(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 109361590 B
(45)授权公告日 2021.04.27

(21)申请号 201811594076.6
(22)申请日 2018.12.25
(65)同一申请的已公布的文献号
申请公布号 CN 109361590 A
(43)申请公布日 2019.02.19
(73)专利权人 杭州迪普科技股份有限公司
地址 310051 浙江省杭州市滨江区通和路68号中财大厦6楼
(72)发明人 黄春平
(74)专利代理机构 北京博思佳知识产权代理有限公司 11415
代理人 林祥
(51)Int.Cl.
H04L 12/46(2006.01)
H04L 12/801(2013.01)
H04L 29/12(2006.01)
审查员 程曦

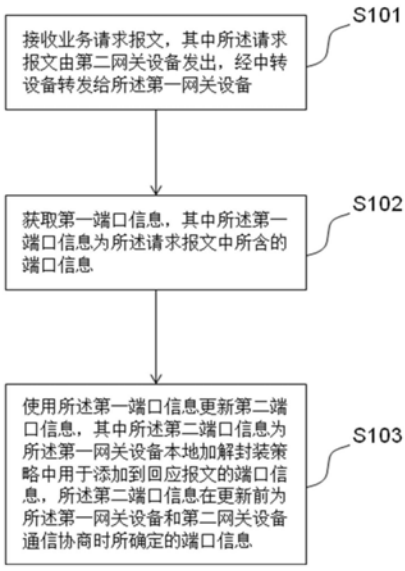
权利要求书2页 说明书7页 附图5页

(54)发明名称

一种解决业务访问不通的方法和装置

(57)摘要

本申请提供一种解决业务访问不通的方法和装置,其方法包括:接收业务请求报文,所述请求报文由第二网关设备发出,经中转设备转发给第一网关设备;获取第一端口信息,所述第一端口信息为请求报文中所含的端口信息;使用第一端口信息更新第二端口信息,所述第二端口信息为第一网关设备本地加解封装策略中用于添加到回应报文的端口信息,第二端口信息在更新前为所述第一网关设备和第二网关设备通信协商时所确定的端口信息。通过端口信息更新机制,克服了回应报文因端口不正确而导致的丢包问题,保证了IPSec业务访问的稳定性,增强了IPSec VPN的实用性和易用性,而且无需保活报文,很好的解决了NAT环境中VPN业务访问不通的问题。



CN 109361590 B

1.一种解决业务访问不通的方法,其特征在于,所述方法用于第一网关设备,所述方法包括:

接收业务请求报文,其中所述请求报文由第二网关设备发出,经中转设备转发给所述第一网关设备;

获取第一端口信息,其中所述第一端口信息为所述请求报文中所含的端口信息;

使用所述第一端口信息更新第二端口信息,其中所述第二端口信息为所述第一网关设备本地加解封装策略中用于添加到回应报文的端口信息,所述第二端口信息在更新前为所述第一网关设备和第二网关设备通信协商时所确定的端口信息;

所述中转设备为NAT设备,所述业务为基于IPSec协议的业务,所述第一网关设备和第二网关设备为VPN网关设备,所述第二网关设备和中转设备在公网环境中,所述第一网关设备是所述中转设备下的内网设备。

2.根据权利要求1所述的方法,其特征在于,使用所述第一端口信息更新第二端口信息之后,所述方法还包括:

获取所述回应报文;

为所述回应报文添加所述第二端口信息;

将所述回应报文发送给所述中转设备,以使所述中转设备将所述回应报文转发给所述第二网关设备。

3.根据权利要求2所述的方法,其特征在于,为所述回应报文添加所述第二端口信息,包括:

在对所述回应报文加封装时在UDP头部填充所述第二端口信息。

4.根据权利要求2所述的方法,其特征在于:

在获取第一端口信息之前,所述方法还包括:

判断所述请求报文是否匹配所述本地加解封装策略;

如果匹配所述本地加解封装策略,则允许对所述请求报文解封装;

在获取所述回应报文之后,所述方法还包括:

判断所述回应报文是否匹配所述本地加解封装策略;

如果匹配所述本地加解封装策略,则允许对所述回应报文加封装。

5.一种解决业务访问不通的装置,其特征在于,所述装置用于第一网关设备,所述装置包括:

报文接收单元,用于接收业务请求报文,其中所述请求报文由第二网关设备发出,经中转设备转发给所述第一网关设备;

端口信息获取单元,用于获取第一端口信息,其中所述第一端口信息为所述请求报文中所含的端口信息;

端口信息更新单元,用于使用所述第一端口信息更新第二端口信息,其中所述第二端口信息为所述第一网关设备本地加解封装策略中用于添加到回应报文的端口信息,所述第二端口信息在更新前为所述第一网关设备和第二网关设备通信协商时所确定的端口信息;

所述中转设备为NAT设备,所述业务为基于IPSec协议的业务,所述第一网关设备和第二网关设备为VPN网关设备,所述第二网关设备和中转设备在公网环境中,所述第一网关设备是所述中转设备下的内网设备。

6.根据权利要求5所述的装置,其特征在于,所述装置还包括:

报文发送单元,用于获取所述回应报文;为所述回应报文添加所述第二端口信息;将所述回应报文发送给所述中转设备,以使所述中转设备将所述回应报文转发给所述第二网关设备。

7.根据权利要求6所述的装置,其特征在于,所述报文发送单元用于为所述回应报文添加所述第二端口信息时,具体用于:

在对所述回应报文加封装时,在UDP头部填充所述第二端口信息。

8.根据权利要求6所述的装置,其特征在于,所述装置还包括:

策略匹配单元,用于判断所述请求报文是否匹配所述本地加解封装策略;如果匹配所述本地加解封装策略,则允许对所述请求报文解封装;判断所述回应报文是否匹配所述本地加解封装策略;如果匹配所述本地加解封装策略,则允许对所述回应报文加封装。

一种解决业务访问不通的方法和装置

技术领域

[0001] 本申请涉及网络通信技术领域,特别涉及一种解决业务访问不通的方法和装置。

背景技术

[0002] VPN(Virtual Private Network)即虚拟专用网络,其作用是在公用网络上建立专用网络,以进行加密通讯。当前随着经济和社会的快速发展,企业信息化程度不断提高,企业各地分公司\办事处与企业总部的信息交互、企业与客户之间的信息传递等需求逐渐被释放,基于IPSec(Internet Protocol Security)的VPN技术被更加广泛的应用,同时VPN的应用场景也越来越多样化,经常被应用于较复杂的组网环境中,其中将VPN部署在有NAT(Network Address Translation网络地址转换)穿越的网络环境中越来越常见。

[0003] 在NAT环境中的VPN连接建立成功后,如果不再有业务流量,则之前的业务数据报文信息在VPN设备上会因老化而被删除。而当下一次的IPSec业务正向报文(或者称为请求报文)经过NAT环境时,其报文的源端口可能会发生改变,例如正向报文的发起方VPN设备加密后的报文源端口为4500,转发过程中经过NAT设备转换后可能变为53560。这样该正向报文的端口信息与VPN对端设备保存的加解封装策略端口信息不一致,而反向报文(或者称为回应报文)是按照VPN设备保存的加解封装策略进行加密封装的,使得加密封装后的正向报文的目的端口可能会与正向报文的源端口不一致,导致正向请求/反向回应的报文的端口不一致,进而导致回应报文在NAT环境中丢包,造成VPN业务访问不通。

[0004] 鉴于存在以上这种业务访问不通的情况,在现有技术中,一种解决办法是开启IPSec保活机制,即保持端口不变,以避免出现因端口不一致而丢包的问题。然而发明人在实现本发明的过程中发现,如果对于VPN隧道较多的网关出口开启保活机制,则每个隧道发送的保活报文也会比较多,在业务数据流量也较大的时候,可能会拥堵网络带宽,影响带宽负荷。可见现有技术中尚未很好的解决NAT环境中IPSec业务访问不通的问题。

发明内容

[0005] 有鉴于此,本申请提供一种解决业务访问不通的方法和装置,以有效解决一些环境中业务访问受阻的问题。

[0006] 具体地,本申请是通过如下技术方案实现的:

[0007] 一种解决业务访问不通的方法,用于第一网关设备,所述方法包括:

[0008] 接收业务请求报文,其中所述请求报文由第二网关设备发出,经中转设备转发给所述第一网关设备;

[0009] 获取第一端口信息,其中所述第一端口信息为所述请求报文中所含的端口信息;

[0010] 使用所述第一端口信息更新第二端口信息,其中所述第二端口信息为所述第一网关设备本地加解封装策略中用于添加到回应报文的端口信息,所述第二端口信息在更新前为所述第一网关设备和第二网关设备通信协商时所确定的端口信息。

[0011] 一种解决业务访问不通的装置,用于第一网关设备,所述装置包括:

[0012] 报文接收单元，用于接收业务请求报文，其中所述请求报文由第二网关设备发出，经中转设备转发给所述第一网关设备；

[0013] 端口信息获取单元，用于获取第一端口信息，其中所述第一端口信息为所述请求报文中所含的端口信息；

[0014] 端口信息更新单元，用于使用所述第一端口信息更新第二端口信息，其中所述第二端口信息为所述第一网关设备本地加解封装策略中用于添加到回应报文的端口信息，所述第二端口信息在更新前为所述第一网关设备和第二网关设备通信协商时所确定的端口信息。

[0015] 由以上本发明申请提供的技术方案可见，在本方案中，在第二网关设备向第一网关设备发送业务请求报文后，第一网关设备会从接收到的请求报文中提取出第一端口信息，然后使用第一端口信息更新本地加解封装策略中的端口信息，这样通过端口信息更新机制，即使端口信息经中转设备转发时发生了变化，第一网关设备也可以封装正确的端口信息发送回应报文，克服了回应报文因端口不正确而导致的丢包问题，有效的保证了IPSec业务访问的稳定性，增强了IPSec VPN的实用性和易用性，而且无需保活报文，在业务数据流量较大的时候也不会拥堵网络带宽，不影响带宽负荷，从而很好的解决了NAT环境中VPN业务访问不通的问题。

附图说明

[0016] 图1为本申请示出的一种解决业务访问不通的方法的流程图；

[0017] 图2为本申请示出的网络组网环境示意图；

[0018] 图3为本申请示出的正向报文发送过程示意图；

[0019] 图4为本申请示出的反向报文丢包示意图；

[0020] 图5为本申请示出的一种解决业务访问不通的方法的流程图；

[0021] 图6为本申请示出的待解封装报文经过第一网关设备的处理流程图；

[0022] 图7为本申请示出的待加封装报文经过第一网关设备的处理流程图；

[0023] 图8为本申请示出的一种解决业务访问不通的方法的信令示意图；

[0024] 图9为本申请示出的一种解决业务访问不通的装置的示意图。

具体实施方式

[0025] 这里将详细地对示例性实施例进行说明，其示例表示在附图中。下面的描述涉及附图时，除非另有表示，不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所描述的实施方式并不代表与本申请相一致的所有实施方式。相反，它们仅是与如所附权利要求书中所详述的、本申请的一些方面相一致的装置和方法的例子。

[0026] 在本申请使用的术语是仅仅出于描述特定实施例的目的，而非旨在限制本申请。在本申请和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式，除非上下文清楚地表示其他含义。还应当理解，本文中使用的术语“和/或”是指并包含一个或多个相关联的列出项目的任何或所有可能组合。

[0027] 应当理解，尽管在本申请可能采用术语第一、第二、第三等来描述各种信息，但这些信息不应限于这些术语。这些术语仅用来将同一类型的信息彼此区分开。例如，在不脱离

本申请范围的情况下，第一信息也可以被称为第二信息，类似地，第二信息也可以被称为第一信息。取决于语境，如在此所使用的词语“如果”可以被解释成为“在……时”或“当……时”或“响应于确定”。

[0028] 请参见图1，图1为本申请示出的一种解决业务访问不通的方法的流程图，该方法可用于第一网关设备，包括以下步骤：

[0029] 步骤S101，接收业务请求报文，其中所述请求报文由第二网关设备发出，经中转设备转发给所述第一网关设备。

[0030] 对于第一网关设备、第二网关设备、中转设备的具体形式，以及业务的具体内容，本实施例并不进行限制，本领域技术人员可以根据不同需求\不同场景而自行选择、设计，可以在此处使用的这些选择和设计都没有背离本发明的精神和保护范围。

[0031] 下面以NAT环境中IPSec业务访问为例进行说明，作为示例中转设备可以为NAT设备，所述业务可以为基于IPSec协议的业务，所述第一网关设备和第二网关设备可以为VPN网关设备：

[0032] IPSec即Internet Protocol Security，指采用IPSec协议来实现远程接入的一种VPN技术，用以提供公用和专用网络的端对端加密和验证服务。IPSec隧道是网络中两IPSec实体建立起来的虚拟连接通信通道。NAT穿越:Network Address Translation网络地址转换，可以让那些使用私有地址的内部网络连接到Internet或其它IP网络上，NAT路由在将内部网络的数据包发送到公用网络时，在IP包的报头把私有地址转换成合法的IP地址，同时也会将源端口转换成其它端口。IPSec在NAT环境中的控制报文和数据报文都是经过UDP封装的，目的端口为4500。VPN设备中保存的IPSec加解封装信息默认是控制通道协商的结果。

[0033] 作为示例请参见图2所示，图2为本申请示出的网络组网环境示意图。图2中的A、B、C为该示例性简易网络组网环境中的三台设备，其中A(即第二网关设备)和B(即第一网关设备)为VPN网关设备，C(即中转设备)为中间NAT设备，A和C在公网环境中，B是C下的内网设备。A和B之间建立IPSec隧道。

[0034] 步骤S102，获取第一端口信息，其中所述第一端口信息为所述请求报文中所含的端口信息。

[0035] 作为示例可参见图3所示，图3为本申请示出的正向报文发送过程示意图，当有IPSec业务数据从A设备发送到B设备时，正向报文(即请求报文P1)的源端口为4500，但经过设备C时，C对请求报文P1中的源端口进行了改变，例如修改为53560。B设备接收到该请求报文后进行IPSec解封装，在本步骤中，B设备将记录该请求报文P1的端口信息(包括源端口和目的端口记录)，且此时B获取到的源端口不是4500，而是53560，因为4500已被设备C修改为了53560。

[0036] 步骤S103，使用所述第一端口信息更新第二端口信息，其中所述第二端口信息为所述第一网关设备本地加解封装策略中用于添加到回应报文的端口信息，所述第二端口信息在更新前为所述第一网关设备和第二网关设备通信协商时所确定的端口信息。

[0037] 使用所述第一端口信息更新第二端口信息也即使用所述第一端口信息替换原有的第二端口信息。

[0038] 第一、第二网关设备建立点对点连接时会先进行协商，从而确定加解封装策略并保存在本地，其中就包括端口信息。例如加解封策略中的源端口和目的端口均为4500，则现

有技术中第一网关设备向第二网关设备发送反向报文(即回应报文P2)时,回应报文P2所含的源端口和目的端口均为4500,作为示例可参见图4所示,图4为本申请示出的反向报文丢包示意图。由于请求报文P1的源端口为53560、目的端口为4500,所以回应报文P2到达NAT设备C时,设备C上没有源端口和目的端口均为4500的转发策略,正向请求/反向回应的报文的端口不一致,造成反向回应报文P2被设备C丢弃,无法到达请求端A,使得设备A所请求的业务不通。

[0039] 而在本步骤中,B设备在发送回应报文P2前,已将存储的IPSec加解封装策略的端口信息替换为接收到的请求报文P1的端口信息,例如加封装策略的目的端口修改为请求报文P1的源端口53560,这样回应报文P2到达设备C后,设备C检测出该回应报文P2的端口信息与请求报文P1的端口信息是相匹配的,能够成功进行NAT还原操作,便将NAT还原后的报文发送给A设备,这样业务报文顺利到达A设备,使业务通畅。

[0040] 参见图5所示,在本实施例或本发明其他某些实施例中,使用所述第一端口信息更新第二端口信息之后,所述方法还可以包括:

[0041] 步骤S501,获取所述回应报文。例如第一网关设备从内层得到针对请求报文的回应报文。

[0042] 步骤S502,为所述回应报文添加所述第二端口信息。

[0043] 易知此时的第二端口信息已被更新,即原有的第二端口信息被替换为第一端口信息。

[0044] 步骤S503,将所述回应报文发送给所述中转设备,以使所述中转设备将所述回应报文转发给所述第二网关设备。

[0045] 另外,对于如何在回应报文添加所述第二端口信息,本发明实施例并不进行限制,例如为所述回应报文添加所述第二端口信息,可以包括:

[0046] 在对所述回应报文加封装时,在UDP头部填充所述第二端口信息。

[0047] 此外,在本实施例或本发明其他某些实施例中,在获取第一端口信息之前,所述方法还可以包括:

[0048] 判断所述请求报文是否匹配所述本地加解封装策略;

[0049] 如果匹配所述本地加解封装策略,则允许对所述请求报文解封装;

[0050] 如果不匹配所述本地加解封装策略,则不再向下执行,例如直接丢弃,或者若匹配上了其他加解封装策略,则按其他加解封装策略处理。

[0051] 在获取所述回应报文之后,所述方法还包括:

[0052] 判断所述回应报文是否匹配所述本地加解封装策略;

[0053] 如果匹配所述本地加解封装策略,则允许对所述回应报文加封装;

[0054] 如果不匹配所述本地加解封装策略,则不再向下执行,例如直接丢弃,或者若匹配上了其他加解封装策略,则按其他加解封装策略处理。

[0055] 在本发明实施例中,在第二网关设备向第一网关设备发送业务请求报文后,第一网关设备会从接收到的请求报文中提取出第一端口信息,然后使用第一端口信息更新本地加解封装策略中的端口信息,这样通过端口信息更新机制,即使端口信息经中转设备转发时发生了变化,第一网关设备也可以封装正确的端口信息发送回应报文,克服了回应报文因端口不正确而导致的丢包问题,有效的保证了IPSec业务访问的稳定性,增强了IPSec

VPN的实用性和易用性，而且无需保活报文，在业务数据流量较大的时候也不会拥堵网络带宽，不影响带宽负荷，从而很好的解决了NAT环境中VPN业务访问不通的问题。

[0056] 下面再对待解封装报文经过第一网关设备的处理流程，以及待加封装报文经过第一网关设备处理流程分别进行描述。

[0057] 请参见图6，图6为本申请示出的待解封装报文经过第一网关设备的处理流程图。

[0058] 步骤S601，接收IPSec业务请求报文P1。

[0059] 步骤S602，判断是否匹配本地IPSec解封装策略。

[0060] 如果匹配本地IPSec解封装策略，则继续向下执行，如果不匹配本地IPSec解封装策略，则跳至步骤S606。

[0061] 步骤S603，使用报文P1中的源和目的端口信息更新本地策略中的源和目的端口信息。

[0062] 步骤S604，解封装IPSec业务请求报文P1。

[0063] 步骤S605，向内层转发解封装后的报文。流程结束。

[0064] 步骤S606，丢弃该报文。流程结束。

[0065] 请参见图7，图7为本申请示出的待加封装报文经过第一网关设备的处理流程图。

[0066] 步骤S701，接收内层回应报文。

[0067] 步骤S702，判断是否匹配本地IPSec加封装策略。

[0068] 如果匹配本地IPSec加封装策略，则继续向下执行，如果不匹配本地IPSec加封装策略，则跳至步骤S705。

[0069] 步骤S703，加封装内层回应报文，其中所用端口信息为更新后的本地策略中的端口信息。

[0070] 步骤S704，加封装成功后发出回应报文P2。流程结束。

[0071] 步骤S705，丢弃该报文。流程结束。

[0072] 请参见图8，图8为本申请示出的一种解决业务访问不通的方法的信令示意图：

[0073] 步骤S801，VPN网关设备A通过NAT设备C向VPN网关设备B发送IPSec业务请求报文。

[0074] 步骤S802，NAT设备C收到请求报文后，将其源端口信息从4500修改为53560。

[0075] 步骤S803，NAT设备C将修改后的请求报文转发给VPN网关设备B。

[0076] 步骤S804，VPN网关设备B收到请求报文后进行解封装并记录下其端口信息，使用所记录下的端口信息替换本地加解封装策略中的原有端口信息。

[0077] 步骤S805，VPN网关设备B将解封装后的报文发送给内层设备。

[0078] 步骤S806，内层设备进行处理。

[0079] 步骤S807，内层设备将回应报文发送给VPN网关设备B。

[0080] 步骤S808，VPN网关设备B加封装报文，此时的端口信息为替换后的本地加解封装策略中的端口信息。

[0081] 步骤S809，VPN网关设备B将加封装后的回应报文发送给NAT设备C。

[0082] 步骤S810，NAT设备C检测出该回应报文的端口信息与请求报文的端口信息是相匹配的，能够进行NAT还原操作。

[0083] 步骤S811，将NAT还原后的报文发送给VPN网关设备A。

[0084] 在本发明实施例中，在第二网关设备向第一网关设备发送业务请求报文后，第一

网关设备会从接收到的请求报文中提取出第一端口信息，然后使用第一端口信息更新本地加解封装策略中的端口信息，这样通过端口信息更新机制，即使端口信息经中转设备转发时发生了变化，第一网关设备也可以封装正确的端口信息发送回应报文，克服了回应报文因端口不正确而导致的丢包问题，有效的保证了IPSec业务访问的稳定性，增强了IPSec VPN的实用性和易用性，而且无需保活报文，在业务数据流量较大的时候也不会拥堵网络带宽，不影响带宽负荷，从而很好的解决了NAT环境中VPN业务访问不通的问题。

[0085] 请参见图9，图9为本申请示出的一种解决业务访问不通的装置的示意图，该装置可用于第一网关设备，该装置可以包括：

[0086] 报文接收单元901，用于接收业务请求报文，其中所述请求报文由第二网关设备发出，经中转设备转发给所述第一网关设备。

[0087] 作为示例中转设备为NAT设备，所述业务为基于IPSec协议的业务，所述第一网关设备和第二网关设备为VPN网关设备。

[0088] 端口信息获取单元902，用于获取第一端口信息，其中所述第一端口信息为所述请求报文中所含的端口信息。

[0089] 端口信息更新单元903，用于使用所述第一端口信息更新第二端口信息，其中所述第二端口信息为所述第一网关设备本地加解封装策略中用于添加到回应报文的端口信息，所述第二端口信息在更新前为所述第一网关设备和第二网关设备通信协商时所确定的端口信息。

[0090] 在本实施例或本发明其他某些实施例中，所述装置还可以包括：

[0091] 报文发送单元，用于获取所述回应报文；为所述回应报文添加所述第二端口信息；将所述回应报文发送给所述中转设备，以使所述中转设备将所述回应报文转发给所述第二网关设备。

[0092] 在本实施例或本发明其他某些实施例中，所述报文发送单元用于为所述回应报文添加所述第二端口信息时，具体用于：

[0093] 在对所述回应报文加封装时，在UDP头部填充所述第二端口信息。

[0094] 在本实施例或本发明其他某些实施例中，所述装置还可以包括：

[0095] 策略匹配单元，用于判断所述请求报文是否匹配所述本地加解封装策略；如果匹配所述本地加解封装策略，则允许对所述请求报文解封装；判断所述回应报文是否匹配所述本地加解封装策略；如果匹配所述本地加解封装策略，则允许对所述回应报文加封装。

[0096] 上述装置中各个单元的功能和作用的实现过程具体详见上述方法中对应步骤的实现过程，在此不再赘述。

[0097] 对于装置实施例而言，由于其基本对应于方法实施例，所以相关之处参见方法实施例的部分说明即可。以上所描述的装置实施例仅仅是示意性的，其中所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部模块来实现本申请方案的目的。本领域普通技术人员在不付出创造性劳动的情况下，即可以理解并实施。

[0098] 在本发明实施例中，在第二网关设备向第一网关设备发送业务请求报文后，第一网关设备会从接收到的请求报文中提取出第一端口信息，然后使用第一端口信息更新本地

加解封装策略中的端口信息，这样通过端口信息更新机制，即使端口信息经中转设备转发时发生了变化，第一网关设备也可以封装正确的端口信息发送回应报文，克服了回应报文因端口不正确而导致的丢包问题，有效的保证了IPSec业务访问的稳定性，增强了IPSec VPN的实用性和易用性，而且无需保活报文，在业务数据流量较大的时候也不会拥堵网络带宽，不影响带宽负荷，从而很好的解决了NAT环境中VPN业务访问不通的问题。

[0099] 以上所述仅为本申请的较佳实施例而已，并不用以限制本申请，凡在本申请的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本申请保护的范围之内。

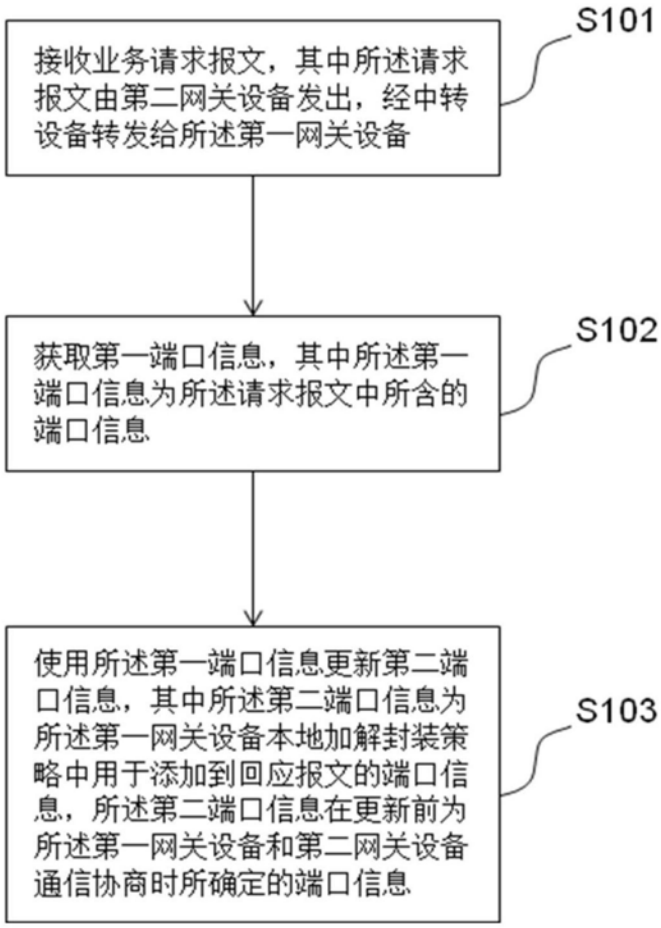

S101
接收业务请求报文，其中所述请求报文由第二网关设备发出，经中转设备转发给所述第一网关设备
S102
获取第一端口信息，其中所述第一端口信息为所述请求报文中所含的端口信息
S103
使用所述第一端口信息更新第二端口信息，其中所述第二端口信息为所述第一网关设备本地加解封装策略中用于添加到回应报文的端口信息，所述第二端口信息在更新前为所述第一网关设备和第二网关设备通信协商时所确定的端口信息

图1

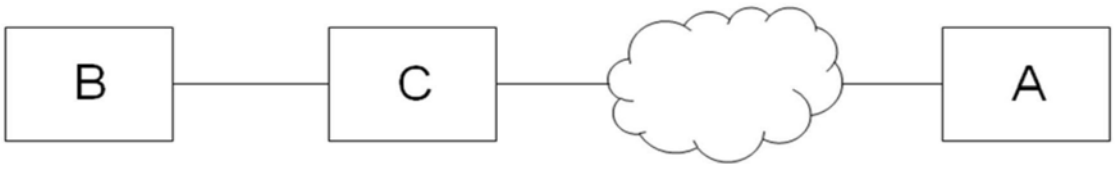

B
C
A

图2

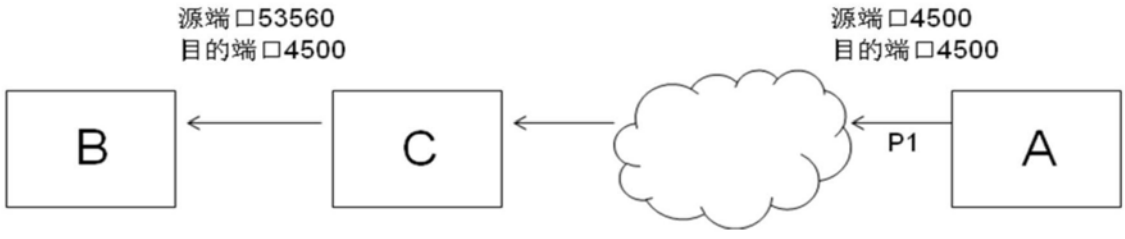

源端口53560
目的端口4500
源端口4500
目的端口4500
B
C
P1
A

图3

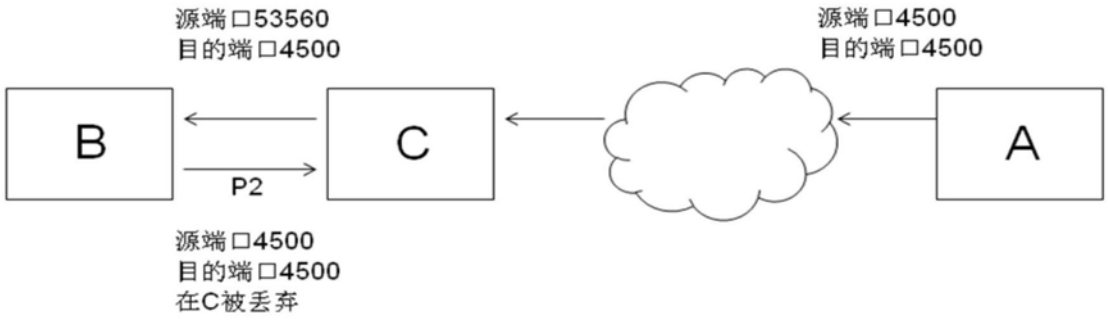

源端口53560
目的端口4500
源端口4500
目的端口4500
B
C
A
P2
源端口4500
目的端口4500
在C被丢弃

图4

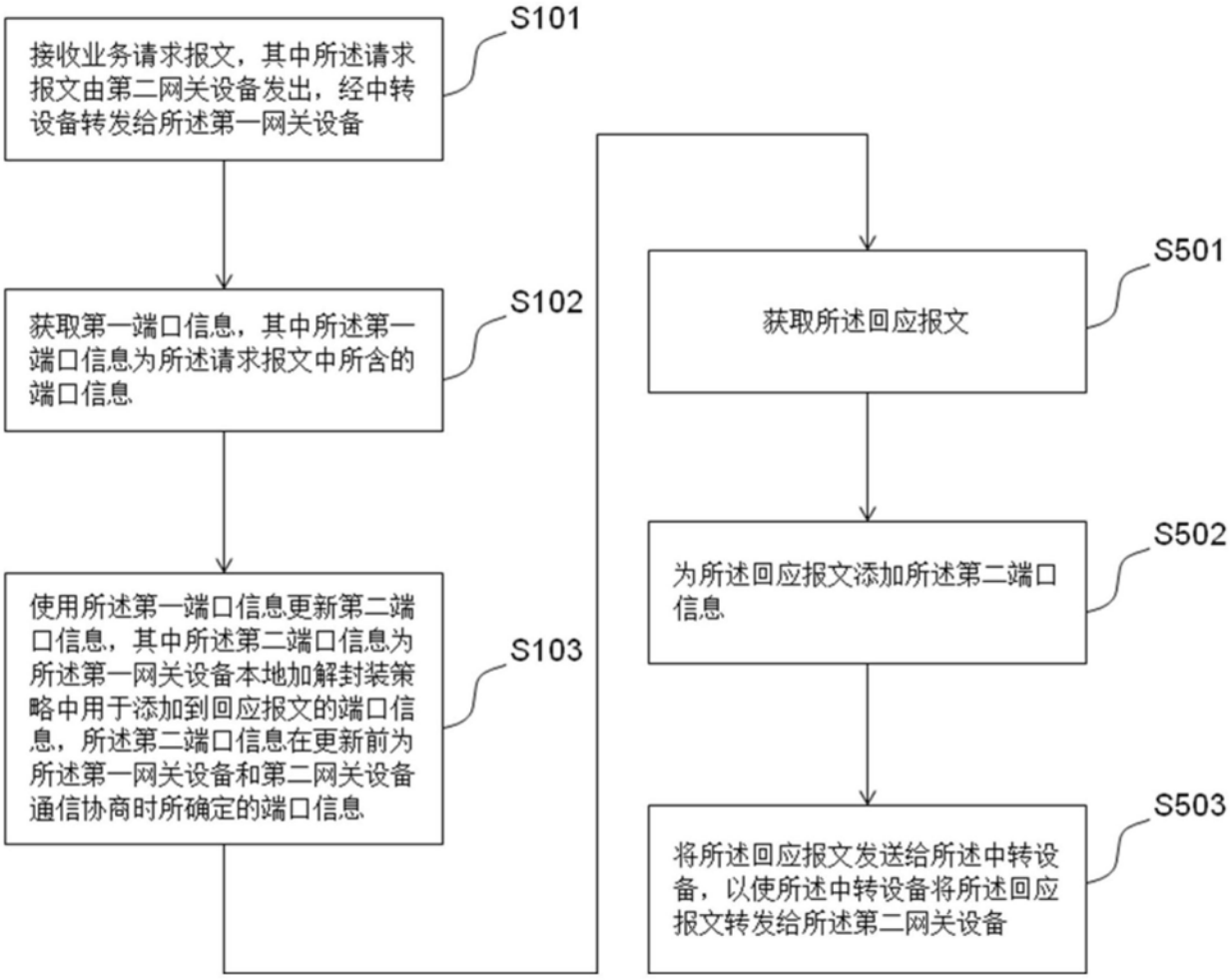

S101
接收业务请求报文，其中所述请求报文由第二网关设备发出，经中转设备转发给所述第一网关设备
S102
获取第一端口信息，其中所述第一端口信息为所述请求报文中所含的端口信息
S103
使用所述第一端口信息更新第二端口信息，其中所述第二端口信息为所述第一网关设备本地加解封装策略中用于添加到回应报文的端口信息，所述第二端口信息在更新前为所述第一网关设备和第二网关设备通信协商时所确定的端口信息
S501
获取所述回应报文
S502
为所述回应报文添加所述第二端口信息
S503
将所述回应报文发送给所述中转设备，以使所述中转设备将所述回应报文转发给所述第二网关设备

图5

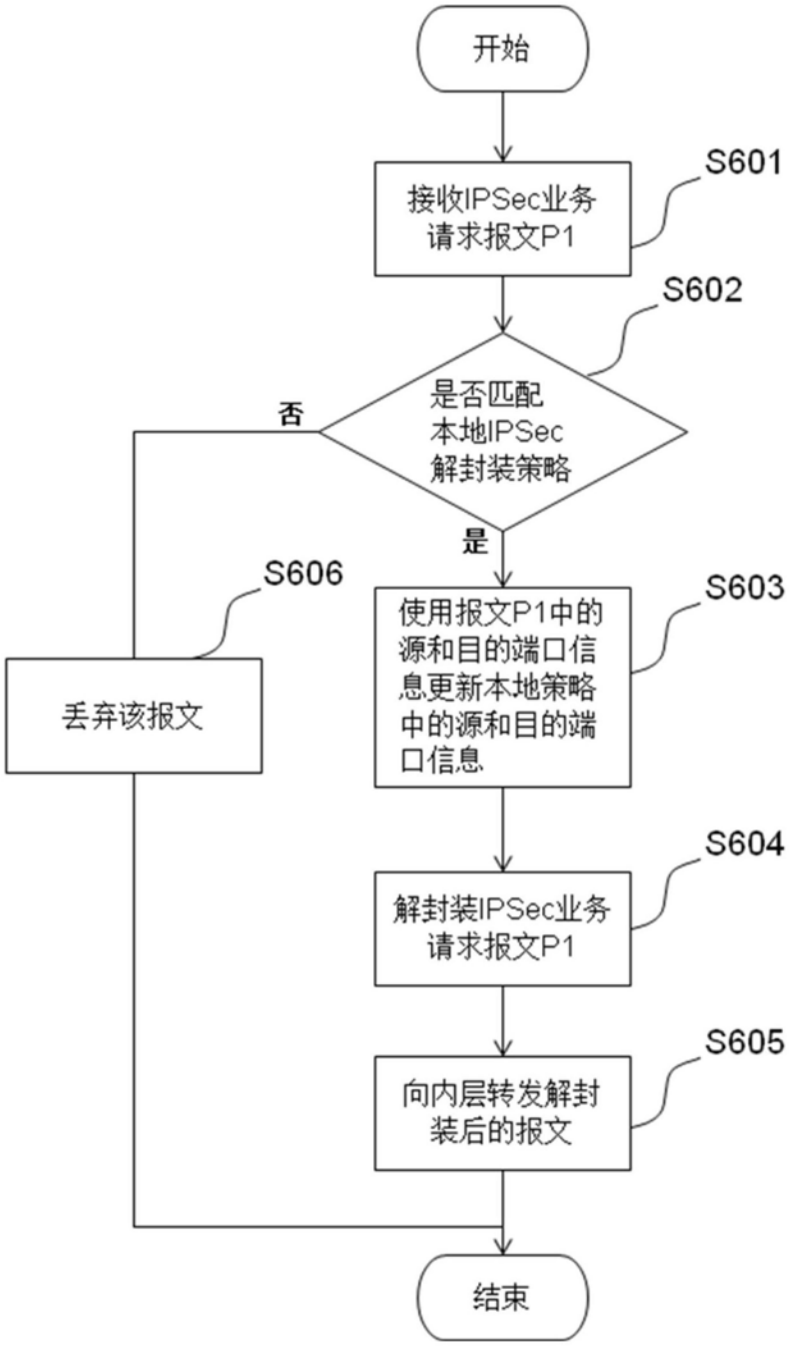

开始
接收IPSec业务请求报文P1
S601
是否匹配本地IPSec解封装策略
S602
否
是
S606
丢弃该报文
使用报文P1中的源和目的端口信息更新本地策略中的源和目的端口信息
S603
解封装IPSec业务请求报文P1
S604
向内层转发解封装后的报文
S605
结束

图6

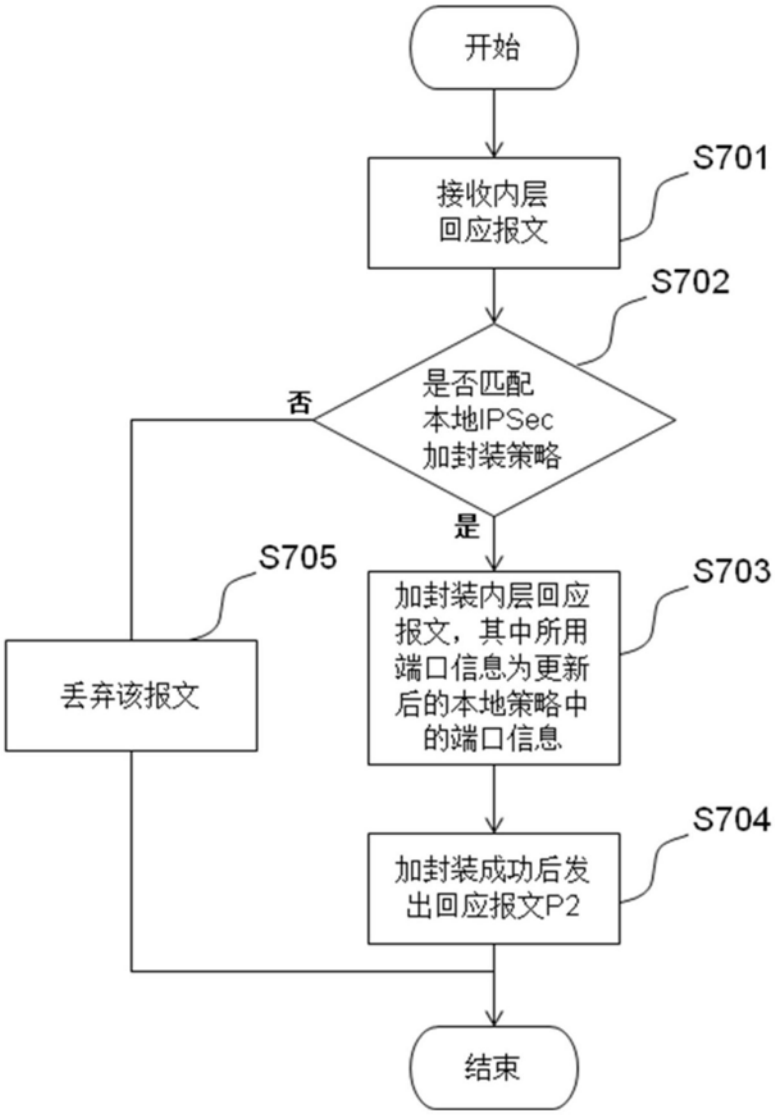

开始
接收内层
回应报文
S701
S702
是否匹配
本地IPSec
加封装策略
否
是
S705
丢弃该报文
S703
加封装内层回应
报文，其中所用
端口信息为更新
后的本地策略中
的端口信息
S704
加封装成功后发
出回应报文P2
结束

图7

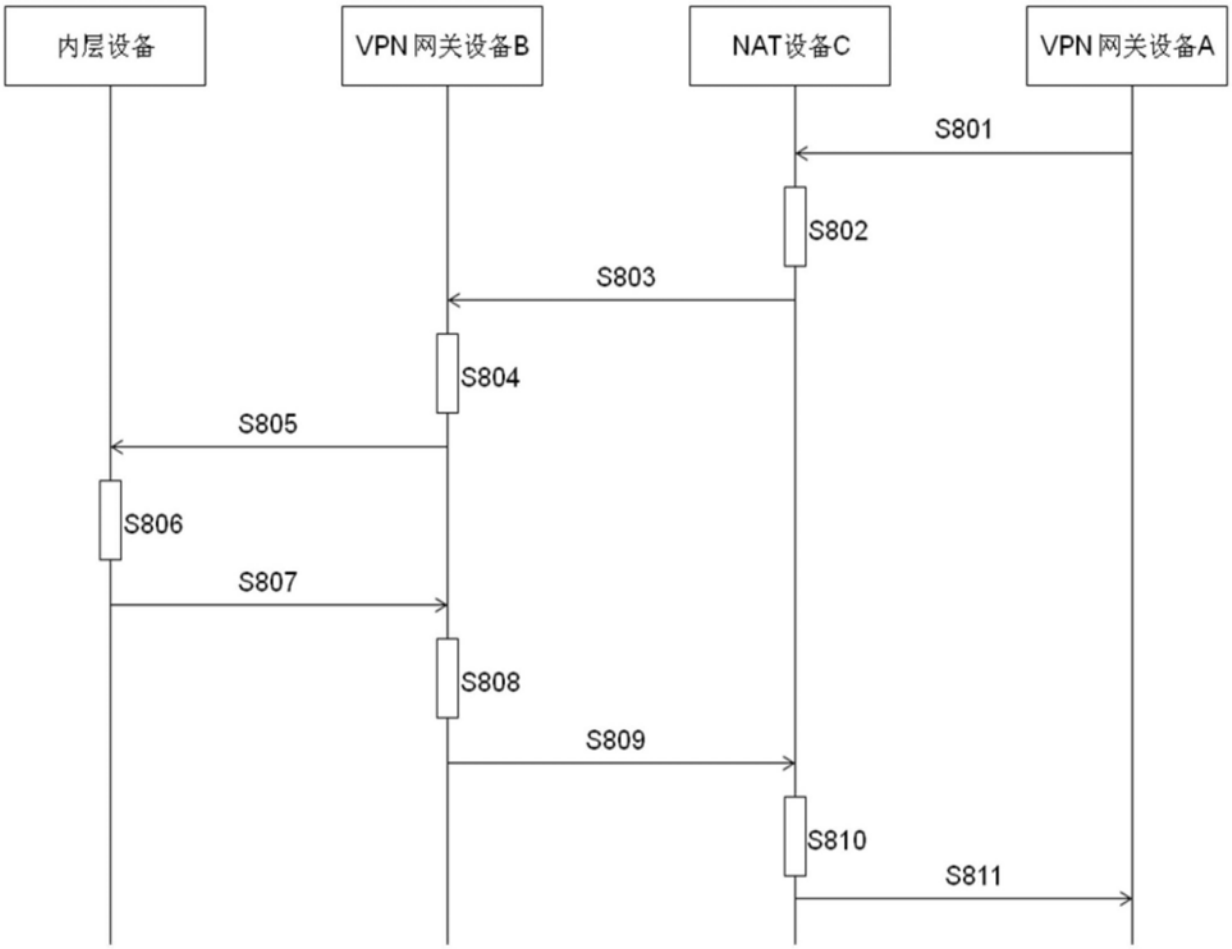

内层设备
VPN网关设备B
NAT设备C
VPN网关设备A
S801
S802
S803
S804
S805
S806
S807
S808
S809
S810
S811

图8

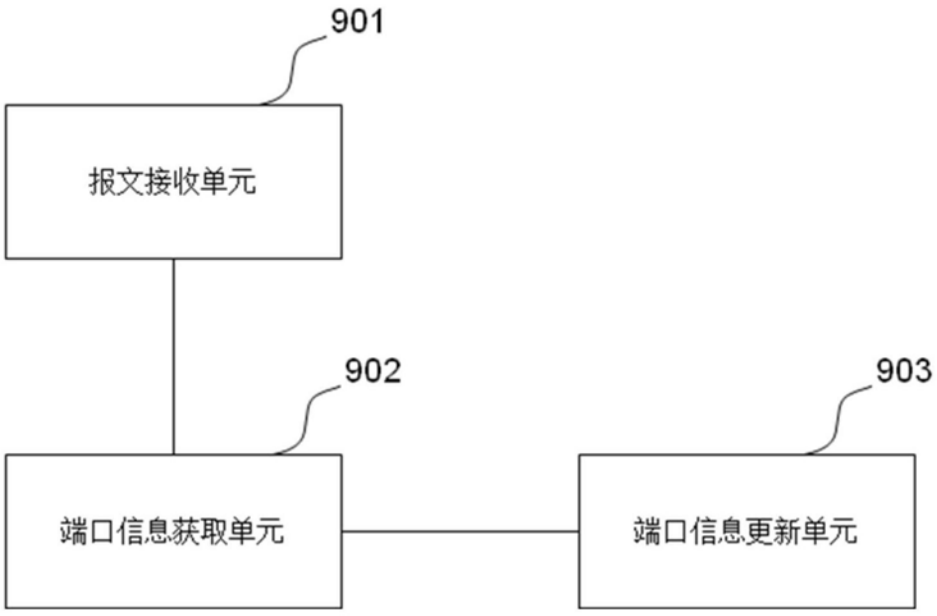

901
报文接收单元
902
端口信息获取单元
903
端口信息更新单元

图9