(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 112636913 B
(45)授权公告日 2021.06.22

(21)申请号 202110242847.0
(22)申请日 2021.03.05
(65)同一申请的已公布的文献号
申请公布号 CN 112636913 A
(43)申请公布日 2021.04.09
(73)专利权人 广东睿江云计算股份有限公司
地址 528000 广东省佛山市禅城区岭南大道北121号二座705-708房
(72)发明人 梁润强 李卢群 韩帆 史伟
(74)专利代理机构 佛山市恒瑞知识产权代理事务所(普通合伙) 44688
代理人 史亮亮
(51)Int.Cl.
H04L 9/14(2006.01)
H04L 29/06(2006.01)
H04L 12/741(2013.01)

(56)对比文件
CN 109041169 A,2018.12.18
CN 111884816 A,2020.11.03
CN 1599312 A,2005.03.23
CN 103975552 A,2014.08.06
CN 107005562 A,2017.08.01
US 2016164782 A1,2016.06.09

审查员 左羽

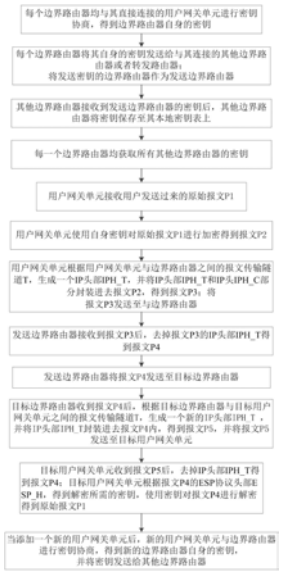
权利要求书2页 说明书8页 附图2页

(54)发明名称

一种密钥共享的组网方法

(57)摘要

本发明公开了一种密钥共享的组网方法，通过在用户网关单元安全接入边界路由器后，再由安全通道共享已有的用户网关密钥，使得每个用户网关都具备其他用户网关单元的密钥，然后用户网关单元把加密的报文，使用隧道直接封装加密后的部分，原报文IP头不加密而是完整地放在隧道IP头的扩展部分，使得原IP头信息得以保留，边界路由器接收到用户网关的报文后，采取解封而不解密的动作，把原IP头恢复，根据原IP头进行路由至目标边界路由器，边界路由器重新进行隧道封装并把报文发至目标用户网关单元，最后由目标用户网关解封解密并发至对应的用户。本发明只需要一次加密和解密，使得边界路由器的负担大大减少，并提高了报文转发效率。



CN 112636913 B

1.一种密钥共享的组网方法,其运行于一种密钥共享的组网系统上,所述组网系统包括若干用户网关单元和若干路由器,路由器分为边界路由器以及转发路由器,其中,边界路由器与用户网关单元连接,转发路由器连接边界路由器或者转发路由器连接另一个转发路由器,其特征在于,所述一种密钥共享的组网方法,包括以下步骤:

步骤S1、每个边界路由器均与其直接连接的用户网关单元进行密钥协商,得到边界路由器自身的密钥;用户网关单元将密钥保存至其本地密钥表上,以及边界路由器将密钥保存至其本地密钥表上;

步骤S2、每个边界路由器将其自身的密钥发送给与其连接的其他边界路由器或者转发路由器;此时,将发送密钥的边界路由器作为发送边界路由器;

步骤S3、当其他边界路由器接收到发送边界路由器的密钥后,其他边界路由器将密钥保存至其本地密钥表上;或者,当转发路由器接收到发送边界路由器的密钥后,转发路由器则将密钥转发至与其连接的转发路由器或者边界路由器;

步骤S4、重复步骤S2-步骤S3,直至每一个边界路由器均获取所有其他边界路由器的密钥;每一个边界路由器将所有其他边界路由器的密钥保存在其本地密钥表上,并将所有其他边界路由器的密钥发送给与其直接连接的用户网关单元,用户网关单元将所有其他边界路由器的密钥保存至其本地密钥表上。

2.根据权利要求1所述的一种密钥共享的组网方法,其特征在于,所述步骤S1中,所述边界路由器均与其直接连接的用户网关单元进行密钥协商,其具体为:边界路由器均与其直接连接的用户网关单元进行IKEv2密钥协商,得到边界路由器自身的密钥,所述边界路由器自身的密钥包括SPI标识符、密钥KEY1和密钥KEY2;其中,所述SPI标识符用于对应标记用户网关单元,每一个用户网关单元都有唯一的SPI标识符,所述密钥KEY1为加密算法密钥,所述密钥KEY2为验证算法密钥。

3.根据权利要求2所述的一种密钥共享的组网方法,其特征在于,所述边界路由器自身的密钥为IPSEC密钥。

4.根据权利要求2所述的一种密钥共享的组网方法,其特征在于,所述步骤S1还包括:在每个边界路由器与其直接连接的用户网关单元之间,使用ESP协议作为加密协议并创建报文传输隧道T。

5.根据权利要求4所述的一种密钥共享的组网方法,其特征在于,所述步骤S4后还包括以下步骤:

步骤S5、用户网关单元接收用户发送过来的原始报文P1,原始报文P1包括IP头IPH_C部分和载荷P_C报文内容部分;

步骤S6、用户网关单元使用自身密钥中的密钥KEY1对载荷P_C报文内容部分进行加密得到加密报文内容ESP_PAYLOAD部分,使用密钥KEY2对加密报文内容ESP_PAYLOAD部分进行检验生成检验部分ESP_T,再生成一个ESP协议头部ESP_H,上述ESP协议头部ESP_H包括用户网关单元自身密钥中的SPI;

用户网关单元对ESP协议头部ESP_H、加密报文内容ESP_PAYLOAD部分以及检验部分ESP_T一起进行封装得到报文P2;

步骤S7、用户网关单元根据用户网关单元与边界路由器之间的报文传输隧道T,生成一个IP头部IPH_T,并将IP头部IPH_T和IP头IPH_C部分封装进去报文P2,得到报文P3,报文P3

包括IP头部IPH_T、IP头IPH_C部分以及报文P2;用户网关单元将报文P3发送至与其连接的边界路由器,此时将发送报文P3的用户网关单元作为发送用户网关单元,将接收报文P3的边界路由器作为发送边界路由器;

步骤S8、发送边界路由器接收到报文P3后,去掉报文P3的IP头部IPH_T得到报文P4,报文P4包括IP头IPH_C部分和报文P2;发送边界路由器根据报文P4的IP头IPH_C部分,得到接收报文P4对应的用户网关单元,将接收报文P4对应的用户网关单元称为目标用户网关单元,将与目标用户网关单元直接连接的边界路由器称为目标边界路由器;

步骤S9、发送边界路由器将报文P4发送至目标边界路由器,具体为:

若发送边界路由器与目标边界路由器直接连接,则发送边界路由器直接将报文P4发送至目标边界路由器;

若发送边界路由器发送报文P4过程中需要经过若干转发路由器,则发送边界路由器首先将报文P4发送给转发路由器,转发路由器根据IP头IPH_C部分中的目标IP地址将报文P4发送给下一个转发路由器,直至将报文P4发送至目标边界路由器;

步骤S10、目标边界路由器收到报文P4后,根据目标边界路由器与目标用户网关单元之间的报文传输隧道T,生成一个新的IP头部IPH_T,并将IP头部IPH_T封装进去报文P4内,得到报文P5,并将报文P5发送至目标用户网关单元;

步骤S11、目标用户网关单元收到报文P5后,去掉IP头部IPH_T得到报文P4;目标用户网关单元根据报文P4的ESP协议头部ESP_H,得到解密所需的密钥;

目标用户网关单元使用密钥KEY2对加密报文内容ESP_PAYLOAD部分进行校验生成一个ESP_T校验结果,判断ESP_T校验结果与报文P4的检验部分ESP_T是否一致,若一致,则目标用户网关单元使用所需的密钥中的密钥KEY1对报文P4的加密报文内容ESP_PAYLOAD部分进行解密得到原始报文P1的载荷P_C报文内容部分,并将将载荷P_C报文内容部分和报文P4的IP头IPH_C部分结合得到原始报文P1;目标用户网关单元将原始报文P1发给用户;

若ESP_T校验结果与报文P4的检验部分ESP_T不一致,则目标用户网关单元丢弃报文P4。

6.根据权利要求5所述的一种密钥共享的组网方法,其特征在于,所述步骤S11后还包括以下步骤:

步骤S12、当添加一个新的用户网关单元后,新的用户网关单元需要连接一个边界路由器,则新的用户网关单元与边界路由器进行密钥协商,得到边界路由器自身的密钥;边界路由器将自身的密钥均发给其他边界路由器;其他边界路由器收到密钥保存至其本地密钥表上,并将密钥发送给与其直接连接的用户网关单元,用户网关单元将密钥保存至其本地密钥表上;

与新的用户网关单元连接的边界路由器将其本地密钥表上的所有密钥发送给新的用户网关单元,新的用户网关单元接收到所有密钥保存至其本地密钥表上;

步骤S13、重复步骤S5-步骤S11。

一种密钥共享的组网方法

技术领域

[0001] 本发明涉及云计算网络技术领域,特别涉及一种密钥共享的组网方法。

背景技术

[0002] 互联网的普及,云计算的浪潮,让我们越来越离不开网络环境。随着移动互联网的快速发展,各种应用和服务层出不穷,应用开发商和服务提供商等需要快速实施他们的项目或产品,在传统的IDC数据中心中一般需要布置他们自己或者租用服务器设备并且还需要自己组建复杂的网络,这其间必定需要大量的时间并且非常容易出错,也不容易扩展和实现灾备。

[0003] 云计算和虚拟化网络作为未来的发展方向,将会使得组网和服务部署变得更加简便,快速部署并分布在不同地点的多个网络,一般也需要进行相互打通,随着网络节点的增加,网络打通的复杂程序也会倍数增长,目前在云计算的网络环境下,一般提供用户使用基于互联网的IPSEC组网方式,由于每个地方节点需要为很多个用户提供安全接入组网,往往一个节点的接入设备可能需要提供成千上万的用户接入服务,所以如何高效地为用户提供加密的传输成为重点需要解决的问题。

[0004] 不同地域的私有网络需要互联互通,并且需要高效地传输,首先需要使用IPSEC安全接入技术,然后在接入边界路由器到目标边界路由器之间进行高效的转发,这个与星型的VPN组网有点相像,不过与星型VPN的中心不同,云计算场景下提供多用户组网互联互通下的中心,是由多个地方节点路由器组成的巨大的路由器转发网,由于用户加密后的报文,需要先到达中心,再由中心转达至目标,一般传统的星型VPN,需要在中心进行一次解密,然后再进行另一次加密,到达目标用户后,再进行最后一次解密,这其间多了一次加密和解密的过程,由于加解密算法的演进和软硬件的进步,加解密的消耗变得越来越少了,但是云计算场景下,一个包含安全接入的路由器组成的转发网,往往需要提供成千上万个用户安全接入并传输数据,单个用户额外增加的加解密操作或许可以忽略不计,但是成千上万个用户增加的加解密操作,往往会使得边界路由器不堪重负。

发明内容

[0005] 本发明为了解决上述问题之一,提供一种密钥共享的组网方法,通过对用户网关单元的密钥进行相互学习及记录,然后在边界路由器处只负责接收用户网关单元的加密报文,只解封而不解密并进行路由转发,最后送达目标用户网关单元后,再进行解密操作,使得用户网关可以专注于数据的安全,让路由器专注于数据的转发,减轻了路由器的负担,提高了报文的转发效率。

[0006] 为解决上述技术问题,本发明提供如下技术方案:一种密钥共享的组网方法,其运行于一种密钥共享的组网系统上,所述组网系统包括若干用户网关单元和若干路由器,路由器分为边界路由器以及转发路由器,其中,边界路由器与用户网关单元连接,转发路由器连接边界路由器或者转发路由器连接另一个转发路由器;所述一种密钥共享的组网方法,

包括以下步骤：

[0007] 步骤S1、每个边界路由器均与其直接连接的用户网关单元进行密钥协商，得到边界路由器自身的密钥；用户网关单元将密钥保存至其本地密钥表上，以及边界路由器将密钥保存至其本地密钥表上；

[0008] 步骤S2、每个边界路由器将其自身的密钥发送给与其连接的其他边界路由器或者转发路由器；此时，将发送密钥的边界路由器作为发送边界路由器；

[0009] 步骤S3、当其他边界路由器接收到发送边界路由器的密钥后，其他边界路由器将密钥保存至其本地密钥表上；或者，当转发路由器接收到发送边界路由器的密钥后，转发路由器则将密钥转发至与其连接的转发路由器或者边界路由器；

[0010] 步骤S4、重复步骤S2-步骤S3，直至每一个边界路由器均获取所有其他边界路由器的密钥；每一个边界路由器将所有其他边界路由器的密钥保存在其本地密钥表上，并将所有其他边界路由器的密钥发送给与其直接连接的用户网关单元，用户网关单元将所有其他边界路由器的密钥保存至其本地密钥表上。

[0011] 进一步地，所述步骤S1中，所述边界路由器均与其直接连接的用户网关单元进行密钥协商，其具体为：边界路由器均与其直接连接的用户网关单元进行IKEv2密钥协商，得到边界路由器自身的密钥，所述边界路由器自身的密钥包括SPI标识符、密钥KEY1和密钥KEY2；其中，所述SPI标识符用于对应标记用户网关单元，每一个用户网关单元都有唯一的SPI标识符，所述密钥KEY1为加密算法密钥，所述密钥KEY2为验证算法密钥。

[0012] 进一步地，所述边界路由器自身的密钥为IPSEC密钥。

[0013] 进一步地，所述步骤S1还包括：在每个边界路由器与其直接连接的用户网关单元之间，使用ESP协议作为加密协议并创建报文传输隧道T。

[0014] 进一步地，所述步骤S4后还包括以下步骤：

[0015] 步骤S5、用户网关单元接收用户发送过来的原始报文P1，原始报文P1包括IP头IPH_C部分和载荷P_C报文内容部分；

[0016] 步骤S6、用户网关单元使用自身密钥中的密钥KEY1对载荷P_C报文内容部分进行加密得到加密报文内容ESP_PAYLOAD部分，使用密钥KEY2对加密报文内容ESP_PAYLOAD部分进行检验生成检验部分ESP_T，再生成一个ESP协议头部ESP_H，上述ESP协议头部ESP_H包括用户网关单元自身密钥中的SPI；

[0017] 用户网关单元对ESP协议头部ESP_H、加密报文内容ESP_PAYLOAD部分以及检验部分ESP_T一起进行封装得到报文P2；

[0018] 步骤S7、用户网关单元根据用户网关单元与边界路由器之间的报文传输隧道T，生成一个IP头部IPH_T，并将IP头部IPH_T和IP头IPH_C部分封装进去报文P2，得到报文P3，报文P3包括IP头部IPH_T、IP头IPH_C部分以及报文P2；用户网关单元将报文P3发送至与其连接的边界路由器，此时将发送报文P3的用户网关单元作为发送用户网关单元，将接收报文P3的边界路由器作为发送边界路由器；

[0019] 步骤S8、发送边界路由器接收到报文P3后，去掉报文P3的IP头部IPH_T得到报文P4，报文P4包括IP头IPH_C部分和报文P2；发送边界路由器根据报文P4的IP头IPH_C部分，得到接收报文P4对应的用户网关单元，将接收报文P4对应的用户网关单元称为目标用户网关单元，将与目标用户网关单元直接连接的边界路由器称为目标边界路由器；

[0020] 步骤S9、发送边界路由器将报文P4发送至目标边界路由器，具体为：

[0021] 若发送边界路由器与目标边界路由器直接连接，则发送边界路由器直接将报文P4发送至目标边界路由器；

[0022] 若发送边界路由器发送报文P4过程中需要经过若干转发路由器，则发送边界路由器首先将报文P4发送给转发路由器，转发路由器根据IP头IPH_C部分中的目标IP地址将报文P4发送给下一个转发路由器，直至将报文P4发送至目标边界路由器；

[0023] 步骤S10、目标边界路由器收到报文P4后，根据目标边界路由器与目标用户网关单元之间的报文传输隧道T，生成一个新的IP头部IPH_T，并将IP头部IPH_T封装进去报文P4内，得到报文P5，并将报文P5发送至目标用户网关单元；

[0024] 步骤S11、目标用户网关单元收到报文P5后，去掉IP头部IPH_T得到报文P4；目标用户网关单元根据报文P4的ESP协议头部ESP_H，得到解密所需的密钥；

[0025] 目标用户网关单元使用密钥KEY2对加密报文内容ESP_PAYLOAD部分进行校验生成一个ESP_T校验结果，判断ESP_T校验结果与报文P4的检验部分ESP_T是否一致，若一致，则目标用户网关单元使用所需的密钥中的密钥KEY1对报文P4的加密报文内容ESP_PAYLOAD部分进行解密得到原始报文P1的载荷P_C报文内容部分，并将将载荷P_C报文内容部分和报文P4的IP头IPH_C部分结合得到原始报文P1；目标用户网关单元将原始报文P1发给用户；

[0026] 若ESP_T校验结果与报文P4的检验部分ESP_T不一致，则目标用户网关单元丢弃报文P4。

[0027] 进一步地，所述步骤S11后还包括以下步骤：

[0028] 步骤S12、当添加一个新的用户网关单元后，新的用户网关单元需要连接一个边界路由器，则新的用户网关单元与边界路由器进行密钥协商，得到边界路由器自身的密钥；边界路由器将自身的密钥均发给其他边界路由器；其他边界路由器收到密钥保存至其本地密钥表上，并将密钥发送给与其直接连接的用户网关单元，用户网关单元将密钥保存至其本地密钥表上；

[0029] 与新的用户网关单元连接的边界路由器将其本地密钥表上的所有密钥发送给新的用户网关单元，新的用户网关单元接收到所有密钥保存至其本地密钥表上；

[0030] 步骤S13、重复步骤S5-步骤S11。

[0031] 采用上述技术方案后，本发明至少具有如下有益效果：本方法通过在用户网关单元安全接入边界路由器后，再由安全通道共享已有的用户网关单元的密钥，使得每个用户网关单元都具备其他用户网关单元的密钥，当然可以基于特定策略，让某些只属于特定组别的用户网关单元之间才共享密钥，符合当下云计算的网络虚拟化场景，然后用户网关单元把加密的报文，使用隧道直接封装加密后的部分，原报文IP头不加密而是完整地放在隧道IP头的扩展部分，使得原IP头信息得以保留，边界路由器接收到用户网关的报文后，采取解封而不解密的动作，把原IP头恢复，根据原IP头进行路由至目标边界路由器，边界路由器重新进行隧道封装并把报文发至目标用户网关，最后由目标用户网关解封解密并发至对应的用户，整个过程只需要一次加密和解密，边界路由器的负担大大减少了，边界路由器和一般路由器都可以专注于报文转发，大大提高报文的传输效率。

附图说明

[0032] 图1为本发明一种密钥共享的组网方法的步骤流程图。

[0033] 图2为本发明一种密钥共享的组网系统的框架图。

具体实施方式

[0034] 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结合,下面结合附图和具体实施例对本申请作进一步详细说明。

[0035] 实施例1

[0036] 本实施例一种密钥共享的组网方法,是运行于一种密钥共享的组网系统上,所述组网系统包括若干用户网关单元和若干路由器,路由器分成若干边界路由器以及若干转发路由器;其中,边界路由器和转发路由器均是一般网络上使用的路由器,为了进行区别,将与所述用户网关单元直接连接的路由器称为边界路由器,而没有直接与用户网关单元直接连接的路由器作为转发路由器;一般地,转发路由器与另一个转发路由器连接,或者某个转发路由器直接连接一个边界路由器,显而易见,转发路由器只作为一个数据传播的中转路由器;另外,也存在一种情况就是,某个边界路由器直接连接另外一个边界路由器;每个边界路由器可以连接多个用户网关单元,由于每一个用户网关单元均与一个边界路由器直接相连,一个边界路由器可以连接多个用户网关单元(所以传统组网中如果在边界路由器对加密报文解密一次,在目标边界路由器再加密一次,就会增加很多加解密操作)。另外,每个用户网关单元会直接连接用户(客户端),用于接收用户原始报文P1或者发送原始报文P1给用户。

[0037] 本实施例公开一种密钥共享的组网方法,如图1所示,包括以下步骤:

[0038] 步骤S1、每个边界路由器均与其直接连接的用户网关单元进行密钥协商,得到边界路由器自身的密钥;用户网关单元将密钥保存至其本地密钥表上,以及边界路由器将密钥保存至其本地密钥表上;

[0039] 所述边界路由器均与其直接连接的用户网关单元进行密钥协商,其具体为:边界路由器均与其直接连接的用户网关单元进行IKEv2密钥协商,得到边界路由器自身的密钥,而密钥为IPSEC密钥,所述IPSEC密钥包括SPI标识符、密钥KEY1和密钥KEY2,所述SPI标识符用于对应标记用户网关单元,每一个用户网关单元都有唯一的SPI标识符,所述密钥KEY1为加密算法密钥,所述密钥KEY2为验证算法密钥;

[0040] 例如,边界路由器A1和用户网关单元B1进行密钥协商,得到一个密钥C1,密钥C1均属于边界路由器A1和用户网关单元B1,并且密钥C1均保存于边界路由器A1的本地密钥表和用户网关单元B1的本地密钥表;密钥C1为IPSEC密钥,密钥C1包括SPI标识符、密钥KEY1和密钥KEY2;SPI标识符是用来标识密钥C1的,当一个原始报文P1使用密钥C1进行加密时,最后接收原始报文P1的目标用户网关单元就可以根据SPI标识符得到采用密钥C1即可解密原始报文P1,从而获取原始报文P1的内容信息;

[0041] 所述步骤S1还包括:在每个边界路由器与其直接连接的用户网关单元之间,使用ESP协议作为加密协议创建报文传输隧道T;

[0042] 这里的报文传输隧道T其实就是一条IP隧道,一条IP隧道会有一对IP组成,比如边界路由器A1与用户网关单元B1之间创建了一条IP隧道,假设A1的IP地址是IP_A1,B1的IP地

址是IP_B1,则当B1需要把一个原始报文C1封装后发送给A1的时候,会使用这条隧道中的IP对来创建一个新的IP头部,这个新的IP头部就是IPH_T,而IPH_T中的源IP即为发送一端的IP地址,目标IP即为对端的IP地址,这种情况下,由于是B1发送到A1,所以此时IPH_T的源IP即为IP_B1,而目的IP则为IP_A1,所以IPH_T意思是指封装时产生的一个新的IP头部,即后面的IP头部IPH_T;

[0043] 步骤S2、每个边界路由器将其自身的密钥发送给与其连接的其他边界路由器或者转发路由器;此时,为了易于与其他边界路由器进行区分,将发送密钥的边界路由器作为发送边界路由器;

[0044] 步骤S3、当其他边界路由器接收到发送边界路由器的密钥后,其他边界路由器将密钥保存至其本地密钥表上;或者,当转发路由器接收到发送边界路由器的密钥后,转发路由器则将密钥转发至与其连接的转发路由器或者边界路由器;

[0045] 步骤S4、重复步骤S2-步骤S3,直至每一个边界路由器均获取所有其他边界路由器的密钥;每一个边界路由器将所有其他边界路由器的密钥保存在其本地密钥表上,并将所有其他边界路由器的密钥发送给与其直接连接的用户网关单元,用户网关单元将所有其他边界路由器的密钥保存至其本地密钥表上;

[0046] 上述步骤S1-步骤S4,每一个用户网关单元通过密钥的相互学习以及记录,使得后面的报文P4在路由器的传输过程中无需解密加密,只需要在用户网关单元根据对应的密钥进行解密,降低路由器的负担,以及大大提高了报文的传输效率;

[0047] 步骤S5、用户网关单元接收用户(客户端)发送过来的原始报文P1,原始报文P1包括IP头IPH_C部分和载荷P_C报文内容部分,所述的IP头IPH_C部分包括这个客户端本身的IP地址和目标客户端的IP地址,用户网关单元和中间所有转发路由器都只是根据这个目标客户端的IP地址做出或者是封装或者是路由转发的动作;所述载荷P_C报文内容部分就是原始报文P1中实际要发送的数据;假设用户网关单元为用户网关单元A1,原始报文P1为原始报文P1,原始报文P1的IP头IPH_C部分用IPH_C表示,载荷P_C报文内容部分使用P_C表示,则原始报文P1为:P1＝IPH_C+P_C;

[0048] 步骤S6、用户网关单元使用自身密钥对原始报文P1进行加密,具体为:用户网关单元使用自身密钥中的密钥KEY1对载荷P_C报文内容部分进行加密得到加密报文内容ESP_PAYLOAD部分,使用密钥KEY2对加密报文内容ESP_PAYLOAD部分进行检验生成检验部分ESP_T,再生成一个ESP协议头部ESP_H,上述ESP协议头部ESP_H包括用户网关单元自身密钥中的SPI,其SPI值填写用户网关单元对应的SPI值;

[0049] 其中,ESP协议头部ESP_H作用为:由于SPI为用户网关单元的唯一标识符,对于最终接收到原始报文P1的目标用户网关单元就可以根据ESP协议头部ESP_H直接得到所发送原始报文P1的用户网关单元所属的密钥,使用此密钥来解密原始报文P1;

[0050] 用户网关单元对ESP协议头部ESP_H、加密报文内容ESP_PAYLOAD部分以及检验部分ESP_T一起进行封装得到报文P2;设报文P2为报文P2,ESP协议头部ESP_H使用ESP_H表示,加密报文内容ESP_PAYLOAD部分使用ESP_PAYLOAD表示,检验部分ESP_T使用ESP_T表示,则报文P2为:P2＝ESP_H+ESP_PAYLOAD+ESP_T;

[0051] 步骤S7、用户网关单元根据用户网关单元与边界路由器之间的报文传输隧道T,生成一个IP头部IPH_T,并将IP头部IPH_T和IP头IPH_C部分封装进去报文P2,得到报文P3,报

文P3包括IP头部IPH_T、IP头IPH_C部分以及报文P2;由上述可得IP头IPH_C部分用IPH_C表示,IP头部IPH_T使用IPH_T表示,则报文P3为:P3＝IPH_T+IPH_C+P2;

[0052] 用户网关单元将报文P3发送至与其连接的边界路由器,此时将发送报文P3的用户网关单元作为发送用户网关单元,将接收报文P3的边界路由器作为发送边界路由器;

[0053] 步骤S8、发送边界路由器接收到报文P3后,去掉报文P3的IP头部IPH_T得到报文P4,报文P4包括IP头IPH_C部分和报文P2,此时由上述可得,报文P4,P4＝IPH_C+P2;发送边界路由器根据报文P4的IP头IPH_C部分,得到接收报文P4对应的用户网关单元,将接收报文P4对应的用户网关单元称为目标用户网关单元,将与目标用户网关单元直接连接的边界路由器称为目标边界路由器;

[0054] 步骤S9、发送边界路由器将报文P4发送至目标边界路由器,具体为:

[0055] 若发送边界路由器与目标边界路由器直接连接,则发送边界路由器直接将报文P4发送至目标边界路由器;

[0056] 若发送边界路由器发送报文P4过程中需要经过若干转发路由器,则发送边界路由器首先将报文P4发送给转发路由器,转发路由器根据IP头IPH_C部分的目标IP地址将报文P4发送给下一个转发路由器,直至将报文P4发送至目标边界路由器;

[0057] 步骤S10、目标边界路由器收到报文P4后,根据目标边界路由器与目标用户网关单元之间的报文传输隧道T,生成一个新的IP头部IPH_T,并将IP头部IPH_T封装进去报文P4内,得到报文P5,并将报文P5发送至目标用户网关单元;

[0058] 步骤S11、目标用户网关单元收到报文P5后,去掉IP头部IPH_T得到报文P4;

[0059] 目标用户网关单元根据报文P4的ESP协议头部ESP_H,得到解密所需的密钥,使用密钥对报文P4进行解密,具体为:

[0060] 目标用户网关单元使用密钥KEY2对加密报文内容ESP_PAYLOAD部分进行验生成一个ESP_T校验结果,判断ESP_T校验结果与报文P4的检验部分ESP_T是否一致,若一致,则目标用户网关单元使用密钥中的密钥KEY1对报文P4的加密报文内容ESP_PAYLOAD部分进行解密得到原始报文P1的载荷P_C报文内容部分;将载荷P_C报文内容部分和报文P4的IP头IPH_C部分结合得到原始报文P1;目标用户网关单元将原始报文P1发给用户(客户端);

[0061] 若ESP_T校验结果与报文P4的检验部分ESP_T不一致,则目标用户网关单元丢弃报文P4。

[0062] 上述步骤S5-步骤S11中,通过在边界路由器和用户网关单元之间进行报文的加密,使得报文更加安全,且报文在转发路由器的传输过程中无需进行加密或解密,边界路由器和转发路由器都可以专注于报文转发,大大提高报文的传输效率以及降低路由器的负担;

[0063] 步骤S12、当添加一个新的用户网关单元后,新的用户网关单元需要连接一个边界路由器,则新的用户网关单元与边界路由器进行密钥协商,得到边界路由器自身的密钥;边界路由器将自身的密钥均发给其他边界路由器;其他边界路由器收到密钥保存至其本地密钥表上,并将密钥发送给与其直接连接的用户网关单元,用户网关单元将密钥保存至其本地密钥表上;

[0064] 与新的用户网关单元连接的边界路由器将其本地密钥表上所有密钥发送给新的用户网关单元,新的用户网关单元接收到所有密钥保存至其本地密钥表上;

[0065] 其中，边界路由器本身的密钥表就实时存放有所有其他边界路由器的密钥，所有的边界路由器都是这样，每个时刻总是同步了其他边界路由器的密钥，所以新的用户网关单元接进来的时候，被接边界路由器此时只要将此时自身的本地密钥全部发送过去就行；

[0066] 步骤S13、重复步骤S5-步骤S11。

[0067] 实施例2

[0068] 本实施是在实施例1的基础上，进行具体实例说明，如图2所示，现有一种密钥共享的组网系统，包括边界路由器A1、边界路由器A2、边界路由器A3、边界路由器A4、用户网关单元B1、用户网关单元B2、用户网关单元B3、用户网关单元B4、转发路由器C1、转发路由器C2、转发路由器C3以及转发路由器C4；其中，边界路由器A1连接用户网关单元B1和转发路由器C1，边界路由器A2连接用户网关单元B2和转发路由器C2，边界路由器A3连接用户网关单元B3和转发路由器C3，边界路由器A4连接用户网关单元B4和转发路由器C4，转发路由器C1、转发路由器C2、转发路由器C3和转发路由器C4之间两两进行连接。

[0069] 密钥共享的组网系统进行如下组网方法：

[0070] 1.密钥共享和管理

[0071] (1)用户网关单元B1向边界路由器A1发起IKEv2密钥协商，并协商出密钥C1：密钥C1包括[SPI1,KEY11,KEY12]并创建隧道T1，用户网关单元B1把密钥C1保存至本地密钥表；

[0072] (2)边界路由器A1查询本地密钥表把已存在密钥发给用户网关单元B1，此时边界路由器A1的本地密钥表为空，所以不需要发送；

[0073] (3)边界路由器A1把密钥C1保存至本地密钥表，并把密钥C1通过一般路由器分发至边界路由器A2、边界路由器A3和边界路由器A4；

[0074] (4)其他边界路由器把密钥C1保存至本地密钥表；

[0075] (5)用户网关单元B2向边界路由器A2发起IKEv2密钥协商，并协商出密钥C2：密钥C2包括[SPI2,KEY21,KEY22]并创建隧道T2，用户网关单元B2把密钥C2保存至本地密钥表；

[0076] (6)边界路由器A2查询本地密钥表，把已存在的密钥C1通过T2发送至用户网关单元B 2，用户网关单元B 2收到后保存至本地密钥表；

[0077] (7)边界路由器A2把密钥C2保存至本地密钥表，并把密钥C2通过一般路由器分发至其他边界路由器；

[0078] (8)边界路由器A1收到密钥C2后，通过隧道T1发送至用户网关单元B1，用户网关单元B1把密钥C2保存至本地密钥表；

[0079] (9)其他边界路由器收到密钥C2后保存至本地密钥表

[0080] (10)用户网关单元B 3和用户网关单元B4接入的过程以此类推，直至全部用户网关单元接入，并且每个用户网关单元的本地密钥表都拥有全部用户网关单元的密钥；

[0081] 2.路由学习

[0082] (1)边界路由器和转发路由器之间运行OSPF协议；

[0083] (2)通过OSPF协议，每个边界路由器和转发路由器学习到每个用户网关所接的网段；

[0084] 3.报文封装转发

[0085] (1)用户网关1接收到报文C1

[0086] ①SIP:10.10.1.100,DIP:10.10.2.100,PAYLOAD

[0087] (2)用户网关单元B1使用密钥C1加密PAYLOAD,变成ESP_P1

[0088] (3)把ESP_P1封装在隧道T1中,然后把原SIP,DIP所属IP头,完整的放在T1的新IP头中的扩展部分,并发至边界路由器A1

[0089] (4)边界路由器A1接收到报文后,去掉T1中的IP头,恢复成原IP头+ESP_P1组成的报文,并查找本地路由发送至转发路由器

[0090] (5)转发路由器收到报文后,查找路由并转发至其他转发路由器或者其他边界路由器;

[0091] (6)报文到达边界路由器A2后,根据IP头DIP所知报文是发送给用户网关单元B2的,边界路由器A2用T2重新封装,把报文的原IP头继续放在新的IP头扩展部分,并发至用户网关单元B2

[0092] (7)用户网关单元B2收到报文后,去掉T2的IP头,通过ESP头部的SPI1查找本地密钥表,并使用密钥C1解密报文,结合原IP头,恢复成原来的整个报文,并最终发至用户。

[0093] 尽管已经示出和描述了本发明的实施例,对于本领域的普通技术人员而言,可以理解的是,在不脱离本发明的原理和精神的情况下可以对这些实施例进行多种等效的变化、修改、替换和变型,本发明的范围由所附权利要求及其等同范围限定。

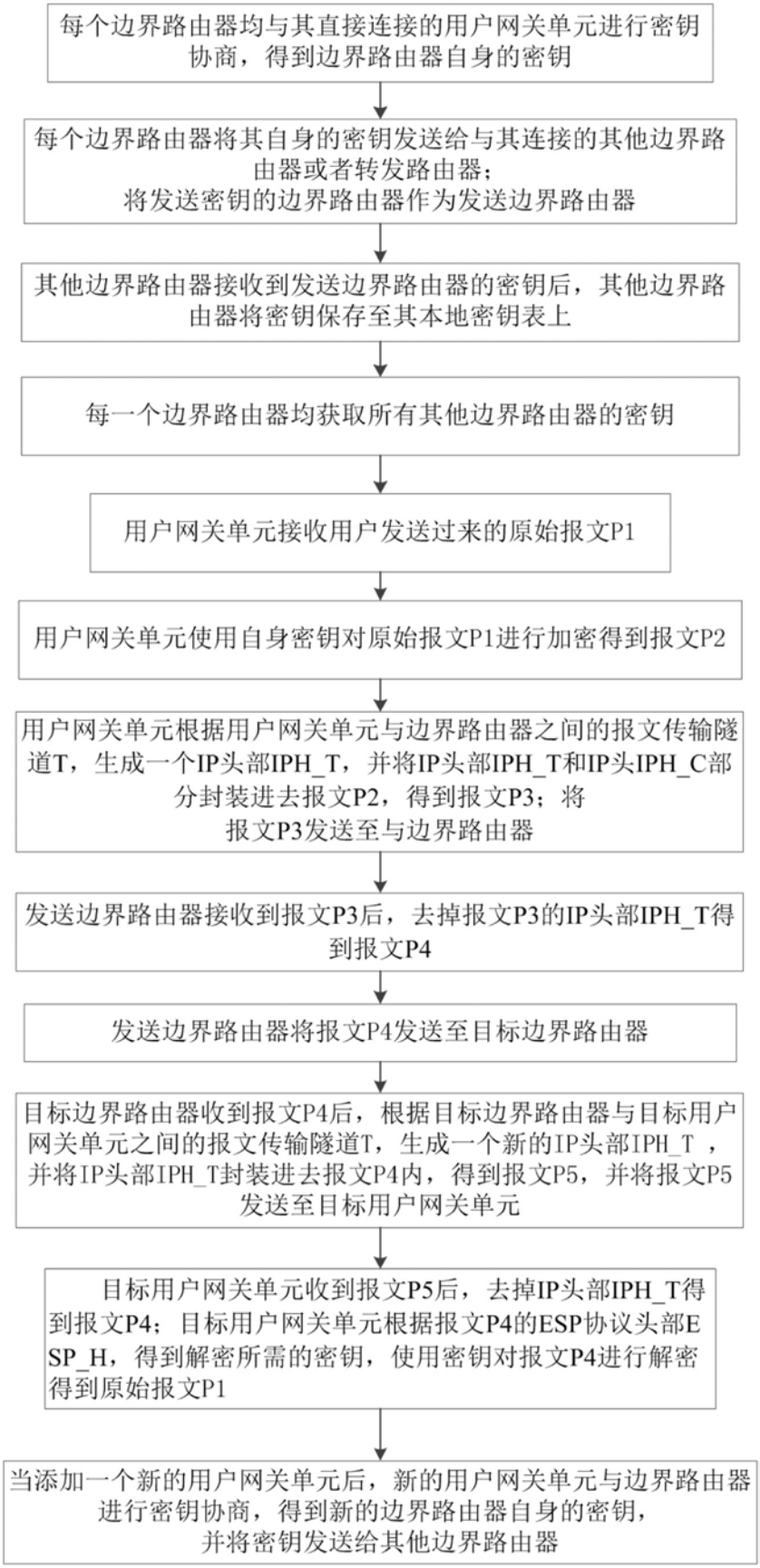

每个边界路由器均与其直接连接的用户网关单元进行密钥协商，得到边界路由器自身的密钥
每个边界路由器将其自身的密钥发送给与其连接的其他边界路由器或者转发路由器；
将发送密钥的边界路由器作为发送边界路由器
其他边界路由器接收到发送边界路由器的密钥后，其他边界路由器将密钥保存至其本地密钥表上
每一个边界路由器均获取所有其他边界路由器的密钥
用户网关单元接收用户发送过来的原始报文P1
用户网关单元使用自身密钥对原始报文P1进行加密得到报文P2
用户网关单元根据用户网关单元与边界路由器之间的报文传输隧道T，生成一个IP头部IPH_T，并将IP头部IPH_T和IP头IPH_C部分封装进去报文P2，得到报文P3；将
报文P3发送至与边界路由器
发送边界路由器接收到报文P3后，去掉报文P3的IP头部IPH_T得到报文P4
发送边界路由器将报文P4发送至目标边界路由器
目标边界路由器收到报文P4后，根据目标边界路由器与目标用户网关单元之间的报文传输隧道T，生成一个新的IP头部IPH_T ，并将IP头部IPH_T封装进去报文P4内，得到报文P5，并将报文P5发送至目标用户网关单元
目标用户网关单元收到报文P5后，去掉IP头部IPH_T得到报文P4；目标用户网关单元根据报文P4的ESP协议头部ESP_H，得到解密所需的密钥，使用密钥对报文P4进行解密得到原始报文P1
当添加一个新的用户网关单元后，新的用户网关单元与边界路由器进行密钥协商，得到新的边界路由器自身的密钥，
并将密钥发送给其他边界路由器

图1

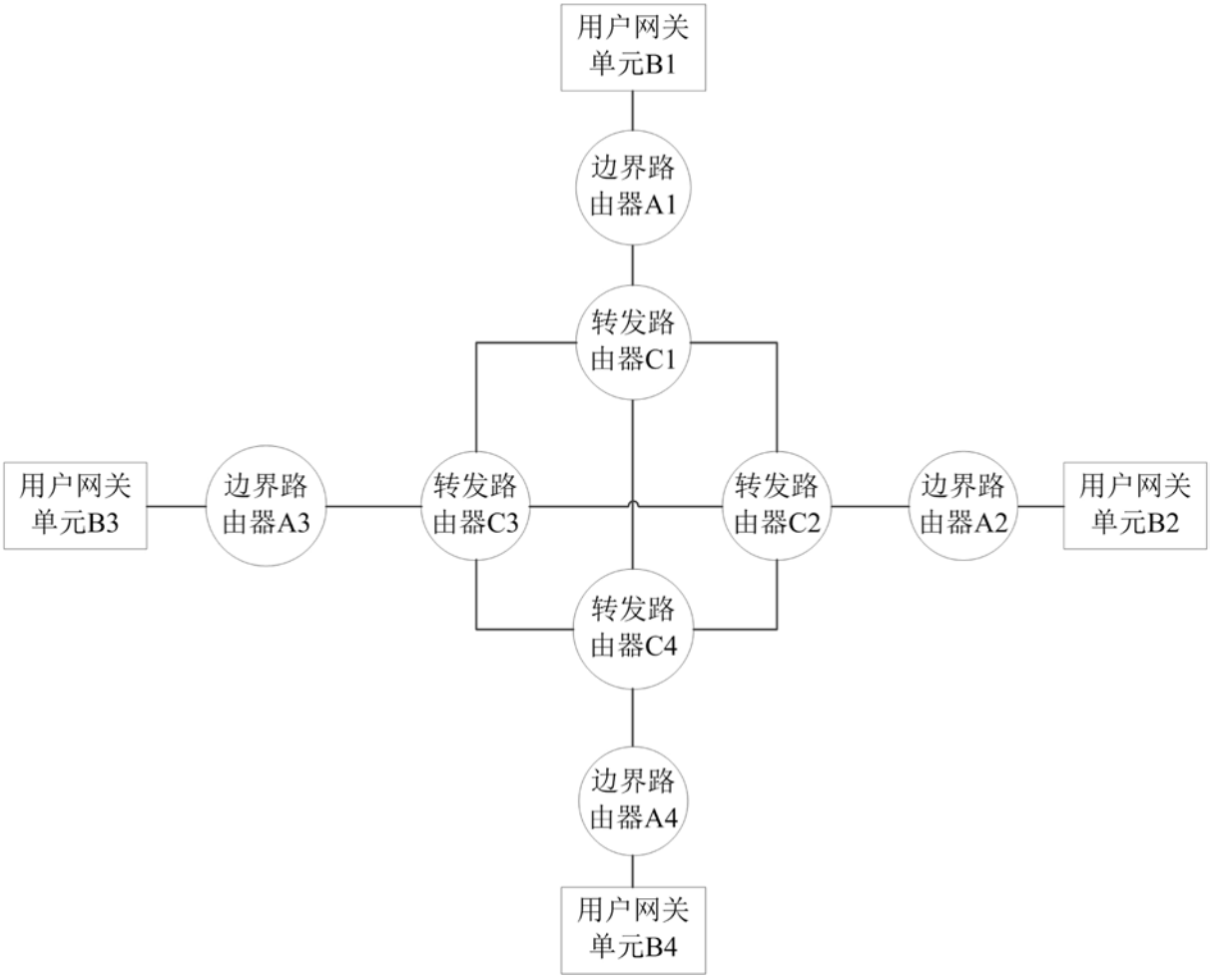

用户网关
单元B1
边界路
由器A1
转发路
由器C1
用户网关
单元B3
边界路
由器A3
转发路
由器C3
转发路
由器C2
边界路
由器A2
用户网关
单元B2
转发路
由器C4
边界路
由器A4
用户网关
单元B4

图2