

一种企业分支机构访问请求处理方法、装置、系统、设备及介质

本申请要求在 2018 年 09 月 28 日提交中国专利局、申请号为 201811140683.5，发明名称为“一种企业分支机构访问请求处理方法、装置及系统”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本申请涉及但不限于互联网技术领域，尤其涉及一种企业分支机构访问请求处理方法、装置、系统、设备及介质。

背景技术

传统大型企业通常会有分布于不同地域的分公司或分部。分部规模通常都比较大，主要是承担区域本地化职能，如当地销售部、当地生产基地等，在总部的组织领导下，采取共同的经营方针、一致的营销行动，实行统一管理和分散运营的有机结合，通过规范化经营实现规模经济效益的联合。下文以常见的全国连锁的大型商场企业为例说明。

大型商场规模都比较大，工作人员超过 100 人以上，有专门的 IT 部门负责网络管理和运营，商场运营所需要的核心服务包括交易系统、仓储管理系统、安保监控系统等，这些系统一般都部署在商场内机房。商场有访问总部服务的需求，总部也有访问各分支商场的服务系统的需求。由于交易、仓储等属于企业核心数据，为防止安全问题及泄漏风险，企业通常不会直接允许商场内网具有访问公网的能力。各地商场都通过部署多协议标记转换（Multiprotocol Label Switch，简称 MPLS）专线与总部联通，方便总部和商场相互访问，访问质量稳定且安全可控，另外商场内网访问公网也需要走总部，方便监管。考虑商场分支和总部线路可能会故障，通常会部署两条不同运营商线路，以做备份，这种备份的方式会额外增加一份成本。

在互联网云时代，企业提供云服务的背景下，企业分支机构会有越来越多访问外网云服务的流量，如公有云备份、SaaS 服务等。

传统大型企业当前为分支的网络扩容方案通常有两种：

第一种，运营商专线扩容，主要存在扩容部署慢，成本昂贵的问题，并且对 MPLS 专线有很高要求，需要持续大量扩容，而专线扩容非常困难，而且成本巨大。

第二种，开放分支访问外网能力，云服务和 SaaS 服务分支直接走本地互联网宽带访问。该方案可以有效缓解专线扩容慢、成本高昂的问题。但是会带来很大安全风险，访问外网流量不可控。另外全国各地直接访问云服务和 SaaS 服务，访问质量得不到稳定保障。

综上所述，传统大型企业在互联网云时代，面临分支大量增加访问外网云服务和 SaaS 服务的需求，现在专线方案运营复杂而且成本极大，无法有效稳定运营的问题，所以，需要提供新的方案使访问成本降低并且能够保障企业分支机构网络访问外网的云端业务及 SaaS 服务的体验效果。

发明内容

为克服相关技术中存在的问题，本申请提供一种企业分支机构访问请求处理方法、装置及系统。

根据本申请的第一方面，提供了一种企业分支机构访问请求处理方法，包括：

在企业分支机构网络中设置客户终端设备，将所述企业分支机构网络中的访问请求导入所述客户终端设备；

所述客户终端设备判断所述访问请求是否需要加速处理的用于访问外网的访问请求，在所述访问请求是需要加速处理的用于访问外网的访问请求时，将所述访问请求转发至加速网络；

所述客户终端设备从所述加速网络接收所述访问请求的响应数据，将所述响应数据发送至所述访问请求的发送方。

其中，所述方法还包括：

所述客户终端设备判断所述访问请求是否是用于访问内网的访问请求，在所述访问请求是用于访问内网的访问请求时，根据分流规则确定转发路径，根

据所述转发路径转发所述访问请求，所述转发路径是经由专线网络转发或者是经由所述加速网络转发。

其中，所述方法还包括：所述客户终端设备从所述加速网络的中央控制器接收所述分流规则。

其中，所述转发路径是经由所述加速网络转发时，所述加速网络中的接入点接收所述访问请求，根据动态路由对所述访问请求进行转发，直至发送到所述访问请求的目标子网中的客户终端设备。

其中，所述将所述企业分支机构网络中的访问请求导入所述客户终端设备包括：所述企业分支机构网络的出口路由器将符合预设规则的访问请求转发至所述客户终端设备。

其中，所述客户终端设备将所述访问请求发送至加速网络包括：所述客户终端设备将所述访问请求加密后发送至加速网络中距所述企业分支机构网络的归属地最近的网络接入点。

其中，所述方法还包括：所述客户终端设备根据预设加密规则对访问请求和响应数据进行加密传输。

根据本申请的第二方面，还提供一种应用于客户终端设备的企业分支机构访问请求处理装置，包括：

导入模块，被设置为导入企业分支机构网络中的访问请求；

判断模块，被设置为判断所述访问请求是否需要加速处理的用于访问外网的访问请求；

第一转发模块，被设置为在所述访问请求是需要加速处理的用于访问外网的访问请求时，将所述访问请求转发至加速网络；

接收模块，被设置为从加速网络接收所述访问请求的响应数据；

响应模块，被设置为将所述响应数据发送至所述访问请求的发送方。

其中，所述装置还包括路径确定模块和第二转发模块；

所述路径确定模块，被设置为在所述访问请求是用于访问内网的访问请求时，根据分流规则确定转发路径；

所述转发路径是经由专线网络转发或者是经由所述加速网络转发；

所述第二转发模块，被设置为根据所述转发路径转发所述访问请求。

其中，所述装置还包括路径确定模块和第二转发模块；

所述路径确定模块，被设置为在所述访问请求是用于访问内网的访问请求时，根据分流规则确定转发路径；

所述转发路径是经由专线网络转发或者是经由所述加速网络转发；

所述第二转发模块，被设置为根据所述转发路径转发所述访问请求。

其中，所述装置还包括加密模块和解密模块，

所述加密模块：被设置为对访问外网的访问请求根据预设加密规则进行加密；

所述解密模块：被设置为对接收到的响应数据根据预设加密规则进行解密。

根据本申请的第三方面，还提供了一种企业分支机构访问请求处理系统，包括：

企业分支机构网络、加速网络；所述企业分支机构网络包括客户终端设备；

所述客户终端设备，被设置为接收所述企业分支机构网络中的访问请求；判断所述访问请求是否需要加速处理的用于访问外网的访问请求，在所述访问请求是需要加速处理的用于访问外网的访问请求时，将所述访问请求转发至加速网络；从所述加速网络接收所述访问请求的响应数据，将所述响应数据发送至所述访问请求的发送方。

其中，所述加速网络还包括中央控制器；

所述中央控制器，被设置为确定所述分流规则，并将所述分流规则发送至所述客户终端设备。

根据本申请的第四方面，还提供了一种计算机设备，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，所述处理器执行所述程序时实现上述方法的步骤。

根据本申请的第五方面，还提供了一种计算机可读存储介质，所述存储介质上存储有计算机程序，所述程序被处理器执行时实现上述方法的步骤。

本申请包括以下优点：

1、可以同时兼顾分支流畅访问云服务、企业数据安全、快速部署及成本控制等需求。

2、可以同时兼顾企业分支机构网络访问总部、云端业务和 SaaS 服务体验，并且部署成本比专线大幅度降低，运营复杂度也大幅度降低，使访问成本降低并且能够保障企业分支机构网络访问外网的云端业务及 SaaS 服务的体验效果。

3、率先引入 SD-WAN 网络作为企业专线备份，有效解决企业双专线成本高的问题，企业可以采用一条专线一条 SD-WAN 线路，可以有效降低成本。

4、率先引入 SD-WAN 网络作为企业专线备份，解决线路容量不足，扩容慢且昂贵的问题，并且可以加速 SaaS 服务及云服务访问。

5、引入 CPE 设备作为接入设备，根据用户设置的规则进行分流或者根据加速网络的中央控制器实时配置或预先设置的规则进行分流，可以有效进行分流管理，方便集团统一管理分支流量。

6、在加速网络内部转发的都是加密过的私有数据，无法被截获。

附图说明

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

图 1 是根据一示例性实施例示出的一种企业分支机构访问请求处理方法的流程图；

图 2 是根据一示例性实施例示出的企业分支机构访问请求处理系统的结构图；

图 3 是根据一示例性实施例示出的一种企业分支机构访问请求处理装置的框图；

图 4 是根据一示例性实施例示出的一种用于企业分支机构访问请求处理方法的装置的框图。

具体实施方式

下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本申请保护的范围。需要说明的是，在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互任意组合。

实施例一

如图 1 所示，企业分支机构访问请求处理方法包括：

步骤 101，在企业分支机构网络中设置客户终端设备（CPE），将企业分支机构网络中的访问请求导入客户终端设备；

步骤 102，客户终端设备判断访问请求是否需要加速处理的用于访问外网的访问请求；

步骤 103，在访问请求是需要加速处理的用于访问外网的访问请求时，将访问请求转发至加速网络；

步骤 104，客户终端设备从加速网络接收访问请求的响应数据，将响应数据发送至访问请求的发送方。

其中，

步骤 101 中，在企业分支机构网络中设置客户终端设备后，客户终端设备便具有属于企业分支机构网络的 IP 地址，客户终端设备可以联通加速网络和专线网络。将企业分支机构网络的访问请求导入客户终端设备包括：企业分支机构网络的出口路由器将符合预设规则的访问请求转发至客户终端设备。

访问请求可以是上传、下载请求，可以是 TCP(http/https 等)请求、UDP 请求等。

步骤 102 中还包括：客户终端设备判断访问请求是否是用于访问内网的访问请求，在访问请求是用于访问内网的访问请求时，分析访问请求数据包协议、来源、目标地址及协议，查找预先设置好的分流规则（分流规则由客户配置，按访问请求的应用类型、来源 ip、目标 ip 配置等参数确定是经由专线网络转发

或者是经由加速网络转发，此分流规则还可以包括是在一条路径满载后自动切换到另一条路径的规则，也可以是根据不同路径的分配比例确定出的分流规则），根据分流规则确定转发路径，根据转发路径转发访问请求，此转发路径是经由专线网络转发或者是经由加速网络转发。客户终端设备中安装有网络管理程序，通过此网络管理程序可以接收用户配置的分流规则，从而可以实时管理专线网络和加速网络的流量。其中访问内网的访问请求，可以是访问企业总部网络的访问请求，也可以是访问企业其他分支机构网络的访问请求。

客户终端设备判断访问请求是否是用于访问内网的访问请求时，根据此访问请求的目标地址进行判断，此目标地址属于内网时，确定访问请求是用于访问内网的访问请求。

客户终端设备判断访问请求是否需要加速处理的用于访问外网的访问请求时，根据访问请求的目标地址和访问请求中是否携带需要加速处理的标识，在访问请求的目标地址属于内网时并且访问请求中携带需要加速处理的标识时，确定此访问请求是需要加速处理的用于访问外网的访问请求。

本方法中还包括，在访问请求是用于访问外网的访问请求同时不需要加速处理时，客户终端设备将访问请求直接发送至外网。

转发路径是经由加速网络转发时，加速网络中的接入点接收访问请求，根据动态路由对访问请求进行转发，直至发送到访问请求的目标子网中的客户终端设备。

本方法中还包括：

转发路径是经由专线网络转发时，客户终端设备将访问请求发送至专线网络，由专线网络将此访问请求发送至目标企业分支机构网络的客户终端设备。

企业分支机构网络是指企业总部网络或者企业分部网络。外网可以是云服务网络或者是 SaaS 服务网络。加速网络为软件定义广域网络（Software-Defined Wide Area Network，简称 SD-WAN），此网络中包括多个网络接入点即入网点（Point-of-Presence，简称 PoP），SD-WAN 网络是由海量资源构成的一张遍布全球的私有网络，通过 PoP 接入，并且经过内部动态路由，选择最优回源路径。典型的应用场景中，可以通过 SD-WAN 可以找到和企业分支机构网络地址最近

(例如同城市)的接入 PoP 点,并且可以找到和源站地址最近(例如同城市)的回源 PoP 点,通过 NAT 方式,将内网访问转换成外网,发送请求到目标地址,并将目标地址响应转换回内网,从而可以非常快速的获取用户所需的外网数据。加速网络中的网络接入点接收客户终端设备转发的访问请求后,根据动态路由对访问请求进行转发,找到下一转发接入点,直至发送到距目标地址最近的接入点,此接入点将访问请求发送至外网的目标地址,并接收响应数据,根据动态路由对访问请求进行转发,转发至距企业分支机构网络的归属地最近的网络接入点,由此网络接入点发送至企业内网的客户终端设备。

加速网络还包括中央控制器,中央控制器与加速网络中各接入点连接,并且与各企业分支机构网络中客户终端设备连接。例如加速网络是 SD-WAN 网络时,此中央控制器为 SD-WAN 控制器。中央控制器为各企业分支机构网络的客户终端设备确定分流规则,将确定后的分流规则发送至企业分支机构网络的客户终端设备。除了确定分流规则,中央控制器还可以确定流量优先级、限流策略等。中央控制器可以提供实时入口用于展示各分支流量情况、各用户带宽使用情况,利于管理。

为提高数据传输的安全性,可以对访问请求和响应数据进行加密传输。

具体的,对访问请求进行加密的过程包括:客户终端设备对需要加速处理的用于访问外网的访问请求根据预设加密规则进行加密,将加密后的访问请求发送至加速网络中距企业分支机构网络的归属地最近的网络接入点。加速网络中网络接入点对加密后的访问请求进行转发后,转发至距访问请求的目标外网的归属地最近的网络接入点,此网络接入点对加密后的访问请求进行解密,将解密后的访问请求发送至访问请求的目标外网。

对响应数据进行加密的过程包括:距访问请求的目标外网的归属地最近的网络接入点接收到响应数据后,根据预设加密规则进行加密。加速网络中网络接入点对加密后的响应数据进行转发后,转发至距企业分支机构网络的归属地最近的网络接入点,此网络接入点将加密后的响应数据发送至企业分支机构网络中的客户终端设备,客户终端设备对加密后的响应数据进行解密。

如图 2 所示,企业分支机构访问请求处理系统包括:企业分支机构网络、加速网络;企业分支机构网络包括客户终端设备。

客户终端设备用于接收企业分支机构网络中的访问请求；判断访问请求是否需要加速处理的用于访问外网的访问请求，在访问请求是需要加速处理的用于访问外网的访问请求时，将访问请求转发至加速网络；从加速网络接收访问请求的响应数据，将响应数据发送至访问请求的发送方。

加速网络包括网络接入点，网络接入点包括加密模块和解密模块。加密模块用于在网络接入点是距外网归属地最近的网络接入点并且从外网接收到响应数据时，对响应数据根据预设加密规则进行加密。解密模块用于在网络接入点是距外网归属地最近的网络接入点并且接收到已加密的访问请求时，对已加密的访问请求根据预设加密规则进行解密。

加速网络还包括中央控制器。中央控制器用于确定分流规则，并将分流规则发送至客户终端设备。

如图 3 所示，应用于客户终端设备的企业分支机构访问请求处理装置，包括导入模块 301、判断模块 302、第一转发模块 303、接收模块 304、响应模块 305。

导入模块 301，被设置为导入企业分支机构网络中的访问请求；

判断模块 302，被设置为判断访问请求是需要加速处理的用于访问外网的访问请求还是用于访问内网的访问请求；

第一转发模块 303，被设置为在访问请求是需要加速处理的用于访问外网的访问请求时，将访问请求转发至加速网络；

接收模块 304，被设置为从加速网络接收访问请求的响应数据；

响应模块 305，被设置为将响应数据发送至访问请求的发送方。

其中，企业分支机构访问请求处理装置还包括路径确定模块和第二转发模块。

路径确定模块被设置为在访问请求是用于访问内网的访问请求时，根据分流规则确定转发路径；转发路径是经由专线网络转发或者是经由加速网络转发；

第二转发模块被设置为根据转发路径转发访问请求。

此企业分支机构访问请求处理装置还包括加密模块和解密模块。加密模块被设置为对用于访问外网的访问请求根据预设加密规则进行加密，解密模块被

设置为对接收到的响应数据根据预设加密规则进行解密。

本发明实施例的方法中的步骤可以根据实际需要进行顺序调整、合并和删减。

本发明实施例的企业分支机构访问请求处理方法中的单元模块可以根据实际需要进行合并、划分和删减。

本发明实施例还提供了一种计算机可读存储介质，此存储介质上存储有计算机程序，所述程序被处理器执行时实现上述方法的步骤。

本发明实施例还提供了一种计算机设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，处理器执行此程序时实现上述方法的步骤。

图 4 是根据一示例性实施例示出的一种用于企业分支机构访问请求处理方法的装置 400 的框图。例如，装置 400 可以被提供为一服务器。参照图 4，装置 400 包括处理器 401，处理器的个数可以根据需要设置为一个或者多个。装置 400 还包括存储器 402，被设置为存储可由处理器 401 执行的指令，例如应用程序。存储器的个数可以根据需要设置一个或者多个，其存储的应用程序可以为一个或者多个。处理器 401 被设置为执行指令，以执行上述方法。

本领域技术人员应明白，本申请的实施例可提供为方法、装置（设备）、或计算机程序产品。因此，本申请可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质上实施的计算机程序产品的形式。计算机存储介质包括在用于存储信息（诸如计算机可读指令、数据结构、程序模块或其他数据）的任何方法或技术中实施的易失性和非易失性、可移除和不可移除介质，包括但不限于 RAM、ROM、EEPROM、闪存或其他存储器技术、CD-ROM、数字多功能盘（DVD）或其他光盘存储、磁盒、磁带、磁盘存储或其他磁存储装置、或者可以用于存储期望的信息并且可以被计算机访问的任何其他的介质等。此外，本领域普通技术人员公知的是，通信介质通常包含计算机可读指令、数据结构、程序模块或者诸如载波或其他传输机制之类的调制数据信号中的其他数据，并且可包括任何信息递送介质。

本申请是参照根据本发明实施例的方法、装置（设备）和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能

这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

在本文中，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的物品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种物品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括……”限定的要素，并不排除在包括所述要素的物品或者设备中还存在另外的相同要素。

尽管已描述了本申请的优选实施例，但本领域内的技术人员一旦得知了基本创造性概念，则可对这些实施例作出另外的变更和修改。所以，所附权利要求意欲解释为包括优选实施例以及落入本申请范围的所有变更和修改。

显然，本领域的技术人员可以对本申请进行各种改动和变型而不脱离本申请的精神和范围。这样，倘若本申请的这些修改和变型属于本申请权利要求及其等同技术的范围之内，则本申请的意图也包含这些改动和变型在内。

工业实用性

本申请可以同时兼顾企业分支机构网络访问云端业务和 SaaS 服务体验，并且部署成本比专线大幅度降低，运营复杂度也大幅度降低，使访问成本降低并且能够保障企业分支机构网络访问外网的云端业务及 SaaS 服务的体验效果。