服务器建立会话连接，因此边缘安全服务器能接收到至少一个连接服务器发送的连接请求，根据接收的连接请求包括的标识信息，建立与这至少一个连接服务器之间的会话连接，该会话连接是边缘安全服务器与连接服务器中安装的连接器之间的会话连接。

在本公开实施例中，边缘安全服务器接收到的连接请求的数量可以为多个，连接请求中包含对应的连接服务器的标识信息。边缘安全服务器根据多个连接请求，分别建立与至少一个连接服务器之间的会话连接，并将各连接请求包括的标识信息与对应的会话连接相关联。具体地，边缘安全服务器将连接请求包括的标识信息与对应的会话存储在连接服务器的标识信息与会话的映射关系中。

在本公开实施例中，连接服务器中的一个连接器可以与一个或多个边缘安全服务器建立会话连接，一个边缘安全服务器可以与一个或多个连接服务器连接，即一个边缘安全服务器可以与一个连接服务器中的一个或多个连接器建立会话连接，如此能够避免某个连接器、某个连接服务器或某个边缘安全服务器出现故障导致

远程访问中断的情况。

在本公开实施例中，连接服务器与边缘安全服务器之间的会话连接是建立在443端口（即网页浏览端口）上，在该会话连接上实现应用层的连接复用，并在该会话连接的回路上实现请求回源。为了实现连接器的高可用，连接器可以与多个边缘安全服务器建立持久的会话连接。对于连接服务器来说，因为连接器对应的会话连接是出向的，目标应用的回源访问只依赖于该会话连接，不需要建立任何入向的连接，因此内网防火墙或者VPC（Virtual Private Cloud，虚拟私有云）的安全策略里不需要设置很复杂的网络策略，只需要开放出向443端口并且阻断一切的入向连接即可。

为了便于理解连接服务器与边缘安全服务器之间的会话连接的建立过程，下面结合附图进行说明。如图4所示，假设连接服务器的服务器配置信息中包括的边缘安全服务器的域名为“abc.yundun-tunnel.com”，连接服务器将该域名“abc.yundun-tunnel.com”的解析请求发送给域名服务器。域名服务器对该域名解析后将解析得到的IP地址发送给连接服务器。连接服务器根据该IP地址建立与边缘安全服务器之间的会话连接，该会话连接是建立在443端口上的。连接服务器基于超文本传输协议http2通过该会话与边缘安全服务器进行数据通信。连接服务器的防火墙只需要开放443端口并阻断所有入向连接即可。

如图5所示，边缘安全服务器上维护连接服务器的标识信息与会话之间的映射关系。图5中IP地址为“1.1.1.1”的边缘安全服务器分别与连接服务器1、2和3中的一个连接器建立了会话连接。因此边缘安全服务器上维护的映射关系中包括连接器12345：会话1、连接器34567：会话2以及连接器45678：会话3。

管理平台上创建了连接器及设置好目标应用对应的应用配置信息，以及连接服务器中安装连接器，且连接器与边缘安全服务器建立会话连接，并将允许进行远程访问的所有目标应用的域名均解析到边缘加速服务器的IP地址上，从而将这些目标应用直接发布在公网中。之后远程终端即可通过本公开实施例提供的方法来访问目标应用。

步骤107：边缘加速服务器接收目标终端发送的针对目标应用的访问请求，该访问请求包括目标应用的域名。

边缘加速服务器上提供了DDoS（Distributed Denial of Service，分布式拒绝服务）清洗、缓存加速、WAF（Web Application Firewall，Web应用防护系统）、负载均衡等功能，同时还作为边缘安全网关提供身份认证、权限管理、访问控制等功能。目标用户在访问目标应用时，先访问到边缘加速服务器。

在一具体应用场景中，在家办公或出差的员工需要访问公司内网中的目标应用时，通过目标终端查看公司在公网上发布的多个目标应用，从中选择自己需要访问的目标应用，例如可以通过点击的方式进行选择。目标终端监测到某个目标应用被点击时，获取被点击的目标应用的域名，发送针对该目标应用的域名的解析请求给域名服务器。域名服务器对该目标应用的域名进行解析，由于之前将发布到公网上的所有目标应用的域名均解析到了边缘加速服务器的 IP 地址上，因此域名服务器对当前的目标应用的域名进行解析能够得到对应的边缘加速服务器的 IP 地址。域名服务器将域名解析得到的 IP 地址返回给该目标终端。目标终端根据该 IP 地址，发送访问请求给对应的边缘加速服务器，该访问请求中包括目标用户需要访问的目标应用的域名。

在本公开的另一些实施例中，边缘加速服务器还可以记录目标用户的访问行为日志，该访问行为日志中可以包括访问时间、访问对象、身份信息等，这些信息可以便于企业的安全管理人员对用户的行为进行审计和管控。

步骤 108：边缘加速服务器根据目标应用的域名，确定与目标应用的域名对应的边缘安全服务器的地址信息。

在本公开一示例性实施例中，边缘加速服务器可以预先从管理平台中获取各目标应用对应的应用配置信息以及连接服务器的服务器配置信息。需要说明的，边缘加速服务器可以直接从管理平台中获取，也可以从配置中心等中间媒介获取该信息，本公开对此不作特殊限定。

当边缘加速服务器接收到针对目标应用的访问请求之后，可以获取该访问请求中所包含的目标应用的域名，根据该目标应用的域名，确定其对应的应用配置信息，再根据该应用配置信息确定与该目标应用相关联的连接服务器的标识信息。基于所确定的连接服务器的标识信息，确定对应的服务器配置信息，由此，可以从该服务器配置信息中获取与该连接服务器相关联的边缘安全服务器的地址信息。

可以理解的，该地址信息可以包括域名和/或 IP 地址，若该地址信息为域名，则边缘加速服务器可以将该边缘安全服务器的域名解析请求发送至域名服务器中进行解析，以使域名服务器反馈对应的边缘安全服务器的 IP 地址。

需要说明的，边缘安全服务器的地址信息可以是一个也可以是多个，例如具有多个边缘安全服务器的 IP 地址，或者域名服务器反馈的域名对应的 IP 地址为一个或者多个，等等。多个地址信息所对应的边缘安全服务器，有的可以作为主用的边缘安全服务器，其他的则可以作为备用的边缘安全服务器。

在本公开另一示例性实施例中，边缘加速服务器向管理平台请求或接受管理平

台关于目标应用的应用配置信息的推送。管理平台根据边缘加速服务器发送的包含该目标应用的域名的查询请求，查询该目标应用的应用配置信息，从该应用配置信息中获取与该目标应用相关联的连接服务器的标识信息，然后根据该标识信息获取该连接服务器的服务器配置信息，从该服务器配置信息中获取与该连接服务器关联的边缘安全服务器的地址信息，发送该边缘安全服务器的地址信息给边缘加速服务器。

在本公开一示例性实施例中，在确定与目标应用的域名对应的边缘安全服务器的地址信息之前，边缘加速服务器可以对用户的身份信息执行认证策略，该认证策略可以包括身份认证策略和/或访问权限认证策略。

具体地，在对用户的身份信息执行身份认证策略时，边缘加速服务器可以在接收到访问请求后，检测该访问请求中是否携带目标用户的身份信息，因为该用户在首次访问时访问请求中是不会携带有身份信息的。若边缘加速服务器检测到访问请求中不包括用户身份信息，则触发身份认证操作。需要说明的，图 1 所示的认证中心可以是设置于边缘加速服务器中的认证组件，或者独立于边缘加速服务器的认证设备，该认证中心可以与第三方身份认证系统或内网中的内部身份认证系统进行数据交互。

其中，第三方身份认证系统通过互联网即可访问，内网中的内部身份认证系统则需要通过边缘加速服务器、边缘安全服务器和连接服务器来访问。在一示例中，通过互联网访问第三方身份认证系统，或通过边缘加速服务器和边缘安全服务器访问内网中的内部身份认证系统，第三方身份认证系统或内网中的内部身份认证系统可以向认证中心返回目标用户的身份信息。需要说明的，若认证中心接收到返回的身份信息，则可以认定该身份信息已经通过身份认证，可以进行后续步骤。

在其他示例中，认证中心也可以向边缘加速服务器发送一个身份认证页面。边缘加速服务器可以将该身份认证页面发送给目标终端，目标终端显示该身份认证页面，该身份认证页面中包括至少一个身份认证选项。例如，该身份认证页面中可以包括但不限于微信认证、企业微信认证、手机号认证等多个身份认证选项，用户可以选择对应的身份认证选项，从而确定对应的身份认证策略。例如，用户选择了微信认证这一选项，则可以通过该用户的微信号、微信密码等信息对该用户进行身份认证，等等。当目标用户选择对应的身份认证选项后，该身份认证页面则可以对应获取目标用户与该身份认证选项相对应的待验证身份信息，例如用户选择了微信认证，则获取对应的微信号和微信密码，等等。认证中心可以将身份认证页面所接收到的待验证身份信息向对应的第三方身份认证系统或者内部身

份认证系统进行认证，由第三方身份认证系统或内部身份认证系统反馈验证结果，即是否通过身份认证。

通过身份认证后，边缘加速服务器会为此次身份认证所基于的用户身份信息设置有效期，存储该用户身份信息及其对应的有效期，并指示后续该目标终端每次请求访问目标应用时都会在访问请求中携带该用户身份信息。

若检测结果为该访问请求中包含用户身份信息，则通过对应的认证策略包括的身份认证策略来对该用户身份信息进行认证。具体地，获取该用户身份信息对应的有效期，若确定其有效期未到达，则表明该用户身份信息之前已通过身份认证且尚在有效期内，无需再次进行身份认证，则直接确定当前用户身份认证通过。

若该检测结果为该访问请求包括用户身份信息，但该用户身份信息的有效期已到达，则根据边缘加速服务器中配置的身份认证策略对目标用户重新进行身份认证。

在本公开一示例性实施例中，在重新认证时，边缘加速服务器可以通过认证中心将该访问请求包括的目标用户的标识信息（例如用户账号等）发送给第三方身份认证系统。第三方身份认证系统根据该目标用户的标识信息获取目标用户的身份信息，并将该目标用户的身份信息反馈给认证中心。边缘加速服务器通过认证中心获得目标用户的身份信息后，根据预先配置的认证策略对该用户身份信息进行身份认证和/或访问权限认证。

在本公开一示例性实施例中，当认证中心需要从内部身份认证系统中获取目标用户的身份信息时，可以将目标用户的标识信息通过边缘加速服务器、边缘安全服务器和连接服务器发送给内网中的内部身份认证系统，以从内部身份认证系统获取目标用户的身份信息。具体地，在一示例中，边缘加速服务器可以发送该目标应用的域名给管理平台，管理平台从与该目标应用相关联的连接服务器对应的服务器配置信息中获取与该连接服务器对应的边缘安全服务器的地址信息，发送该边缘安全服务器的地址信息给边缘加速服务器。若该地址信息包括边缘安全服务器的 IP 地址，则边缘加速服务器根据该 IP 地址，建立与该边缘安全服务器之间的通信连接，并发送访问请求包括的目标用户的标识信息及目标应用的域名给该边缘安全服务器。若该地址信息中仅包括边缘安全服务器的域名，则边缘加速服务器发送该边缘安全服务器的域名的解析请求给域名服务器。域名服务器对边缘安全服务器的域名进行域名解析，得到边缘安全服务器的 IP 地址，发送该 IP 地址给边缘加速服务器。边缘加速服务器根据该 IP 地址建立与该边缘安全服务器之间

的通信连接，发送携带访问请求包括的目标用户的标识信息及目标应用的域名给该边缘安全服务器。

边缘安全服务器可以发送包含该目标应用的域名的查询目标应用相关联的连接服务器的请求给管理平台。管理平台根据该域名从该目标应用对应的应用配置信息中获取与该目标应用相关联的连接服务器的标识信息，发送该连接服务器的标识信息给边缘安全服务器。边缘安全服务器根据该连接服务器的标识信息，从连接服务器的标识信息与会话连接的映射关系中获取该连接服务器对应的会话连接，通过该会话连接将目标用户的标识信息发送给该连接服务器。连接服务器接收到该目标用户的标识信息后，将该目标用户的标识信息转发给该目标应用所属的内网中的内部身份认证系统，内部身份认证系统根据该目标用户的标识信息获取该目标用户的身份信息，并将目标用户的身份信息依次经过该连接服务器、上述边缘安全服务器原路返回给上述边缘加速服务器对应的认证中心。

在另一示例中，边缘安全服务器也可以不向管理平台查询对应的连接服务器的标识信息，而是由边缘加速服务器根据目标应用的域名从管理平台获取该目标应用对应的应用配置信息，并将用户身份信息及该应用配置信息一并发送给边缘安全服务器。边缘安全服务器从该应用配置信息中查询目标应用关联的连接服务器的标识信息，进而依据该标识信息，通过与该连接服务器之间的会话连接将目标用户的标识信息转发至对应的内网中的内部身份认证系统。该内部身份认证系统根据该目标用户的标识信息获取该目标用户的身份信息，并将目标用户的身份信息通过原路返回给边缘加速服务器对应的认证中心。

在本公开的另一些实施例中，也可以不通过首次认证后设置用户身份信息的有效期的方式，而是可以在每次访问时都由边缘加速服务器指示目标终端显示上述身份认证页面，用户对身份认证页面包括的每个身份认证选项进行选择后，目标终端根据用户选择的每个选项信息确定对应的用户身份信息，例如以该用户在该选项对应的应用的登录信息作为用户身份信息，在发送访问请求给边缘加速服务器时，在该访问请求中携带该用户身份信息。然后边缘加速服务器通过认证中心将该用户身份信息转发给第三方身份认证系统或内网中的内部身份认证系统对该用户身份信息进行认证，并将认证结果反馈给认证中心。

通过上述任一方式对访问请求包括的用户身份信息进行身份认证，若认证未通过，则发送错误提示信息给目标终端，该错误提示信息用于提示用户身份认证失败。若身份认证通过，且边缘加速服务器中部署的认证策略中仅包括身份认证

策略，则确定对该目标用户认证通过。若认证策略中还包括访问权限认证策略，则还需要根据访问权限控制策略判断用户是否具有目标应用的访问权限。访问权限控制策略中可以规定能够访问该目标应用的用户身份，比如一些财务相关的目标应用可能只允许财务人员访问，一些人事管理相关的目标应用可能只允许人力资源部门的人员访问，等等。或者，访问权限控制策略中可以规定该目标应用的访问口令，访问口令可以为一个字符串构成的密码，或者为约定好的一句话等。

边缘加速服务器对目标用户进行访问权限认证，可以指示目标终端显示权限认证界面，该权限认证界面中包括一个或多个权限认证选项。例如，权限认证选项可以包括工号、姓名、联系方式、身份证号、访问口令等选项中的一个或多个。用户在该权限认证界面中提交认证选项信息后，目标终端将该认证选项信息发送给边缘加速服务器。边缘加速服务器可以发送目标应用的域名给管理服务器，管理服务器根据目标应用的域名，从该目标应用的应用配置信息中获取该目标应用的访问权限的相关配置信息，该访问权限的相关配置信息中可以包括能够访问该目标应用的用户的工号、姓名、联系方式、身份证号等用户信息，和/或，该访问权限的相关配置信息中还可以包括该目标应用的访问口令。管理平台将该访问权限的相关配置信息发送给边缘加速服务器。边缘加速服务器根据该访问权限的相关配置信息和用户提交的认证选项信息，来判断该目标用户是否具有访问该目标应用的权限。

或者，管理平台也可以直接将该目标应用的应用配置信息发送给边缘加速服务器。边缘加速服务器从该应用配置信息中获取访问权限的相关配置信息，并据此判断该目标用户是否具有访问权限。例如，在应用配置信息中可以包括允许访问该目标应用的岗位名称，例如某一应用可以由财务、经理进行访问，等等。而用户的身份信息可以包括该用户的岗位名称，边缘加速服务器可以将用户的岗位名称与目标应用对应的岗位名称进行比对，若用户的岗位名称与该目标应用对应的岗位名称相匹配，即该用户的岗位名称是允许访问该目标应用的岗位名称之一，则表示该用户通过访问权限认证策略，反之则未通过。

或者，边缘加速服务器也可以不从管理平台获取访问权限的相关配置信息或该目标应用的应用配置信息。而是确定与该目标应用关联的连接服务器，及与该连接服务器管理的边缘安全服务器，然后将该目标用户的认证选项信息依次经过该边缘安全服务器和连接服务器转发给内网中的内部身份认证系统，以对目标用

户的认证选项信息进行权限认证，并将认证结果原路返回给边缘加速服务器。

因通过上述任一方式对目标用户进行访问权限认证，实现了在边缘加速服务器通过访问权限控制策略进行细粒度的访问权限控制，能够有效消除恶意分子对目标应用恶意攻击的风险。

请继续参照图 2，步骤 109：边缘加速服务器根据边缘安全服务器的地址信息，转发该访问请求至边缘安全服务器。

在本公开一示例性实施例中，若边缘安全服务器的地址信息包括边缘安全服务器的 IP 地址，则边缘加速服务器根据该 IP 地址，直接将该访问请求转发给边缘安全服务器。若该地址信息中仅包括边缘安全服务器的域名，则边缘加速服务器发送该边缘安全服务器的域名解析请求给域名服务器。域名服务器对边缘加速服务器发送的域名进行域名解析，得到对应的每个边缘安全服务器的 IP 地址，将得到的每个 IP 地址组成 IP 列表，返回该 IP 列表给边缘加速服务器，该 IP 列表中包括一个或多个边缘安全服务器的 IP 地址。

边缘加速服务器接收域名服务器返回的 IP 列表，从该 IP 列表中选择一个 IP 地址。具体地，若该 IP 列表中仅包括一个 IP 地址，则直接选择该 IP 地址。若该 IP 列表中包括多个 IP 地址，则从这多个 IP 地址中选择一个主用的边缘安全服务器的 IP 地址。边缘加速服务器根据选择的 IP 地址，建立与选择的 IP 地址对应的边缘安全服务器之间的通信连接，然后发送该访问请求给该边缘安全服务器。

在本公开的另一些实施例中，在发送该访问请求给边缘安全服务器之前，边缘加速服务器还可以与边缘安全服务器进行双向认证，进一步确保目标应用访问的安全性。例如，边缘加速服务器发送自身的第一证书给边缘安全服务器。该边缘安全服务器接收边缘加速服务器的第一证书，并对第一证书进行验证，验证第一证书是否由自己新来的 CA 中心所签发，若是则表示验证通过，若不是，则可以向边缘加速服务器返回一个警告信息，警告边缘加速服务器这个第一证书不是可以信赖的。验证通过后，边缘安全服务器可以比较证书里的信息，例如域名和公钥，若该域名或公钥符合预先设定的信息传输规则，则认可该边缘加速服务器的合法身份

边缘加速服务器也可以要求边缘安全服务器发送其自身的第二证书，收到该第二证书之后，边缘加速服务器可以对该第二证书进行验证，若没有通过验证，则拒绝连接，若通过验证，则二者之间可以进行信息传输。

在本公开实施例中，边缘加速服务器与边缘安全服务器之间通过上述方式进行双向认证，第一证书和第二证书中只要有一个认证不通过，边缘加速服务器就不

会将访问请求发送给边缘安全服务器，大大提高了内网访问的安全性。边缘加速服务器还可以先对访问请求进行加密，将加密后的数据发送给边缘安全服务器，以提高数据传输的安全性。

步骤 110：边缘安全服务器接收由边缘加速服务器转发的针对目标应用的访问请求，确定与目标应用对应的目标连接服务器。

在本公开一示例性实施例中，边缘安全服务器是一个中转媒介，可以实现边缘加速服务器与目标应用的打通，当目标应用位于内网，可以实现边缘加速服务器与内网应用的打通。边缘安全服务器启动后，等待边缘加速服务器和连接服务器中连接器的连接并转发来自边缘加速服务器的访问请求。

边缘安全服务器接收到边缘加速服务器转发的目标终端对目标应用的访问请求后，将该访问请求中包括的目标应用的域名发送给管理平台。管理平台根据该目标应用的域名，获取该目标应用的应用配置信息，从该应用配置信息中查询与该目标应用相关联的连接服务器的标识信息，与该目标应用相关联的连接服务器即为目标连接服务器，管理平台将该目标连接服务器的标识信息发送给边缘安全服务器。边缘安全服务器接收该目标连接服务器的标识信息。

在本公开的另一些实施例中，也可以由边缘加速服务器在对目标用户进行认证的阶段从管理平台获取目标应用的应用配置信息及与该目标应用相关联的连接服务器的服务器配置信息，并由边缘加速服务器将访问请求及应用配置信息一并转发给边缘安全服务器。如此边缘安全服务器可以在本地从应用配置信息中获取与该目标应用相关联的连接服务器的标识信息，并确定该标识信息即为目标连接服务器的标识信息。

在本公开再一示例性实施例中，边缘加速服务器在向边缘安全服务器转发该访问请求时，可以将该访问请求对应的目标应用的应用配置信息一起向边缘安全服务器进行发送。由此，边缘安全服务器可以根据该应用配置信息中所包括的与该目标应用相关联的连接服务器的标识信息，确定目标连接服务器。可以理解的，边缘安全服务器确定出的目标连接服务器的数量可以为一个或多个。

若目标连接器的数量为多个即两个或者两个以上的任意数量，则其中一个目标连接服务器可以作为主目标连接服务器，除主目标连接服务器之外的为副目标连接服务器，从而在主目标连接服务器失效或者故障时，可以通过副目标连接服务器进行访问目标应用。

可以理解的，主目标连接服务器和副目标连接服务器二者相关联的目标应用应是相同的，或者主目标连接服务器所关联的目标应用被包含于副目标连接服务器

所关联的目标应用中，又或者主目标连接服务器与副目标连接服务器之间具有部分相同的相关联的目标应用，等等。

步骤 111：边缘安全服务器根据与目标连接服务器对应的会话连接，转发访问请求至目标连接服务器。

在本公开一示例性实施例中，边缘安全服务器根据确定出的每个目标连接服务器的标识信息，从本地存储的连接服务器的标识信息与会话之间的映射关系中，分别获取每个连接服务器对应的会话连接。通过每个连接服务器对应的会话连接，将该访问请求转发给每个目标连接服务器。

在本公开一示例性实施例中，边缘安全服务器在将访问请求转发给目标连接服务器前，还可以通过与连接服务器对应的会话连接获取连接服务器的健康状态信息，该健康状态信息包括连接服务器的负载状态信息、网络状态信息、系统状态信息、磁盘状态信息中的一种或多种。具体地，边缘安全服务器通过与每个连接服务器对应的会话连接发送健康检查请求给每个连接服务器。连接服务器中的连接器接收到该健康检查请求后获取自身的健康状态信息，通过与该边缘安全服务器之间的会话连接将健康状态信息发送给该边缘安全服务器。

边缘安全服务器根据每个连接服务器的健康状态信息，从每个连接服务器中选择一个满足预设健康条件的连接服务器，预设健康条件可以包括负载量小于预设阈值，网络状态、系统状态和磁盘状态无异常，预设健康条件中可以列举出网络状态、系统状态和磁盘状态的一些异常情况，如网络中断、系统资源占用率超过预设比例、磁盘剩余存储空间小于预设值等。若边缘安全服务器确定出多个满足预设健康条件的连接服务器，则可从中随机选取或者依次选取以确定一个目标连接服务器。在确定目标连接服务器之后，边缘安全服务器可以根据该目标连接服务器的标识信息对应的会话连接，将该访问请求转发至该目标连接服务器中的连接器。

在本公开的另一些实施例中，边缘安全服务器还可以通过轮询的方式来将访问请求转发给连接服务器中的连接器。具体地，边缘安全服务器中配置了预设轮询规则，预设轮询规则中规定了该目标应用关联的每个目标连接服务器的轮询顺序，根据该轮询顺序从与该目标应用关联的每个目标连接服务器中选择一个目标连接服务器。根据选择的目标连接服务器的标识信息，从标识信息与会话的映射关系中获取选择的目标连接服务器对应的会话连接，通过获取的会话连接将该访问请求转发给该目标连接服务器。

为了便于理解目标终端的访问请求发送至目标连接服务器的流程，下面结合附

图进行说明。如图 6 所示，远程终端发送访问请求给边缘加速服务器，该访问请求包括待访问的目标应用的域名“oa.companyA.com”。边缘加速服务器根据该域名，从管理平台获取域名“oa.companyA.com”对应的应用配置信息，该应用配置信息中绑定的连接器的唯一标识为“12345”，也从管理平台获取连接器 12345 的服务器配置信息。边缘加速服务器获得该应用配置信息和服务器配置信息后，发送服务器配置信息包括的边缘安全服务器的域名“companyA.connector.com”的解析请求给域名服务器，接收域名服务器返回的该边缘安全服务器的 IP 地址“1.1.1.1”。边缘加速服务器根据该 IP 地址“1.1.1.1”建立与该边缘安全服务器之间的通信连接，将访问请求及应用配置信息发送给该边缘安全服务器。IP 地址为“1.1.1.1”的边缘安全服务器根据应用配置信息中包括的连接器的唯一标识“12345”，从预存的映射关系中获得该连接器对应的会话连接，通过该会话连接将该访问请求发送给企业 A 的连接服务器 1 中的连接器 12345。

步骤 112：连接服务器基于与边缘安全服务器之间的会话连接，若接收到由边缘安全服务器转发的针对目标应用的访问请求，将该访问请求发送至目标应用。

在本公开实施例中，连接服务器中可以配置有与其关联的每个目标应用的域名与回源地址的映射关系。或者管理平台可以将每个目标应用的回源地址或应用配置信息下发给连接服务器。连接服务器若接收到边缘安全服务器通过二者之间的会话连接发送的针对目标应用的访问请求，则连接服务器根据该访问请求包括的目标应用的域名，在本地查询目标应用的回源地址，根据该回源地址，将该访问请求转发给对应的目标应用。

在本公开的另一些实施例中，连接服务器中也可以不配置相关联的目标应用的域名与回源地址的映射关系。而是由边缘安全服务器从管理平台或者边缘加速服务器处获得该目标应用对应的应用配置信息，该应用配置信息中包括目标应用对应的回源地址，边缘安全服务器在将该访问请求转发给目标连接服务器中对应的连接器时还可以将该回源地址发送给连接器。连接器根据该回源地址，将该访问请求转发给对应的目标应用。目标应用对该访问请求进行响应，将生成的响应消息传输给与该目标应用关联的连接服务器。

步骤 113：连接服务器将接收到的请求响应信息向边缘安全服务器进行发送，该请求响应信息由目标应用根据访问请求进行反馈。

在本公开一示例性实施例中，目标应用根据访问请求进行反馈生成请求响应信息，发送该请求响应信息给该连接服务器。该连接服务器再通过自身与边缘安全服务器之间的会话连接将该请求响应信息发送给边缘安全服务器。边缘安全服务

器将该请求响应信息发送给边缘加速服务器，边缘加速服务器再将该请求响应信息发送给该目标终端。

在本公开实施例中，连接服务器与边缘安全服务器之间的会话连接的传输协议可以为加密传输协议，连接服务器与边缘安全服务器之间的数据都是加密传输，以确保传输过程中的数据安全性。

在本公开实施例中，多个连接服务器可以与相同的目标应用关联，对于该相同的目标应用来说，其关联的多个连接服务器可以包括主用连接服务器和备用连接服务器，在主用连接服务器故障时，可以通过备用连接服务器对应的会话连接接收目标终端对目标应用的访问请求，或通过备用连接服务器对应的会话连接发送目标应用对访问请求进行响应而产生的请求响应信息。一个连接服务器中也可以包括多个连接器，分成主连接器和副连接器，在主连接器故障或者达到负载上限后，由副连接器来进行数据传输。

另外，连接服务器还可以每隔预设时间段（例如 2min、0.5h 或者 1h 等）发送自身的健康状态信息及每个连接器的健康状态信息给管理平台，管理平台根据连接服务器的健康状态信息及每个连接器的健康状态信息判断连接服务器及连接器是否出现异常，若有异常则及时向管理人员发出告警信息。

为了便于理解本公开实施例提供的应用访问过程，下面结合附图进行说明。如图 7 所示，连接服务器 A 中的连接器 1 和 2，以及连接服务器 B 中的连接器 3 和 4 均根据各自的配置信息中的边缘安全服务器的域名，从域名服务器获取对应的边缘安全服务器的 IP 地址，然后依据获取的 IP 地址建立与边缘安全服务器之间的会话连接。

远程用户发送访问请求给边缘加速服务器，该访问请求包括目标应用的域名。边缘加速服务器确定访问请求中是否包括尚在有效期内的用户身份信息，如果是，则确定身份认证通过。如果否，则边缘加速服务器重定向至身份认证页面，获得当前用户的用户身份信息。边缘加速服务器从管理平台获取待访问的目标应用的应用配置信息和与该目标应用关联的连接服务器的服务器配置信息。边缘加速服务器根据该应用配置信息包括的身份认证策略对获得的用户身份信息进行身份认证。身份认证通过后，边缘加速服务器将服务器配置信息包括的边缘安全服务器的域名的域名解析请求发送给域名服务器，根据域名服务器返回的边缘安全服务器的 IP 地址，将访问请求和应用配置信息发送到边缘安全服务器中。如图 7 所示，域名“A.yundun-tunnel.com”对应于 IP 地址分别为“1.1.1.1”和“2.2.2.2”的两个边缘安全服务器，IP 地址为“1.1.1.1”的边缘安全服务器为主用的边缘安全服务器，

IP 地址为“2.2.2.2”的边缘安全服务器为备用的边缘安全服务器。域名“B.yundun-tunnel.com”对应于 IP 地址分别为“3.3.3.3”和“4.4.4.4”的两个边缘安全服务器，IP 地址为“3.3.3.3”的边缘安全服务器为主用的边缘安全服务器，IP 地址为“4.4.4.4”的边缘安全服务器为备用的边缘安全服务器。

假设访问请求是对连接服务器 A 中的目标应用的访问，则边缘加速服务器可以将访问请求及应用配置信息发送到 IP 地址为“1.1.1.1”的边缘安全服务器。边缘安全服务器再通过与连接器 1 或连接器 2 之间的会话连接将访问请求发送给连接服务器 A。

在本公开实施例中，不需要使用 VPN 服务器即可实现目标终端访问连内网中的目标应用，解决了 VPN 服务器不稳定且难以维护的问题。直接将目标应用发布到公网上，用户访问体验更好。由边缘加速服务器对用户身份及访问权限进行认证，消除了恶意攻击的风险。不需要对原有的网络拓扑进行修改即可将内网中的目标应用 SaaS 化。且通过增加边缘加速服务器和边缘安全服务器的数量，能够很方便地进行扩容，能够适应目标用户数量很大的应用场景。

本公开的另一些实施例提供了一种远程访问应用的方法，该方法应用于连接服务器。参见图 8，该方法具体包括以下步骤：

步骤 201：连接服务器获取与连接服务器对应的至少一个边缘安全服务器的地址信息。

在本公开一示例性实施例中，连接服务器由管理平台中获取连接服务器对应的服务器配置信息。在一示例中，连接服务器可以直接从管理平台中获取服务器配置信息。在另一示例中，连接服务器也可以通过中间媒介间接从管理平台获取服务器配置信息，例如管理平台将该连接服务器的服务器配置信息下发至配置中心，连接服务器再从配置中心获取该服务器配置信息。连接服务器获得服务器配置信息后，从该服务器配置信息中获取与连接服务器对应的至少一个边缘安全服务器的地址信息。该地址信息包括边缘安全服务器的 IP 地址和/或域名。

步骤 202：连接服务器根据至少一个边缘安全服务器的地址信息，建立与至少一个边缘安全服务器之间的会话连接，所述会话连接为由连接服务器至所述至少一个边缘安全服务器的出站连接。

在本公开一示例性实施例中，若边缘安全服务器的地址信息中仅包括 IP 地址，则连接服务器根据至少一个边缘安全服务器的 IP 地址，建立与这至少一个边缘安

全服务器之间的会话连接。若边缘安全服务器的地址信息中仅包括边缘安全服务器的域名，则连接服务器发送这至少一个边缘安全服务器的域名给域名服务器；接收域名服务器返回的每个域名对应的 IP 地址；根据每个 IP 地址，分别发送连接请求给一个或多个边缘安全服务器，连接请求包括连接服务器的标识信息，以建立连接服务器与一个或多个边缘安全服务器之间的会话连接。

值得注意的是，该会话连接为连接服务器到边缘安全服务器之间的出站连接，其是连接服务器主动向外的通信连接，该连接服务器禁止任何入向的连接请求，从而可以避免遭受他人的恶意攻击，保证目标应用的安全性。在一示例中，可以在连接服务器中配置禁止入向的连接请求，从而使连接服务器能够通过防火墙禁止除上述建立的会话连接以外的所有入向的请求。

在一示例中，该会话连接的传输协议为加密传输协议，即通过该会话连接进行传输的数据均通过加密后以密文的形式进行传输，以提高数据传输的安全性。

步骤 203：连接服务器基于建立的会话连接，若接收到由边缘安全服务器转发的针对目标应用的访问请求，将访问请求发送至目标应用。

步骤 204：连接服务器将接收到的请求响应信息向边缘安全服务器进行发送，该请求响应信息由目标应用根据访问请求进行反馈。

在本公开实施例中，连接服务器可以包括主连接服务器和副连接服务器，在主连接服务器故障时使用副连接服务器。连接服务器中可以部署多个连接器，多个连接器中包括主用连接器和备用连接器，主用连接器和备用连接器与相同的目标应用关联；在主用连接器故障时，通过备用连接器对应的会话连接接收目标终端对目标应用的访问请求。

连接服务器还每隔预设时间段发送连接器的健康状态信息给管理平台，健康状态信息包括连接器的负载状态信息、网络状态信息、系统状态信息、磁盘状态信息中的一种或多种。

连接服务器还可以通过连接器对应的会话连接接收边缘安全服务器发送的健康检查请求，通过该会话连接发送连接器的健康状态信息给边缘安全服务器。

在本公开实施例中，连接服务器的具体操作细节均可参考上述任一实施例中连接服务器的操作，在此不再赘述。

在本公开实施例中，连接服务器通过连接器建立与边缘安全服务器之间的会话连接，通过该会话连接实现目标终端对目标应用的访问。不需要使用 VPN 服务

器，解决了 VPN 服务器不稳定且难以维护的问题。直接将目标应用发布到公网上，用户访问体验更好。不需要对原有的网络拓扑进行修改即可将内网中的目标应用 SaaS 化。

本公开的一些实施例提供了一种远程访问应用的方法，该方法应用于边缘安全服务器，参见图 9，该方法具体包括以下步骤：

步骤 301：边缘安全服务器接收由至少一个连接服务器发送的连接请求。

在一示例中，连接请求的数量可以为多个，连接请求中包含对应的连接服务器的标识信息。

步骤 302：边缘安全服务器根据连接请求，建立与至少一个连接服务器之间的会话连接。

在一示例中，边缘安全服务器根据多个连接请求，分别建立与至少一个连接服务器之间的会话连接，并将各连接服务器的标识信息与对应的会话连接相关联。

步骤 303：边缘安全服务器接收由边缘加速服务器转发的针对目标应用的访问请求，确定与目标应用对应的目标连接服务器。

步骤 304：边缘安全服务器根据与目标连接服务器对应的会话连接，转发访问请求至目标连接服务器。

在一示例中，目标连接服务器的数量可以为多个，边缘安全服务器根据与多个目标连接服务器的标识信息相关联的会话连接，转发访问请求至每个目标连接服务器。

具体地，边缘安全服务器从应用配置信息中提取出与目标应用关联的每个连接服务器的标识信息；根据每个连接服务器的标识信息，从映射关系中分别获取每个连接服务器对应的会话连接；通过每个连接服务器对应的会话连接分别获取每个连接服务器的健康状态信息；根据每个连接服务器的健康状态信息，从每个连接服务器中选择一个满足预设健康条件的目标连接服务器，通过选择的目标连接服务器对应的会话连接将访问请求转发给目标连接服务器。

在本公开的另一些实施例中，边缘安全服务器还可以轮询的机制来转发访问请求。具体地，从应用配置信息中提取出与目标应用关联的每个连接服务器的标识信息；根据预设轮询规则，从每个连接服务器中选择一个目标连接服务器；根据选择的目标连接服务器的标识信息，从映射关系中获取选择的目标连接服务器

对应的会话连接；通过获取的会话连接将访问请求转发给目标连接服务器。

边缘安全服务器的具体操作细节均可参考上述任一实施例中边缘安全服务器的操作，在此不再赘述。

在本公开实施例中，边缘安全服务器建立了与连接服务器中的连接器之间的会话连接，通过该会话连接将来自目标终端的访问请求转发给连接服务器，不使用 VPN 服务器就能实现目标终端对目标应用的访问，解决了 VPN 服务器不稳定且难以维护的问题。不需要对原有的网络拓扑进行修改即可将内网中的目标应用 SaaS 化。且通过增加边缘安全服务器的数量，能够很方便地进行扩容，能够适应目标用户数量很大的应用场景。

本公开的一些实施例提供了一种远程访问应用的方法，该方法应用于边缘加速服务器，参见图 10，该方法具体包括以下步骤：

步骤 401：边缘加速服务器接收由目标终端发送的针对目标应用的访问请求，访问请求包含目标应用的域名。

步骤 402：边缘加速服务器根据目标应用的域名，确定与目标应用的域名对应的边缘安全服务器的地址信息。

在本公开一示例性实施例中，在确定与目标应用的域名对应的边缘安全服务器的地址信息之前，边缘加速服务器还可以检测访问请求中是否携带目标用户的身份信息；根据检测结果，对目标用户的身份信息执行与所述检测结果对应的认证策略，认证策略包括身份认证策略和/或访问权限认证策略；若目标用户的身份信息通过认证策略的认证，则根据目标应用的域名，确定与目标应用的域名对应的边缘安全服务器的地址信息。

步骤 403：边缘加速服务器根据边缘安全服务器的地址信息，转发访问请求至边缘安全服务器。

边缘加速服务器的具体操作细节均可参考上述任一实施例中边缘加速服务器的操作，在此不再赘述。

在本公开实施例中，边缘加速服务器对用户身份及访问权限进行认证，消除了恶意攻击的风险。边缘加速服务器将访问请求及应用配置信息转发给边缘安全服务器，再通过边缘安全服务器将访问请求转发给连接服务器，不需要使用 VPN 服务器即可实现目标终端访问连接服务器中的目标应用，解决了 VPN 服务器不稳定

且难以维护的问题。直接将目标应用发布到公网上，用户访问体验更好。不需要对原有的网络拓扑进行修改即可将内网中的目标应用 SaaS 化。且通过增加边缘加速服务器和边缘安全服务器的数量，能够很方便地进行扩容，能够适应目标用户数量很大的应用场景。

本公开的一些实施例提供了一种远程访问应用的方法，该方法应用于管理平台，参见图 11，该方法具体包括以下步骤：

步骤 501：管理平台生成连接服务器对应的服务器配置信息，服务器配置信息至少包括连接服务器的标识信息和与连接服务器对应的边缘安全服务器的地址信息。

步骤 502：管理平台生成目标应用对应的应用配置信息，应用配置信息包括目标应用的域名、回源地址、相关联的连接服务器的标识信息、身份认证策略以及访问权限控制策略中的至少一种。

步骤 503：管理平台发送连接服务器所需的服务器配置信息。

步骤 504：管理平台发送边缘加速服务器所需的目标应用的应用配置信息以及与目标应用相关联的连接服务器的服务器配置信息。

管理平台的具体操作细节均可参考上述任一实施例中管理平台的操作，在此不再赘述。

在本公开实施例中，管理平台中生成了连接服务器的服务器配置信息，以及生成了目标应用的应用配置信息，将目标应用与连接服务器相关联。并通过管理平台发送服务器配置信息给连接服务器。再发送边缘加速服务器所需的目标应用的应用配置信息以及与目标应用相关联的连接服务器的服务器配置信息。不需要使用 VPN 服务器即可实现目标终端访问连接服务器中的目标应用，解决了 VPN 服务器不稳定且难以维护的问题。不需要对原有的网络拓扑进行修改即可将内网中的目标应用 SaaS 化，能够很方便地进行扩容，能够适应目标用户数量很大的应用场景。

本公开实施例提供了一种远程访问应用的系统，参见图 1，该系统包括：边缘加速服务器、边缘安全服务器、管理平台和连接服务器；

管理平台，设置为生成目标应用的应用配置信息，以及生成连接服务器对应的服务器配置信息；发送边缘加速服务器所需的目标应用的应用配置信息以及与

目标应用相关联的连接服务器的服务器配置信息，并发送连接服务器所需的服务器配置信息；

边缘加速服务器，设置为接收目标终端发送的针对目标应用的访问请求；并根据访问请求包含的目标应用的域名，将访问请求向对应的边缘安全服务器进行发送；

边缘安全服务器，设置为接收边缘加速服务器发送的访问请求；根据在先建立的与连接服务器的会话连接，将访问请求转发至对应的连接服务器；

连接服务器，设置为接收边缘安全服务器发送的访问请求，并将访问请求转发至对应的目标应用。

在一示例性实施例中，会话连接为连接服务器至边缘安全服务器的出站连接。

在一示例性实施例中，该系统还包括：认证中心，设置为根据访问请求携带的目标用户的身份信息，对目标用户的身份信息执行认证策略，认证策略包括身份认证策略和/或访问权限认证策略。

本公开的上述实施例提供的远程访问应用的系统与本公开实施例提供的远程访问应用的方法出于相同的发明构思，具有与其存储的应用程序所采用、运行或实现的方法相同的有益效果。

本公开实施例还提供一种远程访问应用的装置，该装置用于执行上述任一实施例提供的远程访问应用的方法中连接服务器的操作。参见图 12，该装置包括：

获取模块 601，设置为获取与连接服务器对应的至少一个边缘安全服务器的地址信息；

第一建立会话模块 602，设置为根据至少一个边缘安全服务器的地址信息，建立与至少一个边缘安全服务器之间的会话连接，会话连接为由连接服务器至至少一个边缘安全服务器的出站连接；

第一发送模块 603，设置为基于会话连接，若接收到由边缘安全服务器转发的针对目标应用的访问请求，将访问请求发送至目标应用；将接收到的请求响应信息向边缘安全服务器进行发送，请求响应信息由目标应用根据访问请求进行反馈。

上述地址信息为域名，第一建立会话模块 602，还设置为向域名服务器发送至少一个边缘安全服务器的域名；接收由域名服务器发送的至少一个边缘安全服务器的域名对应的 IP 地址；根据各 IP 地址，分别向至少一个边缘安全服务器发送连

接请求，以建立连接服务器与至少一个边缘安全服务器之间的会话连接，连接请求包含连接服务器的标识信息，以使至少一个边缘安全服务器将标识信息与对应的会话连接相关联。

获取模块 601，还设置为由管理平台中获取连接服务器对应的服务器配置信息；从服务器配置信息中获取与连接服务器对应的至少一个边缘安全服务器的地址信息。

上述会话连接的传输协议为加密传输协议。

本公开的上述实施例提供的远程访问应用的装置与本公开实施例提供的远程访问应用的方法出于相同的发明构思，具有与其存储的应用程序所采用、运行或实现的方法相同的有益效果。

本公开实施例还提供一种远程访问应用的装置，该装置用于执行上述任一实施例提供的远程访问应用的方法中边缘安全服务器的操作。参见图 13，该装置包括：

第一接收模块 701，设置为接收由至少一个连接服务器发送的连接请求；

第二建立会话模块 702，设置为根据连接请求，建立与至少一个连接服务器之间的会话连接；

第一接收模块 701，还设置为接收由边缘加速服务器转发的针对目标应用的访问请求；

第一确定模块 703，设置为确定与目标应用对应的目标连接服务器；

第二发送模块 704，设置为根据与目标连接服务器对应的会话连接，转发访问请求至目标连接服务器。

上述连接请求的数量为多个，连接请求中包含对应的连接服务器的标识信息；

第二建立会话模块 702，还设置为根据多个连接请求，分别建立与至少一个连接服务器之间的会话连接，并将各标识信息与对应的会话连接相关联。

目标连接服务器的数量为多个；第二发送模块 704，还设置为根据与多个目标连接服务器的标识信息相关联的会话连接，转发访问请求至目标连接服务器。

本公开的上述实施例提供的远程访问应用的装置与本公开实施例提供的远程访问应用的方法出于相同的发明构思，具有与其存储的应用程序所采用、运行或实现的方法相同的有益效果。

本公开实施例还提供一种远程访问应用的装置，该装置用于执行上述任一实施例提供的远程访问应用的方法中边缘加速服务器的操作。参见图 14，该装置包括：

第二接收模块 801，设置为接收由目标终端发送的针对目标应用的访问请求，访问请求包含目标应用的域名；

第二确定模块 802，设置为根据目标应用的域名，确定与目标应用的域名对应的边缘安全服务器的地址信息；

第三发送模块 803，设置为根据边缘安全服务器的地址信息，转发访问请求至边缘安全服务器。

第二确定模块 802，还设置为检测访问请求中是否携带目标用户的身份信息；根据检测结果，对目标用户的身份信息执行认证策略；若目标用户的身份信息通过认证策略的认证，则根据目标应用的域名，确定与目标应用的域名对应的边缘安全服务器的地址信息。上述认证策略包括身份认证策略和/或访问权限认证策略。

本公开的上述实施例提供的远程访问应用的装置与本公开实施例提供的远程访问应用的方法出于相同的发明构思，具有与其存储的应用程序所采用、运行或实现的方法相同的有益效果。

本公开实施例还提供一种远程访问应用的装置，该装置用于执行上述任一实施例提供的远程访问应用的方法中管理平台的操作。参见图 15，该装置包括：

生成模块 901，设置为生成连接服务器对应的服务器配置信息，服务器配置信息至少包括连接服务器的标识信息和与连接服务器对应的边缘安全服务器的地址信息；生成目标应用对应的应用配置信息，应用配置信息包括目标应用的域名、回源地址、相关联的连接服务器的标识信息、身份认证策略以及访问权限控制策略中的至少一种；

第四发送模块 902，设置为发送连接服务器所需的服务器配置信息；发送边缘加速服务器所需的目标应用的应用配置信息以及与目标应用相关联的连接服务器的服务器配置信息。

本公开的上述实施例提供的远程访问应用的装置与本公开实施例提供的远程访问应用的方法出于相同的发明构思，具有与其存储的应用程序所采用、运行或

实现的方法相同的有益效果。

本公开实施方式还提供一种电子设备，以执行上述远程访问应用的方法。请参考图 16，其示出了本公开的一些实施方式所提供的一种电子设备的示意图。如图 16 所示，电子设备 10 包括：处理器 1000，存储器 1001，总线 1002 和通信接口 1003，所述处理器 1000、通信接口 1003 和存储器 1001 通过总线 1002 连接；所述存储器 1001 中存储有可在所述处理器 1000 上运行的计算机程序，所述处理器 1000 运行所述计算机程序时执行本公开前述任一实施方式所提供的远程访问应用的方法。

其中，存储器 1001 可能包含高速随机存取存储器（RAM：Random Access Memory），也可能还包括非不稳定的存储器（non-volatile memory），例如至少一个磁盘存储器。通过至少一个通信接口 1003（可以是有线或者无线）实现该系统网元与至少一个其他网元之间的通信连接，可以使用互联网、广域网、本地网、城域网等。

总线 1002 可以是 ISA 总线、PCI 总线或 EISA 总线等。所述总线可以分为地址总线、数据总线、控制总线等。其中，存储器 1001 用于存储程序，所述处理器 1000 在接收到执行指令后，执行所述程序，前述本公开实施例任一实施方式揭示的所述远程访问应用的方法可以应用于处理器 1000 中，或者由处理器 1000 实现。

处理器 1000 可能是一种集成电路芯片，具有信号的处理能力。在实现过程中，上述方法的各步骤可以通过处理器 1000 中的硬件的集成逻辑电路或者软件形式的指令完成。上述的处理器 1000 可以是通用处理器，包括中央处理器（Central Processing Unit，简称 CPU）、网络处理器（Network Processor，简称 NP）等；还可以是数字信号处理器（DSP）、专用集成电路（ASIC）、现成可编程门阵列（FPGA）或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件。可以实现或者执行本公开实施例中的公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。结合本公开实施例所公开的方法的步骤可以直接体现为硬件译码处理器执行完成，或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器，闪存、只读存储器，可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器 1001，处理器 1000 读取存储器 1001 中的信息，

结合其硬件完成上述方法的步骤。

本公开实施例提供的电子设备与本公开实施例提供的远程访问应用的方法出于相同的发明构思，具有与其采用、运行或实现的方法相同的有益效果。

本公开实施方式还提供一种与前述实施方式所提供的远程访问应用的方法对应的计算机可读存储介质，请参考图 17，其示出的计算机可读存储介质为光盘 30，其上存储有计算机程序（即程序产品），所述计算机程序在被处理器运行时，会执行前述任意实施方式所提供的远程访问应用的方法。

需要说明的是，所述计算机可读存储介质的例子还可以包括，但不限于相变内存（PRAM）、静态随机存取存储器（SRAM）、动态随机存取存储器（DRAM）、其他类型的随机存取存储器（RAM）、只读存储器（ROM）、电可擦除可编程只读存储器（EEPROM）、快闪记忆体或其他光学、磁性存储介质，在此不再一一赘述。

本公开的上述实施例提供的计算机可读存储介质与本公开实施例提供的远程访问应用的方法出于相同的发明构思，具有与其存储的应用程序所采用、运行或实现的方法相同的有益效果。

需要说明的是：

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，本公开的实施例可以在没有这些具体细节的情况下实践。在一些实例中，并未详细示出公知的结构和技术，以便不模糊对本说明书的理解。

类似地，应当理解，为了精简本公开并帮助理解各个发明方面中的一个或多个，在上面对本公开的示例性实施例的描述中，本公开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。然而，并不应将该公开的方法解释成反映如下示意图：即所要求保护的本公开要求比在每个权利要求中所明确记载的特征更多的特征。更确切地说，如下面的权利要求书所反映的那样，发明方面在于少于前面公开的单个实施例的所有特征。因此，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公开的单独实施例。

此外，本领域的技术人员能够理解，尽管在此所述的一些实施例包括其它实施例中所包括的某些特征而不是其它特征，但是不同实施例的特征的组合意味着

处于本公开的范围之内并且形成不同的实施例。例如，在下面的权利要求书中，所要求保护的实施例的任意之一都可以以任意的组合方式来使用。

以上所述，仅为本公开的具体实施方式，但本公开的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本公开揭露的技术范围内，可轻易想到的变化或替换，都应涵盖在本公开的保护范围之内。因此，本公开的保护范围应以所述权利要求的保护范围为准。

工业实用性

在本公开实施例中，通过连接服务器的设置并建立连接服务器与边缘安全服务器之间的会话连接，该会话连接为连接服务器至边缘安全服务器之间的出站连接，使得用户不需要使用 VPN 服务器即可实现目标终端远程访问目标应用，解决了 VPN 服务器不稳定且难以维护的问题。同时，基于该会话连接，接收由边缘安全服务器转发的针对目标应用的访问请求，可以避免由其他服务器主动向连接服务器发送信息或者建立连接的情况发生，降低了遭受恶意攻击的风险，保证了目标应用的安全性。

权利要求

1、一种远程访问应用的方法，应用于连接服务器，所述连接服务器与至少一个目标应用相关联，包括：

获取与所述连接服务器对应的至少一个边缘安全服务器的地址信息；

根据所述至少一个边缘安全服务器的地址信息，建立与所述至少一个边缘安全服务器之间的会话连接，所述会话连接为由所述连接服务器至所述至少一个边缘安全服务器的出站连接；

基于所述会话连接，若接收到由边缘安全服务器转发的针对目标应用的访问请求，将所述访问请求发送至所述目标应用；

将接收到的请求响应信息向所述边缘安全服务器进行发送，所述请求响应信息由所述目标应用根据所述访问请求进行反馈。

2、根据权利要求 1 所述的方法，其中，所述地址信息为域名，所述根据所述至少一个边缘安全服务器的地址信息，建立与所述至少一个边缘安全服务器之间的会话连接，包括：

向域名服务器发送所述至少一个边缘安全服务器的域名解析请求；

接收由所述域名服务器发送的所述至少一个边缘安全服务器的域名对应的 IP 地址；

根据至少一个所述 IP 地址，分别向所述至少一个边缘安全服务器发送连接请求，以建立所述连接服务器与所述至少一个边缘安全服务器之间的会话连接，所述连接请求包含所述连接服务器的标识信息，以使所述至少一个边缘安全服务器将所述标识信息与对应的会话连接相关联。

3、根据权利要求 1 所述的方法，其中，所述获取与所述连接服务器对应的至少一个边缘安全服务器的地址信息，包括：

由管理平台中获取所述连接服务器对应的服务器配置信息；

从所述服务器配置信息中获取与所述连接服务器对应的至少一个边缘安全服务器的地址信息。

4、根据权利要求 1 所述的方法，其中，所述会话连接的传输协议为加密传输协议；

和/或

所述会话连接建立在 443 端口上。

5、一种远程访问应用的方法，应用于边缘安全服务器，包括：

接收由至少一个连接服务器发送的连接请求；

根据所述连接请求，建立与所述至少一个连接服务器之间的会话连接；

接收由边缘加速服务器转发的针对目标应用的访问请求，确定与所述目标应用对应的目标连接服务器；

根据与所述目标连接服务器对应的会话连接，转发所述访问请求至所述目标连接服务器。

6、根据权利要求 5 中所述的方法，其中，所述连接请求的数量为多个，所述连接请求中包含对应的连接服务器的标识信息；

根据所述连接请求，建立与所述至少一个连接服务器之间的会话连接，包括：

根据多个所述连接请求，分别建立与所述至少一个连接服务器之间的会话连接，并将多个所述标识信息与对应的会话连接相关联。

7、根据权利要求 5 所述的方法，其中，所述目标连接服务器的数量为多个；所述根据与所述目标连接服务器对应的会话连接，转发所述访问请求至所述目标连接服务器，包括：

根据与多个所述目标连接服务器的标识信息相关联的会话连接，转发所述访问请求至所述目标连接服务器。

8、一种远程访问应用的方法，应用于边缘加速服务器，包括：

接收由目标终端发送的针对目标应用的访问请求，所述访问请求包含所述目标应用的域名；

根据所述目标应用的域名，确定与所述目标应用的域名对应的边缘安全服务器的地址信息；

根据所述边缘安全服务器的地址信息，转发所述访问请求至所述边缘安全服务器。

9、根据权利要求 8 所述的方法，其中，所述根据所述目标应用的域名，确定与所述目标应用的域名对应的边缘安全服务器的地址信息，包括：

检测所述访问请求中是否携带目标用户的身份信息；

根据检测结果，对所述目标用户的身份信息执行与所述检测结果对应的认证策略；

若所述目标用户的身份信息通过所述认证策略的认证，则根据所述目标应用

的域名，确定与所述目标应用的域名对应的边缘安全服务器的地址信息。

10、根据权利要求 9 所述的方法，其中，所述认证策略包括身份认证策略和/或访问权限认证策略。

11、一种远程访问应用的方法，应用于管理平台，包括：

生成连接服务器对应的服务器配置信息，所述服务器配置信息至少包括连接服务器的标识信息和与连接服务器对应的边缘安全服务器的地址信息；

生成目标应用对应的应用配置信息，所述应用配置信息包括目标应用的域名、回源地址、相关联的连接服务器的标识信息、身份认证策略以及访问权限控制策略中的至少一种；

发送所述连接服务器所需的服务器配置信息；

发送边缘加速服务器所需的所述目标应用的应用配置信息以及与所述目标应用相关联的连接服务器的服务器配置信息。

12、一种远程访问应用的系统，包括：管理平台、边缘加速服务器、边缘安全服务器和连接服务器；

管理平台，设置为生成目标应用的应用配置信息，以及生成连接服务器对应的服务器配置信息；发送边缘加速服务器所需的所述目标应用的应用配置信息以及与所述目标应用相关联的连接服务器的服务器配置信息，并发送所述连接服务器所需的服务器配置信息；

边缘加速服务器，设置为接收目标终端发送的针对目标应用的访问请求；并根据所述访问请求包含的目标应用的域名，将所述访问请求向对应的边缘安全服务器进行发送；

边缘安全服务器，设置为接收所述边缘加速服务器发送的所述访问请求；根据在先建立的与连接服务器的会话连接，将所述访问请求转发至对应的连接服务器；

连接服务器，设置为接收所述边缘安全服务器发送的所述访问请求，并将所述访问请求转发至对应的目标应用。

13、根据权利要求 12 所述的系统，其中，所述会话连接为所述连接服务器至所述边缘安全服务器的出站连接。

14、根据权利要求 12 所述的系统，所述系统还包括：

认证中心，设置为根据所述访问请求携带的目标用户的标识信息获取所述目

标用户的身份信息，以使所述边缘加速服务器根据所述目标用户的身份信息和认证策略对所述目标用户进行认证，所述认证策略包括身份认证策略和/或访问权限认证策略。

15、一种远程访问应用的装置，应用于连接服务器，包括：

获取模块，设置为获取与所述连接服务器对应的至少一个边缘安全服务器的地址信息；

建立会话模块，设置为根据所述至少一个边缘安全服务器的地址信息，建立与所述至少一个边缘安全服务器之间的会话连接，所述会话连接为由所述连接服务器至所述至少一个边缘安全服务器的出站连接；

发送模块，设置为基于所述会话连接，若接收到由边缘安全服务器转发的针对目标应用的访问请求，将所述访问请求发送至所述目标应用；将接收到的请求响应信息向所述边缘安全服务器进行发送，所述请求响应信息由所述目标应用根据所述访问请求进行反馈。

16、一种远程访问应用的装置，应用于边缘安全服务器，包括：

接收模块，设置为接收由至少一个连接服务器发送的连接请求；

建立会话模块，设置为根据所述连接请求，建立与所述至少一个连接服务器之间的会话连接；

所述接收模块，还设置为接收由边缘加速服务器转发的针对目标应用的访问请求；

确定模块，设置为确定与所述目标应用对应的目标连接服务器；

发送模块，设置为根据与所述目标连接服务器对应的会话连接，转发所述访问请求至所述目标连接服务器。

17、一种远程访问应用的装置，应用于边缘加速服务器，包括：

接收模块，设置为接收由目标终端发送的针对目标应用的访问请求，所述访问请求包含所述目标应用的域名；

确定模块，设置为根据所述目标应用的域名，确定与所述目标应用的域名对应的边缘安全服务器的地址信息；

发送模块，设置为根据所述边缘安全服务器的地址信息，转发所述访问请求至所述边缘安全服务器。

18、一种远程访问应用的装置，应用于管理平台，包括：

生成模块，设置为生成连接服务器对应的服务器配置信息，所述服务器配置信息至少包括连接服务器的标识信息和与连接服务器对应的边缘安全服务器的地址信息；生成目标应用对应的应用配置信息，所述应用配置信息包括目标应用的域名、回源地址、相关联的连接服务器的标识信息、身份认证策略以及访问权限控制策略中的至少一种；

发送模块，设置为发送所述连接服务器所需的服务器配置信息；发送边缘加速服务器所需的所述目标应用的应用配置信息以及与所述目标应用相关联的连接服务器的服务器配置信息。

19、一种电子设备，包括存储器、处理器及存储在所述存储器上并可在所述处理器上运行的计算机程序，其中，所述处理器运行所述计算机程序以实现如权利要求 1-11 任一项所述的方法。

20、一种计算机可读存储介质，其上存储有计算机程序，其中，所述程序被处理器执行实现如权利要求 1-11 中任一项所述的方法。

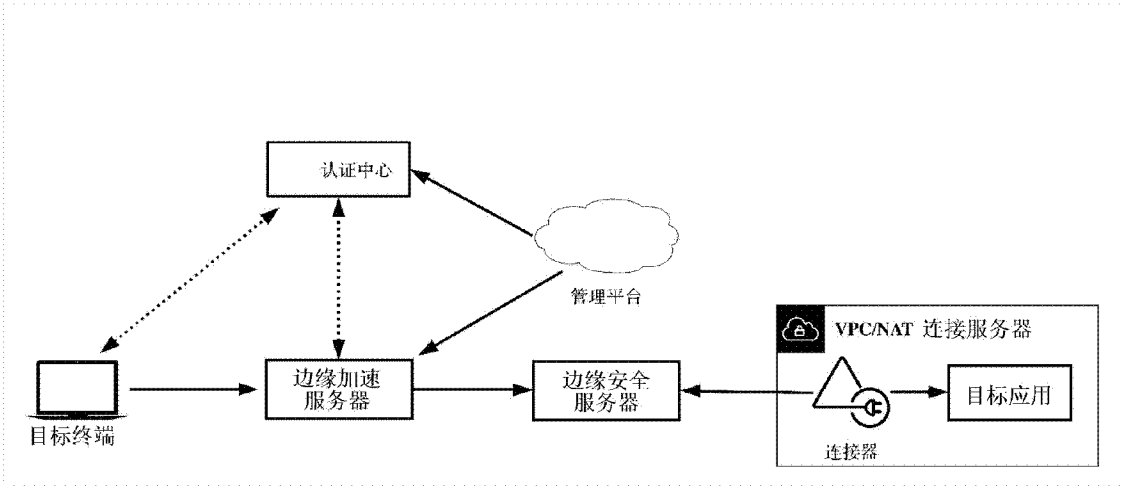
认证中心
管理平台
VPC/NAT 连接服务器
目标终端
边缘加速服务器
边缘安全服务器
目标应用
连接器

图 1

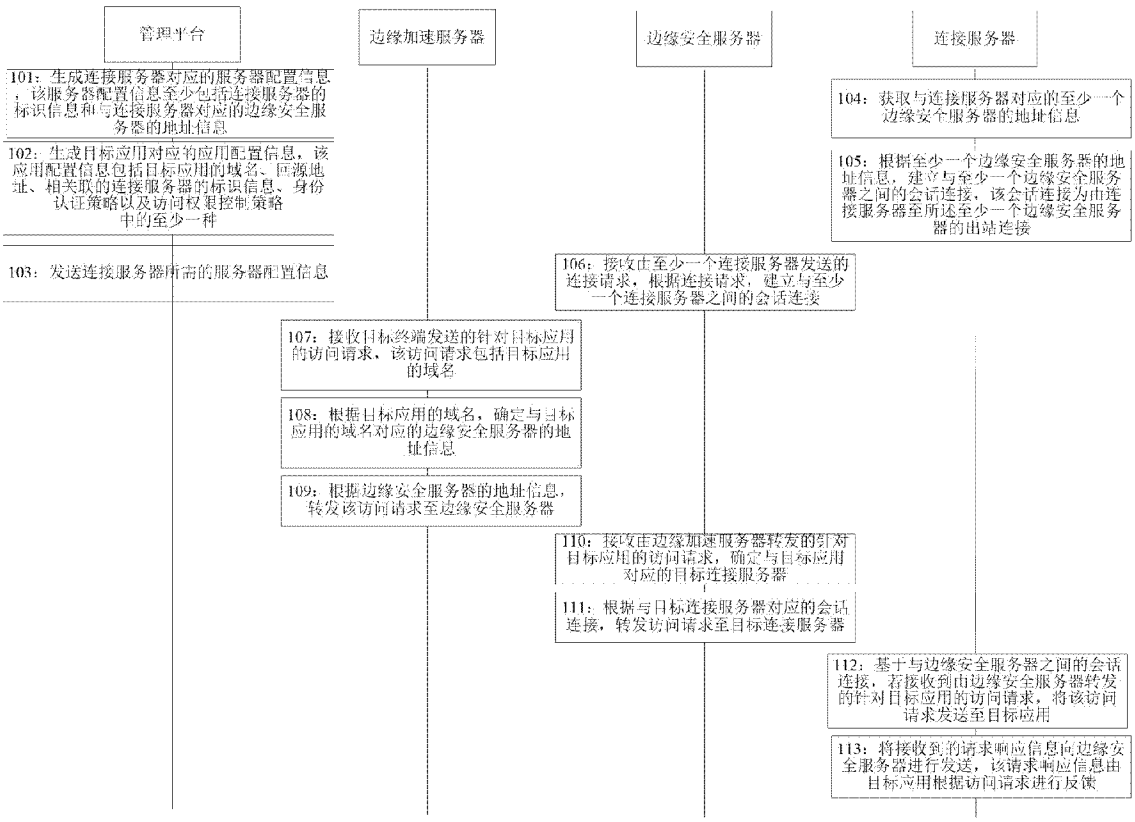
管理平台
边缘加速服务器
边缘安全服务器
连接服务器
101：生成连接服务器对应的服务器配置信息，该服务器配置信息至少包括连接服务器的标识信息和与连接服务器对应的边缘安全服务器的地址信息
102：生成目标应用对应的应用配置信息，该应用配置信息包括目标应用的域名、回源地址、相关联的连接服务器的标识信息、身份认证策略以及访问权限控制策略中的至少一种
103：发送连接服务器所需的服务器配置信息
104：获取与连接服务器对应的至少一个边缘安全服务器的地址信息
105：根据至少一个边缘安全服务器的地址信息，建立与至少一个边缘安全服务器之间的会话连接，该会话连接为由连接服务器至所述至少一个边缘安全服务器的出站连接
106：接收由至少一个连接服务器发送的连接请求，根据连接请求，建立与至少一个连接服务器之间的会话连接
107：接收目标终端发送的针对目标应用的访问请求，该访问请求包括目标应用的域名
108：根据目标应用的域名，确定与目标应用的域名对应的边缘安全服务器的地址信息
109：根据边缘安全服务器的地址信息，转发该访问请求至边缘安全服务器
110：接收由边缘加速服务器转发的针对目标应用的访问请求，确定与目标应用对应的目标连接服务器
111：根据与目标连接服务器对应的会话连接，转发访问请求至目标连接服务器
112：基于与边缘安全服务器之间的会话连接，若接收到由边缘安全服务器转发的针对目标应用的访问请求，将该访问请求发送至目标应用
113：将接收到的请求响应信息向边缘安全服务器进行发送，该请求响应信息由目标应用根据访问请求进行反馈

图 2

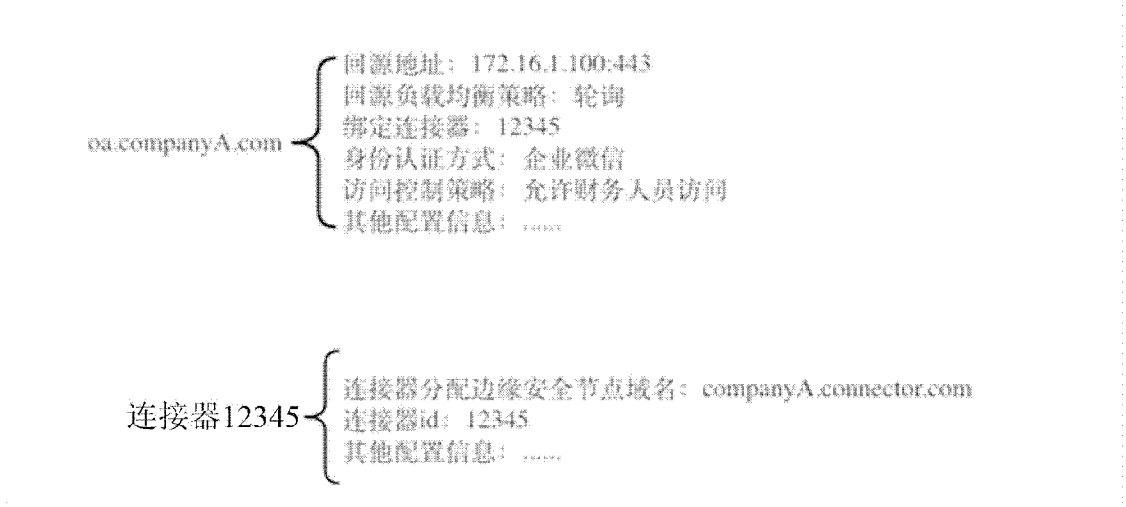
oa.companyA.com
回源地址：172.16.1.100:443
回源负载均衡策略：轮询
绑定连接器：12345
身份认证方式：企业微信
访问控制策略：允许财务人员访问
其他配置信息：.....
连接器12345
连接器分配边缘安全节点域名：companyA.connector.com
连接器id：12345
其他配置信息：.....

图 3

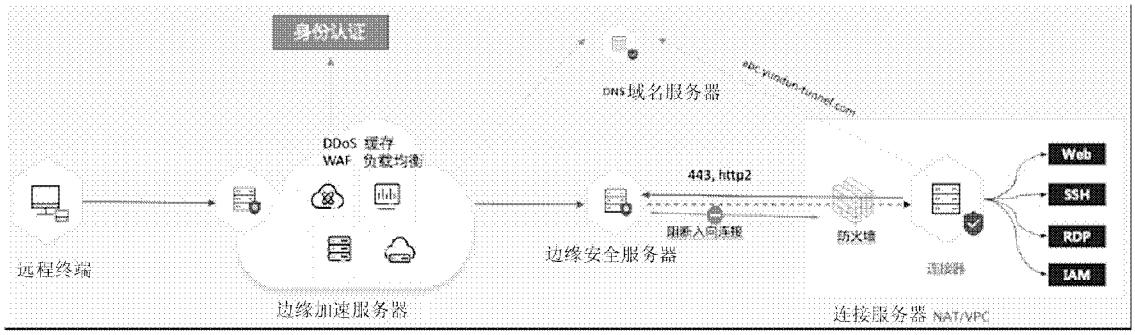
身份认证
DNS域名服务器
DDoS 缓存
WAF 负载均衡
443, http2
阻断入向连接
防火墙
Web
SSH
RDP
IAM
远程终端
边缘加速服务器
边缘安全服务器
连接服务器 NAT/VPC

图 4

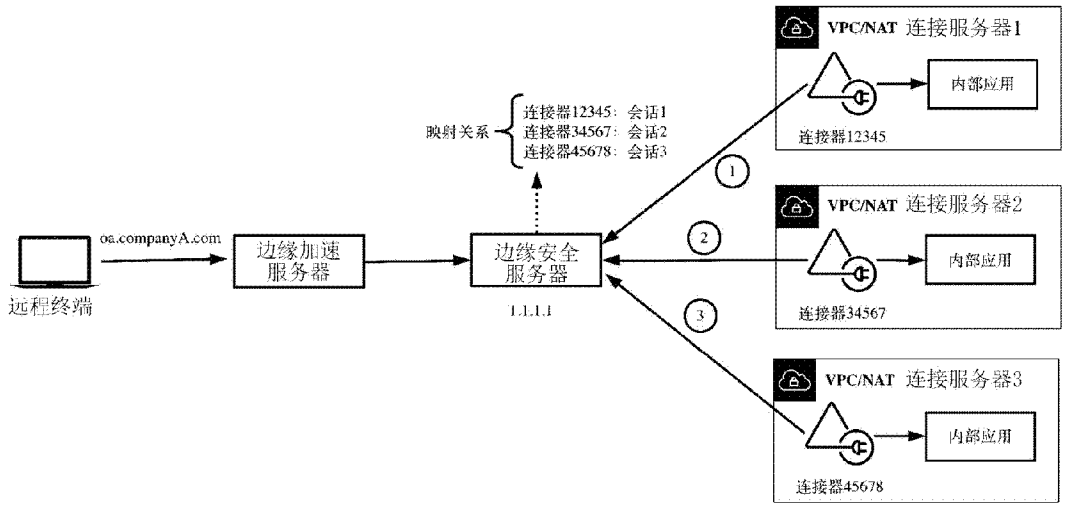
映射关系
连接器12345：会话1
连接器34567：会话2
连接器45678：会话3
VPC/NAT 连接服务器1
内部应用
连接器12345
VPC/NAT 连接服务器2
内部应用
连接器34567
VPC/NAT 连接服务器3
内部应用
连接器45678
oa.companyA.com
远程终端
边缘加速服务器
边缘安全服务器
1.1.1.1
1
2
3

图 5

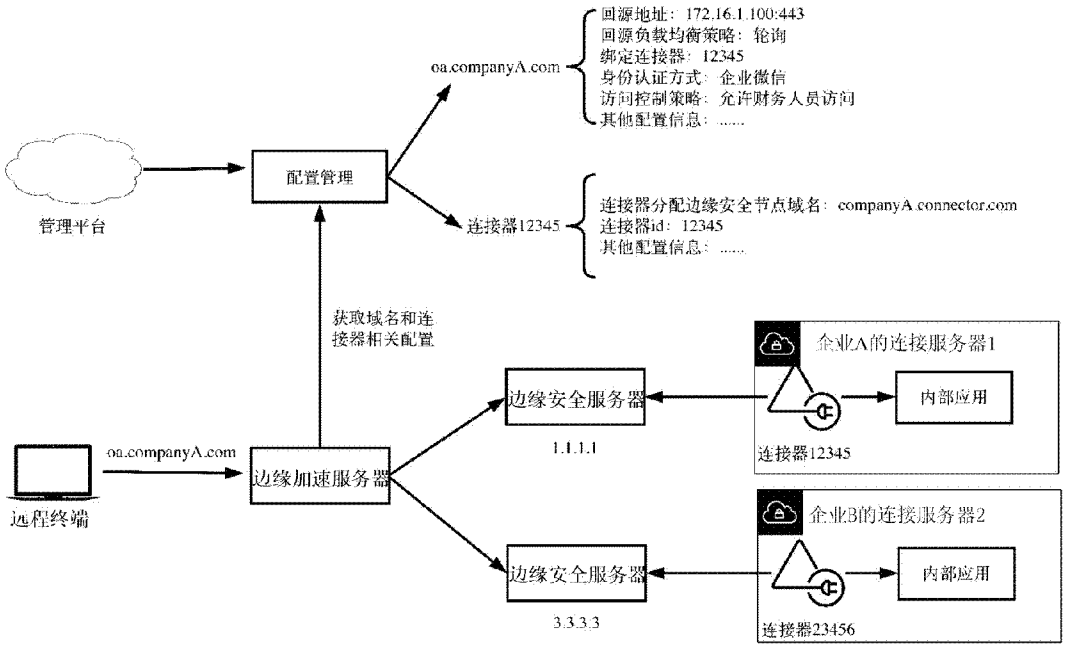
oa.companyA.com
回源地址：172.16.1.100:443
回源负载均衡策略：轮询
绑定连接器：12345
身份认证方式：企业微信
访问控制策略：允许财务人员访问
其他配置信息：.....
管理平台
配置管理
连接器12345
连接器分配边缘安全节点域名：companyA.connector.com
连接器id：12345
其他配置信息：.....
获取域名和连接器相关配置
企业A的连接服务器1
边缘安全服务器
内部应用
1.1.1.1
连接器12345
oa.companyA.com
边缘加速服务器
远程终端
企业B的连接服务器2
边缘安全服务器
内部应用
3.3.3.3
连接器23456

图 6

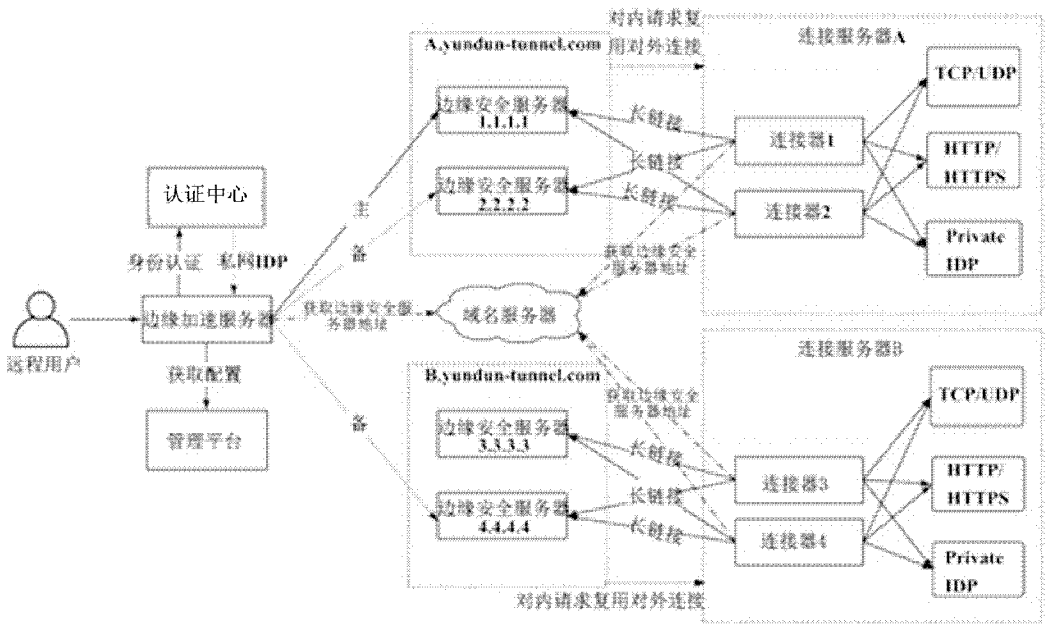
对内请求复用对外连接
A.yundun-tunnel.com
连接服务器A
TCP/UDP
HTTP/HTTPS
Private IDP
连接器1
连接器2
长链接
认证中心
主
备
身份认证
私网IDP
边缘加速服务器
域名服务器
远程用户
获取配置
管理平台
B.yundun-tunnel.com
连接服务器B
连接器3
连接器4
对内请求复用对外连接

图 7

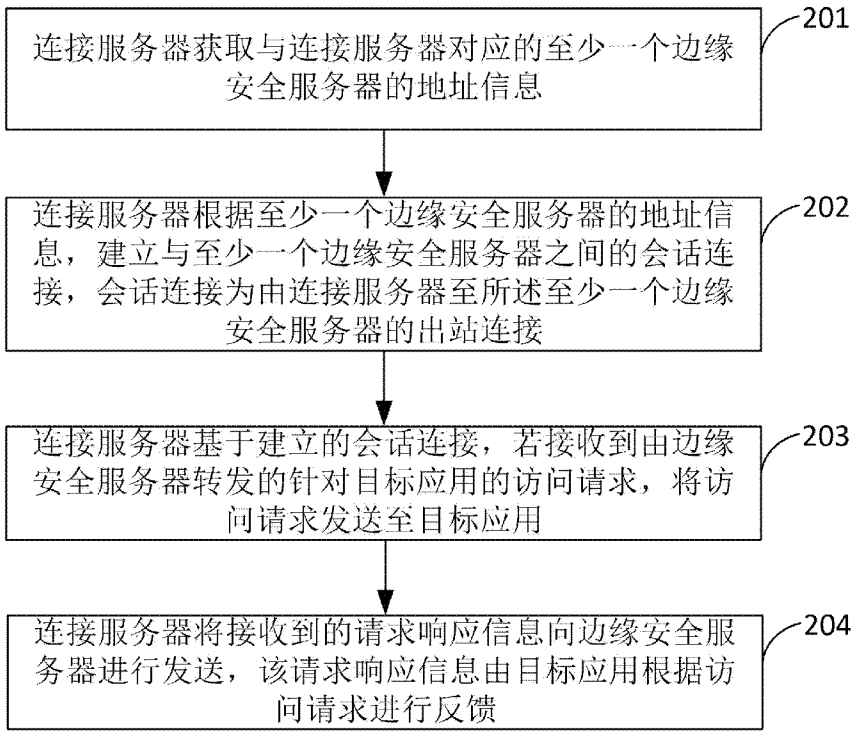
连接服务器获取与连接服务器对应的至少一个边缘安全服务器的地址信息
201
连接服务器根据至少一个边缘安全服务器的地址信息，建立与至少一个边缘安全服务器之间的会话连接，会话连接为由连接服务器至所述至少一个边缘安全服务器的出站连接
202
连接服务器基于建立的会话连接，若接收到由边缘安全服务器转发的针对目标应用的访问请求，将访问请求发送至目标应用
203
连接服务器将接收到的请求响应信息向边缘安全服务器进行发送，该请求响应信息由目标应用根据访问请求进行反馈
204

图 8

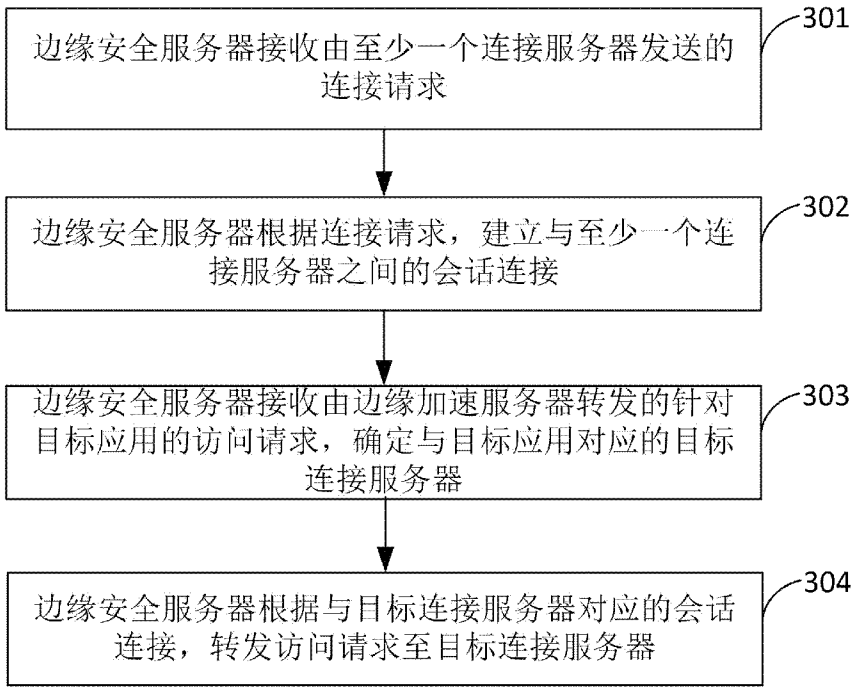
边缘安全服务器接收由至少一个连接服务器发送的连接请求
301
边缘安全服务器根据连接请求，建立与至少一个连接服务器之间的会话连接
302
边缘安全服务器接收由边缘加速服务器转发的针对目标应用的访问请求，确定与目标应用对应的目标连接服务器
303
边缘安全服务器根据与目标连接服务器对应的会话连接，转发访问请求至目标连接服务器
304

图 9

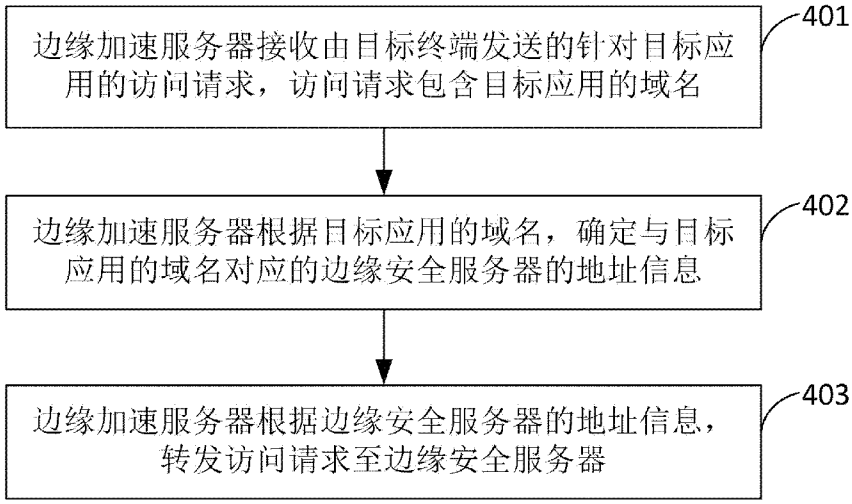
边缘加速服务器接收由目标终端发送的针对目标应用的访问请求，访问请求包含目标应用的域名
401
边缘加速服务器根据目标应用的域名，确定与目标应用的域名对应的边缘安全服务器的地址信息
402
边缘加速服务器根据边缘安全服务器的地址信息，转发访问请求至边缘安全服务器
403

图 10

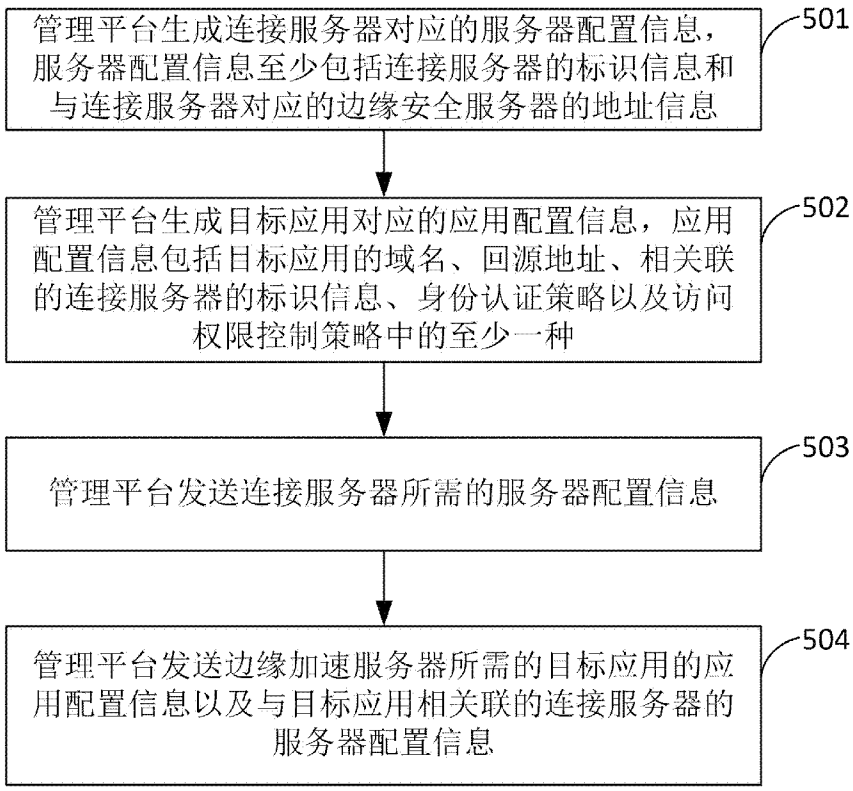
管理平台生成连接服务器对应的服务器配置信息，服务器配置信息至少包括连接服务器的标识信息和与连接服务器对应的边缘安全服务器的地址信息
501
管理平台生成目标应用对应的应用配置信息，应用配置信息包括目标应用的域名、回源地址、相关联的连接服务器的标识信息、身份认证策略以及访问权限控制策略中的至少一种
502
管理平台发送连接服务器所需的服务器配置信息
503
管理平台发送边缘加速服务器所需的目标应用的应用配置信息以及与目标应用相关联的连接服务器的服务器配置信息
504

图 11

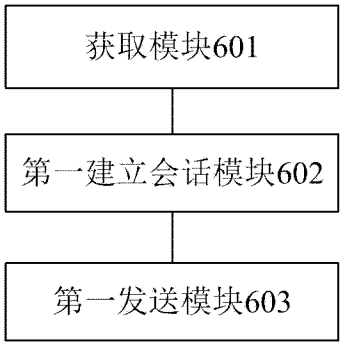

图 12

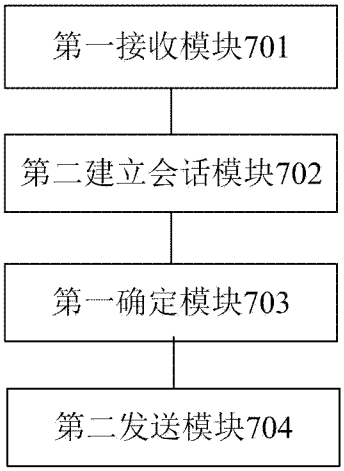

图 13

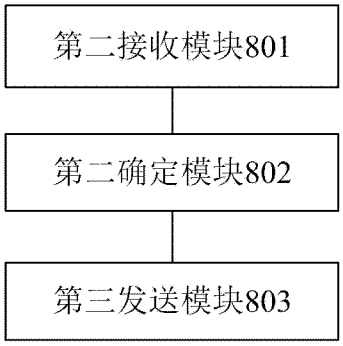

图 14

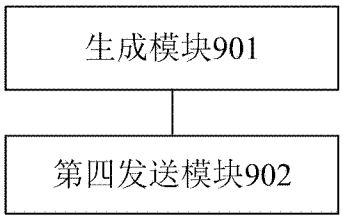

图 15

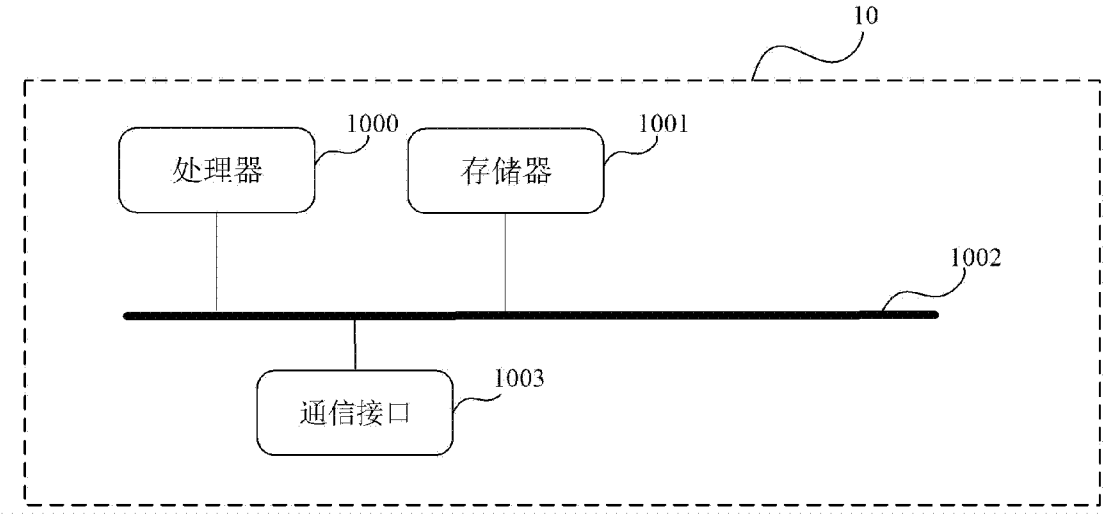

图 16

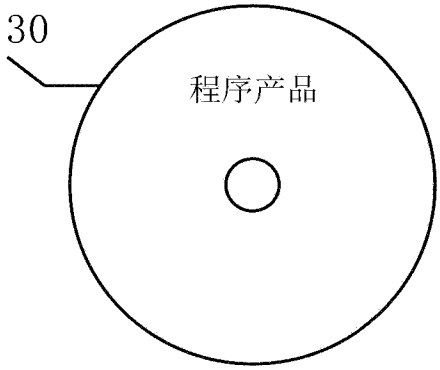

图 17

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2022/094195

A. CLASSIFICATION OF SUBJECT MATTER

G05B 19/042(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G05B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNABS; CNTXT; CNKI; VEN; USTXT; WOTXT; EPTXT: 上海云盾信息技术, 胡金涌, 刘贺, 远程, 加速, 服务器, 安全, 边缘, 域名, 管理平台, 终端, 连接, 云, VPC, remote+, access+, edge, security, safety, server+, connect+, management platform, domain name, cloud, terminal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 113341798 A (SHANGHAI YUNDUN INFORMATION TECHNOLOGY CO., LTD.) 03 September 2021 (2021-09-03) claims 1-20	1-20
X	CN 109417536 A (QUALCOMM INC.) 01 March 2019 (2019-03-01) description, paragraphs [0091]-[0162], and figures 1-16	1-7, 11-16, 18-20
X	CN 112256308 A (TENCENT TECHNOLOGY SHENZHEN CO., LTD.) 22 January 2021 (2021-01-22) description, paragraphs [0130]-[0146], and figures 1-7	8-10, 17, 19, 20
A	CN 106302512 A (SHANGHAI YUNDUN INFORMATION TECHNOLOGY CO., LTD.) 04 January 2017 (2017-01-04) entire document	1-20
A	CN 103117907 A (XINGYUNRONGCHUANG (BEIJING) INFORMATION TECHNOLOGY COMPANY LIMITED) 22 May 2013 (2013-05-22) entire document	1-20
A	US 2014149552 A1 (GO DADDY OPERATING CO., LLC) 29 May 2014 (2014-05-29) entire document	1-20

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
06 July 2022	**29 July 2022**
Name and mailing address of the ISA/CN **China National Intellectual Property Administration (ISA/CN)** **No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088, China** Facsimile No. **(86-10)62019451**	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2022/094195

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

[1] 1. Independent claim 1 and dependent claims 2-4 thereof relate to a method for remotely accessing an application.

[2] 2. Independent claim 15 relates to an apparatus for remotely accessing an application.

[3] 3. Independent 5 and dependent claims 6 and 7 thereof relate to a method for remotely accessing an application.

[4] 4. Independent 8 and dependent claims 9 and 10 thereof relate to a method for remotely accessing an application.

[5] 5. Independent claim 11 relates to a method for remotely accessing an application.

[6] 6. Independent 12 and dependent claims 13 and 14 thereof relate to a system for remotely accessing an application.

[7] 7. Independent claim 16 relates to an apparatus for remotely accessing an application.

[8] 8. Independent claim 17 relates to an apparatus for remotely accessing an application.

[9] 9. Independent claim 18 relates to an apparatus for remotely accessing an application.

[10] In the nine inventions, a "connection server" and an "edge security sever" in independent claims 1 and 15 and independent claims 5 and 16 are the corresponding technical features. However, the described features are common general knowledge in the art. The "edge security sever" in independent claims 1 and 15 and independent claims 8 and 17 is the corresponding technical feature. However, the described feature is common general knowledge in the art. The "connection server" and the "edge security sever" in independent claims 1 and 15 and independent claims 11 and 18 are the corresponding technical features. However, the described features are common general knowledge in the art. The "connection server" and the "edge security sever" in independent claims 1 and 15 and independent claim 12 are the corresponding technical features. However, the described features are common general knowledge in the art.

[11] Therefore, the first and second inventions and the third to ninth inventions do not share a same or corresponding special technical feature, are not technically linked, do not belong to a single general inventive concept, and therefore do not comply with the requirement of unity of invention as defined in PCT Rule 13.1.

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☑ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2022/094195

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	113341798	A	03 September 2021	None			
CN	109417536	A	01 March 2019	BR	112018071151	A2	05 February 2019
				US	2019036908	A1	31 January 2019
				KR	20180135446	A	20 December 2018
				EP	3443721	A1	20 February 2019
				AU	2016402775	A1	27 September 2018
				WO	2017177449	A1	19 October 2017
				IN	201847033739	A	14 September 2018
				EP	3443721	A4	18 March 2020
CN	112256308	A	22 January 2021	None			
CN	106302512	A	04 January 2017	CN	106302512	B	20 October 2020
CN	103117907	A	22 May 2013	CN	103117907	B	28 September 2016
US	2014149552	A1	29 May 2014	US	9160809	B2	13 October 2015

国际检索报告

国际申请号
PCT/CN2022/094195

A. 主题的分类

G05B 19/042(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

G05B

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNABS;CNTXT;CNKI;VEN;USTXT;WOTXT;EPTXT:上海云盾信息技术，胡金涌，刘贺，远程，加速，服务器，安全，边缘，域名，管理平台，终端，连接，云，VPC，remote+，access+，edge，security，safety，server+，connect+，management platform，domain name，cloud，terminal

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
PX	CN 113341798 A (上海云盾信息技术有限公司) 2021年9月3日 (2021-09-03) 权利要求1-20	1-20
X	CN 109417536 A (高通股份有限公司) 2019年3月1日 (2019-03-01) 说明书第[0091]-[0162]段，图1-16	1-7、11-16、18-20
X	CN 112256308 A (腾讯科技深圳有限公司) 2021年1月22日 (2021-01-22) 说明书第[0130]-[0146]段，图1-7	8-10、17、19、20
A	CN 106302512 A (上海云盾信息技术有限公司) 2017年1月4日 (2017-01-04) 全文	1-20
A	CN 103117907 A (星云融创北京信息技术有限公司) 2013年5月22日 (2013-05-22) 全文	1-20
A	US 2014149552 A1 (GO DADDY OPERATING CO LLC) 2014年5月29日 (2014-05-29) 全文	1-20

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2022年7月6日	2022年7月29日
ISA/CN的名称和邮寄地址 中国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 郑勇龙 电话号码 （86-512）88997016

国际检索报告

国际申请号
PCT/CN2022/094195

第III栏　缺乏发明单一性的意见(续第1页第3项)

本国际检索单位在该国际申请中发现多项发明，即：

[1] 1、独立权利要求1与其从属权利要求2-4涉及一种远程访问应用的方法；

[2] 2、独立权利要求15涉及一种远程访问应用的装置；

[3] 3、独立权利要求5与其从属权利要求6、7涉及一种远程访问应用的方法；

[4] 4、独立权利要求8与其从属权利要求9、10涉及一种远程访问应用的方法；

[5] 5、独立权利要求11涉及一种远程访问应用的方法；

[6] 6、独立权利要求12与其从属权利要求13、14涉及一种远程访问应用的系统；

[7] 7、独立权利要求16涉及一种远程访问应用的装置；

[8] 8、独立权利要求17涉及一种远程访问应用的装置；

[9] 9、独立权利要求18涉及一种远程访问应用的装置。

[10] 上述9项发明中：独立权利要求1、15和5、16中的“连接服务器”、“边缘安全服务器”是相应的技术特征，但上述特征是本领域的公知常识。独立权利 要求1、15和8、17中的“边缘安全服务器”是相应的技术特征，但上述特征是本领域的公知常识。独立权利要求1、15和11、18中的“连接服务器”、“边缘安全服务器”是相应的技术特征，但上述特征是本领域的公知常识。独立权利要求1、15和12中的“连接服务器”、“边缘安全服务器”是相应的技术特征，但上述特征是本领域的公知常识。

[11] 因此，上述第1、2项发明和第3-9项发明之间均不存在相同或相应的特定技术特征，不存在技术关联，不属于一个总的发明构思，因而本申请不满足发明单一性的要求，不符合PCT细则13.1的规定。

1. ☐ 由于申请人按时缴纳了被要求缴纳的全部附加检索费，本国际检索报告涉及全部可作检索的权利要求。

2. ☑ 由于无需付出有理由要求附加费的劳动即能对全部可检索的权利要求进行检索，本单位未通知缴纳任何加费。

3. ☐ 由于申请人仅按时缴纳了部分被要求缴纳的附加检索费，本国际检索报告仅涉及已缴费的那些权利要求，具体地说，是权利要求：

4. ☐ 申请人未按时缴纳被要求缴纳的附加检索费。因此，本国际检索报告仅涉及权利要求书中首先提及的发明；包含该发明的权利要求是：

对异议的意见

☐ 申请人缴纳了附加检索费，同时提交了异议书，适用时，缴纳了异议费。

☐ 申请人缴纳了附加检索费，同时提交了异议书，但未在通知书规定的时间期限内缴纳异议费。

☐ 缴纳附加检索费时未提交异议书。

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2022/094195

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	113341798	A	2021年9月3日	无			
CN	109417536	A	2019年3月1日	BR	112018071151	A2	2019年2月5日
				US	2019036908	A1	2019年1月31日
				KR	20180135446	A	2018年12月20日
				EP	3443721	A1	2019年2月20日
				AU	2016402775	A1	2018年9月27日
				WO	2017177449	A1	2017年10月19日
				IN	201847033739	A	2018年9月14日
				EP	3443721	A4	2020年3月18日
CN	112256308	A	2021年1月22日	无			
CN	106302512	A	2017年1月4日	CN	106302512	B	2020年10月20日
CN	103117907	A	2013年5月22日	CN	103117907	B	2016年9月28日
US	2014149552	A1	2014年5月29日	US	9160809	B2	2015年10月13日